udv|group

UDV DATAPK Industrial Kit

Руководство по эксплуатации

Версия 3.0.0.0

udv.group | support@udv.group

Содержание

1. Глоссарий ... 12

2. Введение ... 25

3. Что нового? ... 26

3.1. Изменения в Руководстве по эксплуатации ... 34

4. Условные обозначения ... 35

5. Общие сведения о Комплексе ... 36

6. Логическая структура комплекса и режимы функционирования ... 37

7. Сведения о сертификатах ... 39

8. Разделение функций по администрированию ... 40

9. Первичная настройка ... 42

9.1. Первичное подключение ... 42

9.1.1. Подключение к веб-интерфейсу по протоколу HTTPS ... 42

9.1.2. Первоначальная настройка ... 45

9.2. Настройка локальных реквизитов и контролируемой сети ... 47

9.2.1. Изменение сведений о Комплексе и сенсорах ... 47

9.2.2. Настройка контролируемой сети ... 49

9.3. Настройка парольной политики ... 52

9.4. Импорт справочников из архива ... 53

9.5. Запуск обнаружения вторжений и синхронизация правил с сенсорами ... 55

9.6. Первичная настройка модуля «Анализ промышленного сетевого трафика» ... 56

9.7. Проверка работоспособности Комплекса ... 60

9.7.1. Проверка работоспособности системы передачи данных по иерархии ... 60

9.7.2. Проверка обнаружения активов из контролируемой сети ... 61

9.7.3. Проверка работоспособности модуля «Анализ промышленного сетевого трафика» ... 61

10. Мониторинг событий ... 63

10.1. Поиск и просмотр событий в упрощенном режиме ... 66

10.2. Просмотр событий и создание запросов в экспертном режиме ... 72

10.3. Просмотр главной панели мониторинга «Статус защищенности» ... 75

10.4. Импортируемые панели мониторинга ... 78

10.4.1. Принцип работы с мониторингом ... 79

10.4.2. Действия в случае обнаружения событий в панели мониторинга ... 79

10.4.3. Создание фильтров на панелях мониторинга ... 79

10.4.4. Выбор периода отображения событий на панели мониторинга ... 81

10.4.5. Главный дашборд ... 83

10.4.6. Информационные панели....104
10.4.7. Экспорт событий из панели мониторинга....107
10.4.8. Панели мониторинга модуля «EDR for PLC»....107
10.5. Настройка сбора событий....108
10.5.1. Экспорт и импорт правил нормализации событий....109
10.5.2. Экспорт и импорт источников событий....110
10.5.3. Включение и отключение служебных источников....111
10.5.4. Создание источника событий....113
10.5.5. Управление источниками событий....114
10.5.6. Выгрузка внешних событий Комплекса в архив....115
10.5.7. Настройка отправки внутренних событий во внешнюю систему по протоколу Syslog....116
10.5.8. Настройка отправки событий во внешнюю систему по протоколу Syslog при установленном модуле «Управление внешними событиями»....118
10.6. Настройка и управление мониторингом....120
10.6.1. Создание шаблона индекса....121
10.6.2. Удаление шаблона индекса....123
10.6.3. Создание и настройка виджета....124
10.6.4. Просмотр и управление виджетами....126
10.6.5. Создание и настройка панели мониторинга....127
10.6.6. Настройка пользовательских правил нормализации событий....130
10.6.7. Настройка форматирования чисел и дат в разделе «Мониторинг»....131
10.6.8. Экспорт и импорт объектов раздела «Мониторинг»....132
11. Работа с инцидентами....138
11.1. Поиск инцидентов....139
11.2. Анализ инцидентов....142
11.3. Изменение параметров инцидентов....145
11.4. Удаление инцидентов....151
11.5. Групповые операции над инцидентами....152
11.6. Настройка инцидентов....153
11.6.1. Экспорт и импорт политики корреляции....155
11.6.2. Экспорт и импорт статусов инцидентов....160
11.6.3. Управление службой корреляции событий....161
11.6.4. Управление схемой корреляции....162
11.6.5. Управление правилами корреляции событий....166
11.6.6. Анализ событий для генерации инцидентов....171
11.6.7. Настройка оповещений при появлении инцидентов....177

11.6.8. Управление статусами инцидентов ... 185
11.6.9. Управление внутренними правилами корреляции событий ... 187
11.7. Выгрузка отчета по инцидентам ... 188
12. Работа с активами ... 190
12.1. Экспорт и импорт активов и их групп ... 192
12.1.1. Экспорт активов ... 193
12.1.2. Экспорт групп активов ... 193
12.1.3. Импорт активов ... 194
12.1.4. Импорт групп активов ... 195
12.2. Управление активами ... 195
12.2.1. Кнопки управления активами ... 196
12.2.2. Фильтрация списка активов ... 197
12.3. Создание актива ... 200
12.4. Группировка активов ... 201
12.4.1. Создание группы активов ... 202
12.4.2. Добавление активов в группу ... 203
12.4.3. Управление группами активов ... 205
12.5. Редактирование актива ... 207
12.6. Удаление активов ... 214
12.7. Выгрузка отчета по активам ... 217
12.8. Настройки активов ... 218
12.8.1. Настройка учетных данных активов ... 219
12.8.2. Настройка классификаторов ... 225
13. Активный сбор данных с активов ... 234
13.1. Просмотр сводки конфигураций ... 235
13.2. Настройка сбора конфигураций активов ... 236
13.2.1. Экспорт и импорт задач сбора данных, сканеров и их групп ... 237
13.2.2. Настройка сканеров сбора данных ... 240
13.2.3. Сбор данных с активов ... 253
13.2.4. Просмотр статуса сбора данных ... 263
13.2.5. Работа с архивом изменений конфигурации актива ... 267
13.2.6. Добавление сетевых атрибутов активу с помощью сканера сбора данных по SNMP ... 274
13.2.7. Цифровая подпись Python-скрипта ... 276
13.3. Настройка активного сбора событий ... 277
13.4. Настройка сбора данных об операционной системе и установленном ПО ... 278
13.4.1. Запуск сбора данных об операционной системе и установленном ПО ... 280

14. Поиск уязвимостей и проверка соответствия требованиям информационной безопасности..... 282

14.1. Поиск уязвимостей ПО и ОС в базах CVE, CPE и БДУ ФСТЭК России.....283

14.1.1. Проверка актуальности справочников поиска уязвимостей.....285

14.1.2. Импорт справочников CVE и CPE и файла сопоставления ПО с CPE.....286

14.1.3. Импорт справочника БДУ ФСТЭК России.....287

14.1.4. Запуск поиска уязвимостей в базах CVE, CPE и БДУ ФСТЭК России.....287

14.1.5. Выгрузка отчета по результатам сопоставления собранного ПО со справочником CPE..... 291

14.2. Проверки на уязвимости и соответствие требованиям информационной безопасности с помощью OVAL.....292

14.2.1. Импорт и экспорт скриптов, настроек, групп определений OVAL.....295

14.2.2. Настройка OVAL-проверки актива на соответствие требованиям информационной безопасности.....301

14.2.3. Запуск OVAL-проверки актива на соответствие требованиям информационной безопасности...310

14.2.4. Просмотр и выгрузка результатов проверки актива на соответствие требованиям информационной безопасности.....312

14.2.5. Повторный запуск OVAL-проверки на соответствие требованиям ИБ.....314

14.2.6. Удаление OVAL-проверок актива на соответствие требованиям информационной безопасности.....315

15. Анализ промышленного сетевого трафика.....316

15.1. Просмотр карты сети..... 318

15.2. Настройка представлений на карте..... 322

15.3. Управление сетевыми соединениями.....326

15.3.1. Просмотр сессий и пакетов..... 326

15.3.2. Поиск по списку сессий..... 331

15.3.3. Фильтрация списка сессий.....333

15.3.4. Экспорт копии сетевого трафика.....334

15.3.5. Экспорт файлов, обнаруженных в сетевом трафике.....336

15.4. Правила сессий..... 339

15.4.1. Просмотр правил сессий..... 340

15.4.2. Управление правилами сессий.....344

15.5. Правила контроля тегов..... 359

15.5.1. Просмотр правил контроля тегов..... 359

15.5.2. Управление правилами контроля тегов.....363

15.6. Контроль критичных функций технологического процесса..... 370

15.6.1. Управление сервисом регистрации событий техпроцесса..... 370

15.6.2. Изменение списка критичных функций.....371

15.7. Служба обнаружения вторжений..... 372

15.7.1. Создание правил обнаружения вторжений....375
15.7.2. Управление службой обнаружения вторжений....376
15.7.3. Экспорт и импорт правил службы обнаружения вторжения....379
15.7.4. Создание исключений для правил обнаружения вторжений....384
15.7.5. Удаление исключений для правил обнаружения вторжений....388
16. Управление проектами ПЛК....390
16.1. Version Control Management....390
16.2. Version Control Desktop App....390
16.2.1. Системные требования....390
16.2.2. Вход в систему Version Control Desktop App....391
16.2.3. Использование Version Control Desktop App по назначению....394
17. Управление модулем обнаружения и реагирования для ПЛК («EDR for PLC»)....451
17.1. Выполнение операций с моделями....452
17.1.1. Получение списка всех моделей....452
17.1.2. Перевод всех моделей в режим детектирования аномалий....455
17.1.3. Перевод определенной модели в режим детектирования аномалий....455
17.1.4. Удаление модели....456
17.1.5. Постановка модели на паузу....457
17.1.6. Продолжение функционирования модели....457
17.1.7. Повторное обучение модели....458
17.1.8. Принудительный расчет маски для всех моделей....458
17.1.9. Принудительный расчет маски для определенной модели....458
17.1.10. Просмотр информации о модели на основе иерархического словаря....459
17.1.11. Просмотр информации о модели на основе временного автомата....461
17.1.12. Просмотр информации о модели на основе гибридного автомата....464
17.1.13. Запуск дообучения для модели на основе временного автомата....466
17.1.14. Запуск дообучения модели на основе иерархического словаря....468
17.1.15. Экспорт модели на основе гибридного автомата....469
17.1.16. Получение информации об элементах словаря моделей по идентификатору....470
17.2. Получение информации об адресах по идентификаторам....472
17.3. Получение информации о сетевом узле по идентификатору....473
17.4. Получение списка сетевых узлов модуля «EDR for PLC»....474
17.5. Просмотр статистики по разбору сетевого трафика модулем «EDR for PLC»....475
17.6. Просмотр статуса активности формирования немодельных аномалий....477
17.7. Включение/отключение создания немодельных аномалий....477
17.8. Возможные ошибки API модуля «EDR for PLC»....478

18. Управление Комплексом ... 479
18.1. Изменение сведений о Комплексе и сенсорах ... 479
18.2. Сканирование сети и определение интерфейсов активного сетевого оборудования ... 480
18.2.1. Интерпретация результатов пассивного сканирования сети ... 482
18.3. Настройка контролируемой сети ... 482
18.4. Управление пользователями ... 484
18.4.1. Управление учетными записями пользователей ... 492
18.4.2. Настройка парольной политики ... 498
18.4.3. Отключение ограничения на количество сессий пользователей ... 500
18.5. Экспорт отдельных справочников ... 500
18.6. Диагностика состояния системы Комплекса ... 501
18.7. Диагностика состояния сенсора ... 503
18.8. Удаление сенсора ... 504
19. Интеграция Комплекса с другими системами ... 506
19.1. Интеграция Комплекса с ПО InfoWatch ARMA Industrial Firewall ... 506
19.1.1. Предварительная настройка взаимодействия с ПО InfoWatch ARMA Industrial Firewall ... 506
19.1.2. Сбор событий ПО InfoWatch ARMA Industrial Firewall ... 508
19.1.3. Сбор конфигураций ПО InfoWatch ARMA Industrial Firewall по протоколу SSH ... 509
19.1.4. Сбор конфигураций ПО InfoWatch ARMA Industrial Firewall по протоколу SNMP ... 511
19.2. Работа с REST API Комплекса ... 513
19.2.1. Установка Swagger UI ... 513
19.2.2. Конечные точки REST API Комплекса ... 516
20. Регламентные работы ... 621
20.1. Резервное копирование данных ... 621
20.1.1. Резервное копирование рабочей директории и данных Комплекса уровня Management ... 622
20.1.2. Резервное копирование Комплекса уровня Sensor ... 625
20.1.3. Выгрузка внешних событий Комплекса в архив ... 625
20.1.4. Экспорт отдельных справочников ... 626
20.1.5. Экспорт нескольких справочников ... 628
20.2. Смена паролей ... 629
20.2.1. Смена пароля системной учетной записи администратора ... 629
20.2.2. Смена пароля учетной записи в веб-интерфейсе Комплекса ... 630
20.3. Удаление данных Комплекса ... 630
20.4. Очистка дискового пространства от внутренних событий ... 630
21. Нештатные ситуации и действия по их устранению ... 633
21.1. Диагностика сервисов и иерархии ... 633

21.2. Действия по восстановлению комплекса при сбойных ситуациях и ошибках в данных....634
21.2.1. Веб-интерфейс не загружается.... 634
21.2.2. Время на Комплексе отличается от времени получения события.... 637
21.2.3. После запуска Комплекса при попытке загрузки веб-интерфейса открывается пустая страница....638
21.2.4. 502-я ошибка при загрузке страницы авторизации, 500-е ошибки сразу после авторизации....639
21.2.5. Не обнаруживаются новые сессии.... 640
21.2.6. Комплекс не обнаруживает активы в автоматическом режиме.... 642
21.2.7. Два актива с одинаковым IP-адресом....644
21.2.8. Не осуществляется сбор необходимых событий или конфигураций с активов.... 645
21.2.9. При попытке сбора данных в результатах выводится предупреждение «Превышено время ожидания выполнения задачи сбора событий».... 647
21.2.10. Сбор конфигураций осуществляется, но результаты сбора не отображаются....648
21.2.11. Отсутствуют внутренние события на странице «События»....649
21.2.12. Отсутствуют внешние события на странице «События».... 649
21.2.13. Не принимаются Syslog-сообщения от активов....651
21.2.14. Не принимаются сообщения от службы обнаружения вторжений....652
21.2.15. Не принимаются сообщения от службы корреляции....652
21.2.16. Не инициализируются сервисы udv-opensearch, udv-opensearch-dashboards, udv-logstash модуля «Управление внешними событиями» 653
21.2.17. Не создается индекс в экспертном режиме страницы «События».... 654
21.2.18. Не удается отфильтровать записи в экспертном режиме страницы «События» по новым значениям полей после нормализации....655
21.2.19. Объекты мониторинга и визуализации импортируются с ошибкой....655
21.2.20. Не удается импортировать сканер сбора данных в веб-интерфейсе.... 655
21.2.21. Не выполняется архивация внешних событий при превышении размера или времени хранения индекса....657
21.2.22. Ошибки вида «<...>Cannot start service <...>. Bind for <ip_address>:<TCP/UDP_port> is ready allocated» при попытке запуска сервисов....658
21.2.23. При бездействии в веб-интерфейсе сеанс завершается раньше, чем через 10 минут....658
21.2.24. Ошибки поиска уязвимостей в базах CVE, CPE и БДУ ФСТЭК России.... 659
21.2.25. Не устанавливается соединение с сенсором.... 661
21.2.26. Не работает сложное исключение для правила службы обнаружения вторжений....664
21.2.27. Обнаружен конфликт версий проектов ПЛК....664
21.2.28. Каталог проекта ПЛК содержит информацию других файлов.... 665
21.2.29. Путь к файлу превышает допустимую длину.... 666
21.3. Восстановление данных из резервных копий....667

21.3.1. Восстановление данных из резервных копий Комплекса уровня Management и Комплекса уровня Management+Sensor ... 668
21.3.2. Восстановление данных из резервных копий Комплекса уровня Sensor ... 670
21.4. Действия в случаях несанкционированного доступа к данным ... 671
21.4.1. Просмотр журнала действий пользователей Комплекса ... 671
21.4.2. Изменение статуса активности учетной записи пользователя Комплекса ... 672
21.5. Действия в других аварийных ситуациях ... 672
21.6. Анкета при обращении в сервисный центр ... 673
21.7. Диагностика сервиса сбора данных по протоколам SSH, Telnet, WinRM, winexe ... 678
22. Справочная информация ... 680
22.1. Архитектура UDV DATAPK Industrial Kit ... 680
22.1.1. Список модулей UDV DATAPK Industrial Kit ... 683
22.1.2. Интерфейс Комплекса ... 684
22.1.3. Дополнительные функции Комплекса ... 751
22.2. Условия эксплуатации Комплекса ... 760
22.3. Описание источников событий ... 760
22.3.1. Описание служебных источников событий ... 761
22.3.2. Описание безагентного сбора событий Eventlog ... 764
22.4. Описание полей событий в экспертном режиме страницы «События» ... 766
22.5. Переменные Комплекса ... 769
22.5.1. Переменные Комплекса уровня Management ... 770
22.5.2. Переменные Комплекса уровня Sensor ... 786
22.5.3. Переменные Комплекса уровня Supervision ... 791
22.5.4. Переменные службы обнаружения вторжений ... 793
22.5.5. Конфигурационные файлы модуля «EDR for PLC» ... 796
22.5.6. Рекомендации по использованию переменных файлов manager.env и sensor.env ... 802
22.6. События Комплекса ... 803
22.7. Механизмы хранения событий ... 874
22.8. Отправка внутренних событий по протоколу Syslog ... 875
22.9. Перечень данных, собираемых Комплексом с помощью сканеров ... 876
22.10. Работа с импортируемыми панелями мониторинга ... 884
22.10.1. Навигация в разделах мониторинга ... 885
22.10.2. Средства управления панелями мониторинга ... 885
22.10.3. Элементы управления интерфейсом визуализации ... 887
22.10.4. Диаграммы и таблицы на панелях мониторинга ... 888
22.11. Рекомендации по настройке сбора данных ... 893

22.12. Определение максимально допустимого количества активов сбора данных ... 893
22.13. Содержание Python-скриптов ... 894
22.14. Перечень SCADA, с которых поддерживается сбор данных ... 895
22.15. Реестр сканеров Комплекса ... 895
22.16. Сетевые взаимодействия Комплексов ... 946
22.17. Поддерживаемые типы событий ... 950
22.17.1. Поля внутренних событий Комплекса ... 950
22.17.2. Поля событий KICS4Net ... 958
22.17.3. Поля событий Linux ... 959
22.17.4. Поля событий Cisco ... 959
22.17.5. Поля событий RuggedCOM ... 960
22.17.6. Поля событий Eltex ... 961
22.17.7. Поля событий FortiGate ... 961
22.17.8. Поля событий Hirschmann ... 962
22.17.9. Поля событий Enterasys ... 963
22.17.10. Поля событий Windows ... 963
22.17.11. Поля событий SNMP ... 964
22.17.12. Поля событий Syslog ... 964
22.18. Синтаксис правил корреляции событий ... 964
22.18.1. Ключевые поля событий для создания правил корреляции ... 966
22.18.2. Фильтр событий ... 966
22.18.3. Временное окно ... 966
22.18.4. Группировка ... 967
22.18.5. Условие инцидента ... 968
22.18.6. Шаблоны обработки сложных событий ... 968
22.18.7. Сообщение инцидента ... 970
22.18.8. Приоритет и активность правил ... 970
22.19. Список внутренних правил корреляции событий ... 971
22.20. Отображение времени в Комплексе ... 976
22.21. Структура директорий Комплекса ... 976
22.22. Работа с контрольными суммами исполняемых файлов сертифицированного Комплекса ... 978
22.22.1. Создание эталонных контрольных сумм исполняемых файлов Комплекса вручную ... 980
22.22.2. Проверка контрольных сумм исполняемых файлов Комплекса вручную ... 981
22.23. Справочная информация о модуле «Анализ промышленного сетевого трафика» ... 982
22.23.1. Переменные файла белого списка ... 983
22.23.2. Возможные состояния сессий ... 993

22.23.3. Поддерживаемые протоколы передачи данных....994
22.23.4. Поддерживаемые функции промышленных протоколов....1002
22.23.5. Детектируемые тактики и техники атак....1010
22.24. Справочная информация о модуле «Управление проектами ПЛК»....1012
22.24.1. Общая информация о модуле «Управление проектами ПЛК»....1012
22.24.2. Статусы репозиториев....1015
22.24.3. Системные журналы Version Control Desktop App....1017
22.24.4. Шаблоны для настройки исключений....1017
22.25. Справочная информация о модуле «EDR for PLC»....1020
22.25.1. Общие сведения о модуле «EDR for PLC»....1020
22.25.2. Типы моделей модуля «EDR for PLC»....1020
22.26. Справочная информация о компоненте Supervision....1027
22.26.1. Статусы компонентов Management....1028
22.26.2. Роли пользователей Supervision....1036

1. Глоссарий

1.1. Автоматизированная система

Автоматизированная система (АС) — система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

Аббревиатура: АС

1.2. Актив

Актив — сетевой узел, подлежащий защите от потенциальных угроз и неправомерных действий, например несанкционированного доступа и изменения данных третьими лицами.

Аббревиатура: Актив

1.3. Активная и неактивная модель

Активная модель — модель в рамках модуля UDV DATAPK EDR for PLC, которая находится на любом этапе, кроме паузы.

Неактивная модель — модель в рамках модуля UDV DATAPK EDR for PLC, которая находится на паузе.

1.4. Автоматизированная система управления производственными и технологическими процессами

Автоматизированная система управления производственными и технологическими процессами — группа решений технических и программных средств, предназначенных для автоматизации управления технологическим оборудованием на промышленных предприятиях.

Аббревиатура: АСУ ТП

Синонимы: Автоматизированная система управления производственно-технологическим комплексом

Аббревиатура: АСУ ПТК

1.5. Банк данных угроз безопасности информации ФСТЭК России

Банк данных угроз безопасности информации ФСТЭК России (БДУ ФСТЭК России) — база данных уязвимостей, созданная ФСТЭК России. Содержит сведения об основных угрозах безопасности информации и уязвимостях, в первую очередь, характерных для государственных информационных систем и автоматизированных систем управления производственными и технологическими процессами критически важных объектов.

Аббревиатура: БДУ ФСТЭК России

1.6. Бесклассовая адресация

Бесклассовая адресация (англ. Classless Inter-Domain Routing) — метод IP-адресации, позволяющий гибко управлять пространством IP-адресов, не используя жёсткие рамки классовой адресации.

Аббревиатура: CIDR

1.7. Виджет

Виджет (визуализация) — представление информации о событиях в виде, удобном для зрительного наблюдения и анализа.

1.8. Глобальная сеть

Глобальная сеть — совокупность сетевых узлов за пределами локальной и контролируемой сетей.

См. также

Просмотр карты сети

1.9. Группа объектов

Группа объектов — группа репозиториев, объединенная по каким-либо признакам.

1.10. Децентрализованное управление

Децентрализованное управление — модель управления решением, при выборе которой для каждого Менеджмента можно устанавливать локальные наборы пользователей и ролей, а также парольные политики. Активируется по умолчанию.

1.11. Дообучение модели

Дообучение модели — процесс передачи в модель набора данных в специальном формате с использованием интерфейса API с целью расширения представления модели о допустимом сетевом взаимодействии.

1.12. «Жадный» фильтр

«Жадный» фильтр — правило с избыточно общими условиями, которое срабатывает на нерелевантных событиях. Например:

- поиск ключевого слова `error` без уточнения источника;
- поиск IP-адреса в сообщении без проверки типа события.

1.13. Задача сбора данных

Сущность, позволяющая при помощи групп сканеров собирать конфигурации и события с активов и их групп, в том числе с использованием расписания cron.

1.14. Индекс событий

Индекс событий — совокупность событий за сутки.

1.15. Информационная безопасность

Информационная безопасность — состояние информационной системы, при котором она наименее восприимчива к вмешательству и нанесению ущерба со стороны третьих лиц. Безопасность данных также подразумевает управление рисками, которые связаны с разглашением информации или влиянием на аппаратные и программные модули защиты.

Аббревиатура: ИБ

1.16. Источник событий

Источник событий — объект или сервис от которого поступают события.

1.17. Карта сети

Карта сети — модель, описывающая состав вычислительной сети предприятия: узлы и сессии между узлами на сетевом и канальном уровнях.

1.18. Классификатор

Классификатор — сгруппированный по различным признакам перечень наименованных объектов, где каждому из них присвоен уникальный код в соответствии с их общими признаками или различиями.

1.19. Компонент

Автономная часть в составе всего решения UDV DATAPK Industrial Kit, устанавливаемая на определенном физическом или сетевом уровне инфраструктуры предприятия с АСУ ТП (технологическом комплексе, филиале или верхнем уровне всего предприятия) для выполнения отдельного набора функций на этом уровне (сбора, анализа и визуализации данных). Для обеспечения максимальной заявленной киберзащиты АСУ ТП средствами UDV DATAPK компоненты на одном предприятии необходимо настроить для взаимодействия друг с другом по сети. UDV DATAPK содержит три компонента:

- Management;
- Sensor;
- Supervision.

См. также

Модуль

Сервис

1.20. Конечная точка

Конечная точка — это конкретный URL-адрес или путь, по которому клиентское приложение может отправлять запросы к API для взаимодействия с сервером и получения данных или выполнения определенных действий.

1.21. Контролируемая сеть

Контролируемая сеть — список подсетей, настраиваемый вручную на странице **Сенсоры**. Узлы этих подсетей автоматически обнаруживаются ом как контролируемые активы. Взаимодействие контролируемой сети с локальной сетью регистрируется как событие, с глобальной сетью — как инцидент.

См. также

Просмотр карты сети

Настройка контролируемой сети

1.22. Конфигурация актива

Конфигурация актива — набор параметров актива, связанных с состоянием информационной безопасности. Как правило, каждому набору параметров соответствует своя конфигурация. Например, для ПЛК Siemens могут проверяться конфигурации по протоколу snap 7 на соответствие эталонным настройкам системы, ее версии и контрольным суммам блоков.

1.23. Корреляция

Корреляция — способность системы выявлять неочевидные закономерности в событиях и формировать инциденты на их основе.

1.24. Локальная сеть

Локальная сеть — список подсетей, зарезервированных для локального использования.

1.25. Локальная учетная запись

Учетная запись пользователя на компьютере, которая хранится только на одном конкретном устройстве и не синхронизируется с другими устройствами или серверами. Она используется для входа в систему и управления правами доступа локально.

1.26. Маска данных модели

Маска данных модели — механизм дополнительной фильтрации данных, поступающих в модели на основе временного автомата и иерархического словаря для протокола CIP. Основным предназначением маски является фильтрация данных с высокой энтропией (как правило это могут быть случайные данные или шум). Для каждой модели конфигурация маски и ее расчет выполняются индивидуально.

1.27. Метрики

Метрики — это количественные показатели, которые собираются и формируются в системе для оценки ее производительности и общего состояния, отслеживания процессов. Анализ метрик позволяет принимать обоснованные решения по развитию и оптимизации системы.

1.28. Модель

Модель — объект, формируемый в рамках модуля UDV DATAPK EDR for PLC различными методами машинного обучения. Модель формируется с целью выявления каких-либо закономерностей и позволяющий генерировать прогноз поведения сетевого взаимодействия двух конечных точек.

1.29. Модуль

Отдельный набор функциональностей Комплекса, объединенных по принципу решения одной группы задач (например, контроль версий ПЛК или анализ сетевого трафика) или удовлетворения одной группе функций безопасности. Отсутствие модуля в комплекте поставки Комплекса не влияет на работоспособность других поставляемых модулей (за исключением некоторых модулей — подробнее см. раздел «Список модулей UDV DATAPK Industrial Kit» Руководства по внедрению и поддержке). Каждый модуль приобретается отдельно. Модуль `Core` является базовым и обязательным для всех остальных модулей.

1.30. Немодельные аномалии

Немодельные аномалии — аномалии, которые формируются без участия набора моделей, анализирующих сетевое взаимодействие контроллера с другими устройствами, на этапе разбора трафика, формирования адресной иерархии или словаря сигналов.

1.31. Неразрешенная сессия

Неразрешенная сессия — входящее соединение, зарегистрированное Комплексом в контролируемой сети, и признанное нелегитимным согласно правилам сессий.

1.32. Несанкционированный доступ

Несанкционированный доступ (НСД) — доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами.

Внимание:

Под штатными средствами понимается совокупность программного, микропрограммного и технического обеспечения средств вычислительной техники или автоматизированных систем.

Аббревиатура: НСД

1.33. Нормализация событий

Нормализация событий — приведение событий из разных источников к единому формату, принятому в Комплексе.

1.34. Операционная система

Операционная система (ОС) — комплекс взаимосвязанных программ, предназначенных для управления ресурсами компьютера и организации взаимодействия с пользователем.

Аббревиатура: ОС

1.35. Панель мониторинга

Панель мониторинга — тип графического интерфейса, использующий интерактивные визуализации для обзора ключевых показателей.

Синонимы: Dashboard

1.36. Программируемый логический контроллер

Программируемый логический контроллер (ПЛК) — унифицированная цифровая управляющая электронная система, специально разработанная для использования в производственных условиях.

Аббревиатура: ПЛК

1.37. Политика корреляции событий

Политика корреляции событий — справочник, который содержит схему и правила корреляции.

1.38. Политика хранения

Политика хранения — перечень правил, определяющих сроки, условия и методы хранения данных в системе.

1.39. Правила корреляции событий

Правила корреляции событий — набор команд, которые оперируют событиями из разных источников и выдают на основе их анализа инциденты. На основе инцидентов могут быть сформированы уведомления, которые отправляются инженеру информационной безопасности или другим сотрудникам.

1.40. Программно-техническое средство

Программно-техническое средство (ПТС) — комплексное решение, состоящее из программных и аппаратных компонентов.

Аббревиатура: ПТС

1.41. Программное обеспечение

Программное обеспечение (ПО) — программа или множество программ, используемых для управления компьютером.

Аббревиатура: ПО

1.42. Программный комплекс

Программный комплекс (ПК) — набор программных средств, работающих совместно для выполнения одной или нескольких сходных задач.

Аббревиатура: ПК

1.43. Проект

Проект — каталог с набором файлов и подкаталогов, с которым работает пользователь.

1.44. Разрешенная сессия

Разрешенная сессия — входящее соединение, зарегистрированное Комплексом в контролируемой сети, и признанное легитимным согласно правилам сессий.

1.45. Регламентные работы

Регламентные работы — комплекс профилактических работ и проверок, выполняемых на объектах систем автоматики в определенные (регламентированные) моменты времени периода эксплуатации и направленных на поддержание их надежности в течение межрегламентного срока.

1.46. Репликация

Репликация — автоматическое копирование (синхронизация) данных между Супервижн и связанными с ним Менеджментами. Активируется при выборе централизованного управления и подразумевает замену локальных данных на передаваемые с Супервижн.

1.47. Репликация (статус)

Репликация — статус репликации данных с Менеджмента на Супервижн и статус работы сервисов, отвечающих за репликацию данных. Доступные значения: `Активно`, `Ошибка`, `Недоступно`.

1.48. Реплицированная учетная запись

Реплицированная учетная запись — учетная запись, которая создается на компоненте Супервижн и при активации централизованного управления передается (реплицируется) на привязанные Менеджменты, деактивируя их локальные учетные записи (при их наличии).

1.49. Репозиторий

Репозиторий — серверное хранилище данных, состоящее из проекта и истории его изменений.

1.50. Роль пользователя

Роль пользователя — совокупность возможностей, которые получает пользователь Комплекса, входящий в определенное множество встроенных групп доступа, и оперирующий с заданными наборами возможностей.

1.51. Сбор метрик (статус)

Сбор метрик — статус работы сервисов, отвечающих за сбор метрик с Менеджментов, которые затем отображаются на виджетах Супервижн. Доступные значения: `Активно`, `Ошибка`, `Недоступно`.

1.52. Сервис

Программная единица компонента Комплекса или модуля компонента Комплекса, реализующая определенные технические функции и взаимодействующая с другими сервисами, модулями и компонентами.

См. также

Компонент

Модуль

1.53. Сервис глубокой инспекции пакетов

Сервис глубокой инспекции пакетов — технология накопления статистических данных, проверки и фильтрации сетевых пакетов по их содержимому. В отличие от брандмауэра, производится анализ полного содержимого трафика на уровнях модели OSI со второго и выше.

Аббревиатура: DPI

Синонимы: Deep packet inspection

См. также

UDV Network Traffic Analyzer

1.54. Сессия

Установленное сетевое соединение между клиентом и сервером для возможности обмена данными в ограниченный промежуток времени. Сессия имеет признак начала и конца. Начало определяется по соответствующим пакетам протоколов транспортного уровня; завершение также определяется по пакетам, либо по таймауту, установленному в модуле «Анализ промышленного сетевого трафика» для каждого протокола транспортного уровня.

См. также

Просмотр сессий и пакетов

1.55. Система обнаружения вторжений

Система обнаружения вторжений (СОВ) — программное или аппаратное средство, предназначенное для выявления фактов неавторизованного доступа в компьютерную систему или сеть либо несанкционированного управления ими через Интернет.

Аббревиатура: СОВ

1.56. Сканер

Сканер — исполняемый скрипт сбора данных.

1.57. Скрипт

Скрипт — исполняемый файл, содержащий последовательность действий на скриптовом языке программирования Python. Предназначен для сбора данных с активов с помощью сканеров.

1.58. Соединение (статус)

Соединение — статус активности подключения между Менеджментом и Супервижн. Доступные значения: `Установлено`, `Ошибка`, `Недоступно`.

1.59. Справочник

Справочник — систематизированный список данных об одном или нескольких компонентах конкретного Комплекса.

1.60. Служба обнаружения вторжений

Служба обнаружения вторжений — служба Комплекса, которая позволяет обнаруживать подозрительную сетевую активность, сравнивая встроенные правила обнаружения вредоносного трафика с данными, проходящими по локальной сети.

1.61. Средство защиты информации

Средство защиты информации (СрЗИ) — техническое, программное, программно-техническое средство, вещество и (или) материал, предназначенные или используемые для защиты информации.

Аббревиатура: СрЗИ

1.62. Статус модели

Статус модели — отображение текущего этапа жизненного цикла модели в рамках модуля UDV DATAPK EDR for PLC.

1.63. Супервижн

Транслитерация для Supervision.

См. также

UDV DATAPK уровня Supervision

1.64. Схема корреляции событий

Схема корреляции событий — набор сущностей, используемый для представления и обработки событий, включает в себя представления различных типов событий, таких как: окна данных, таблицы, контексты, переменные.

1.65. Тег

Тег — параметр технологического процесса или оборудования, передаваемый в промышленной сети по определенным протоколам. Теги используются для мониторинга и управления оборудованием через системы автоматизации (например, ПЛК).

См. также

Правила контроля тегов

1.66. Технические условия

Технические условия (ТУ) — документ, устанавливающий технические требования, которым должны соответствовать конкретное изделие, материал, вещество и пр. или их группа.

Аббревиатура: ТУ

1.67. Техническое обслуживание

Техническое обслуживание — комплекс организационно-технических мероприятий и работ, производимых на объекте и направленных на поддержание в рабочем или исправном состоянии оборудования (программного обеспечения) технических систем в процессе их использования по назначению с целью повышения надежности и эффективности их работы.

Аббревиатура: ТО

1.68. Туннелирование DNS

Туннелирование DNS — сетевая атака, которая направляет DNS-запросы на сервер злоумышленника для предоставления ему скрытого канала управления и контроля, а также для кражи данных. DNS-туннелирование выполняется через межсетевые экраны путем кодирования сообщений управления и контроля (C&C) или небольших объемов данных в незаметные ответы и запросы DNS. Для выявления DNS-туннелирования среди обычного DNS-трафика, как правило, применяются технологии машинного обучения.

Аббревиатура: Туннелирование DNS

1.69. Узел

Узел — элемент сети предприятия, взаимодействующий с другими элементами сети.

1.70. Уровень индикации

Уровень индикации — уровень, определяющий уровень детализации (глубину) разбора передаваемых данных. Он указывает, какая часть информации отображается или обрабатывается при мониторинге или дешифровке трафика. В зависимости от настроек уровень индикации может показывать:

- только высокоуровневую информацию (например, тип пакета);
- часть информации (отдельные поля протокола);
- полную информацию (все уровни вложенности).

1.71. Условие сходимости модели

Условие сходимости модели — набор условий, при достижении которых возможно досрочное завершение этапа обучения с последующим переходом на следующий этап жизненного цикла модели.

1.72. Учетная запись

Учетная запись — хранимая в компьютерной системе совокупность данных о пользователе, необходимая для его опознавания (аутентификации) и предоставления доступа к его личным данным и настройкам.

1.73. Федеральная служба по техническому и экспортному контролю

Федеральная служба по техническому и экспортному контролю — орган исполнительной власти, осуществляющий контроль за сертификацией и аттестацией автоматизированных систем с учетом требований информационной безопасности.

Аббревиатура: ФСТЭК России

1.74. Фильтрация

Фильтрация — способ вывода нужных пользователю данных при помощи встроенных фильтров.

1.75. Централизованное управление

Централизованное управление — модель управления решением, при выборе которой учетные записи и парольная политика передаются из Супервижн на привязанные Менеджметы.

1.76. Этап жизненного цикла модели

Этап жизненного цикла модели — элемент структуры, описывающей процесс существования модели.

1.77. Common Platform Enumeration

Common Platform Enumeration (CPE) — структурированная схема именования систем информационных технологий, программного обеспечения и пакетов.

Аббревиатура: CPE

1.78. Common Vulnerabilities and Exposures

Common Vulnerabilities and Exposures (CVE) — база данных общеизвестных уязвимостей информационной безопасности.

Аббревиатура: CVE

1.79. Open Vulnerability and Assessment Language

OVAL — основанный на xml формат, предназначенный для автоматизированной оценки безопасности систем и предоставляющий средства для описания исследуемой системы, анализа ее состояния и формирования отчетов о результатах проверки.

Аббревиатура: OVAL

1.80. Syslog

Syslog — стандарт отправки и регистрации сообщений о происходящих в системе событиях. Используется в компьютерных сетях, работающих по протоколу IP. Термином Syslog называют как ныне стандартизированный сетевой протокол Syslog, так и программное обеспечение (приложение, библиотеку), которое занимается отправкой и получением системных сообщений.

Синонимы: system log

1.81. Version Control

Version Control — система, состоящая из серверной части Version Control Management и клиентской части Version Control Desktop App.

1.82. Version Control Desktop App

Version Control Desktop App — клиентское ПО, предназначенное для работы с репозиториями Version Control Management.

1.83. Version Control Management

Version Control Management — серверное ПО, предназначенное для централизованного управления репозиториями проектов ПЛК, резервного копирования и восстановления проектов ПЛК, отслеживания и контроля изменений в исходном коде проектов ПЛК.

1.84. UDV DATAPK Industrial Kit

Маркетинговое наименование программного комплекса UDV DATAPK.

Аббревиатура: UDV DATAPK

1.85. UDV DATAPK уровня Management

UDV DATAPK уровня Management с функциями управления сенсорами и анализа полученных с них данных.

Аббревиатура: Management

См. также

Комплекс

1.86. UDV DATAPK уровня Sensor

UDV DATAPK уровня Sensor — UDV DATAPK с базовым набором функций по получению информации с активов технологического комплекса.

Аббревиатура: Sensor

1.87. UDV DATAPK уровня Supervision

UDV DATAPK уровня Supervision — компонент системы Комплекса, устанавливающийся в корпоративном или технологическом сегментах сети и отвечающий за централизованное управление учетными записями, а также предоставление аналитической информации об общем состоянии защищенности АСУ ТП.

Аббревиатура: Supervision

Синонимы: Супервижн

1.88. UDV DATAPK EDR for PLC

Маркетинговое наименование модуля UDV DATAPK «Обнаружение и реагирование для ПЛК».

Аббревиатура: UDV DATAPK EDR for PLC

1.89. UDV DATAPK Version Control

Маркетинговое наименование модуля UDV DATAPK «Управление проектами ПЛК» и отдельного программного комплекса «UDV DATAPK Version Control».

Аббревиатура: UDV DATAPK Version Control

1.90. UDV Network Traffic Analyzer

Маркетинговое наименование модуля UDV DATAPK «Анализ промышленного сетевого трафика» и отдельного программного комплекса «Система контроля и анализа сетевого трафика UDV NTA».

1.91. Модуль «Анализ промышленного сетевого трафика»

Программный комплекс для защиты сетевой инфраструктуры от кибератак, основанный на глубоком анализе трафика. Основной целью функционирования модуля является выявление и инвентаризация устройств, обнаружение вторжений, построение карты сети.

Аббревиатура: Модуль «Анализ промышленного сетевого трафика»

1.92. Модуль «Обнаружение и реагирование для ПЛК»

Программный комплекс для обнаружения инцидентов ИБ в автоматизированных системах, основанный на интеллектуальных алгоритмах. Основной целью функционирования модуля является детектирование отклонений в работе контроллеров автоматизированных систем.

Аббревиатура: Модуль «Обнаружение и реагирование для ПЛК»

1.93. Модуль «Управление внешними событиями»

Программный модуль для получения и обработки событий информационной безопасности из сторонних источников и других модулей, нормализации и корреляции событий, формирования инцидентов ИБ и отправки событий/инцидентов в сторонние системы по протоколу Syslog.

Аббревиатура: Модуль «Управление внешними событиями»

1.94. Модуль «Управление конфигурациями»

Программный модуль для контроля конфигурационных параметров, влияющих на защищенность, и выявления отклонений параметров от эталонных значений.

Аббревиатура: Модуль «Управление конфигурациями»

1.95. Модуль «Контроль версий»

Программное обеспечение, предназначенное для централизованного управления репозиториями проектов ПЛК, резервного копирования и восстановления проектов ПЛК, отслеживания и контроля изменений в исходном коде проектов ПЛК

Аббревиатура: Модуль «Контроль версий»

1.96. Модуль «Управление уязвимостями»

Программный модуль для выявления угроз информационной безопасности и проверки соответствия требованиям ИБ с помощью технологий OVAL и CPE to CVE, а также обнаружения уязвимостей из БДУ ФСТЭК России.

Аббревиатура: Модуль «Управление уязвимостями»

2. Введение

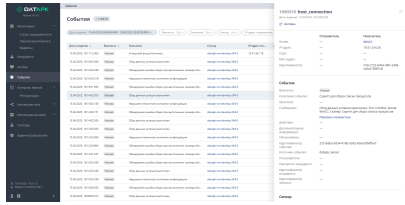
В настоящем документе приведено Руководство по эксплуатации Программного комплекса UDV DATAPK (далее — UDV DATAPK, Комплекс). В документе описаны: область назначения, краткое описание возможностей комплекса, описание процедуры подготовки к работе и мониторинга работоспособности комплекса, описание выполняемых пользователями функций, задач и процедур Комплекса, а также действия в нештатных ситуациях.

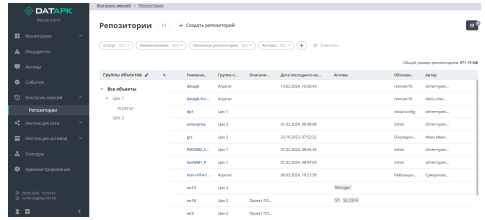
3. Что нового?

В этом разделе:

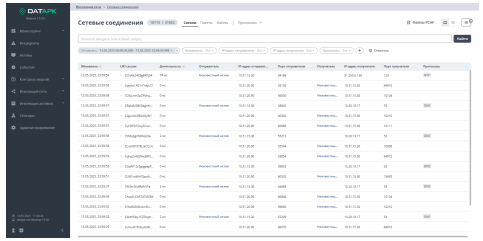
1. **Изменения в Руководстве по эксплуатации**

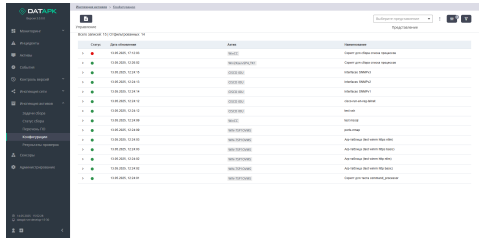
Обновления Программного комплекса UDV DATAPK в версии 3.0.0.0 представлены в таблице ниже.

ОПИСАНИЕ	РАЗДЕЛЫ ДОКУМЕНТАЦИИ	КАТЕГОРИЯ	ИЛЛЮСТРАЦИЯ ИЗМЕНЕНИЙ
Реализована модульная архитектура UDV DATAPK для возможности установки и использования только тех модулей, которые необходимы в зависимости от потребностей бизнеса	Список модулей UDV DATAPK Industrial Kit, Архитектура UDV DATAPK Industrial Kit	Архитектура	—
Добавлен REST API с конечными точками для получения данных о UDV DATAPK и для изменения его различных функций	Работа с REST API Комплекса	Интеграция с другими системами	—
Разделены механизмы хранения внутренних и внешних событий	Мониторинг событий → Хранение событий Механизмы хранения событий	События	—
Изменена работа с событиями в упрощенном режиме: • переименованы поля событий • добавлены новые быстрые фильтры • добавлена карточка события для просмотра подробной информации о событии	Поиск и просмотр событий в упрощенном режиме	События	

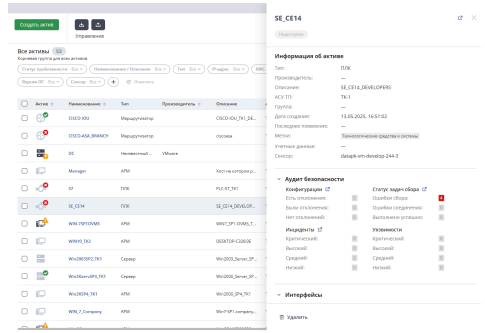
ОПИСАНИЕ	РАЗДЕЛЫ ДОКУМЕНТАЦИИ	КАТЕГОРИЯ	ИЛЛЮСТРАЦИЯ ИЗМЕНЕНИЙ
• в карточку событий об обнаружении новой сессии добавлена ссылка для просмотра сессии на странице **Сетевые соединения → Сессии**			
Добавлен новый механизм корреляции внутренних событий с ограниченным набором правил. Новый механизм применяется для генерации инцидентов, если не установлен модуль «Управление внешними событиями»	Управление внутренними правилами корреляции событий Список внутренних правил корреляции событий	Инциденты, Корреляция событий	—
Добавлен новый механизм сканирования сети, при выполнении которого на странице **Активы** создаются новые неизвестные активы	Сканирование сети и определение интерфейсов активного сетевого оборудования	Сканирование сети	—
Добавлен модуль «Управление проектами ПЛК», предлагающий следующие возможности: • загрузка, выгрузка и централизованное хранение проектов ПЛК; • иерархическая структура хранения проектов ПЛК; • проверка соответствия версий проектов ПЛК в Version Control Desktop App и Version Control Management; • ведение истории изменений проектов ПЛК;	Управление проектами ПЛК	Контроль версий	

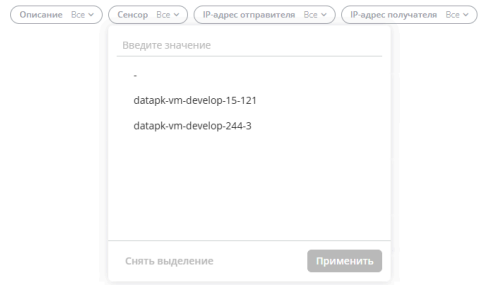
ОПИСАНИЕ	РАЗДЕЛЫ ДОКУМЕНТАЦИИ	КАТЕГОРИЯ	ИЛЛЮСТРАЦИЯ ИЗМЕНЕНИЙ
• блокировка и разблокировка проектов ПЛК для внесения изменений; • резервное копирование и восстановление версий проектов ПЛК; • отображение расширенной статистической информации по проектам ПЛК; • настройка связи ПЛК с проектом ПЛК; • настройка исключений файлов и каталогов в проектах ПЛК; • многопользовательский режим работы; • ролевая модель доступа; • просмотр событий информационной безопасности; • отображение информации о ПЛК, связанных с проектом ПЛК, в Version Control Desktop App; • просмотр проектов ПЛК в Version Control Desktop App при отсутствии сетевого соединения с Version Control Management; • непрерывная репликация проектов ПЛК для отказоустойчивого хранения			

ОПИСАНИЕ	РАЗДЕЛЫ ДОКУМЕНТАЦИИ	КАТЕГОРИЯ	ИЛЛЮСТРАЦИЯ ИЗМЕНЕНИЙ
Удален механизм управления потоками данных. Добавлен модуль «Анализ промышленного сетевого трафика», предлагающий следующие возможности: • Глубокий анализ трафика: детализация сетевых событий до протоколов приложений для выявления и анализа первопричин инцидентов. • Проактивный поиск угроз: хранение истории сетевой активности по всем соединениям, из которой возможно извлечь артефакты, относящиеся к нарушению политики ИБ компании или преступной группировке. • Визуализация сетевой активности: отображение карты устройств и соединений для понимания взаимодействий в сети. • Обнаружение аномалий и несанкционированных действий: выявление подозрительной активности, неавторизованных устройств (Shadow IT, BYOD), и нелегитимного использования средств удаленного администрирования.	Анализ промышленного сетевого трафика	Инспекция сети, управление сетевым трафиком, Карта сети, Обнаружение вторжений	

ОПИСАНИЕ	РАЗДЕЛЫ ДОКУМЕНТАЦИИ	КАТЕГОРИЯ	ИЛЛЮСТРАЦИЯ ИЗМЕНЕНИЙ
• Защита без агентов: поддержка IoT и других устройств, где установка агентов затруднена. • Точная комплексная оценка атаки в реальном времени: обнаружение потенциальных угроз и их реализации, регистрация инцидентов, локализация атаки, восстановление хронологии и запись доказательств.			
Добавлен модуль «Управление модулем обнаружения и реагирования для ПЛК», предлагающий следующие возможности: • Выявление аномалий в сетевом трафике ПЛК; • Детализация причин выявленных аномалий; • Автоматические переходы между режимами работы модели с возможностью дообучения; • Агрегация и корреляция событий модуля в рамках Комплекса.	Управление модулем обнаружения и реагирования для ПЛК («EDR for PLC»)	Инспекция сети, управление сетевым трафиком	—
Выделен отдельный модуль «Управление конфигурациями», предлагающий следующие возможности: • Контроль соответствия любых конфигурационных параметров IT-устройств и устройств АСУ ТП	Просмотр сводки конфигураций, Настройка сбора конфигураций активов	Инспекция активов, Конфигурации, Задачи сбора	

ОПИСАНИЕ	РАЗДЕЛЫ ДОКУМЕНТАЦИИ	КАТЕГОРИЯ	ИЛЛЮСТРАЦИЯ ИЗМЕНЕНИЙ
на соответствие необходимым значениям. • Отслеживание изменений в значениях и оперативное реагирование на изменения.			
Выделен отдельный модуль «Управление уязвимостями», предлагающий следующие возможности: • Проведение неинвазивного аудита защищенности компонентов АСУ ТП методом белого ящика (White Box). • Выявление угроз информационной безопасности и их устранение. • Проверка соответствия активов требованиям ИБ.	Поиск уязвимостей и проверка соответствия требованиям информационной безопасности	Скрипты OVAL, Группы OVAL, Определения OVAL, Настройки OVAL	—
Добавлен новый компонент Supervision, предлагающий следующие возможности: • Централизованная аналитика состояния ИБ АСУ ТП. • Мониторинг состояния компонентов Management и Sensor.	Архитектура UDV DATAPK Industrial Kit	Архитектура, Централизованное управление	—

ОПИСАНИЕ	РАЗДЕЛЫ ДОКУМЕНТАЦИИ	КАТЕГОРИЯ	ИЛЛЮСТРАЦИЯ ИЗМЕНЕНИЙ
• Дополнительная точка хранения проектов ПЛК. • Централизованное управление учетными записями пользователей.			
Улучшен пользовательский интерфейс ключевых страниц: • Страница **События**: ◦ новые фильтры списка событий; ◦ новая боковая панель просмотра информации о событии. • Страница **Активы**: ◦ новые фильтры списка активов; ◦ добавлены групповые операции с активами; ◦ новая боковая панель просмотра информации об активе. • Страница **Инциденты**: ◦ новые фильтры списка инцидентов; ◦ множественные визуальные улучшения.	Поиск и просмотр событий в упрощенном режиме Работа с активами Работа с инцидентами	Пользовательский интерфейс	
Улучшен модуль «Управление уязвимостями»:	Поиск уязвимостей ПО и ОС в базах CVE, CPE и БДУ ФСТЭК России	Поиск уязвимостей активов	—

ОПИСАНИЕ	РАЗДЕЛЫ ДОКУМЕНТАЦИИ	КАТЕГОРИЯ	ИЛЛЮСТРАЦИЯ ИЗМЕНЕНИЙ
• улучшено быстродействие при поиске уязвимостей ПО и ОС в базах CVE, CPE и БДУ ФСТЭК России; • улучшена возможность тонкой настройки справочников сопоставления ПО с CPE.			
Добавлены новые сканеры для сбора данных о ПЛК Regul: • Конфигурация ПЛК Regul (SNMPv3); • Контрольная сумма программы ПЛК Regul (OPCUA); • Контрольная сумма программы ПЛК Regul (FTP)	Реестр сканеров Комплекса	Сканеры	–
Обновлен механизм сохранения представлений в связи с изменением механизма фильтрации данных на следующих страницах: • **Активы** • **Инциденты** • **События** • **Сетевые соединения** • **Правила сессий** • **Правила контроля тегов**	Представления	Представления, Фильтры	

ОПИСАНИЕ	РАЗДЕЛЫ ДОКУМЕНТАЦИИ	КАТЕГОРИЯ	ИЛЛЮСТРАЦИЯ ИЗМЕНЕНИЙ
Обновлен список всех внутренних событий Комплекса, изменены идентификаторы событий	События Комплекса	События	—
В событие `1170002 Неудачная попытка входа в Комплекс` добавлена информация о причине неудачного входа в Комплекс	События Комплекса	События	—
При работе с уязвимостями максимальное количество потребляемой оперативной памяти не превышает 6 ГБ	Поиск уязвимостей ПО и ОС в базах CVE, CPE и БДУ ФСТЭК России	Поиск уязвимостей	—
Добавлена возможность настройки точности, с которой будут подбираться элементы CPE для наименования, версии и поставщика ПО	Поиск уязвимостей ПО и ОС в базах CVE, CPE и БДУ ФСТЭК России	Поиск уязвимостей	—
Добавлена обработка столбцов **Производитель ПО** и **Наименование ПО** в файле сопоставления ПО и CVE с помощью регулярных выражений	Поиск уязвимостей ПО и ОС в базах CVE, CPE и БДУ ФСТЭК России	Поиск уязвимостей	—

3.1. Изменения в Руководстве по эксплуатации

В таблице ниже приведена история изменений документа «Руководство по эксплуатации» для UDV DATAPK.

ДАТА ИЗМЕНЕНИЯ	СОДЕРЖАНИЕ ИЗМЕНЕНИЙ
12.09.2025	Первоначальная версия

4. Условные обозначения

В настоящем руководстве приняты условные обозначения, ознакомиться с которыми можно в таблице (Таблица 1. Условные обозначения).

Табл. 1. Условные обозначения

ПРИМЕР ТЕКСТА С УСЛОВНЫМ ОБОЗНАЧЕНИЕМ	ОПИСАНИЕ
ОСТОРОЖНО: Если вы увидите сообщение `Текущая конфигурация совпадает с эталонной. В период между получением эталонной конфигурации и текущей было обнаружено отклонение. Убедитесь в легитимности изменений, убедитесь в том, что изменения не были произведены злоумышленником.`	Критически значимая информация о потенциальных рисках, которые могут нарушить работу Комплекса или привести к неправильным действиям пользователя
Внимание: Сеанс доступа к веб-интерфейсу Комплекса автоматически завершается по истечении периода времени, заданного в переменной `USER_SESSION_INACTIVITY_TIMEOUT` в файле `manager.env`. По умолчанию значение переменной составляет 600 секунд (10 минут).	Важная информация, требующая осмысленного подхода при работе с Комплексом, включая справочные сведения и рекомендации
Прим.: При необходимости воспользуйтесь кнопками (**Показать еще по 5 окружающих строк**) и (**Скрыть по 5 окружающих строк**), а также возможностью отображения спецсимволов.	Оптимизационные советы, раскрывающие эффективные приемы работы с Комплексом, включая альтернативные способы использования функций и сокращение времени выполнения задач
`cd /opt/datapk`	Блок кода. Содержит исполняемые команды или выдержки из кода программ

5. Общие сведения о Комплексе

Программный комплекс UDV DATAPK (, Комплекс) применяется для выявления несанкционированных изменений в АСУ ТП, регистрации событий ИБ в АСУ ТП, выявления компонентов АСУ ТП, подверженных критическим уязвимостям, обнаружения попыток эксплуатации уязвимостей компонентов АСУ ТП до момента их устранения и автоматизированного контроля выполнения требований ИБ в АСУ ТП.

ОСТОРОЖНО:

Производитель не несет ответственности за внесение пользователями изменений в систему, на которой установлен экземпляр . Включение графического интерфейса, установка сторонних программ или иные произвольные изменения системы могут повлечь нарушение целостности , исчерпание ресурсов системы и ряд других проблем.

обеспечивает:

6. Логическая структура комплекса и режимы функционирования

Комплекс предназначен для оперативного мониторинга состояния информационной безопасности и контроля состояния защищенности АСУ ТП на всех уровнях иерархии АСУ ТП.

Подсистема идентификации и аутентификации субъектов доступа и объектов доступа в рамках ведения каталога активов создает, присваивает, изменяет, уничтожает идентификаторы, позволяет вести каталог активов АСУ ТП и выявлять изменения в их составе.

Подсистема регистрации событий безопасности компонентов АСУ ТП собирает, записывает и хранит информацию о событиях безопасности, позволяет просматривать результаты регистрации событий безопасности с генерированием временных меток и защищает информацию о таких событиях.

Подсистема контроля (анализа) защищенности информации выявляет и анализирует уязвимости, контролирует установку обновлений программного обеспечения и контролирует состав технических средств, программного обеспечения и средств защиты информации в АСУ ТП.

Подсистема защиты автоматизированной системы и ее компонентов защищает настройки средств защиты информации, программного обеспечения и иные данные, которые не должны меняться при обработке информации в АСУ ТП.

Подсистема выявления инцидентов и реагирования на них обнаруживает и регистрирует инциденты ИБ на активах.

Подсистема управления конфигурацией АСУ ТП и ее механизмов защиты управляет изменениями конфигурации активов АСУ ТП и документирует такие изменения.

Подсистема управления доступом Комплекса выполняет идентификацию, проверку подлинности и контроль доступа пользователей в Комплекс и к его отдельным функциям.

В Комплексе предусмотрено два режима функционирования:

1. Режим наблюдения (пассивный мониторинг), который подразумевает:
    - однонаправленное получение данных;
    - прослушивание сетевого трафика и прием событий.
2. Режим «запрос-ответ» (активный мониторинг), который подразумевает:
    - получение конфигурации и событий;
    - взаимодействие с активами в режиме «запрос-ответ» с использованием штатных механизмов и протоколов;
    - выявление уязвимостей и проверки на соответствие требованиям ИБ.

Табл. 2. Режимы функционирования Комплекса

ФУНКЦИИ	РЕЖИМ НАБЛЮДЕНИЯ	РЕЖИМ ОПРОСА
Сбор событий ИБ	× ✓	✓
Обнаружение атак	✓	✓
Выявление сетевых аномалий	✓	✓

Табл. 2. Режимы функционирования Комплекса

ФУНКЦИИ	РЕЖИМ НАБЛЮДЕНИЯ	РЕЖИМ ОПРОСА
Сбор конфигураций	×	✓
Определение текущего состава активов	✓	✓
Выявление изменений в составе активов	✓	✓
Проверка активов на уязвимости	× ✓	✓

7. Сведения о сертификатах

Сертификат соответствия ФСТЭК России № 4719 от 28 сентября 2023 г. (действительный до 28 сентября 2028 г.) удостоверяет, что Программный комплекс «CyberLympha DATAPK», разработанный и производимый ООО «СайберЛимфа», является системой обнаружения вторжений, соответствует требованиям по безопасности информации, установленным в документах «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» (ФСТЭК России, 2020) — по 6 уровню доверия, «Требования к системам обнаружения вторжений» (ФСТЭК России, 2011), «Профиль защиты систем обнаружения вторжений уровня сети шестого класса защиты. ИТ.СОВ.С6.ПЗ» (ФСТЭК России, 2012) и задании по безопасности 05028144.620129.118-ЗБ при выполнении указаний по эксплуатации, приведенных в формуляре 05028144.620129.118-ФО.

Сертификат выдан на основании технического заключения от 25.08.2023, оформленного по результатам сертификационных испытаний, проведенных испытательной лабораторией ООО «КБ-Лаб» (аттестат аккредитации от 29.12.2020 г. № СЗИ RU.0001.01БИ00.Б041), и экспертного заключения от 01.09.2023, оформленного органом по сертификации ЗАО «НПП «БИТ» (аттестат аккредитации от 22.05.2017 № СЗИ RU.0001.01БИ00.А008).

Заявитель: ООО «СайберЛимфа».

8. Разделение функций по администрированию

Функциональные роли пользователей Комплекса и краткое описание выполняемых ими функций приведены в таблице ниже.

Табл. 3. Функциональные роли по администрированию Комплекса

НАИМЕНОВАНИЕ ФУНКЦИОНАЛЬНОЙ РОЛИ	КРАТКОЕ ОПИСАНИЕ ОСНОВНЫХ ФУНКЦИЙ
Администратор	• Контроль функционирования компонентов ПТС • Техническое обслуживание ПО • Техническое обслуживание аппаратных средств • Сопровождение и внедрение ПО • Обновление Комплекса • Изменение перечня информационных ресурсов, списков доступа и учетных записей пользователей • Замена неисправного устройства • Управление пользователями, в том числе присвоение ролей пользователям • Управление парольной политикой • Проверка реализации требований информационной безопасности • Разработка правил корреляции событий ИБ • Настройка сбора событий ИБ • Настройка источников событий ИБ • Настройка проверок актива на уязвимости и соответствие требованиям информационной безопасности • Сканирование сети • Управление сенсорами
Инженер	• Определение состава активов • Добавление активов в каталог активов • Определение легитимности изменений в составе активов • Определение легитимности сетевых соединений • Определение легитимности изменения конфигурации активов • Установка эталонной версии конфигурации активов • Привязывание интерфейсов к активам • Формирование отчетов по результатам сканирования активов на уязвимости • Формирование отчетов по результатам оценки выполнения требований по безопасной конфигурации активов • Формирование отчетов по событиям и инцидентам ИБ • Анализ событий и инцидентов ИБ

Табл. 3. Функциональные роли по администрированию Комплекса

НАИМЕНОВАНИЕ ФУНКЦИОНАЛЬНОЙ РОЛИ	КРАТКОЕ ОПИСАНИЕ ОСНОВНЫХ ФУНКЦИЙ
	• Разработка задач сбора конфигураций с активов • Запуск и контроль мероприятий по сбору конфигураций с активов
Просмотр веб-интерфейса	Просмотр всех страниц Комплекса
Просмотр панели мониторинга	Непрерывный просмотр страниц раздела **Мониторинг**

9. Первичная настройка

В этом разделе:

1. **Первичное подключение**
2. **Настройка локальных реквизитов и контролируемой сети**
3. **Настройка парольной политики**
4. **Импорт справочников из архива**
5. **Запуск обнаружения вторжений и синхронизация правил с сенсорами**
6. **Первичная настройка модуля «Анализ промышленного сетевого трафика»**
7. **Проверка работоспособности Комплекса**

Для выполнения первичной настройки Комплекс подключается к рабочей станции администратора и к подсети управляющего контура.

Рекомендуется производить первичную настройку в предложенном порядке.

9.1. Первичное подключение

В этом разделе:

- Подключение к веб-интерфейсу по протоколу HTTPS
- Первоначальная настройка

Порядок включения аппаратной платформы установленного Комплекса для выполнения первичной настройки:

1. Соедините сетевым кабелем разъем управляющего контура Комплекса с разъемом сетевой карты рабочей станции администратора.
2. Один конец кабеля питания вставьте в разъем питания Комплекса, другой – в заземленную сетевую розетку.
3. Включите Комплекс. Для этого кратковременно нажмите кнопку питания. Комплекс издаст одиночный звуковой сигнал, запустится операционная система, системное и прикладное ПО.

9.1.1. Подключение к веб-интерфейсу по протоколу HTTPS

Для подключения к веб-интерфейсу Комплекса по протоколу HTTPS:

1. Проверьте возможность подключения к UDV DATAPK уровня Management по протоколу HTTPS. Для этого:
    a. Откройте веб-браузер на клиентском компьютере.
    б. Введите адрес для подключения в веб-интерфейсу в формате `https://[IP-адрес]`, где `[IP-адрес]` — IP-адрес интерфейса управления Комплекса уровня Management.

▸ **Результат шага:** отобразится окно входа в веб-интерфейс Комплекса.

Рис. 1. Окно входа в веб-интерфейс Комплекса

2. Если в веб-браузере появится предупреждение о незащищенном подключении (по причине того, что созданный серверный сертификат не является доверенным для веб-браузера):
    a. Нажмите кнопку **Дополнительные**.

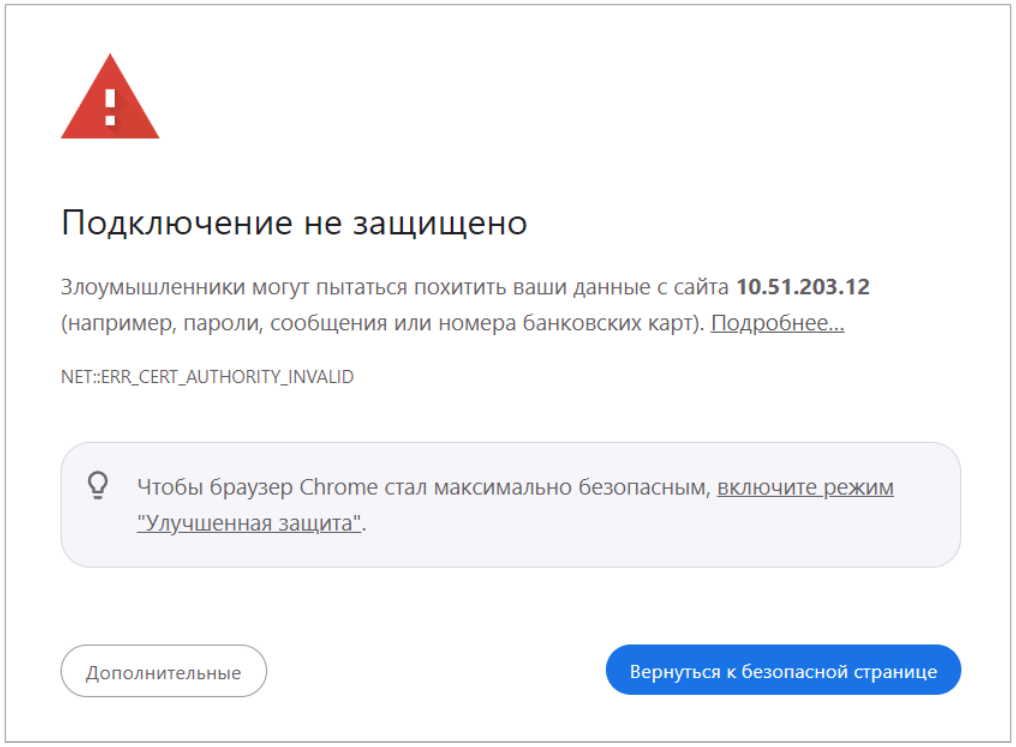


Рис. 2. Окно предупреждения о незащищенном подключении

- **Результат шага:** открыты дополнительные настройки для подключения к веб-интерфейсу Комплекса в браузере.

б. Для продолжения подключения к UDV DATAPK нажмите ссылку `Перейти на сайт [IP-адрес] (небезопасно)`.

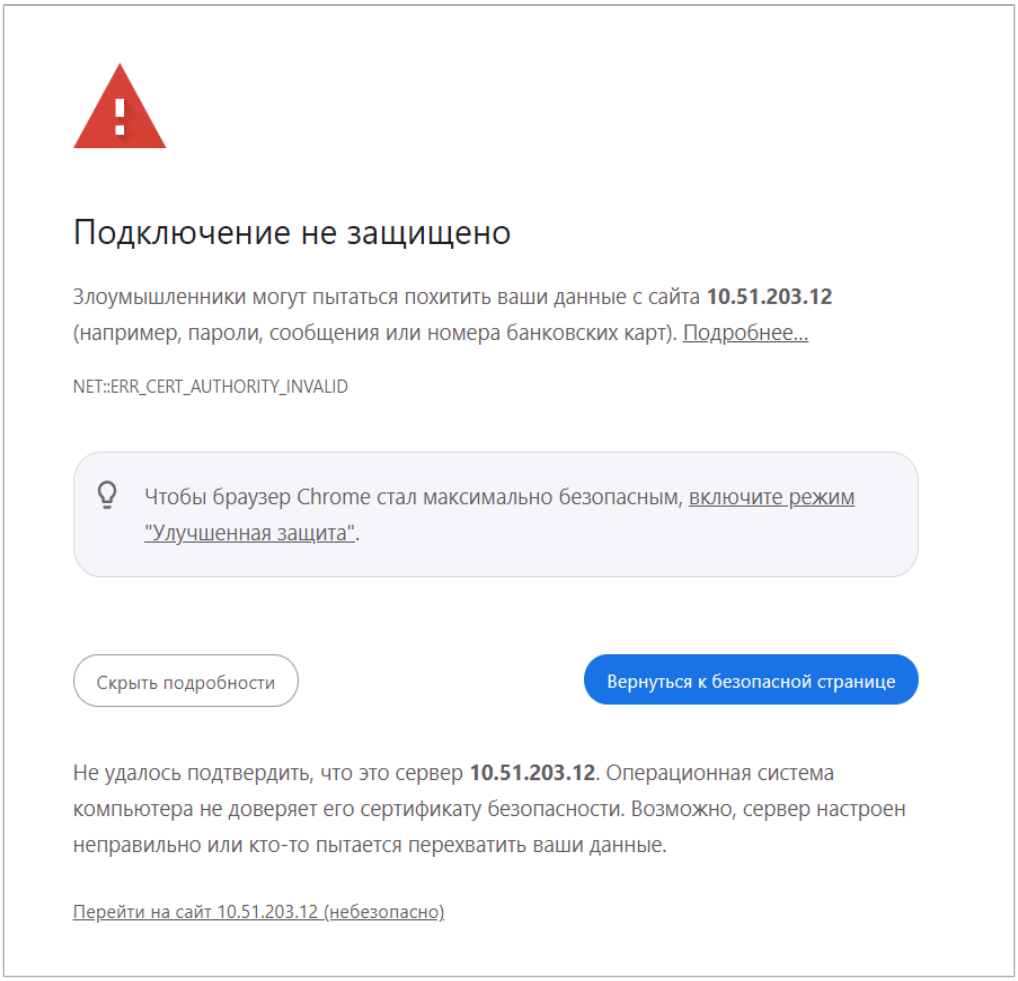


Рис. 3. Подключение к ПК UDV DATAPK по HTTPS

- **Результат шага:** отобразится окно входа в веб-интерфейс Комплекса.

3. Введите в поля окна входа предустановленное для первичной настройки Комплекса имя пользователя (логин): `datapk` и пароль: `datapk`. Нажмите кнопку **Войти**.

> Внимание:
>
> Количество неудачных попыток ввода пароля по умолчанию равно 3.
>
> По умолчанию при превышении неудачных попыток ввода пароля учетная запись блокируется на 600 секунд (10 минут).
>
> Количество неудачных попыток и время блокировки регулируются администратором на странице **Парольная политика**.

> Внимание:
>
> Сеанс доступа к веб-интерфейсу Комплекса автоматически завершается по истечении периода времени, заданного в переменной `USER_SESSION_INACTIVITY_TIMEOUT` в файле `manager.env`. По умолчанию значение переменной составляет 600 секунд (10 минут).

См. также

Настройка парольной политики

9.1.2. Первоначальная настройка

При первом входе в веб-интерфейс Комплекса вам будет предложено произвести первоначальную настройку.

> Подсказка:
>
> Обязательными шагами являются только принятие лицензионного соглашения и создание пользователя. Остальные настройки можно выполнить позже.

Для настройки:

1. Ознакомьтесь с условиями лицензионного соглашения. В случае согласия с условиями лицензионного соглашения установите чекбокс **Принимаю условия лицензионного соглашения** и нажмите кнопку **Далее**.

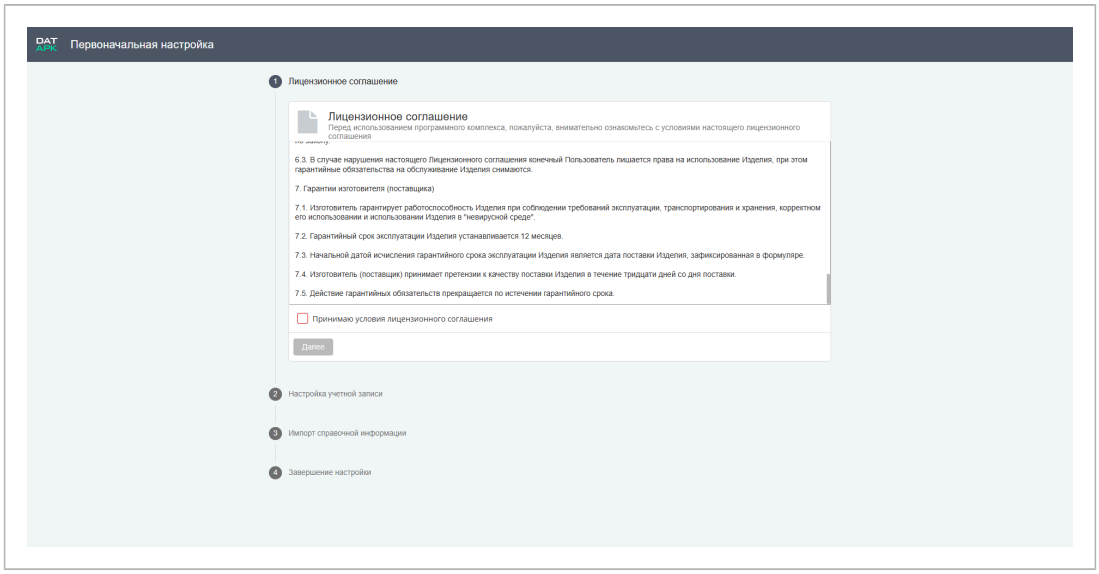


Рис. 4. Окно «Лицензионное соглашение» при выполнении первоначальной настройки

- **Результат шага:** появится окно **Настройка учетной записи**.

2. Настройте предустановленную учетную запись администратора Комплекса. Для этого:
    a. В окне **Настройка учетной записи** введите следующие параметры:
        - введите новый логин в поле **Логин**;
        - пароль учетной записи и его подтверждение в полях **Новый пароль** и **Подтверждение нового пароля**;

> Внимание:
>
> Пароль не должен содержать старый или новый логин учетной записи, должен состоять не менее, чем из 6 символов, содержать не менее одной буквы и числа. После завершения настройки парольную политику можно изменить на странице **Администрирование** → **Пользователи** → **Пользователи** → **Парольная политика**.

- фамилию, имя и отчество пользователя учетной записи в соответствующих полях.

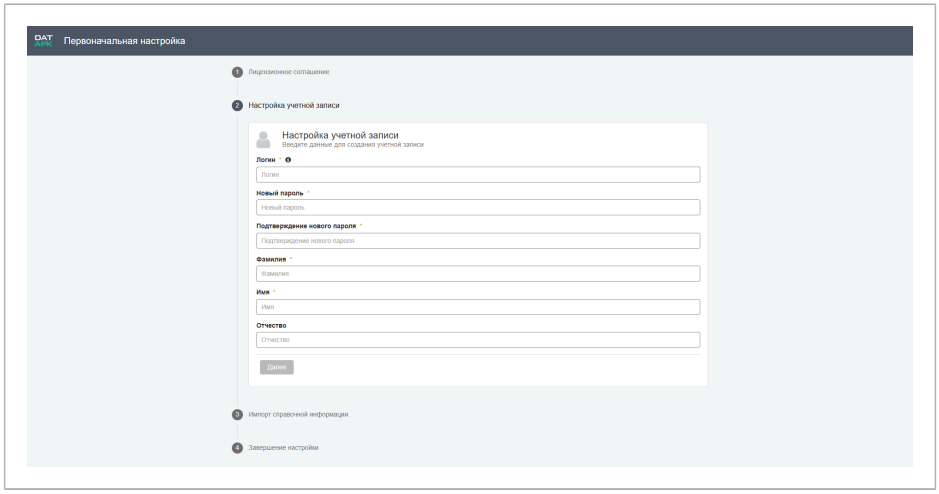


Рис. 5. Окно «Настройка учетной записи»

б. Нажмите кнопку **Далее** для сохранения данных и перехода к следующему шагу.

▸ **Результат шага:** появится окно **Импорт справочников.**

3. Импортируйте справочники. Для этого:

а. Нажмите кнопку **Выбрать файл**.

б. Выберите архив формата `.tar`, содержащий справочники, и нажмите кнопку **Открыть**.

> Подсказка:
>
> Если результат импорта вас не устраивает или файл был выбран ошибочно, то можно сразу отменить импорт, нажав кнопку **Сбросить**.

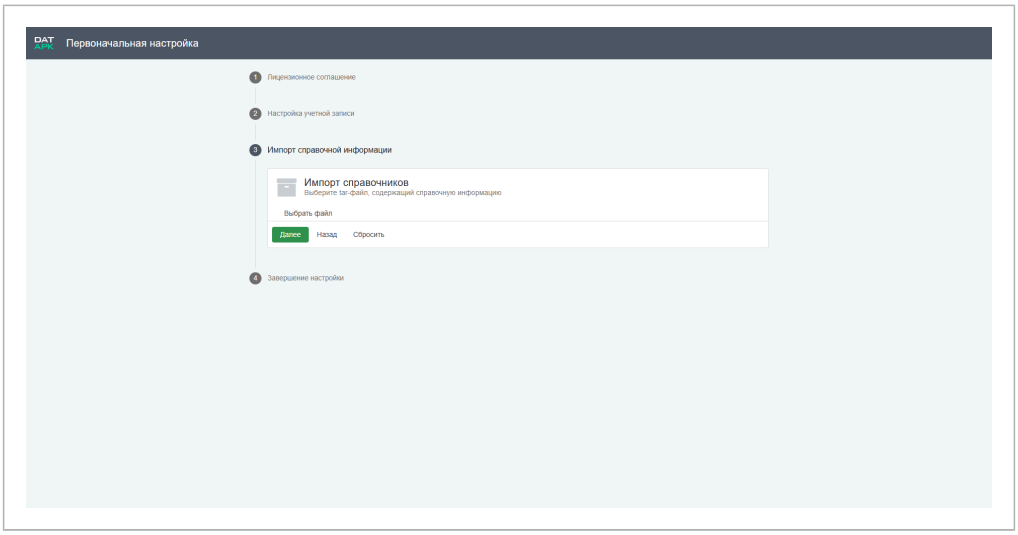


Рис. 6. Окно «Импорт справочников»

в. Нажмите кнопку **Далее** для сохранения данных и перехода к следующему этапу.

4. Если необходимая начальная настройка выполнена, нажмите кнопку **Завершить**.

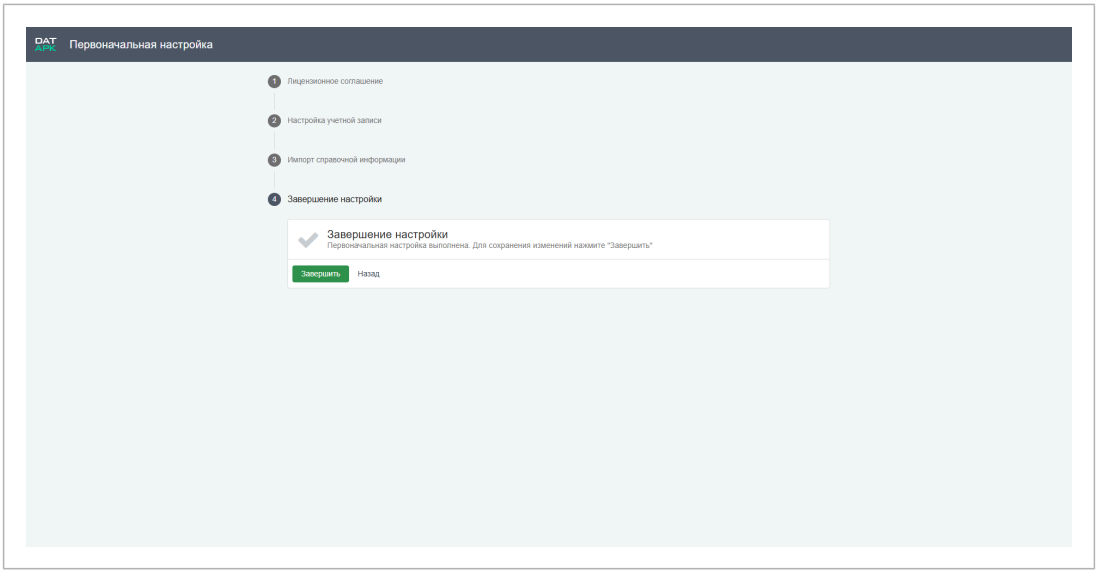


Рис. 7. Окно «Завершение настройки»

5. Войдите в веб-интерфейс Комплекса с новым логином и паролем.
6. Если в правом верхнем углу отобразится ошибка: `Непредвиденная ошибка. Перезапустить синхронизацию`, нажмите на ссылку **Перезапустить синхронизацию** для перезапуска синхронизации сенсоров с Комплексом.

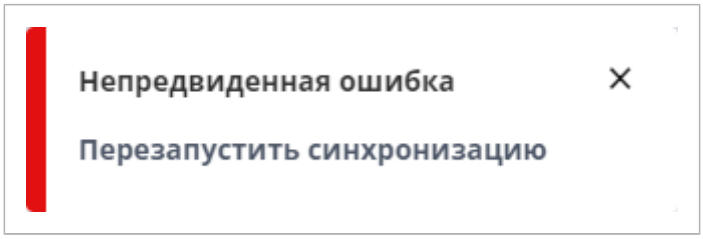


Рис. 8. Ошибка синхронизации сенсоров с Комплексом

9.2. Настройка локальных реквизитов и контролируемой сети

В этом разделе:

- Изменение сведений о Комплексе и сенсорах
- Настройка контролируемой сети

9.2.1. Изменение сведений о Комплексе и сенсорах

9.2.1.1. Изменение сведений о текущем Комплексе

1. Перейдите на страницу **Администрирование → Основные настройки → О системе**.
2. В блоке **Сведения о Комплексе** введите описание Комплекса, наименование эксплуатирующей организации и место установки. Наименование Комплекса настраивается автоматически.

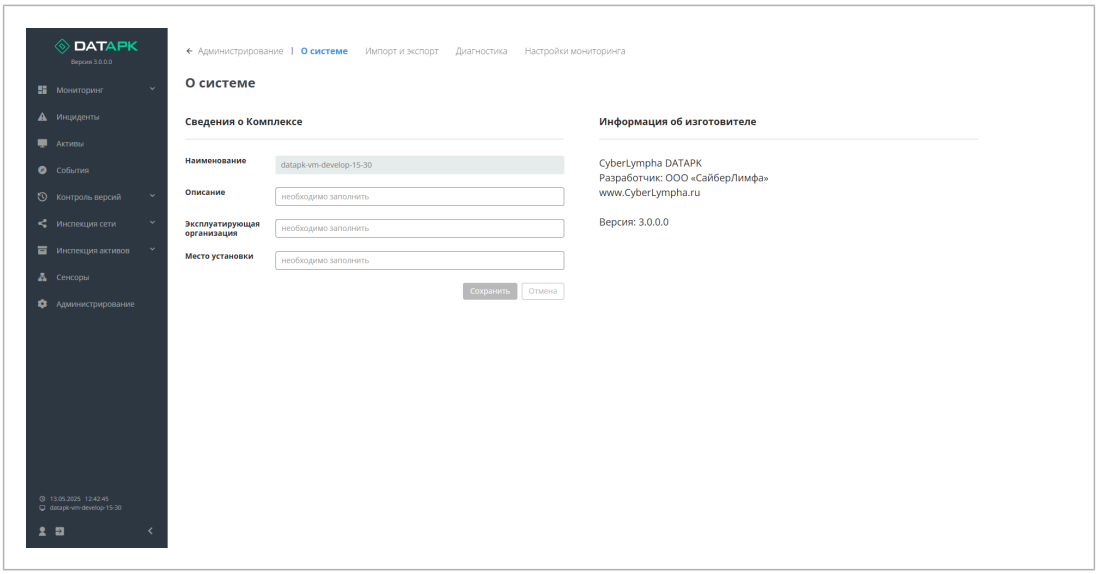


Рис. 9. Страница «О системе»

3. Нажмите кнопку **Сохранить** для подтверждения изменений.

9.2.1.2. Изменение сведений о сенсорах, подключенных к Комплексу

1. Перейдите на страницу **Сенсоры**.
2. Выберите сенсор из списка.
   - **Результат шага:** справа откроется карточка выбранного сенсора.
3. В открывшейся панели нажмите кнопку ✎ (**Редактировать**) напротив наименования сенсора.

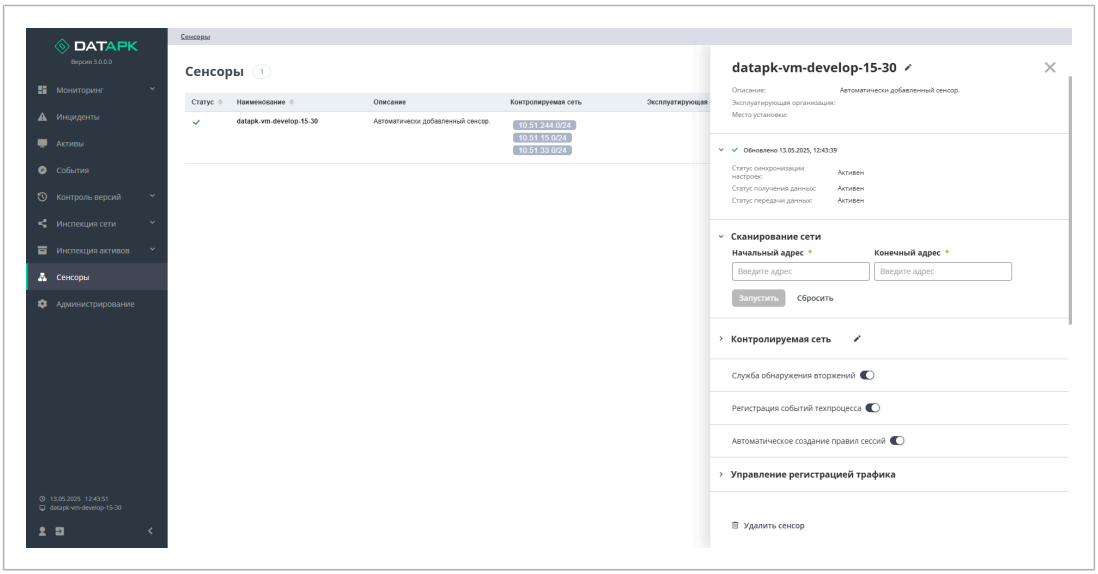


Рис. 10. Страница «Сенсоры»

4. Введите описание сенсора, наименование эксплуатирующей организации и место установки.

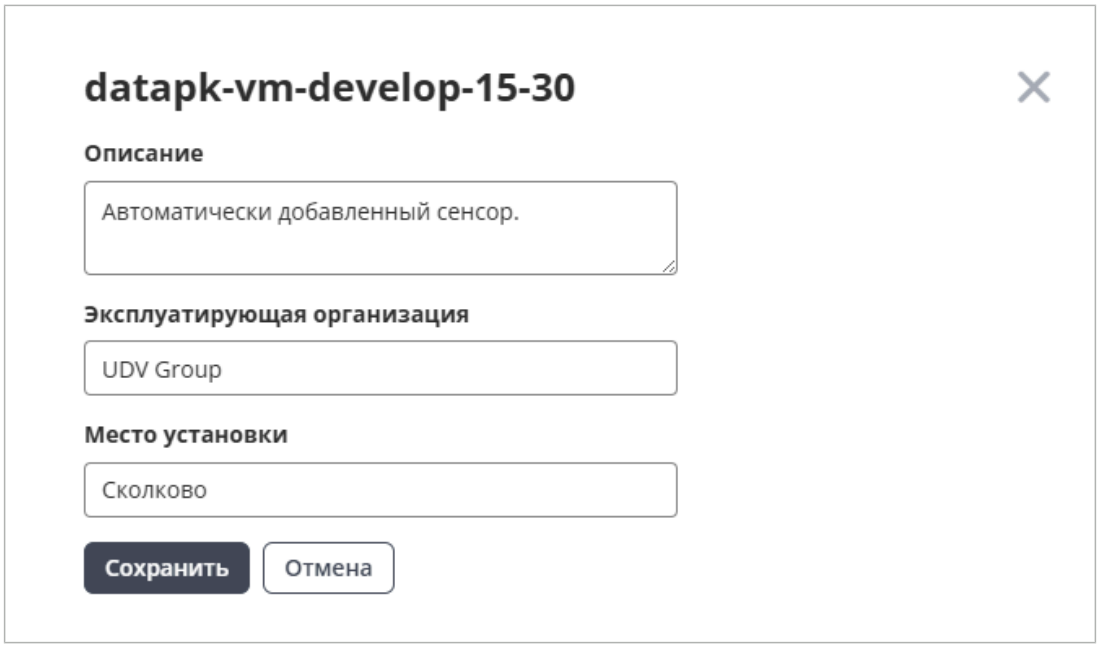


Рис. 11. Блок редактирования информации о сенсоре

5. Нажмите кнопку **Сохранить** для подтверждения изменений.

9.2.2. Настройка контролируемой сети

Настройка контролируемой сети необходима для отображения на странице **Активы** активов, IP-адреса которых входят в контролируемую сеть, а также для обнаружения сетевых соединений в контролируемой сети и отображения информации о них на страницах раздела **Сетевые соединения**. До выполнения настройки контролируемой сети, в зависимости от настроек Комплекса, в списке активов отображаются все активы, найденные только по MAC-адресу, независимо от наличия у них IP-адреса, либо только активы, у которых не определен IP-адрес (подробнее см. раздел «Сканирование сети и определение интерфейсов активного сетевого оборудования»).

Для настройки контролируемой сети Комплекса:

1. Перейдите на страницу **Сенсоры**.
2. Выберите сенсор из списка.
   - **Результат шага:** справа откроется карточка выбранного сенсора.

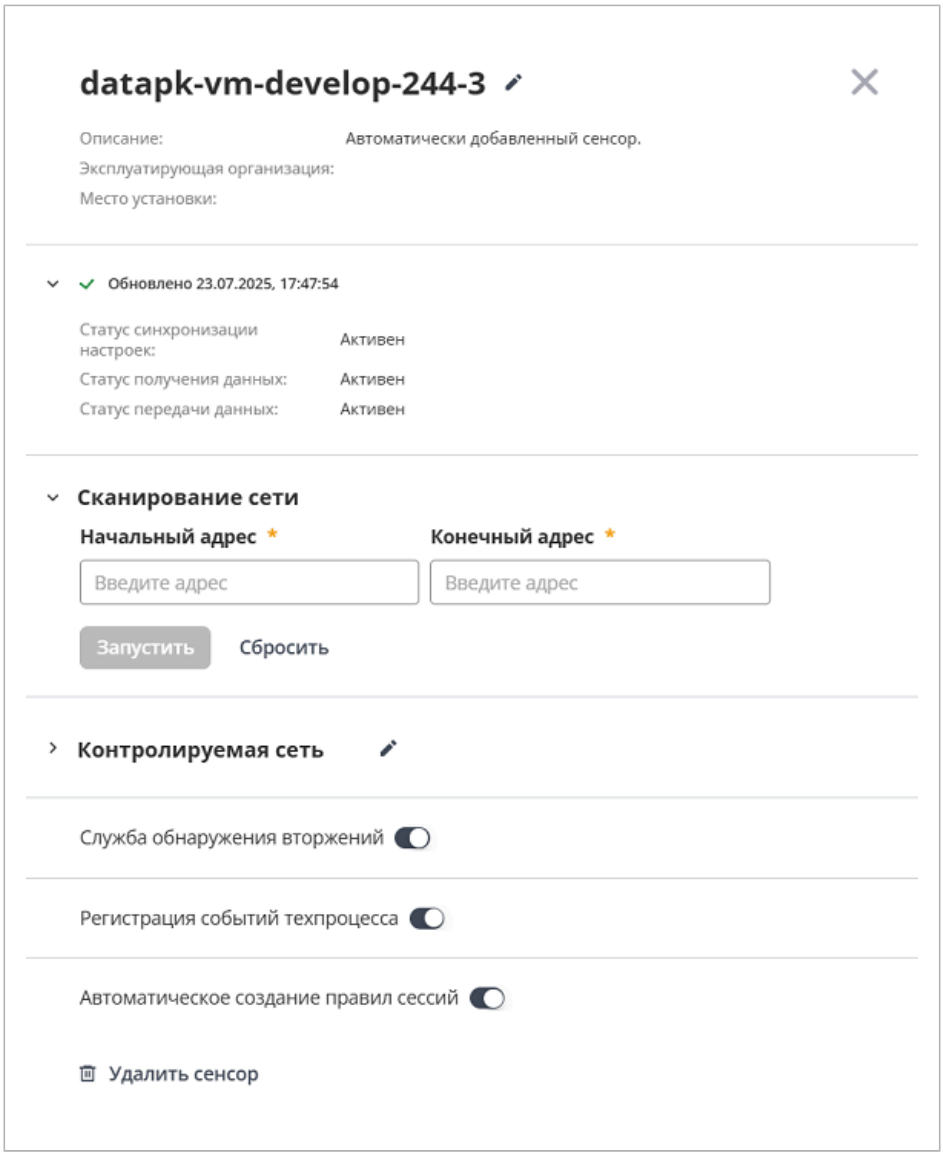


Рис. 12. Карточка сенсора

3. В открывшейся карточке в блоке **Контролируемая сеть** нажмите на (**Редактировать сеть**) для входа в режим редактирования.

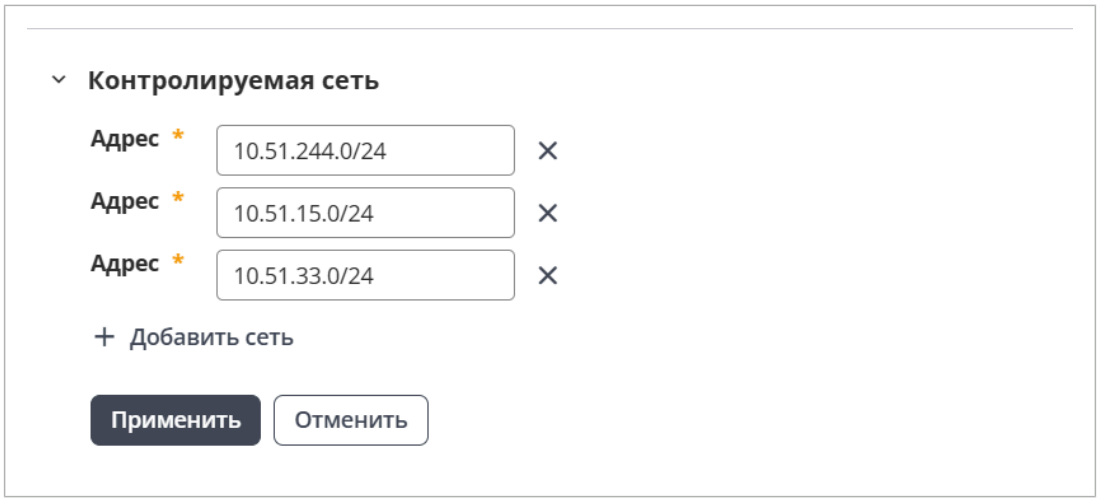


Рис. 13. Блок настроек сенсора «Контролируемая сеть» в режиме редактирования

4. Нажмите кнопку **+ Добавить сеть** и введите IP-адрес и маску подсети управляющего контура в качестве контролируемой подсети. Если требуется удалить добавленную ранее подсеть из списка, нажмите кнопку ✕ (**Удалить сеть**).
5. Нажмите кнопку **Применить** для сохранения внесенных изменений.

> ОСТОРОЖНО:
>
> Внесенные изменения в блоках **Контролируемая сеть** и **Управление файлами, извлеченными из трафика** сохраняются также при закрытии карточки сенсора, если в окне **Несохраненные данные** нажать кнопку **Закрыть**. Чтобы изменения не сохранились, нажмите **Отменить** в каждом измененном блоке, затем закройте карточку сенсора.

▸ **Результат шага:** Появится окно с предупреждением: `При смене контролируемой сети активы и сессии, не входящие в новую сеть, будут удалены.`

6. Нажмите **Подтвердить** для подтверждения всех изменений и запуска обновления списка активов в соответствии с указанными контролируемыми сетями.
7. Выполните шаги 2 - 6 для всех подключенных сенсоров, для которых нужно настроить контролируемую сеть.

▸ **Результат шага:**

- В список активов на странице **Активы** будут добавлены обнаруженные активы, IP-адреса которых входят в настроенные контролируемые сети.
- Каждому сетевому атрибуту обнаруженного актива будет присвоен сенсор, в чью контролируемую сеть входит IP-адрес атрибута. Присвоенный сенсор будет отображаться в поле **Сенсор** блока **Сетевые атрибуты** в **карточке актива**.
- На страницах раздела **Сетевые соединения** отображается информация о сетевых соединениях, обнаруживаемых в контролируемой сети.

9.3. Настройка парольной политики

Для настройки единой парольной политики для всех пользователей:

1. Перейдите на страницу **Администрирование → Пользователи → Парольная политика**.

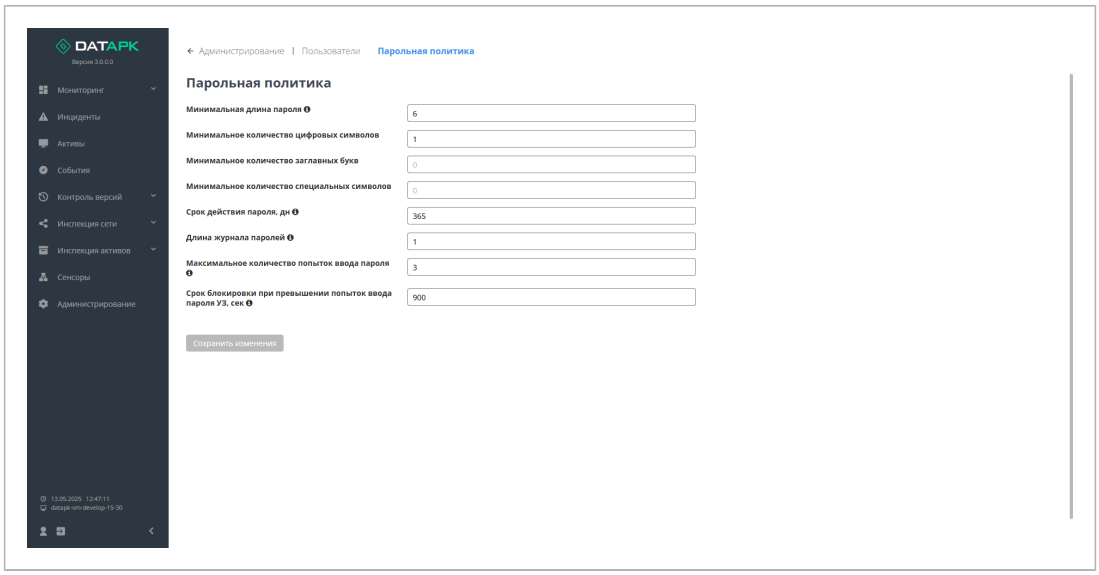


Рис. 14. Страница «Парольная политика»

2. Настройте следующие параметры парольной политики:
   - общее минимальное количество символов, которое должен содержать пароль;

     Внимание:

     Доступен ввод значений в диапазоне от 6 до 128. Суммарное количество цифровых символов, заглавных букв и спецсимволов не должно превышать это значение.

   - минимальное количество цифровых символов, которое должен содержать пароль;
   - минимальное количество символов в верхнем регистре, которое должен содержать пароль;
   - минимальное количество специальных символов, которое должен содержать пароль;
   - максимальное количество дней, в течение которых может действовать пароль (во время или до окончания указанного срока действия пароля его необходимо будет заменить);

     Внимание:

     Доступен ввод значений в диапазоне от `0` до `998`. Чтобы сделать все пароли бессрочными, введите значение `0`.

   - количество последних паролей пользователя, сохраняемых в Комплексе, которые нельзя будет использовать повторно;

     Внимание:

     Доступен ввод значений в диапазоне от `1` до `24`.

- максимальное количество попыток ввода пароля, после которых пользователь автоматически блокируется;

> Внимание:
>
> Доступен ввод значений в диапазоне от `0` до `12`. Чтобы отменить ограничение на количество попыток, введите значение `0`.

- срок автоматической блокировки пользователя при превышении попыток ввода пароля в секундах.

> Внимание:
>
> Чтобы отключить автоматическую блокировку, введите значение `0`.

3. Нажмите кнопку **Сохранить изменения**.
   - **Результат шага:** в правом верхнем углу страницы появится уведомление: `Парольная политика успешно обновлена`. Настроенная парольная политика начнет действовать для новых паролей (при изменении текущих паролей существующих учетных записей и при создании новых учетных записей).

9.4. Импорт справочников из архива

Для первоначальной настройки Комплекса предусмотрена возможность импорта всех справочников из единого архива формата `.tar` на странице **Импорт и экспорт**. Порядок ручной подготовки архива приведен в подразделе «Резервное копирование данных».

> Внимание:
>
> Источники событий импортируются отдельно из файла формата `*.json` на странице **Источники** (см. подраздел «Импорт источников событий»).

Справочники, доступные для импорта из архива на странице **Импорт и экспорт**, представлены в таблице ниже (Таблица 4. Справочники, которые можно импортировать).

Табл. 4. Справочники, которые можно импортировать

НАЗВАНИЕ СПРАВОЧНИКА	РАЗДЕЛ
События	
Правила разбора событий	Импорт правил разбора событий
Правила обогащения событий	Импорт правил обогащения событий
Схема событий	Импорт схемы событий
Источники событий	Импорт источников событий

Табл. 4. Справочники, которые можно импортировать

НАЗВАНИЕ СПРАВОЧНИКА	РАЗДЕЛ
Элементы иерархии	
Иерархия АСУ ТП	Импорт справочника с классификаторами АСУ ТП
Иерархия меток активов	Импорт меток
Группы активов	
Обнаружение уязвимостей *(CVE)*	
Справочники ПО и уязвимостей (CPE и CVE)	Импорт справочников CVE и CPE и файла сопоставления ПО с CPE
Сопоставление собранного сканерами ПО со справочником CPE	
Справочник БДУ ФСТЭК	Импорт справочника БДУ ФСТЭК России
Корреляция событий	
Правила корреляции	Импорт правил корреляции
Схема корреляции	Импорт схемы корреляции
Политика корреляции	Импорт политики корреляции
Сбор данных	
Группы сканеров	Импорт сканеров и их групп
Учетные данные активов	Импорт учетных данных активов
Задачи сбора данных	Импорт задач сбора данных
Инциденты	
Статусы инцидентов	Импорт статусов инцидентов
Обнаружение вторжений	
Правила обнаружения вторжений	Импорт правил обнаружения вторжений в формате *.json
Наборы сигнатур правил обнаружения вторжений в формате Suricata	Импорт правил обнаружения вторжений в формате *.rules

Табл. 4. Справочники, которые можно импортировать

НАЗВАНИЕ СПРАВОЧНИКА	РАЗДЕЛ
OVAL	
Группы Open Vulnerability and Assessment Language-определений вместе с OVAL-определениями	Импорт групп OVAL-определений
Скрипты OVAL	Импорт скриптов OVAL
Настройки OVAL	Импорт настроек OVAL

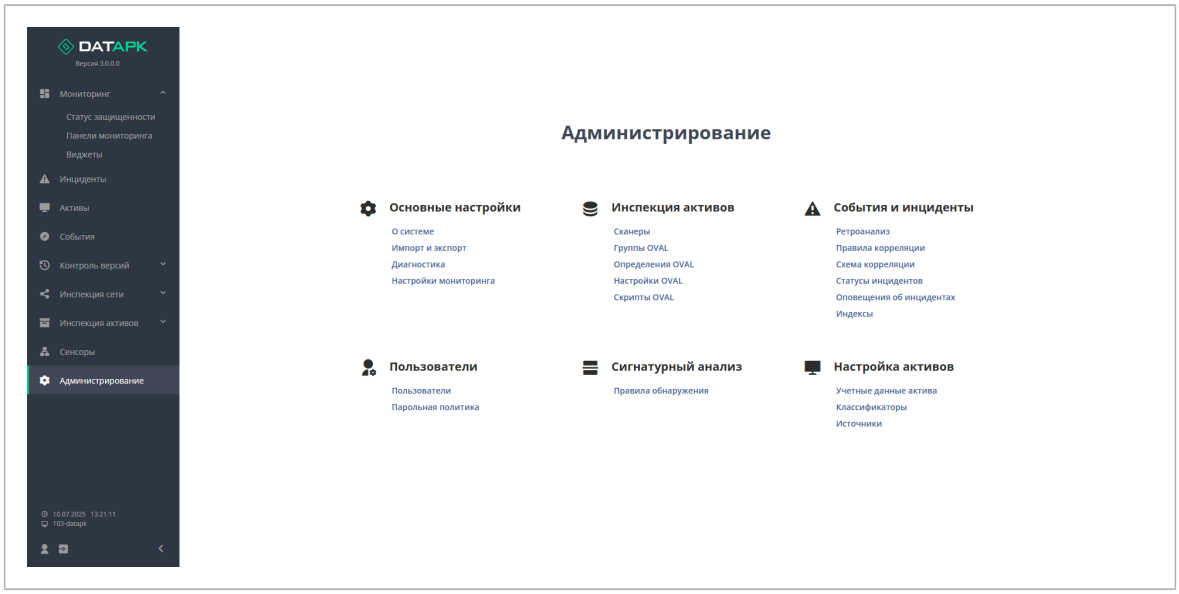


Рис. 15. Страница «Импорт и экспорт» в случае установки всех модулей UDV DATAPK Industrial Kit

9.5. Запуск обнаружения вторжений и синхронизация правил с сенсорами

Перед выполнением: Импортируйте правила обнаружения вторжений в Комплекс на странице **Импорт и экспорт**. Варианты импорта в разных форматах приведены в разделах «Импорт правил обнаружения вторжений в формате *.json» и «Импорт правил обнаружения вторжений в формате *.rules».

После импорта правил обнаружения вторжений необходимо включить сервис обнаружения вторжений на сенсорах и передать на них новые правила. Для этого:

1. Перейдите на страницу **Сенсоры**.
2. Нажмите на строку с сенсором, для которого нужно проверить статус службы обнаружения вторжений.
   - **Результат шага:** справа откроется карточка выбранного сенсора.
3. В открывшейся справа карточке включите или выключите службу обнаружения вторжений сенсора с помощью переключателя: если переключатель в состоянии — служба включена.
4. Перейдите на страницу **Администрирование → Правила обнаружения**.

5. Нажмите кнопку (**Синхронизация правил**).
   - **Результат шага:** правила будут обновлены на сенсорах, подключенных к текущему Комплексу, и активные правила начнут автоматически применяться для обнаружения вторжений на сенсорах, на которых включен этот сервис.

9.6. Первичная настройка модуля «Анализ промышленного сетевого трафика»

На странице **Сенсоры** для каждого сенсора доступны следующие настройки модуля «Анализ промышленного сетевого трафика» (UDV Network Traffic Analyzer), которые рекомендуется выполнить перед началом работы:

- Управление службой обнаружения вторжений — активация и деактивация службы обнаружения подозрительной и потенциально вредоносной сетевой активности в локальной сети.
- Управление сервисом регистрации событий техпроцесса — активация и деактивация сервиса, отвечающего за создание оповещений при обнаружении критичных функций техпроцесса в контролируемой сети.
- Управление режимом контроля сессий — переключение между режимом обучения Комплекса, при котором правила сессий создаются автоматически, и режимом обнаружения неразрешенных сессий в контролируемой сети.
- Управление регистрацией трафика — активация и деактивация регистраторов протоколов и сетевых атак, которые будет распознавать сенсор модуля «Анализ промышленного сетевого трафика».
- Управление записью трафика — активация и деактивация записи на диск трафика, обнаруживаемого модулем «Анализ промышленного сетевого трафика». При активации записи доступен выбор максимального объема диска, при достижении которого самые ранние записи трафика будут удалены.
- Управление файлами, извлеченными из трафика — активация и деактивация записи на диск файлов, которые обнаруживает модуль «Анализ промышленного сетевого трафика» в сетевом трафике. При активации записи доступен выбор максимального объема диска, при достижении которого самые ранние хранимые файлы будут удалены.

9.6.1. Управление регистрацией трафика

Для настройки списка протоколов и сетевых атак, которые будет распознавать сенсор модуля «Анализ промышленного сетевого трафика»:

1. Выберите сенсор на странице **Сенсоры**.
   - **Результат шага:** справа откроется карточка выбранного сенсора.
2. В карточке сенсора раскройте панель **Управление регистрацией трафика**, нажав кнопку слева от заголовка панели.

Рис. 16. Панель настроек «Управление регистрацией трафика»

3. В раскрывшейся панели активируйте или деактивируйте необходимые регистраторы с помощью переключателей: если переключатель в состоянии — регистратор активен.

9.6.2. Управление записью трафика

Для настройки записи трафика на сенсоре:

1. Выберите сенсор на странице **Сенсоры**.
   - **Результат шага:** справа откроется карточка выбранного сенсора.
2. В карточке сенсора перейдите в режим редактирования настроек, нажав кнопку (**Редактировать**) справа от заголовка блока **Управление записью трафика**.

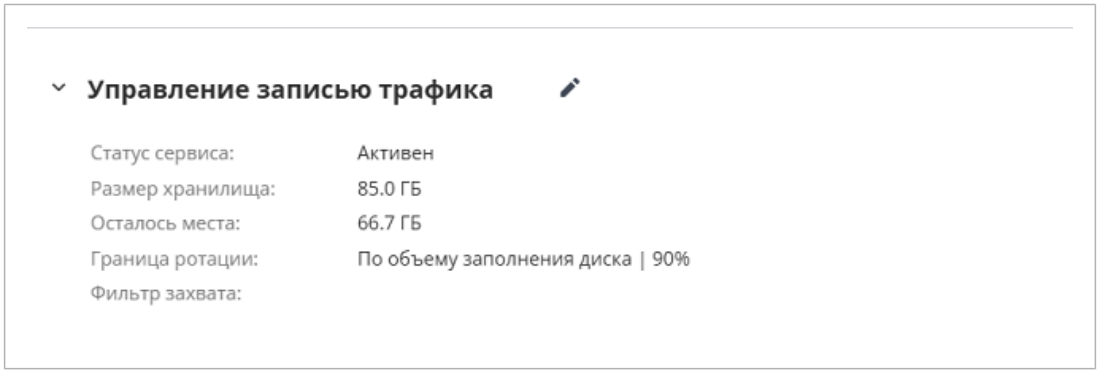


Рис. 17. Блок настроек сенсора «Управление записью трафика»

3. В режиме редактирования активируйте или деактивируйте запись трафика с помощью переключателя **Запись трафика**: если переключатель в состоянии — запись активна.

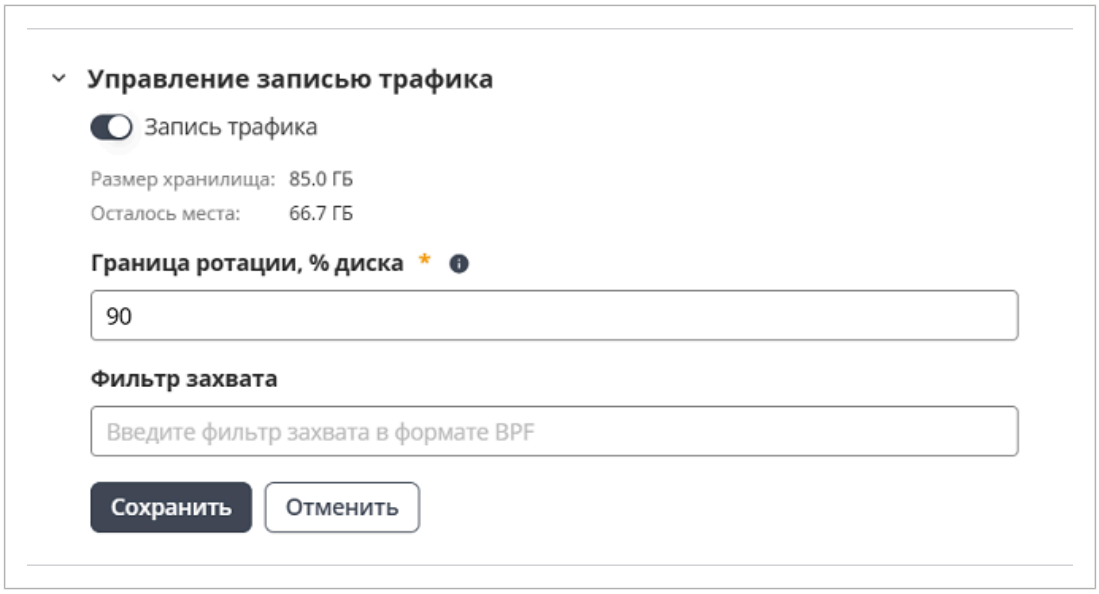


Рис. 18. Блок настроек сенсора «Управление записью трафика» в режиме редактирования

4. Если запись трафика активна, введите в поле **Граница ротации, % диска** максимальный объем диска[1] для хранения трафика. Значение задается в процентах от 1 до 100.

> Внимание:
>
> При достижении границ ротации самые ранние записи трафика будут удалены.

5. В поле **Фильтр захвата** введите параметры фильтра захвата трафика на языке фильтрации BPF.
6. Нажмите кнопку **Сохранить**, чтобы применить внесенные изменения.

> Прим.:
>
> При попытке закрыть карточку сенсора в режиме редактирования блока **Управление записью трафика** можно столкнуться с цикличным появлением окна **Несохраненные данные**. Чтобы корректно завершить настройку сенсора, нажмите кнопку **Сохранить** для применения текущих настроек, либо **Отменить** для выхода из режима редактирования без сохранения внесенных изменений.

- **Результат шага:** если запись трафика активна, записи будут доступны для скачивания на вкладке **Пакеты** страницы **Инспекция сети → Сетевые соединения**. Подробнее см. инструкцию «Экспорт копии сетевого трафика»

9.6.3. Управление файлами, извлеченными из трафика

Для настройки извлечения и хранения файлов на сенсоре:

1. Выберите сенсор на странице **Сенсоры**.
   - **Результат шага:** справа откроется карточка выбранного сенсора.

1. Ограничение применяется к логическому разделу диска, выделенному для хранения трафика перед установкой Комплекса уровня Sensor.

2. В карточке сенсора перейдите в режим редактирования настроек, нажав кнопку (**Редактировать**) справа от заголовка блока **Управление файлами, извлеченными из трафика**.

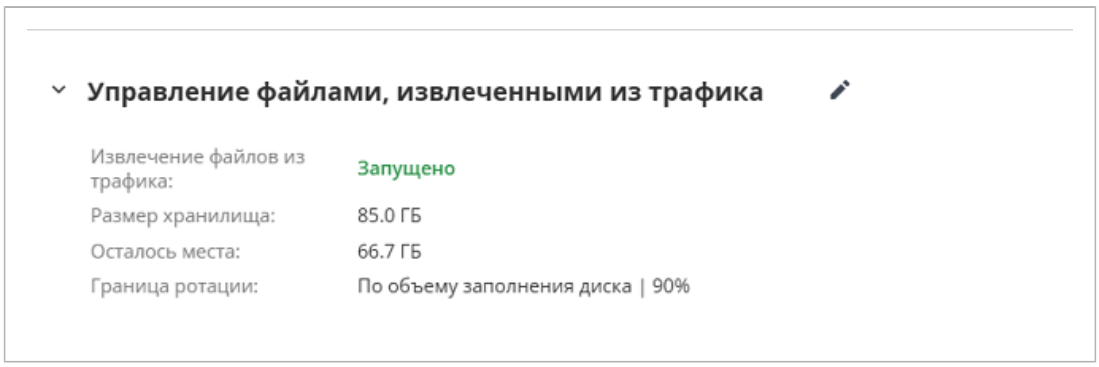


Рис. 19. Блок настроек сенсора «Управление файлами, извлеченными из трафика»

3. В режиме редактирования активируйте или деактивируйте извлечение файлов с помощью переключателя **Извлечение файлов из трафика**: если переключатель в состоянии — извлечение файлов активно.

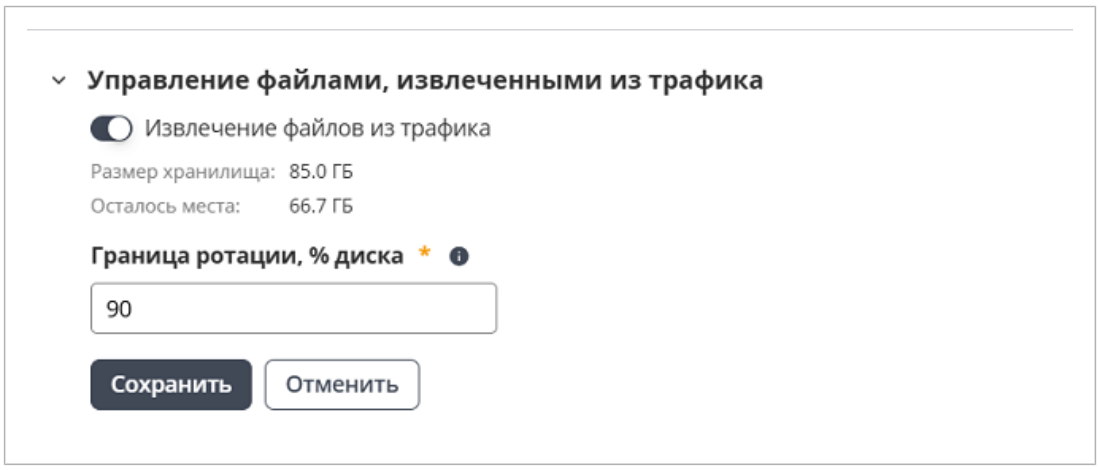


Рис. 20. Блок настроек сенсора «Управление файлами, извлеченными из трафика» в режиме редактирования

4. Если извлечение файлов из трафика активно, введите в поле **Граница ротации, % диска** максимальный объем диска[2] для хранения файлов. Значение задается в процентах от 1 до 100.
5. Нажмите кнопку **Сохранить**, чтобы применить внесенные изменения.

> ОСТОРОЖНО:
>
> Внесенные изменения в блоках **Контролируемая сеть** и **Управление файлами, извлеченными из трафика** сохраняются также при закрытии карточки сенсора, если в окне **Несохраненные данные** нажать кнопку **Закрыть**. Чтобы изменения не сохранились, нажмите **Отменить** в каждом измененном блоке, затем закройте карточку сенсора.

Результат шага: если извлечение файлов активно, файлы будут доступны для скачивания на вкладке **Файлы** на странице **Инспекция сети → Сетевые соединения**. Подробнее см. инструкцию «Экспорт файлов, обнаруженных в сетевом трафике».

2. Ограничение применяется к логическому разделу диска, выделенному для хранения извлеченных файлов перед установкой Комплекса уровня Sensor.

9.7. Проверка работоспособности Комплекса

Чтобы убедиться в работоспособности Комплекса после подключения к нему сенсоров, необходимо:

1. Проверить работоспособность системы передачи данных от сенсоров к Комплексу уровня Management. Подробнее см. в разделе «Проверка работоспособности системы передачи данных по иерархии».
2. Проверить обнаружение активов при прослушивании трафика после настройки контролируемой сети на сенсорах. Подробнее см. в разделе «Проверка обнаружения активов из контролируемой сети».
3. Проверить работоспособность модуля «Анализ промышленного сетевого трафика». Подробнее см. в разделе «Проверка работоспособности модуля «Анализ промышленного сетевого трафика»».

9.7.1. Проверка работоспособности системы передачи данных по иерархии

Для проверки работоспособности системы передачи данных по иерархии вы можете воспользоваться следующими способами:

1. Просмотр статуса синхронизации настроек и получения данных с Комплекса уровня Sensor:
   a. На Комплексе уровня Management перейдите на страницу **Сенсоры**.
   б. Выберите сенсор.
   - **Результат шага:** справа откроется карточка с описанием и настройками выбранного сенсора.

   в. Просмотрите статусы синхронизации настроек и получения данных с сенсора.

Рис. 21. Статусы исправной синхронизации настроек и получения данных с сенсора

> Подсказка:
>
> В качестве дополнительного способа просмотра наличия ошибок получения данных воспользуйтесь панелью мониторинга «Сбор данных».

2. Просмотр ошибок на панели мониторинга **Эксплуатационный мониторинг**. Для просмотра:

а. Убедитесь, что объекты раздела **Мониторинг** ранее были созданы или импортированы (см. раздел «Импорт сохраненных объектов в экспертном режиме просмотра событий»).

б. Перейдите на страницу **Мониторинг → Панели мониторинга**.

в. Если на странице отображается панель мониторинга с названием, отличным от **Эксплуатационный мониторинг**, нажмите на ссылку **Панели мониторинга** в левом верхнем углу.

г. Выберите из списка панель мониторинга **Эксплуатационный мониторинг**.

д. Установите нужный временной период и убедитесь, что отсутствуют ошибки синхронизации настроек и получения данных с сенсора.

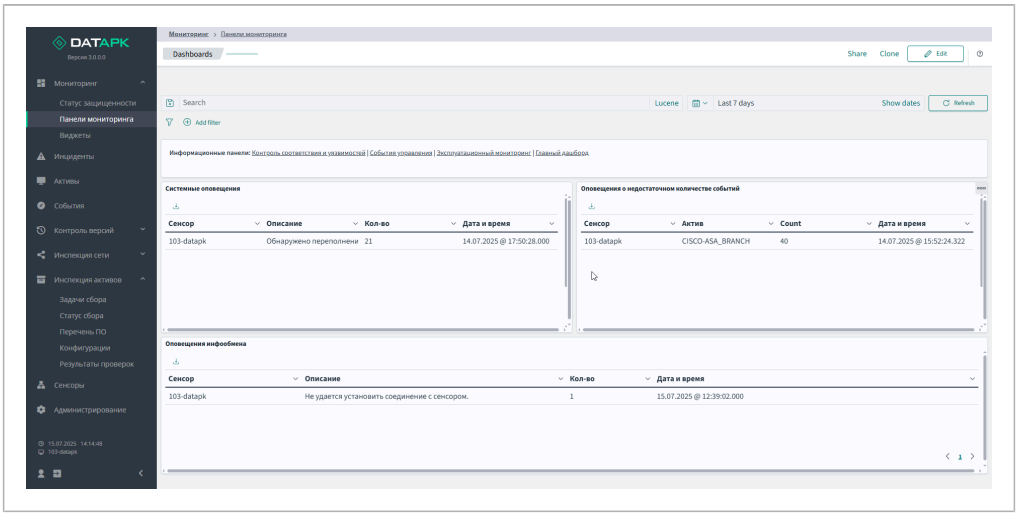


Рис. 22. Панель мониторинга «Эксплуатационный мониторинг»

9.7.2. Проверка обнаружения активов из контролируемой сети

Для проверки обнаружения активов в результате настройки контролируемой сети на сенсорах:

1. Перейдите на страницу **Активы** Комплекса уровня Management.
2. Убедитесь, что в группе активов `Неизвестный тип` отображаются:
   - активы с MAC-адресом и IP-адресом — узлы, соответствующие контролируемой подсети;
   - активы с MAC-адресом, но без IP-адреса — узлы, принадлежность которых к контролируемой подсети невозможно определить в автоматическом режиме из-за отсутствия IP-адреса.

9.7.3. Проверка работоспособности модуля «Анализ промышленного сетевого трафика»

Для проверки работоспособности модуля «Анализ промышленного сетевого трафика»:

1. Перейдите на страницу **Инспекция сети → Сетевые соединения**.
   - **Результат шага:** откроется вкладка **Сессии**.

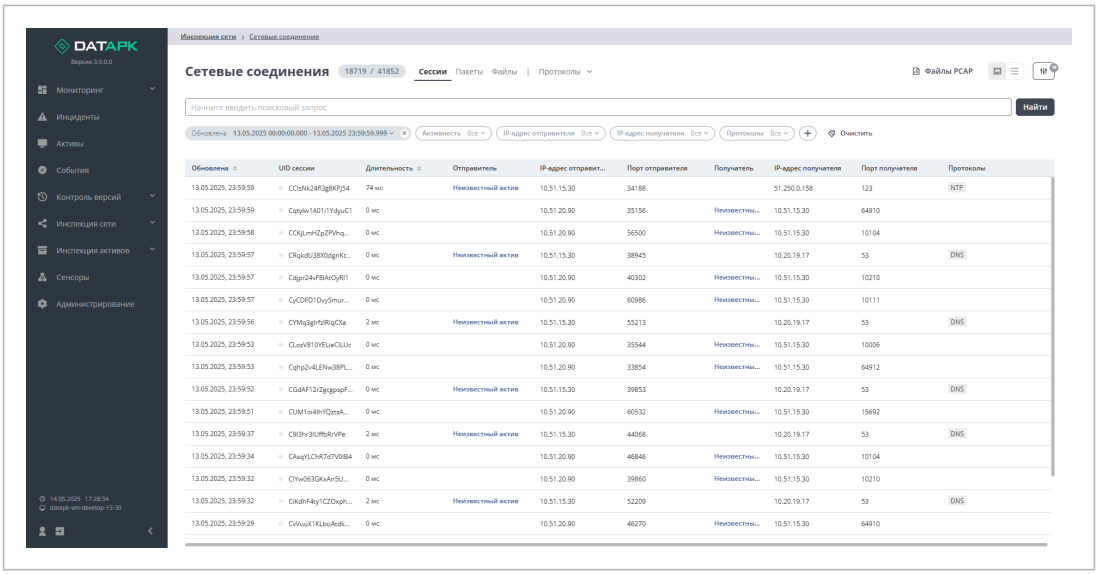


Рис. 23. Страница «Сетевые соединения»

2. Сбросьте фильтр **Обнаружена**.
3. Убедитесь, что модуль обнаруживает новые сессии: в столбце **Обнаружена** есть записи с текущим временем.
4. Убедитесь, что модуль отображает активные сессии: в столбце **Сессия (UID)** активные сессии имеют иконку зеленого цвета.

10. Мониторинг событий

В этом разделе:

1. **Поиск и просмотр событий в упрощенном режиме**
2. **Просмотр событий и создание запросов в экспертном режиме**
3. **Просмотр главной панели мониторинга «Статус защищенности»**
4. **Импортируемые панели мониторинга**
5. **Настройка сбора событий**
6. **Настройка и управление мониторингом**

Визуализация событий

Комплекс регистрирует события и их атрибуты: дату и время обнаружения, данные о протоколе взаимодействия, адреса источника, цели и другие. Дата и время хранятся во временной зоне UTC и адаптируются под время рабочей станции, с которой ведется просмотр. Если время на рабочей станции отличается от времени на операционной системе Комплекса, то и в интерфейсе будут обнаружены расхождения.

Все события отображаются на странице **События** и в экспертном режиме в порядке их обнаружения от последних к более ранним. Чтобы посмотреть подробную информацию о событии, нажмите на него.

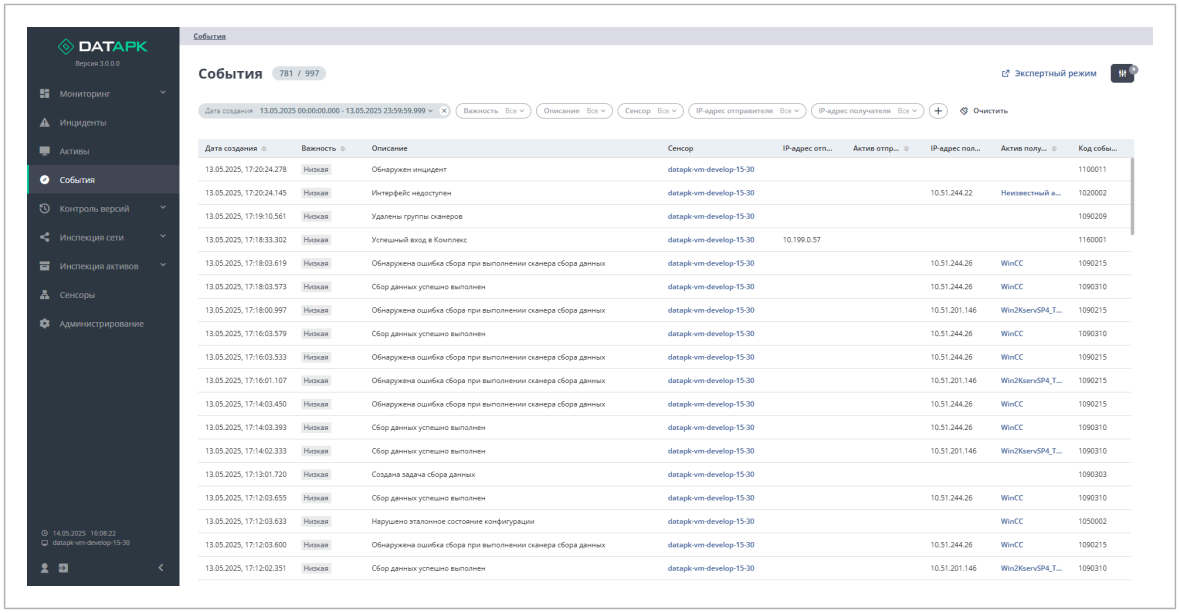


Рис. 24. Список событий на странице «События»

Событие можно развернуть и посмотреть подробности в виде боковой панели (карточки события).

> Подсказка:
>
> Для обновления данных на странице сбросьте вручную фильтр **Дата создания**. Для этого нажмите кнопку ✕ справа от фильтра.

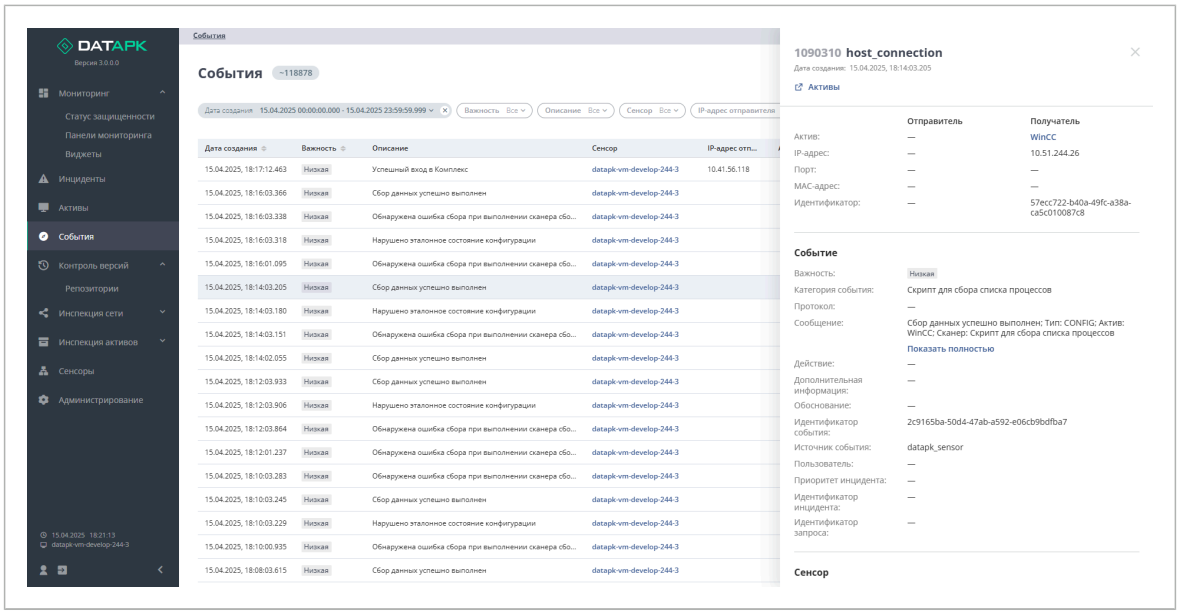


Рис. 25. Карточка события с подробной информацией о событии

В разделе **Мониторинг** предусмотрено сохранение и дальнейшее использование результатов нормализации событий в виде объектов. Объектами раздела **Мониторинг** являются сохраненные запросы, а также графические объекты на страницах **Виджеты** и **Панели мониторинга**.

Страница **Мониторинг → Статус защищенности** является главной панелью мониторинга Комплекса для отслеживания статистики и изменений ключевых оперативных данных в реальном времени.

На странице **События** предусмотрен переход на страницу сенсора из события. При нажатии на название сенсора открывается страница **Сенсоры**, на которой отображается подробная информация о сенсоре, участвующем в событии.

Также возможен переход на страницу **Сессии** из событий модуля «Анализ промышленного сетевого трафика». При переходе по ссылке Сессия, расположенной в карточке события, откроется страница **Сессии** с предварительно установленным фильтром **UID сессии**.

Генерация событий

Комплекс предоставляет возможности по выявлению критичных событий ИБ, называемых инцидентами. Подробнее см. в главе «Работа с инцидентами».

События Комплекса делятся на два типа:

- внутренние события, автоматически генерируемые собственными сервисами Комплекса;
- внешние события, получаемые от настроенных источников и в результате активного сбора событий с активов.

> Внимание:
>
> Получение внешних событий недоступно на сертифицированной версии Комплекса и при отсутствии установленного модуля «Управление внешними событиями».

Все типы внешних событий, необходимых для обеспечения информационной безопасности АСУ ТП, могут быть зарегистрированы Комплексом, если корректно настроена их отправка с активов.

Сбор событий с активов выполняется при помощи протоколов TCP/UDP и SNMP. Прием реализуется механизмами Syslog (стандарты RFC 3164 и RFC 5424), SNMP-trap и Eventlog. Предусмотрена возможность интеграции с внешними системами для отправки событий с Комплекса по протоколу Syslog путем настройки конфигурационных файлов в директории `etc/logstash` Комплекса уровня Management. Для сбора событий, не предусмотренных по умолчанию, можно также создать сканеры с собственными Python-скриптами сбора данных.

Администратор Комплекса, имеющий доступ к консольному управлению, может настроить включение и отключение, а также критичность служебных событий. Для этого в файл `manager.env` добавляются соответствующие переменные. Ознакомиться с доступными для настройки переменными вы можете в разделе «Описание служебных источников событий».

Внимание:

Служебные источники не отображаются на странице **Администрирование** → **Настройка активов** → **Источники**.

Поиск событий

Для работы с событиями доступны следующие страницы:

1. Страница **События** — данная страница отображает внутренние события Комплекса.
2. Страница **Экспертный режим** — данная страница отображает как внутренние, так и внешние события Комплекса.

Для работы с внутренними событиями доступна страница **События**. При наличии установленного модуля «Анализ промышленного сетевого трафика» на странице **События**, помимо внутренних событий, отображаются и события от созданных правил обнаружения вторжений, а также самого модуля «Анализ промышленного сетевого трафика».

Поиск событий на странице **События** можно выполнять с помощью фильтров. Наименования фильтров совпадают с наименованиями полей событий. Подробнее о полях событий см. в разделе «Описание полей событий в экспертном режиме страницы «События»».

Инструменты для работы с запросами (создание нового запроса, сохранение текущего запроса, открытие сохраненного результата) расположены в экспертном режиме страницы **События**.

Список всех событий, генерируемых Комплексом, приведен в справочном разделе «События Комплекса».

Хранение событий

Внешние события, которые доступны к просмотру через веб-интерфейс, хранятся в оперативном архиве — индексе `datapk_events_[дата_создания_индекса]`. По умолчанию при превышении размера или времени хранения в индексе события переходят в глубокий архив. При достижении лимита объема или времени хранения в глубоком архиве события удаляются безвозвратно. Такой процесс называется ротацией событий. Архивированные индексы событий расположены в директории `/var/backups/elasticsearch/indices` Комплекса уровня Management.

Общий объем зарегистрированных внешних событий ограничен значениями, указанными в переменных файла `manager.env`. Регистрацию новых событий при переполнении оперативного архива можно отключить.

Внутренние события, которые доступны к просмотру через веб-интерфейс, хранятся в базе данных сервиса `udv-postgresql`. Для внутренних событий также реализован настраиваемый механизм ротации: архив внутренних событий создается раз во временной промежуток, заданный пользователем в переменной

`EVENTS_RETENTION_MONTHS`; архивные события, время хранения которых превышено, удаляются. Отключение архивных событий происходит автоматически.

Кроме того, пользователь может установить максимально допустимый объем архива событий и при его достижении регистрация новых событий будет останавливаться.

Подробнее о работе и настройке механизмов хранения событий см. в разделе «Механизмы хранения событий».

10.1. Поиск и просмотр событий в упрощенном режиме

При обновлении страницы **События** все результаты фильтрации сохраняются.

10.1.1. Просмотр событий

Для просмотра события:

1. Нажмите на событие.
   - **Результат шага:** справа отобразится карточка события с подробной информация о событии.

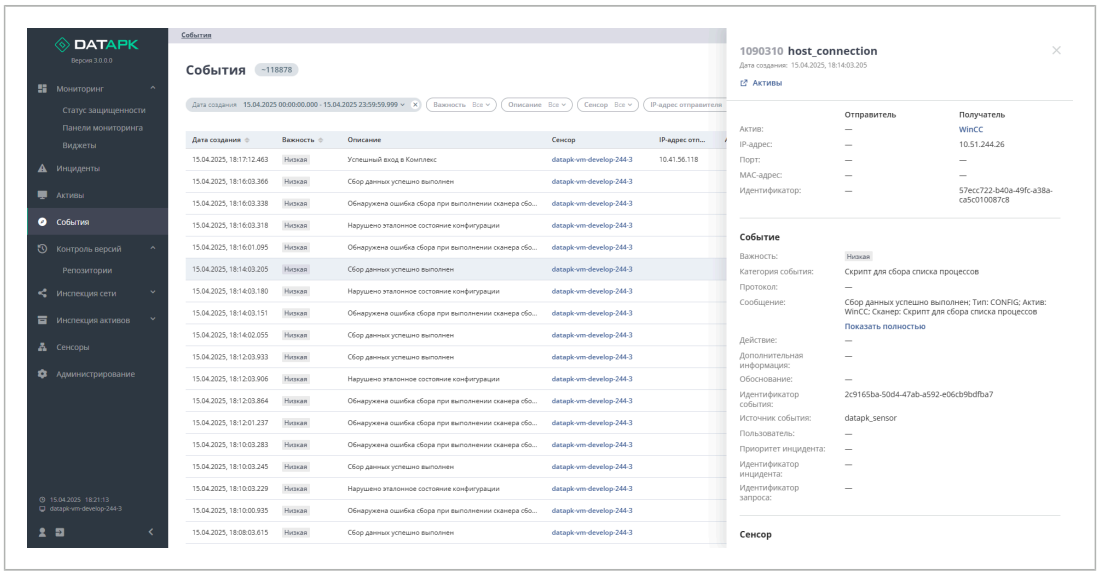


Рис. 26. Подробная информация о событии

2. Для перехода к активам, связанным с событием, нажмите ссылку Активы в верхней части карточки события.

> Внимание:
>
> Ссылка Активы доступна, если к моменту регистрации события Комплекс уже зарегистрировал активы, чьи сетевые атрибуты и идентификаторы присутствуют в событии в полях **Отправитель** и **Получатель**.

   - **Результат шага:** откроется страница **Активы** со списком активов, связанных с событием.

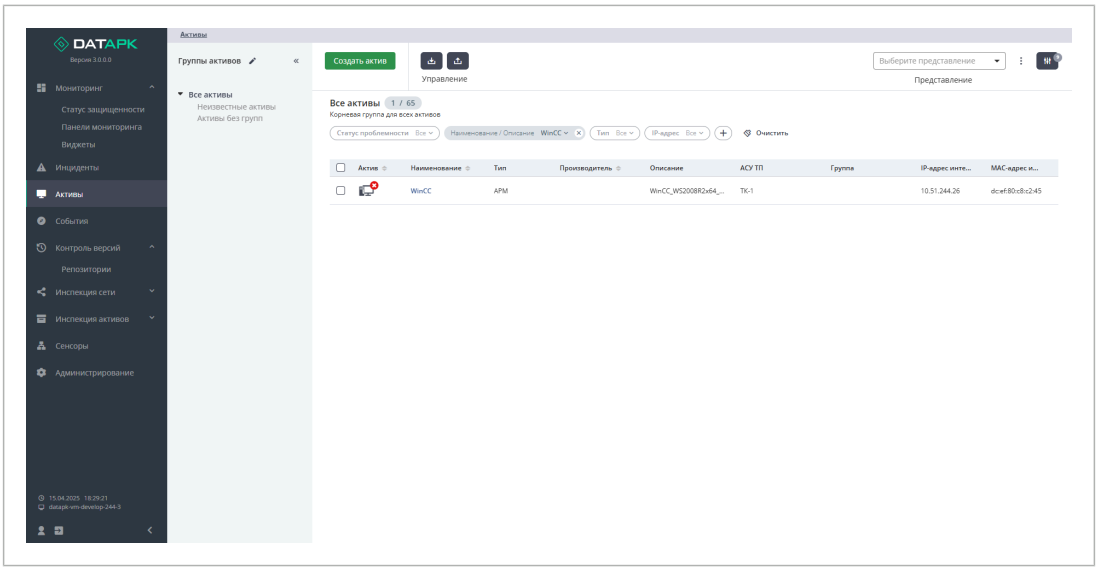


Рис. 27. Активы, связанные с событием, на странице «Активы»

3. Для перехода к сессии, связанной с событием, нажмите ссылку Сессия в верхней части карточки события.
   - **Результат шага:** откроется страница **Сетевые соединения → Сессии** с сессией, связанной с событием.

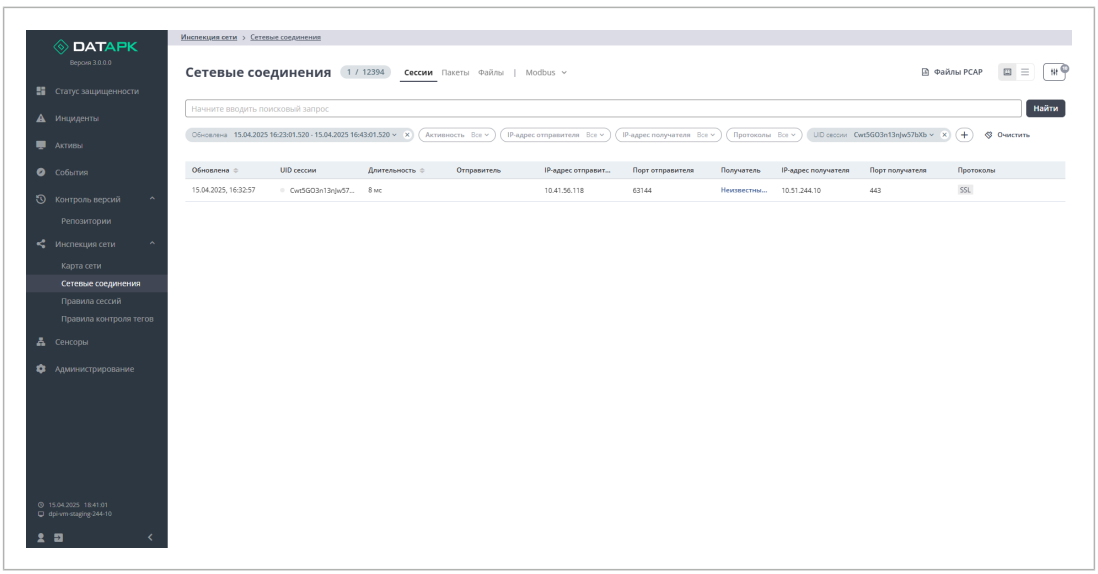


Рис. 28. Сессия, связанная с событием, на странице «Сессии»

10.1.2. Поиск событий с помощью фильтров

Фильтры — это набор инструментов на странице **События** для фильтрации событий по заданным параметрам. Фильтрация выполняется после ввода значения в фильтр. В следующих фильтрах можно выбрать предустановленные значения из списка:

- **Важность** — `Низкая` и `Критическая`;
- **Тип события** — различные значения типов событий (подробнее см. в разделе «Поддерживаемые типы событий»);
- **Сенсор** — автоматически дополняемый список сенсоров, подключенных к текущему Комплексу.

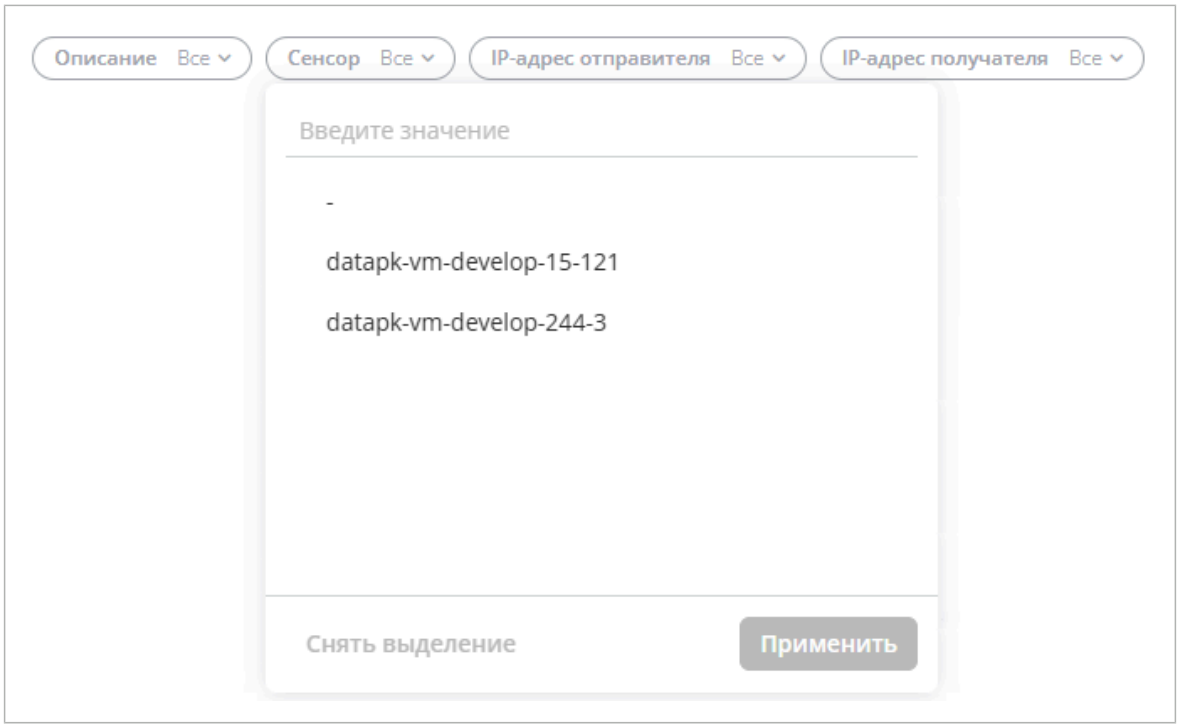


Рис. 29. Поле с предустановленными значениями

Для поиска события с помощью фильтра:

1. Нажмите на фильтр.
   - **Результат шага:** отобразится поле ввода значения фильтра.

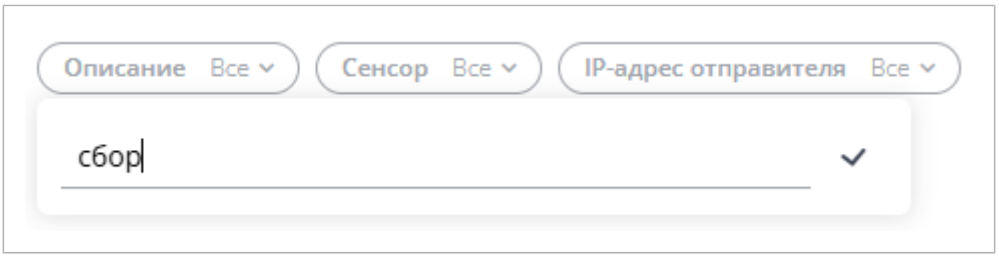


Рис. 30. Поле ввода значения фильтра

2. Введите значение в поле.
3. Нажмите кнопку ✔.
   - **Результат шага:** результаты поиска будут отображены на странице.
4. При необходимости повторите шаги 1-3 с другими фильтрами для более точного поиска событий.

10.1.3. Поиск событий с помощью фильтра «Дата создания»

По умолчанию на странице **События** отображаются события за текущую дату.

Для поиска события с помощью фильтра **Дата создания**:

1. Выберите фильтр **Дата создания**.
   - **Результат шага:** откроется календарь выбора временного периода, в котором были зарегистрированы события.

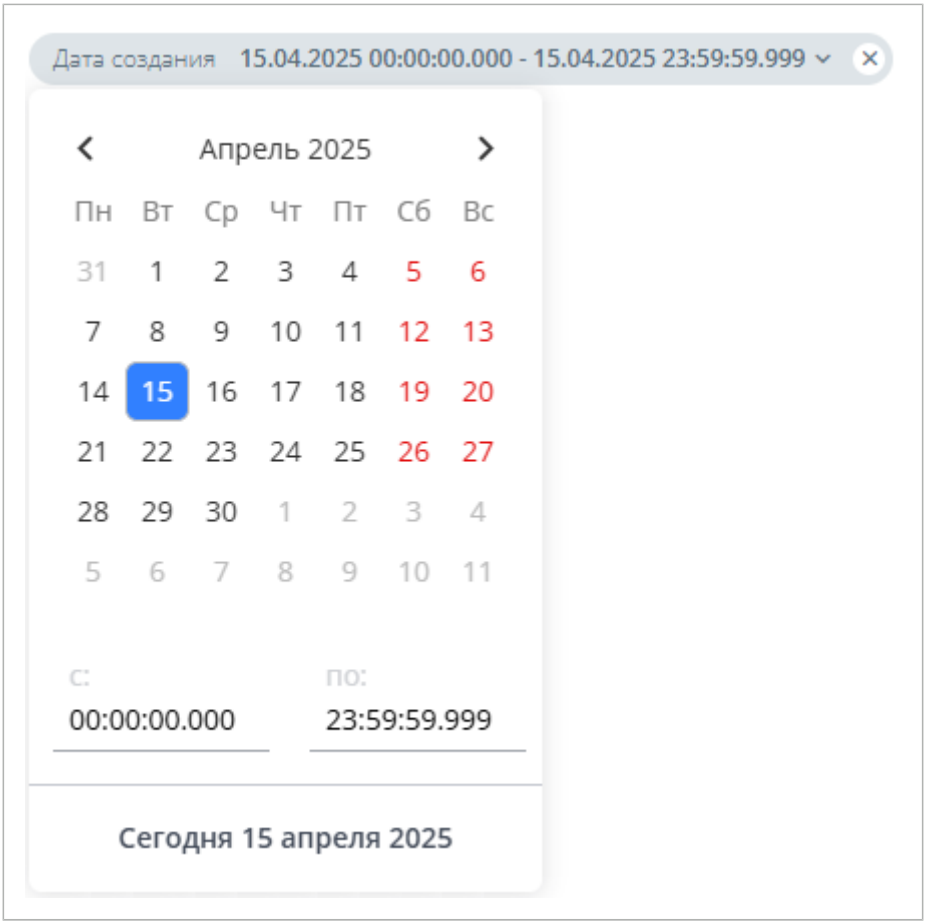


Рис. 31. Календарь выбора временного периода регистрации событий

2. Выберите начальную дату.

> Подсказка:
>
> - Для выбора текущего дня в качестве всего диапазона нажмите `Сегодня [текущая дата]` в нижней части фильтра.
> - Для быстрой навигации по месяцам и годам нажмите на название месяца и года в верхней части фильтра: первое нажатие отображает список всех месяцев, второе нажатие отображает список из 12 лет, ближайших к текущему году.

- **Результат шага:** автоматически отобразятся события за выбранную дату.

3. При необходимости выберите конечную дату.

- **Результат шага:** в календаре будут выделены все даты между выбранными начальной и конечной. На странице автоматически отобразятся события за установленный временной период.

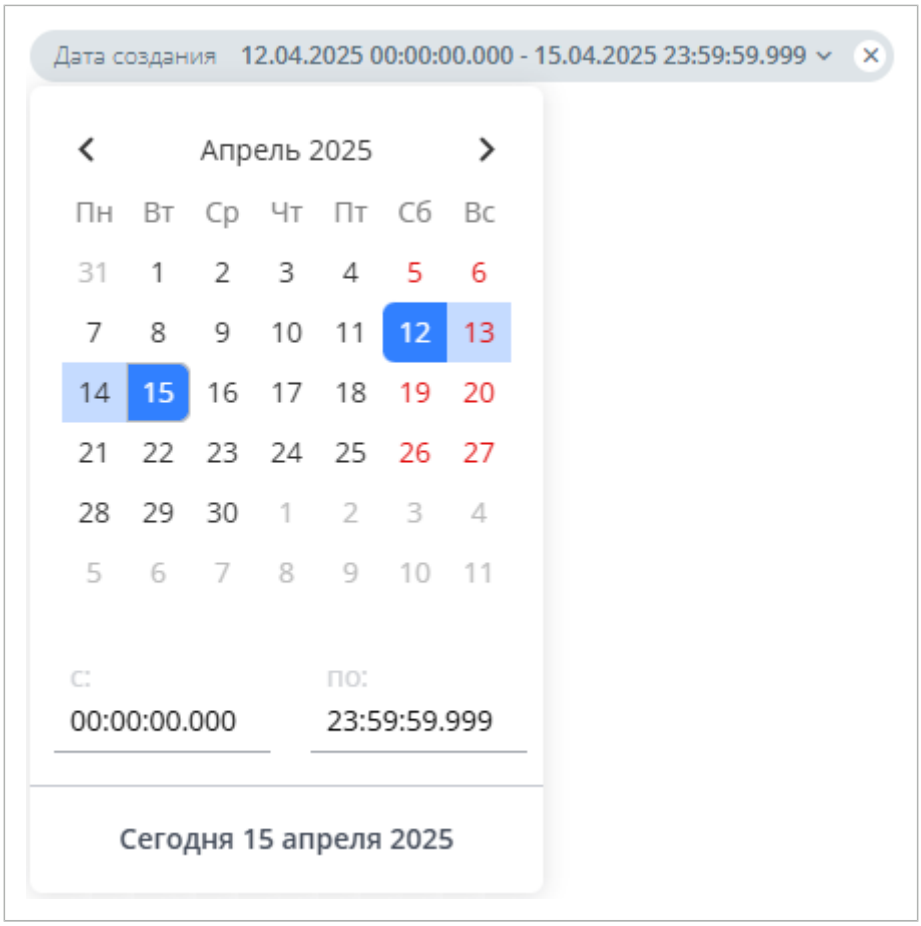


Рис. 32. Выбранные даты в календаре

4. При необходимости введите время в поля **с:** и **по:** (время вводится в формате `ЧЧ:ММ:СС.ССС`).

> Внимание:
>
> Если выбраны разные начальная и конечная даты, поля **с:** и **по:** будут работать следующим образом:
> - в поле **с:** необходимо указать время для начальной даты;
> - в поле **по:** необходимо указать время для конечной даты.

▸ **Результат шага:** на странице автоматически отобразятся события за установленный временной период.

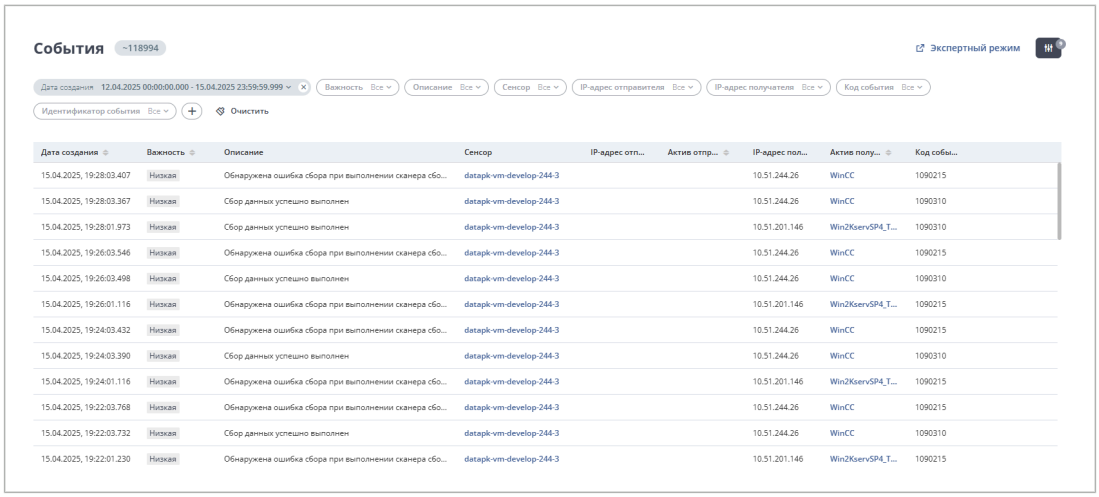


Рис. 33. Отображение событий за установленный временной период

5. Для очистки результатов поиска по выбранному временному периоду нажмите кнопку ✕ справа от фильтра **Дата создания**.
   - **Результат шага:** на странице автоматически отобразятся события за текущую дату.

10.1.4. Добавление фильтров

Для добавления фильтров на страницу **События**:

1. Нажмите кнопку ⊕, расположенную справа от последнего фильтра.
   - **Результат шага:** Отобразится выпадающий список с доступными фильтрами. Фильтры, уже выбранные для отображения на странице, имеют серый цвет и иконку ✔ слева от названия.

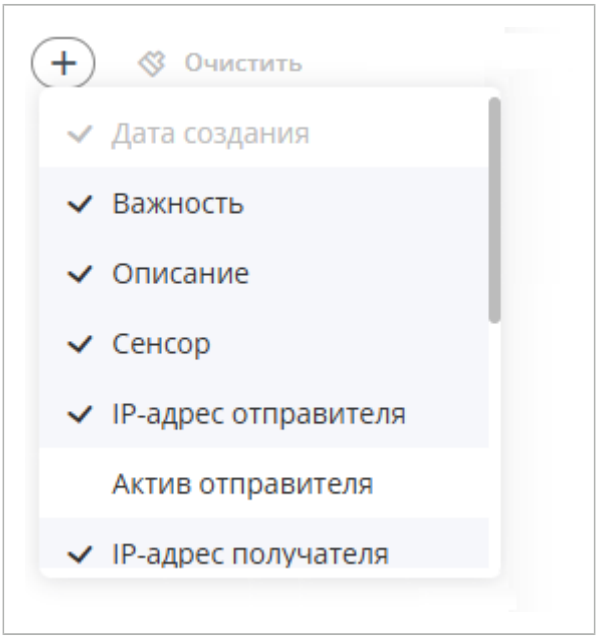
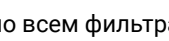


Рис. 34. Список доступных фильтров

2. В выпадающем списке выберите необходимые фильтры.
   - **Результат шага:** выбранные фильтры отобразятся на панели фильтров.

10.1.5. Удаление фильтров

Для удаления фильтров со страницы **События**:

1. Нажмите кнопку , расположенную под строкой поиска.
2. В выпадающем списке отмените выбор необходимых фильтров.
   - **Результат шага:** фильтры перестанут отображаться на панели фильтров.
3. Для очистки результатов поиска воспользуйтесь одним из способов:
   - для очистки результатов по одному из фильтров нажмите кнопку справа от фильтр;
   - для очистки результатов по всем фильтрам нажмите кнопку  справа от всех фильтров.
   - **Результат шага:** результаты поиска будут автоматически обновлены на странице.

10.2. Просмотр событий и создание запросов в экспертном режиме

Перед выполнением: Перед созданием запросов убедитесь, что создан шаблон индекса согласно инструкции «Создание шаблона индекса».

Расширенный просмотр событий и настройка нормализации осуществляется на странице **События** → **Экспертный режим**.

Запросы и фильтры можно сохранять для дальнейшего экспорта или для графической визуализации результатов. Инструменты для работы с запросами (создание нового запроса, сохранение текущего запроса, открытие сохраненного результата) расположены в правой верхней части страницы **Экспертный режим**.

В левой части страницы и в каждом событии расположены поля, для которых генерируются уникальные данные. Подробнее о полях событий см. в разделе «Описание полей событий в экспертном режиме страницы «События»».

Для создания нового запроса:

1. Перейдите на страницу **События**.
2. Нажмите кнопку в верхнем правом углу.
   - **Результат шага:** откроется страница **Экспертный режим**
3. Нажмите кнопку напротив необходимых полей в блоке **Available fields**.
   - **Результат шага:** будут отображены только выбранные поля.

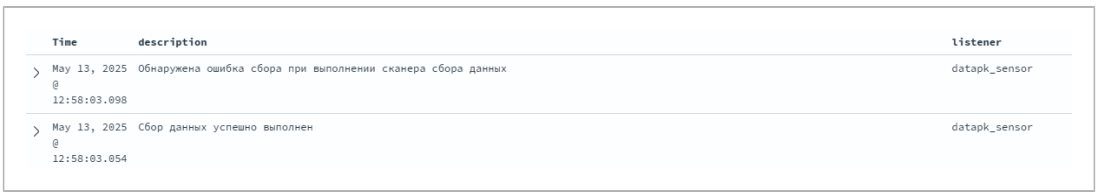


Рис. 35. Результат выбора столбцов «description» и «listener»

4. Для ввода запросов в формате Lucene воспользуйтесь полем **Search**.
5. Для добавления фильтров нажмите кнопку **+ Add filter**.
6. Для сохранения запроса в виде объекта нажмите кнопку **Save** в верхнем правом углу страницы.
7. В появившемся окне введите название сохраняемого объекта.

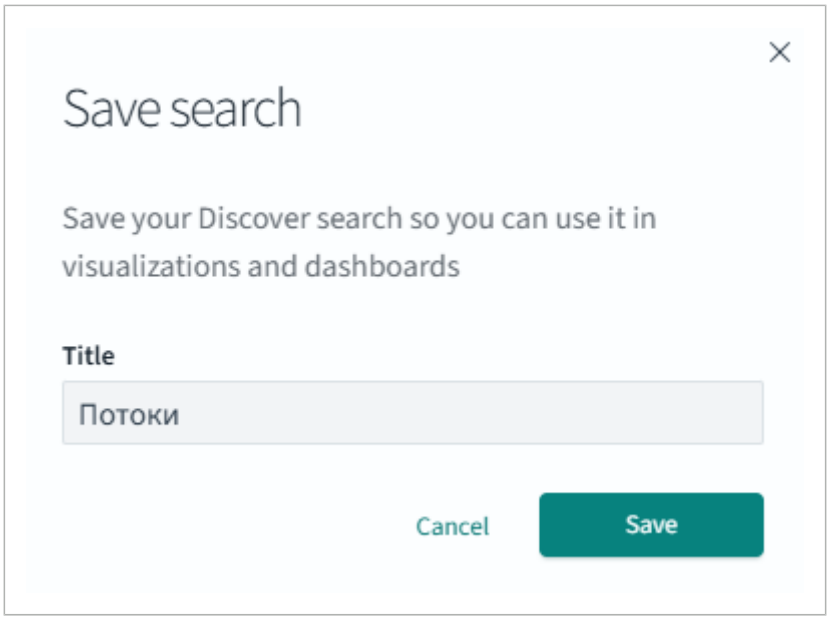


Рис. 36. Окно сохранения поиска

8. Нажмите кнопку **Save**.
9. Перейдите на страницу **Администрирование → Основные настройки → Настройки мониторинга**.
10. Выберите вкладку **Saved Objects**.
11. Выберите тип `search` и убедитесь, что в списке запросов присутствует сохраненный объект.

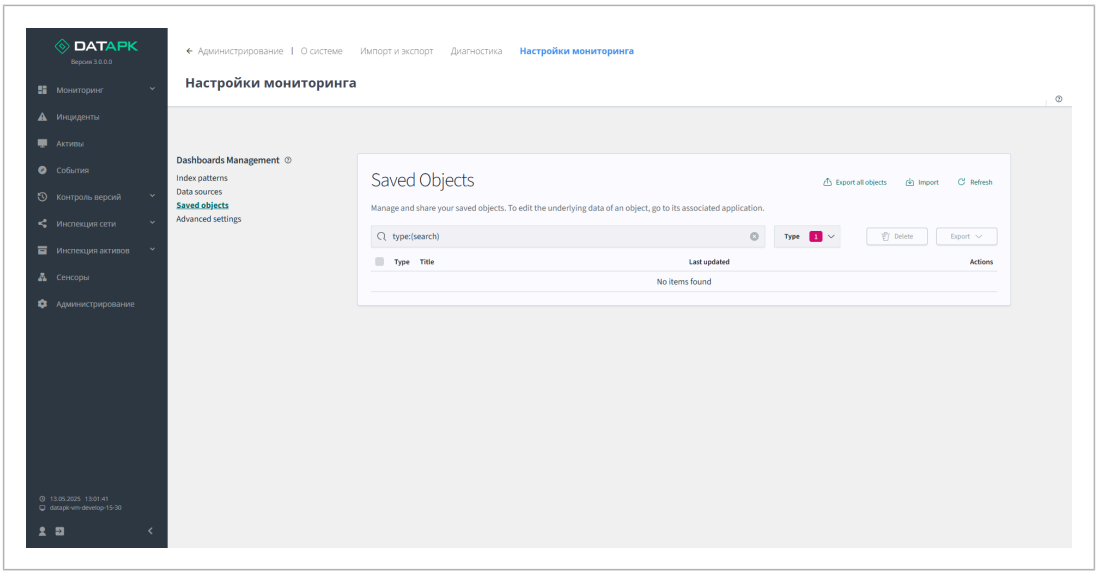


Рис. 37. Выбор типа «search» в разделе «Saved objects» страницы «Настройки мониторинга»

12. Для применения сохраненного запроса перейдите на страницу **События → Экспертный режим**, нажмите кнопку **Open** в верхнем правом углу страницы и выберите из списка сохраненный запрос.

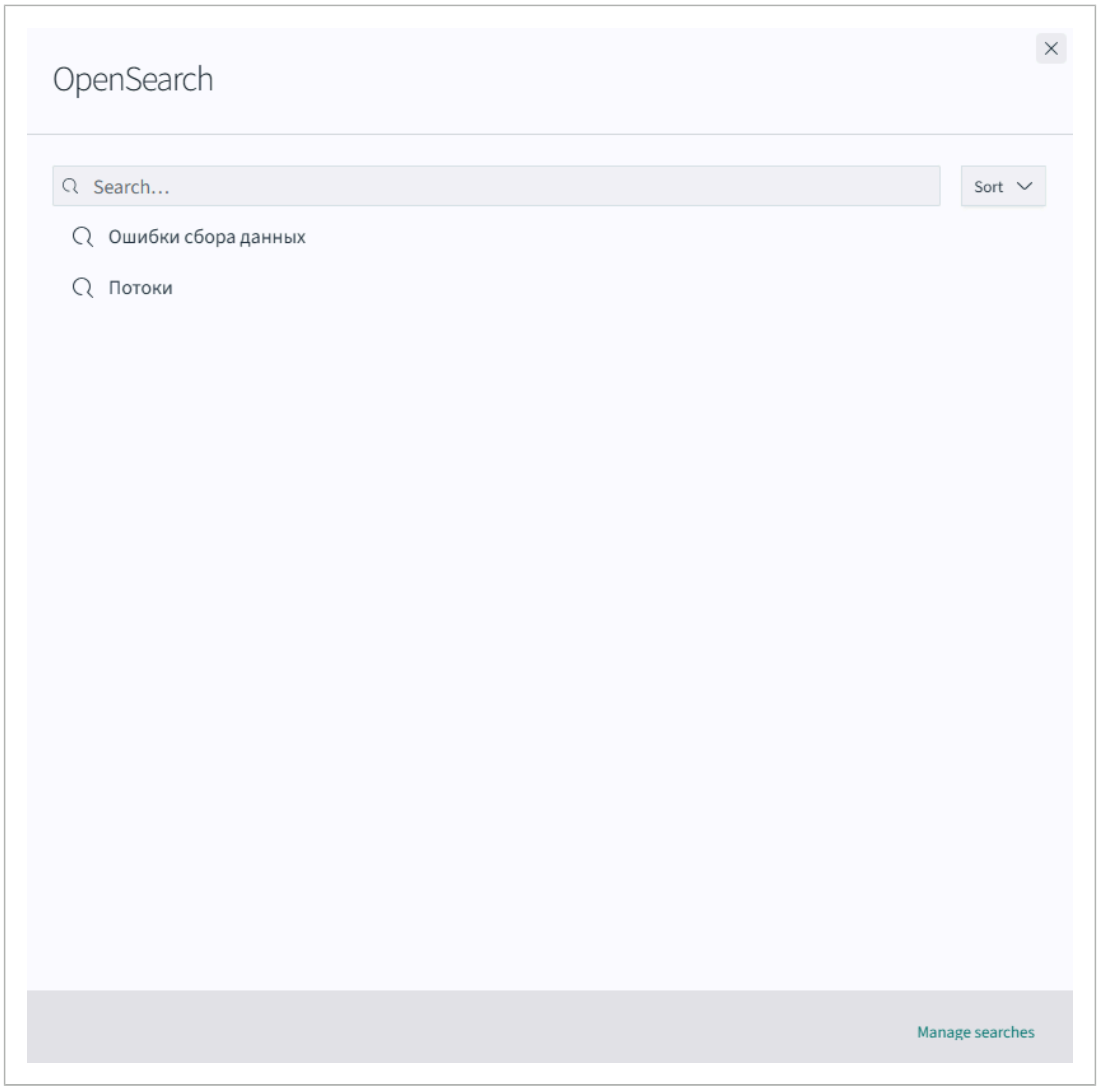


Рис. 38. Окно выбора поискового запроса

10.3. Просмотр главной панели мониторинга «Статус защищенности»

Общая информация

Страница **Мониторинг → Статус защищенности** является главной панелью мониторинга Комплекса для отслеживания статистики и изменений ключевых оперативных данных в реальном времени.

Пользователь с ролью `Просмотр панели мониторинга` может просматривать страницу **Статус защищенности** непрерывно — сеанс пользователя с такой ролью не имеет ограничения по времени бездействия.

Данные на странице обновляются автоматически раз в 5 минут. Чтобы обновить данные вручную, нажмите кнопку Обновить в правом верхнем углу.

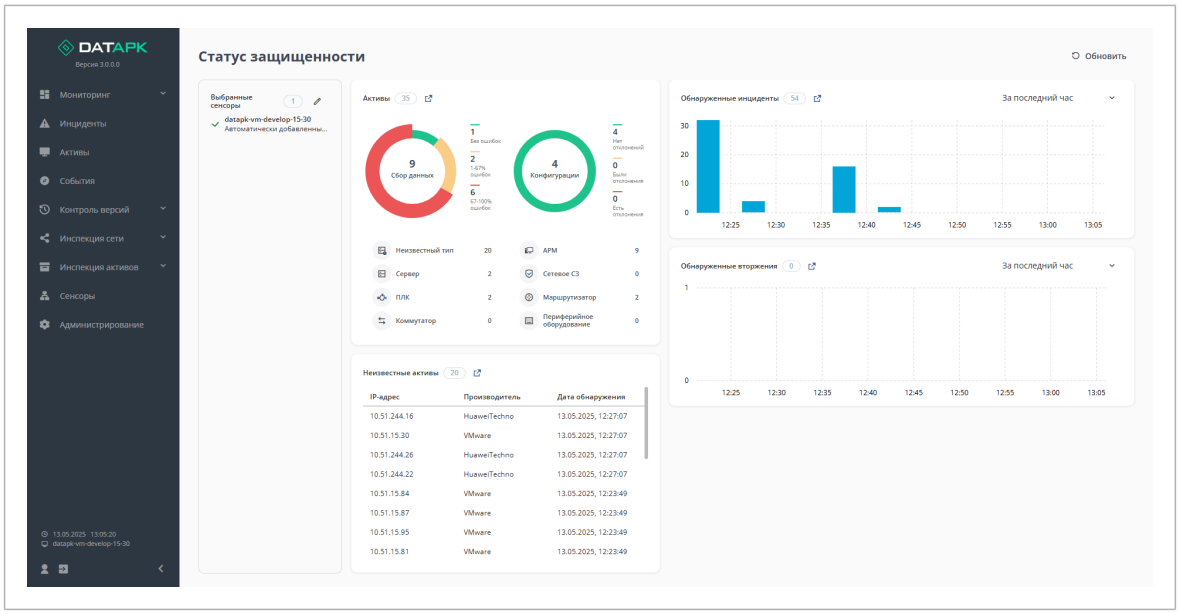


Рис. 39. Страница «Статус защищенности»

Таблица сенсоров

Слева расположен список всех подключенных к Комплексу сенсоров. В виджетах информация отображается для сенсоров, выбранных из списка.

Сенсоры в списке сортируются по статусу подключения и могут иметь следующие статусы:

- ⚠ — сенсоры, получение данных с которых недоступно. Отображаются в верхней части списка — рекомендуется в первую очередь провести диагностику и устранение причин, по которым недоступно получение данных.
- ✓ — сенсоры, которые функционируют в штатном режиме и успешно передают данные на Комплекс.

> Подсказка:
>
> Подробнее о возможных причинах недоступности сенсоров и способов восстановления доступа см. в разделе «Не устанавливается соединение с сенсором».

При нажатии на сенсор откроется страница **Сенсоры** с подробной информацией о выбранном сенсоре.

Виджеты

На странице присутствуют следующие виджеты:

- **Активы**. Виджет содержит:
  - в верхней части отображаются диаграммы общего состояния компонентов ИБ на активах:
    - **Сбор данных** — выполненные попытки сбора данных, сгруппированные по проценту неуспешных попыток по отношению к общему количеству попыток (`Без ошибок`, `1-67% ошибок`, `67-100% ошибок`);
    - **Конфигурации** — количество собранных конфигураций, сгруппированных по статусу их отклонения от эталонных конфигураций (`Нет отклонений`, `Были отклонения`, `Есть отклонения`);
  - в нижней части отображается количество всех обнаруженных активов, сгруппированных по типам.

> Внимание:
>
> Количество активов в виджете **Активы** включает в себя только активы с интерфейсами. Количество активов на странице **Активы** включает в себя активы с интерфейсами и без интерфейсов.

- **Неизвестные активы** — список обнаруженных неизвестных активов. Для каждого неизвестного актива фиксируется IP-адрес, наименование производителя и дата обнаружения.
- **Обнаруженные инциденты** — количество инцидентов, обнаруженных в выбранный период времени до текущего момента.
- **Обнаруженные вторжения** — количество вторжений, обнаруженных в выбранный период времени до текущего момента.

Над графиком **Обнаруженные инциденты** и **Обнаруженные вторжения** отображается примерное количество обнаруженных объектов за период, которое рассчитывается с учетом аппроксимации и исторических данных обнаружения относительно фактических значений на странице **Инциденты** и **События** соответственно. Погрешность отображаемых данных на графиках — `±1%`.

Существует возможность установить один из следующих интервалов обнаружения:

- за последний час;
- за последние 6 часов;
- за последние 12 часов;
- за последние 24 часа;
- за последние 7 дней.

По умолчанию отображается интервал **За последний час**. При выборе другого интервала и повторном входе на страницу **Статус защищенности** выбранный интервал будет сохраняться.

Ссылки в виджетах на смежные страницы

Ссылка в каждом виджете предназначена для перехода к подробным данным на соответствующей странице Комплекса. При переходе по ссылкам данные фильтруются по выбранному периоду времени и сенсорам.

В виджетах присутствуют следующие ссылки:

- Ссылка **Перейти к активам** в виджете **Активы** открывает страницу **Активы** со списком всех активов, чьи сетевые атрибуты сбора данных привязаны к выбранным сенсорам.
- Ссылка **Перейти к активам** в виджете **Неизвестные активы** открывает страницу **Активы** со списком всех активов с типом `Неизвестный тип`, чьи сетевые атрибуты сбора данных привязаны к выбранным сенсорам.
- Ссылка **Перейти к фактическим данным** в виджете **Обнаруженные инциденты** открывает страницу **Инциденты** со списком инцидентов, обнаруженных выбранными сенсорами за указанный период.
- Ссылка **Перейти к фактическим данным** в виджете **Обнаруженные вторжения** открывает страницу **События** со списком вторжений (событий с параметром `event_type = "ids_event"`), обнаруженных выбранными сенсорами за указанный период.

> **Внимание:**
>
> Пользователям с ролью `Просмотр панели мониторинга` недоступен просмотр данных при переходе по ссылкам.

10.4. Импортируемые панели мониторинга

В этом разделе:

- Принцип работы с мониторингом
- Действия в случае обнаружения событий в панели мониторинга
- Создание фильтров на панелях мониторинга
- Выбор периода отображения событий на панели мониторинга
- Главный дашборд
- Информационные панели
- Экспорт событий из панели мониторинга
- Панели мониторинга модуля «EDR for PLC»

Одним из вариантов использования Комплекса может быть последовательный мониторинг возникающих событий при помощи панелей мониторинга.

Панель мониторинга или дашборд (Dashboard) — тип графического интерфейса, использующий интерактивные визуализации для обзора ключевых показателей.

Виджет — представление информации о событиях в виде, удобном для зрительного наблюдения и анализа.

Производитель Комплекса предоставляет следующий набор панелей мониторинга:

- Главный дашборд — основное средство мониторинга событий, которое позволяет инженеру своевременно обнаруживать аномалии. Подразделы главного дашборда:
    - Раздел аналитики главного дашборда
    - Анализ трафика:
        - Контроль активов.
        - Контроль неодобренных сессий.
        - Обнаружение вторжений.
    - Контроль конфигураций:
        - Контроль конфигураций.
        - Сбор данных.
    - Контроль событий:
        - События активов.
        - Инциденты ИБ.
- Контроль соответствия и уязвимостей — средство визуализации уязвимостей и соответствия требованиям информационной безопасности, использующее проверки на соответствие требованиям ИБ.
- События управления Комплексами — список всех событий доступа и управления экземпляра Комплекса.
- Эксплуатационный мониторинг — содержит три списка событий, относящихся к непосредственному функционированию Комплекса.

10.4.1. Принцип работы с мониторингом

Структура страниц мониторинга предполагает последовательный мониторинг событий по категориям. Последовательный мониторинг включает в себя своевременное обнаружение и первичную аналитику возникающих событий. Инженеру доступна установка удобного ему периода и автообновление для обнаружения событий на активах в реальном времени. Чтобы заметить аномалию, достаточно взглянуть на графики в верхней части экрана. При обнаружении пика или спада на графике необходимо исследовать причины появления событий (или их отсутствия).

Пример первичного анализа событий с использованием главного дашборда:

1. Инженер обнаруживает пик на графиках событий.
2. Выбирает интересующий отрезок времени на графике.
3. Определяет точный момент и тип событий (изменение конфигураций) на графике.
4. Переходит по ссылке **Контроль конфигураций** в разделе аналитики.
5. Находит нужный пик на графике **Изменения конфигураций во времени**, выделяет его.
6. На странице видит всю необходимую для проверки информацию: Комплекс, название актива, название конфигурации, детальное описание, дату обнаружения, IP-адрес актива, статусы конфигураций.

10.4.2. Действия в случае обнаружения событий в панели мониторинга

Согласно рекомендациям по использованию Комплекса, на главном дашборде не должно отображаться никаких событий; соответственно, при их обнаружении необходимо предпринять действия по проверке легитимности обнаруженных событий. Конкретные действия будут зависеть от типа событий. В интерфейсе страниц мониторинга даны общие рекомендации в случае обнаружения событий определенного типа.

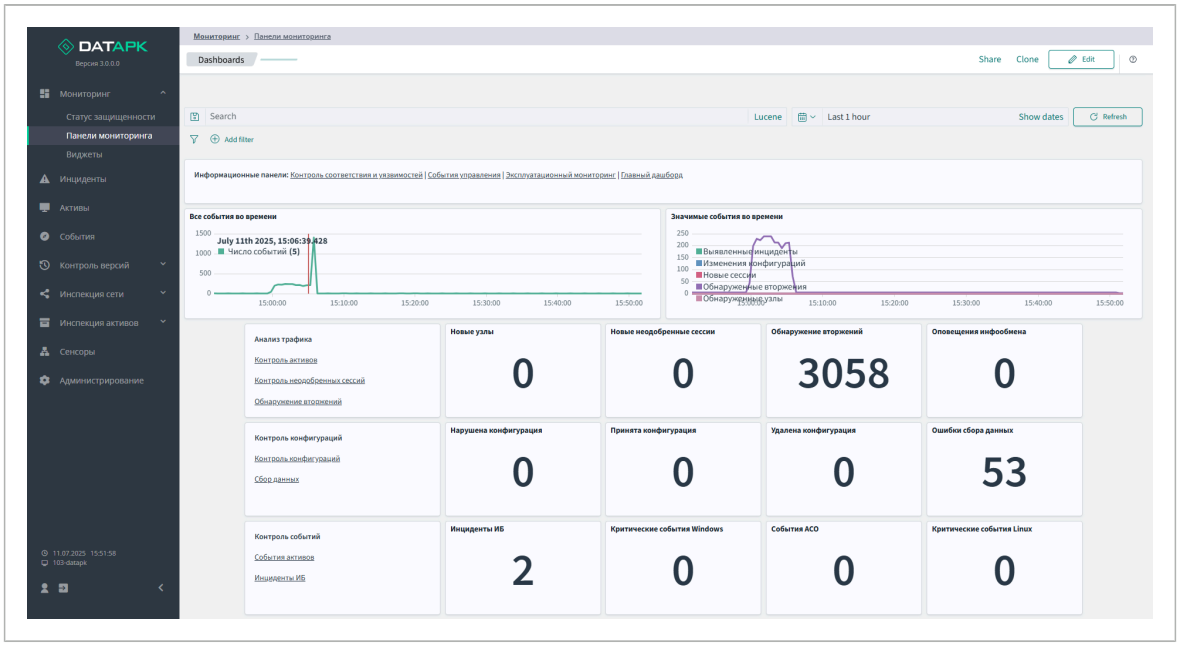


Рис. 40. Главный дашборд

10.4.3. Создание фильтров на панелях мониторинга

Чтобы создать фильтр на страницах мониторинга:

1. Нажмите **+ Add filter** под строкой поиска.
2. В появившемся окне выберите поле для фильтрации.
3. Выберите из выпадающего списка логическую операцию.

> Подсказка:
>
> Доступны следующие операции:
>
> - `is` — будут выведены все события точно подходящие под условие;
> - `is not` — события, подходящие под условие будут исключены из выборки;
> - `is one of` — события, подходящие хотя бы под одно из условий будут выведены;
> - `is not one of` — события, подходящие хотя бы под одно из условий не будут выведены;
> - `exists` — будут выведены события, в которых искомое поле присутствует;
> - `does not exist` — события с искомым полем выведены не будут.

4. Введите или выберите из списка значение фильтра, если выбранная логическая операция это предусматривает.
5. При необходимости нажмите на переключатель **Create custom label?** и введите текстовое описание фильтра.
6. Нажмите кнопку **Save**.

> Подсказка:
>
> Для сохранения фильтров или их набора без закрепления сохраните страницу в закладки браузера.

▸ **Результат шага:** после сохранения отобразятся данные, соответствующие запросу фильтра. Сам фильтр не будет закреплен.

10.4.3.1. Фильтр по значениям из таблицы

Помимо базового способа создания фильтров существует возможность взять данные из таблицы любой страницы мониторинга. Для создания фильтров по значениям полей таблицы:

1. Наведите курсор мыши на любой (кроме даты) столбец интересующей строки таблицы. Справа от курсора вы увидите две кнопки: ⊕ и ⊖.

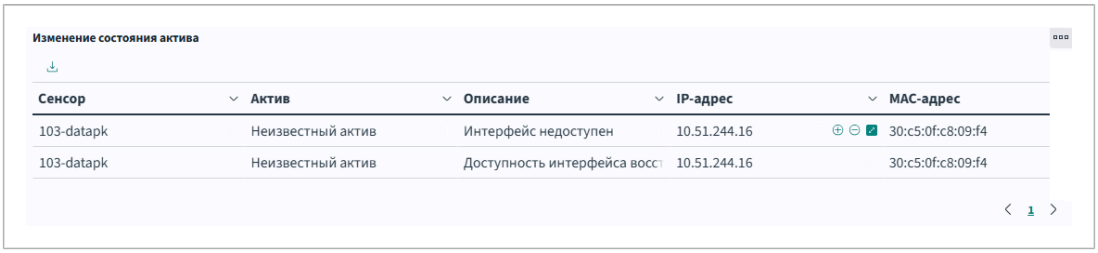


Рис. 41. Создание фильтра по значению таблицы «Изменение состояния актива»

> Подсказка:
>
> Нажмите кнопку рядом с кнопками ⊕ и ⊖, чтобы целиком отобразить значение, по которому будет выполнена фильтрация, и продублированные кнопки фильтрации.

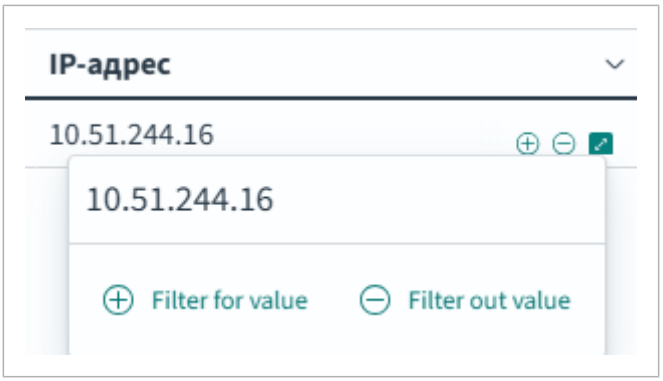


Рис. 42. Отображение значения, выбранного для фильтрации

2. В зависимости от необходимого типа фильтрации нажмите на одну из кнопок:
   - ⊕ (**Filter for value**) — для создания фильтра, включающего значения полей по запросу;
   - ⊖ (**Filter out value**) — для создания фильтра, исключающего значения полей по запросу.

Результат шага: в результате применения фильтров отобразится страница с событиями, содержащими только выбранные значения полей. В некоторых визуализациях может не быть результатов.

10.4.4. Выбор периода отображения событий на панели мониторинга

Основным способом выбора времени отображения событий является панель управления временем отображения. Она находится в верхней части страницы.

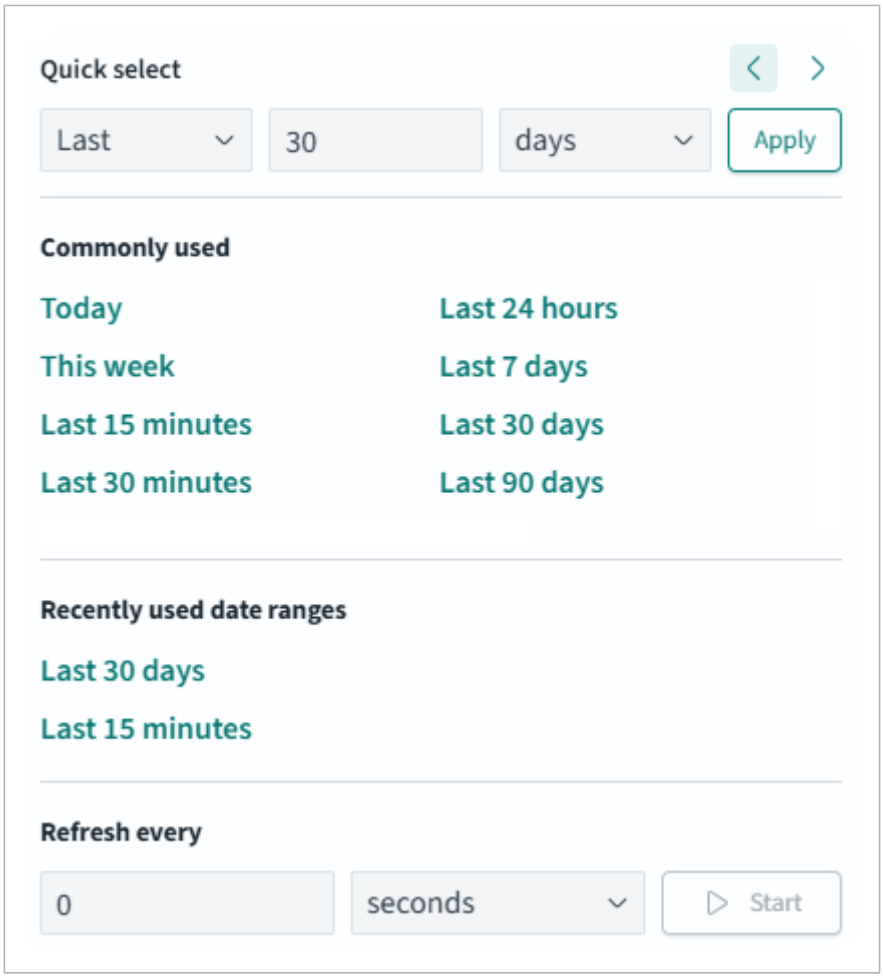


Рис. 43. Выбор периода отображения событий

Панель позволяет выбрать любой период в прошлом: до текущего момента, за период (например, год), относительно (например, неделю назад), абсолютно (например, 20.03.2024).

Дополнительным способом выбора периода отображения событий является визуальный. При работе с графиками есть возможность выбрать период прямо на визуальном представлении. Для этого:

1. Наведите на начало интересующего периода на любом из графиков. Рядом с курсором вы увидите вертикальную красную полосу;

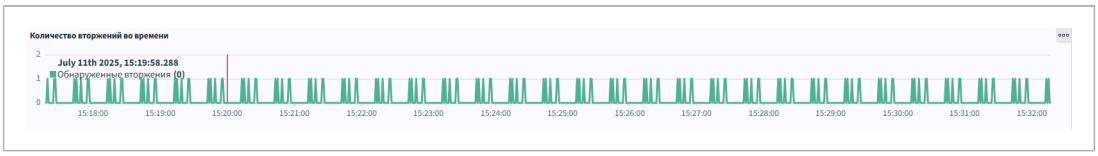


Рис. 44. Выбор начала периода отображения событий

   a. Зажмите левую клавишу мыши.

   б. Не отпуская, ведите до окончания интересующего периода. Область выбора времени на графике станет серой.

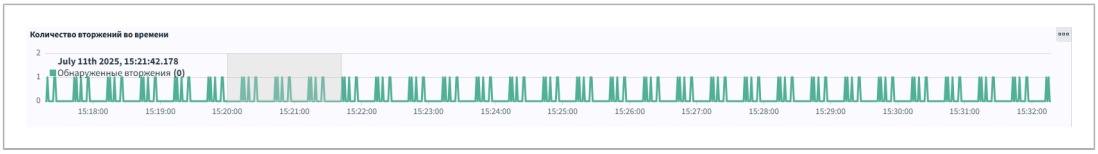


Рис. 45. Выбор окончания периода отображения событий

2. Отпустите левую клавишу мыши.

   Результат шага: в результате этих действий визуализации перестроятся в соответствии с выбранным периодом, а в панели управления временем отображения можно будет увидеть выбранный период с точностью до миллисекунды.

10.4.4.1. Автообновление

Для оперативного мониторинга событий в режиме реального времени можно включить автообновление. Для этого:

1. В верхней правой части страницы нажмите ;
2. В нижней части окна выбора периода отображения, в строке **Refresh every** введите число и выберите единицу измерения времени.

> Подсказка:
>
> Доступны следующие единицы измерения времени:
>
> - `seconds` — секунды;
> - `minutes` — минуты;
> - `hours` — часы;

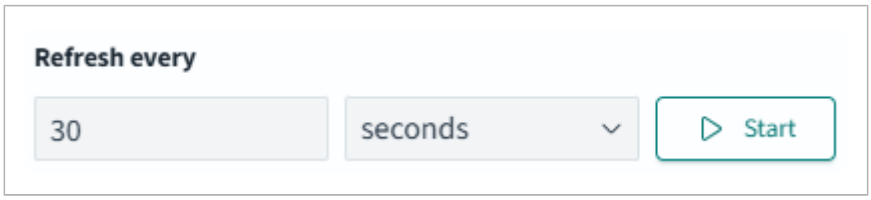


Рис. 46. Выбор интервала автообновления

3. Нажмите **Start** для инициации процедуры автообновления.

10.4.5. Главный дашборд

В этом разделе:

- Раздел аналитики главного дашборда
- Анализ трафика
  - Контроль активов
  - Контроль неодобренных сессий
  - Обнаружение вторжений
- Контроль конфигураций
  - Контроль конфигураций
  - Сбор данных
- Контроль событий

- События активов
- Инциденты ИБ

Чтобы попасть в основную панель мониторинга перейдите на страницу **Мониторинг → Панели мониторинга** и выберите **Главный дашборд**.

На странице можно видеть визуальное представление статистических данных по типам событий.

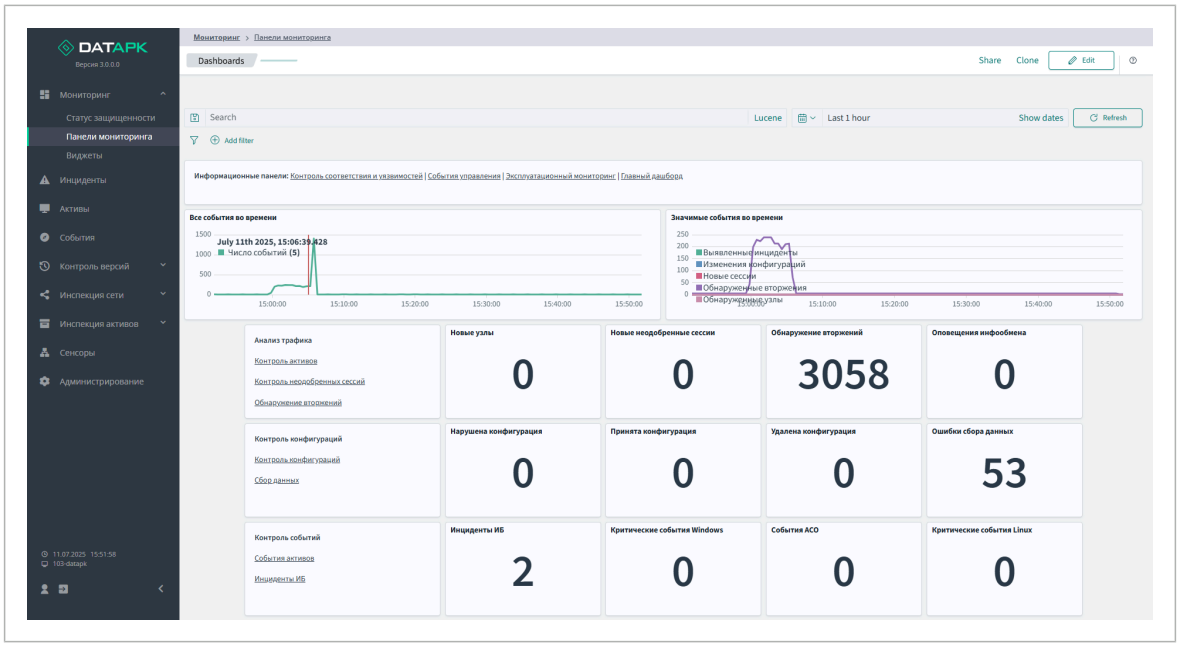


Рис. 47. Главный дашборд

Основные элементы страницы мониторинга:

- Визуальное представление событий — находится в средней части страницы под разделом навигации. Содержит два графика:
  - **Все события во времени**;
  - **Значимые события во времени**.
- Раздел аналитики — расположен в нижней части страницы. Состоит из трех блоков:
  - **Анализ трафика**;
  - **Контроль конфигураций**;
  - **Контроль событий**.

Графики главного дашборда

Основным средством отслеживания количества событий на главном дашборде являются графики.

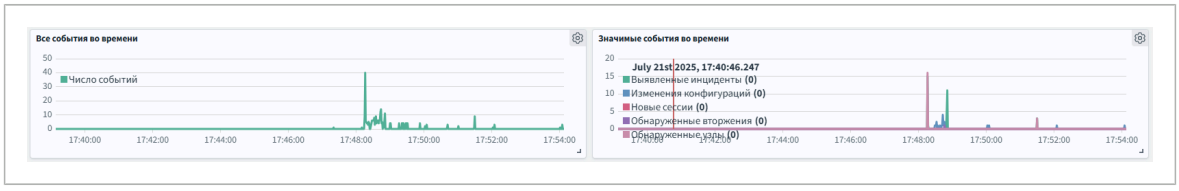


Рис. 48. Графики главного дашборда

Главный дашборд содержит два графика:

- **Все события во времени** — график по всем событиям за выбранный период позволяет инженеру быстро видеть аномалии и реагировать на них.
- **Значимые события во времени** — график содержит события за период по основным категориям:
  - **Выявленные инциденты**;
  - **Изменения конфигураций**;
  - **Новые сессии**;
  - **Обнаруженные вторжения**;
  - **Обнаруженные узлы**.

Благодаря этим графикам можно оперативно обнаружить изменения в количестве событий за выбранный период.

10.4.5.1. Раздел аналитики главного дашборда

В нижней части главного дашборда находятся дополнительные средства отслеживания изменений: визуализация количества новых событий и ссылки на панели мониторинга. При помощи визуализации количества новых событий по категориям инженер может мгновенно увидеть, в какой из категорий возникли события, и перейти по ссылке в левой части страницы, чтобы проанализировать события.

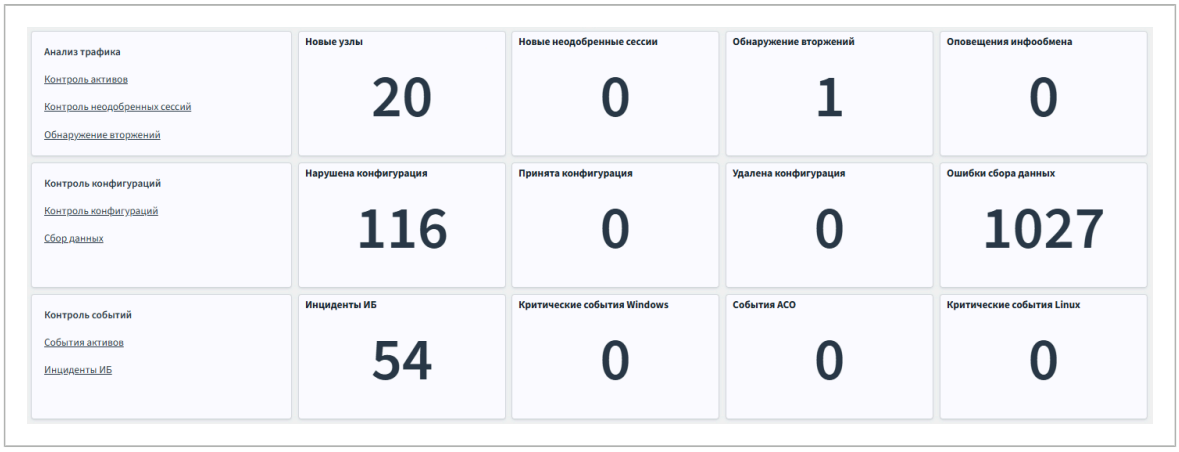


Рис. 49. Раздел аналитики главного дашборда

> Внимание:
>
> При работе с панелью мониторинга на Комплексе, который не завершил процедуру настройки, возможно попадание «лишних» событий в статистику мониторинга. Рекомендуется использование страниц мониторинга только после окончательной настройки. Убедиться в корректности настройки для мониторинга можно по количеству событий в визуализации: везде должен быть `0`.

Визуализации и ссылки на разделы мониторинга логически сгруппированы по строкам. Группы раздела аналитики главного дашборда представлены в таблице ниже (Таблица 5. Группировка визуализаций на главном дашборде).

Табл. 5. Группировка визуализаций на главном дашборде

ГРУППА	СТРАНИЦЫ	ВИЗУАЛИЗАЦИИ			
Анализ трафика	Контроль активов	Новые узлы	Новые сессии	Обнаружение вторжений	Ошибки ин-фообмена

Табл. 5. Группировка визуализаций на главном дашборде

ГРУППА	СТРАНИЦЫ	ВИЗУАЛИЗАЦИИ			
	Контроль неодобренных сессий				
	Обнаружение вторжений				
Контроль конфигураций	Контроль конфигураций	Нарушена конфигурация	Принята конфигурация	Удалена конфигурация	Ошибки сбора данных
	Сбор данных				
Контроль событий	События активов	Инциденты ИБ	Критические события Windows	События АСО	Критические события Linux
	Инциденты ИБ				

Благодаря выводу основных данных по каждой из групп в правой части страницы, инженеру легко найти ссылку в левой части на визуализированный раздел конкретного типа событий.

10.4.5.2. Анализ трафика

В этом разделе:

- Контроль активов
- Контроль неодобренных сессий
- Обнаружение вторжений

В разделе **Анализ трафика** расположены подразделы мониторинга для контроля и обнаружения сетевых узлов, потоков данных и вторжений. Все страницы мониторинга в подразделе обладают сквозной навигацией по подразделу **Анализ трафика**.

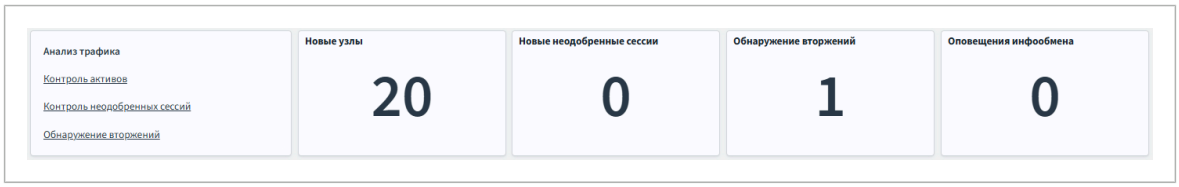


Рис. 50. Раздел «Анализ трафика» на главном дашборде

10.4.5.2.1. Контроль активов

Панель мониторинга **Контроль активов** позволяет просматривать информацию о событиях, связанных с активами, в визуализированной форме. Доступны визуализации в виде таблиц и графика.

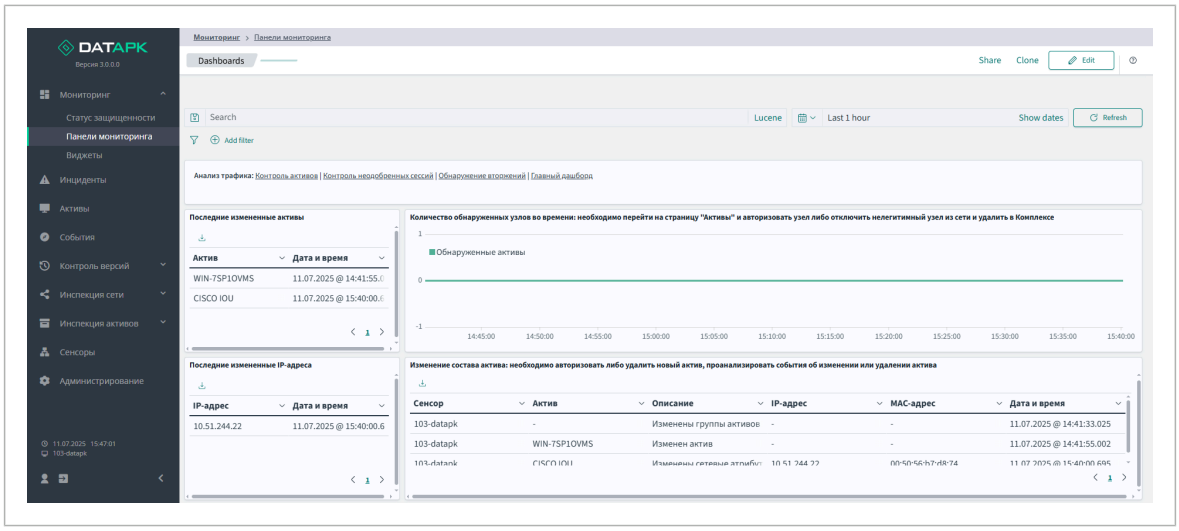


Рис. 52. Панель мониторинга «Контроль активов»

Подробнее о назначении визуализаций — в таблице ниже (Таблица 6. Описание визуализаций на странице «Контроль сетевых узлов»).

Табл. 6. Описание визуализаций на странице «Контроль сетевых узлов»

НАЗВАНИЕ	ОПИСАНИЕ	СОДЕРЖАНИЕ
Диаграммы		
Количество обнаруженных узлов во времени	График позволяет увидеть аномалии количества событий изменения сетевых узлов во времени	Время, обнаруженные узлы
Таблицы		
Последние измененные узлы	Позволяет проследить, на каких узлах были обнаружены события и идентифицировать их по названию	Название узла, Дата и время
Последние измененные IP-адреса	Позволяет проследить, какие IP-адреса были изменены	IP-адрес, Дата и время
Последние измененные MAC-адреса	Позволяет проследить, какие MAC-адреса были изменены	MAC узла, Дата и время
Изменение состава актива	Позволяет комплексно проанализировать, какие события были обнаружены и на каком узле	Комплекс, Название узла, Описание, IP-адрес, MAC-адрес, Дата и время
Привязка интерфейса к активу	Позволяет проследить события привязки интерфейса к активу	Комплекс, Действие, Наименование актива, IP адрес актива, MAC-адрес актива, Дата и время

Табл. 6. Описание визуализаций на странице «Контроль сетевых узлов»

НАЗВАНИЕ	ОПИСАНИЕ	СОДЕРЖАНИЕ
Изменение состояния актива	Позволяет проследить изменения доступности интерфейса на активах	Комплекс, Название узла, Описание, IP-адрес, MAC-адрес, Количество, Дата и время

10.4.5.2.1.1. Рекомендуемые действия в случае обнаружения событий на странице «Контроль активов»

События в таблице «Количество обнаруженных узлов во времени»

Необходимо перейти на страницу **Активы** и легитимизировать узел, либо отключить нелегитимный узел из сети и удалить его в Комплексе. Для легитимизации или удаления нелегитимного узла:

1. Перейдите на страницу **Активы**.
2. Найдите интересующий актив при помощи фильтров в правой части страницы.
3. В зависимости от выбранного решения, воспользуйтесь следующими функциями:
    а. Для удаления нелегитимного узла:
        - Откройте **карточку актива**.
        - Нажмите (**Удалить актив**) справа от интересующего актива;
        - Введите текст обоснования.
        - Нажмите **Подтвердить**.
    б. Для легитимизации узла:
        - Откройте **карточку актива**.
        - Нажмите справа от заголовка блока **Описание актива**, чтобы перейти к редактированию описания актива.
        - Во всплывающем окне введите наименование, описание и тип актива.

События в таблице «Изменение состава актива»

Необходимо легитимизировать, либо удалить новый узел, проанализировать события об удалении актива.

События в таблице «Привязка интерфейса к активу»

Необходимо проверить, что интерфейс с MAC-адресом сетевого устройства корректно привязан к активу. Для этого:

1. Перейдите в **карточку актива**.
2. В разделе **Сетевые атрибуты** найдите интерфейс с наименованием `with_router_mac`.
3. Убедитесь, что актив имеет возможность отправлять трафик через маршрутизирующее устройство с MAC-адресом, указанным справа от названия интерфейса `with_router_mac`.

10.4.5.2.2. Контроль неодобренных сессий

Панель мониторинга **Контроль неодобренных сессий** позволяет просматривать информацию о событиях, связанных с обнаружением новых сессий в визуализированной форме. Доступны визуализации в виде таблиц и диаграмм.

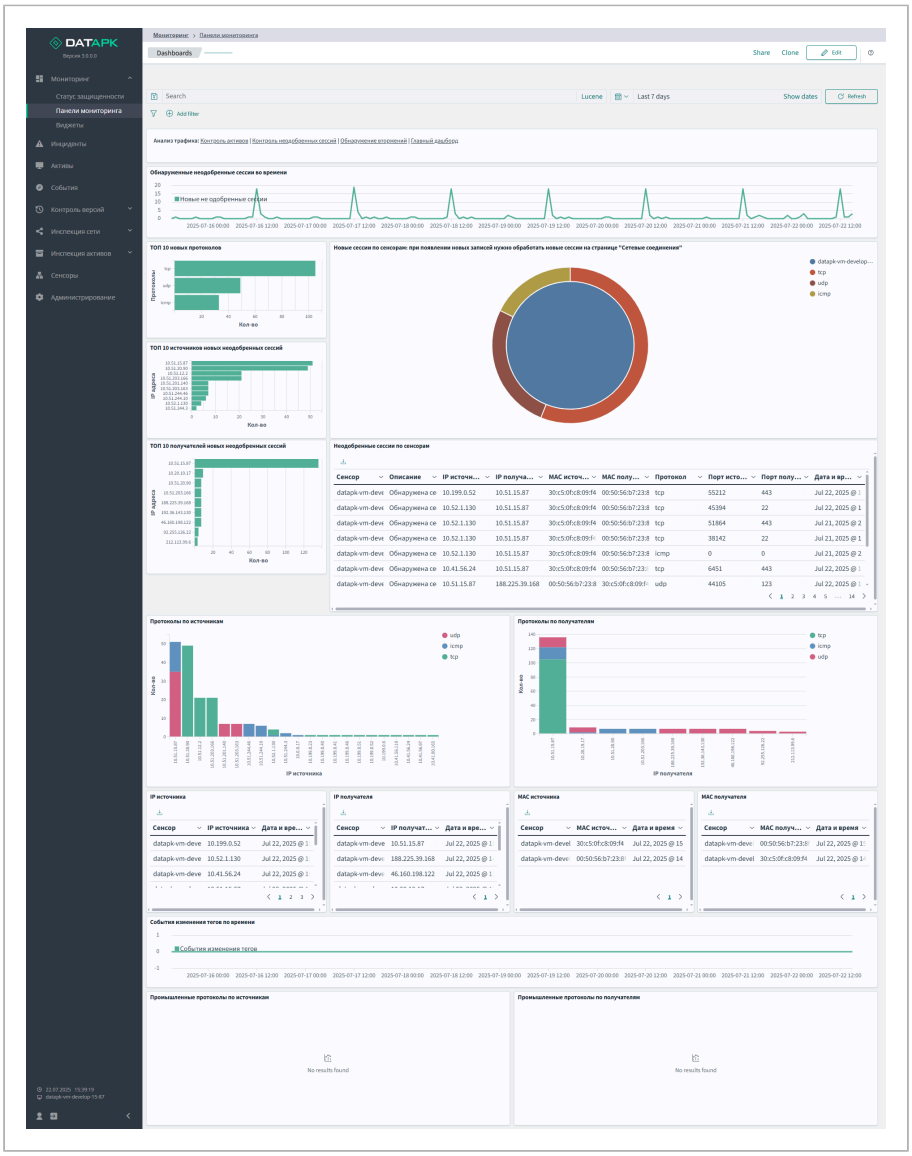


Рис. 53. Панель мониторинга «Контроль неодобренных сессий»

Подробнее о назначении визуализаций — в таблице ниже (Таблица 7. Описание визуализаций на странице «Контроль неодобренных сессий»).

Табл. 7. Описание визуализаций на странице «Контроль неодобренных сессий»

НАЗВАНИЕ	ОПИСАНИЕ	СОДЕРЖАНИЕ	
Диаграммы			
Обнаруженные сессии во времени	График позволяет отследить динамику появления событий за выбранный период времени	Время, Новые сессии	
Новые сессии по сенсорам	Круговая диаграмма позволяет оценить соотношение количества событий, которые создают новые сессии	Внутренний круг	Комплекс, на котором были обнаружены события

Табл. 7. Описание визуализаций на странице «Контроль неодобренных сессий»

НАЗВАНИЕ	ОПИСАНИЕ	СОДЕРЖАНИЕ	
		Внешний круг	Протоколы обнаруженных событий
ТОП 10	Горизонтальные столбчатые диаграммы позволяют изучить соотношение количества событий сессий по следующим категориям: • ТОП 10 новых протоколов; • ТОП 10 источников новых неодобренных сессий; • ТОП 10 получателей новых неодобренных сессий	Протоколы, Количество IP-адреса источников, Количество IP-адреса получателей, Количество	
Протоколы	Вертикальные столбчатые диаграммы позволяют оценить, какие протоколы используют предполагаемые злоумышленники. Диаграммы разделены по следующим категориям: • Протоколы по источникам; • Протоколы по получателям	IP источника, Количество IP получателя, Количество	
Таблицы			
Неодобренные сессии по сенсорам	Позволяют оценить динамику появления новых сессий на управляемых сенсорах за выбранный период времени	Сенсоры, IP-адреса источников, IP-адреса получателей, MAC-адреса источников, MAC-адреса получателей, Протоколы, Порты источников, Порты получателей, Время	
Новые сессии по Комплексам	Позволяет изучить основные данные сетевых настроек источника и получателя, в том числе порты.	Комплекс, Описание, IP источника, IP получателя, MAC источника, MAC получателя, Протокол, Порт источника, Порт получателя, Дата и время последнего обнаружения	
IP-адрес	Позволяют изучить все обнаруженные IP-адреса новых неодобренных сессий. • IP источника; • IP получателя	Комплекс, IP источника / IP получателя, Дата и время последнего обнаружения	

Табл. 7. Описание визуализаций на странице «Контроль неодобренных сессий»

НАЗВАНИЕ	ОПИСАНИЕ	СОДЕРЖАНИЕ
MAC-адрес	Позволяют изучить все обнаруженные MAC-адреса новых неодобренных сессий. • MAC источника; • MAC получателя	Название Комплекса, MAC источника / MAC получателя, Дата и время последнего обнаружения
События изменения тегов по времени	Позволяют отследить события, связанные с изменением значений тегов	Событие, Количество, Время
Промышленные протоколы	Позволяют изучить промышленные протоколы, используемые в новых неодобренных сессиях. • Промышленные протоколы по источникам; • Промышленные протоколы по получателям	IP-адрес отправителя / IP-адрес получателя, Протокол, Количество

10.4.5.2.3. Обнаружение вторжений

Панель мониторинга **Обнаружение вторжений** позволяет просматривать информацию о событиях, связанных со вторжениями в визуализированной форме. Доступны визуализации в виде таблиц и диаграмм.

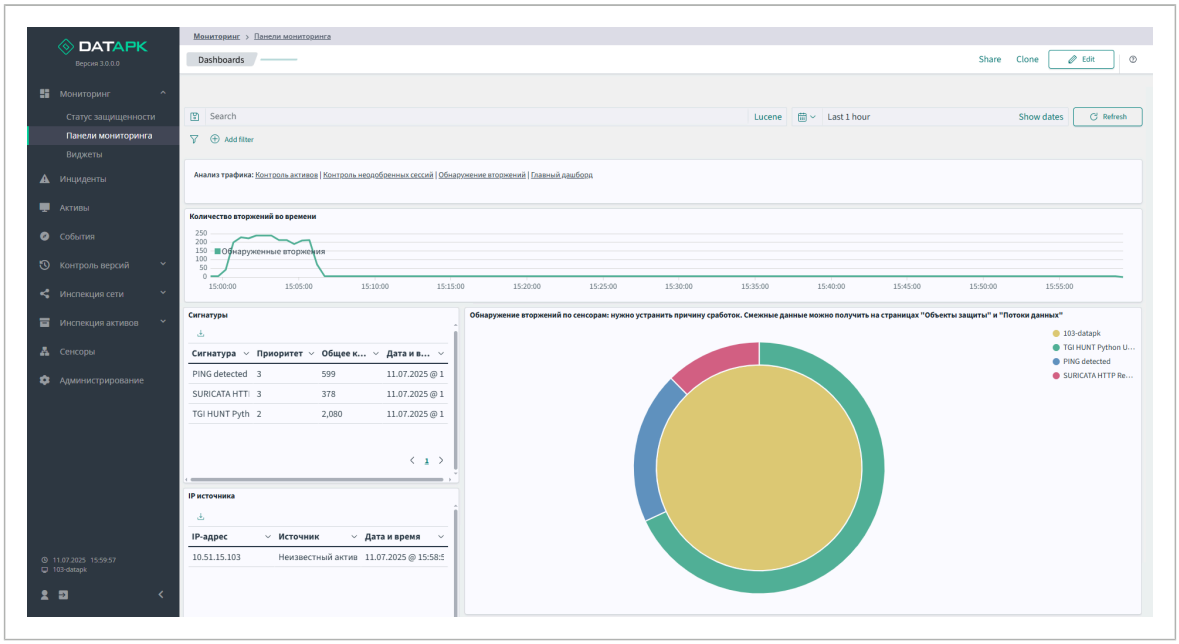


Рис. 55. Панель мониторинга «Обнаружение вторжений»

Подробнее о назначении визуализаций — в таблице ниже (Таблица 8. Описание визуализаций на странице «Обнаружение вторжений»).

Табл. 8. Описание визуализаций на странице «Обнаружение вторжений»

НАЗВАНИЕ	ОПИСАНИЕ	СОДЕРЖАНИЕ	
Диаграммы			
Количество вторжений во времени	График позволяет увидеть аномалии количества вторжений во времени.	Время, Обнаруженные вторжения	
Обнаружение вторжений по Комплексам	Круговая диаграмма позволяет оценить соотношение количества вторжений по сигнатуре	Внутренний круг	Комплекс, на котором были обнаружены события
		Внешний круг	Сигнатуры обнаруженных вторжений
Обнаружение вторжений	Столбчатые диаграммы, отображающие все события, сгруппированные по IP-адресу. На столбцах можно увидеть сигнатуры, по которым произошла сработка и их количество. Визуализации отображаются по адресатам: • Сработки по источнику; • Сработки по получателю	Источник (IP-адрес), Количество Получатель (IP-адрес), Количество	
Таблицы			
Сигнатуры	Позволяет изучить сигнатуры вторжений и их количество	Сигнатура, Приоритет, Общее количество, Дата и время	
IP-адрес	Позволяет изучить, с каких IP-адресов были обнаружены вторжения. Виджет разделена на две таблицы: • IP источника; • IP получателя	IP источника, Источник, Дата и время IP получателя, Получатель, Дата и время	
Обнаружение вторжений (IDS)	Позволяет подробно изучить и проанализировать возникшие вторжения	Комплекс, Описание, Приоритет, IP источника, Источник, IP получателя, Получатель, Количество, Дата и время	

10.4.5.2.3.1. Рекомендуемые действия в случае обнаружения событий на странице «Обнаружение вторжений»

В случае обнаружения вторжений нужно устранить причину срабатывания сигнатуры. Дополнительные сведения об активах можно получить на страницах **Активы** и **Сетевые соединения**. После получения необходимых

сведений устранение причины срабатывания происходит непосредственно на активах, вне интерфейса Комплекса.

10.4.5.3. Контроль конфигураций

В этом разделе:

- Контроль конфигураций
- Сбор данных

В разделе **Контроль конфигураций** расположены панели мониторинга для контроля и обнаружения событий изменения конфигураций и сбора данных. Все страницы мониторинга в подразделе обладают сквозной навигацией по подразделу **Контроль конфигураций**.

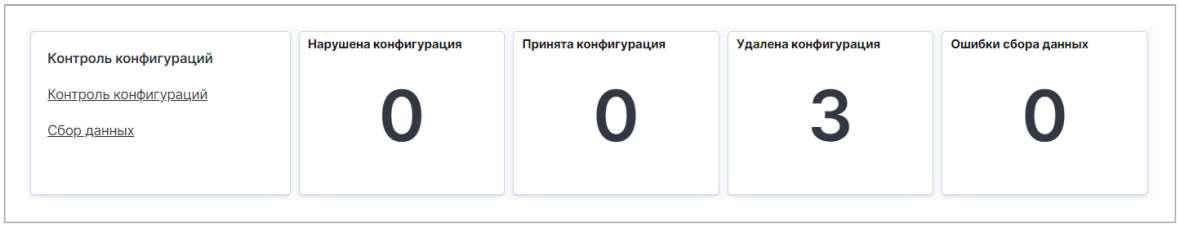


Рис. 56. Раздел «Контроль конфигураций» на главном дашборде

10.4.5.3.1. Контроль конфигураций

Панель мониторинга **Контроль конфигураций** позволяет просматривать информацию о событиях, связанных с изменением эталонных конфигураций, в визуализированной форме. Доступны визуализации в виде таблиц и диаграмм.

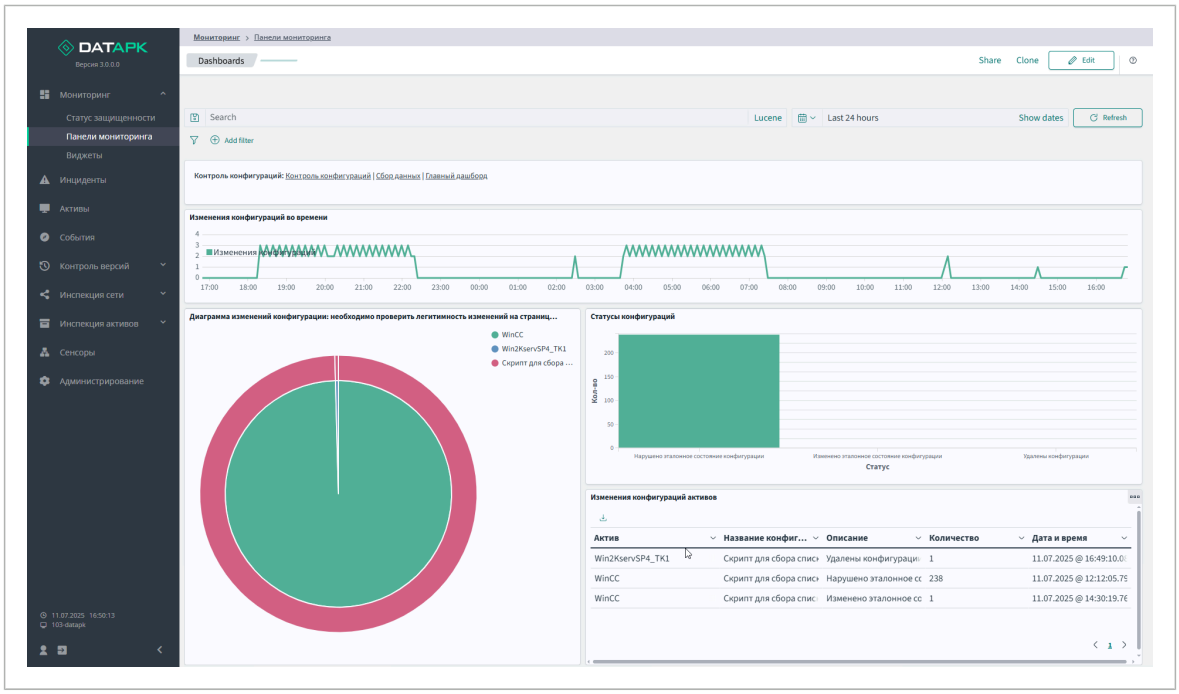


Рис. 58. Панель мониторинга «Контроль конфигураций»

Подробнее о назначении визуализаций — в таблице ниже (Таблица 9. Описание визуализаций на странице «Контроль конфигураций»).

Табл. 9. Описание визуализаций на странице «Контроль конфигураций»

НАЗВАНИЕ	ОПИСАНИЕ	СОДЕРЖАНИЕ	
Диаграммы			
Изменения конфигураций во времени	График позволяет увидеть аномалии количества событий изменений эталонных конфигураций во времени	Время, Изменения конфигураций	
Диаграмма изменений конфигурации	Круговая диаграмма позволяет оценить соотношение количества поступающих событий по типам	Внутренний круг	Комплекс, на котором были обнаружены события
		Первый внешний круг	Активы, на которых произошли изменения
		Второй внешний круг	Измененные конфигурации
Статусы конфигураций	Столбчатая диаграмма позволяет проанализировать соотношение количества событий по статусам: нарушено эталонное состояние конфигурации, изменено эталонное состояние конфигурации	Статус, Количество	
Таблицы			
Изменения конфигураций активов	Позволяет изучить, какие конфигурации и на каких активах были изменены	Комплекс, Название актива, Название конфигурации, Описание, Кол-во, Дата и время	
Удаление конфигурации активов	Позволяет изучить, какие конфигурации, кем и на каких активах были удалены	Комплекс, Название актива, Название конфигурации, Описание, Пользователь, Обоснование, Кол-во, Дата и время	
Детали изменения конфигураций	Позволяет изучить детальную информацию об изменении конфигураций (например, какие строки были добавлены в системный файл Windows)	Название Комплекса, Название актива, Конфигурация, Действие, Детализация, Последнее обнаружение	

10.4.5.3.1.1. Рекомендуемые действия в случае обнаружения событий на странице «Контроль конфигураций»

Необходимо проверить легитимность изменений на странице **Активы**. Для этого:

1. Перейдите на страницу **Активы**.
2. Найдите интересующий актив при помощи фильтров в правой части страницы.
3. Нажмите (**Конфигурация актива**) в разделе **Связанные данные** для просмотра подробностей конфигурации. На странице вы можете сравнить текущую конфигурацию с эталонной при помощи соответствующего чекбокса.
4. Если изменения легитимны, нажмите **Принять за эталонную**.
5. Если изменения нелегитимны, предпримите действия вне интерфейса Комплекса по возвращению эталонной конфигурации. Чтобы убедиться в корректности проведенных изменений:
    a. Просканируйте конфигурацию в **карточке актива**. Для этого:
        - Перейдите в **карточку актива**.
        - В разделе **Статус сбора данных** напротив интересующей конфигурации нажмите (**Запустить сканирование повторно**).
    б. Убедитесь, что между новой конфигурацией и эталонной нет различий. Для этого:
        - Перейдите на страницу **Конфигурации актива**;
        - Убедитесь, что различий в ходе сканирования не найдено.
    в. Если различий не найдено, нажмите **Принять за эталонную**.

10.4.5.3.2. Сбор данных

Панель мониторинга **Сбор данных** позволяет просматривать информацию о событиях, связанных со сбором данных, в визуализированной форме. Доступны визуализации в виде таблиц и диаграмм.

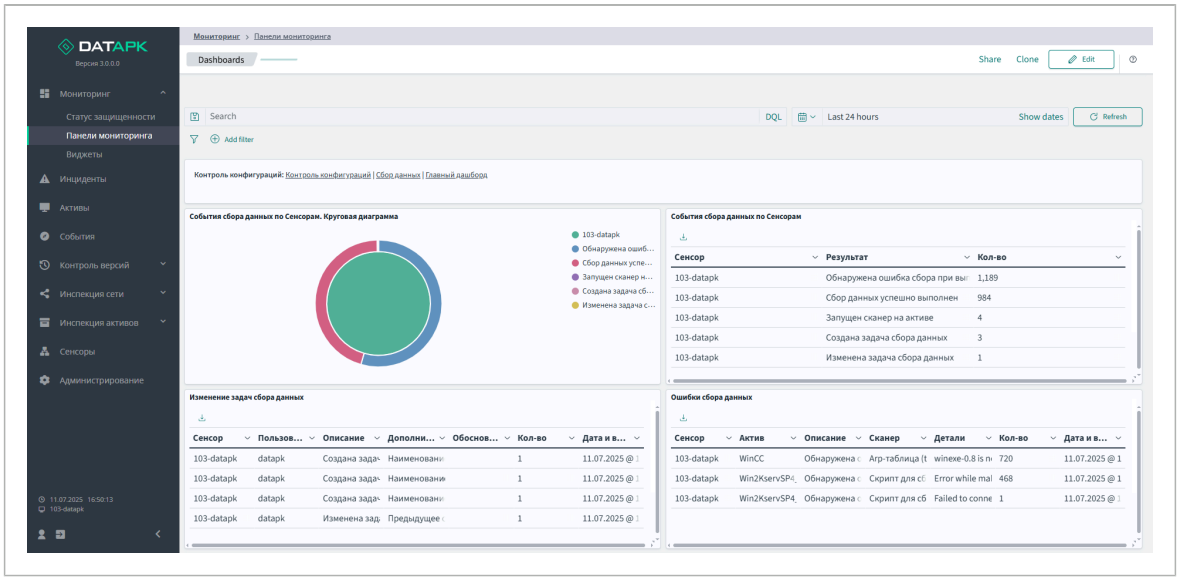


Рис. 60. Панель мониторинга «Сбор данных»

Подробнее о назначении визуализаций — в таблице ниже (Таблица 10. Описание визуализаций на странице «Сбор данных»).

Табл. 10. Описание визуализаций на странице «Сбор данных»

НАЗВАНИЕ	ОПИСАНИЕ	СОДЕРЖАНИЕ	
Диаграммы			
События сбора данных по Комплексам	Круговая диаграмма позволяет оценить по типам соотношение количества событий, поступающих на текущий Комплекс	Внутренний круг	Актив, с которого были получены события
		Внешний круг	Описание события
Таблицы			
События сбора данных по сенсорам	Позволяет изучить список результатов сбора данных на различных сенсорах, подключенных к текущему Комплексу	Сенсор, Результат, Количество	
Изменение задач сбора данных	Позволяет изучить список действий пользователя с задачами	Комплекс, Пользователь, Описание, Дополнительная информация, Обоснование, Количество, Дата и время	
Ошибки сбора данных	Позволяет изучить ошибки сбора данных на активах	Комплекс, Актив, Описание, Сканер, Детали, Кол-во, Дата и время	
События сбора данных	Позволяет изучить список событий сбора данных на активах	Комплекс, Актив, Описание, Наименование сканера, Детали, Количество, Дата и время	

10.4.5.3.2.1. Рекомендуемые действия в случае обнаружения событий на панели мониторинга «Сбор данных»

Проблема: «Ошибка выполнения команды (No route to host)»

Причина

Нет доступа к активу, либо данный протокол сбора данных не применим к активу.

Способ устранения

Для устранения затруднения:

1. Настройте доступ к активу. Для этого:
    а. Настройте учетные данные. Подробнее см. раздел «Добавление учетных данных актива».
    б. Настройте порты на межсетевом экране/маршрутизаторе.
    в. Настройте брандмауэр (сетевой экран, firewall) на активе.
2. Если п. 1 не помог, используйте другой протокол сбора данных.

Проблема: «Учетные данные для пользователя не найдены»

Причина

Учетные данные не привязаны к активу, либо используется некорректный тег.

Способ устранения

Для устранения затруднения:

Настройте корректный доступ к активу. Подробнее см. раздел «Добавление учетных данных актива»

Проблема: «Ошибка выполнения команды», «the specified credentials were rejected by the server»

Причина

Неверные учетные данные, не хватает прав на активе.

Способ устранения

Для устранения затруднения:

Настройте корректный доступ к активу. Подробнее см. раздел «Добавление учетных данных актива»

Проблема: «Ошибка выполнения команды. Соединение неожиданно закрылось»

Причина

Различные ошибки winexe: отсутствие доступа, неверный пароль, нехватка прав.

Способ устранения

Для устранения затруднения:

1. Настройте сбор данных по winrm.
2. Если возможность осуществить п. 1 отсутствует, проверьте реквизиты на странице **Активы → Настройка активов→ Учетные данные**. Подробнее о настройке см. раздел «Настройка учетных данных активов».
3. Убедитесь, что учетная запись пользователя Windows располагает правами администратора.

Проблема: «Превышено время ожидания выполнения задачи сбора событий» или «Превышено время ожидания выполнения задачи сбора данных»

Причина

Актив не смог выгрузить все данные за отведенное время.

Способ устранения

Для устранения затруднения:

1. Увеличьте максимальное время ожидания выполнения задачи в настройках сканера. Для этого:
    a. Перейдите на страницу **Администрирование → Инспекция активов → Сканеры**.
    б. Напротив проблемного сканера нажмите (**Редактировать**).

в. В появившемся окне **Редактирование сканера** увеличьте значение параметра **Максимальное время ожидания выполнения задачи, сек**.

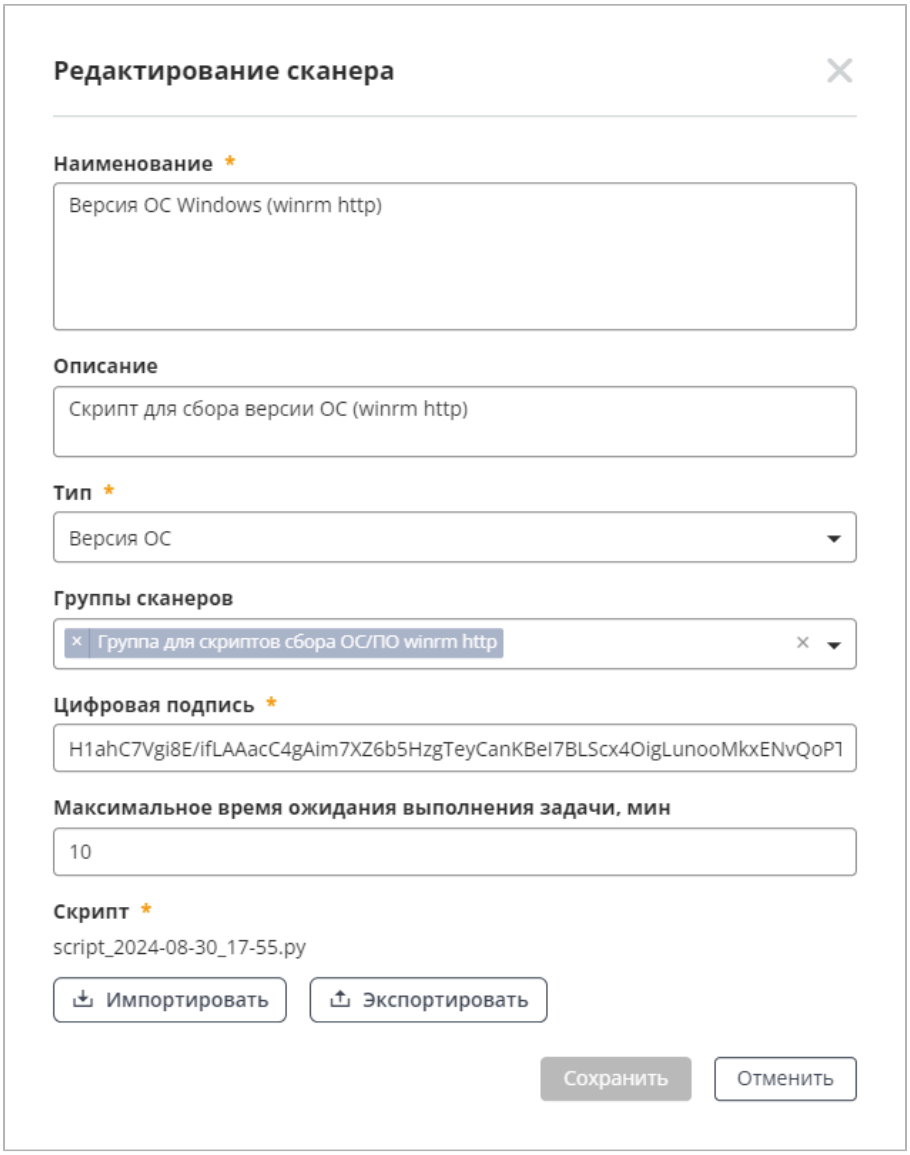


Рис. 61. Окно «Редактирование сканера»

2. Убедитесь в доступности активов.
3. Если действия из п. 1 не дали нужного результата — перезапустите сервисы Комплекса.

Проблема: «Ошибка компиляции Python-скрипта»

Причина

Ошибка в синтаксисе Python-скрипта, импортированного в сканер.

Способ устранения

Для устранения затруднения:

1. Исправьте Python-скрипт сбора данных.
2. Повторно выполните цифровую подпись Python-скрипта. Подробнее см. раздел «Цифровая подпись Python-скрипта».
3. Создайте новый сканер или измените существующий, импортировав в него новый Python-скрипт и его цифровую подпись. Либо импортируйте набор сканеров с новыми цифровыми подписями в веб-интерфейсе Комплекса.

Проблема: «Превышено время ожидания, ошибка выполнения сканера, не удалось получить ожидаемое сообщение»

Причина

Сканер сбора данных не получил ожидаемый результат от актива:

- нет доступа к активу;
- неверное ожидаемое значение.

Способ устранения

Для устранения затруднения:

1. Убедитесь в наличии доступа к активу.
2. Исправьте Python-скрипт сбора данных.
3. Повторно выполните цифровую подпись Python-скрипта. Подробнее см. раздел «Цифровая подпись Python-скрипта».
4. Создайте новый сканер или измените существующий, импортировав в него новый Python-скрипт и его цифровую подпись. Либо импортируйте набор сканеров с новыми цифровыми подписями в веб-интерфейсе Комплекса.

Проблема: «Некорректный формат ответа»

Причина

Некорректная обработка вывода: сканер не ожидал полученные данные от Актив.

Способ устранения

Для устранения затруднения:

1. Исправьте Python-скрипт сбора данных.
2. Повторно выполните цифровую подпись Python-скрипта. Подробнее см. раздел «Цифровая подпись Python-скрипта».
3. Создайте новый сканер или измените существующий, импортировав в него новый Python-скрипт и его цифровую подпись. Либо импортируйте набор сканеров с новыми цифровыми подписями в веб-интерфейсе Комплекса.

Проблема: «Ошибка при выполнении запроса к хосту: 'WMI Session Error: code: 0x80041017 - WBEM_E_INVALID_QUERY»

Причина

Актив не может обработать полученный WMI-запрос.

Подсказка:

В основном ошибка появляется на активах с устаревшими системами (Windows 2000 и старше).

Способ устранения

Для устранения затруднения:

1. Настройте для сбора данных другой протокол транспортного уровня вместо WMI.
2. Исправьте Python-скрипт сбора данных.
3. Повторно выполните цифровую подпись Python-скрипта. Подробнее см. раздел «Цифровая подпись Python-скрипта».
4. Создайте новый сканер или измените существующий, импортировав в него новый Python-скрипт и его цифровую подпись. Либо импортируйте набор сканеров с новыми цифровыми подписями в веб-интерфейсе Комплекса.

Проблема: Ошибка выполнения команды SMB SessionError: STATUS_LOGON_FAILURE(The attempted logon is invalid. This is either due to a bad username or authentication information.

Причина

Некорректные учетные данные.

Способ устранения

Для устранения затруднения:

Проверьте реквизиты на странице **Учетные данные**. Подробнее о настройке см. раздел «Настройка учетных данных активов».

Проблема: Ошибка выполнения команды rpc_s_access_denied

Причина

Некорректные учетные данные либо недостаточно полномочий на выполнение WMI-запроса.

Способ устранения

Для устранения затруднения:

1. Проверьте реквизиты на странице **Учетные данные**. Подробнее о настройке см. раздел «Настройка учетных данных активов».
2. Убедитесь, что учетная запись пользователя Windows располагает правами администратора.

10.4.5.4. Контроль событий

В этом разделе:

- События активов
- Инциденты ИБ

В разделе **Контроль событий** расположены подразделы мониторинга для контроля и обнаружения событий и инцидентов информационной безопасности. Все панели мониторинга в подразделе обладают сквозной навигацией по разделу **Контроль событий**.

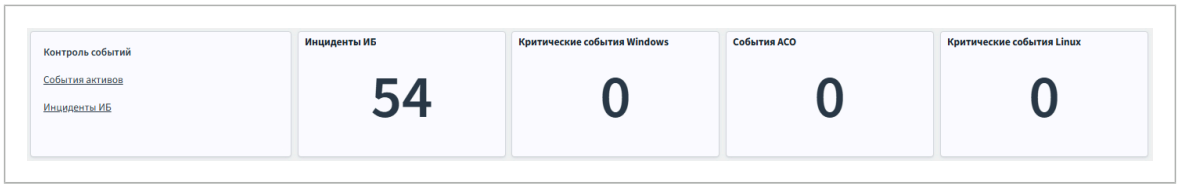


Рис. 62. Раздел «Контроль событий» на главном дашборде

10.4.5.4.1. События активов

Панель мониторинга **События активов** позволяет просматривать информацию о событиях непосредственно на активах в упрощенных таблицах.

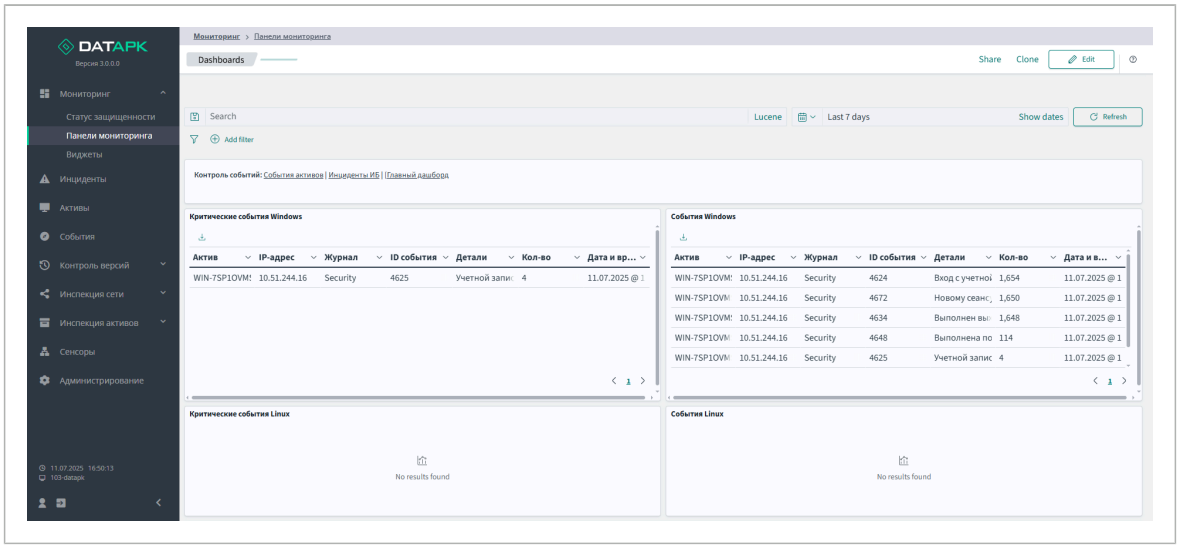


Рис. 64. Панель мониторинга «События активов»

Подробнее о назначении визуализаций — в таблице ниже (Таблица 11. Описание визуализаций на странице «События активов»).

Табл. 11. Описание визуализаций на странице «События активов»

НАЗВАНИЕ	ОПИСАНИЕ	СОДЕРЖАНИЕ
Таблицы		
Критические события Windows	Позволяет обнаружить наиболее важные события с активов, на которых установлена ОС Windows	Наименование актива, IP-адрес актива, Журнал, ID события, Тип, Детали, Кол-во, Дата и время
События Windows	Позволяет обнаружить все события с активов, на которых установлена ОС Windows	Наименование актива, IP-адрес актива, Журнал, ID события, Тип, Детали, Кол-во, Дата и время
События Linux	Позволяет обнаружить все события с активов, на которых установлена операционная система Linux	IP-адрес актива, Тип события, Описание, Пользователь, Кол-во, Дата и время

Табл. 11. Описание визуализаций на странице «События активов»

НАЗВАНИЕ	ОПИСАНИЕ	СОДЕРЖАНИЕ
Критические события Linux	Позволяет обнаружить наиболее важные события с активов, на которых установлена операционная система Linux	Комплекс, IP-адрес актива, Журнал, Тип события, Описание, Пользователь, Кол-во, Дата и время
События АСО	Позволяет обнаружить все события с активного сетевого оборудования	Наименование актива, IP-адрес актива, Пользователь, Описание, Кол-во, Дата и время

Подсказка:

В случае обнаружения нелегитимных событий на странице рекомендуется произвести проверку непосредственно на активах за пределами интерфейса Комплекса.

10.4.5.4.2. Инциденты ИБ

Панель мониторинга **Инциденты ИБ** позволяет просматривать информацию о произошедших инцидентах в визуализированной форме. Доступны визуализации в виде таблиц и диаграмм.

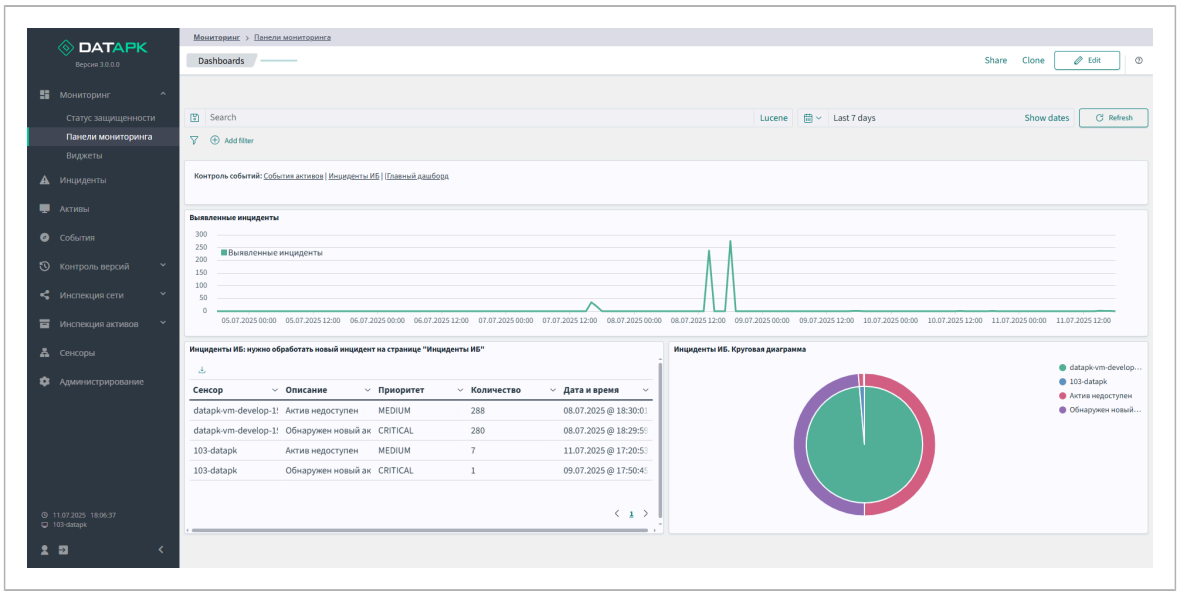


Рис. 65. Панель мониторинга «Инциденты ИБ»

Подробнее о назначении визуализаций — в таблице ниже (Таблица 12. Описание визуализаций на странице «Инциденты ИБ»).

Табл. 12. Описание визуализаций на странице «Инциденты ИБ»

НАЗВАНИЕ	ОПИСАНИЕ	СОДЕРЖАНИЕ
Диаграммы		

Табл. 12. Описание визуализаций на странице «Инциденты ИБ»

НАЗВАНИЕ	ОПИСАНИЕ	СОДЕРЖАНИЕ	
Выявленные инциденты	График позволяет увидеть появление инцидентов во времени	Время, Выявленные инциденты	
Инциденты ИБ	Круговая диаграмма позволяет оценить соотношение количества поступающих инцидентов по типам	Внутренний круг	Комплекс, на котором были обнаружены события
		Внешний круг	Количество инцидентов разных типов
Таблицы			
Инциденты ИБ	Позволяет просмотреть список возникших инцидентов; их количество и приоритет	Комплекс, Описание, Приоритет, Количество, Дата и время	

10.4.5.4.2.1. Рекомендуемые действия в случае обнаружения событий

Нужно обработать новый инцидент на панели мониторинга **Инциденты ИБ**. Для этого:

1. Перейдите на страницу основного интерфейса **Инциденты**, воспользовавшись соответствующей ссылкой в верхней части страницы.
2. Найдите интересующие инциденты при помощи фильтров в правой части страницы.
3. Ознакомьтесь с подробностями инцидентов и примите решение об их легитимности.
4. Измените статус и приоритет инцидентов.

> Подсказка:
>
> Подробнее см. в разделе «Изменение параметров инцидентов».

5. Для удаления инцидентов воспользуйтесь кнопкой .
6. Для создания отчета по инцидентам:
   - Выберите несколько инцидентов из списка.
   - В открывшемся нижнем меню нажмите кнопку Отчет
   - Выберите формат отчета и столбцы, включаемые в отчет, в открывшемся окне **Создание отчета по инцидентам**.
   - Нажмите кнопку **Запустить создание отчета**.

См. также

Групповые операции над инцидентами

Выгрузка отчета по инцидентам

10.4.6. Информационные панели

В этом разделе:

- Контроль соответствия и уязвимостей
- События управления Комплексами
- Эксплуатационный мониторинг

Информационные панели предназначены для анализа внутренних событий Комплекса, а также просмотра проверок на уязвимости. Перейти к информационным панелям можно с главного дашборда, воспользовавшись ссылками в его верхней части или со страницы **Панели мониторинга**.

> Подсказка:
>
> Подробнее с навигацией в панелях мониторинга вы можете ознакомиться в разделе «Навигация в разделах мониторинга».

10.4.6.1. Контроль соответствия и уязвимостей

Панель мониторинга **Контроль соответствия и уязвимостей** содержит таблицу, которая позволяет просмотреть список OVAL-проверок на наличие несоответствий требованиям информационной безопасности и уязвимостей.

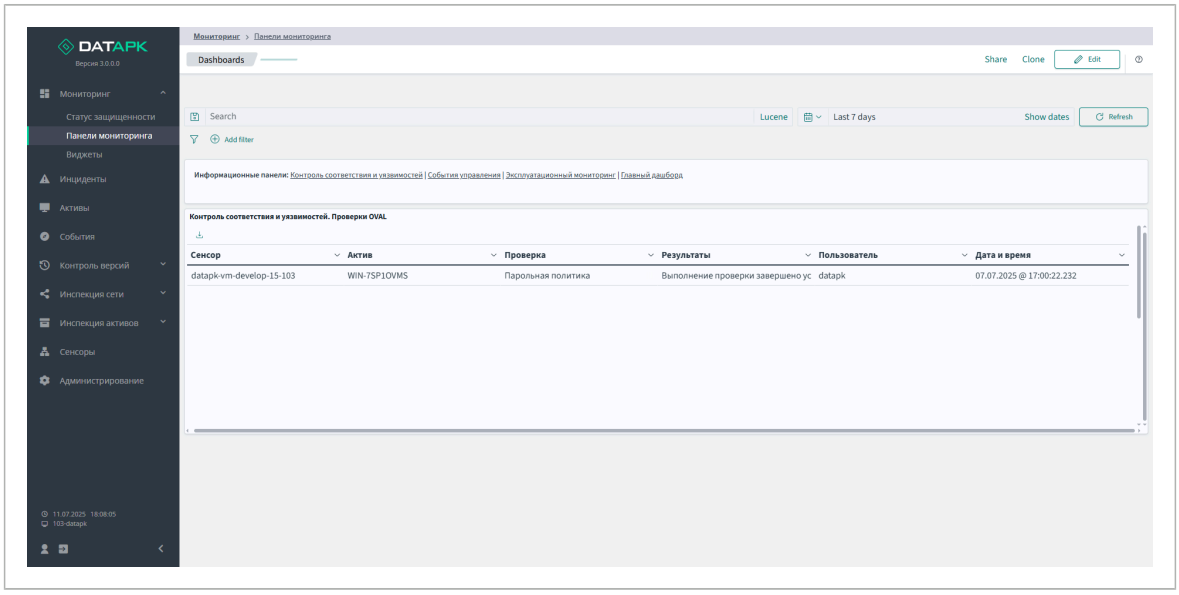


Рис. 66. Панель мониторинга «Контроль соответствия и уязвимостей»

Таблица включает в себя следующие столбцы:

- **Сенсор**;
- **Актив**;
- **Проверка** — название проверки на соответствие требованиям ИБ, которое можно увидеть на странице **Результаты проверок**;
- **Результаты** — основные данные по результатам выполненной проверки: есть ли уязвимости, несоответствия, в каком количестве;
- **Пользователь**;
- **Дата и время**.

Если проверки прошли успешно, действия не требуются. Иначе после обнаружения уязвимостей можно обратиться в главный интерфейс Комплекса для дальнейшего расследования.

10.4.6.2. События управления Комплексами

Панель мониторинга **События управления Комплексами** содержит две таблицы, которые позволяют проследить, какие пользователи и с каких IP-адресов входили в Комплекс, а также совершенные ими изменения.

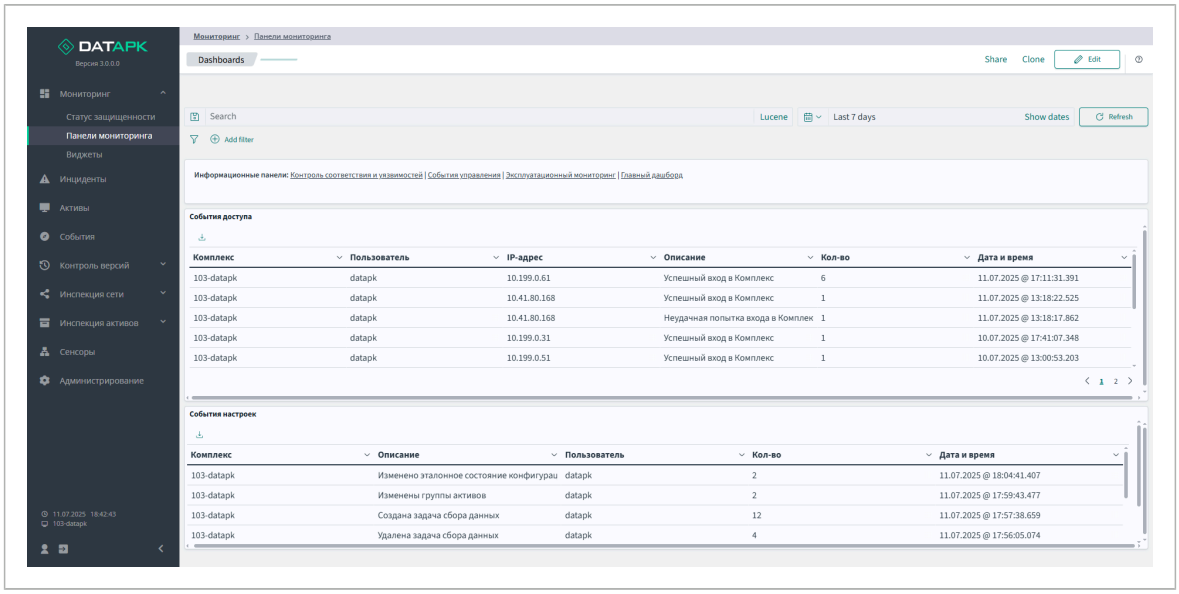


Рис. 67. Панель мониторинга «События управления»

Подробнее о назначении визуализаций — в таблице ниже (Таблица 13. Описание визуализаций на странице «События управления»).

Табл. 13. Описание визуализаций на странице «События управления»

НАЗВАНИЕ	ОПИСАНИЕ	СОДЕРЖАНИЕ
Таблицы		
События доступа к Комплексам	Позволяет просмотреть все попытки входа в систему	Комплекс, Пользователь, IP-адрес источника, Описание, Кол-во, Дата и время
События настроек Комплексов	Содержит список событий изменения настроек и управления Комплексом	Комплекс, Описание, Пользователь, Кол-во, Дата и время

Содержимое панели мониторинга может понадобиться для расследования случаев неправильной настройки Комплекса, кем и когда они были сделаны.

10.4.6.3. Эксплуатационный мониторинг

Панель мониторинга **Эксплуатационный мониторинг** содержит таблицы, которые позволяют отследить события между Комплексом и сенсорами, найти ошибки сбора событий, просмотреть события режима функционирования Комплекса.

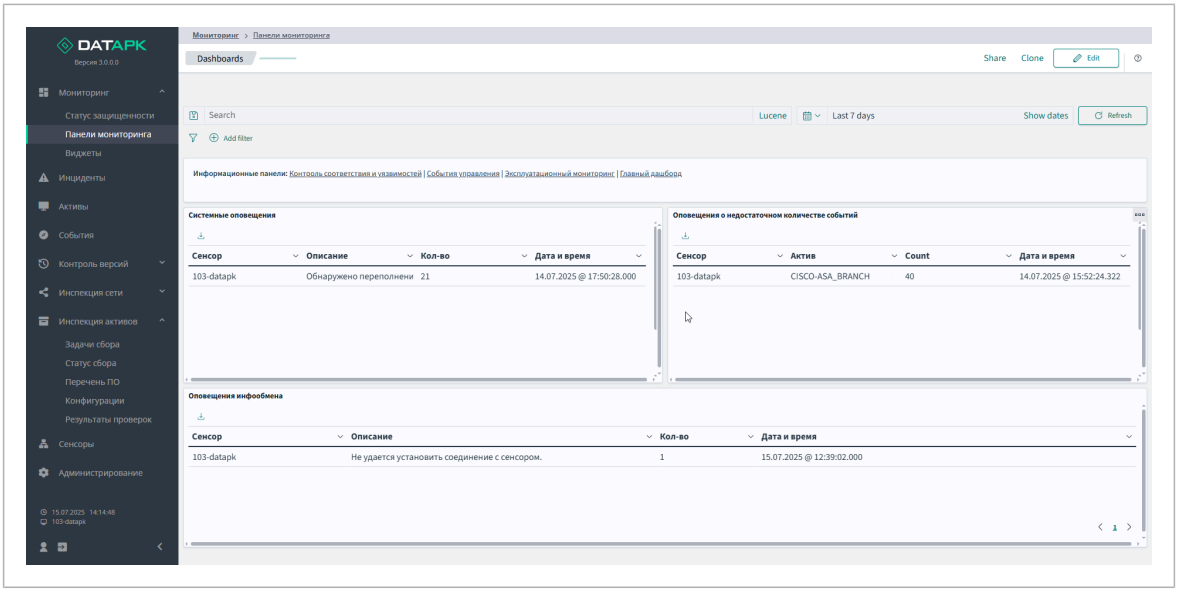


Рис. 68. Панель мониторинга «Эксплуатационный мониторинг»

Подробнее о назначении визуализаций — в таблице ниже (Таблица 14. Описание визуализаций на странице «Эксплуатационный мониторинг»).

Табл. 14. Описание визуализаций на странице «Эксплуатационный мониторинг»

НАЗВАНИЕ	ОПИСАНИЕ	СОДЕРЖАНИЕ
Таблицы		
Системные оповещения	Содержит список событий об изменении состояния служб текущего Комплекса или о существенном изменении нагрузки на текущий Комплекс	Комплекс, Описание, Count, Дата и время
Оповещения о недостаточном количестве событий	Содержит список событий об отклонении количества событий от источников от ожидаемого количества	Комплекс, Описание, Count, Дата и время
Оповещения инфообмена Комплексов	Содержит список событий об изменении состояния информационного обмена между текущим Комплексом и подключенными к нему сенсорами	Комплекс, Описание, Детализация, Кол-во, Дата и время

В случае обнаружения ошибок сбора данных следует обратиться в главный интерфейс Комплекса для дальнейшего расследования и устранения ошибок.

Для оповещений инфообмена Комплекса действия требуются только в случае обнаружения событий, не свойственных нормальному функционированию системы.

10.4.7. Экспорт событий из панели мониторинга

На каждой панели мониторинга, где есть список, возможен экспорт содержащихся в таблице элементов.

Для экспорта:

1. Наведите курсор мыши на таблицу в панели мониторинга.
2. В начале таблицы нажмите кнопку .
3. Выберите нужный вам тип экспорта из выпадающего списка:
    - **Formatted** — дата и время выгружаются в форматированном виде;
    - **Raw** — дата и время выгружаются в формате числа.

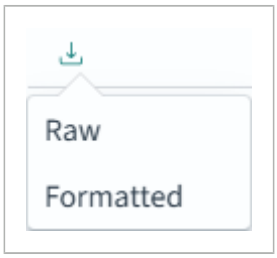


Рис. 69. Типы экспорта событий

- **Результат шага:** сразу после нажатия файл формата `*.csv` сформируется и будет скачан автоматически.

10.4.8. Панели мониторинга модуля «EDR for PLC»

Панели мониторинга модуля UDV DATAPK EDR for PLC предоставляют сводную информацию о функционировании модуля и позволяют визуализировать данные моделей. Примеры панелей мониторинга модуля UDV DATAPK EDR for PLC представлены ниже.

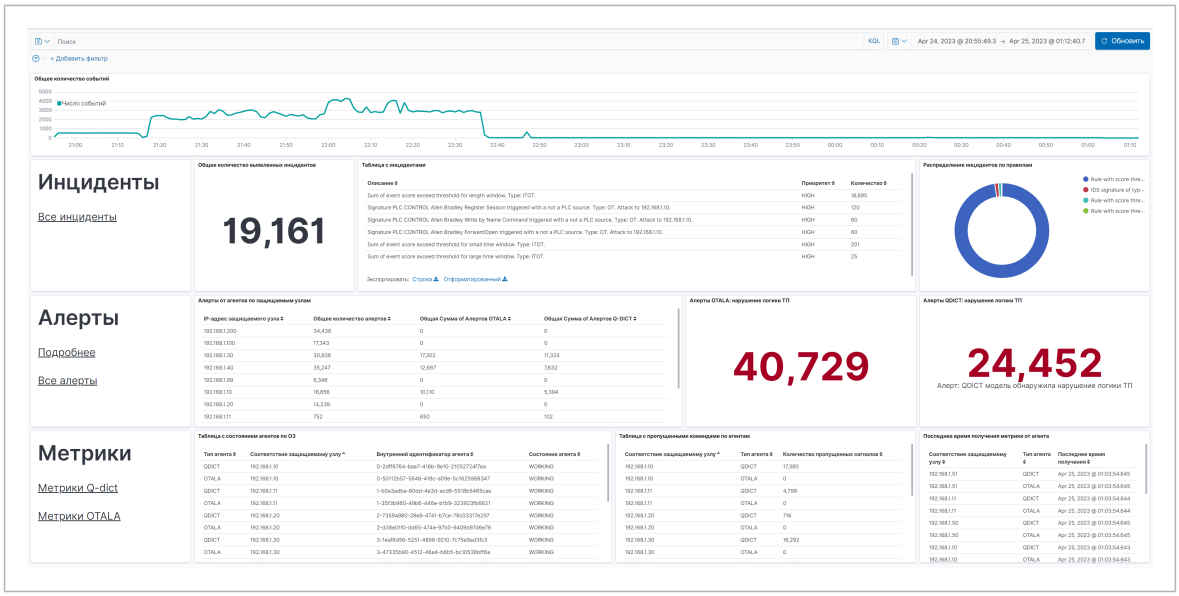


Рис. 70. Основная панель мониторинга модуля «EDR for PLC»

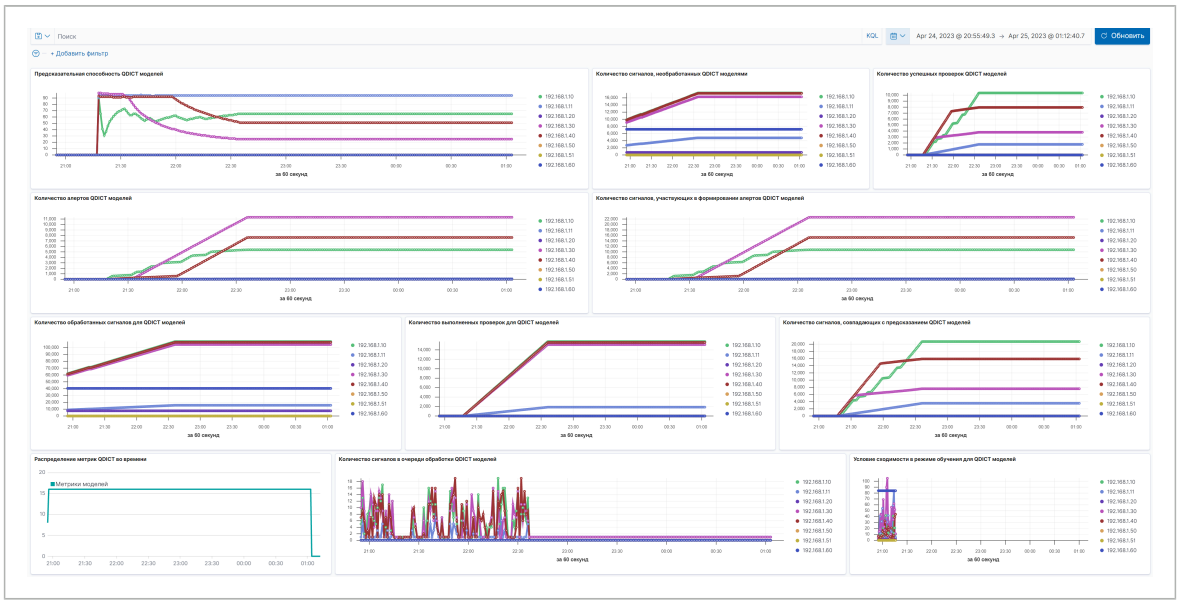


Рис. 71. Отображение информации о моделях на основе иерархического словаря

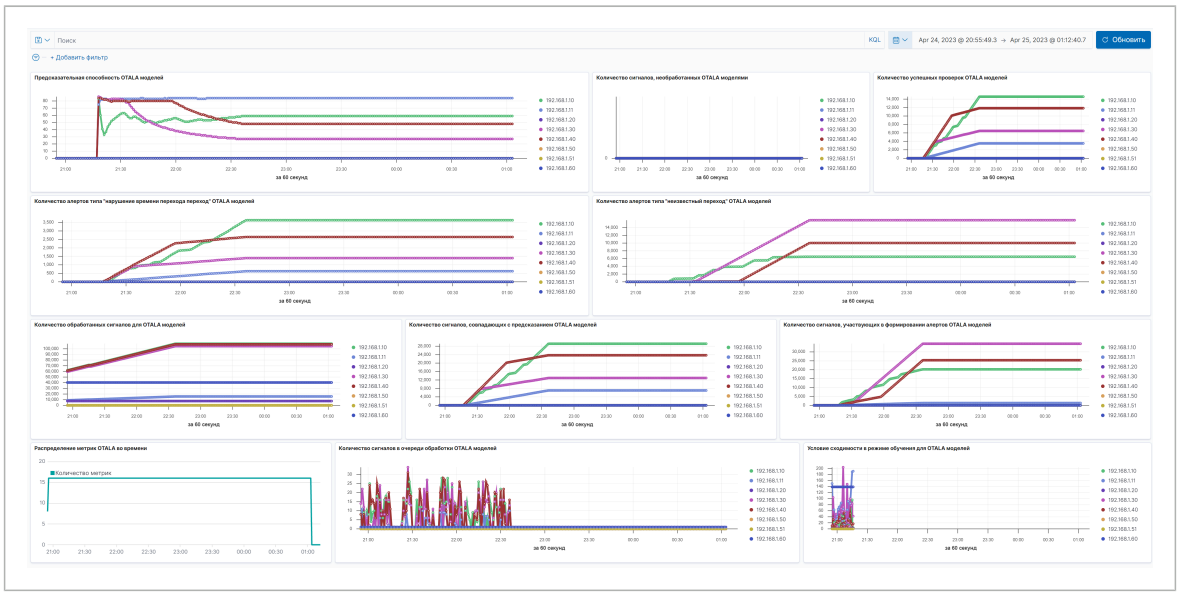


Рис. 72. Отображение информации о моделях на основе временных автоматов

10.5. Настройка сбора событий

В этом разделе:

- Экспорт и импорт правил нормализации событий
- Экспорт и импорт источников событий
- Включение и отключение служебных источников
- Создание источника событий
- Управление источниками событий
- Выгрузка внешних событий Комплекса в архив
- Настройка отправки событий во внешнюю систему по протоколу Syslog при установленном модуле «Управление внешними событиями»

10.5.1. Экспорт и импорт правил нормализации событий

В этом разделе:

- Экспорт правил разбора событий
- Экспорт правил обогащения событий
- Экспорт схемы событий
- Импорт правил разбора событий
- Импорт правил обогащения событий
- Импорт схемы событий

10.5.1.1. Экспорт правил разбора событий

Для экспорта архива формата `*.zip`, содержащего правила разбора событий:

1. Перейдите на страницу **Администрирование → Основные настройки → Импорт и экспорт**.
2. На панели **События** в строке **Правила разбора событий** нажмите кнопку (**Экспортировать**).
3. Для скачивания файла нажмите на его название в верхнем правом углу под заголовком **Результат последнего экспорта**.
   - **Результат шага:** файл со списком правил `event_normalization_[дата_и_время].zip` будет загружен.

10.5.1.2. Экспорт правил обогащения событий

Для экспорта архива формата `*.zip`, содержащего правила обогащения событий:

1. Перейдите на страницу **Администрирование → Основные настройки → Импорт и экспорт**.
2. На панели **События** в строке **Правила обогащения событий** нажмите кнопку (**Экспортировать**).
3. Для скачивания файла нажмите на его название в верхнем правом углу под заголовком **Результат последнего экспорта**.
   - **Результат шага:** файл со списком правил `event_enhancement_[дата_и_время].zip` будет загружен.

10.5.1.3. Экспорт схемы событий

Перед выполнением:

Для экспорта архива формата `*.zip`, содержащего схему событий (шаблон индекса):

1. Перейдите на страницу **Администрирование → Основные настройки → Импорт и экспорт**.
2. На панели **События** в строке **Схема событий** нажмите кнопку (**Экспортировать**).
3. Для скачивания файла нажмите на его название в верхнем правом углу под заголовком **Результат последнего экспорта**.
   - **Результат шага:** файл со схемой событий `event_mapping_[дата_и_время].json` будет загружен.

10.5.1.4. Импорт правил разбора событий

Для импорта архива формата `*.zip`, содержащего правила разбора событий:

1. Перейдите на страницу **Администрирование → Основные настройки → Импорт и экспорт**.
2. На панели **События** в строке **Правила разбора событий** нажмите кнопку (**Импортировать**).
3. В открывшемся окне укажите расположение импортируемого файла.
4. Дождитесь успешного результата импорта.
   - **Результат шага:** сразу после загрузки файла в правом верхнем углу страницы в поле **Результат последнего импорта** появится статус `Успешно`, и правила будут загружены.

10.5.1.5. Импорт правил обогащения событий

Для импорта архива формата `*.zip`, содержащего правила обогащения событий:

1. Перейдите на страницу **Администрирование → Основные настройки → Импорт и экспорт**.
2. На панели **События** в строке **Правила обогащения событий** нажмите кнопку (**Импортировать**).
3. В открывшемся окне укажите расположение импортируемого файла.
4. Дождитесь успешного результата импорта.
   - **Результат шага:** сразу после загрузки файла в правом верхнем углу страницы в поле **Результат последнего импорта** появится статус `Успешно`, и правила будут загружены.

10.5.1.6. Импорт схемы событий

Перед выполнением:

Для импорта архива формата `*.zip`, содержащего схему событий (шаблон индекса):

1. Перейдите на страницу **Администрирование → Основные настройки → Импорт и экспорт**.
2. На панели **События** в строке **Схема событий** нажмите кнопку (**Импортировать**).
3. В открывшемся окне укажите расположение импортируемого файла.
4. Дождитесь успешного результата импорта.
   - **Результат шага:** сразу после загрузки файла в правом верхнем углу страницы в поле **Результат последнего импорта** появится статус `Успешно`, и схема будет загружена.

10.5.2. Экспорт и импорт источников событий

В этом разделе:

- Экспорт источников событий
- Импорт источников событий

10.5.2.1. Экспорт источников событий

Для экспорта источников событий в файл формата `*.json` с Комплекса:

1. Перейдите на страницу **Администрирование → Настройка активов → Источники**.
2. Нажмите кнопку **Экспортировать**.
   - **Результат шага:** файл `sources_[дата_и_время].json` будет загружен.

10.5.2.2. Импорт источников событий

Для импорта источников событий из файла формата `*.json` в Комплекс:

1. Перейдите на страницу **Администрирование → Настройка активов → Источники**.
2. Нажмите кнопку **Импортировать**.
3. В открывшемся окне укажите расположение импортируемого файла формата `*.json` и подтвердите выбор.
4. В открывшемся окне **Подготовка к импорту** выберите действие для элементов, которые отсутствуют в новом справочнике:
   - **Оставить** — новые элементы будут добавлены к уже существующим;
   - **Удалить** — старые элементы будут удалены и добавлены новые.

> Внимание:
>
> Доступен импорт только тех источников, для которых уже создан актив. Если актив, указанный в импортируемом источнике, отсутствует, то такой источник будет пропущен при импорте.

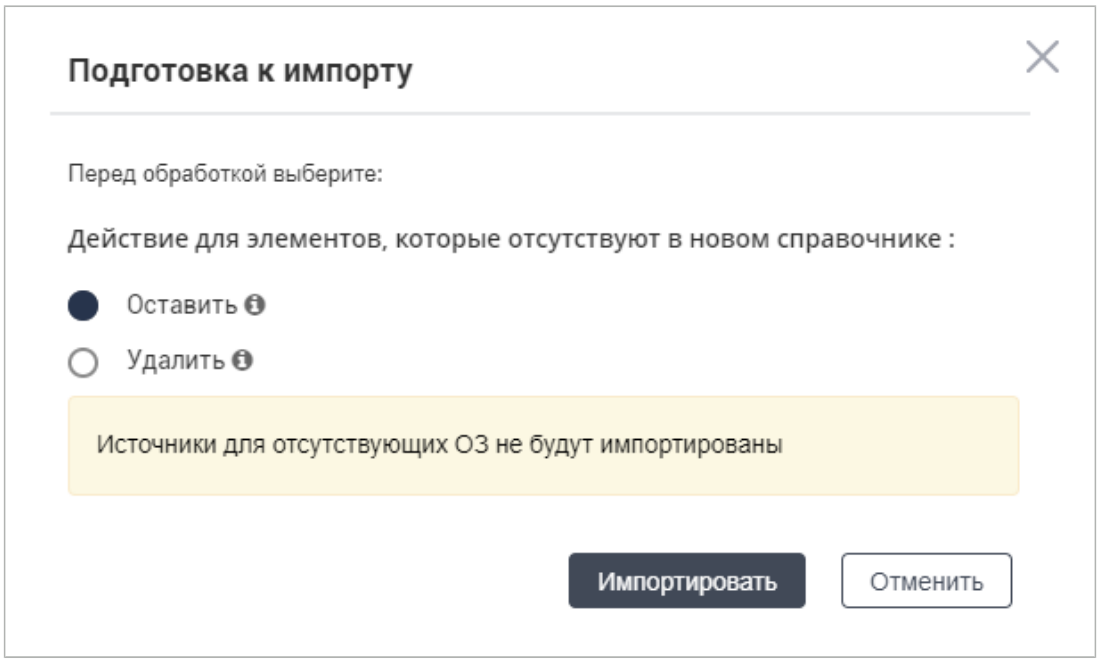


Рис. 73. Окно «Подготовка к импорту» при импорте источников событий активов

5. Нажмите кнопку **Импортировать** для выполнения импорта.
   - **Результат шага:** сразу после загрузки файла в правом вернем углу страницы появится уведомление: `Список «Источники» успешно обновлен`, и на странице отобразятся импортированные источники.

10.5.3. Включение и отключение служебных источников

По умолчанию все служебные источники Комплекса активны. Подробное описание служебных источников см. в разделе «Описание служебных источников событий».

Для управления запуском служебных источников:

1. Подключитесь к операционной системе Комплекса уровня Management.
2. Перейдите в рабочую директорию Комплекса (по умолчанию путь к рабочей директории Комплекса – `/usr/share/udv/datapk`). Для этого выполните команду:

   ```
   cd [Путь к рабочей директории Комплекса]
   ```

3. Остановите работу сервисов Комплекса с помощью команды:

   ```
   systemctl stop udv-* --all
   ```

4. Откройте конфигурационный файл `sensor.env` в режиме редактирования:

   ```
   mcedit sensor.env
   ```

5. Добавьте в конец файла необходимые переменные для настройки источников событий.

   > Подсказка:
   >
   > Подробное описание сенсоров и возможных переменных см. в разделе «Описание служебных источников событий».

6. Сохраните изменения в конфигурационном файле нажатием клавиши **F2**.
7. Подтвердите сохранение и нажмите клавишу **F10** для выхода.
8. Запустите работу сервисов Комплекса с помощью команды:

   ```
   systemctl start udv-* --all
   ```

9. Дождитесь запуска работы всех сервисов.

события от включенных источников будут регистрироваться на странице **События**.

10.5.4. Создание источника событий

Для создания SNMP-trap и Syslog-источников для сбора событий активов:

1. Перейдите на страницу **Администрирование → Настройка активов → Источники**.

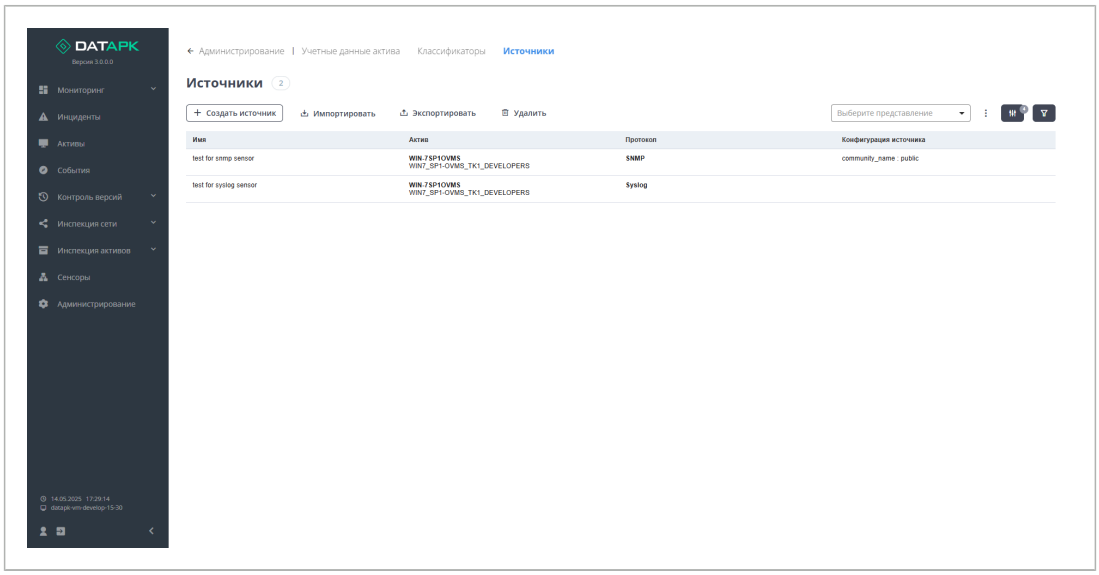


Рис. 74. Страница «Источники»

2. Нажмите кнопку **Создать источник**.
3. В открывшемся окне **Создание источника** задайте следующие параметры:
    а. наименование и описание источника;
    б. актив, который будет отправлять события на Комплекс;
    в. важность получаемых событий;
    г. чекбокс **Контроль активности источника** для автоматической проверки доступности источника и формирования события при отсутствии указанного количества событий за период.
    ▸ **Результат шага:** при установке чекбокса появятся два дополнительных поля: **Минимальное количество событий за период** и **Период, сек**.
    д. протокол `Syslog` или `SNMP`, по которому актив будет отправлять сообщения.
    ▸ **Результат шага:** При выборе `SNMP` появится дополнительное поле **Community**, в которое нужно ввести пароль для приема сообщений SNMP-trap. Для `Syslog` дополнительных полей нет.

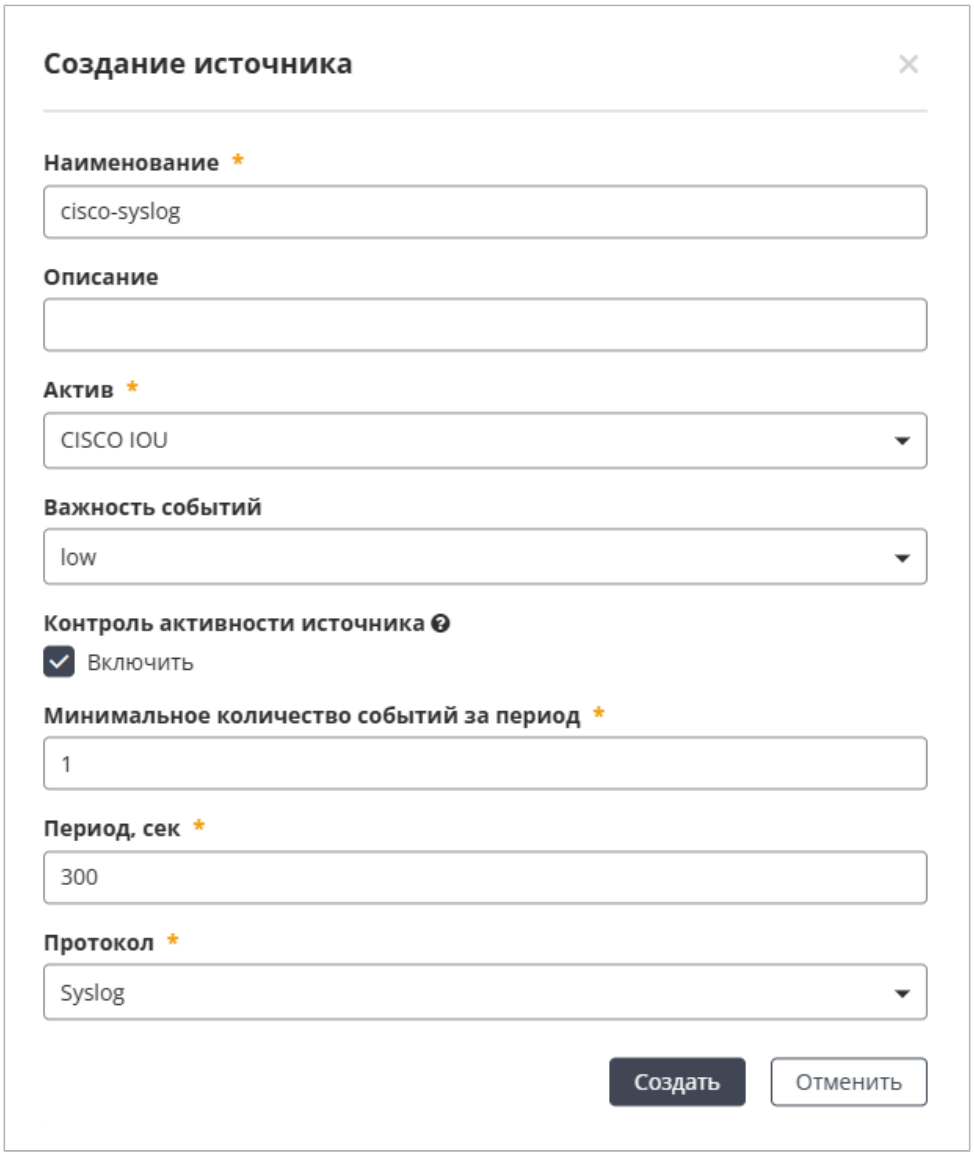


Рис. 75. Окно «Создание источника» при создании источника syslog_rfc3164_sensor

4. Нажмите кнопку **Создать** для подтверждения изменений.
   - **Результат шага:** будет создан новый источник событий.

10.5.5. Управление источниками событий

Для управления источниками событий присутствуют следующие возможности:

1. Запуск сбора событий от источника. Для возобновления процесса получения событий от определенного источника:
   a. Перейдите на страницу **Администрирование → Настройка активов → Источники**.
   б. Нажмите кнопку ▶ (**Запустить**) в строке с выбранным источником событий.
2. Приостановка сбора событий от источника. Для временной остановки процесса получения событий от источника, созданного вручную:
   a. Перейдите на страницу **Администрирование → Настройка активов → Источники**.
   б. Нажмите кнопку ⏸ (**Остановить**) в строке с выбранным источником событий.
3. Удаление источника событий. Для прекращения получения событий от источника:

a. Перейдите на страницу **Администрирование → Настройка активов → Источники**.

б. Нажмите кнопку (**Удалить источник**).

в. Введите текст обоснования удаления источника.

10.5.6. Выгрузка внешних событий Комплекса в архив

Комплекс сохраняет архивы индексов событий в операционную систему в директорию `/var/backups/elasticsearch/indices`.

10.5.6.1. Выгрузка индекса событий в архив

Чтобы сохранить отдельный индекс с событиями в архив в операционную систему Комплекса:

1. Перейдите на страницу **Администрирование → События и инциденты → Индексы**.

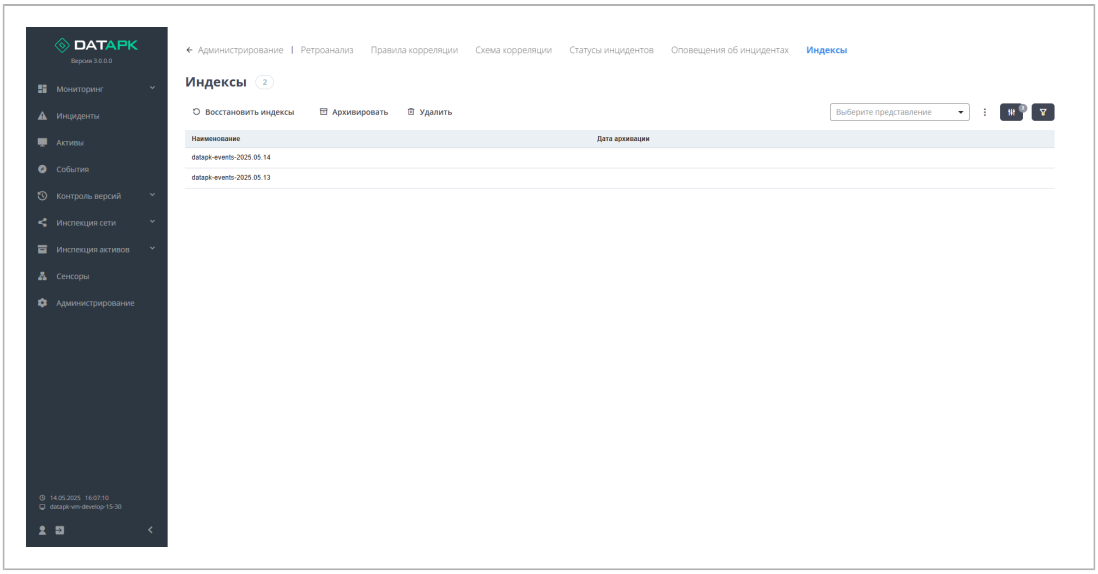


Рис. 76. Страница «Индексы»

2. Нажмите кнопку (**Архивировать**) справа от выбранного индекса.

   ▸ **Результат шага:** архив с событиями `datapk_events_[тип_индекса]_[дата_индекса]` будет загружен в директорию `/var/backups/elasticsearch/indices` в операционной системе Комплекса.

10.5.6.2. Выгрузка нескольких индексов событий в архив

Чтобы сохранить отфильтрованные индексы с событиями в архивы в операционную систему Комплекса:

1. Перейдите на страницу **Администрирование → События и инциденты → Индексы**.
2. Воспользуйтесь фильтрами для получения списка индексов, подлежащих архивированию.
3. Нажмите кнопку (**Архивировать**) в верхней части страницы.

   ▸ **Результат шага:** для каждого отфильтрованного индекса отдельный архив `datapk_events_[тип_индекса]_[дата_индекса]` будет загружен в директорию `/var/backups/elasticsearch/indices` в операционной системе Комплекса.

10.5.7. Настройка отправки внутренних событий во внешнюю систему по протоколу Syslog

Внутренние события Комплекса могут отправляться во внешние системы по следующим протоколам:

- UDP;
- TCP 5424.

10.5.7.1. Отправка событий по протоколу UDP

Для отправки внутренних событий по протоколу UDP:

1. Подключитесь к UDV DATAPK по протоколу SSH:

> Внимание:
>
> Если подключение по протоколу SSH в UDV DATAPK недоступно, убедитесь, что был корректно настроен сетевой интерфейс на шаге 13 инструкции «Установка сертифицированной ОС Альт Сервер 10.2 SP». При необходимости настройте интерфейс UDV DATAPK вручную по инструкции «Настройка сетевых интерфейсов в терминале Комплекса» и повторите подключение по SSH.

   а. Откройте программу-клиент SSH и выполните подключение к Комплексу с учетной записью, созданной на этапе установки (например, `user`).

   б. В окне подключения введите пароль учетной записи и нажмите **Enter**

> Прим.:
>
> При вводе пароль отображаться не будет.

   в. Повысьте привилегии, выполнив команду для смены учетной записи на `root`:

```
su -
```

   г. Введите пароль учетной записи `root` и нажмите клавишу **Enter**.

> Прим.:
>
> При вводе пароль отображаться не будет.

   ▸ **Результат шага:** будет выполнен вход в операционную систему под учетной записью `root` по протоколу SSH.

2. Откройте на редактирование файл `manager.env` командой:

```
mcedit /usr/share/udv/datapk/manager.env
```

3. Установите следующие значения переменных:

```
EVENT_SYSLOG_SEND=true
EVENT_SYSLOG_PROTOCOL=UDP
```

4. Дополнительно настройте фильтрацию сообщений о передаче внутренних событий, установив требуемое значение переменной `EVENT_SYSLOG_SEVERITY`.

> Внимание:
>
> При значении переменной `INFORMATIONAL` будут отображаться информационные сообщения.
> При значении переменной `CRITICAL` будут отображаться информационные сообщения, а также сообщения о состоянии системы, сообщения об ошибках, предупреждения о возможных проблемах.

5. Сохраните изменения в файле, нажав клавишу **F10**, и подтвердите сохранение изменений, выбрав **Да** или **Yes**.
6. Перезапустите сервис `udv-event-manager` командой:

```
systemctl restart udv-event-manager
```

7. Убедитесь, что новые события отправляются по Syslog. Для этого выполните команду:

```
tcpdump -i lo port 514 -s0 -v
```

10.5.7.2. Отправка событий по протоколу TCP 5424

Для отправки внутренних событий по протоколу TCP 5424:

1. Подключитесь к UDV DATAPK по протоколу SSH:

> Внимание:
>
> Если подключение по протоколу SSH в UDV DATAPK недоступно, убедитесь, что был корректно настроен сетевой интерфейс на шаге 13 инструкции «Установка сертифицированной ОС Альт Сервер 10.2 SP». При необходимости настройте интерфейс UDV DATAPK вручную по инструкции «Настройка сетевых интерфейсов в терминале Комплекса» и повторите подключение по SSH.

   а. Откройте программу-клиент SSH и выполните подключение к Комплексу с учетной записью, созданной на этапе установки (например, `user`).
   б. В окне подключения введите пароль учетной записи и нажмите **Enter**

> Прим.:
>
> При вводе пароль отображаться не будет.

   в. Повысьте привилегии, выполнив команду для смены учетной записи на `root`:

```
su -
```

   г. Введите пароль учетной записи `root` и нажмите клавишу **Enter**.

> Прим.:
>
> При вводе пароль отображаться не будет.

▸ **Результат шага:** будет выполнен вход в операционную систему под учетной записью `root` по протоколу SSH.

2. Откройте на редактирование файл `manager.env` командой:

```
mcedit /usr/share/udv/datapk/manager.env
```

3. Установите следующие значения переменных:

```
EVENT_SYSLOG_SEND=true
EVENT_SYSLOG_PORT=515
EVENT_SYSLOG_PROTOCOL=TCP
```

4. Дополнительно настройте фильтрацию сообщений о передаче внутренних событий, установив требуемое значение переменной `EVENT_SYSLOG_SEVERITY`.

> Внимание:
>
> При значении переменной `INFORMATIONAL` будут отображаться информационные сообщения.
> При значении переменной `CRITICAL` будут отображаться информационные сообщения, а также сообщения о состоянии системы, сообщения об ошибках, предупреждения о возможных проблемах.

5. Сохраните изменения в файле, нажав клавишу **F10**, и подтвердите сохранение изменений, выбрав **Да** или **Yes**.
6. Перезапустите сервис `udv-event-manager` командой:

```
systemctl restart udv-event-manager
```

7. Убедитесь, что новые события отправляются по Syslog. Для этого выполните команды:

```
tcpdump -i lo port 514 -s0 -v
ssh -L localhost:15672:127.0.0.1:15672 root@[IP-адрес Комплекса]
```

См. также

Отправка внутренних событий по протоколу Syslog

10.5.8. Настройка отправки событий во внешнюю систему по протоколу Syslog при установленном модуле «Управление внешними событиями»

Для отправки событий во внешнюю систему, например SIEM:

1. Проверьте наличие файла `95-siem-output.conf` в директории `/etc/logstash/pipeline`, выполнив команду:

```
ls /etc/logstash/pipeline
```

2. Если конфигурационный файл `95-siem-output.conf` отсутствует в директории `/etc/logstash/pipeline`, скопируйте его в текущую директорию одним из способов:
   - скопируйте его из дистрибутива Комплекса;
   - создайте новый файл вручную, выполнив команду:

```
> 95-siem-output.conf
```

ОСТОРОЖНО:

Данная команда должна выполняться не в директории `/etc/logstash/pipeline`

3. Откройте конфигурационный файл `95-siem-output.conf` для редактирования.
4. Если файл `95-siem-output.conf` пустой и был создан вручную, скопируйте в него следующий текст:

```
output {
    syslog {
        host => "1.1.1.1" # IP-адрес внешнего сервера
        port => 514 # порт получения на внешнем сервере, если он не стандартный
        codec => "json"
        protocol => "udp"
        facility => "loc0"
        severity => "informational"
        sourcehost => "${DATAPK_NAME}"
        appname => "datapk_event"
    }
}
```

5. При необходимости измените в файле `95-siem-output.conf` следующие параметры:
   - в поле `host` измените IP-адрес внешнего сервера, на который будет выполняться отправка событий;
   - в поле `port` измените номер порта, если на внешнем сервере настроен другой порт для получения событий по Syslog UDP.
6. Сохраните изменения в файле, нажав клавишу **F10**, и подтвердите сохранение изменений, выбрав **Yes**.
7. Поместите созданный файл в `/etc/logstash/pipeline` командой:

```
mv 95-siem-output.conf /etc/logstash/pipeline
```

8. Измените права на файл `95-siem-output.conf`, выполнив команду:

```
chmod 777 /etc/logstash/pipeline/95-siem-output.conf
```

9. Перезапустите сервис `udv-logstash`, выполнив команду:

```
systemctl restart udv-logstash.service
```

10. Убедитесь в отсутствии ошибок в журнале сообщений сервиса `udv-logstash`, выполнив команду:

```
journalctl -u udv-logstash.service
```

11. Откройте веб-интерфейс Комплекса и убедитесь, что события генерируются.
12. Убедитесь, что сетевой трафик отправляется на внешний Syslog-сервер. Для этого перейдите в режим командной строки Комплекса и введите команду:

```
tcpdump -nn -i [наименование интерфейса для отправки событий] host [адрес Syslog-сервера]
```

```
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp11s0, link-type EN10MB (Ethernet), capture size 262144 bytes
11:52:22.716156 IP 10.51.202.39.33624 > 10.51.201.130.514: SYSLOG console.info,
length: 1042
11:52:22.716391 IP 10.51.202.39.33624 > 10.51.201.130.514: SYSLOG console.info,
length: 872
11:52:22.716551 IP 10.51.202.39.33624 > 10.51.201.130.514: SYSLOG console.info,
length: 944
11:52:22.716721 IP 10.51.202.39.33624 > 10.51.201.130.514: SYSLOG console.info,
length: 744
11:52:22.717552 IP 10.51.201.130 > 10.51.202.39: ICMP 10.51.201.130 udp port 514
 unreachable, length 556
11:52:22.717605 IP 10.51.201.130 > 10.51.202.39: ICMP 10.51.201.130 udp port 514
 unreachable, length 556
11:52:22.717647 IP 10.51.201.130 > 10.51.202.39: ICMP 10.51.201.130 udp port 514
 unreachable, length 556
11:52:22.718272 IP 10.51.201.130 > 10.51.202.39: ICMP 10.51.201.130 udp port 514
 unreachable, length 556
11:52:22.949030 IP 10.51.202.39.33624 > 10.51.201.130.514: SYSLOG console.info,
length: 686
11:52:22.950098 IP 10.51.201.130 > 10.51.202.39: ICMP 10.51.201.130 udp port 514
 unreachable, length 556
11:52:23.006557 IP 10.51.202.39.33624 > 10.51.201.130.514: SYSLOG console.info,
length: 686
```

Рис. 77. Пример отправки сетевого трафика на внешний Syslog-сервер

13. Остановите просмотр сетевого трафика на интерфейсе, используя комбинацию клавиш `Ctrl+C`.

10.5.8.1. Остановка отправки событий во внешнюю систему по протоколу Syslog

Для остановки отправки событий во внешнюю систему по протоколу Syslog:

1. Удалите конфигурационный файл `95-siem-output.conf` из директории `/etc/logstash/pipeline`, выполнив команду:

   ```
   rm -f /etc/logstash/pipeline/95-siem-output.conf
   ```

2. Перезапустите сервис `udv-logstash`, выполнив команду:

   ```
   systemctl restart udv-logstash.service
   ```

3. Убедитесь в отсутствии ошибок в журнале сообщений сервиса `udv-logstash`, выполнив команду:

   ```
   journalctl -u udv-logstash.service
   ```

10.6. Настройка и управление мониторингом

В этом разделе:

- Создание шаблона индекса
- Создание и настройка виджета
- Просмотр и управление виджетами
- Создание и настройка панели мониторинга
- Настройка пользовательских правил нормализации событий
- Настройка форматирования чисел и дат в разделе «Мониторинг»
- Экспорт и импорт объектов раздела «Мониторинг»

10.6.1. Создание шаблона индекса

Перед выполнением:

Для создания шаблона индекса необходимо, чтобы был настроен сбор событий. Служебные источники событий по умолчанию генерирует события безопасности, если они не были отключены вручную перед запуском Комплекса.

Подсказка:

- События, которые Комплекс генерирует по умолчанию, и их настройка описаны в разделах «Описание служебных источников событий» и «Включение и отключение служебных источников».
- Создание источников для пассивного сбора событий описано в разделе «Создание источника событий», настройка активного сбора событий описана в разделе «Настройка активного сбора событий».

Для создания шаблона индекса:

1. Перейдите на страницу **Администрирование → Основные настройки → Настройки мониторинга** и откройте вкладку **Шаблоны индексов**.

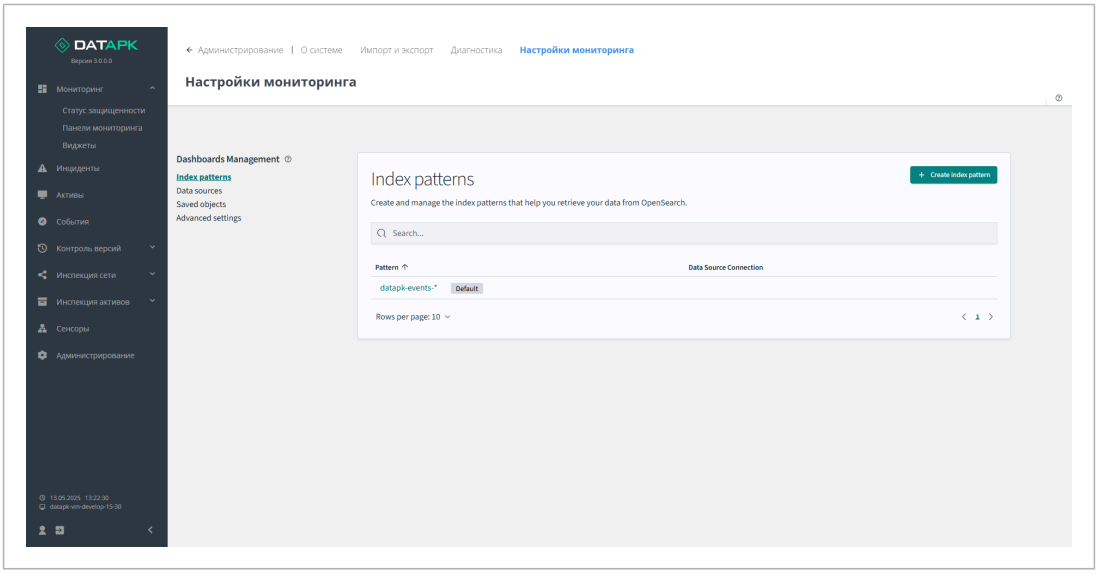


Рис. 78. Страница «Настройки мониторинга»

2. Нажмите **Create index pattern**.
   - **Результат шага:** Откроется окно **Create index pattern**.
3. В окне **Create index pattern**:
   a. Введите название предустановленного шаблона `datapk-events-*` в поле **Index pattern name**.
   б. Нажмите **Next step**.

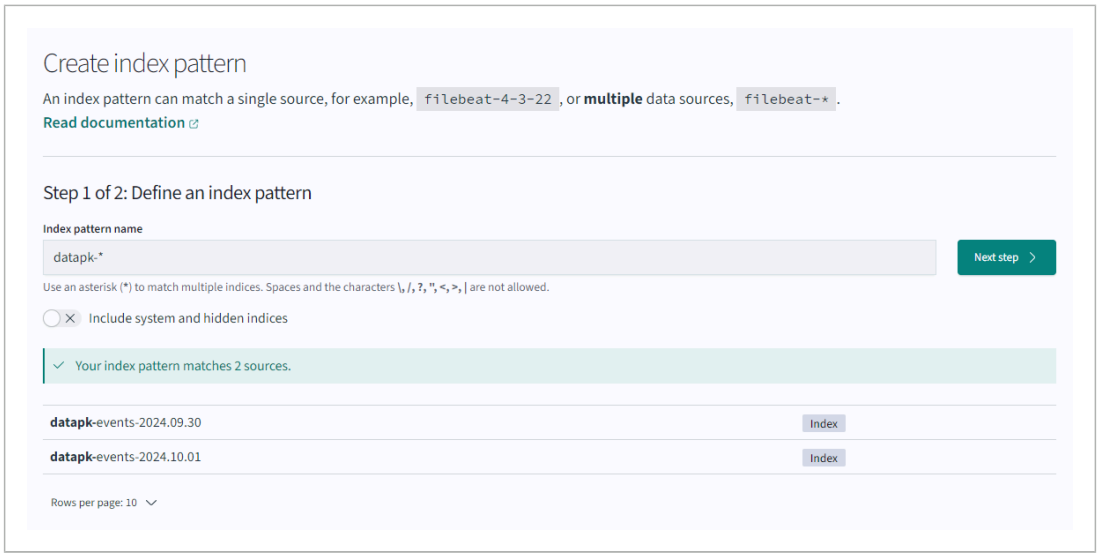


Рис. 79. Окно создания нового шаблона нормализации событий

4. В поле **Time field** выберите из списка поле фильтра времени `create_time` (время создания события).

> Внимание:
>
> Если в вашей инсталляции не используется активный сбор событий, допускается выбор сортировки по времени получения события (`receive_time`).

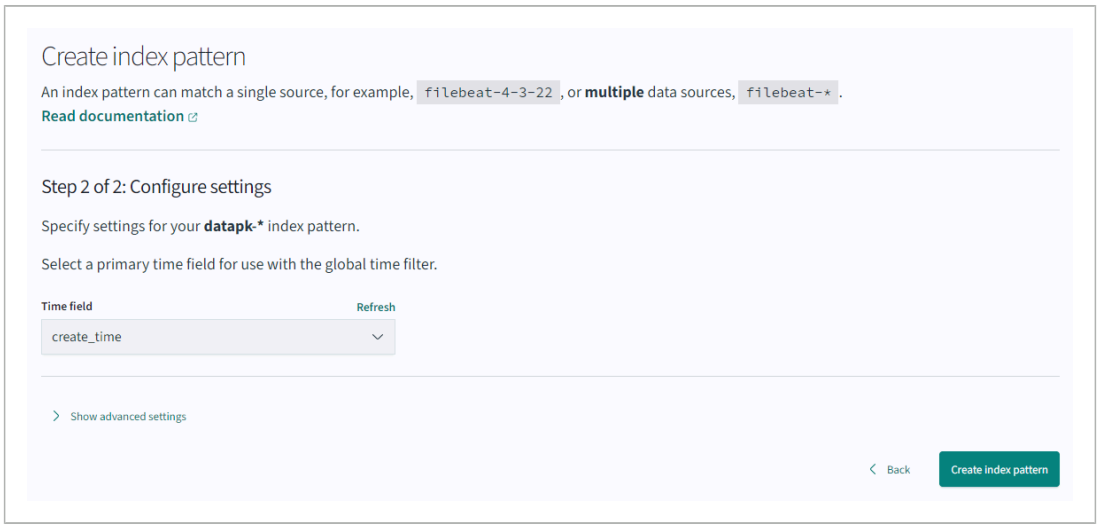


Рис. 80. Окно настройки атрибута временного фильтра в интерфейсе визуализации

5. Нажмите кнопку **Create index pattern**.
6. Откройте страницу **События → Экспертный режим**.

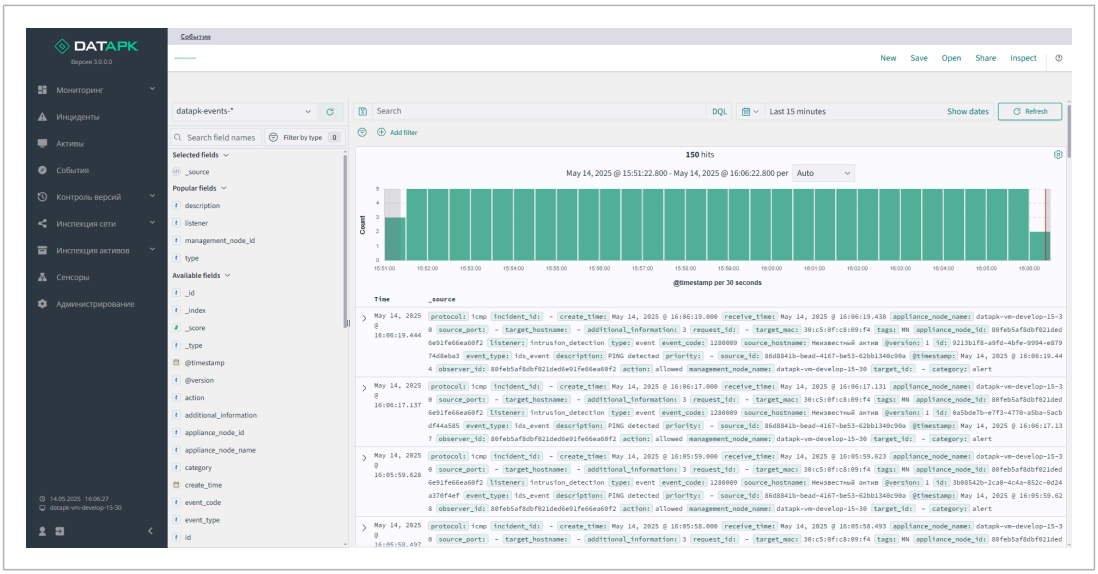


Рис. 81. Страница «События» → «Экспертный режим»

7. Убедитесь, что в список полей **Available fields** были загружены поля из предустановленного шаблона.

10.6.2. Удаление шаблона индекса

Для удаления шаблона индекса:

1. В веб-интерфейсе Комплекса откройте страницу **Администрирование → Основные настройки → Настройки мониторинга** и откройте вкладку **Шаблоны индексов**.
2. Нажмите на название шаблона индекса, который необходимо удалить. Откроется страница выбранного шаблона.

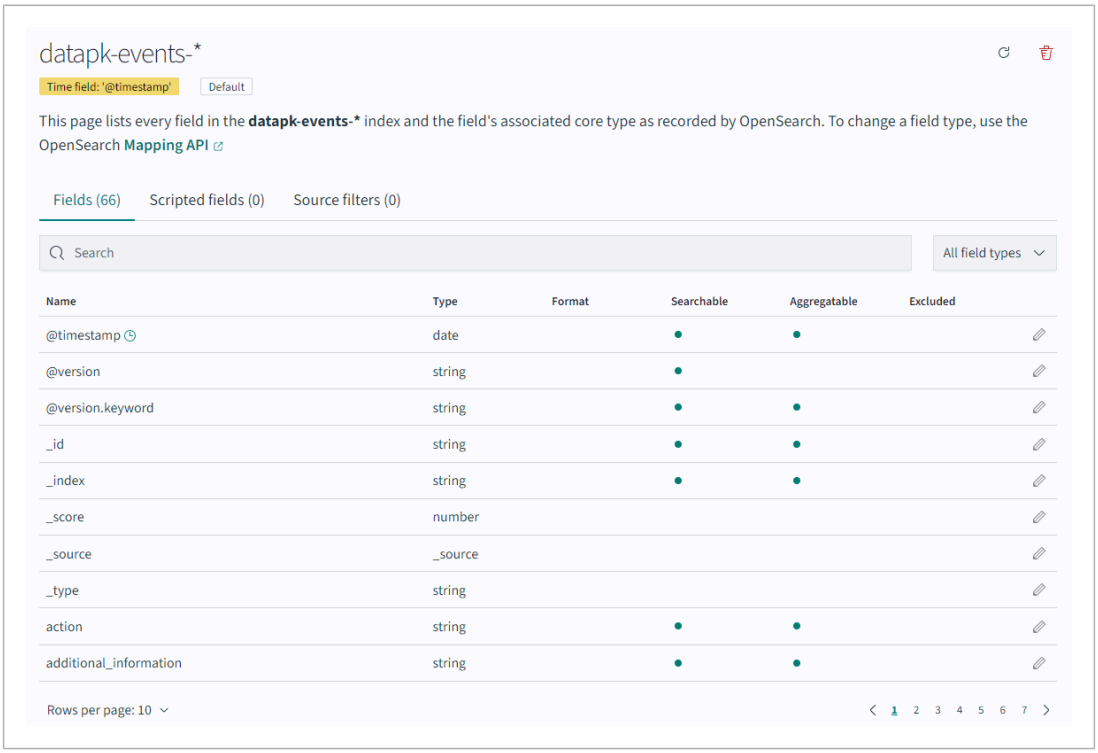


Рис. 82. Внешний вид страницы шаблона индекса

3. Нажмите в правом верхнем углу.

4. В открывшемся окне нажмите **Delete**.

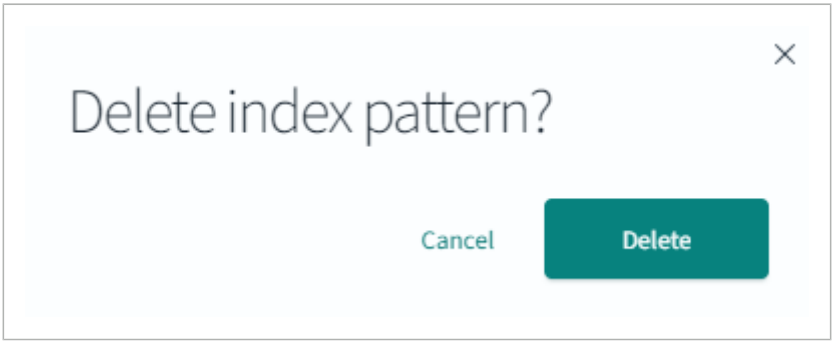


Рис. 83. Окно подтверждения удаления шаблона индекса

- **Результат шага:** Шаблон индекса будет удален. После удаления шаблона индекса просмотр событий будет недоступен, в том числе на панелях мониторинга и визуализациях, но события не будут удалены.

5. Для возможности дальнейшего просмотра событий создайте новый шаблон индекса — подробнее см. Создание шаблона индекса.

10.6.3. Создание и настройка виджета

Для создания и настройки виджета (визуализации):

1. Перейдите на страницу **Мониторинг → Виджеты**.

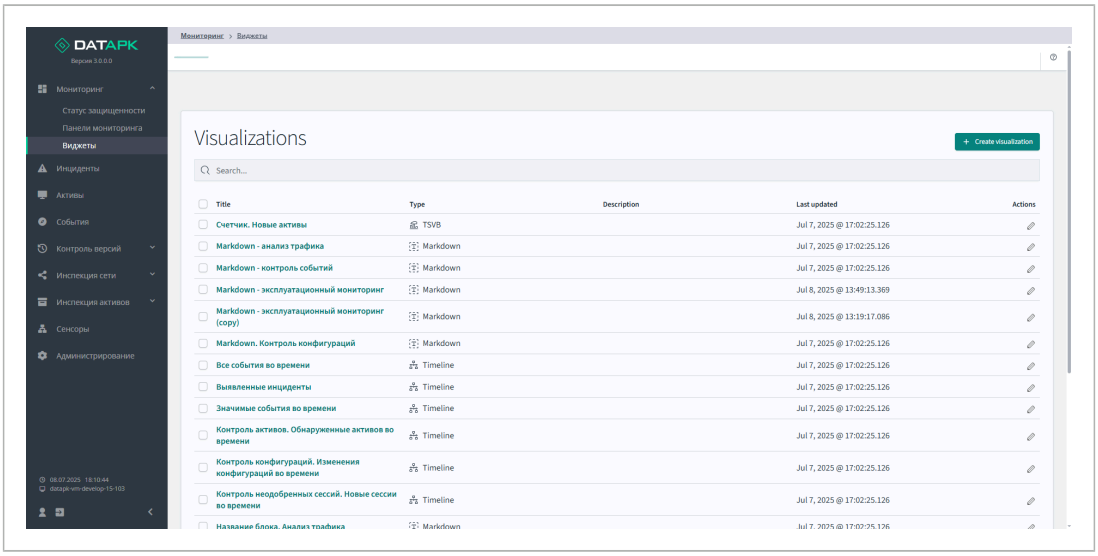


Рис. 84. Страница «Виджет»

2. Нажмите кнопку **Create new visualization**.
3. В открывшемся окне **New visualization** выберите тип виджета.

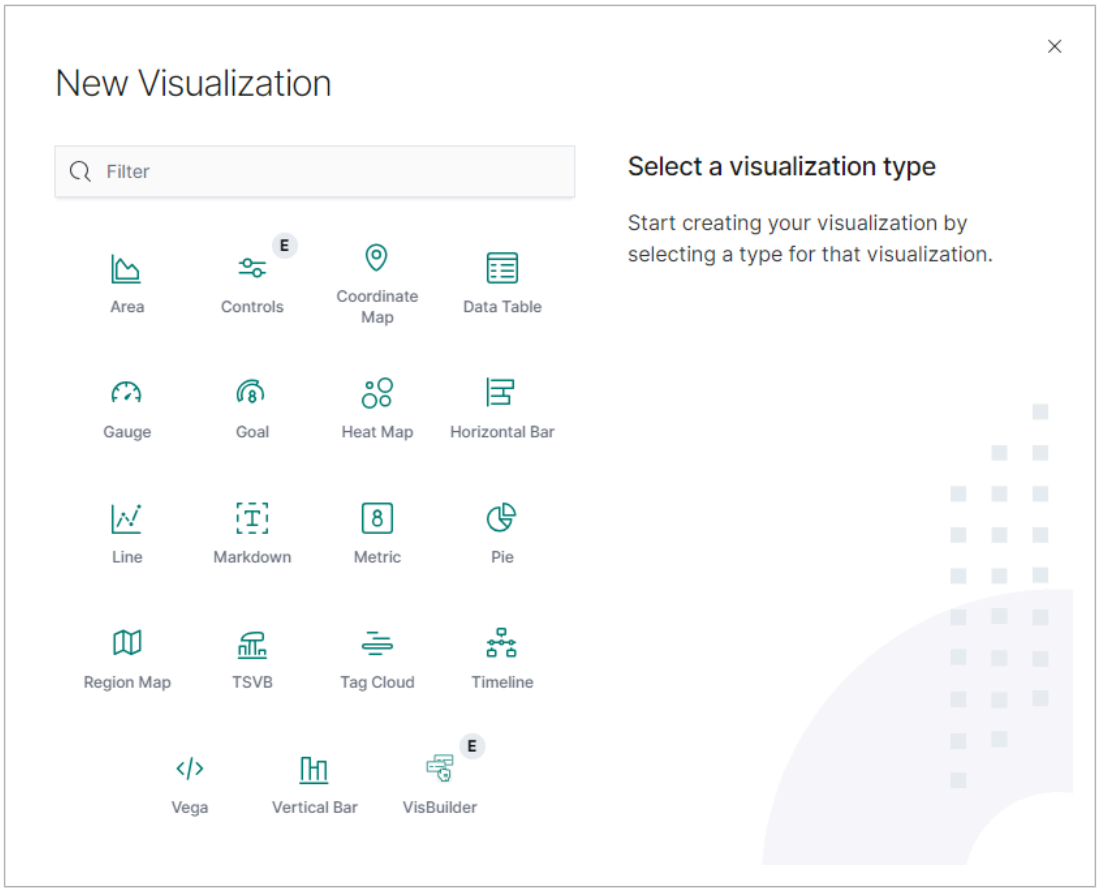


Рис. 85. Окно «New visualization»

4. Выберите источник данных для графического представления.

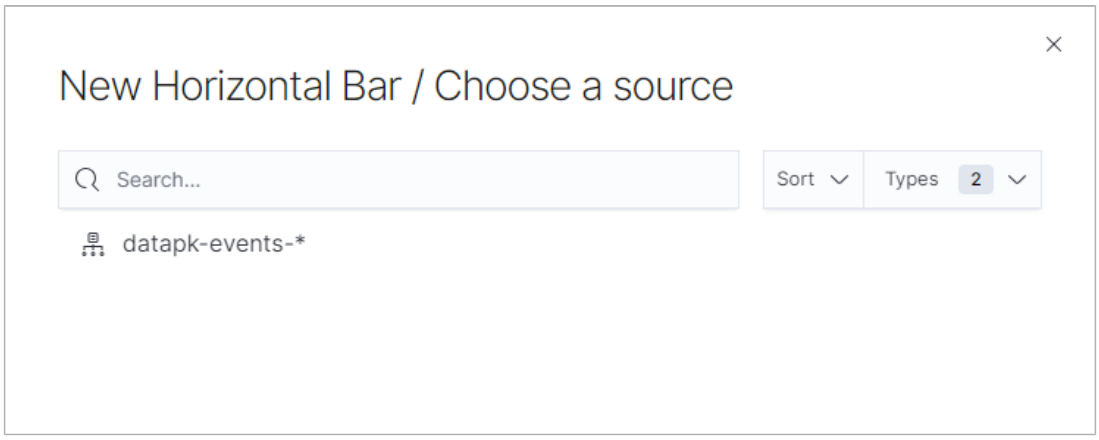


Рис. 86. Выбор источника данных для визуализации

5. Настройте визуализируемые параметры в правой части страницы. Для подтверждения изменений и получения результата нажмите в нижней части страницы кнопку **Update**.

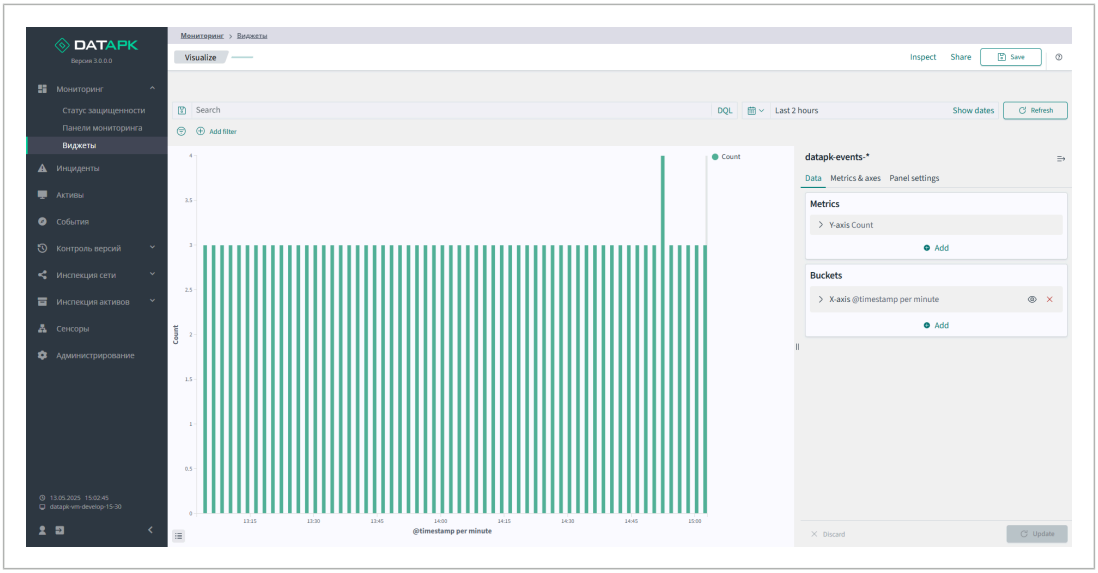


Рис. 87. Виджет типа «Вертикальная диаграмма» с разбивкой событий по временным интервалам

6. Для сохранения визуализации:
    a. нажмите кнопку **Refresh** в верхней части страницы;
    б. нажмите кнопку **Save** в верхней части страницы;
    в. в появившемся окне в поле **Title** введите название сохраняемого объекта;
    г. нажмите кнопку **Save**.
7. Перейдите на страницу **Администрирование → Основные настройки → Настройки мониторинга**, вкладка **Saved Objects**.
8. Убедитесь, что в списке присутствует сохраненный объект.

10.6.4. Просмотр и управление виджетами

Для работы с уже имеющимися виджетами (визуализациями) в интерфейсе Комплекса предусмотрены следующие возможности:

1. Просмотр виджета. Для просмотра:
    a. Перейдите на страницу **Мониторинг → Виджеты**.
    б. Нажмите на название виджета.
    - **Результат шага:** произойдет переход к режиму редактирования визуализации.
2. Редактирование визуализаций. Для редактирования:
    a. Перейдите на страницу **Мониторинг → Виджеты**.
    б. Нажмите (**Edit**).
    в. Измените параметры визуализации.
    г. Нажмите кнопку **Update** в нижнем правом углу страницы, чтобы применить изменения.
    д. Нажмите кнопку **Save** в верхнем правом углу страницы.
    e. В появившемся окне при необходимости измените название и описание визуализации и нажмите кнопку **Save**.
3. Удаление визуализаций. Для удаления одной или нескольких визуализаций:

а. Перейдите на страницу **Мониторинг → Виджеты**.

б. Выберите виджеты при помощи чекбокса слева.

> Подсказка:
>
> Для выбора всех виджетов на странице, установите самый первый чекбокс.

в. Нажмите кнопку **Delete [N] visualization(s)** в верхней части страницы. Параметр `[N]` в названии кнопки — количество удаляемых объектов.

10.6.5. Создание и настройка панели мониторинга

Создание, изменение и просмотр пользовательских панелей мониторинга осуществляется на странице **Панели мониторинга**. Панели мониторинга объединяют несколько визуализаций (виджетов) в одну страницу и могут фильтровать их. Создание новой панели мониторинга возможно при наличии хотя бы одного сохраненного запроса или визуализации.

10.6.5.1. Создание панели мониторинга

Для создания панели мониторинга:

1. Перейдите на страницу **Мониторинг → Панели мониторинга**.

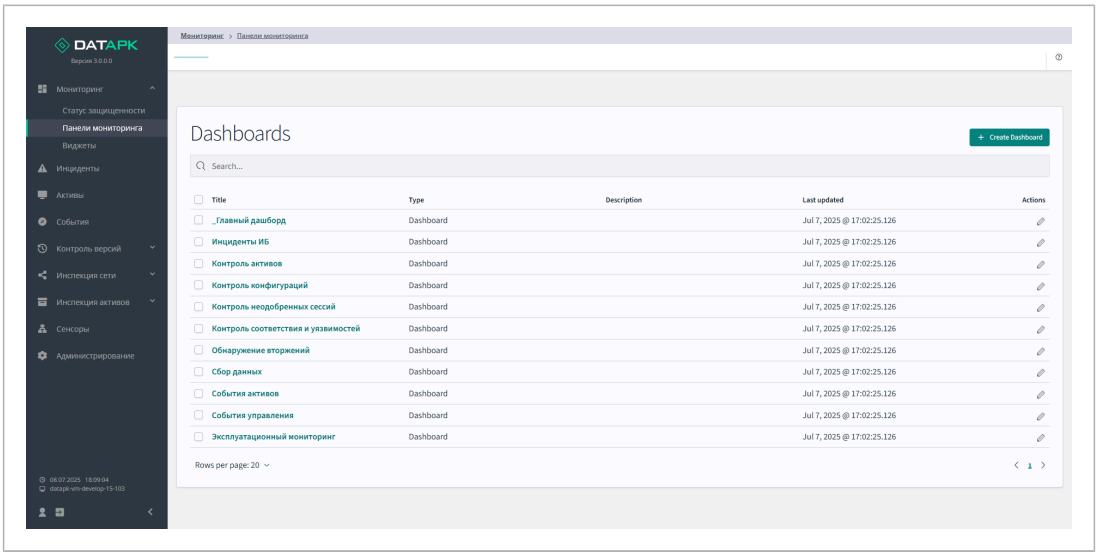


Рис. 88. Страница «Панели мониторинга»

2. Нажмите кнопку **Create new dashboard**.
   - **Результат шага:** появится страница редактирования новой панели мониторинга.
3. Для добавления новой визуализации (виджета):

   а. Нажмите кнопку **Create new** (подробнее см. в разделе «Создание и настройка виджета»).

   б. Для добавления созданного виджета на панель перейдите к следующему шагу текущей инструкции.

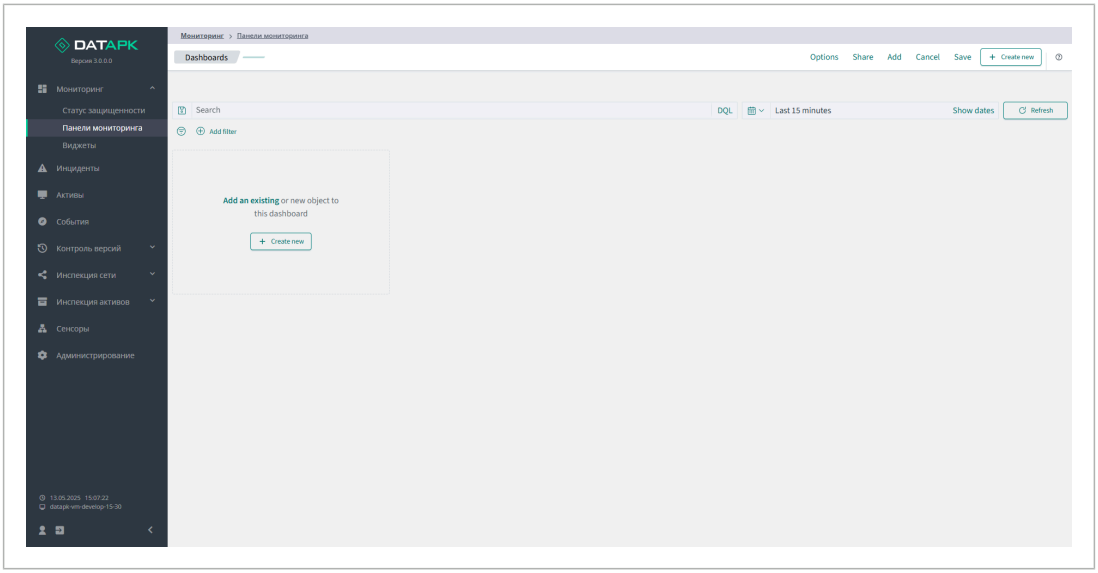


Рис. 89. Страница добавления новой визуализации на панель мониторинга

4. Для добавления существующей визуализации:
    a. Нажмите кнопку **Add an existing**.
    б. В появившемся окне выберите один или несколько виджетов.
    в. Нажмите ✕, чтобы закрыть окно выбора виджетов и вернуться к панели мониторинга.
5. При необходимости фильтрации данных введите запрос в поле запроса и добавьте фильтры с помощью кнопки **+ Add filter**.
6. Для сохранения панели мониторинга:
    a. Нажмите кнопку **Save** в верхнем правом углу страницы.
    б. В появившемся окне в поле **Title** введите название сохраняемого объекта.
    в. Нажмите кнопку **Save**.
7. Перейдите на страницу **Администрирование → Основные настройки → Настройки мониторинга**, вкладка **Saved objects** и убедитесь, что в списке присутствует сохраненный объект.

10.6.5.2. Добавление виджета

Для добавления виджета на панель мониторинга:

1. Перейдите на страницу **Мониторинг → Панели мониторинга**.
2. Нажмите на название нужной панели мониторинга в списке.
    - **Результат шага:** откроется выбранная панель мониторинга.
3. Нажмите кнопку **Edit** в верхнем правом углу страницы.
    - **Результат шага:** панель станет доступна для редактирования.
4. Для добавления нового виджета:
    a. Нажмите кнопку **Create new** в верхнем правом углу страницы (подробнее см. в разделе «Создание и настройка виджета»).
    б. Для добавления созданного виджета на панель перейдите к следующему шагу текущей инструкции.
5. Для добавления существующего виджета:

a. Нажмите кнопку **Add** в верхнем правом углу страницы.

б. В появившемся окне выберите один или несколько виджетов.

в. Нажмите ✕, чтобы закрыть окно выбора виджетов и вернуться к панели мониторинга.

6. Для сохранения изменений нажмите кнопку **Save** в верхнем правом углу страницы.
7. В открывшемся окне нажмите кнопку **Save**.

10.6.5.3. Изменение виджета

Для изменения виджета на панели мониторинга:

1. Перейдите на страницу **Мониторинг → Панели мониторинга**.
2. Нажмите на название нужной панели мониторинга в списке.
   - **Результат шага:** откроется выбранная панель мониторинга.
3. Нажмите кнопку **Edit** в верхнем правом углу страницы.
   - **Результат шага:** панель станет доступна для редактирования.
4. Нажмите кнопку ⚙ в верхнем правом углу виджета, который нужно изменить.
5. В появившемся списке выберите пункт **Edit visualization**.
   - **Результат шага:** откроется страница редактирования виджета.
6. Измените настройки виджета.
7. Чтобы применить настройки, нажмите кнопку **Update** в нижнем правом углу.
8. Для сохранения изменений виджета нажмите кнопку **Save** в верхнем правом углу страницы.
9. В открывшемся окне при необходимости измените заголовок и описание виджета и нажмите кнопку **Save**.
10. Вернитесь на страницу **Мониторинг → Панели мониторинга** и убедитесь, что виджет обновился.
11. Для сохранения изменений панели мониторинга нажмите кнопку **Save** в верхнем правом углу страницы.
12. В открывшемся окне нажмите кнопку **Save**.

10.6.5.4. Удаление виджета

Для удаления виджета с панели мониторинга:

1. Перейдите на страницу **Мониторинг → Панели мониторинга**.
2. Нажмите на название нужной панели мониторинга в списке.
   - **Результат шага:** откроется выбранная панель мониторинга.
3. Нажмите кнопку **Edit** в верхнем правом углу страницы.
   - **Результат шага:** панель станет доступна для редактирования.
4. Выберите виджет, который нужно удалить, и нажмите на кнопку ⚙ в верхнем правом углу виджета.
5. В появившемся списке выберите пункт **More**.
6. В появившемся списке выберите **Delete from dashboard**.
   - **Результат шага:** виджет будет удален с панели мониторинга.
7. Для сохранения изменений нажмите кнопку **Save** в верхнем правом углу страницы.
8. В открывшемся окне нажмите кнопку **Save**.

10.6.6. Настройка пользовательских правил нормализации событий

Для настройки пользовательских правил нормализации событий:

1. Убедитесь, что конфигурационный файл `09-custom-filter.conf` присутствует в директории `/etc/logstash/pipeline`:

   ```
   ls -la /etc/logstash/pipeline
   ```

2. Заполните файл `09-custom-filter.conf` пользовательскими фильтрами и сохраните его. Подробнее о заполнении файла см. в разделе «Работа с файлами с расширением .conf».
3. Перезапустите сервис `udv-logstash`:

   ```
   systemctl restart udv-logstash.service
   ```

4. Перейдите на страницу **Администрирование → Основные настройки → Настройки мониторинга**.
5. Откройте вкладку **Index patterns**.

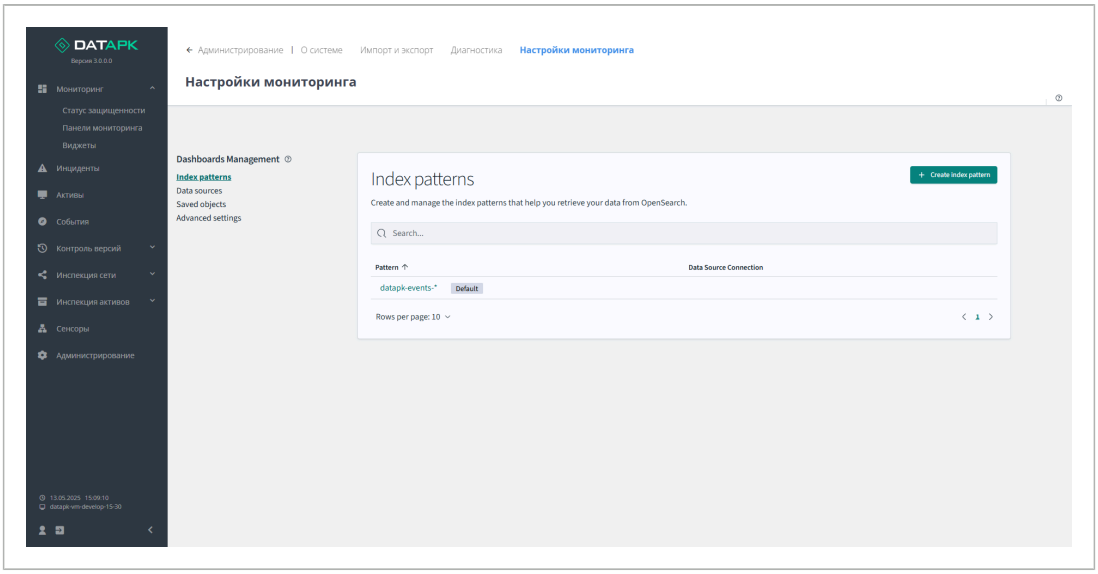


Рис. 90. Вкладка «Index patterns» для управления шаблонами индексов

6. Нажмите на интересующий набор индексов.
   - **Результат шага:** появится окно с перечислением всех полей.
7. Обновите список полей. Для этого в правом верхнем углу нажмите кнопку .
8. В появившемся окне **Refresh field list?** нажмите кнопку **Refresh**.
9. Убедитесь, что в список были добавлены дополнительные поля из пользовательского фильтра.

См. также

Нормализация событий

10.6.7. Настройка форматирования чисел и дат в разделе «Мониторинг»

В разделе **Мониторинг** доступна настройка формата чисел и дат. Для настройки формата:

1. Перейдите на страницу **Администрирование → Основные настройки → Настройки мониторинга**.

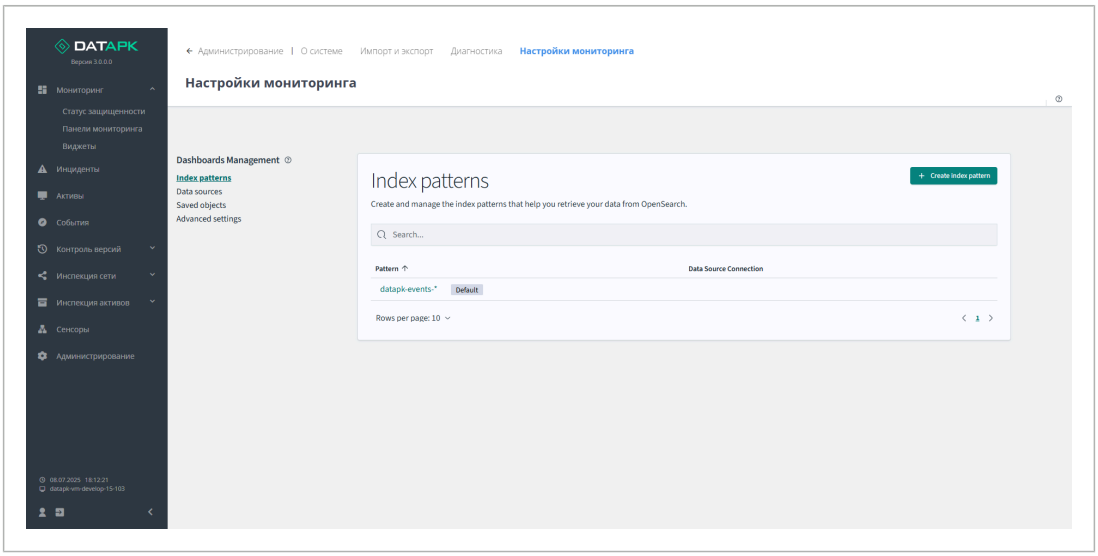


Рис. 91. Страница «Настройки мониторинга»

2. Перейдите на вкладку **Advanced Settings**.

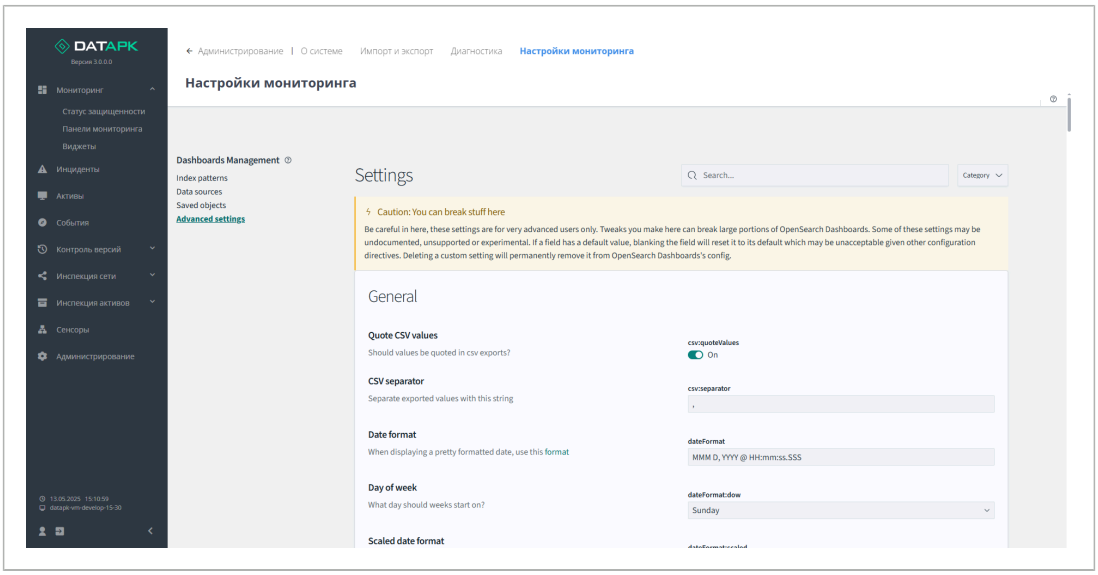


Рис. 92. Вкладка «Advanced Settings»

3. Найдите в списке следующие настройки:

   а. `format:number:defaultLocale` — для изменения локали формата чисел (разделять разряды запятой, точкой и тд.);

> Подсказка:
>
> Настройка локали автоматически меняет формат дат и начало недели. Производитель Комплекса рекомендует устанавливать локаль **ru**.

   б. `format:number:defaultPattern` — для изменения формата чисел;

в. `dateFormat` — для изменения формата даты;

г. `dateFormat:scaled` — для изменения расширенного формата даты;

д. `dateFormat:dow` — для изменения дня, с которого начинается неделя в календаре;

е. `dateFormat:tz` — для изменения часового пояса.

4. При необходимости измените значения настроек.

10.6.8. Экспорт и импорт объектов раздела «Мониторинг»

В этом разделе:

- Импорт сохраненных объектов в экспертном режиме просмотра событий
- Экспорт сохраненных объектов в экспертном режиме просмотра событий

Экспорт и импорт визуализаций, панелей мониторинга, поисковых запросов и настроек мониторинга осуществляется на вкладке **Saved Objects** страницы **Администрирование** → **Основные настройки** → **Настройки мониторинга**.

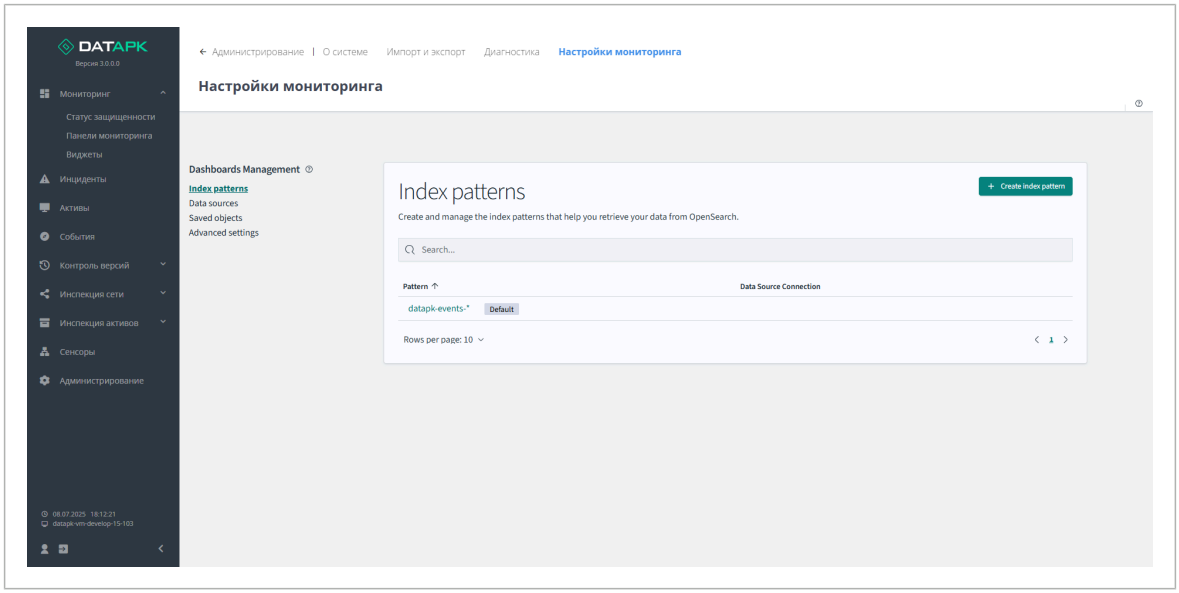


Рис. 93. Страница «Настройки мониторинга»

10.6.8.1. Импорт сохраненных объектов в экспертном режиме просмотра событий

Для импорта объектов раздела **Мониторинг** из файлов формата `*.ndjson`:

1. Создайте новый индекс событий или восстановите индексы из архива.

> Подсказка:
>
> Создание индексов описано в подразделе «Создание шаблона индекса». Восстановление индексов событий из архивов описано в подразделе «Восстановление данных из резервных копий».

2. Перейдите на страницу **Администрирование** → **Основные настройки** → **Настройки мониторинга**.
3. Выбрать вкладку **Saved Objects**.

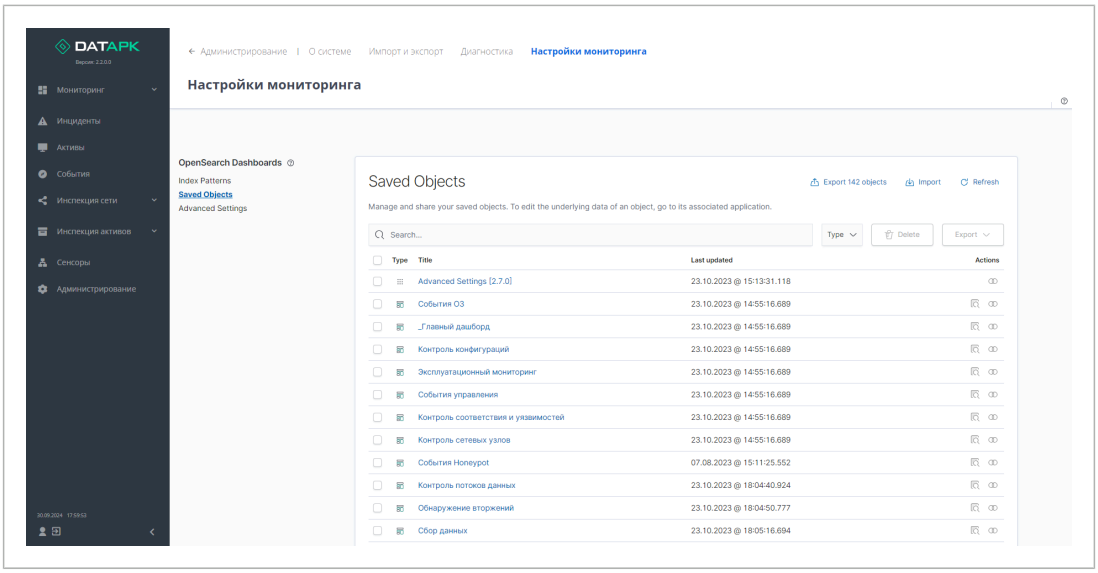


Рис. 94. Вкладка «Saved Objects»

4. Нажмите кнопку **Import**.
   - **Результат шага:** появится окно импорта сохраненных объектов.
5. В открывшемся окне:
   a. Оставьте включенным переключатель **Automatically overwrite conflicts**.
   б. Перетащите или выберите по нажатию на **Import** файл формата `*.ndjson` с объектами раздела **Мониторинг**.

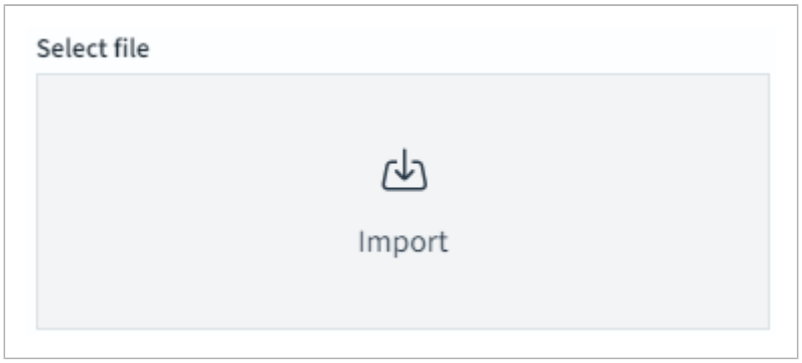


Рис. 95. Область выбора файла для импорта

6. Нажмите **Import**.

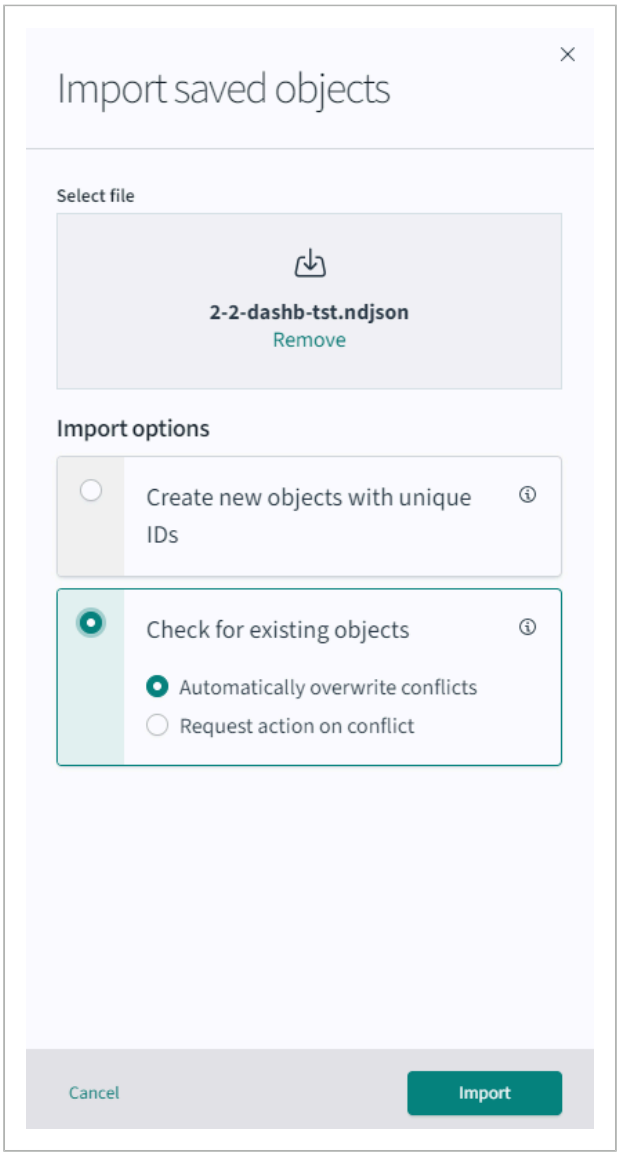


Рис. 96. Окно импорта сохраненных объектов

7. При отображении предупреждения `Index Pattern Conflicts. The following saved objects use index patterns that do not exist` выберите из выпадающего списка в столбце **New Index Pattern** наименование существующего шаблона индекса и нажмите кнопку **Confirm all changes**.

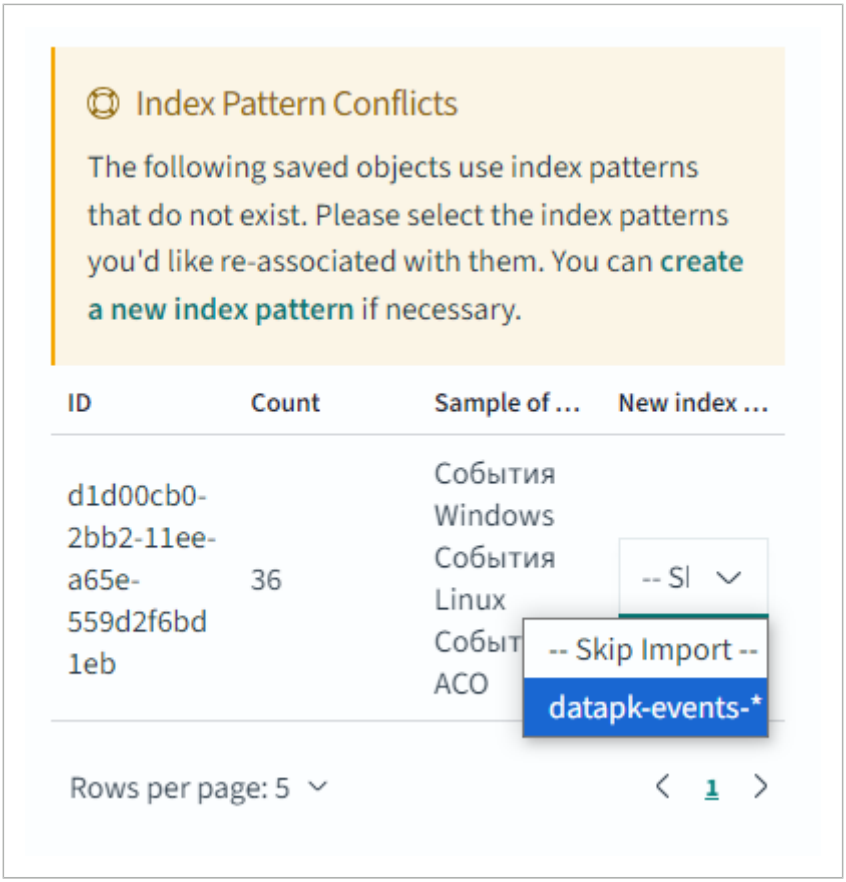


Рис. 97. Список шаблонов индекса в столбце «New Index Pattern»

8. В открывшемся окне с результатами импорта нажмите кнопку **Done**.
9. Убедитесь, что на вкладке **Saved Objects** страницы **Настройки мониторинга** отобразились импортированные объекты.

10.6.8.2. Экспорт сохраненных объектов в экспертном режиме просмотра событий

Для экспорта объектов раздела **Мониторинг** в файл формата `*.ndjson`:

1. Перейдите на страницу **Администрирование → Основные настройки → Настройки мониторинга**.
2. Выбрать вкладку **Saved Objects**.

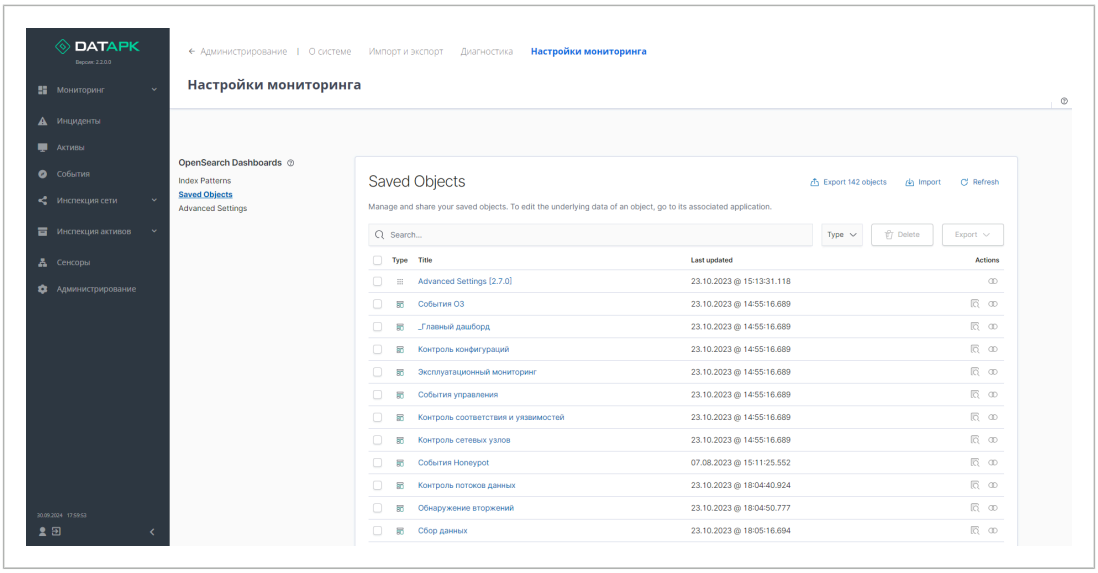


Рис. 98. Вкладка «Saved Objects»

3. Нажмите кнопку **Export [number] objects**, где `[number]` — количество экспортируемых объектов.
   - **Результат шага:** появится окно экспорта объектов.
4. В появившемся окне выберите типы объектов для экспорта.

> Внимание:
>
> Тип `index-pattern` (шаблон индекса) и включение связанных объектов выбирать не рекомендуется, так как при последующем импорте эти объекты окажутся дублированием уже существующих.

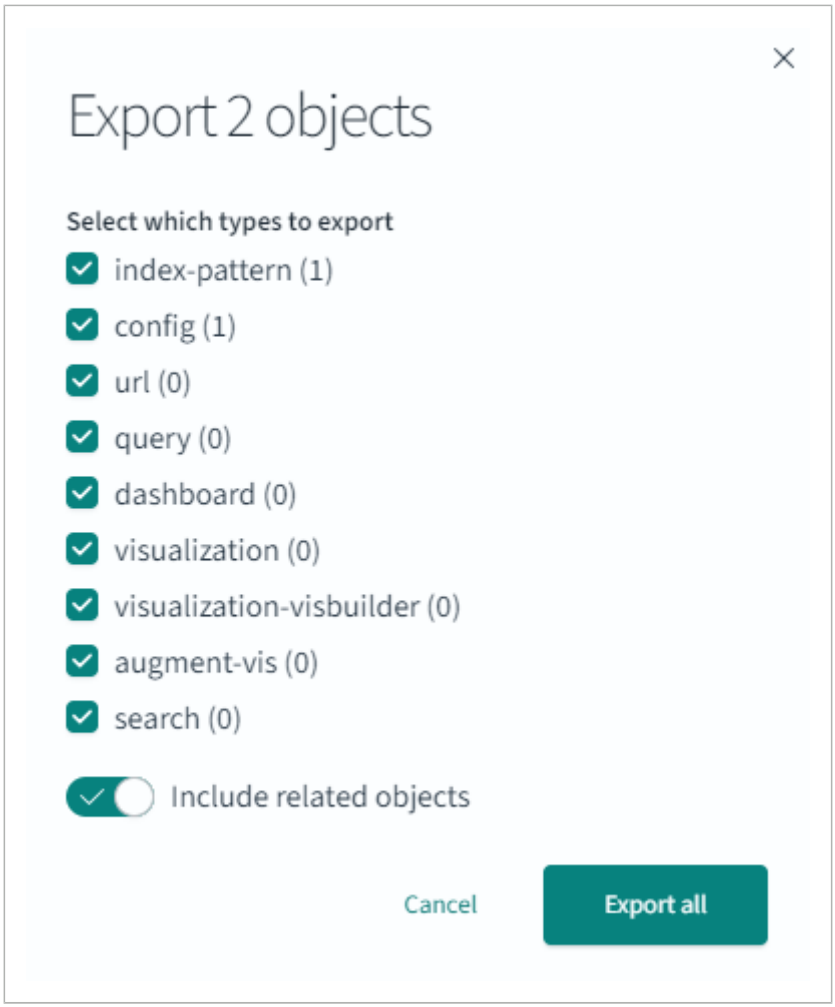


Рис. 99. Окно экспорта объектов

5. Нажмите **Export all**.
   - **Результат шага:** начнется формирование файлов для экспорта.
6. Дождитесь окончания сбора экспортируемых элементов.
   - **Результат шага:** файлы будут сформированы и автоматически скачаны в папку, установленную по умолчанию в вашем браузере.

11. Работа с инцидентами

В этом разделе:

1. **Поиск инцидентов**
2. **Анализ инцидентов**
3. **Изменение параметров инцидентов**
4. **Удаление инцидентов**
5. **Групповые операции над инцидентами**
6. **Настройка инцидентов**
7. **Выгрузка отчета по инцидентам**

Комплекс создает записи об инцидентах на основе событий. Инциденты создаются на основе правил корреляции событий (подробнее см. в секции «Правила корреляции событий»).

Инцидент информационной безопасности — событие или серия событий, которые привели, приводят или могут привести к нарушению бизнес-процессов и реализации угроз информационной безопасности.

В веб-интерфейсе Комплекса предусмотрена возможность просмотра списка инцидентов – событий от службы корреляции событий. Для просмотра списка инцидентов перейдите на страницу **Инциденты**.

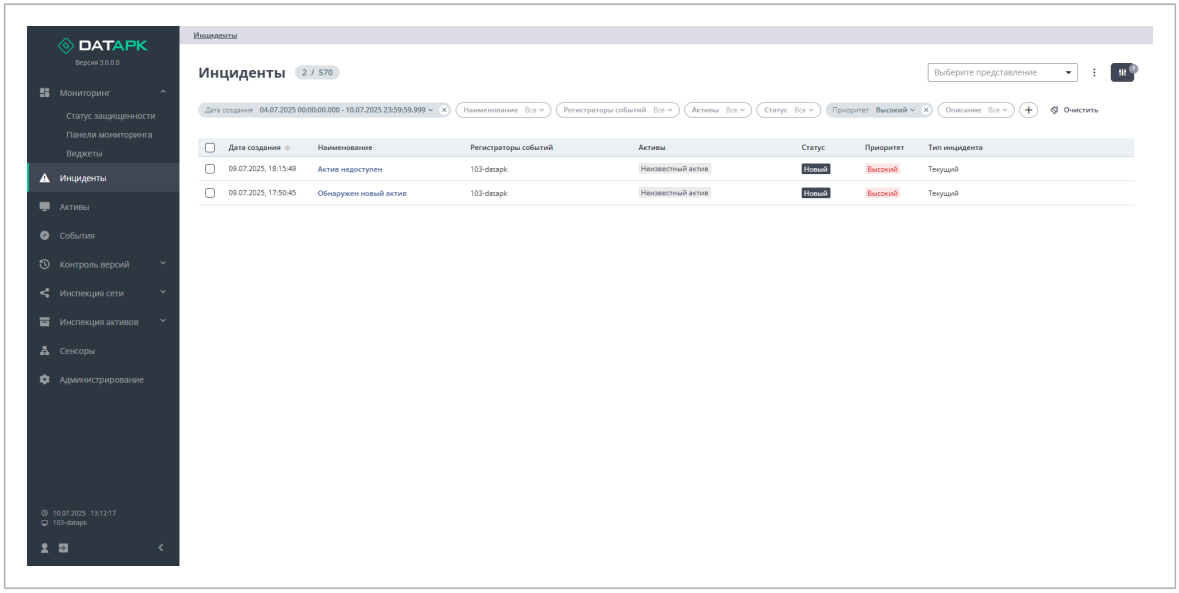


Рис. 100. Страница «Инциденты»

Правила корреляции событий

В Комплексе можно использовать один из двух видов правил корреляции:

- Встроенные в код (внутренние) правила корреляции, если не установлен модуль «Управление внешними событиями». Данные правила позволяют генерировать инциденты только на основе внутренних событий Комплекса. Список этих правил ограничен.
- Правила корреляции, используемые модулем «Управление внешними событиями». Данные правила предоставляют более гибкие возможности генерации инцидентов на основе внутренних событий Комплекса и внешних событий от активов.

Статусы инцидентов

По умолчанию инциденты получают статус Новый. Комплекс позволяет изменять приоритет полученного инцидента и статус его отслеживания для фиксации процесса реагирования на инцидент. Новые инциденты выделяются в общем списке.

Набор статусов поставляется с Комплексом, и его состав доступен к изменению пользователем.

В таблице на странице **Активы** в столбце **Инциденты** можно просматривать статистику по новым обнаруженным инцидентам с цветной индикацией для каждого актива. Подробнее см. раздел «Статусы активов».

11.1. Поиск инцидентов

Фильтры — это набор инструментов на странице **Инциденты** для фильтрации по заданным параметрам.

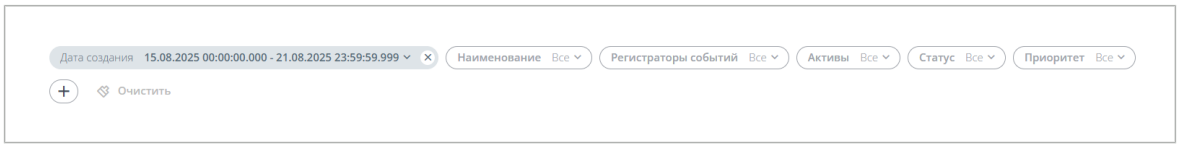


Рис. 101. Панель фильтров на странице «Инциденты»

11.1.1. Поиск инцидентов с помощью фильтров

В следующих фильтрах можно выбрать предустановленные значения из списка:

- **Регистраторы событий** — автоматически дополняемый список сенсоров и других регистраторов, подключенных к текущему Комплексу;
- **Активы** — автоматически дополняемый список активов, зарегистрированных в текущем Комплексе;

> Прим.:
>
> В списке приводятся только первые 20 доступных записей. Чтобы уточнить запрос, начните набирать нужное значение в поле над списком.

При нажатии на наименование актива можно просмотреть краткую информацию о нем в окне **Информация об активе** и перейти к карточке актива по ссылке **Подробнее**.

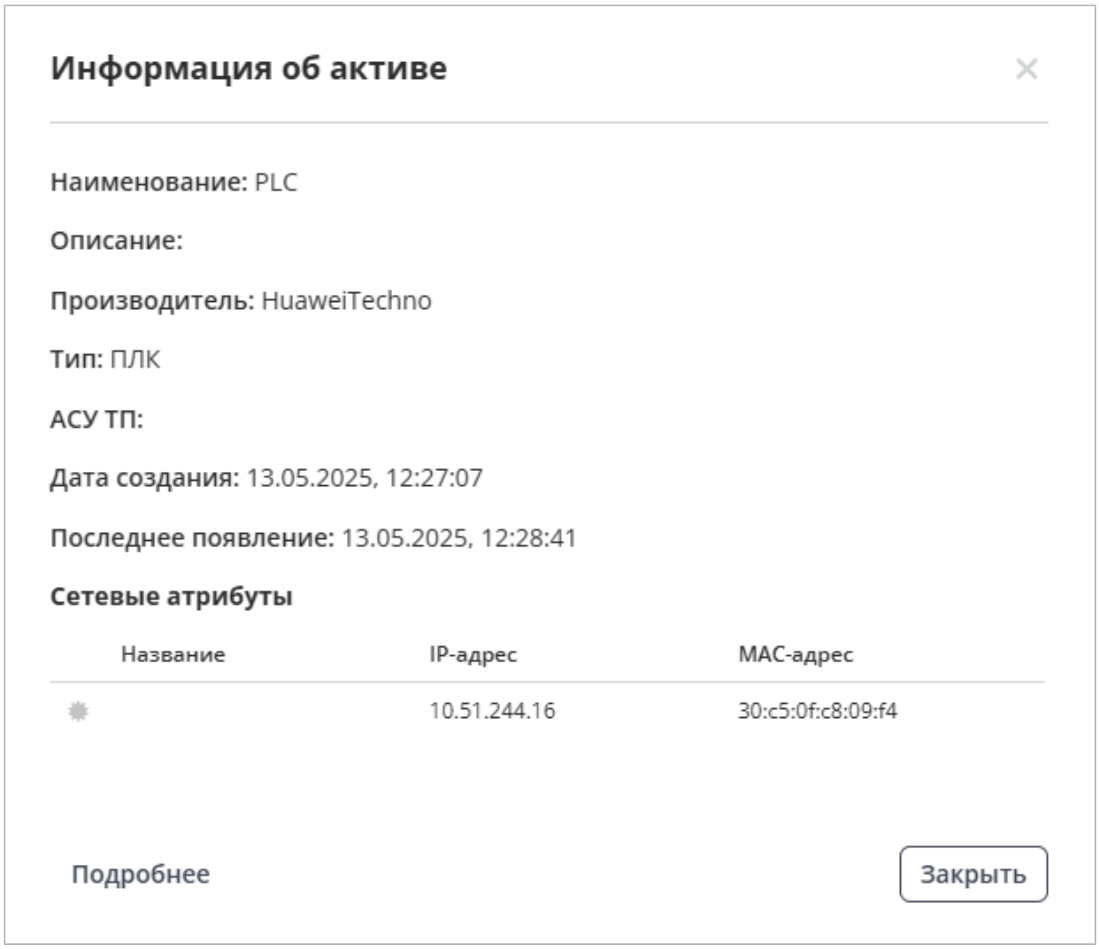


Рис. 102. Просмотр краткой информации об активе

- **Статус** — статус работы над инцидентом: `Новый`, `Закрыт`, `В работе. Оценен`, `В работе. Зарегистрирован`, `В работе. Выполнено реагирование`, `В работе. Проведен анализ`;
- **Приоритет** — `Критический`, `Высокий`, `Средний`, `Низкий`;
- **Тип инцидента** — `Ретроспективный`, `Текущий`;
- **Ретроспективная проверка** — автоматически дополняемый список с доступными в системе названиями проверок;
- **Подтвержден** — признак того, что специалист, расследующий инцидент, вручную подтвердил наличие инцидента ИБ: `Подтвержден`, `Не подтвержден`.

Чтобы воспользоваться другими фильтрами (кроме **Дата создания** и **Дата обновления**), введите нужное значение в текстовое поле и нажмите ✓.

Инциденты можно сортировать по полю **Дата создания**.

11.1.2. Поиск инцидентов с помощью фильтров «Дата создания» и «Дата обновления»

По умолчанию на странице отображаются инциденты за последние семь дней.

Для поиска инцидентов с помощью фильтра **Дата создания**:

1. Выберите фильтр **Дата создания**.
   - **Результат шага:** откроется календарь выбора временного периода, в котором были зарегистрированы инциденты.

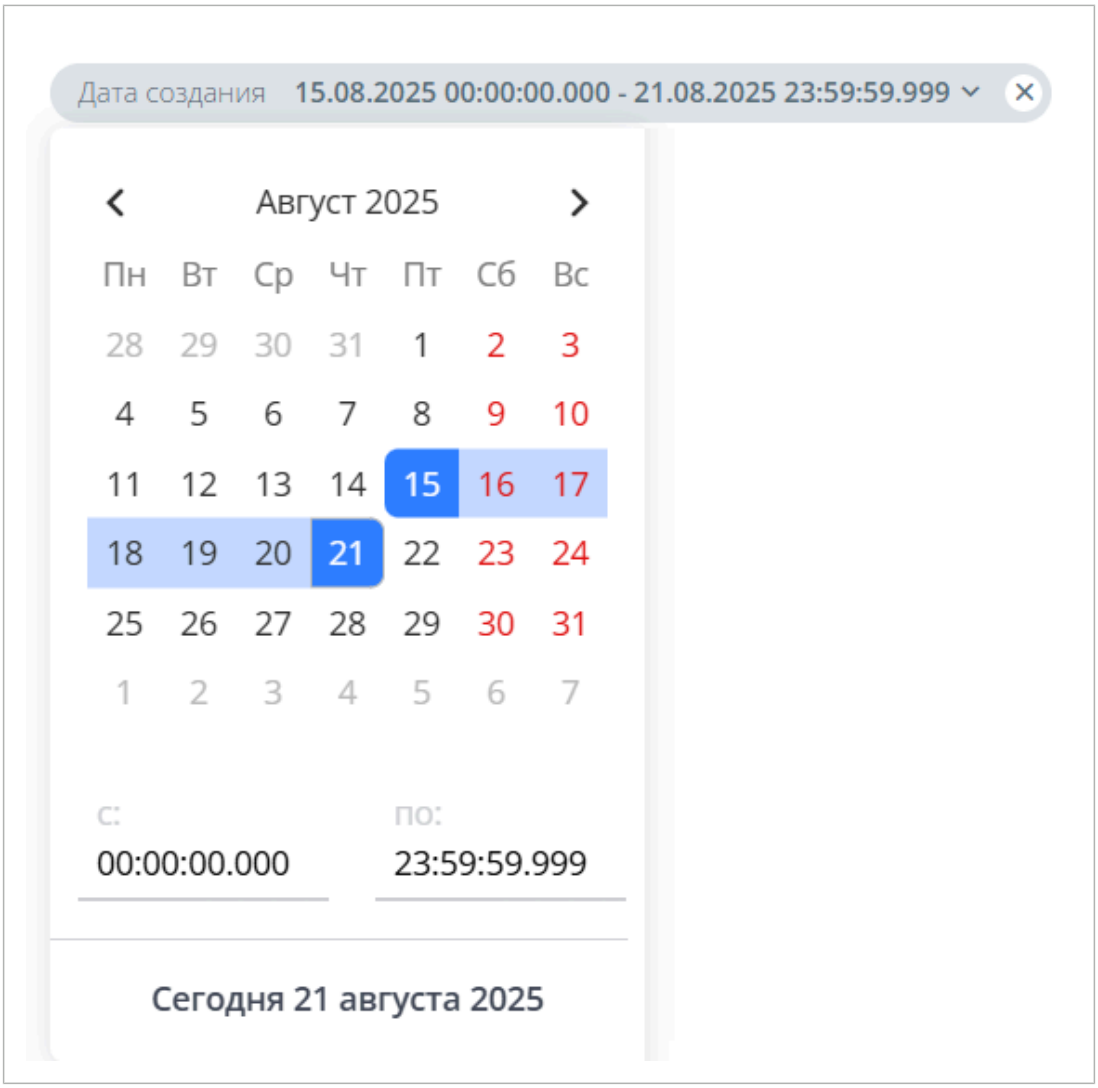


Рис. 103. Календарь выбора временного периода регистрации инцидентов

2. Выберите начальную дату.

> Подсказка:
>
> - Для выбора текущего дня в качестве всего диапазона нажмите `Сегодня [текущая дата]` в нижней части фильтра.
> - Для быстрой навигации по месяцам и годам нажмите на название месяца и года в верхней части фильтра: первое нажатие отображает список всех месяцев, второе нажатие отображает список из 12 лет, ближайших к текущему году.

- **Результат шага:** автоматически отобразятся события за выбранную дату.

3. При необходимости выберите конечную дату.

- **Результат шага:** в календаре будут выделены все даты между выбранными начальной и конечной. На странице автоматически отобразятся события за установленный временной период.

4. При необходимости введите время в поля **с:** и **по:** (время вводится в формате `ЧЧ:ММ:СС.СССС`).

> Внимание:
>
> Если выбраны разные начальная и конечная даты, поля **с:** и **по:** будут работать следующим образом:
> - в поле **с:** необходимо указать время для начальной даты;
> - в поле **по:** необходимо указать время для конечной даты.

- **Результат шага:** на странице автоматически отобразятся события за установленный временной период.

5. Для очистки результатов поиска по выбранному временному периоду нажмите кнопку справа от фильтра **Дата создания**.
   - **Результат шага:** на странице автоматически отобразятся инциденты за последнюю неделю.
6. Для поиска инцидентов с помощью фильтра **Дата обновления** используйте изложенные выше инструкции аналогичным образом. Список инцидентов будет дополнительно фильтроваться по дате и времени, когда в инциденты последний раз вносились изменения.

11.2. Анализ инцидентов

Подробности о выявленных инцидентах можно просматривать на странице **Инциденты**. Специалист, расследующий ИБ-инцидент, может воспользоваться следующими возможностями:

1. Просмотр детальной информации об инциденте. Для просмотра детальной информации о конкретном инциденте:
   a. Нажмите на наименование нужного инцидента.
   - **Результат шага:** откроется карточка инцидента.

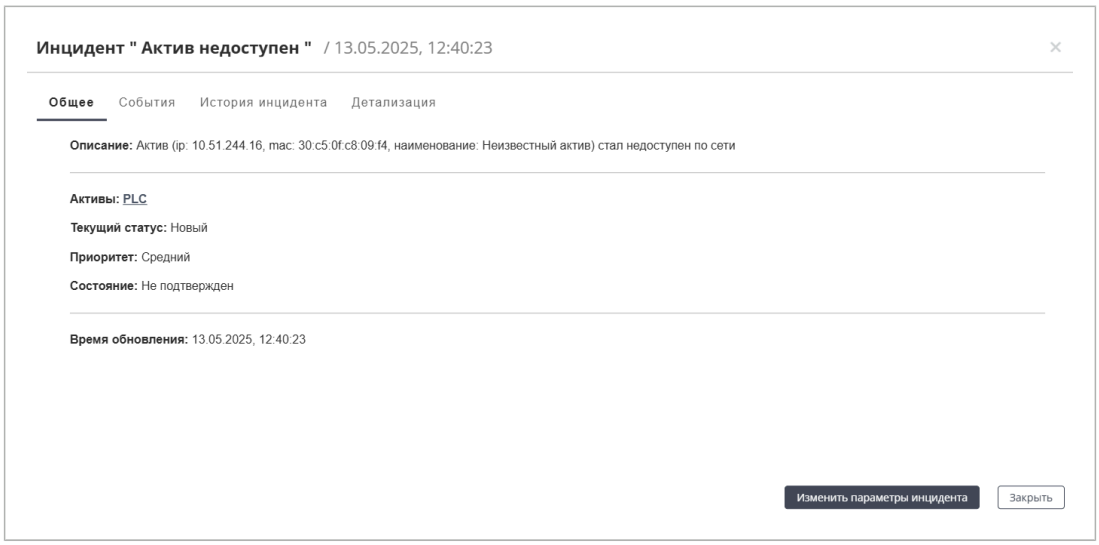


Рис. 104. Детальная информация об инциденте

2. Просмотр событий. Для просмотра списка событий, относящихся к инциденту:
   a. Откройте окно просмотра детальной информации об инциденте (см. п. 1.а).
   б. Перейдите на вкладку **События**.
   - **Результат шага:** откроется список событий, относящихся к инциденту.

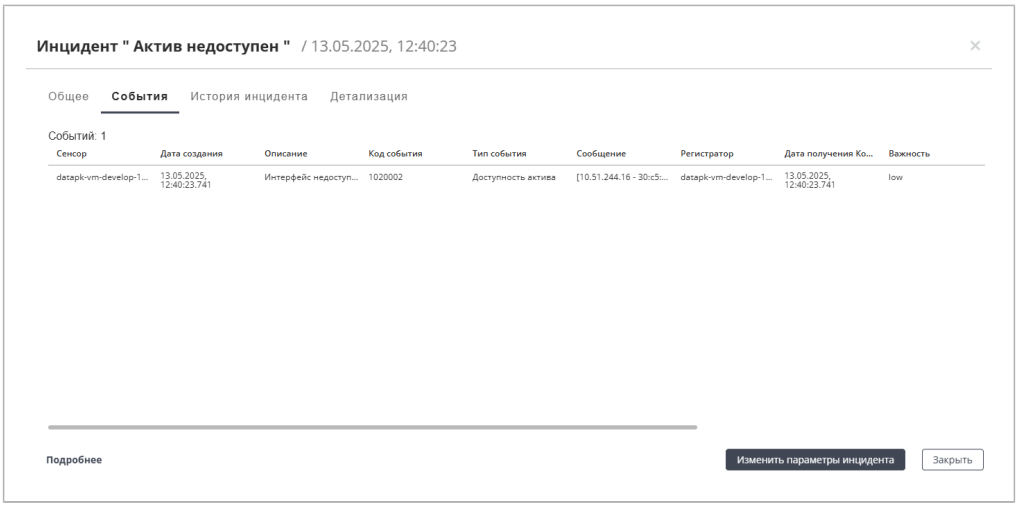


Рис. 105. События инцидента

в. Нажмите **Подробнее**.

- **Результат шага:** откроется страница **События → Экспертный режим**, содержащая список событий, относящихся к выбранному инциденту.

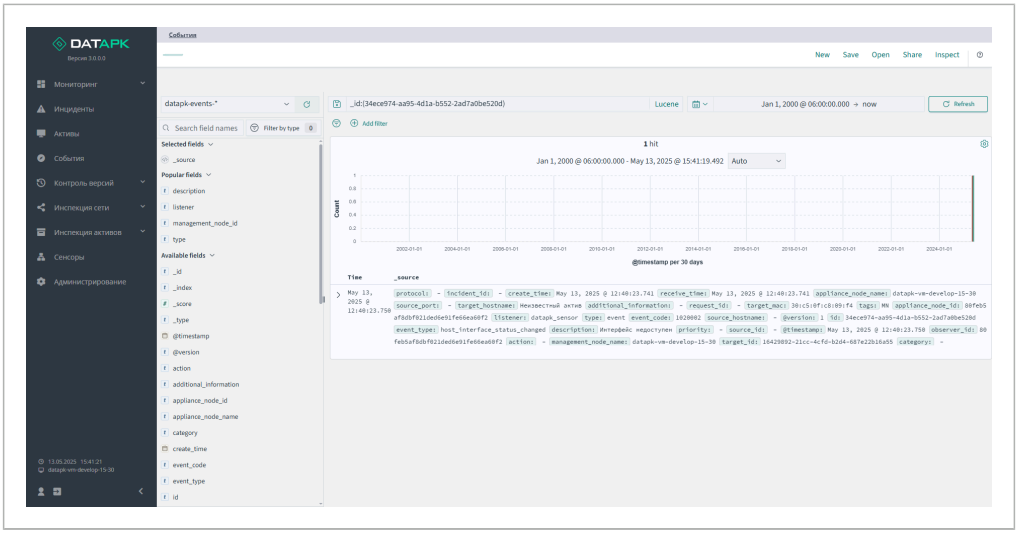


Рис. 106. Экспертный режим страницы «События», содержащей список событий инцидента

Прим.:

Если в системе не установлен модуль «Управление внешними событиями», будет открываться страница События с упрощенным режимом поиска событий.

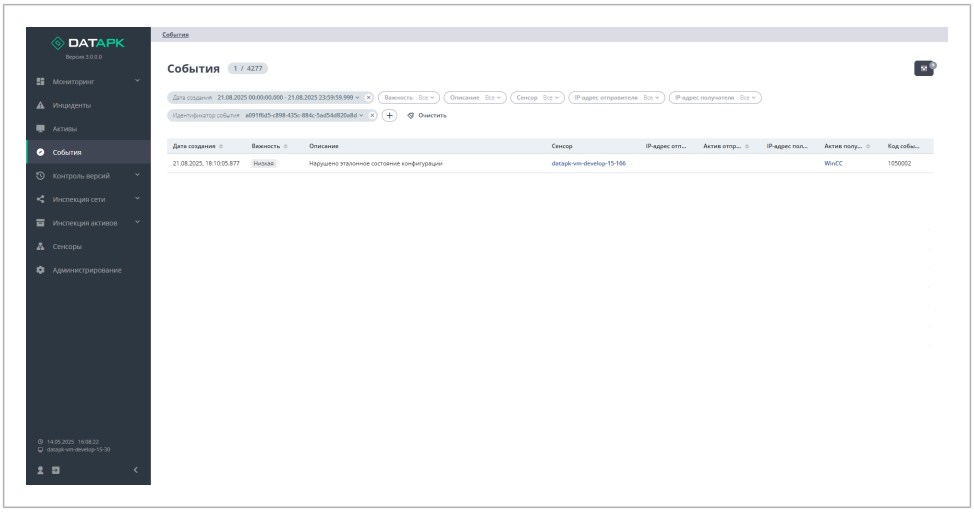


Рис. 107. Страница «События» с упрощенным поиском событий, содержащая список событий инцидента

3. Просмотр истории изменений инцидента. Для просмотра истории:
    a. Откройте окно просмотра детальной информации об инциденте (см. п. 1.а).
    б. Перейдите на вкладку **История инцидента**.

- **Результат шага:** откроется список изменений инцидента.

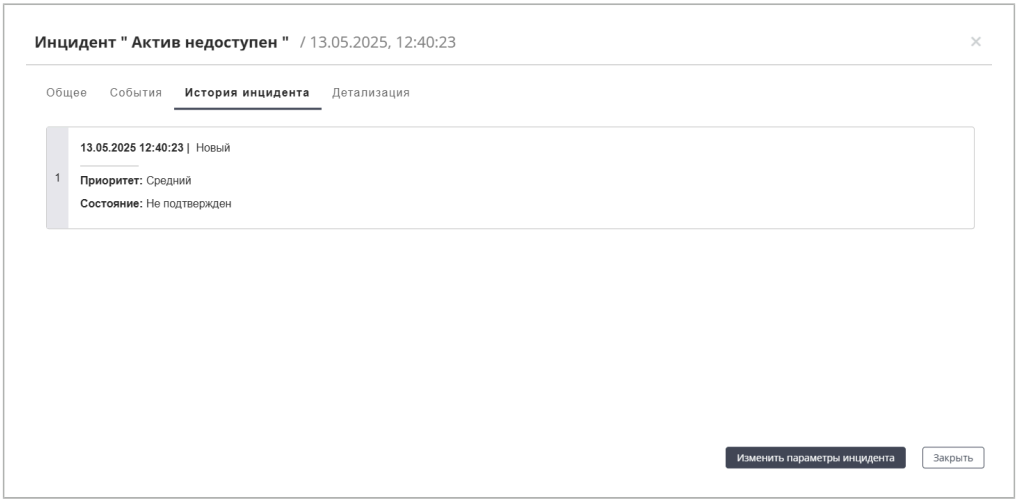


Рис. 108. История инцидента

4. Просмотр события, созданного службой корреляции. Для просмотра события корреляции:
   a. Откройте окно просмотра детальной информации об инциденте (см. п. 1.а).
   б. перейдите на вкладку **Детализация**.

- **Результат шага:** откроются подробности события корреляции.

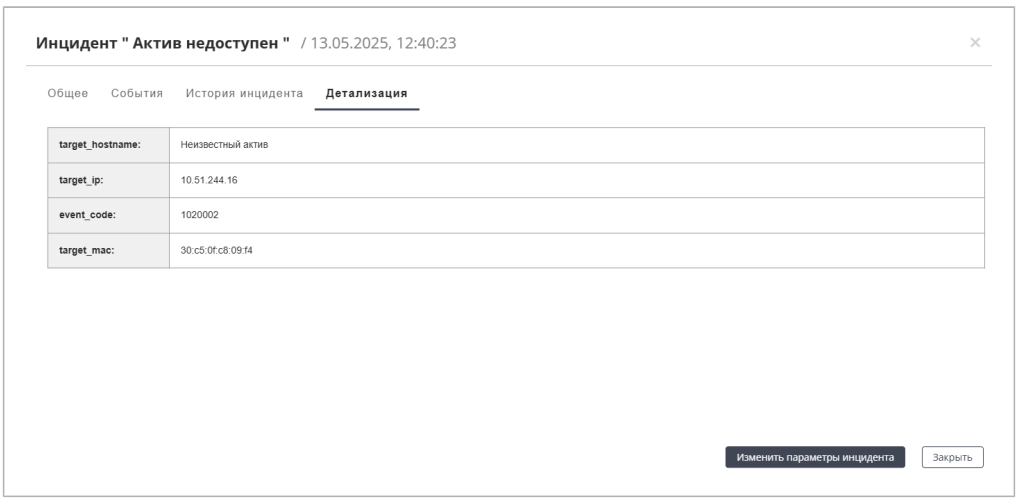


Рис. 109. Подробности события корреляции

11.3. Изменение параметров инцидентов

В веб-интерфейсе Комплекса можно:

- изменять приоритет и статус отдельных инцидентов с помощью кнопок управления в общей таблице или формы в карточке;
- изменять приоритет и статус нескольких инцидентов одновременно в общей таблице;
- подтверждать инциденты, не изменяя их статус или приоритет.

11.3.1. Изменение параметров инцидента в общей таблице инцидентов

Для редактирования инцидента можно воспользоваться элементами управления в таблице инцидентов. Таким способом можно изменить статус и приоритет инцидента.

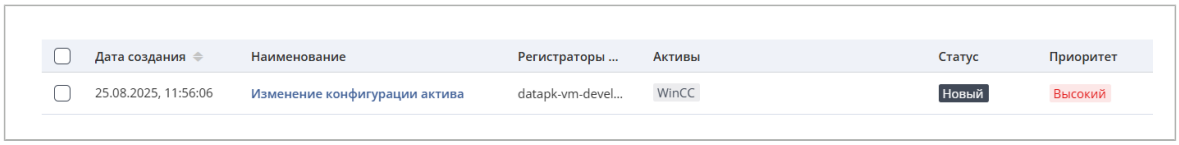


Рис. 110. Кнопки управления инцидентом

1. Для изменения статуса инцидента:
    a. Перейдите на страницу **Инциденты**.
    б. В строке с нужным инцидентом нажмите на значение столбца **Статус**.
    - **Результат шага:** откроется окно **Изменение статуса инцидента**.

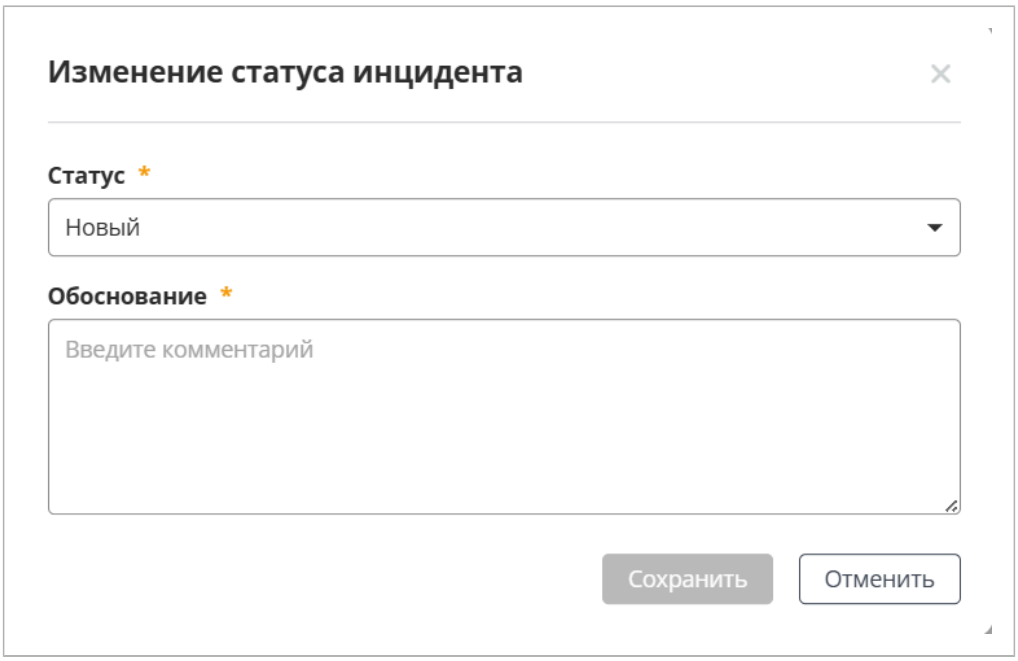


Рис. 111. Окно «Изменение статуса инцидента»

    в. Заполните следующие обязательные поля:
        - **Статус**;
        - **Обоснование**.
    г. Нажмите **Сохранить**.
    - **Результат шага:** будет зафиксировано событие об изменении инцидента. На странице **Инциденты** появится уведомление об обновлении инцидента с датой и временем обновления. Изменивший параметры пользователь будет назначен ответственным за обновленный инцидент.
2. Для изменения приоритета инцидента:
    a. Перейдите на страницу **Инциденты**.
    б. В строке с нужным инцидентом нажмите на значение столбца **Приоритет**.
    - **Результат шага:** откроется окно **Изменение приоритета инцидента**.

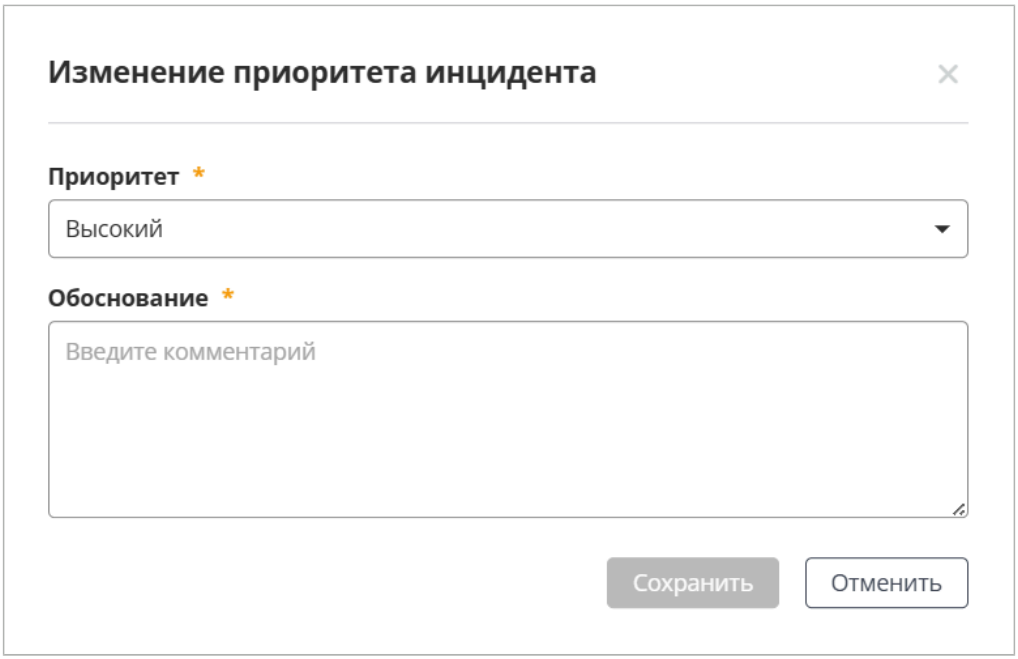


Рис. 112. Окно «Изменение приоритета инцидента»

в. Заполните следующие обязательные поля:

- **Приоритет**;
- **Обоснование**.

г. Нажмите **Сохранить**.

- **Результат шага:** будет зафиксировано событие об изменении инцидента. На странице **Инциденты** появится уведомление об обновлении инцидента с датой и временем обновления. Изменивший параметры пользователь будет назначен ответственным за обновленный инцидент.

11.3.2. Изменение параметров инцидента в карточке инцидента

Для редактирования инцидента:

1. Перейдите на страницу **Инциденты**.
2. Нажмите на название инцидента в таблице инцидентов.
   - **Результат шага:** откроется окно детальной информации об инциденте.
3. Нажмите **Изменить параметры инцидента**.
   - **Результат шага:** откроется окно **Изменение параметров инцидента**.
4. Заполните следующие обязательные поля:

   а. **Статус** — этап работы над инцидентом (`Новый`, `Закрыт`, `В работе. Оценен`, `В работе. Зарегистрирован`, `В работе. Выполнено реагирование` или `В работе. Проведен анализ`);

   б. **Приоритет** — степень важности и срочности работы над инцидентом (`Критический`, `Высокий`, `Средний` или `Низкий`);

   в. **Обоснование** — пояснение произведенных операций над инцидентом.

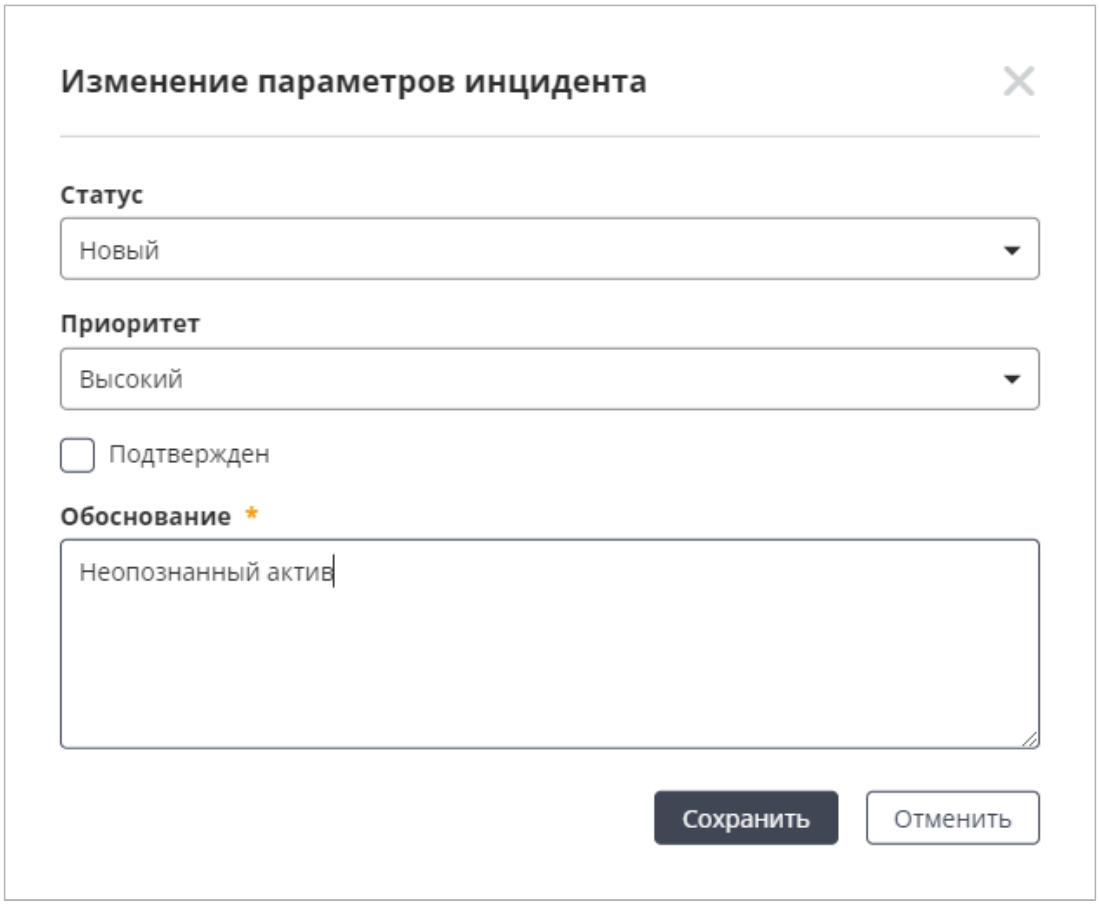


Рис. 113. Окно «Изменение параметров инцидента»

5. При необходимости установите чекбокс **Подтвержден**.
6. Нажмите **Сохранить**.

   ▸ **Результат шага:** будет зафиксировано событие с данными о пользователе и заполненных полях. На странице **Инциденты** появится уведомление об обновлении инцидента с датой и временем обновления. Изменивший параметры пользователь будет назначен ответственным за обновленный инцидент.

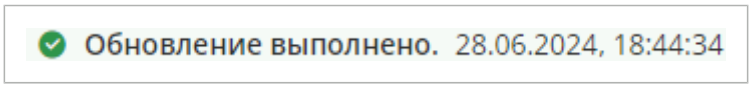


Рис. 114. Уведомление об обновлении инцидента

11.3.3. Изменение параметров нескольких инцидентов

При редактировании нескольких инцидентов приоритет и статус инцидентов можно устанавливать отдельно.

1. Для изменения приоритета нескольких инцидентов:
   a. Перейдите на страницу **Инциденты**.
   б. Установите чекбокс возле необходимых инцидентов.
   в. В открывшемся внизу меню нажмите **Приоритет**.

   ▸ **Результат шага:** откроется окно **Изменение приоритета инцидентов**.

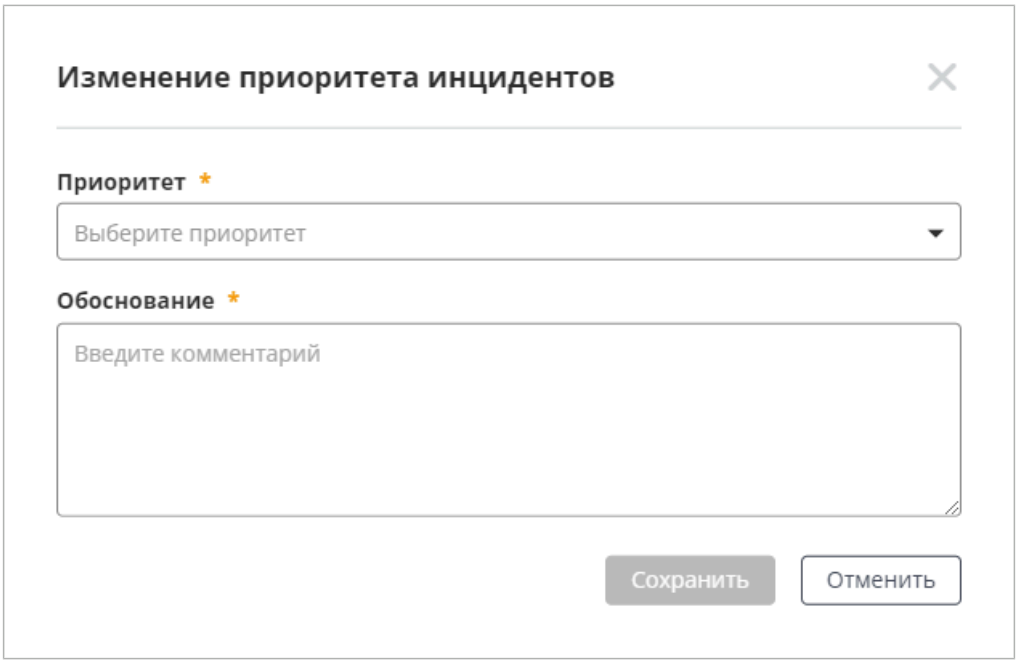


Рис. 115. Окно «Изменение приоритета инцидентов»

г. Заполните следующие обязательные поля:

- **Приоритет**;
- **Обоснование**.

д. Нажмите **Сохранить**.

- **Результат шага:** будет зафиксировано событие об изменении группы инцидентов. На странице **Инциденты** появится уведомление об обновлении инцидентов с датой и временем обновления. Изменивший параметры пользователь будет назначен ответственным за обновленные инциденты.

2. Для изменения статуса нескольких инцидентов:

а. Перейдите на страницу **Инциденты**.

б. Установите чекбокс возле необходимых инцидентов.

в. В открывшемся внизу меню нажмите **Статус**.

- **Результат шага:** откроется окно **Изменение статуса инцидентов**.

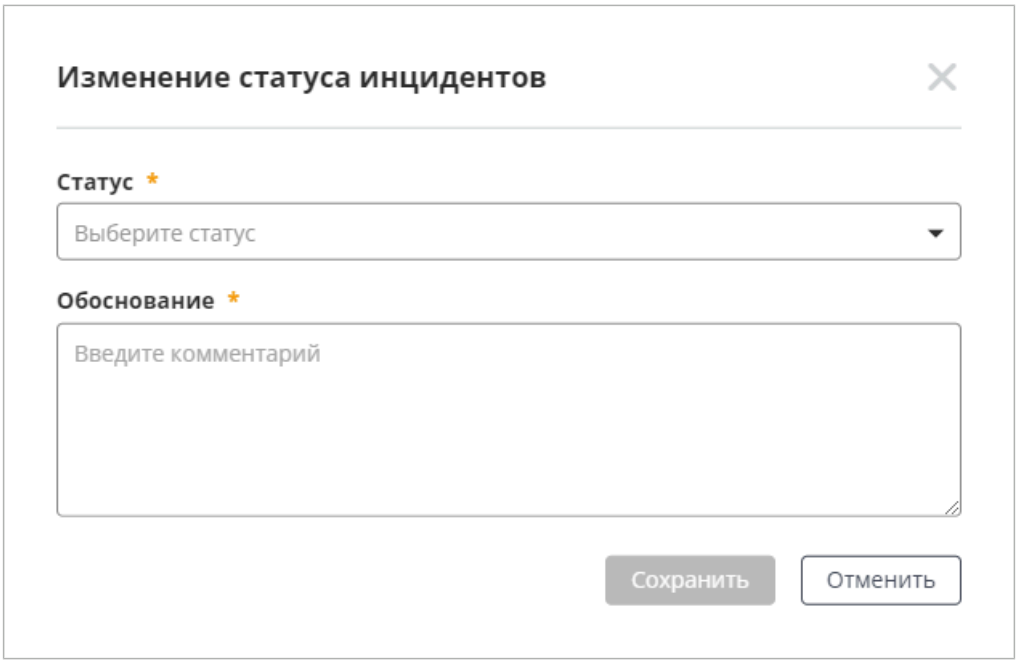


Рис. 116. Окно «Изменение статуса инцидентов»

г. Заполните следующие обязательные поля:

- **Статус**;
- **Обоснование**.

д. Нажмите **Сохранить**.

Результат шага: будет зафиксировано событие об изменении группы инцидентов. На странице **Инциденты** появится уведомление об обновлении инцидентов с датой и временем обновления. Изменивший параметры пользователь будет назначен ответственным за обновленные инциденты.

11.3.4. Подтверждение инцидента

Для подтверждения инцидента без изменения статуса и обоснования:

1. Перейдите на страницу **Инциденты**.
2. Установите чекбокс **Подтвержден** в соответствующей колонке таблицы инцидентов.

> Подсказка:
>
> При отсутствии чекбокса **Подтвержден** отрегулируйте отображение столбцов в правом верхнем углу страницы.

11.4. Удаление инцидентов

Если инцидентов слишком много или они уже не нужны, их можно удалить. При этом удаленные инциденты останутся в событиях.

11.4.1. Удаление инцидента

Для удаления одного инцидента:

1. Перейдите на страницу **Инциденты**.
2. Нажмите кнопку справа от выбранного инцидента.
   - **Результат шага:** появится окно подтверждения удаления инцидента.
3. В окне подтверждения введите обоснование удаления и нажмите **Подтвердить**.

> Внимание:
>
> Текст обоснования должен содержать минимум три символа. Без обоснования удалить инцидент невозможно.

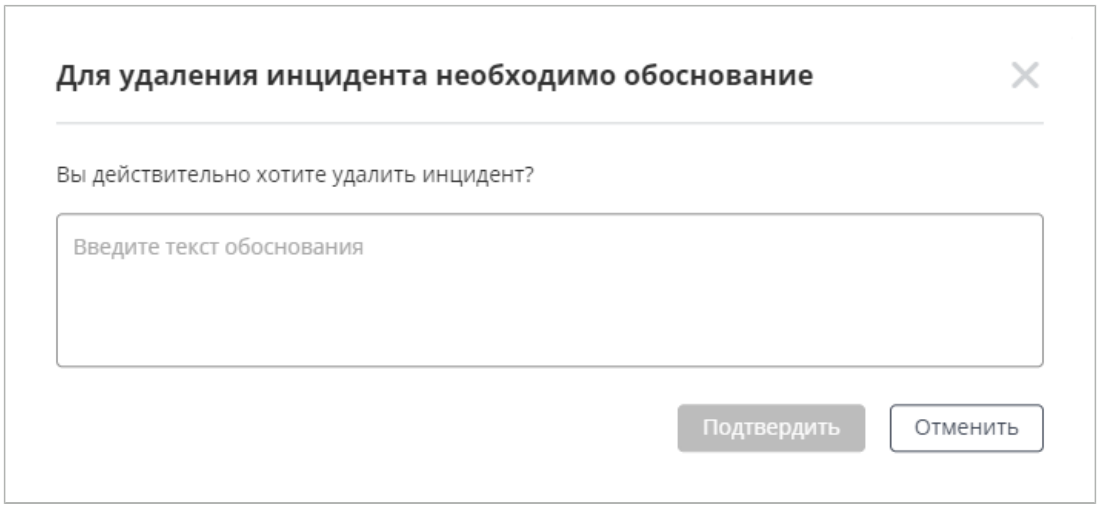


Рис. 117. Окно обоснования удаления инцидента

- **Результат шага:** Инцидент будет удален. Будет зафиксировано соответствующее событие с обоснованием удаления. На странице **Инциденты** появится уведомление об удалении инцидента с датой и временем удаления.

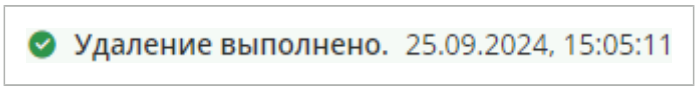


Рис. 118. Уведомление об удалении инцидента

11.4.2. Удаление нескольких инцидентов

Для удаления нескольких инцидентов:

1. Перейдите на страницу **Инциденты**.
2. Установите чекбоксы возле инцидентов, которые необходимо удалить.
3. В открывшемся внизу меню нажмите → (**Удалить**).

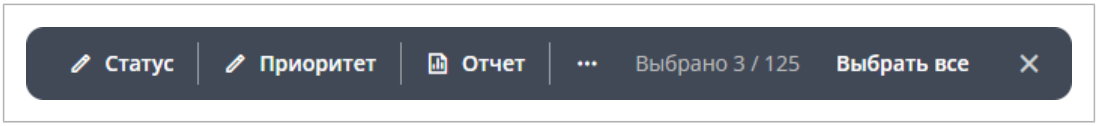


Рис. 119. Меню групповых операций над инцидентами

4. Во всплывающем окне введите обоснование удаления и нажмите **Подтвердить**.

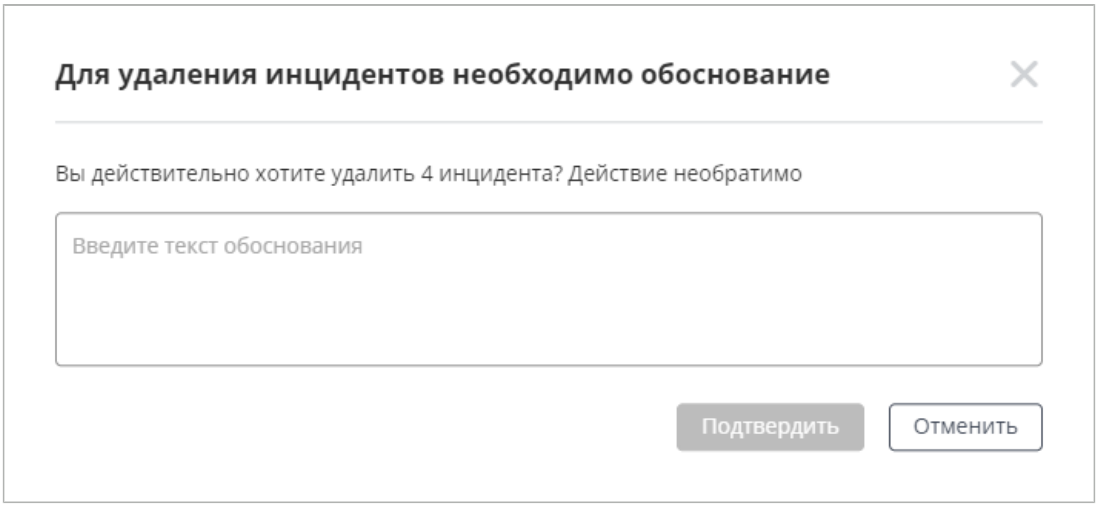


Рис. 120. Окно обоснования удаления нескольких инцидентов

▸ **Результат шага:** Инциденты будут удалены. Будет зафиксировано соответствующее событие с обоснованием удаления. На странице **Инциденты** появится уведомление об удалении инцидентов с датой и временем удаления.

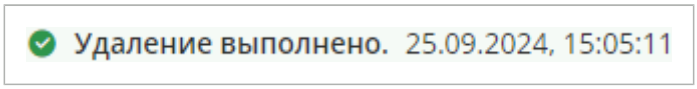


Рис. 121. Уведомление об удалении инцидентов

11.5. Групповые операции над инцидентами

Комплекс позволяет выполнять следующие групповые операции над инцидентами:

- подтверждать инциденты или отменять подтверждение, устанавливать инцидентам статус и приоритет (подробнее см. раздел «Изменение параметров инцидентов»);
- создавать отчет (подробнее см. раздел «Выгрузка отчетов»);
- удалять инциденты (подробнее см. раздел «Удаление инцидентов»).

Групповые действия применяются ко всем инцидентам, выбранным на странице **Инциденты**. При этом предыдущее значение статуса или приоритета заменяется, а в истории фиксируется действие и обоснование. Для удаленных инцидентов обоснование будет сохранено в событиях.

Групповые операции отображаются внизу страницы после выбора хотя бы одного инцидента.

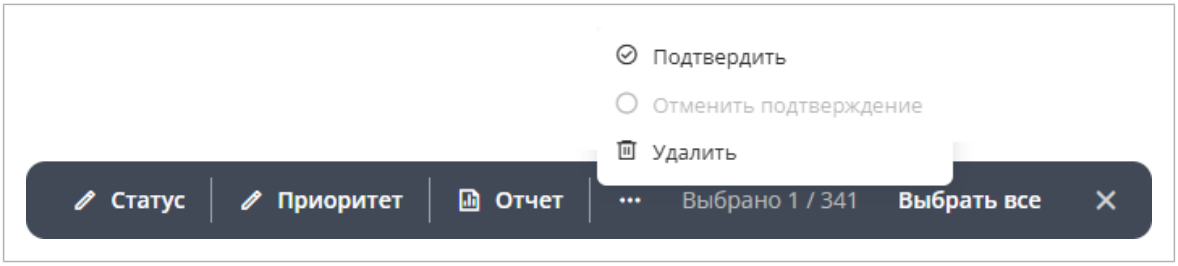


Рис. 122. Меню групповых операций над инцидентами

При работе с групповыми операциями возможны следующие виды статусов:

1. `В очереди на выполнение` — операция находится в очереди. Если нет других продолжительных операций, статус исчезает быстрее, чем пользователь успевает его заметить. В этом статусе кнопка имеет оранжевый цвет. При нажатии на кнопку, которой была запущена групповая операция, выполнение операции будет отменено, но останется соответствующая запись в журнале событий.
2. `Выполняется` — операция по изменению или удалению инцидента выполняется в данный момент. При этом есть возможность остановить операцию, нажав на кнопку, которой было запущено выполнение операции.

> Подсказка:
>
> Подробнее о статусах см. в разделе «Цветовая индикация и виды уведомлений».

11.6. Настройка инцидентов

В этом разделе:

- Экспорт и импорт политики корреляции
- Экспорт и импорт статусов инцидентов
- Управление службой корреляции событий
- Управление схемой корреляции
- Управление правилами корреляции событий
- Анализ событий для генерации инцидентов
- Настройка оповещений при появлении инцидентов
- Управление статусами инцидентов
- Управление внутренними правилами корреляции событий

Для того, чтобы служба корреляции могла генерировать инциденты, необходимо настроить получение событий, загрузить политику корреляции и включить использование правил корреляции в текущем или ретроспективном анализе. Дополнительно можно настроить собственные статусы инцидентов.

Корреляция — способность системы выявлять закономерности в событиях и формировать инциденты на их основе.

В Комплексе можно использовать один из двух видов правил корреляции:

- Встроенные в код (внутренние) правила корреляции, если не установлен модуль «Управление внешними событиями». Данные правила позволяют генерировать инциденты только на основе внутренних событий Комплекса. Список этих правил ограничен.
- Правила корреляции, используемые модулем «Управление внешними событиями». Данные правила предоставляют более гибкие возможности генерации инцидентов на основе внутренних событий Комплекса и внешних событий от активов.

Служба корреляции в модуле «Управление внешними событиями» работает на основе инструмента Esper. Для выполнения корреляции создаются правила обработки событий на языке EPL (Event Processing Language).

Механизм корреляции в модуле «Управление внешними событиями» можно применять как для событий, поступающих в данный момент (текущий анализ), так и событий, полученных ранее (ретроспективный анализ).

Текущий анализ — режим работы службы корреляции событий, при котором выполняется анализ событий, поступающих на Комплекс в реальном времени.

Ретроспективный анализ — режим работы службы корреляции событий, который позволяет проанализировать уже имеющуюся базу событий.

Для анализа используется политика корреляции. Политика корреляции событий — справочник, который содержит схему и правила корреляции.

Схема корреляции событий — набор сущностей, используемый для обработки событий. Схема определяет то, с чем может работать служба корреляции: например, окна данных, таблицы, контексты, переменные.

Пример

Примеры элементов схемы корреляции событий:

- Элемент схемы представления событий аутентификации пользователей Комплекса:

```
@public @buseventtype create json schema appliance_authentication as (action string,
 additional_information string, observer_id string, category string, create_time
 string, description string, event_code string, observer_id string, observer_name
 string, id string, observer_ip string, protocol string, receive_time string, severity
 string, listener string, source_id string, source_ip string, source_hostname string,
 source_mac string, source_port string, tags string, target_id string, target_ip
 string, target_hostname string, target_port string, target_mac string, timestamp
 string, user string)
```

- Элемент схемы представления событий о конфигурациях активов:

```
@public @buseventtype create json schema host_config as (action string,
 additional_information string, observer_id string, category string, create_time
 string, description string, event_code string, observer_id string, observer_name
 string, id string, observer_ip string, protocol string, receive_time string, severity
 string, listener string, source_id string, source_ip string, source_hostname string,
 source_mac string, source_port string, tags string, target_id string, target_ip
 string, target_hostname string, target_port string, target_mac string, timestamp
 string, user string)
```

- Элемент схемы представления событий инфообмена Комплекса:

```
@public @buseventtype create json schema info_exchange as (action string,
 additional_information string, observer_id string, category string, create_time
```

```
string, description string, event_code string, observer_id string, observer_name
string, id string, observer_ip string, protocol string, receive_time string, severity
string, listener string, source_id string, source_ip string, source_hostname string,
source_mac string, source_port string, tags string, target_id string, target_ip
string, target_hostname string, target_port string, target_mac string, timestamp
string, user string)
```

Правила корреляции событий — набор команд, которые оперируют нормализованными событиями из разных источников и выдают на основе их анализа инциденты. В результате обнаружения инцидентов могут быть сформированы уведомления, которые отправляются инженеру информационной безопасности или другим сотрудникам.

Пример

Примеры правил для корреляции событий при установленном модуле «Управление внешними событиями»:

- подбор пароля в ОС Windows:

```
select eventID, observer_name, prevwindow(UID) from WindowsEvent(eventID=\"4625\" or
 eventID=\"529\").win:time(180 sec) group by observer_name having count(eventID) = 3
```

- удаленная чистка журнала безопасности в ОС Windows:

```
select a.hostnameSrc, a.IPsrc, a.MACsrc, lastEvent.eventID,
 lastEvent.observer_name, a.UID, lastEvent.UID from
 pattern [every a=DataFlowEvent(protocol=\"rdp\")
 -> every lastEvent=WindowsEvent((eventID=\"1102\" or
 eventID=\"517\") and a.hostnameDst=observer_name)].win:time(1 hour)
```

- удаленный вход в систему Windows с помощью службы RDP:

```
select a.hostnameSrc, a.IPsrc, a.MACsrc, lastEvent.eventID,
 lastEvent.observer_name, a.UID, lastEvent.UID from
 pattern [every a=DataFlowEvent(protocol=\"rdp\") ->
 lastEvent=WindowsEvent((eventID=\"4624\" or eventID=\"528\" or
 eventID=\"540\") and a.hostnameDst=observer_name)].win:time(10 min)
```

Подсказка:

Подробнее о синтаксисе, возможностях и примерах создания правил корреляции см. в разделе «Синтаксис правил корреляции событий».

В Комплексе с установленным модулем «Управление внешними событиями» доступно создание правил корреляции событий, либо загрузка готового списка правил из файла формата `*.json`.

11.6.1. Экспорт и импорт политики корреляции

В этом разделе:

- Импорт правил корреляции
- Импорт схемы корреляции

- Импорт политики корреляции
- Экспорт политики корреляции

Экспорт и импорт политики корреляции (правил и схемы по отдельности) осуществляется на странице **Администрирование** → **Основные настройки** → **Импорт и экспорт** на панели **Корреляция событий**.

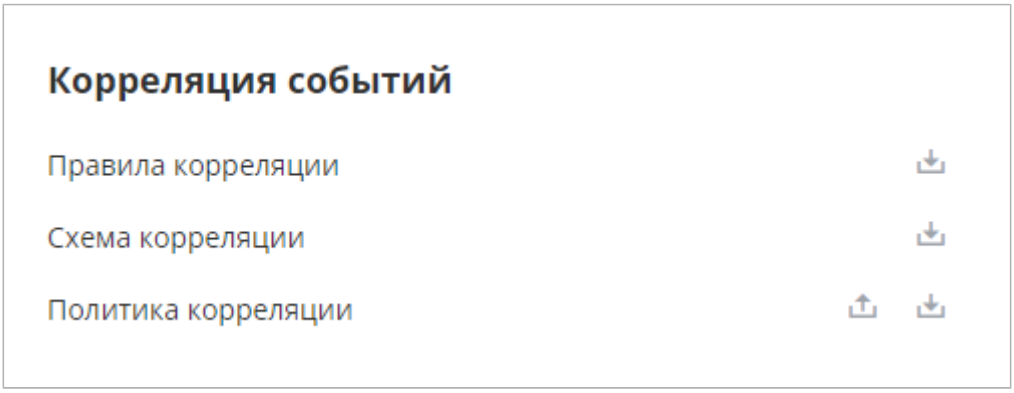


Рис. 123. Панель «Корреляция событий» на странице «Импорт и экспорт»

11.6.1.1. Импорт правил корреляции

> Внимание:
>
> Рекомендуется импортировать правила корреляции в составе политики корреляции (вместе со схемой). Подробнее см. в разделе «Импорт политики корреляции».

Для импорта файла формата `*.json` с правилами корреляции в Комплекс:

1. Перейдите на страницу **Администрирование** → **Основные настройки** → **Импорт и экспорт**.
2. На панели Корреляция событий в строке **Правила корреляции** нажмите кнопку (**Импортировать**).
3. В открывшемся окне укажите расположение импортируемого файла формата `*.json` и подтвердите выбор.
4. В окне **Подготовка к импорту** выберите:
    a. действие для элементов, которые отсутствуют в новом (загружаемом) справочнике:
        - **Оставить** — новые элементы будут добавлены к уже существующим;
        - **Удалить** — старые элементы будут удалены и добавлены новые
    б. активность службы после импорта:
        - **Запустить принудительно** — служба будет включена вне зависимости от ее статуса до импорта (даже если она была отключена);
        - **Оставить в текущем состоянии** — состояние службы не изменится. Если служба в момент импорта не запущена и выбран этот вариант, то правила будут записаны и применены только после запуска службы.
    в. статус активности элементов справочника после импорта:
        - **Оставить как есть** — статус активности элементов справочника будет сохранен;
        - **Присвоить старым статус, как в файле** — статус активности элементов справочника будет перезаписан в соответствии со значениями в импортируемом файле.
5. Нажмите **Импортировать** для запуска процедуры импорта.

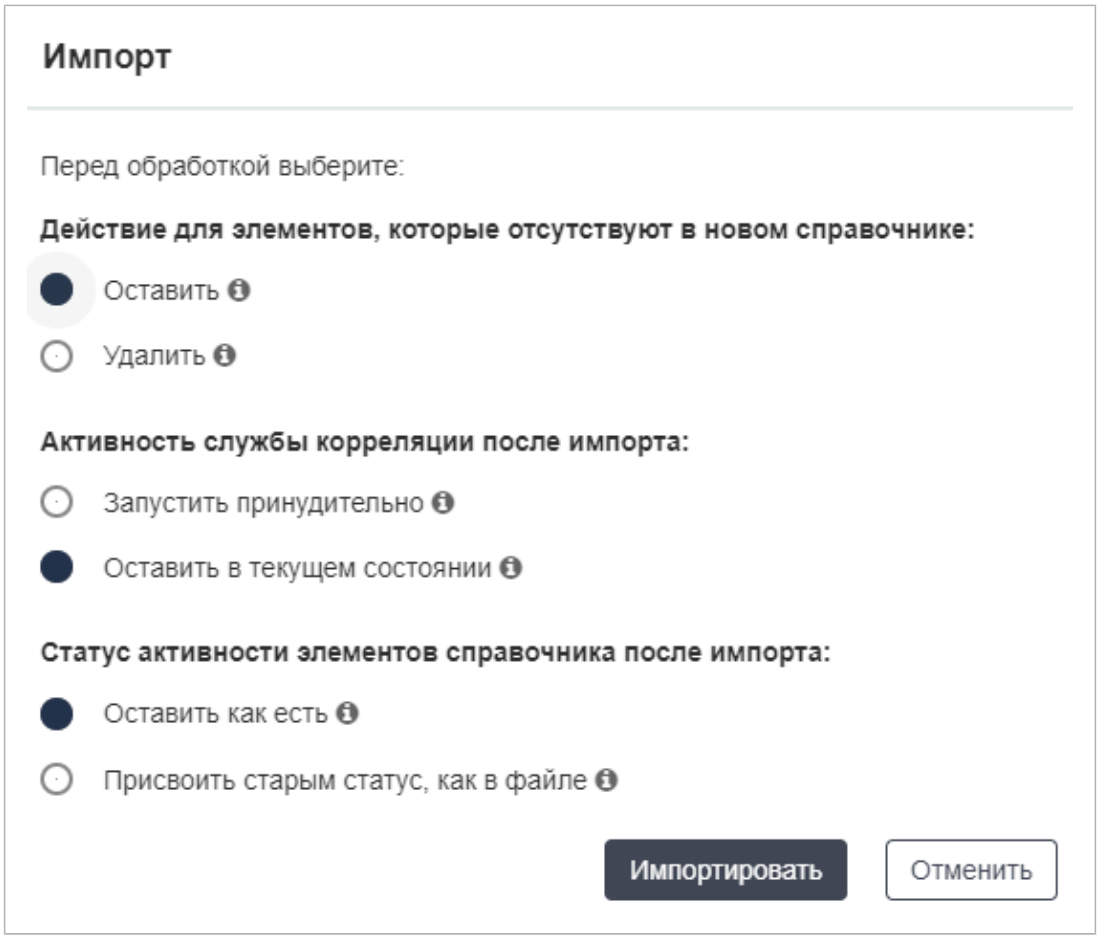


Рис. 124. Окно импорта правил корреляции

- **Результат шага:** появится уведомление `Список «Правила корреляции» успешно обновлен`, и на странице **Правила корреляции** появятся загруженные правила.

6. Убедитесь, что правила были успешно загружены. Для этого перейдите на страницу **Правила корреляции**.

11.6.1.2. Импорт схемы корреляции

> Внимание:
>
> Рекомендуется импортировать схему корреляции в составе политики корреляции (вместе с правилами). Подробнее см. в разделе «Импорт политики корреляции».

Для импорта файла формата `*.json` со схемой корреляции событий в Комплекс:

1. Перейдите на страницу **Администрирование → Основные настройки → Импорт и экспорт**.
2. На панели Корреляция **событий** в строке **Схема корреляции** нажмите кнопку (**Импортировать**).
3. В открывшемся окне укажите расположение импортируемого файла формата `*.json` и подтвердите выбор.
4. В окне **Подготовка к импорту** выберите:
    a. действие для элементов, которые отсутствуют в новом (загружаемом) справочнике:
        - **Оставить** — новые элементы будут добавлены к уже существующим;
        - **Удалить** — старые элементы будут удалены и добавлены новые

б. активность службы после импорта:

- **Запустить принудительно** — служба будет включена вне зависимости от ее статуса до импорта (даже если она была отключена);
- **Оставить в текущем состоянии** — состояние службы не изменится. Если служба в момент импорта не запущена и выбран этот вариант, то правила будут записаны и применены только после запуска службы.

в. статус активности элементов справочника после импорта:

- **Оставить как есть** — статус активности элементов справочника будет сохранен;
- **Присвоить старым статус, как в файле** — статус активности элементов справочника будет перезаписан в соответствии со значениями в импортируемом файле.

5. Нажмите **Импортировать** для запуска процедуры импорта.

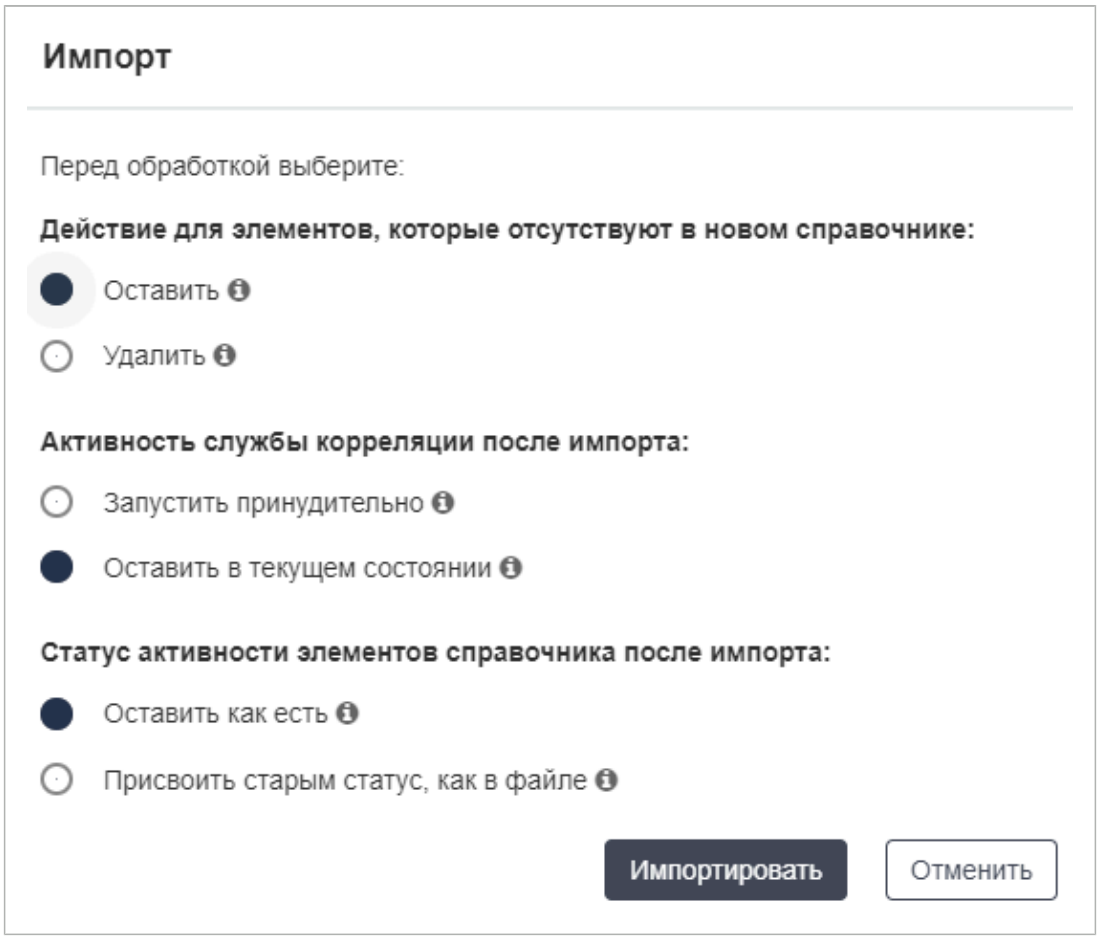


Рис. 125. Окно «Подготовка к импорту» при загрузке схемы корреляции

▸ **Результат шага:** появится уведомление `Список «Схема корреляции» успешно обновлен`, и на странице **Схема корреляции** появятся элементы схемы.

6. Убедитесь, что схема была успешно загружена. Для этого перейдите на страницу **Схема корреляции**.

11.6.1.3. Импорт политики корреляции

Для импорта файла формата `*.json` с политикой корреляции в Комплекс:

1. Перейдите на страницу **Администрирование → Основные настройки → Импорт и экспорт**.
2. На панели Корреляция **событий** в строке **Политика корреляции** нажмите кнопку (**Импортировать**).

3. В открывшемся окне укажите расположение импортируемого файла формата `*.json` и подтвердите выбор.
4. В окне **Подготовка к импорту** выберите:
    а. действие для элементов, которые отсутствуют в новом (загружаемом) справочнике:
        - **Оставить** — новые элементы будут добавлены к уже существующим;
        - **Удалить** — старые элементы будут удалены и добавлены новые

    б. активность службы после импорта:
        - **Запустить принудительно** — служба будет включена вне зависимости от ее статуса до импорта (даже если она была отключена);
        - **Оставить в текущем состоянии** — состояние службы не изменится. Если служба в момент импорта не запущена и выбран этот вариант, то правила будут записаны и применены только после запуска службы.

    в. статус активности элементов справочника после импорта:
        - **Оставить как есть** — статус активности элементов справочника будет сохранен;
        - **Присвоить старым статус, как в файле** — статус активности элементов справочника будет перезаписан в соответствии со значениями в импортируемом файле.
5. Нажмите **Импортировать** для запуска процедуры импорта.

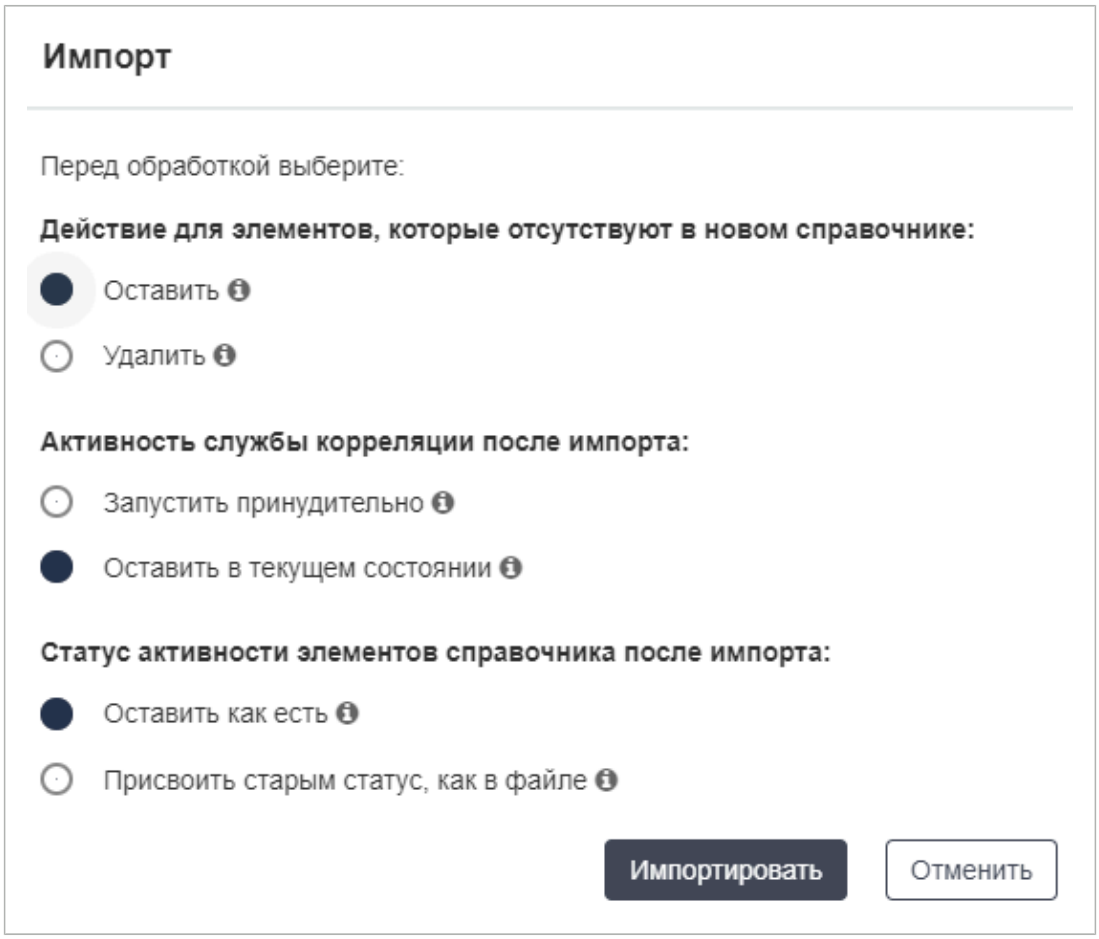


Рис. 126. Окно импорта политики корреляции

▸ **Результат шага:** появится уведомление `Список «Политика корреляции» успешно обновлен`, и на страницах **Схема корреляции** и **Правила корреляции** появятся загруженные элементы.

6. Убедитесь, что политика корреляции была успешно загружена. Для этого перейдите на страницы **Схема корреляции** и **Правила корреляции**.

11.6.1.4. Экспорт политики корреляции

Перед выполнением: В составе политики корреляции экспортируются правила корреляции и схема корреляции.

Для экспорта политики корреляции событий в файл формата `.json`:

1. Перейдите на страницу **Администрирование → Основные настройки → Импорт и экспорт**.
2. На панели **Корреляция событий** в строке **Политика корреляции** нажмите кнопку (**Экспортировать**).
   - **Результат шага:** файл с политикой корреляции `policy_correlation_[дата_и_время].json` будет сформирован и доступен для скачивания в правом верхнем углу страницы **Импорт и экспорт** под заголовком **Результат последнего экспорта**.
3. Для скачивания файла нажмите на название сформированного файла под заголовком **Результат последнего экспорта**.
4. В открывшемся окне укажите расположение для экспортируемого файла, при необходимости изменив его название, и нажмите кнопку **Сохранить**.
   - **Результат шага:** файл `policy_correlation_[дата_и_время].json` будет загружен на компьютер.

11.6.2. Экспорт и импорт статусов инцидентов

В этом разделе:

- Импорт статусов инцидентов
- Экспорт статусов инцидентов

Управление экспортом и импортом Комплексы статусов инцидентов осуществляется на панели **Инциденты**.

Рис. 127. Панель «Инциденты» на странице «Импорт и экспорт»

11.6.2.1. Импорт статусов инцидентов

Для импорта файла формата `*.json` со статусами инцидентов в Комплекс:

1. Перейдите на страницу **Администрирование → Основные настройки → Импорт и экспорт**.
2. На панели «Инциденты» в строке «Статусы инцидентов» нажмите кнопку «Загрузить из файла».
3. В открывшемся окне укажите расположение импортируемого файла формата `*.json` и подтвердите выбор.
   - **Результат шага:** появится уведомление `Список «Статусы инцидентов» успешно обновлен`, и на странице **Статусы инцидентов** появятся записи импортированных элементов
4. Убедитесь, что статусы были успешно загружены.

11.6.2.2. Экспорт статусов инцидентов

Для экспорта статусов инцидентов в файл формата `.json`:

1. Перейдите на страницу **Администрирование → Основные настройки → Импорт и экспорт**.
2. На панели **Инциденты** в строке **Статусы инцидентов** нажмите кнопку (**Экспортировать**).
   - **Результат шага:** файл со статусами инцидентов `incidents_statuses_[дата_и_время].json` будет сформирован и доступен для скачивания в правом верхнем углу страницы **Импорт и экспорт** под заголовком **Результат последнего экспорта**.
3. Для скачивания файла нажмите на название сформированного файла под заголовком **Результат последнего экспорта**.
4. В открывшемся окне укажите расположение для экспортируемого файла, при необходимости изменив его название, и нажмите кнопку **Сохранить**.
   - **Результат шага:** файл `policy_correlation_[дата_и_время].json` будет загружен на компьютер.

11.6.3. Управление службой корреляции событий

В верхней части страницы **Администрирование → События и инциденты → Правила корреляции** доступны следующие возможности по управлению службой:

1. Запуск службы корреляции событий. Для запуска нажмите (**Запустить службу**).
2. Остановка службы корреляции событий. Для остановки нажмите (**Остановить службу**).
3. Перезапуск службы корреляции событий. Для перезапуска нажмите (**Перезапустить службу**).
   - **Результат шага:** появится уведомление `Служба корреляции событий перезапущена`.
4. Просмотр событий и текущего состояния службы корреляции событий. Для просмотра:
   a. Нажмите (**Состояние службы корреляции**).
   - **Результат шага:** откроется окно **Состояние службы корреляции**.

б. Ознакомьтесь со списком событий службы корреляции.

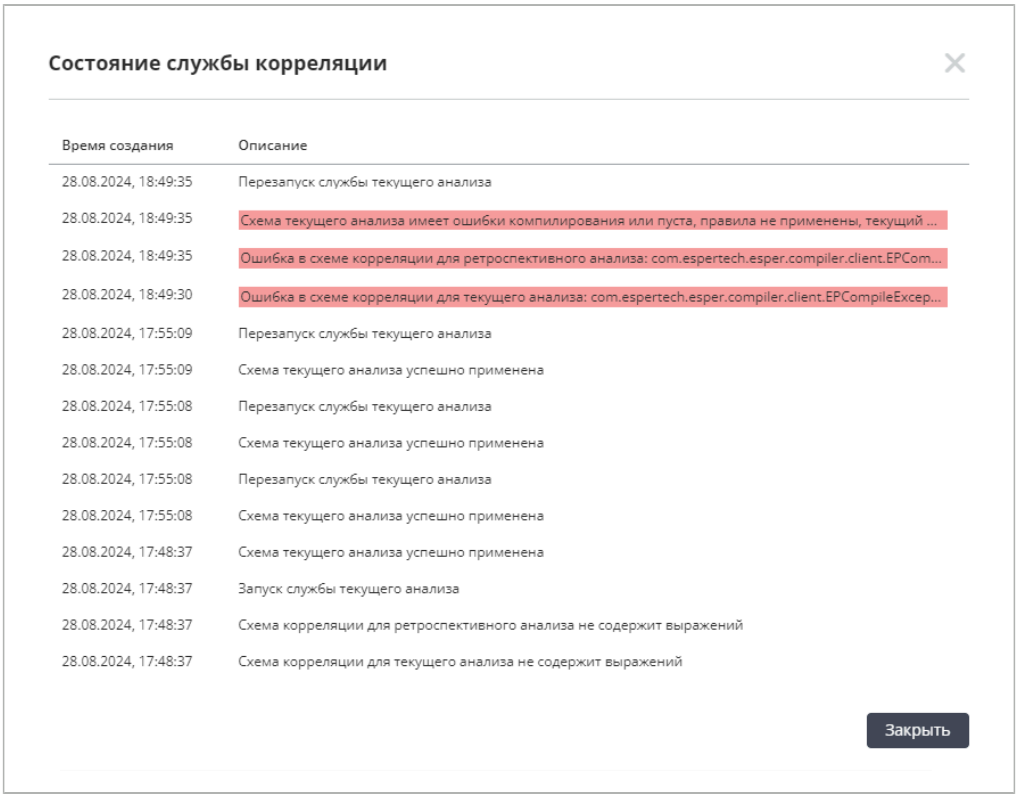


Рис. 128. Окно «Состояние службы корреляции»

Подсказка:

В случае появления ошибок в работе компонентов службы корреляции можно просмотреть подробности в колонке **Описание**.

11.6.4. Управление схемой корреляции

Подсказка:

Для применения изменений перезапуск службы не требуется. При редактировании или удалении элемента схемы, задействованного в текущем анализе, происходит автоматический перезапуск службы.

Веб-интерфейс предоставляет следующие возможности по изменению состава элементов схемы корреляции:

1. Создание. Для создания элемента схемы:
    a. На странице **Схема корреляции** нажмите **Создать элемент схемы**.

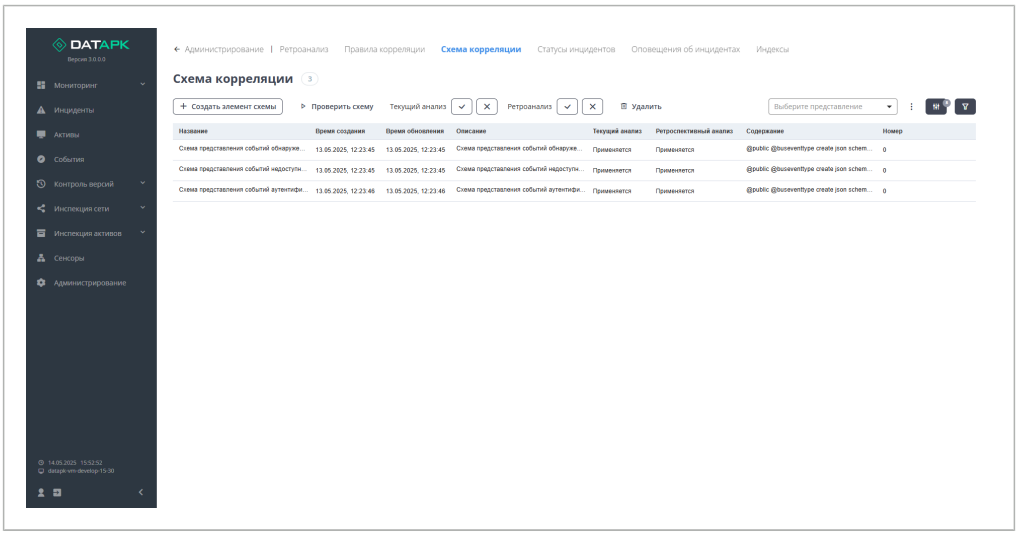


Рис. 129. Страница «Схема корреляции»

- **Результат шага:** появится окно **Создание элемента схемы**.

    б. Заполните следующие обязательные поля:

- **Наименование** — отображаемое название элемента схемы;
- **Содержание** — состав схемы: переменные, контексты, окна;
- **Номер** — номер по порядку применения схемы.

> Подсказка:
>
> Если необходимости в определении порядка нет, введите в поле значение `0`.

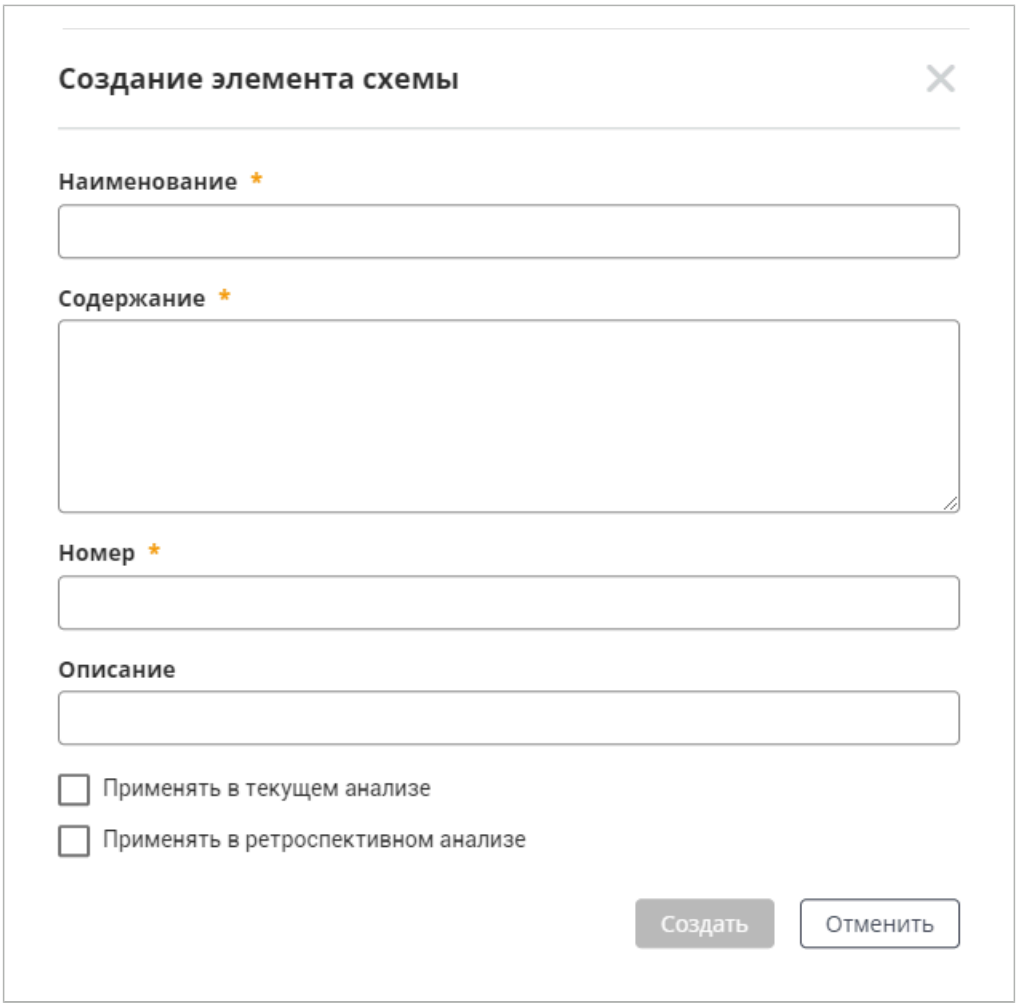


Рис. 130. Окно «Создание элемента схемы»

в. При необходимости введите описание и установите чекбоксы для применения в текущем или ретроспективном анализах.

> Подсказка:
>
> Подробнее о запуске анализа см. в разделе «Анализ событий для генерации инцидентов».

г. Нажмите **Создать**.

2. Проверка — позволяет оценить корректность созданных элементов схемы без запуска анализа. Для проверки схемы:

   а. Воспользуйтесь фильтрами на странице **Схема корреляции**. Для этого нажмите в правом верхнем углу.

   б. Нажмите **Проверить схему**.

   в. Дождитесь окончания проверки.

▸ **Результат шага:** В правом верхнем углу появится уведомление `Отфильтрованные элементы схемы корректны.`

> Внимание:
>
> В случае получения ошибок измените элементы схемы.

3. Редактирование. Для редактирования элемента схемы:
   a. Наведите курсор на строку с элементом схемы, который нужно отредактировать.
   б. В правой части страницы нажмите (**Редактировать**).
   ▸ **Результат шага:** откроется окно **Редактирование элемента схемы**.
   в. Измените необходимые параметры и нажмите **Сохранить**.

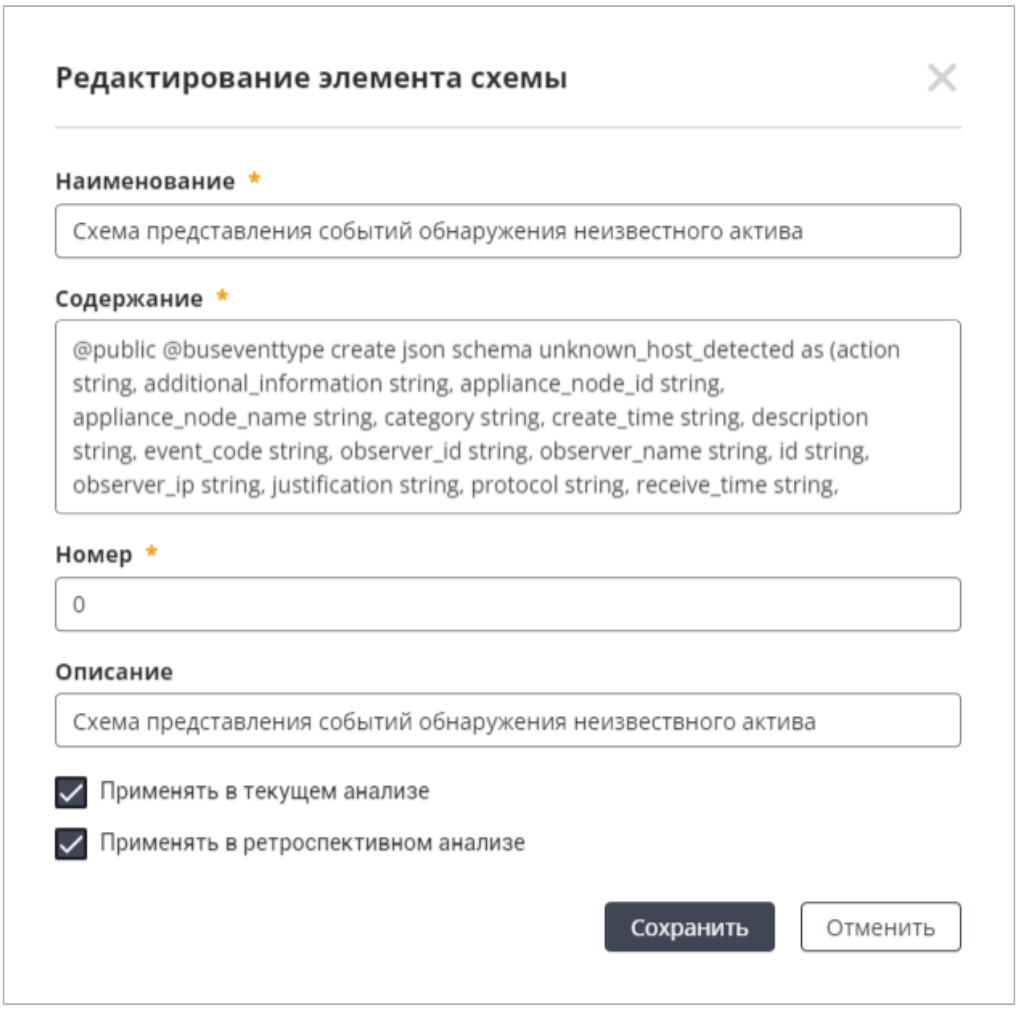


Рис. 131. Окно «Редактирование элемента схемы»

4. Удаление. Для удаления одного элемента схемы:
   a. Наведите курсор на строку с элементом, который нужно удалить.
   б. Нажмите (**Удалить элемент схемы**).
   ▸ **Результат шага:** появится окно подтверждения удаления.

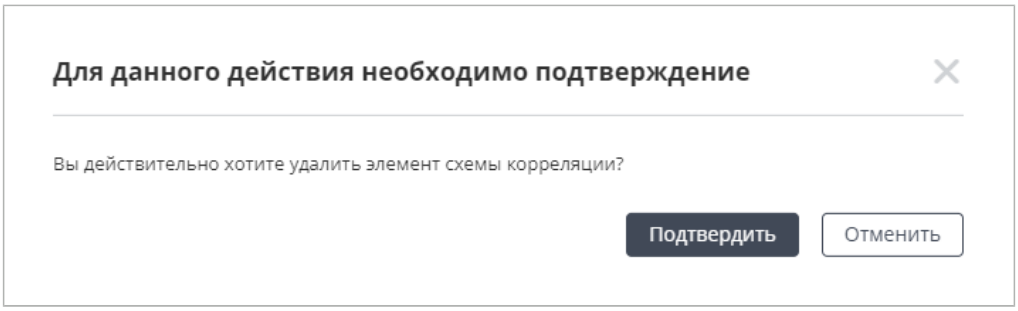


Рис. 132. Окно подтверждения удаления элемента схемы корреляции

в. Нажмите **Подтвердить**.

5. Групповое удаление. Для удаления всех отображаемых на странице элементов:

а. Воспользуйтесь фильтрами на странице **Схема корреляции**. Для этого нажмите в правом верхнем углу.

б. В верхней части страницы нажмите (**Удалить**).

Результат шага: появится окно подтверждения удаления.

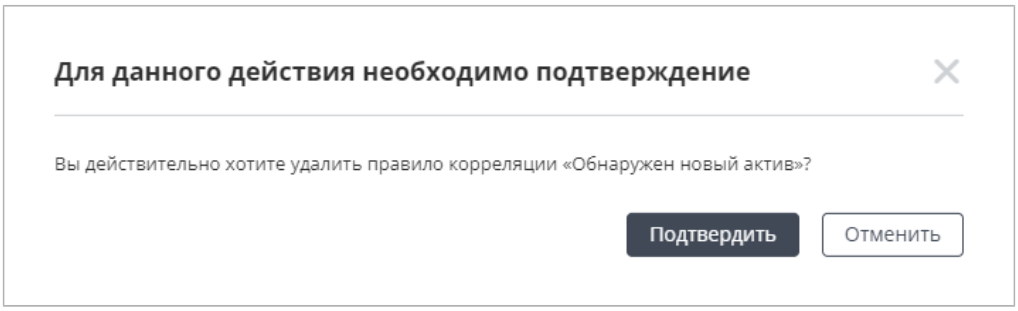


Рис. 133. Окно подтверждения удаления элементов схемы корреляции

в. Нажмите **Подтвердить**.

11.6.5. Управление правилами корреляции событий

Для управления правилами корреляции в веб-интерфейсе Комплекса предусмотрены следующие возможности:

- Создание правил корреляции событий;
- Редактирование правил корреляции событий;
- Копирование правил корреляции событий;

- Удаление правила корреляции событий;
- Групповое удаление правил корреляции событий.

11.6.5.1. Создание правил корреляции событий

Для создания правила:

1. Перейдите на страницу **Администрирование → События и инциденты → Правила корреляции**.

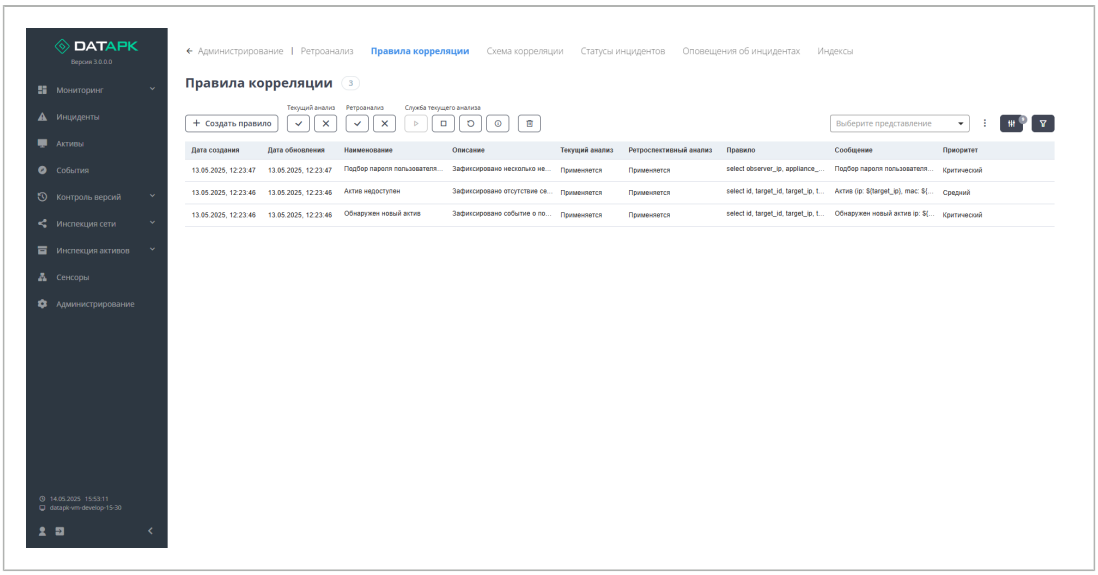


Рис. 134. Страница «Правила корреляции»

2. Нажмите кнопку **Создать правило**. В открывшемся окне настройте следующие параметры:
   - наименование и описание;

   > Внимание:
   >
   > Для поля **Описание** установлен лимит, равный 2000 символов.

   - правило;
   - сообщение, которое будет отображаться при возникновении события;
   - при необходимости установите чекбоксы для применения в текущем и (или) ретроспективном анализе.

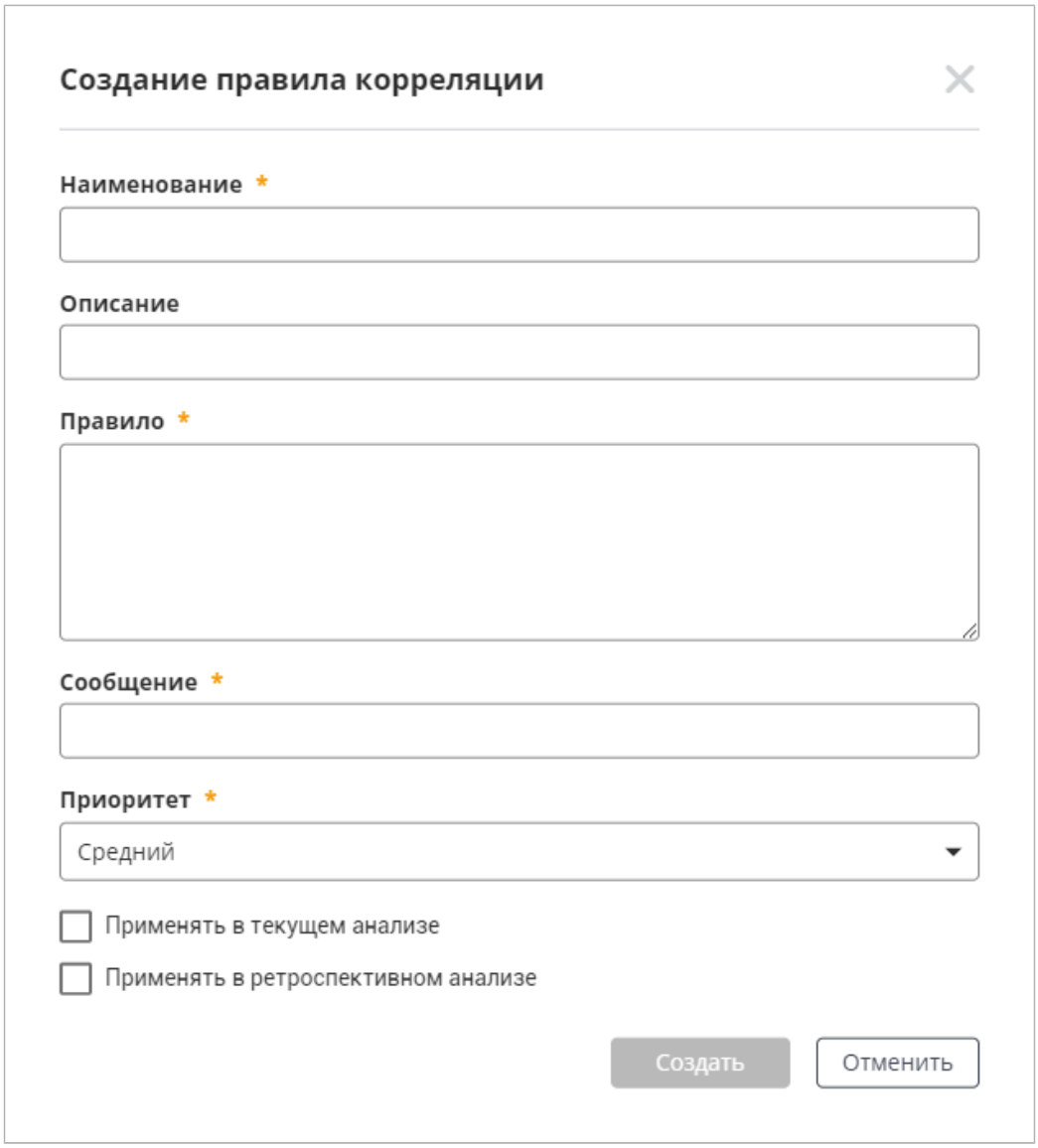


Рис. 135. Окно «Создание правила корреляции»

3. Нажмите кнопку **Создать** для подтверждения изменений.

> Внимание:
>
> В процессе сохранения правило будет проверено на корректность синтаксиса для выбранного анализа. В случае появления несоответствий и ошибок, правило не будет сохранено.

- **Результат шага:** правило будет доступно для применения в текущем и ретроспективном анализе.

11.6.5.2. Редактирование правил корреляции событий

Для редактирования правила:

1. Перейдите на страницу **Правила корреляции**.
2. В правой части страницы нажмите (**Редактировать**).
   - **Результат шага:** откроется окно **Редактирование правила корреляции**.

3. Измените необходимые параметры и нажмите **Сохранить**.

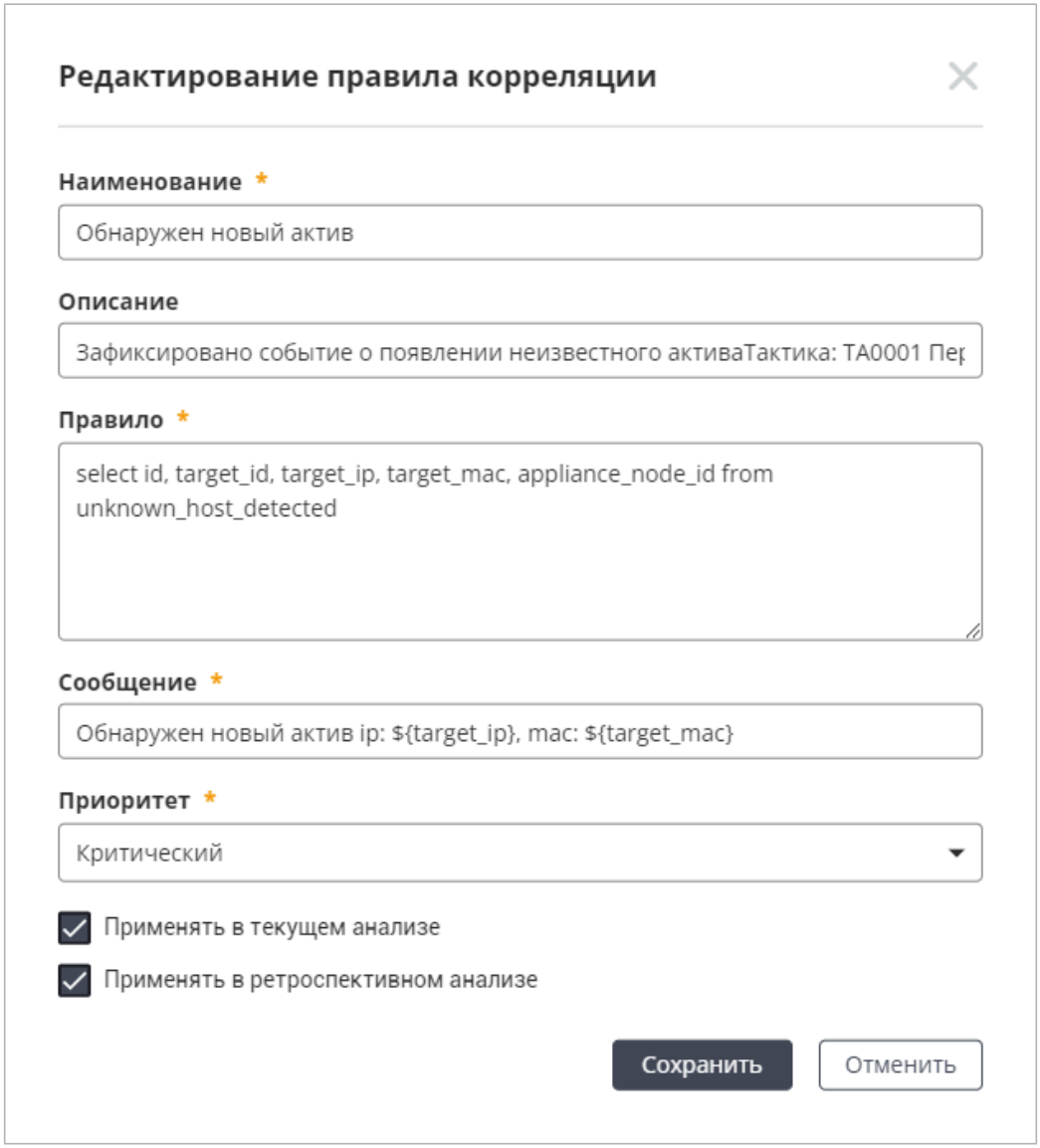


Рис. 136. Окно «Редактирование правила корреляции»

- **Результат шага:** отредактированное правило будет сохранено как новое правило корреляции. Исходное правило также сохранится.

11.6.5.3. Копирование правил корреляции событий

Для копирования правила:

1. Наведите курсор на строку с правилом, которое нужно скопировать.
2. Нажмите кнопку (**Создать копию правила**), расположенную справа в списке правил.
   - **Результат шага:** откроется окно **Создание копии правила корреляции**.

3. Измените необходимые параметры и нажмите **Сохранить**.

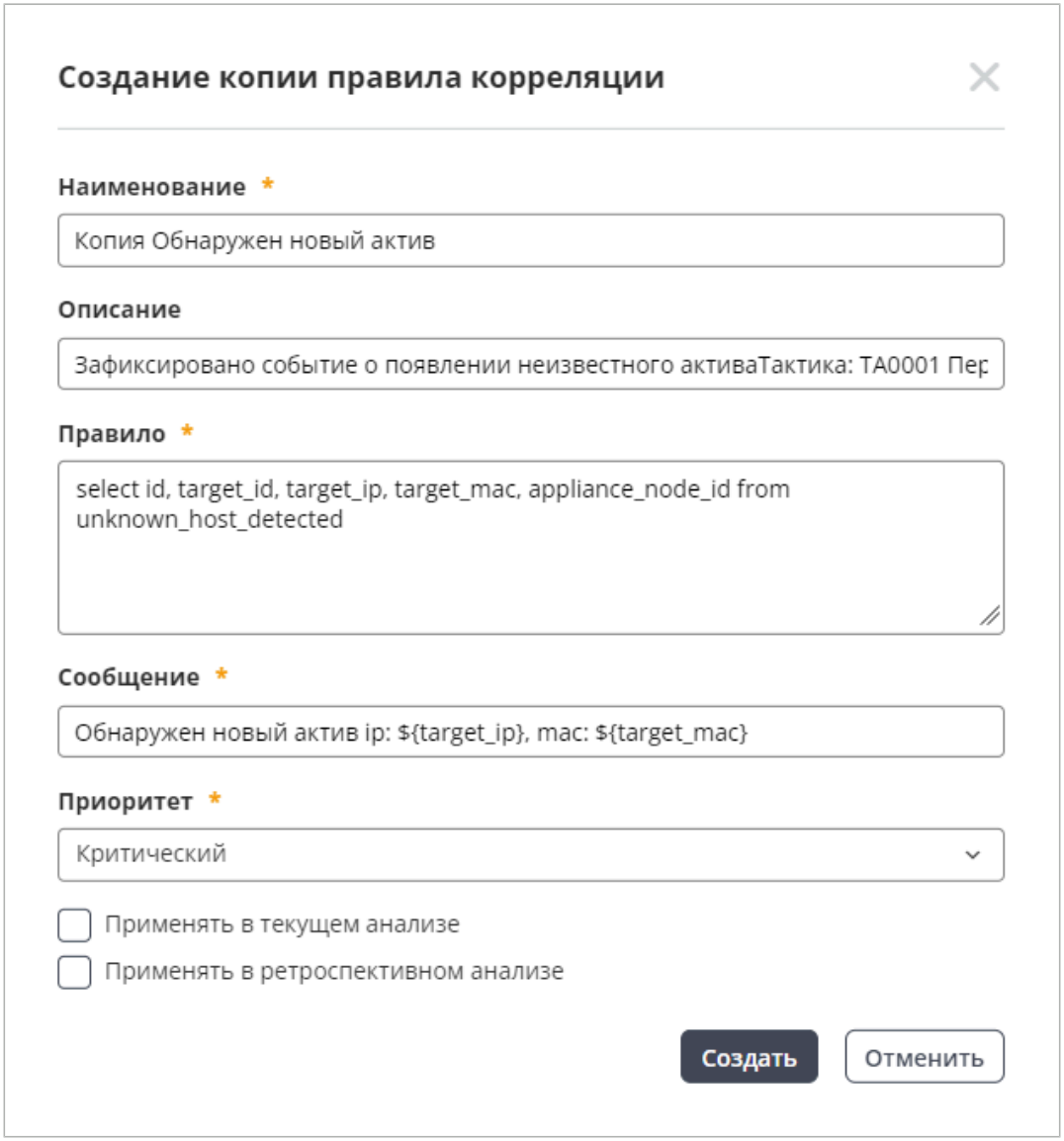


Рис. 137. Окно «Создание копии правила корреляции»

- **Результат шага:** созданная копия правила корреляции событий появится в списке правил и будет доступна для применения в текущем и ретроспективном анализе. Исходное правило также сохранится.

11.6.5.4. Удаление правила корреляции событий

Для удаления одного правила:

1. Наведите курсор на строку с правилом, которое нужно удалить.
2. Нажмите (**Удалить правило**).
   - **Результат шага:** появится окно ввода обоснования удаления.
3. Введите обоснование удаления и нажмите **Подтвердить**.
   - **Результат шага:** правило будет удалено.

11.6.5.5. Групповое удаление правил корреляции событий

1. Воспользуйтесь фильтрами на странице **Правила корреляции**.
2. В верхней части страницы нажмите (**Удалить правила**).
   - **Результат шага:** появится окно ввода обоснования удаления.
3. Введите обоснование и нажмите **Удалить**.
   - **Результат шага:** выбранные правила будут удалены.

11.6.6. Анализ событий для генерации инцидентов

В этом разделе:

- Текущий анализ событий
- Ретроспективный анализ событий
- Управление ретроспективными проверками

После настройки правил и схемы корреляции последним шагом для появления инцидентов является запуск анализа событий. Комплекс позволяет производить как анализ событий реального времени (текущий), так и анализ событий, полученных раннее (ретроспективный).

Для управления использованием схем и правил корреляции в текущем и ретроспективном анализах в верхней части страниц расположены управляющие элементы, позволяющие отрегулировать список схем и правил, используемых в том или ином анализе.

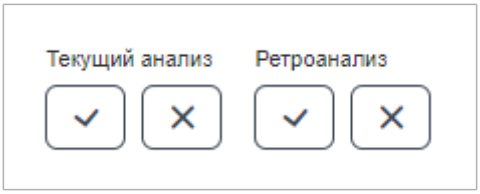


Рис. 138. Кнопки управления активностью элементов в анализах

Разница в запуске текущего и ретроспективного анализа заключается в том, что для запуска текущего анализа достаточно установить активность соответствующих политик корреляции (правил и схем корреляции), а для ретроспективного анализа нужно также выбрать период, за который будут проанализированы события в соответствии с политикой корреляции.

11.6.6.1. Текущий анализ событий

Для запуска текущего анализа событий:

1. Убедитесь в наличии элементов схемы корреляции. Для этого перейдите на страницу **Администрирование → События и инциденты → Схема корреляции**.
2. Активируйте один или несколько элементов схем корреляции. Для этого:
   a. Воспользуйтесь фильтрами на странице **Схема корреляции**. Для этого нажмите в верхнем правом углу страницы.
   б. Для активации элемента схемы:

- наведите курсор на строку с элементом схемы и нажмите (**Редактировать**);
- установите чекбокс **Применение в текущем анализе**;
- нажмите **Сохранить**.

в. Для активации всех выбранных в фильтре элементов схемы нажмите (**Включить элементы схемы для текущего анализа**).

3. Убедитесь в наличии правил корреляции. Для этого перейдите на страницу **Инциденты → Правила корреляции**.
4. Активируйте одно или несколько правил корреляции. Для этого:
   а. Воспользуйтесь фильтрами в левой части страницы **Правила корреляции**.
   б. Для активации отдельных правил:
   - в строке с правилом нажмите (**Редактировать**);
   - установите чекбокс **Активно в текущем анализе**;
   - нажмите **Сохранить**.

   в. Для активации всех выбранных в фильтре правил нажмите (**Применить правила для текущего анализа**).

Результат шага: правила будут задействованы в текущем анализе без необходимости перезапуска службы.

5. Убедитесь в том, что произведенные настройки были применены. Для этого:
   а. В верхней части страницы **Правила корреляции** нажмите (**Состояние службы корреляции**).
   б. Убедитесь, что список последних событий службы не содержит ошибок.

Возможные затруднения: Для устранения ошибок, связанных с применением правил, вы можете перезапустить службу корреляции. Для этого в верхней части страницы **Правила корреляции** нажмите (**Перезапустить службу**).

11.6.6.2. Ретроспективный анализ событий

Для запуска ретроспективного анализа событий:

1. Убедитесь в наличии элементов схемы корреляции. Для этого перейдите на страницу **Администрирование → События и инциденты → Схема корреляции**.
2. Активируйте один или несколько элементов схемы корреляции. Для этого:
   а. Нажмите кнопку в верхнем правом углу страницы и воспользуйтесь представленными фильтрами.
   б. Для активации элемента схемы:
   - наведите курсор на строку со схемой и нажмите (**Редактировать**);
   - установите чекбокс **Применение в ретроспективном анализе**;
   - нажмите **Сохранить**.

   в. Для активации всех выбранных в фильтре элементов схемы нажмите (**Включить элементы схемы для ретроспективного анализа**).

3. Убедитесь в наличии правил корреляции. Для этого перейдите на страницу **Администрирование → События и инциденты → Правила корреляции**.
4. Активируйте одно или несколько правил корреляции. Для этого:
   а. Воспользуйтесь фильтрами на странице **Правила корреляции**.
   б. Для активации отдельных правил:
      - в строке с правилом нажмите (**Редактировать**);
      - установите чекбокс **Активно в ретроспективном анализе**;
      - нажмите **Сохранить**.
   в. Для активации всех выбранных в фильтре правил нажмите (**Включить правила для ретроспективного анализа**).
5. Запустите ретроспективную проверку. Для этого:

> Внимание:
>
> Возможен запуск только одной проверки за раз.

   а. Перейдите на страницу **Администрирование → События и инциденты → Ретроанализ**.
   б. Нажмите **Запустить анализ**.

   Результат шага: появится окно **Запуск ретроспективного анализа**.

   в. В открывшемся окне задайте следующие обязательные параметры анализа:
      - название;
      - период, за который будут проанализированы события;

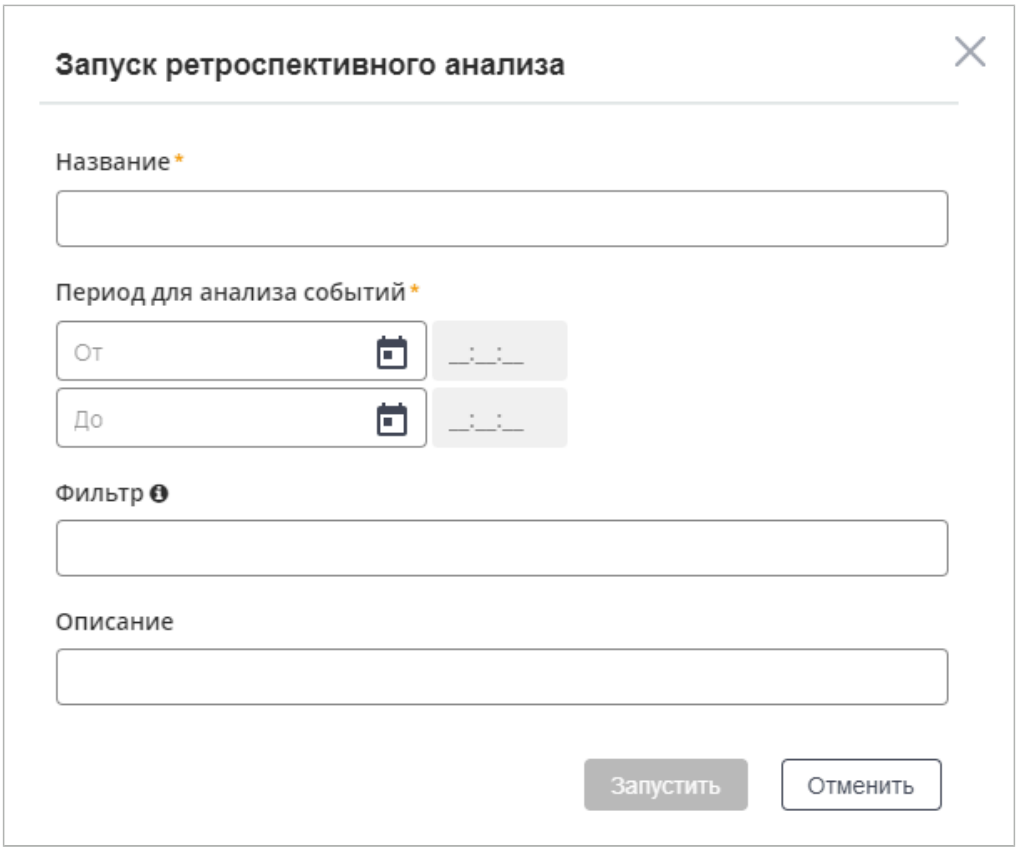


Рис. 139. Окно запуска ретроспективного анализа

> Внимание:
>
> При указании периода ретроспективного анализа вы можете указать дату окончания в будущем. Этот способ позволит учитывать события, которые могут возникнуть из-за разницы часовых поясов на распределенных инсталляциях или из-за некорректно настроенного времени на источнике данных.

г. При необходимости введите описание и фильтр в формате Lucene.

д. Нажмите **Запустить**.

> Подсказка:
>
> Если необходимо остановить процесс анализа, нажмите кнопку **Остановить анализ** в верхней части страницы.

> Внимание:
>
> Запуск других ретроспективных анализов будет недоступен до окончания проверки. Удалять анализ до окончания проверки не рекомендуется.

e. Дождитесь окончания выполнения анализа.

- **Результат шага:** по завершении анализа будет получен статус и число выявленных инцидентов. Для просмотра списка инцидентов нажмите на число в колонке **Число инцидентов**.

6. Если был получен статус Ошибка или Выполнено с ограничениями:

a. Наведите курсор на строку с выполненной проверкой.

б. Нажмите на ячейку статуса или кнопку (**Просмотреть статус анализа**) в конце строки.

- **Результат шага:** появится окно **Статус анализа**.

в. Ознакомьтесь с представленной в окне информацией.

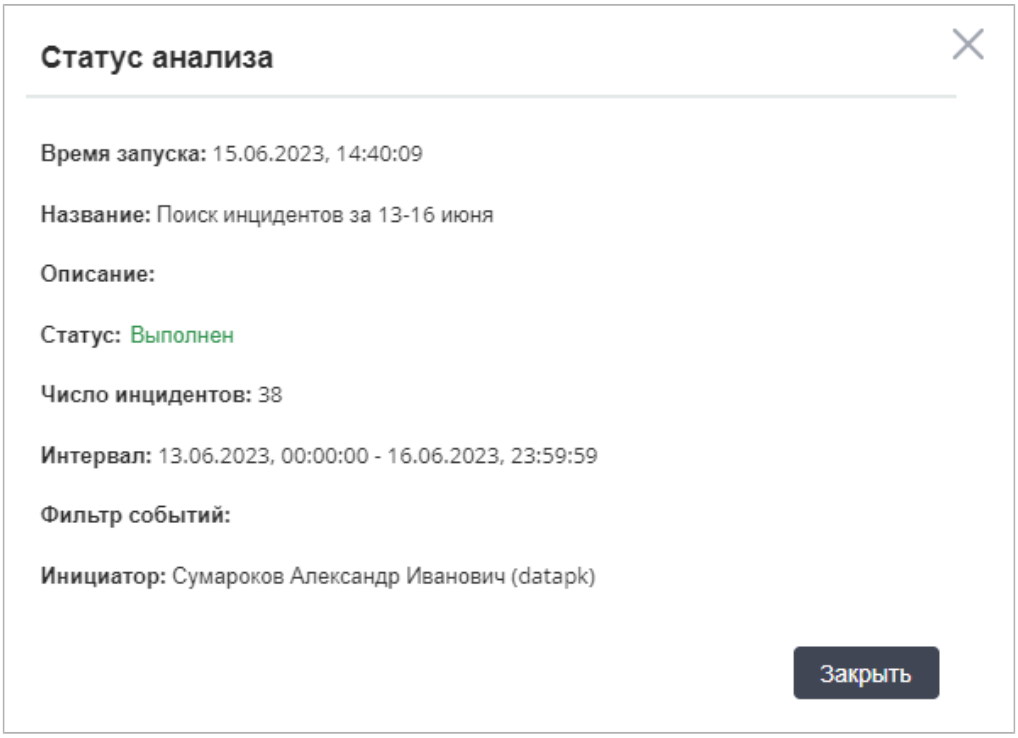


Рис. 140. Окно «Статус анализа»

См. также

Недоступен сервис корреляции событий

11.6.6.3. Управление ретроспективными проверками

Помимо первичного запуска ретроспективного анализа можно перезапускать, удалять проверки и создавать по ним отчет.

Возможности для управления ретроспективными проверками:

1. Просмотр статуса проверки. Для просмотра:

a. Наведите курсор на строку с выполненной проверкой.

б. Нажмите на ячейку статуса или кнопку (**Просмотреть статус анализа**) в конце строки.

- **Результат шага:** появится окно **Статус анализа**.

в. Ознакомьтесь с представленной в окне информацией.

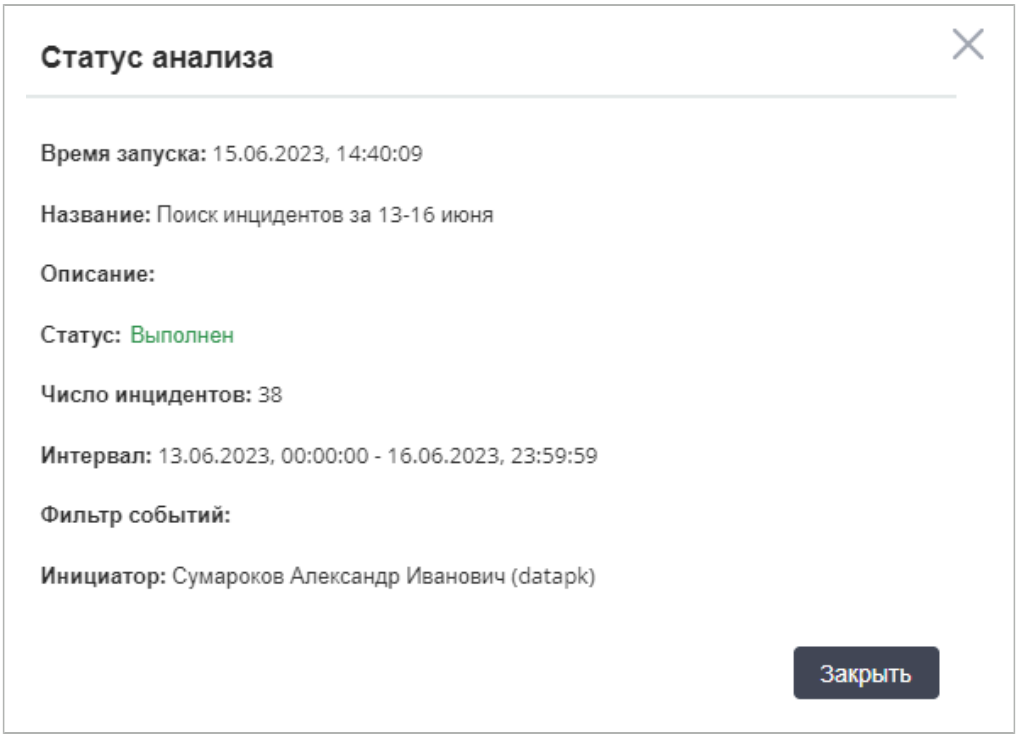


Рис. 141. Окно «Статус анализа»

2. Просмотр инцидентов по результатам проверки. Для просмотра всех выявленных в рамках анализа инцидентов:
   а. Наведите курсор на строку с выполненной проверкой.
   б. Нажмите на число в колонке **Число инцидентов**.

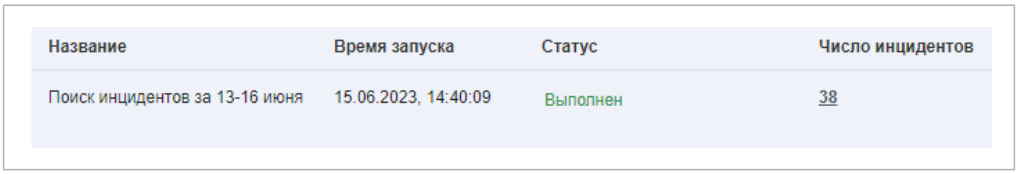


Рис. 142. Переход к просмотру инцидентов по результатам ретроспективной проверки

▸ **Результат шага:** будет выведен список всех инцидентов, полученных в результате ретроспективного анализа.

3. Перезапуск. Для перезапуска созданного ранее ретроспективного анализа:
   а. Наведите курсор на строку с выполненной проверкой.
   б. В правой части страницы нажмите (**Повторить анализ**).

▸ **Результат шага:** на месте кнопки запуска анализа появится кнопка **Остановить анализ**. При необходимости вы можете воспользоваться возможностью прервать проверку, нажав соответствующую кнопку.

4. Удаление одной проверки. Для удаления ретроспективной проверки:

> Внимание:
>
> Инциденты, полученные в результате анализа, будут сохранены.

а. Наведите курсор на строку с выполненной проверкой.

б. Убедитесь, что удаляемый анализ не запущен. Если запущен — остановите выполнение проверки.

в. В правой части страницы нажмите (**Удалить анализ**).

- **Результат шага:** проверка будет удалена.

5. Удаление проверок, отображаемых на странице. Для удаления ретроспективных проверок:

> Внимание:
>
> Инциденты, полученные в результате проверок, будут сохранены.

а. Наведите курсор на строку с выполненной проверкой.

б. Убедитесь, что ни один из удаляемых анализов не запущен. Если запущен — остановите выполнение проверки.

в. В правой части страницы нажмите (**Удалить анализ**).

- **Результат шага:** проверка будет удалена.

См. также

Недоступен сервис корреляции событий

11.6.7. Настройка оповещений при появлении инцидентов

В этом разделе:

- Настройка оповещения пользователей по электронной почте
- Настройка правила для отправки оповещений на OPC-сервер

После того, как служба корреляции событий сформирует инциденты, можно автоматически отправлять оповещения пользователям по E-mail или на OPC-сервер.

Управление отправкой оповещений осуществляется на странице **Оповещения об инцидентах**.

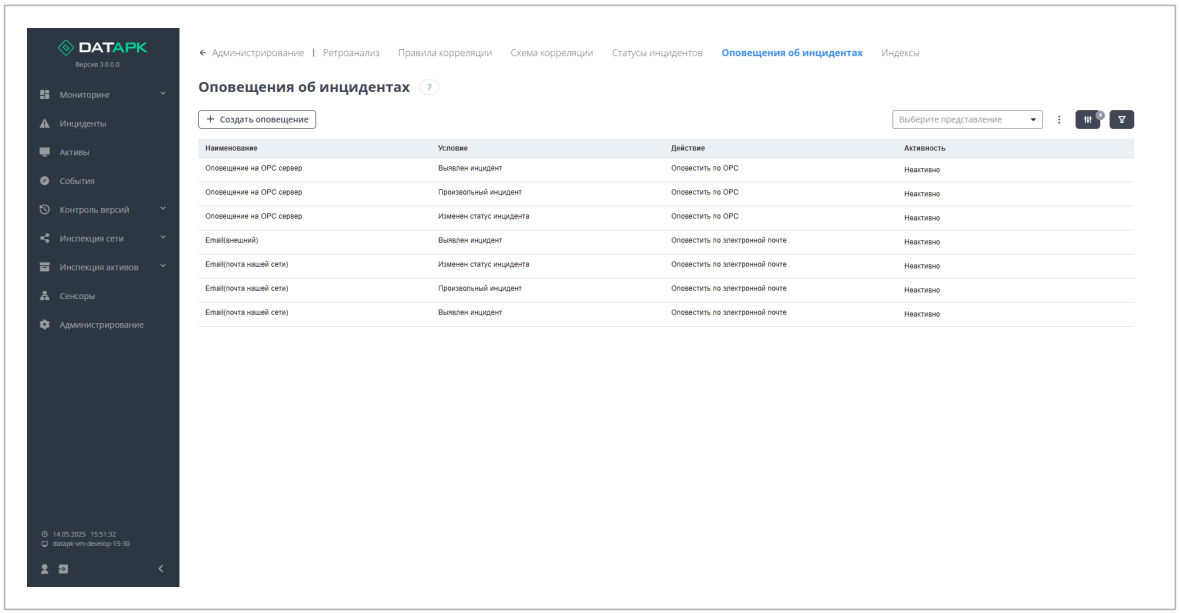


Рис. 143. Страница «Оповещения об инцидентах»

11.6.7.1. Настройка оповещения пользователей по электронной почте

Для настройки правила для оповещения пользователей по электронной почте (с использованием протокола SMTP/SMTPS) при появлении любых инцидентов или изменении их статуса:

1. Перейдите на страницу **Администрирование → События и инциденты → Оповещения об инцидентах**.
2. Нажмите **Создать оповещение** в верхней части страницы.
3. В открывшемся окне **Создание оповещения** настройте следующие параметры:
   а. тип оповещения — `Оповестить по электронной почте`;
   б. наименование оповещения;
   в. условие, при котором будет выполняться оповещение, в поле **Условие**;
   г. если выбрано условие `Произвольный инцидент`, в появившемся поле **Ключевое слово** введите ключевое слово для одного из полей инцидента;

> Подсказка:
>
> В качестве значения поля **Ключевое слово** можно задать наименование, описание или Комплекс, на котором был обнаружен инцидент.

> Внимание:
>
> Доступен ввод значения только одного поля инцидента в одном ключевом слове. При этом допускается ввести строку из нескольких слов, которая целиком содержится в наименовании или описании инцидента.

   д. адрес SMTP сервера;
   е. Email-адрес отправителя;
   ж. TCP-порт для обращения к почтовому серверу по протоколу SMTP — целое число от 1 до 65535;

з. добавьте Email-адреса получателей писем. Для этого:

- введите адрес в поле **Email Адрес получателя**;
- нажмите кнопку ;
- добавьте другие адреса при необходимости.

и. тему письма, которое будет получать пользователь при возникновении указанного события;

к. протокол шифрования;

л. установите чекбокс **Использовать авторизацию**, если необходим пароль для входа на почтовый сервер;

м. если чекбокс **Использовать авторизацию** установлен, введите пароль для возможности аутентификации на почтовом сервере;

н. установите чекбокс **Активность** для активации правила.

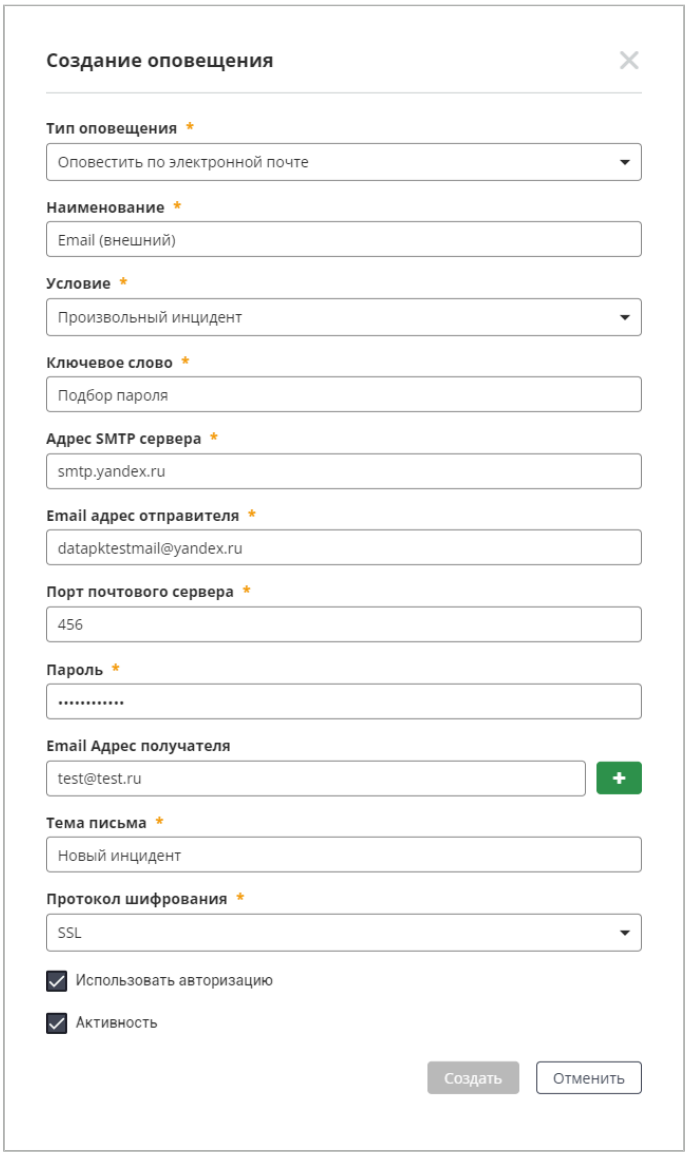


Рис. 144. Окно «Создание оповещения» при настройке оповещения о любых инцидентах по электронной почте

4. Нажмите кнопку **Создать**.
   - **Результат шага:** созданное правило оповещения будет отображаться на странице **Оповещения об инцидентах**.

11.6.7.1.1. Отправка тестового оповещения об инциденте

Для отправки тестового оповещения об инциденте:

1. Перейдите на страницу **Администрирование → События и инциденты → Оповещения об инцидентах**.
2. Наведите курсор на необходимое правило оповещения.
3. Нажмите кнопку (**Отправить тестовое оповещение**).
   - **Результат шага:** появится уведомление **Тестовое оповещение успешно отправлено**.

> Подсказка:
>
> оповещения будут приходить в следующем формате:

```
Описание события: [Текст с описанием события].
Инцидент: [Наименование инцидента].
Дата создания: [дата и время с указанием часового пояса в формате UTC].
Активы: [наименования активов].
Описание инцидента: [Текст с описанием инцидента].
Ссылка на инцидент: https://[IP-адрес текущего Комплекса]/app/incidents/[идентификатор
 инцидента]
```

Внимание:

В случае установки некорректных настроек при отправке тестового оповещения будет отображаться уведомление `Не удается отправить тестовое оповещение: почтовый сервер недоступен, либо один или несколько параметров оповещения имеют некорректные значения`

11.6.7.1.2. Изменение пароля для подключения к почтовому серверу

У ранее созданного правила оповещения можно изменить пароль для подключения к почтовому серверу. Для этого:

1. Перейдите на страницу **Администрирование → События и инциденты → Оповещения об инцидентах**.
2. Нажмите кнопку (**Редактировать оповещение**) в таблице оповещений.
3. В открывшемся окне **Редактирование оповещения** нажмите кнопку **Изменить пароль**.
4. В открывшемся окне **Изменение пароля для подключения к SMTP серверу** введите новый пароль в поля **Новый пароль** и **Подтверждение нового пароля** и нажмите кнопку **Сохранить**.

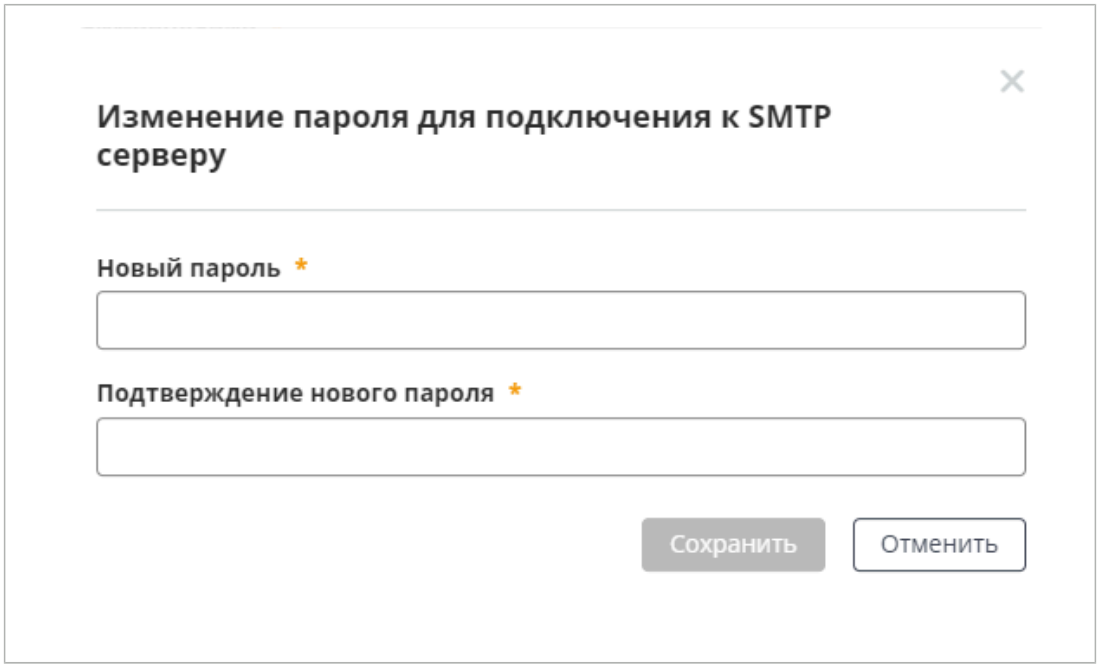


Рис. 145. Окно «Изменение пароля для подключения к SMTP серверу»

5. Нажмите кнопку **Сохранить** в окне **Редактирование оповещения**.
   - **Результат шага:** изменения, внесенные в оповещение, будут перезаписаны.

11.6.7.2. Настройка правила для отправки оповещений на OPC-сервер

Для настройки правила отправки оповещений на OPC-сервер при появлении инцидентов или изменении их статуса:

1. Перейдите на страницу **Администрирование → События и инциденты → Оповещения об инцидентах**.
2. Нажмите кнопку **Создать оповещение**.
3. В открывшемся окне **Создать оповещения** настройте следующие параметры:
   а. выберите `Оповестить по OPC` в поле **Тип оповещения**;
   б. наименование создаваемого оповещения;
   в. условие, при котором будет выполняться оповещение, в поле **Условие**;
   г. если выбрано условие `Произвольный инцидент`, в появившемся поле **Ключевое слово** введите ключевое слово для одного из полей инцидента;

> Подсказка:
>
> В качестве значения поля **Ключевое слово** можно задать наименование, описание или Комплекс, на котором был обнаружен инцидент.

> Внимание:
>
> Доступен ввод значения только одного поля инцидента в одном ключевом слове. При этом допускается ввести строку из нескольких слов, которая целиком содержится в наименовании или описании инцидента.

   д. IP-адрес OPC-сервера;
   е. TCP-порт для обращения к OPC-серверу по протоколу OPC UA — целое число от 1 до 65535;
   ж. URL-ссылку на OPC-сервер (при наличии);
   з. индекс пространства имен, в котором расположен тег, в поле **NamespaceIndex**;
   и. формат значения поля `Identifier` в поле **IdentifierType**;

> Подсказка:
>
> Для отправки сообщений с текстом необходимо создавать оповещения со значением поля **IdentefierType**, равным `String`.

   к. идентификатор тега OPC-сервера в соответствии с выбранным форматом данных в поле **Identifier**;
   л. логин и пароль для входа на OPC-сервер (если требуется);
   м. формат значения тега в поле **Тип тега**;

> **Внимание:**
>
> Если выбран тип `String`, в качестве сообщения будет отправлено стандартное сообщение; если выбран тип `Boolean`, в качестве сообщения может быть отправлено только значение `true`.

н. установите чекбокс **Активность** для включения активности правила.

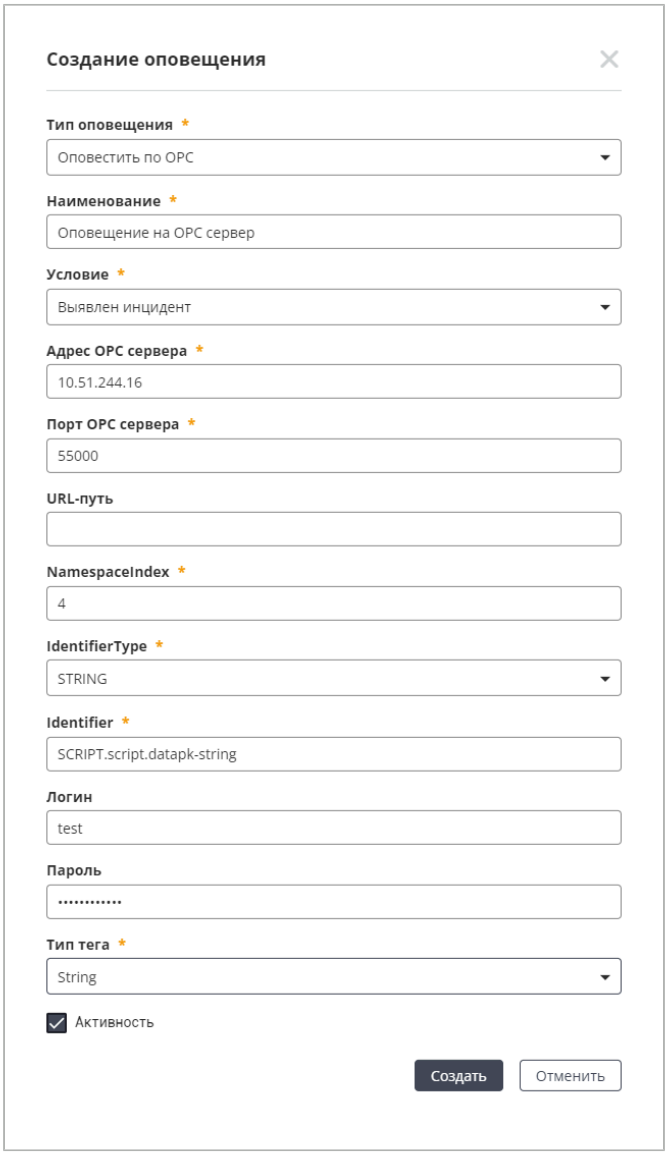


Рис. 146. Окно «Создание оповещения» при настройке оповещения об инцидентах по протоколу OPC

4. Нажмите кнопку **Создать**.

   ▸ **Результат шага:** созданное правило оповещения будет отображаться на странице **Оповещения об инцидентах**.

11.6.7.2.1. Отправка тестового оповещения об инциденте

Для отправки тестового оповещения об инциденте:

1. Перейдите на страницу **Администрирование → События и инциденты → Оповещения об инцидентах**.
2. Наведите курсор на необходимое правило оповещения.
3. Нажмите кнопку (**Отправить тестовое оповещение**).
   - **Результат шага:** появится уведомление **Тестовое оповещение успешно отправлено**.

> Подсказка:
>
> при выборе типа тега `String` оповещения будут приходить в следующем формате:
>
> ```
> Описание события: [Текст с описанием события].
> Инцидент: [Наименование инцидента].
> Дата создания: [Дата и время с указанием часового пояса в формате UTC].
> Активы: [Наименования активов].
> Описание инцидента: [Текст с описанием инцидента].
> Ссылка на инцидент: [Ссылка на инцидент].
> ```

> Внимание:
>
> В случае установки некорректных настроек при отправке тестового оповещения будет отображаться уведомление `Не удается отправить тестовое оповещение: OPC-сервер недоступен, либо один или несколько параметров оповещения имеют некорректные значения`

11.6.7.2.2. Изменение пароля для подключения к OPC-серверу

У ранее созданного правила оповещения можно изменить пароль для подключения к OPC-серверу. Для этого:

1. Перейдите на страницу **Администрирование → События и инциденты → Оповещения об инцидентах**.
2. Нажмите кнопку (**Редактировать оповещение**) в таблице оповещений.
3. В открывшемся окне **Редактирование оповещения** нажмите кнопку **Изменить пароль**.
4. В открывшемся окне **Изменение пароля для подключения к OPC серверу** введите новый пароль в поля **Новый пароль** и **Подтверждение нового пароля** и нажмите кнопку **Сохранить**.

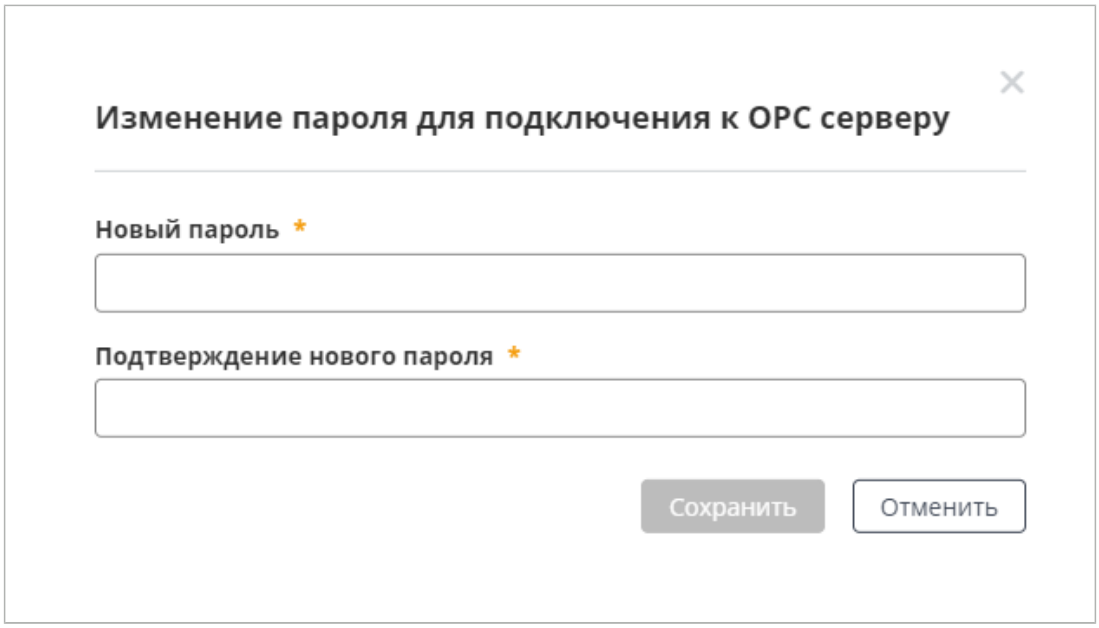


Рис. 147. Окно «Изменение пароля для подключения к OPC серверу»

5. Нажмите кнопку **Сохранить** в окне **Редактирование оповещения**.
   - **Результат шага:** изменения, внесенные в оповещение, будут перезаписаны.

11.6.8. Управление статусами инцидентов

Для изменения состава статусов инцидентов:

1. Перейдите на страницу **Администрирование → События и инциденты → Статусы инцидентов**.
2. Для создания нового статуса инцидента:
   a. Нажмите **Создать статус**.
   - **Результат шага:** появится окно **Создание статуса инцидента**.
   б. В окне создания статуса задайте следующие параметры:
      - категорию статуса инцидента: Новый, В работе или Закрыт;
      - наименование;
      - обоснование создания.

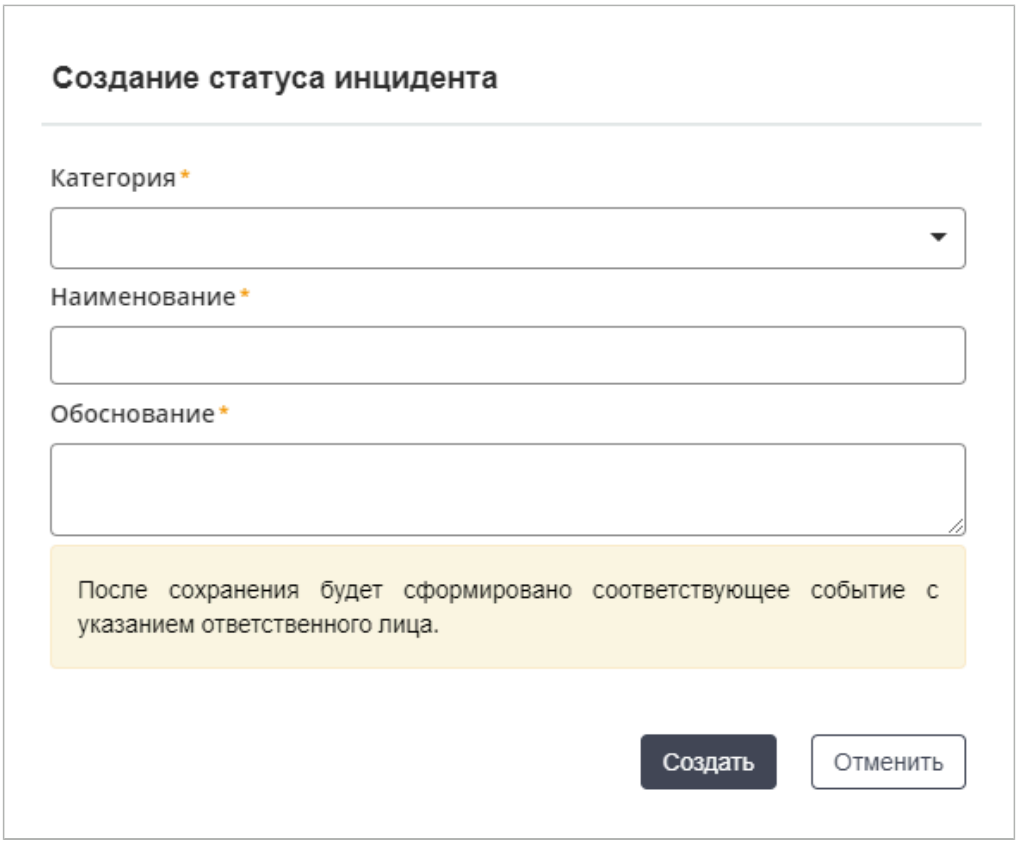


Рис. 148. Окно «Создание статуса инцидента»

в. Нажмите **Создать**.

- **Результат шага:** статус появится на странице и будет доступен для использования.

3. Для редактирования статуса инцидента:

а. Наведите курсор на строку со статусом, который нужно отредактировать.

б. Нажмите (**Редактировать статус**).

- **Результат шага:** появится окно **Редактирование статуса инцидента**.

в. Измените параметры статуса, введите обоснование изменения и нажмите **Сохранить**.

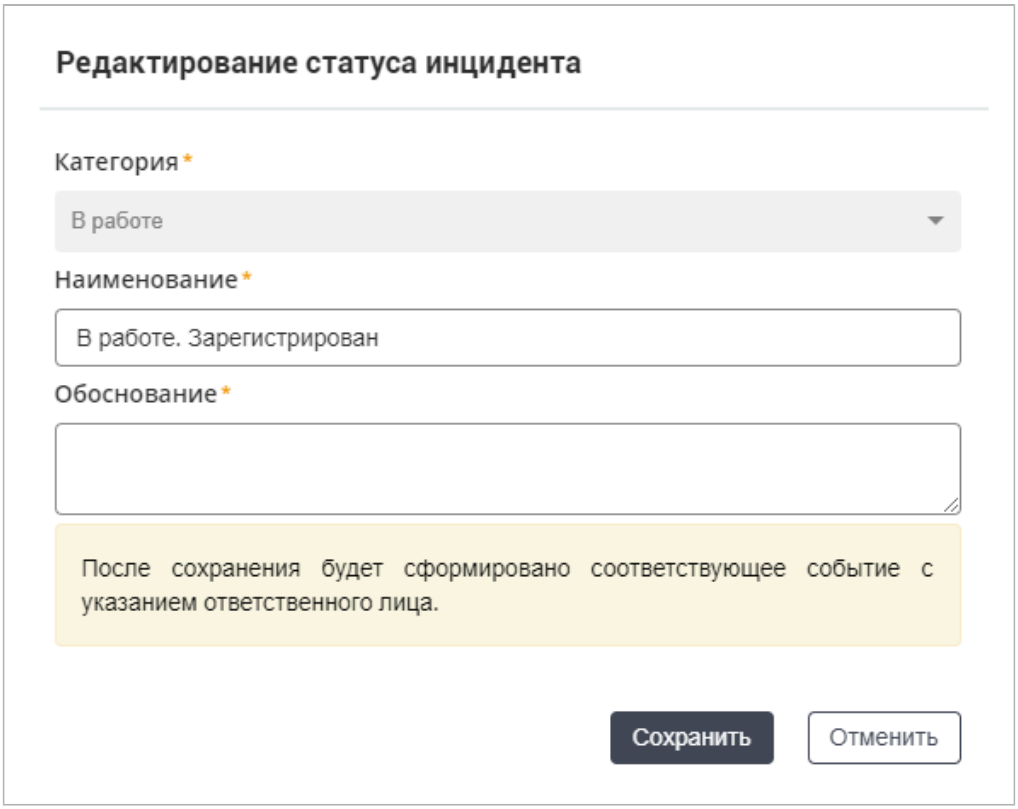


Рис. 149. Окно «Редактирование статуса инцидента»

4. Для удаления одного из статусов инцидентов:
   а. Наведите курсор на строку со статусом, который нужно удалить.
   б. Нажмите (**Удалить статус**).
   - **Результат шага:** появится окно ввода обоснования удаления статуса.

> Внимание:
>
> В окне может появиться предупреждение: `Внимание! В системе присутствуют инциденты с данным статусом. Вы действительно хотите удалить статус?`. Это значит, что статус на момент удаления еще назначен хотя бы одному инциденту. После удаления такого статуса инциденты, которым он был назначен, будут иметь тот же статус, но с отметкой «(удален)».

   в. Введите обоснование удаления статуса и нажмите **Подтвердить**.

11.6.9. Управление внутренними правилами корреляции событий

Для управления внутренними правилами корреляции в Комплексе предусмотрена возможность отключения отдельных внутренних правил корреляции.

Для отключения внутреннего правила корреляции:

1. Войдите в терминал Комплекса под учетной записью `root`.
2. Откройте на редактирование файл `exceptions_rules.json`, выполнив команду:

```
mcedit /usr/share/udv/event-correlator/exceptions_rules.json
```

3. Добавьте в файл номер правила, которое необходимо отключить в Комплексе. Если правил несколько, укажите их через запятую.

   Пример
   `["0001","0004","0005"]`

   Внимание:

   Перечень номеров внутренних правил корреляции представлен в разделе «Список внутренних правил корреляции событий».

4. Сохраните изменения в файле, нажав клавишу **F10**, и подтвердите сохранение изменений, выбрав **Yes**.
5. Перезагрузите службу корреляции внутренних событий, выполнив команду:

```
systemctl restart udv-event-correlator
```

11.7. Выгрузка отчета по инцидентам

Для выгрузки отчета по инцидентам:

1. Перейдите на страницу **Инциденты**.
2. Установите чекбокс возле необходимых инцидентов.
3. В открывшемся внизу меню нажмите **Отчет**.
   - **Результат шага:** откроется окно **Создание отчета по инцидентам**.

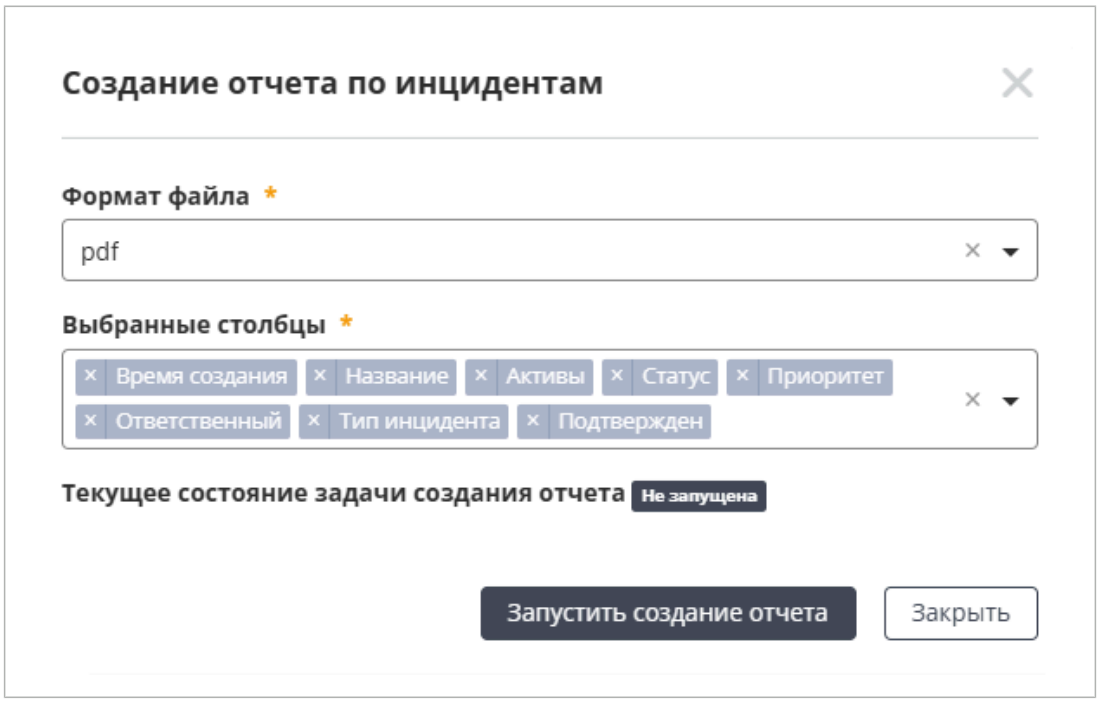


Рис. 150. Окно «Создание отчета по инцидентам»

4. Выберите формат файла отчета из выпадающего списка **Формат файла**. Для выбора доступен формат `html` или `xlsx`.
5. Выберите столбцы, которые будут отражены в отчете.

> Подсказка:
>
> По умолчанию в окне создания отчета указаны те же столбцы, которые ранее были выбраны для отображения в таблице.

6. Нажмите кнопку **Запустить создание отчета**.
   - **Результат шага:** В правом верхнем углу будет отображено всплывающее уведомление `Задача создания отчета запущена`
7. Для сохранения отчета после того, как он сформирован, нажмите на ссылку с названием файла отчета.

12. Работа с активами

В этом разделе:

1. **Экспорт и импорт активов и их групп**
2. **Управление активами**
3. **Создание актива**
4. **Группировка активов**
5. **Редактирование актива**
6. **Удаление активов**
7. **Выгрузка отчета по активам**
8. **Настройки активов**

Актив — это сетевой узел, подлежащий защите от потенциальных угроз и неправомерных действий, например, несанкционированного доступа и изменения данных третьими лицами.

На сводной странице **Активы** отображается список всех найденных автоматически и добавленных пользователем активов. На странице присутствуют широкие возможности фильтрации и перехода к отдельным страницам различных аспектов активов (карточка актива, события, инциденты, учетные данные актива, конфигурации), кнопки экспорта, импорта, поиска уязвимостей, создания отчетов и удаления активов, столбцы статусов и статистики по сбору данных, отклонениям конфигураций, инцидентам, уязвимостям.

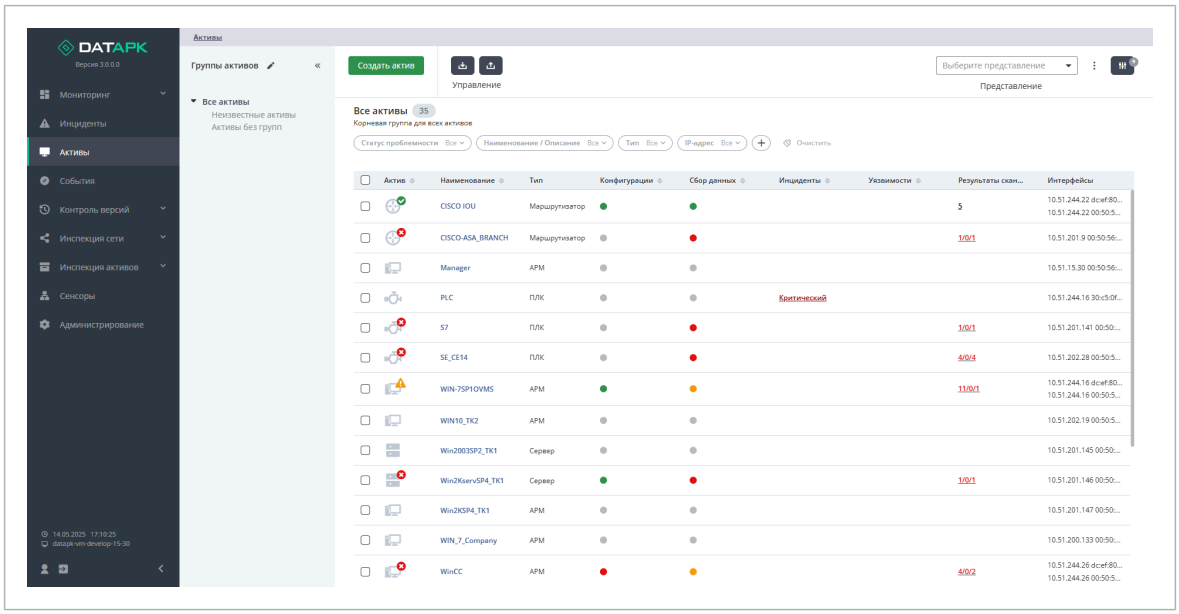


Рис. 151. Страница «Активы»

На основе данных из трафика Комплекс может автоматически определять следующие параметры актива:

- IP и MAC-адреса интерфейсов;
- производителя;
- тип актива;
- операционную систему (для активов с типом `ПЛК` — прошивку) и ее версию;
- по наличию трафика — доступность актива.

На странице **Активы** доступно табличное представление списка активов с возможностью сортировки по столбцам. В таблице можно настроить отображение столбцов со статусами и статистикой по выполненным операциям активного сбора данных и по обнаруженным инцидентам и уязвимостям.

> Подсказка:
>
> Подробнее о статусах активов см. разделы «Статусы активов» и «Цветовая индикация активов».

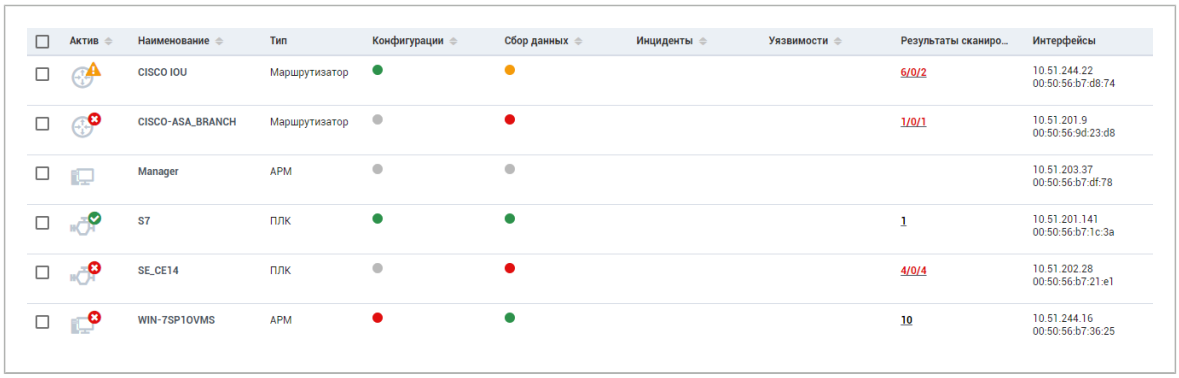


Рис. 152. Табличное представление активов

После обнаружения активов или добавления их вручную доступна группировка активов, используемая при последующем сборе данных, а также для управления активами, входящими в группы.

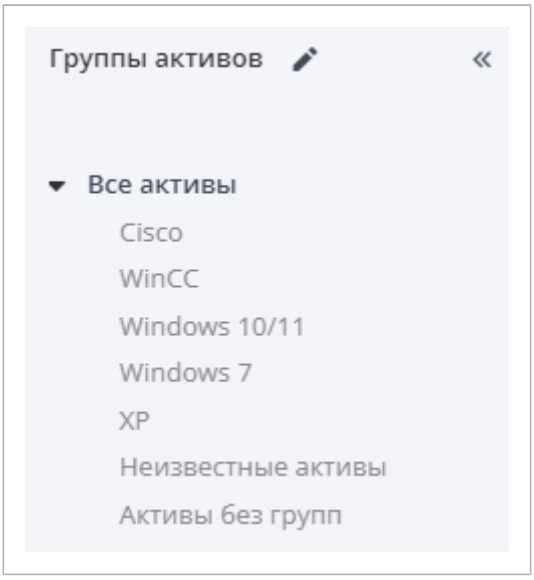


Рис. 153. Панель управления группами активов

По нажатию на иконку актива или его наименование появляется **Карточка актива**, отображающая:

- описание актива: наименование, описание, производитель, тип, группа, АСУ ТП, дата и время создания, дата и время, когда актив последний раз был доступен;
- учетные данные;
- информацию об ОС (для активов с типом ПЛК — информацию о прошивке): дату и время последнего изменения указанных данных, производителя, наименование и версию ОС;
- сетевые атрибуты: название, IP и MAC-адреса;
- набор присвоенных меток со страницы **Классификаторы**;
- статистику по задачам сбора данных, собранным конфигурациям, инцидентам и уязвимостям;
- связанные данные, позволяющие просмотреть данные об активе в других разделах:

- инциденты
- конфигурации
- события
- сессии
- источники
- учетные данные актива
- перечень ПО, установленного на активе

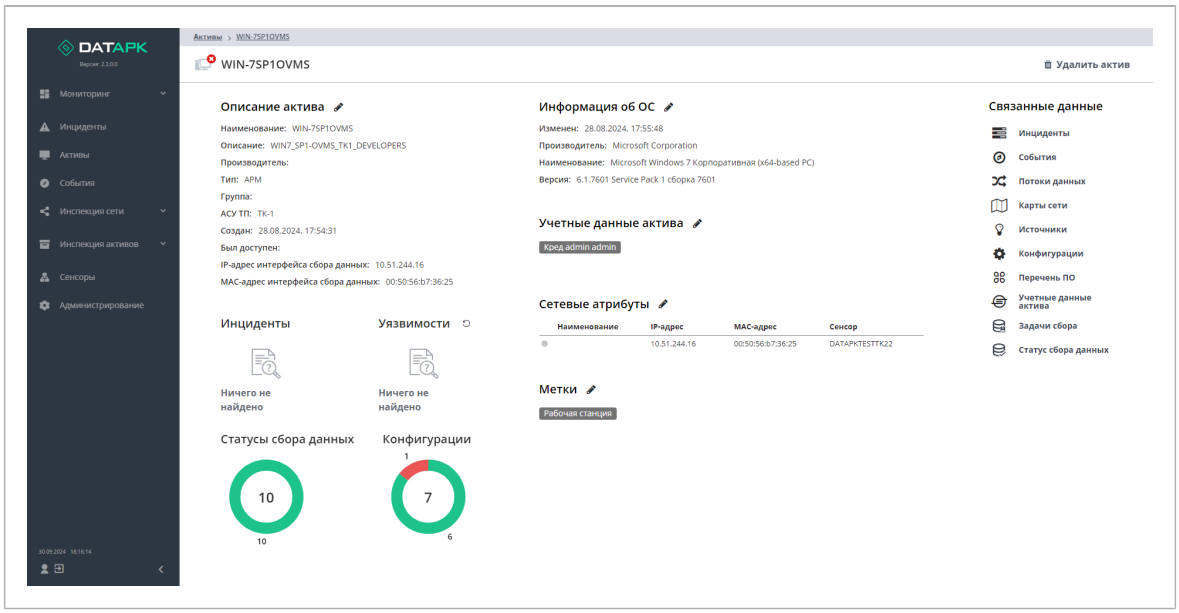


Рис. 154. Карточка актива

12.1. Экспорт и импорт активов и их групп

В этом разделе:

- Экспорт активов
- Экспорт групп активов
- Импорт активов
- Импорт групп активов

Экспорт и импорт активов доступен на странице **Активы** на панели **Управление**.

Экспорт и импорт групп активов доступен на странице **Администрирование** → **Основные настройки** → **Импорт и экспорт** на панели **Элементы иерархии**.

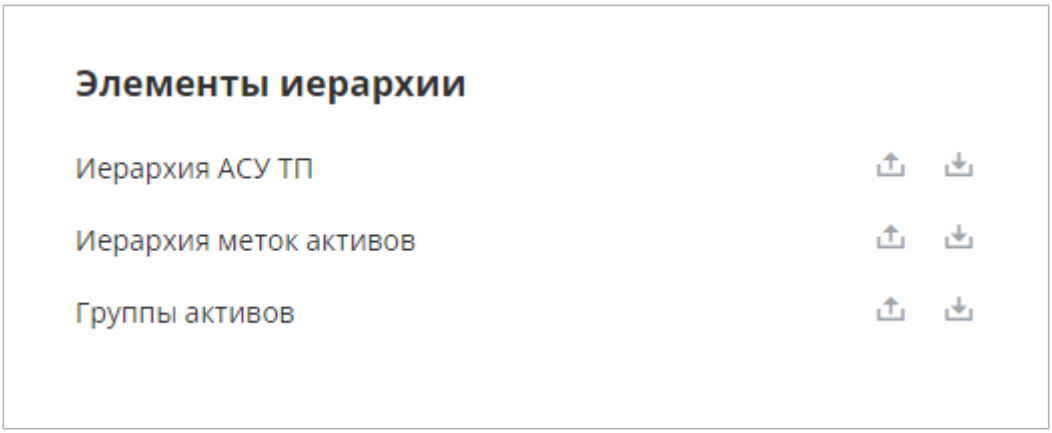


Рис. 155. Панель «Элементы иерархии» на странице «Импорт и экспорт»

12.1.1. Экспорт активов

> Прим.:
>
> Экспорт выполняется для всех активов, их групп, меток, АСУ ТП, независимо от выбора и фильтрации активов.

Для экспорта всех активов в файл формата `json`:

1. Перейдите на страницу **Активы**.
2. Нажмите кнопку (**Экспортировать активы**) на панели **Управление** в верхней части страницы.
   - **Результат шага:** откроется окно выбора папки для хранения экспортируемого файла `hosts_[дата.время].json`.
3. В открывшемся окне укажите расположение для экспортируемого файла, при необходимости изменив его название, и нажмите кнопку **Сохранить**.
   - **Результат шага:** файл `*.json` будет загружен на компьютер.

   > Прим.:
   >
   > Сохраненный файл, при необходимости, можно импортировать на тот же Комплекс, с которого он экспортирован (см. инструкцию «Импорт активов»).

12.1.2. Экспорт групп активов

> Внимание:
>
> Файл `asset_groups_[дата-время].json` со справочником групп активов содержит наименования и иерархию групп без связи с активами, поэтому после импорта справочника активы в группы необходимо добавить вручную.

Для экспорта справочника групп активов в файл формата `*.json`:

1. Перейдите на страницу **Администрирование → Основные настройки → Импорт и экспорт**.
2. На панели **Элементы иерархии** в строке **Группы активов** нажмите кнопку (**Экспортировать**) .

- **Результат шага:** файл со списком групп активов `asset_groups_[дата-время].json` будет сформирован и доступен для скачивания в правом верхнем углу страницы **Импорт и экспорт** под заголовком **Результат последнего экспорта**

3. Для скачивания файла нажмите на название сформированного файла под заголовком **Результат последнего экспорта**.
4. В открывшемся окне укажите расположение для экспортируемого файла, при необходимости изменив его название, и нажмите кнопку **Сохранить**.
   - **Результат шага:** файл `asset_groups_[дата-время].json` будет загружен на компьютер.

12.1.3. Импорт активов

> Внимание:
>
> Импорт на Комплекс выполняется только для активов, экспортированных с того же Комплекса. Перенос активов между разными Комплексами не поддерживается.
>
> Импорт активов не требуется после восстановления Комплекса из резервной копии, поскольку все активы в этом случае восстанавливаются автоматически.

Для импорта активов из файла формата `*.json` в Комплекс:

1. Перейдите на страницу **Активы**.
2. Нажмите кнопку (**Импортировать актив**) на панели **Управление** в верхней части страницы.
3. В открывшемся окне **Импорт активов** нажмите левой кнопкой мыши на область выбора файла или перетащите файл из проводника. В открывшемся окне укажите расположение импортируемого файла формата `*.json` и подтвердите выбор.

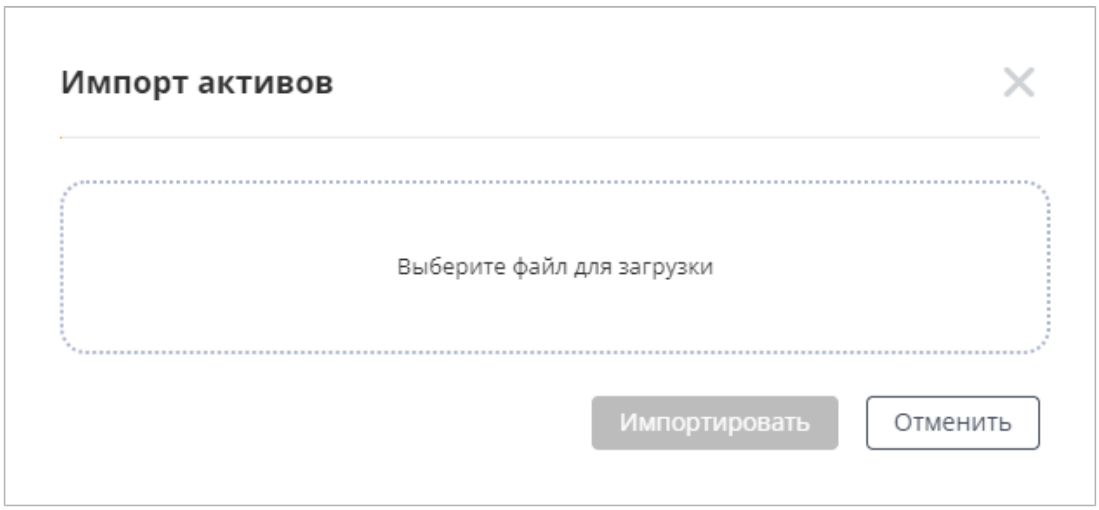


Рис. 156. Окно «Импорт активов»

4. Нажмите кнопку **Импортировать** для выполнения импорта списка активов.
5. Убедитесь, что на странице **Активы** активы успешно импортированы из файла.

12.1.4. Импорт групп активов

> Внимание:
>
> Файл формата `.json` со справочником групп активов содержит наименования и иерархию групп без связи с активами, поэтому после импорта справочника активы в группы необходимо добавить вручную.

Для импорта справочника групп активов из файла формата `.json` в Комплекс:

1. Перейдите на страницу **Администрирование → Основные настройки → Импорт и экспорт**.
2. На панели **Элементы иерархии** в строке **Группы активов** нажмите кнопку (**Импортировать**).
3. В открывшемся окне укажите расположение импортируемого файла формата `.json` и подтвердите выбор.
   - **Результат шага:** появится окно подтверждения импорта.
4. Нажмите **Импортировать**.

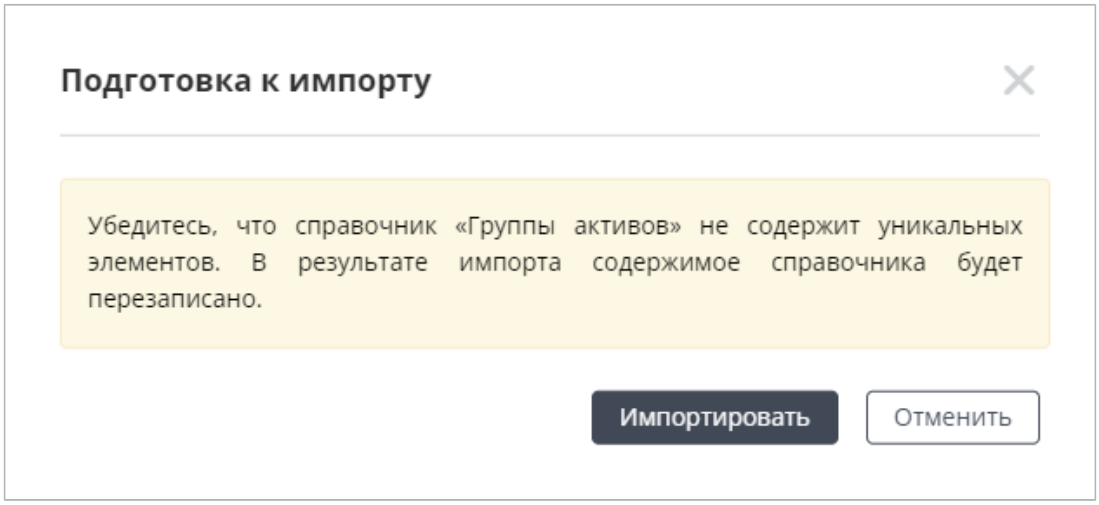


Рис. 157. Окно «Подготовка к импорту» при импорте групп активов

5. Убедитесь, что группы активов были успешно загружены.
   - **Результат шага:** сразу после загрузки файла в правом верхнем углу страницы в поле **Результат последнего импорта** появится статус `Успешно`, и группы активов будут загружены на страницу **Активы**.
6. Перейдите на страницу **Активы** и убедитесь, что группы активов были успешно загружены.

См. также

Добавление активов в группу

12.2. Управление активами

В этом разделе:

- Кнопки управления активами
- Фильтрация списка активов

12.2.1. Кнопки управления активами

На странице **Активы** расположен ряд кнопок для управления активами. Ознакомиться со списком кнопок в верхней части страницы вы можете в таблице ниже (Таблица 15. Кнопки управления активами в верхней части страницы).

Табл. 15. Кнопки управления активами в верхней части страницы

КНОПКА	ДЕЙСТВИЕ	РАЗДЕЛ ДОКУМЕНТАЦИИ	УСЛОВИЯ ДОСТУПНОСТИ
Создать актив	Создание актива	Создание актива	—
	Экспорт активов	Экспорт активов	Выполняется для всех активов независимо от того, какие активы были выбраны или отфильтрованы
	Импорт активов	Импорт активов	Выполняется только для активов, экспортированных с того же Комплекса. Перенос активов между разными Комплексами не поддерживается. Импорт активов не требуется после восстановления Комплекса из резервной копии, поскольку все активы в этом случае восстанавливаются автоматически

Рис. 158. Кнопки управления активами

При выборе одного или нескольких активов с помощью чекбоксов внизу появляется меню с кнопками для дополнительного управления выбранными активами. Ознакомиться со списком кнопок в верхней части страницы вы можете в таблице ниже (Рисунок 159. Нижнее меню на странице «Активы»).

Подсказка:

Для выделения множества строк выше или ниже выбранной нажмите клавишу **Shift** и выделите строку с последним активом, который необходимо добавить в группу.

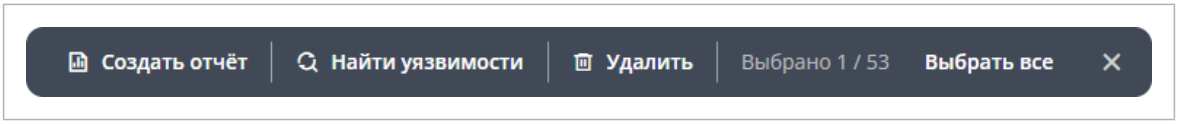


Рис. 159. Нижнее меню на странице «Активы»

Табл. 16. Кнопки управления активами в нижнем меню

КНОПКА	ДЕЙСТВИЕ	РАЗДЕЛ ДОКУМЕНТАЦИИ
Найти уязвимости	Поиск уязвимостей в базе CVE для выбранных активов	Поиск уязвимостей ПО и ОС в базах CVE, CPE и БДУ ФСТЭК России
Удалить	Групповое удаление выбранных активов	Удаление активов
Создать отчёт	Создание отчета по выбранным активам	Выгрузка отчета по активам

При нажатии в любом месте в строке с активом (кроме его иконки и наименования) справа открывается боковая панель с подробной информацией об активе. Ссылки на смежные страницы для просмотра подробной информации, связанной с активом, доступны в блоках **Аудит безопасности** и **Связанные данные**.

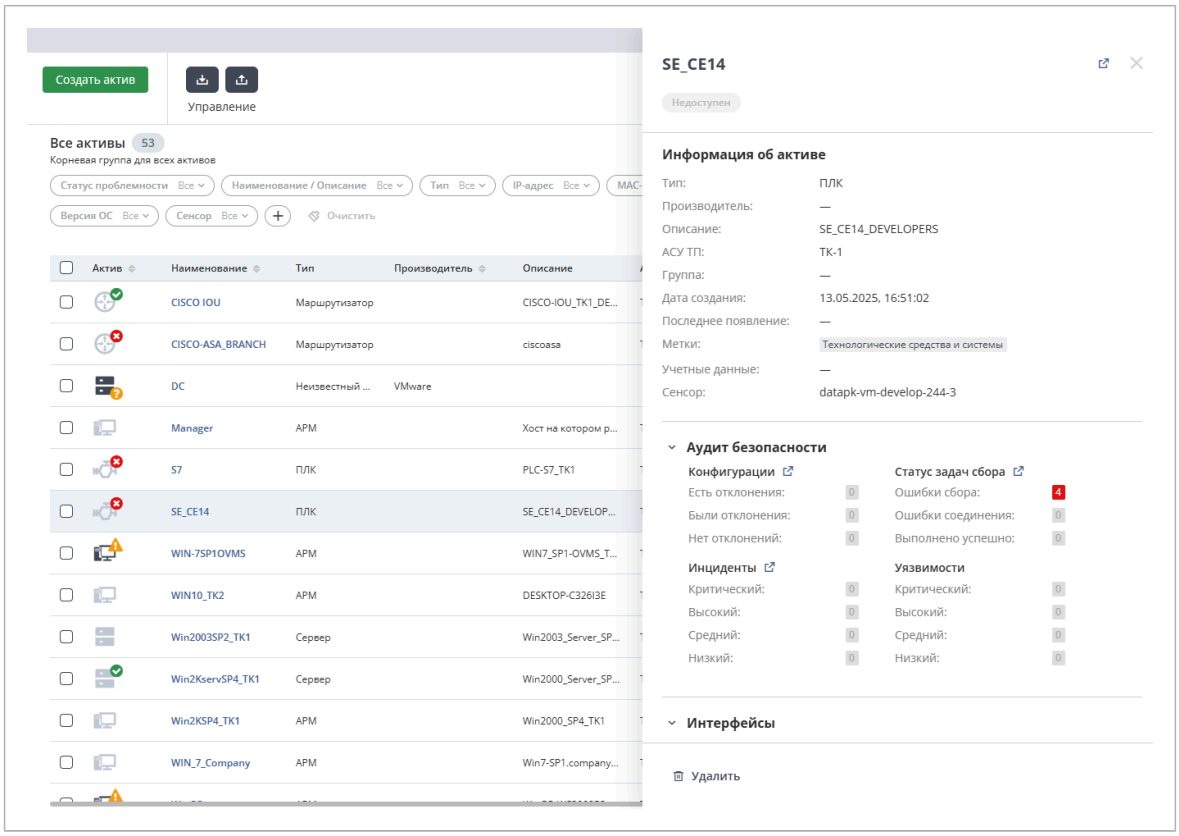


Рис. 160. Боковая панель с подробной информацией о выбранном активе

12.2.2. Фильтрация списка активов

Комплекс позволяет фильтровать обнаруженные активы.

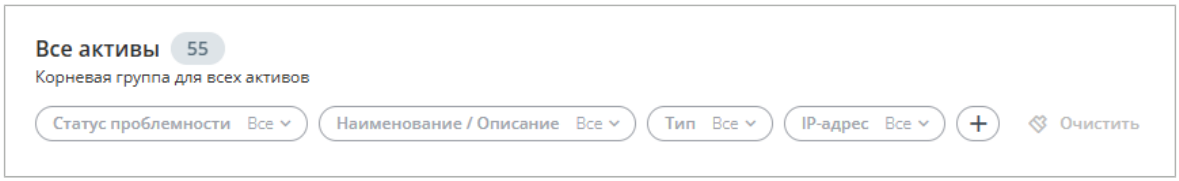


Рис. 161. Панель фильтров на странице «Активы»

На странице **Активы** над списком активов доступны следующие фильтры:

1. **Статус проблемности**. Статусы **Сбор данных** и **Конфигурации** формируют единый показатель активa **Статус проблемности**. Проблемность для каждого актива принимает одно из следующих значений:
    - **Критический**: хотя бы один из статусов актива — **Сбор данных** или **Конфигурации** — имеет красный индикатор.
    - **Важный**: хотя бы один из статусов актива — **Сбор данных** или **Конфигурации** — имеет оранжевый индикатор, но красные индикаторы отсутствуют.
    - **ОК**: оба статуса имеют зеленый индикатор.
    - **Нет данных**: сбор данных не выполнялся.

    > Подсказка:
    >
    > Подробнее о статусах **Сбор данных** и **Конфигурации** см. раздел «Статусы активов».

    В данном фильтре можно выбирать несколько значений.
2. **Наименование/Описание.** Фильтрация активов по наименованию или описанию выполняется прямо в фильтре следующим образом:
    a. Начните вводить наименование или описание активов — отобразится список найденных активов.
    b. Выберите необходимые активы из списка найденных.
    c. Нажмите кнопку **Применить** — результаты поиска отобразятся на странице.

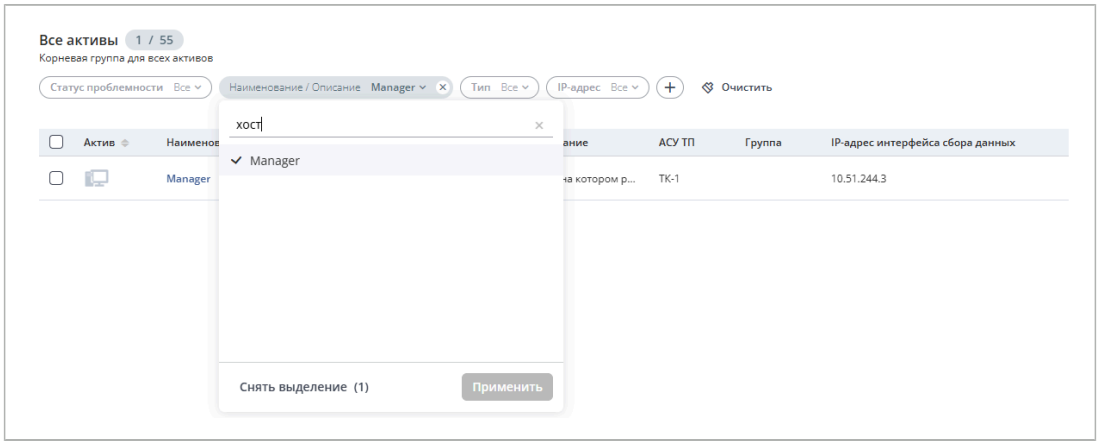


Рис. 162. Результаты поиска среди значений фильтра «Наименование/Описание»

3. **Тип**. Фильтрация по типам, назначенным активам. Можно выбирать несколько значений из списка.
4. **IP-адрес**. Фильтрация по IP-адресам, привязанным к сетевым атрибутам активов. Фильтрация выполняется следующим образом:

a. Полностью введите в поле IP-адрес, диапазон адресов или подсеть.

> Прим.:
>
> Диапазон IP-адресов задается через дефис. Подсеть задается в формате CIDR.

b. Для подтверждения ввода значения нажмите клавишу **Space**, **Tab** или **Enter**, либо нажмите левой кнопкой мыши рядом со значением. Корректное значение будет иметь серый цвет, некорректное — красный.
c. Повторите пункты 4.a-4.b для других IP-адресов, по которым необходимо отфильтровать активы.
d. Нажмите кнопку ✔ — результаты поиска отобразятся на странице.

5. **MAC-адрес**. Фильтрация по MAC-адресу, привязанному к сетевому атрибуту актива. Для ввода в поле разрешены цифры и английские символы. Можно ввести только одно значение.

> Внимание:
>
> Вводить разделители для октетов MAC-адресов не требуется — при вводе цифр или английских символов разделитель `:` устанавливается автоматически при необходимости.

6. **Производители**. Фильтрация по наименованиям производителей аппаратного обеспечения актива, информация о которых получена Комплексом. Можно выбирать несколько значений из списка.
7. **АСУ ТП**. Фильтрация по наименованиям классификаторов АСУ ТП, назначенным активам. Можно выбирать несколько значений из списка.
8. **Метки**. Фильтрация по меткам, назначенным активам. Можно выбирать несколько значений из списка.
9. **Производитель ОС**. Фильтрация по ключевому слову среди наименований производителей ОС или прошивок, информация о которых получена Комплексом.
10. **ОС**. Фильтрация по ключевому слову среди наименований ОС или прошивок, информация о которых получена Комплексом.
11. **Версия ОС**. Фильтрация выполняется по ключевому слову среди версий ОС или прошивок, информация о которых получена Комплексом.
12. **Сенсор**. Фильтр содержит наименования сенсоров, подключенных к Комплексу. Можно выбирать несколько наименований из списка. При применении фильтра отобразятся активы, чьи основные интерфейсы сбора данных привязаны к выбранным сенсорам.

> Внимание:
>
> Групповое удаление активов будет недоступно при следующих условиях, выполненных одновременно:
>
> - Применен хотя бы один из фильтров: **Статус проблемности**, **Производитель ОС**, **ОС**, **Версия ОС**.
> - По результатам фильтрации получилось больше 100 записей.
> - Применено действие **Выбрать все записи (>100) в данной таблице**.

12.3. Создание актива

В Комплексе предусмотрено создание новых активов в ручном режиме. Для создания нового актива:

1. Перейдите на страницу **Активы**.
2. Нажмите кнопку **Создать актив** в верхней части страницы.
3. В открывшемся окне **Создание актива** задайте параметры для нового актива в следующем порядке:
    а. Выберите тип актива.

> Подсказка:
>
> При выборе любого типа актива, кроме `Неизвестный тип` и `Комплекс`, для редактирования станет доступным поле **Наименование**.

    б. Введите наименование в зависимости от выбранного типа Актив:
        - при выборе типа `Сенсор` выберите из выпадающего списка наименование сенсора, подключенного к текущему Комплексу;
        - при выборе типа `Комплекс` наименование актива будет присвоено автоматически;
        - в остальных случаях введите наименование актива вручную.
    в. При необходимости введите описание, выберите АСУ ТП и укажите группу.
    г. При необходимости введите наименование производителя.

> Внимание:
>
> При создании актива невозможно автоматическое распознавание производителя по нажатию кнопки **определить**.

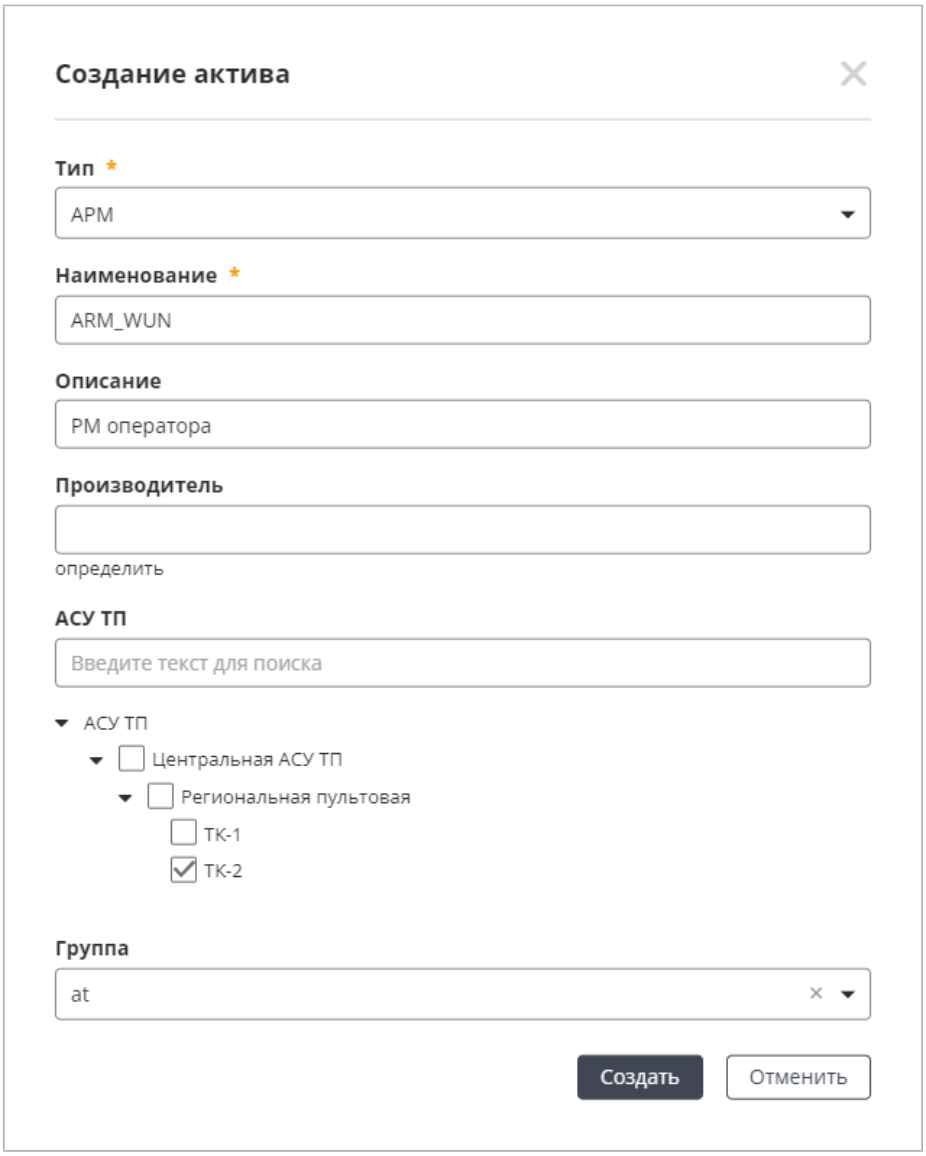


Рис. 163. Окно создания нового актива

4. Нажмите кнопку **Создать** для подтверждения изменений.

12.4. Группировка активов

В этом разделе:

- Создание группы активов
- Добавление активов в группу
- Управление группами активов

Активы с типом, отличным от неизвестного, можно собирать в группы. Эти группы используются в задачах сбора данных и для упрощения управления активами.

По умолчанию доступны следующие группы:

- **Неизвестные активы** — группа, в которую автоматически добавляются все активы с типом `Неизвестный тип`;
- **Активы без групп** — группа, в которую автоматически добавляются все активы, у которых не заполнено поле **Группа**.

Удаление и редактирование этих групп, а также добавление активов в эти группы вручную и удаление активов из этих групп недоступно.

Список групп отображается на панели в левой части экрана. Если в списке выбрана конкретная группа активов, то фильтры будут применяться только для элементов этой группы.

12.4.1. Создание группы активов

Для создания группы активов:

1. Перейдите на страницу **Активы**.

> Подсказка:
>
> Управление группами активов также доступно на странице **Задачи сбора**.

2. Над панелью с группами активов в левой части страницы нажмите (**Редактировать**).
   - **Результат шага:** появится окно **Редактирование групп активов**.
3. Нажмите кнопку напротив группы, которая будет вышестоящей для создаваемой.

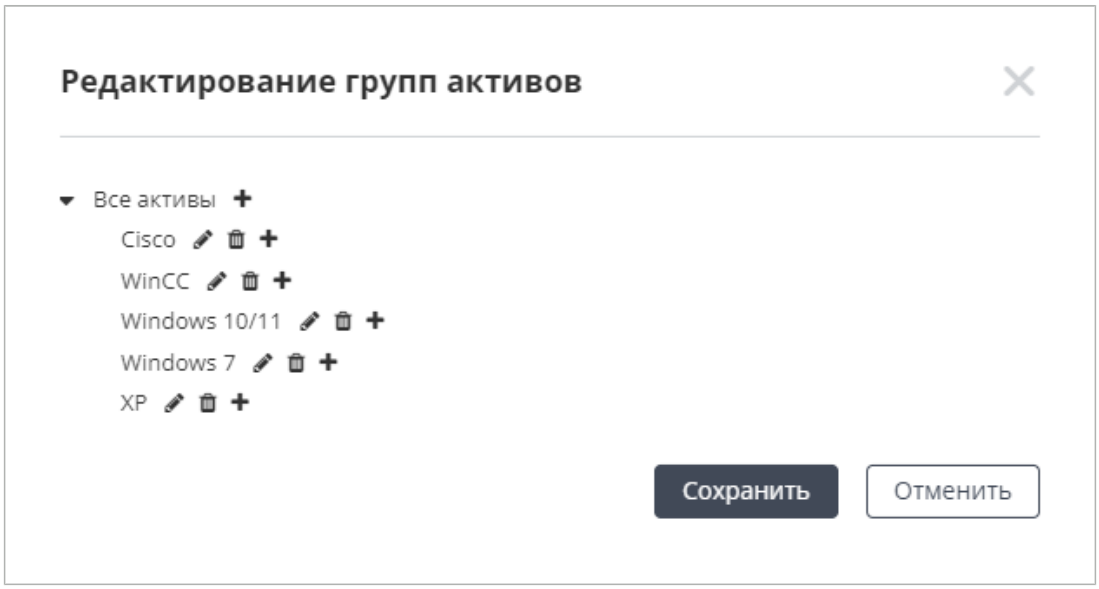


Рис. 164. Окно «Редактирование групп активов»

   - **Результат шага:** появится окно **Создание группы активов**.
4. В окне создания задайте наименование и описание новой группы. При необходимости выберите другую вышестоящую группу.

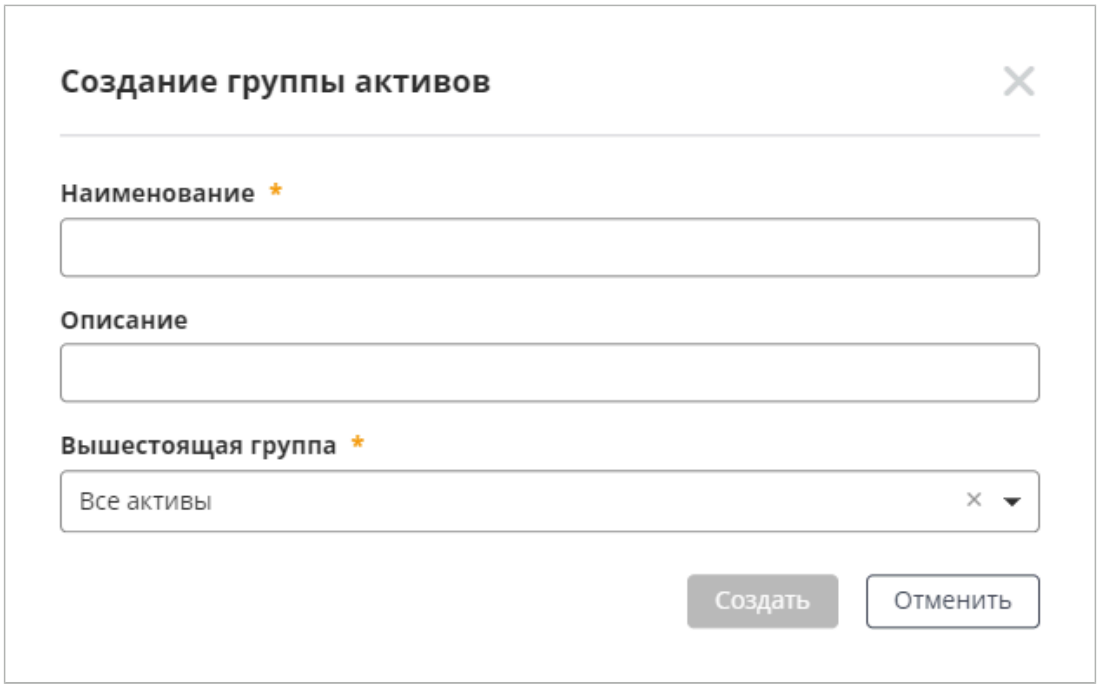


Рис. 165. Окно «Создание группы активов»

5. Нажмите кнопку **Создать** для подтверждения локальных изменений.

> Внимание:
>
> Без сохранения в окне редактирования групп в шаге 7 изменения не будут отражены в Комплексе.

   - **Результат шага:** созданная группа появится в списке в окне **Редактирование групп активов**.
6. При необходимости добавьте другие группы активов.
7. В окне **Редактирование групп активов** нажмите **Сохранить**.
   - **Результат шага:** появится предупреждение о неизменности задач сбора данных в результате изменения состава групп.
8. Нажмите **Подтвердить** для сохранения изменения состава групп.
   - **Результат шага:** изменения групп будут сохранены, окно редактирования групп будет закрыто, появится уведомление `Список "Группы активов" успешно обновлен.`

12.4.2. Добавление активов в группу

> Внимание:
>
> Актив может находиться только в одной группе.

Для добавления активов в ранее созданную группу активов:

1. Перейдите на страницу **Активы**.
2. При необходимости отфильтруйте список активов — подробнее см. раздел «Фильтрация списка активов».
3. Убедитесь, что активам, которые будут добавлены в группу, назначен тип, отличный от неизвестного.
4. Добавьте активы в группу. Для этого:

а. Отметьте все отфильтрованные активы с помощью чекбокса в заголовке таблицы, либо отметьте с помощью чекбоксов рядом с активами, отдельные активы, которые необходимо добавить в группу.

> Подсказка:
>
> Для выделения множества строк выше или ниже выбранной нажмите клавишу **Shift** и выделите строку с последним активом, который необходимо добавить в группу.

б. Наведите курсор на один из выделенных активов и зажмите левую кнопку мыши.

- **Результат шага:** появится полупрозрачный квадрат с количеством выделенных активов.

в. Не отпуская левую кнопку мыши, перетащите активы в левую часть страницы так, чтобы курсор оказался на наименовании группы, в которую будут перемещены активы.

г. Отпустите левую кнопку мыши.

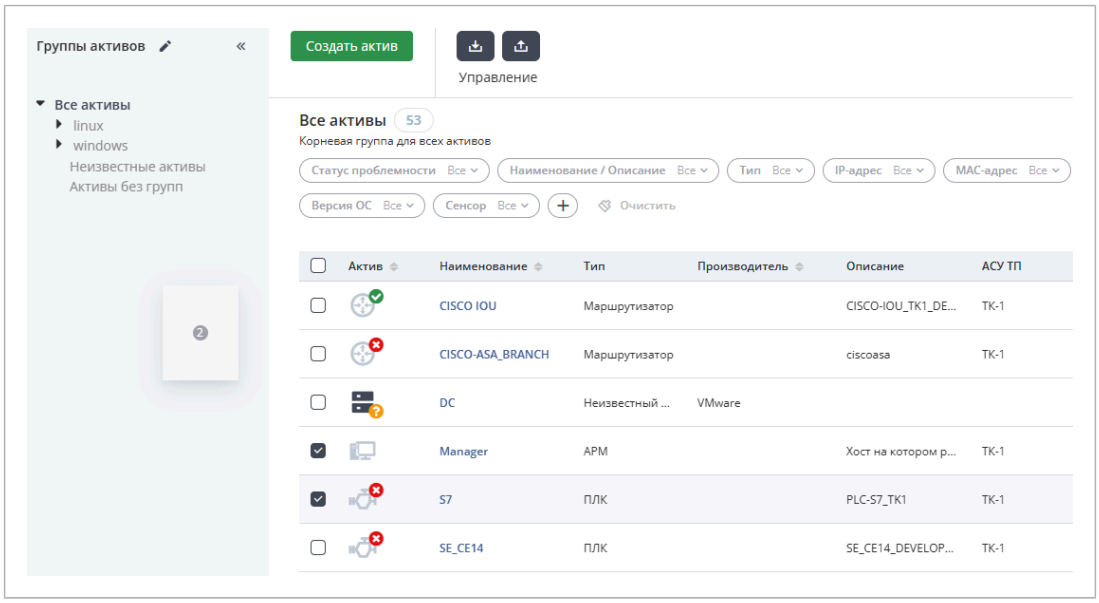


Рис. 166. Добавление активов в группу

- **Результат шага:** появится окно подтверждения добавления активов в группу.

5. Для подтверждения переноса нажмите **Подтвердить**.

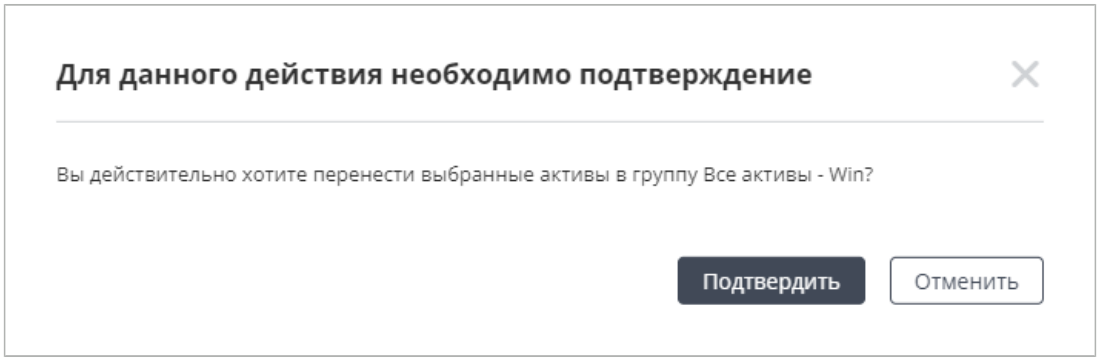


Рис. 167. Окно подтверждения перемещения актива

- **Результат шага:** активы будут перенесены в группу. В правом верхнем углу экрана появится уведомление `Перемещение активов прошло успешно`.

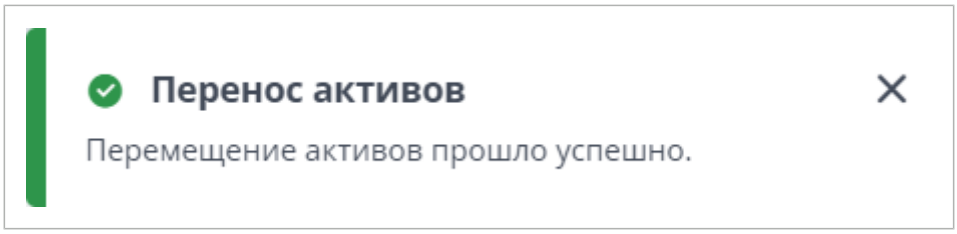


Рис. 168. Уведомление «Перемещение актива прошло успешно»

6. При необходимости изменить группу можно также в карточке актива. Для этого:
   а. Откройте карточку актива.
   б. Нажмите (**Редактировать**) напротив подзаголовка **Описание актива**.
   - **Результат шага:** появится окно **Основная информация об активе**.

   в. Измените значение поля **Группа**.
   г. Нажмите **Сохранить**.
   - **Результат шага:** группа актива будет изменена.

Что дальше: Если необходимо исключить актив из группы, аналогично измените соответствующее поле в окне **Основная информация об активе**.

12.4.3. Управление группами активов

Управление группами активов может осуществляться на страницах **Активы** и **Задачи сбора**. Возможности для управления группами активов:

1. Изменение группы. Для изменения:
   а. Над панелью с группами активов в левой части страницы нажмите кнопку (**Редактировать**).
   - **Результат шага:** появится окно **Редактирование групп** Актив.

   б. Нажмите кнопку (**Редактировать**) напротив группы, которую необходимо изменить.

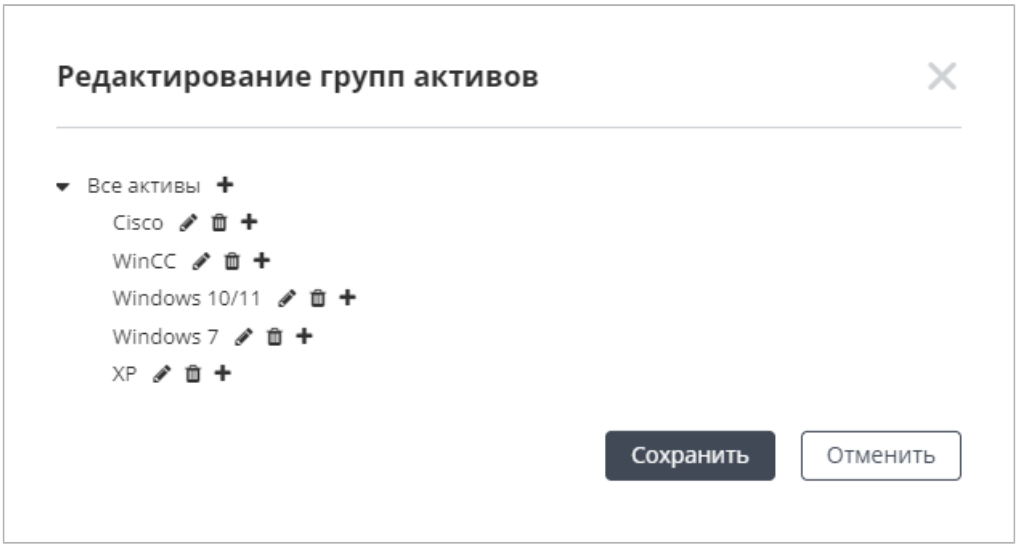


Рис. 169. Окно «Редактирование групп активов»

   - **Результат шага:** появится окно **Редактирование группы активов**.

   в. Измените необходимые параметры группы активов.

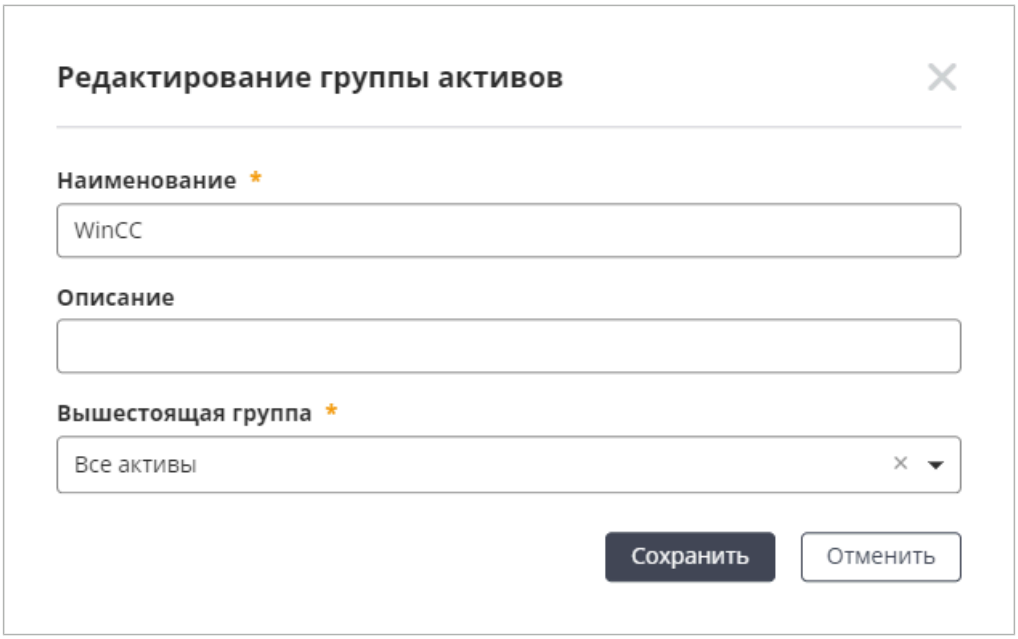


Рис. 170. Окно «Редактирование группы активов»

г. Нажмите кнопку **Сохранить** для подтверждения локальных изменений.

> Внимание:
>
> Без сохранения изменения в окне редактирования групп не будут отражены в Комплексе.

- **Результат шага:** изменения названия группы появятся в окне **Редактирование групп активов**.

д. При необходимости измените другие группы активов.

е. В окне **Редактирование групп активов** нажмите **Сохранить**.

- **Результат шага:** появится предупреждение о неизменности задач сбора данных в результате изменения состава групп.

ж. Нажмите **Подтвердить** для сохранения изменения состава групп.

- **Результат шага:** изменения будут сохранены, окно редактирования групп будет закрыто, появится уведомление `Список "Группы активов" успешно обновлен.`

2. Удаление группы. Для удаления:

а. Над панелью с группами активов в левой части страницы нажмите кнопку (**Редактировать**).

- **Результат шага:** появится окно **Редактирование групп активов**.

б. Нажмите кнопку (**Удалить**) напротив группы, которую необходимо удалить.

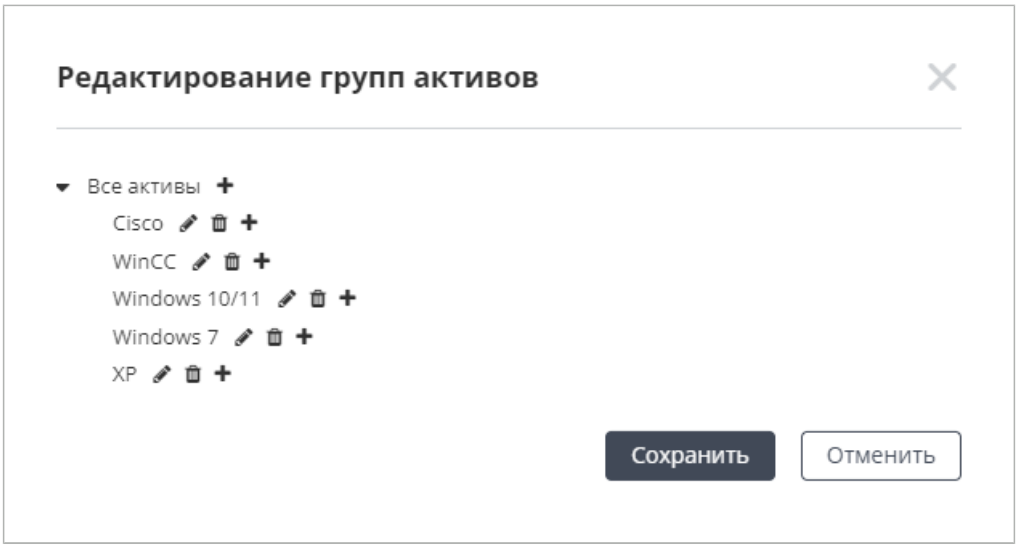


Рис. 171. Окно «Редактирование групп активов»

- **Результат шага:** группа активов будет удалена, но данные изменения не будут сохранены до нажатия **Сохранить** в окне редактирования групп активов.

в. При необходимости измените другие группы активов.

г. В окне **Редактирование групп** Актив нажмите **Сохранить**.

- **Результат шага:** появится предупреждение о неизменности задач сбора данных в результате изменения состава групп. Это значит, что удаляемые группы останутся в задачах сбора данных, если такие были созданы. Для возобновления периодического сбора измените или создайте задачи заново, в том числе при помощи копирования.

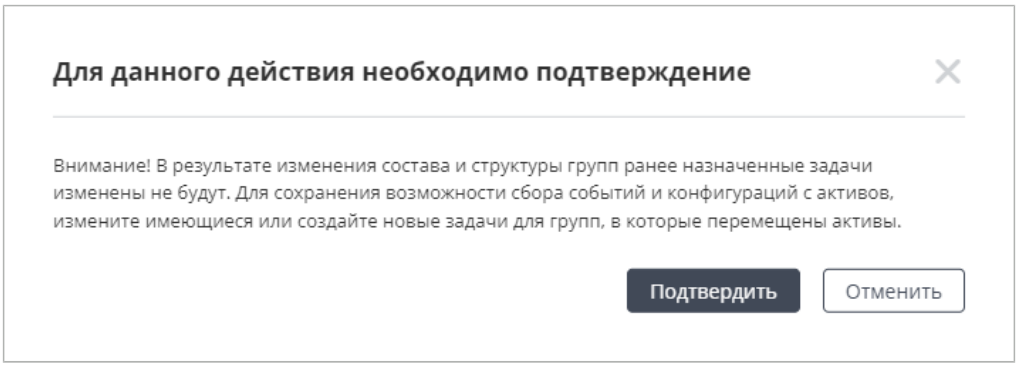


Рис. 172. Окно подтверждения изменений групп

д. Нажмите **Подтвердить** для сохранения изменения состава групп.

- **Результат шага:** изменения будут сохранены, окно редактирования групп будет закрыто.

12.5. Редактирование актива

Для редактирования актива:

1. Перейдите на страницу **Активы**.
2. Нажмите на иконку или наименование актива.

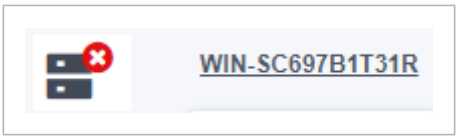


Рис. 173. Переход к карточке актива

- **Результат шага:** отобразится **Карточка актива**.

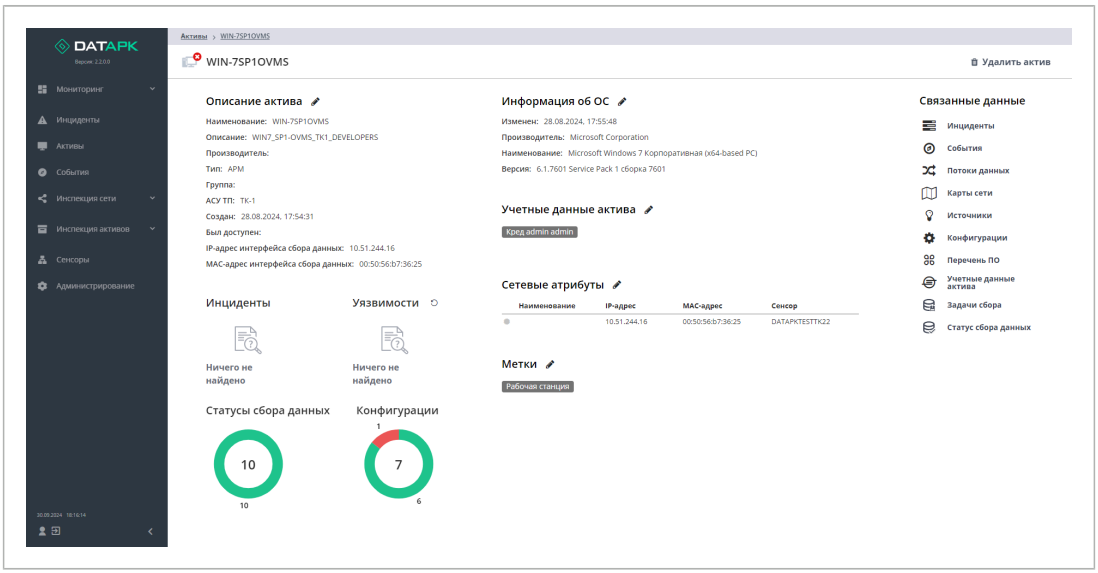


Рис. 174. Карточка актива

3. Убедитесь в доступности актива для Комплекса. Для этого между активом и прослушивающими интерфейсами Комплекса должен присутствовать сетевой трафик.

> Подсказка:
>
> Если актив доступен, его индикатор будет иметь темно-синий цвет. Подробнее об индикации активов см. в разделе «Цветовая индикация и виды уведомлений».

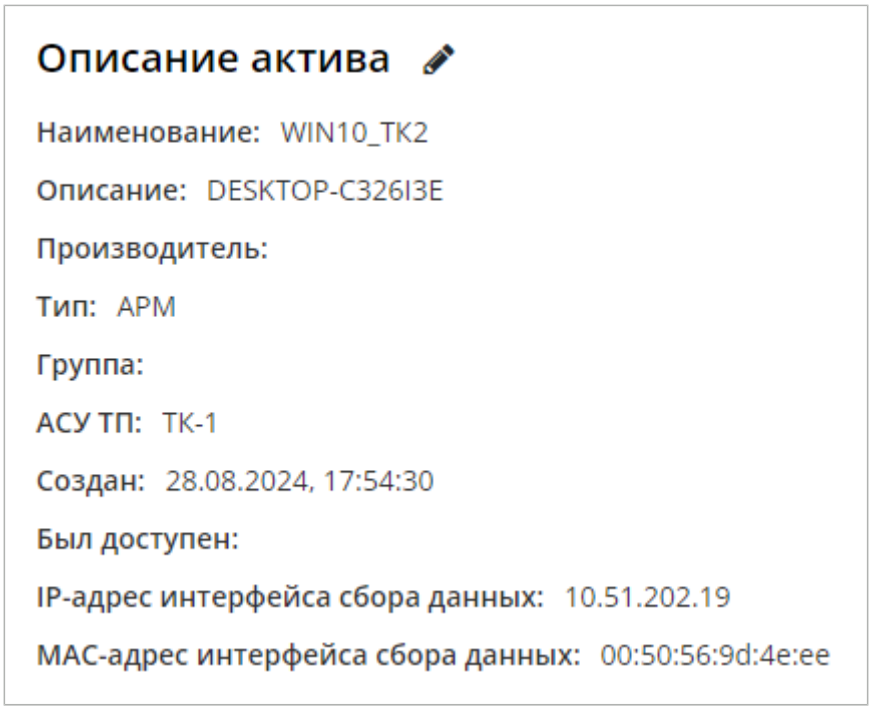


Рис. 175. Содержание полей блока «Описание актива»

4. Для редактирования общей информации об активе:
    a. Нажмите кнопку (**Редактировать**) напротив блока **Описание актива**.
    - **Результат шага:** появится окно **Основная информация об активе**.
    б. Измените необходимые параметры актива:
    - тип и наименование актива;

> Внимание:
>
> - Повторное присвоение активу типа `Неизвестный тип` будет запрещено, если ранее он был сохранен с другим типом.
> - Если активу назначен новый тип `Сенсор`, в качестве нового наименования необходимо выбрать из выпадающего списка сенсор, подключенный к текущему Комплексу.
> - Если активу назначен новый тип `Комплекс`, ему автоматически будет присвоено наименование текущего Комплекса.
> - При изменении типа актива на `ПЛК` или обратно необходимо обновить информацию в блоке **Информация об ОС**. Для этого выполните шаг 6 после редактирования общей информации.

    - описание;
    - АСУ ТП;
    - группу;

- наименование производителя.

> Подсказка:
>
> Если активу назначен интерфейс для сбора данных, возможно автоматическое распознавание производителя на основе первых трех октетов его MAC-адреса. Для этого нажмите кнопку **определить** под полем **Производитель**.

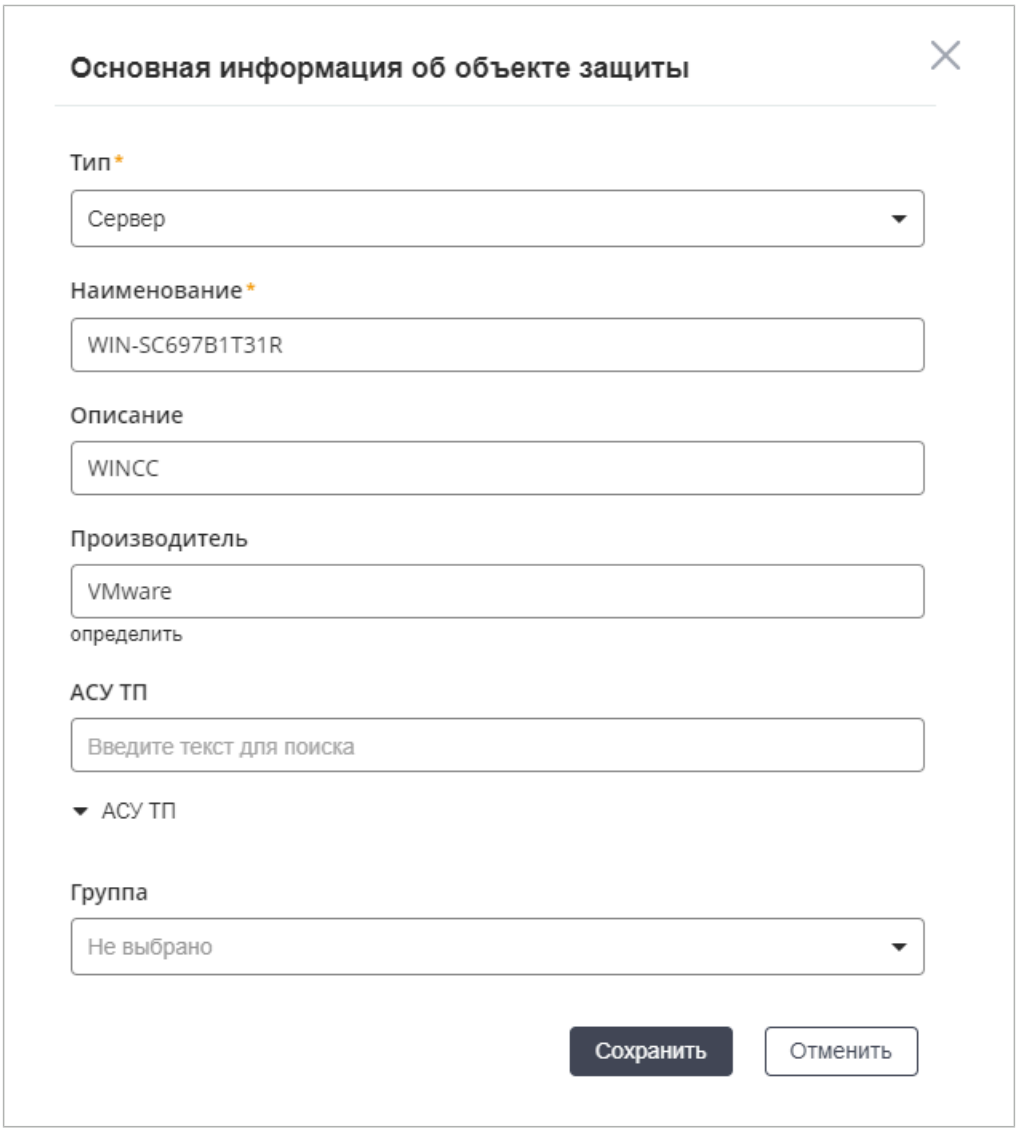


Рис. 176. Окно «Основная информация об активе»

5. Для изменения учетных данных актива:

а. Нажмите кнопку напротив блока **Учетные данные**.

б. Установите чекбокс рядом с добавленной ранее учетной записью для привилегированного доступа к активу и нажмите кнопку **Сохранить**.

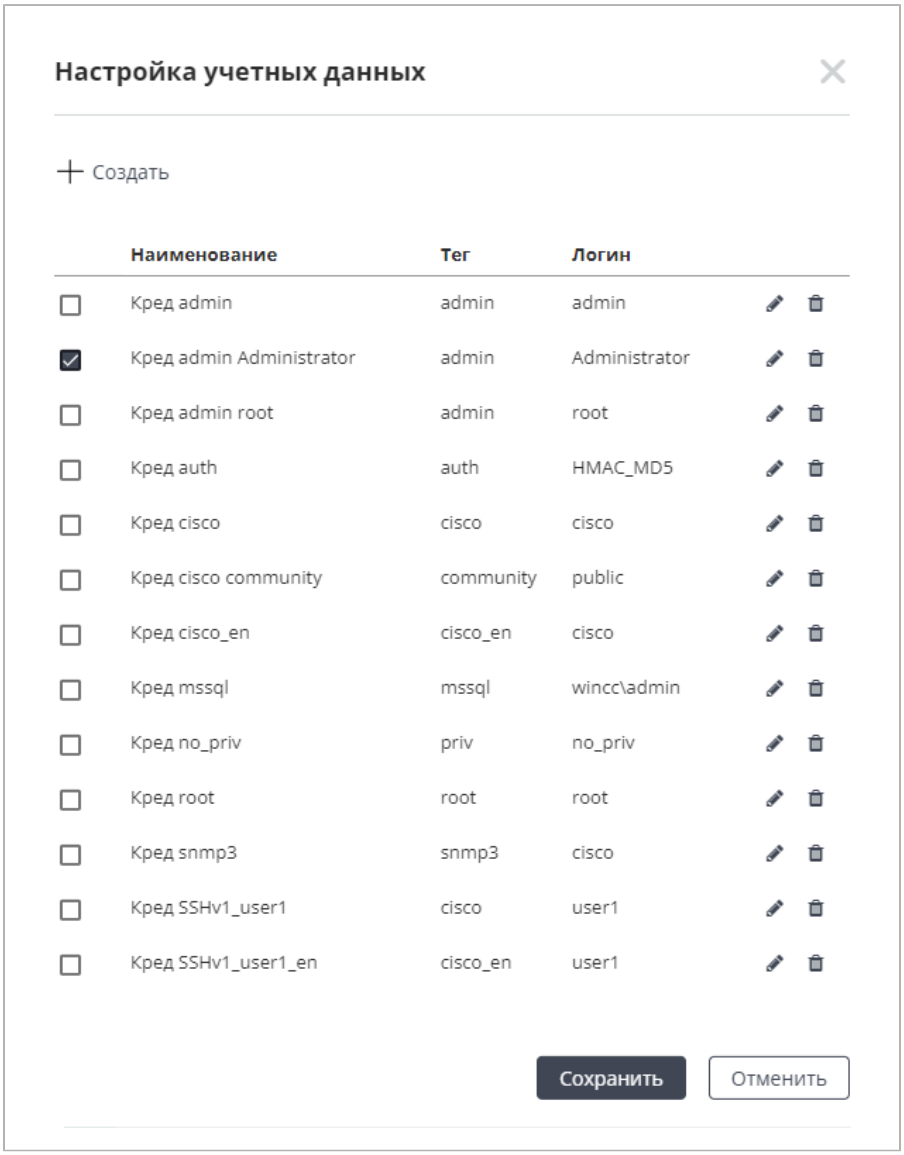


Рис. 177. Окно «Настройка учетных данных»

6. Для изменения информации об ОС актива:

а. Нажмите кнопку напротив блока **Информация об ОС**.

- **Результат шага:** появится окно **Редактирование информации об ОС**.

б. Измените данные операционной системы актива:

- производителя;
- название;
- версию.

> Внимание:
>
> Тип информации, сохраняемой в блоке **Информация об ОС**, зависит от настроенного типа актива: для активов с типом `ПЛК` собирается и сохраняется информация о прошивке, для остальных активов — информация об операционной системе.

При изменении типа актива на `ПЛК` или обратно необходимо обновить информацию в блоке **Информация об ОС**.

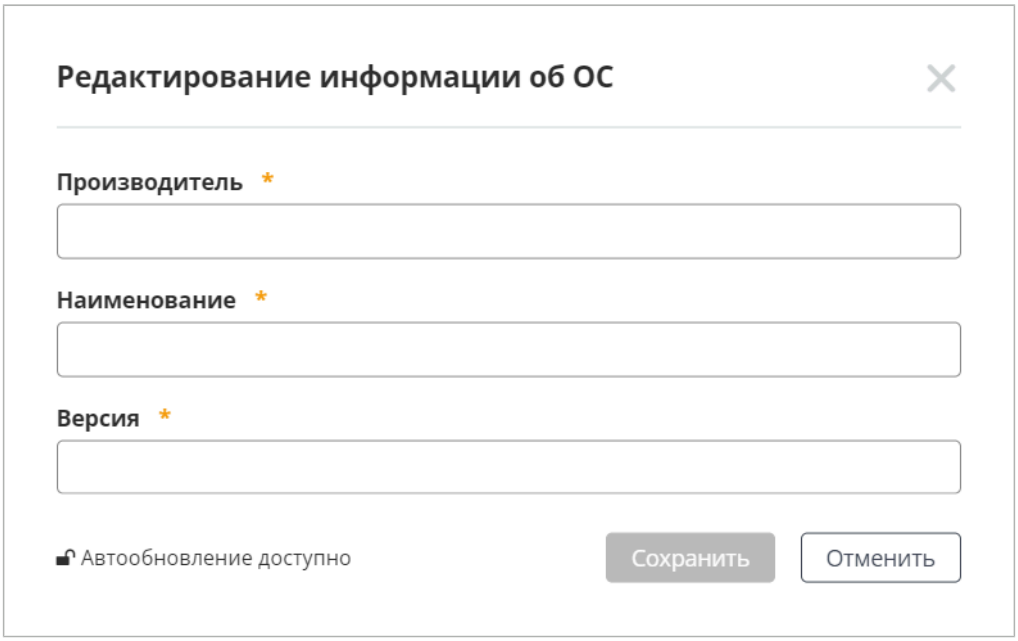


Рис. 178. Окно «Редактирование информации об ОС»

в. При необходимости отключите автообновление данных об операционной системе при сборе задачами сбора данных. Для этого нажмите **Автообновление доступно**.

- **Результат шага:** появится надпись Автообновление заблокировано.

г. Нажмите кнопку **Сохранить**.

7. Для настройки сетевых атрибутов актива:

> Внимание:
>
> Настройка сетевых атрибутов актива возможна только для активов с типом, отличным от `Неизвестный тип`.

а. Нажмите кнопку напротив блока **Сетевые атрибуты**.

- **Результат шага:** появится окно **Редактирование сетевых атрибутов актива**.

б. В открывшемся окне сетевых атрибутов измените следующие параметры:

- название сетевого интерфейса;
- IP-адрес сетевого интерфейса;
- MAC-адрес сетевого интерфейса;

> Внимание:
>
> Вводить разделители для октетов MAC-адресов не требуется — при вводе цифр или английских символов разделитель `:` устанавливается автоматически при необходимости.

- выберите из списка сенсор, в чью контролируемую сеть входит новый IP-адрес.

> **Подсказка:**
>
> Если ранее было проведено сканирование контролируемой сети, можно привязать интерфейсы неизвестного актива. Для этого:
>
> - Отметьте параметр **Выбрать сетевой атрибут неизвестного актива**.
> - В выпадающем списке выберите интерфейс неизвестного актива.

в. При необходимости установите чекбокс **Интерфейс для сбора данных** напротив интерфейса.

> **Внимание:**
>
> - У актива всегда должен быть интерфейс сбора данных — при попытке сохранения сетевых атрибутов актива при условии, что ни один атрибут не выбран в качестве интерфейса сбора, появится предупреждение: `Ошибка! Не выбран интерфейс сбора данных. Установите чекбокс напротив сетевых атрибутов для их выбора в качестве интерфейса сбора данных.`
> - Только один сетевой атрибут актива может быть выбран в качестве интерфейса сбора данных.

г. Нажмите (**Создать сетевой атрибут**) для подтверждения изменений.

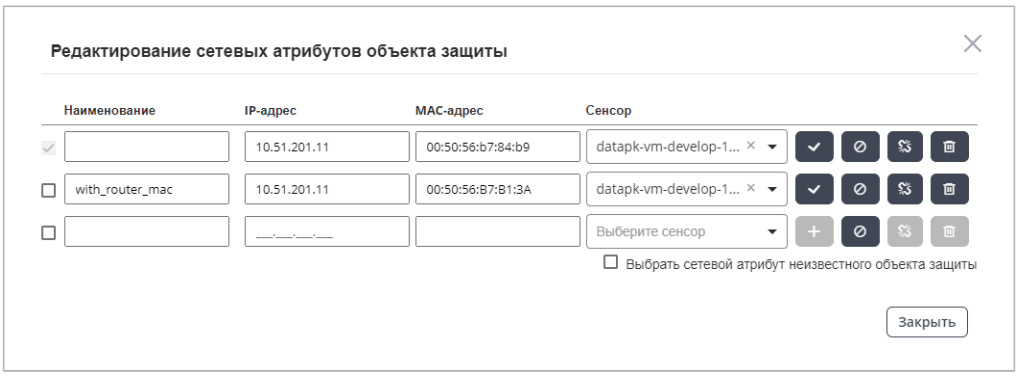


Рис. 179. Окно «Редактирование сетевых атрибутов актива»

8. Для изменения списка меток, которым принадлежит редактируемый актив:
   a. Нажмите кнопку напротив блока **Метки**.

   ▸ **Результат шага:** появится окно **Редактирование меток**.

б. Измените состав присвоенных активу меток и нажмите **Сохранить.**

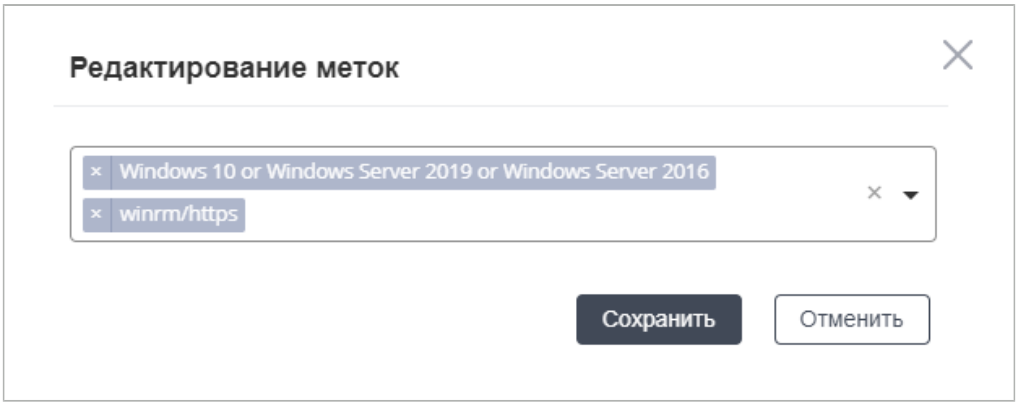


Рис. 180. Окно «Редактирование меток»

12.6. Удаление активов

ОСТОРОЖНО:

При удалении одного или нескольких активов с Комплекса будут удалены все связанные с ними данные: конфигурации, данные об операционной системе и программном обеспечении, информация о найденных уязвимостях.

На странице **Активы** удалить один актив можно из **карточки актива** или из боковой панели актива. Также на странице доступно групповое удаление активов.

12.6.1. Удаление одного актива из боковой панели актива

Для удаления актива из боковой панели актива:

1. Перейдите на страницу **Активы**.
2. Нажмите в любом месте в строке с активом (кроме его иконки и наименования).
   - **Результат шага:** справа откроется боковая панель актива.
3. Нажмите кнопку **Удалить** в правом нижнем углу.

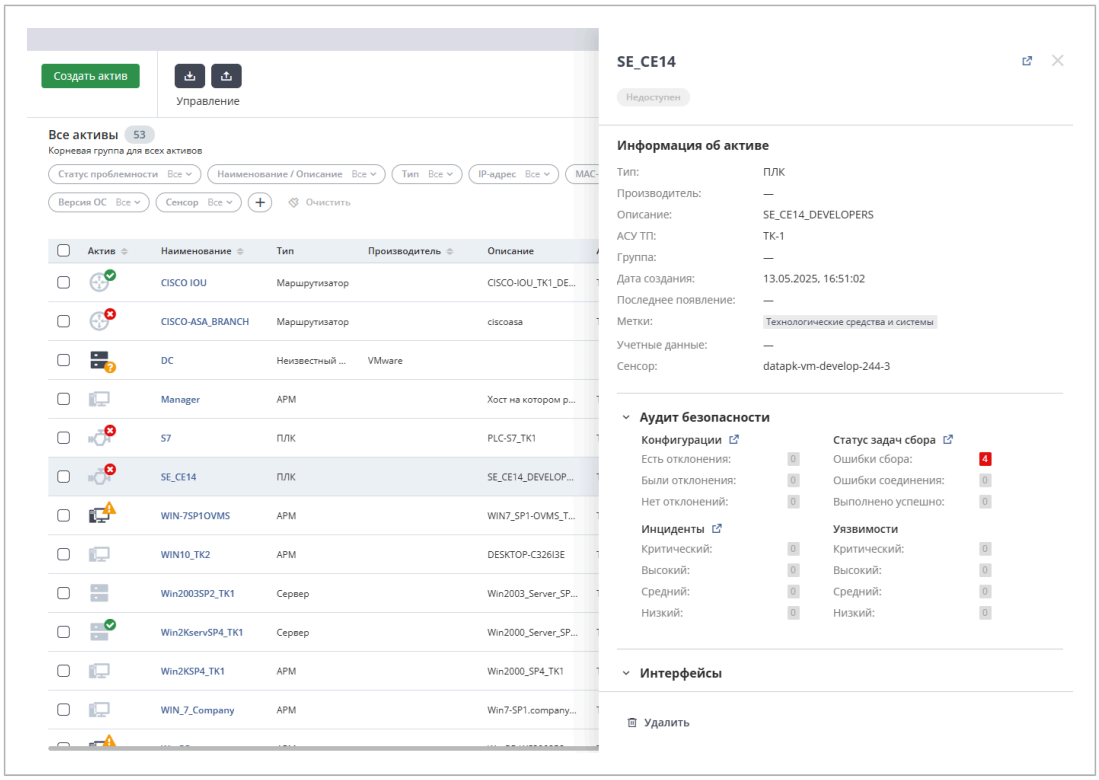


Рис. 181. Боковая панель актива

4. В открывшемся окне введите обоснование удаления актива и нажмите кнопку **Подтвердить**.

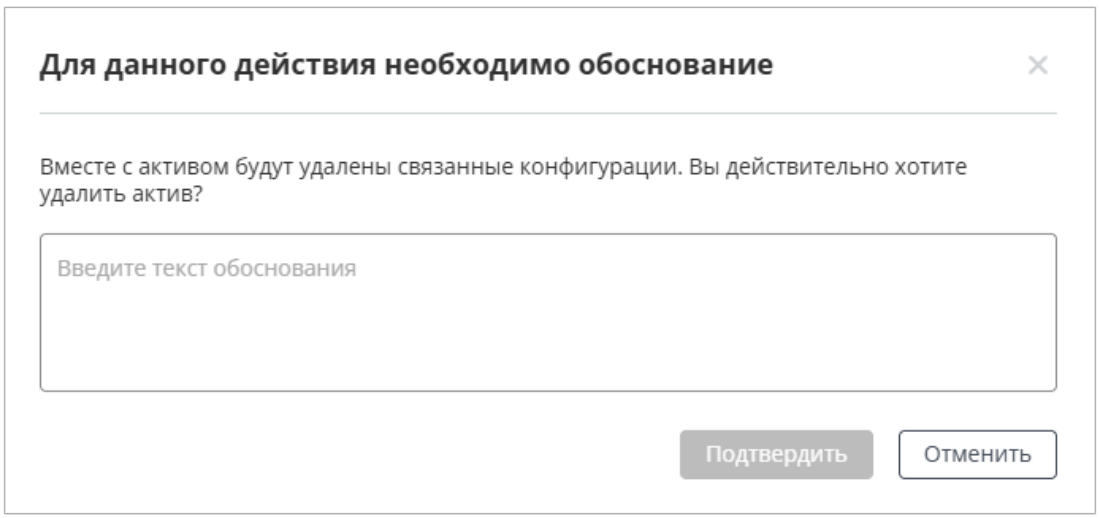


Рис. 182. Окно обоснования удаления актива

- **Результат шага:** актив будет удален.

12.6.2. Удаление одного актива из карточки актива

Для удаления актива из карточки актива:

1. Перейдите на страницу **Активы**.
2. Нажмите на иконку или наименование актива.
   - **Результат шага:** появится **Карточка актива**.
3. Нажмите кнопку **Удалить актив** в правом верхнем углу.

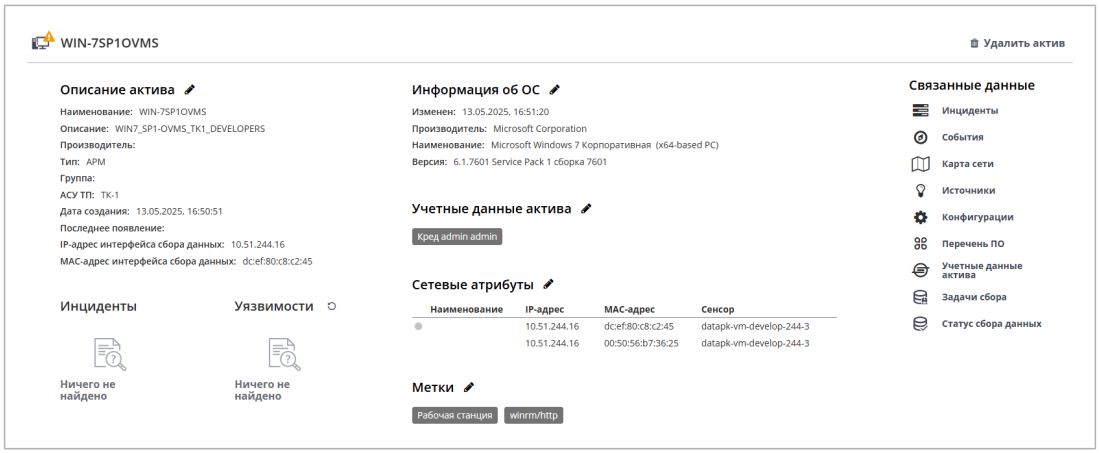


Рис. 183. Кнопка «Удалить актив» в карточке актива

4. В открывшемся окне введите обоснование удаления актива и нажмите кнопку **Подтвердить**.

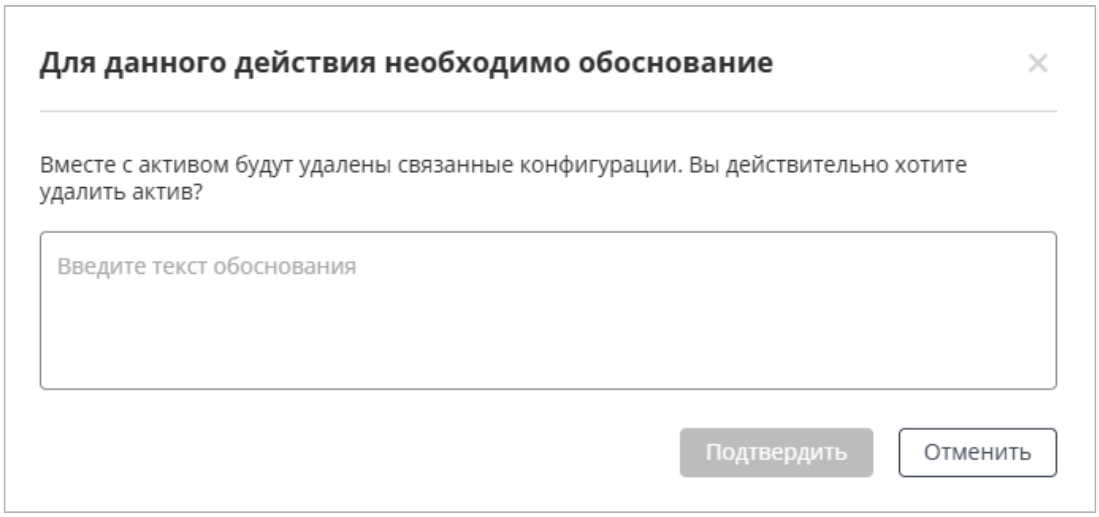


Рис. 184. Окно обоснования удаления актива

- **Результат шага:** актив будет удален. Откроется страница **Активы**.

12.6.3. Групповое удаление активов

Для удаления нескольких активов:

1. Перейдите на страницу **Активы**.
2. Получите необходимую выборку активов с помощью фильтров и выбора групп активов.

> Внимание:
>
> Если выбрана группа активов, параметры фильтрации и групповые операции будут применяться только к активам из группы.

> Внимание:
>
> Групповое удаление активов будет недоступно при следующих условиях, выполненных одновременно:

- Применен хотя бы один из фильтров: **Статус проблемности**, **Производитель ОС**, **ОС**, **Версия ОС**.
- По результатам фильтрации получилось больше 100 записей.
- Применено действие **Выбрать все записи (>100) в данной таблице**.

3. Отметьте отфильтрованные активы на удаление с помощью чекбокса **Выбрать видимые строки** в заголовке таблицы, либо отметьте отдельные активы с помощью чекбоксов рядом с активами. Для выбора всех активов:
    a. Выберите один актив.
    б. В нижнем меню нажмите **Выбрать все**.
4. В нижнем меню нажмите кнопку Удалить.

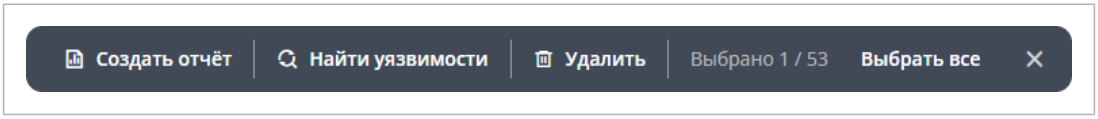


Рис. 185. Нижнее меню на странице «Активы»

5. В открывшемся окне введите обоснование удаления активов и нажмите кнопку **Подтвердить.**
    - **Результат шага:** появится всплывающее уведомление об успешном удалении: `Удаление актива запущено`.

12.7. Выгрузка отчета по активам

Для выгрузки отчета по активам:

1. Перейдите на страницу **Активы**.
2. Установите чекбокс возле необходимых активов.
3. Нажмите кнопку **Создать отчет** (Создать отчёт) в открывшемся нижнем меню.
    - **Результат шага:** откроется окно **Создание отчета**.

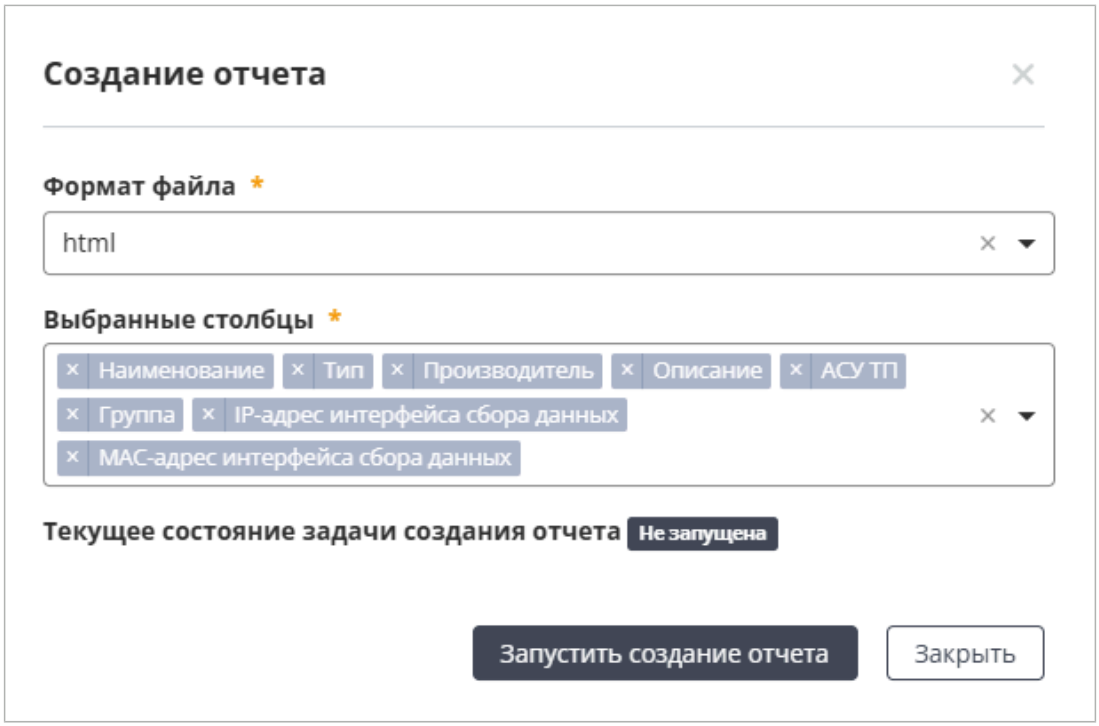


Рис. 186. Окно «Создание отчета»

4. Выберите формат файла отчета из выпадающего списка **Формат файла**. Для выбора доступен формат `html` или `xlsx`.
5. Выберите столбцы, которые будут отражены в отчете.

> Подсказка:
>
> По умолчанию в окне создания отчета указаны те же столбцы, которые ранее были выбраны для отображения в таблице.

6. Нажмите кнопку **Запустить создание отчета**.
   - **Результат шага:** В правом верхнем углу будет отображено всплывающее уведомление `Задача создания отчета запущена`
7. Для сохранения отчета после того, как он создан, нажмите на ссылку с названием файла отчета.

12.8. Настройки активов

В этом разделе:

- Настройка учетных данных активов
  - Добавление учетных данных актива
  - Редактирование и удаление учетных данных актива
  - Импорт учетных данных активов
- Настройка классификаторов
  - Создание классификатора АСУ ТП
  - Создание метки
  - Редактирование и удаление классификаторов
  - Экспорт и импорт классификаторов

Для работы с активами в Комплексе предусмотрено создание, редактирование и удаление групп (классификаторов) АСУ ТП и иных пользовательских групп и классификаторов.

Для возможности активного сбора данных (конфигураций и проверок на соответствие требованиям ИБ) пользователь может добавить учетные данные актива.

12.8.1. Настройка учетных данных активов

В этом разделе:

- Добавление учетных данных актива
- Редактирование и удаление учетных данных актива
- Импорт учетных данных активов

Для возможности сбора конфигурации и событий с активов создайте и настройте учетные записи в операционных системах активов. При настройке необходимо учесть права, обеспечивающие доступ к информации о конфигурации и событиях актива. Учетные данные (логин и пароль) таких учетных записей указываются в Комплексе и используются сканерами и источниками событий для привилегированного доступа к активу.

В веб-интерфейсе Комплекса можно просмотреть как список всех учетных данных активов, так и учетные данные конкретного актива.

Чтобы просмотреть список всех учетных данных активов Комплекса, перейдите на страницу **Администрирование** → **Настройка активов** → **Учетные данные**. Для фильтрации элементов в списке используется фильтр по активам и поля поиска по наименованию и логину.

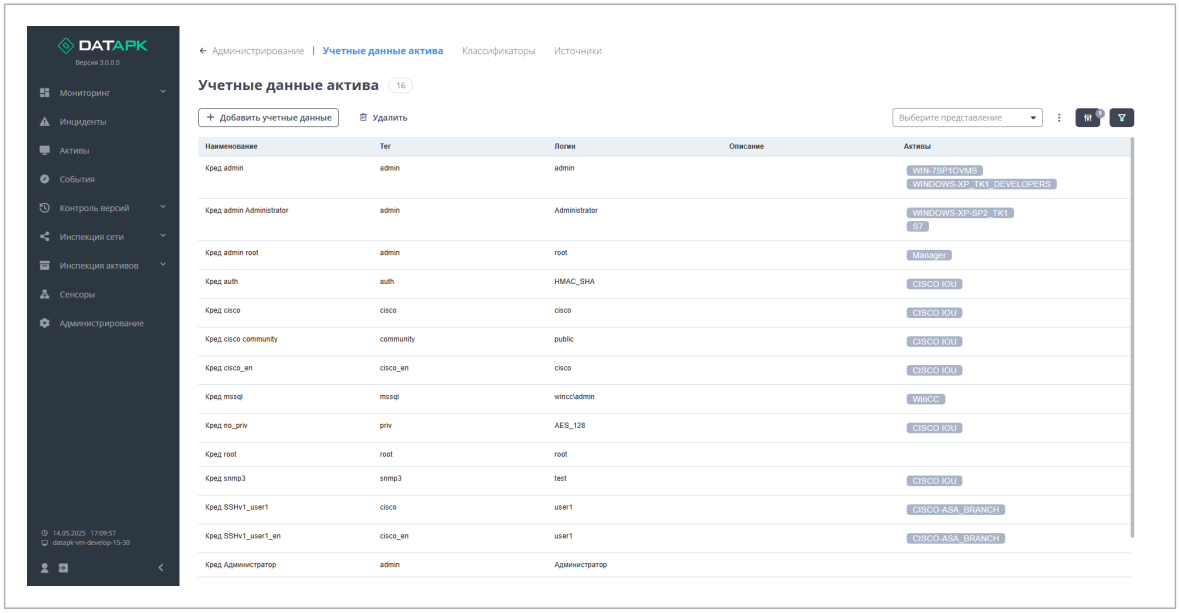


Рис. 187. Страница «Учетные данные»

Чтобы просмотреть список учетных данных определенного актива, перейдите в карточку актива и просмотрите блок **Учетные данные**, либо перейдите по ссылке **Учетные данные актива** в блоке **Связанные данные**.

Помимо непосредственно создания учетных данных в веб-интерфейсе, пользователь может также импортировать список учетных данных, сформированный вручную. Функция экспорта учетных записей активов отключена с целью предотвращения утечки учетных данных.

12.8.1.1. Добавление учетных данных актива

Перед выполнением: Перед непосредственно добавлением учетных данных в Комплекс создайте средствами операционной системы выбранного актива учетную запись и настройте для нее права доступа, необходимые для сбора конфигурации и событий.

Для добавления учетных данных для привилегированного доступа к активу:

1. Откройте веб-интерфейс Комплекса и откройте окно добавления учетных данных одним из указанных способов:
   - Способ 1:
     a. Перейдите на страницу **Администрирование** → **Настройка активов** → **Учетные данные**.
     b. Нажмите кнопку **Добавить учетные данные**.
   - Способ 2:
     a. Перейдите в карточку актива.
     b. Перейдите по ссылке **Учетные данные актива** в блоке **Связанные данные**.
     c. На открывшейся странице нажмите кнопку **Добавить учетные данные**.
   - Способ 3:
     a. Перейдите в карточку актива.
     b. Нажмите кнопку напротив блока **Учетные данные**.
     c. В открывшемся окне нажмите кнопку **+ Создать**.

   ▸ **Результат шага:** появится окно **Редактирование учетных данных актива**.
2. В открывшемся окне введите следующие параметры:
   - наименование и описание новой учетной записи;
   - тег (может совпадать с логином учетной записи, созданной в операционной системе актива) — используется в Python-скриптах сбора данных для поиска соответствующей учетной записи в списке;

     > Подсказка:
     >
     > См. подробнее в разделе «Содержание Python-скриптов».

   - логин (должен совпадать с логином учетной записи, созданной в операционной системе актива);
   - пароль (должен совпадать с паролем учетной записи, созданной в операционной системе актива);
   - подтверждение пароля.

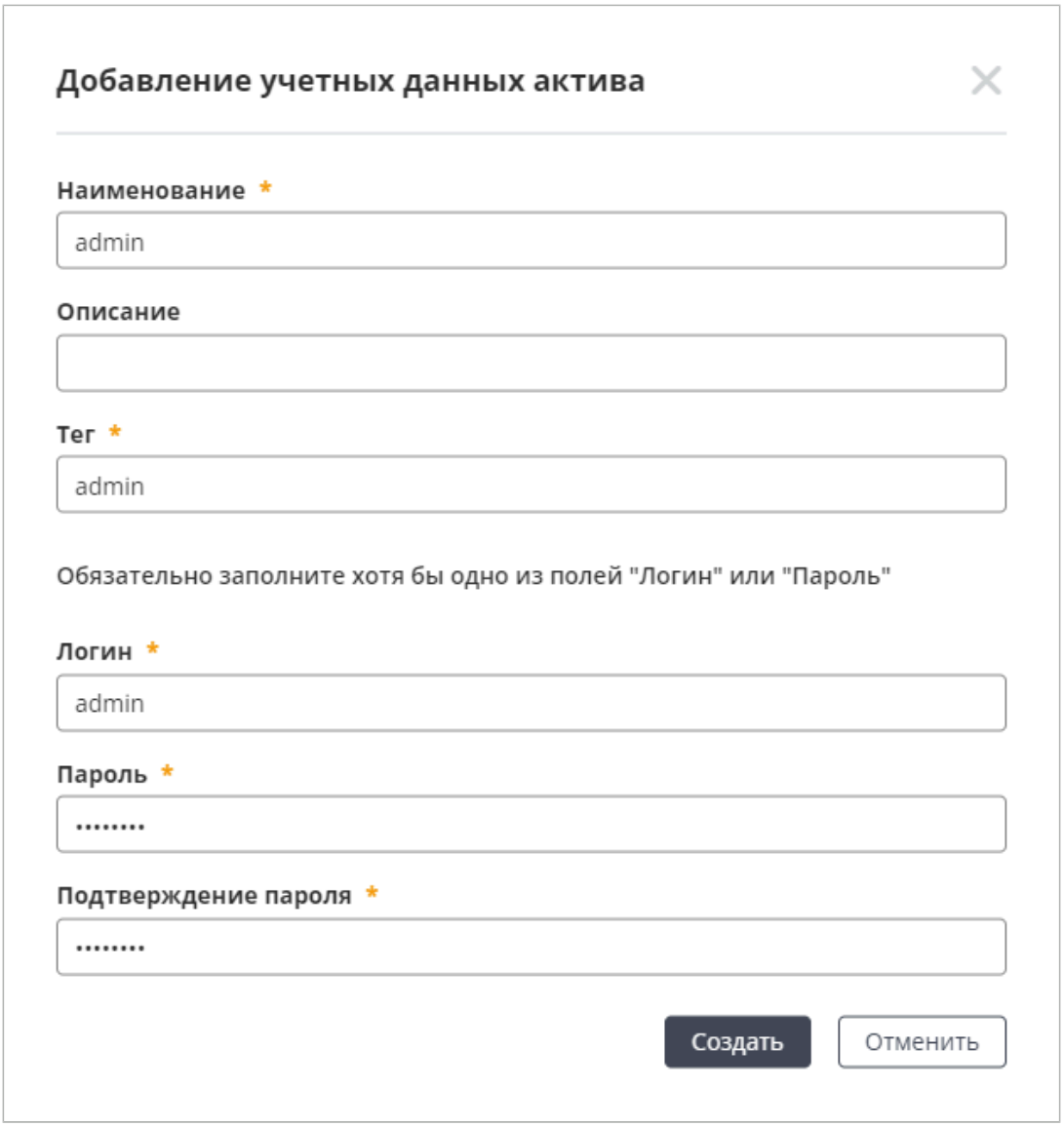


Рис. 188. Окно «Добавление учетных данных актива»

3. Нажмите кнопку **Создать**.

> Подсказка:
>
> Для использования учетных данных при сборе конфигураций, событий и OVAL-объектов необходимо связать созданные учетные данные с активом. См. подробнее в разделе «Настройка активов для сбора данных».

Пример

Примеры учетных данных для доступа к активам:

- Доступ к устройствам производителя Cisco в привилегированном режиме (enable).
  - Тег: cisco_en.
  - Логин: —.
  - Пароль: [пароль].
- Доступ к устройствам производителя Cisco по протоколу SNMP:

- Тег: community.
- Логин: public.
- Пароль: —.

- Доступ по протоколу telnet:
  - Тег: cisco.
  - Логин: —.
  - Пароль: [пароль].

12.8.1.2. Редактирование и удаление учетных данных актива

Для изменения состава учетных данных актива в веб-интерфейсе предусмотрено несколько способов:

1. Редактирование учетных данных на странице **Учетные данные**. Для редактирования:
   a. Перейдите на страницу **Администрирование → Настройка активов → Учетные данные**.
   б. Выберите учетную запись в списке и нажмите кнопку (**Редактировать учетные данные**).
   Результат шага: появится окно **Редактирование учетных данных актива**.
   в. Измените необходимые параметры и нажмите кнопку **Сохранить**.

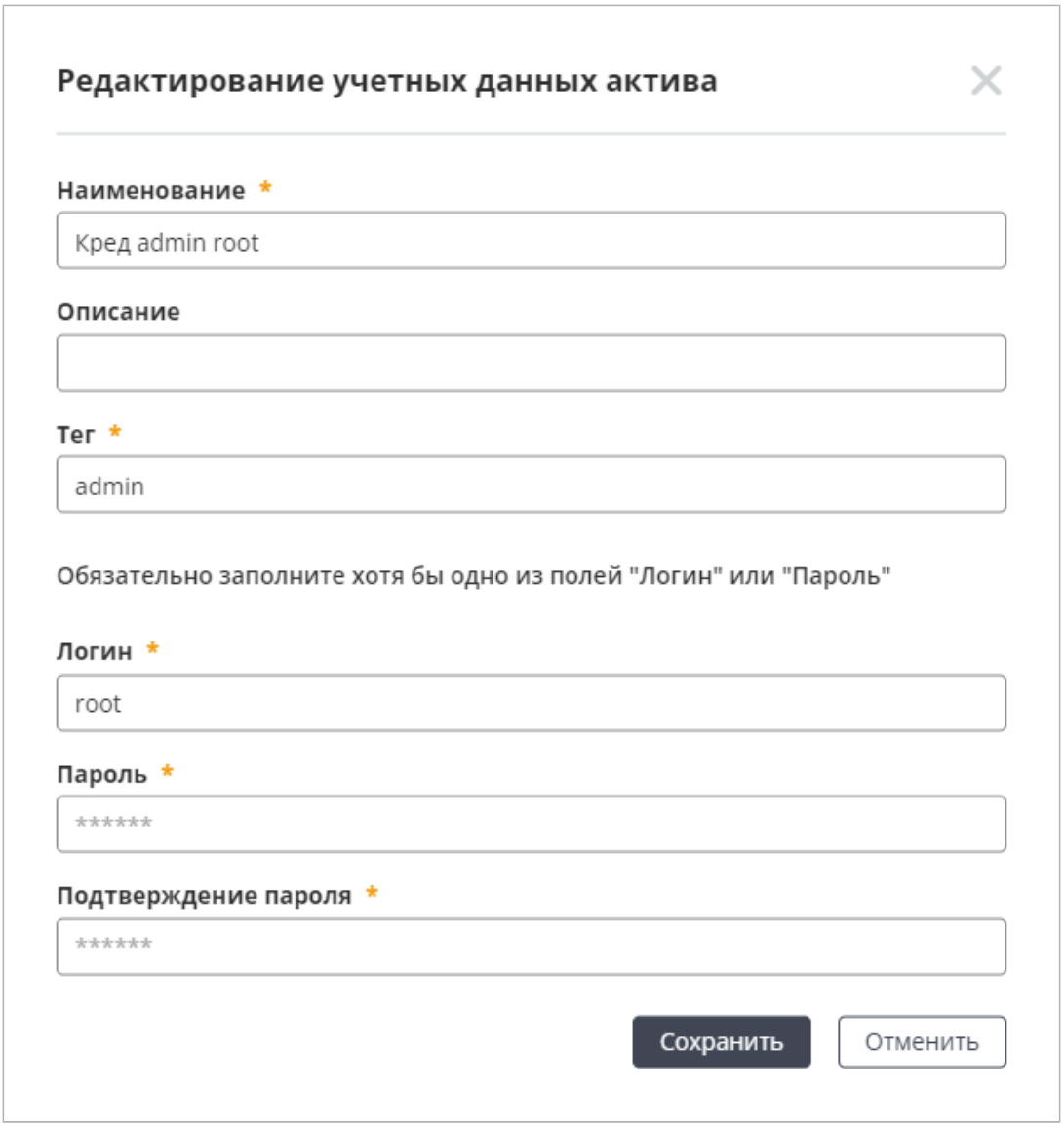


Рис. 189. Окно «Редактирование учетных данных актива»

2. Редактирование учетных данных в карточке актива. Для редактирования:
    а. Перейдите в карточку актива.
    б. Перейдите по ссылке **Учетные данные актива** в блоке **Связанные данные**.
    в. Нажмите (**Редактировать учетные данные**) напротив учетной записи, которую нужно изменить.
    - **Результат шага:** появится окно **Редактирование учетных данных актива**.

    г. Измените необходимые параметры и нажмите кнопку **Сохранить**.
3. Удаление одной записи об учетных данных на странице **Учетные данные**. Для удаления:
    а. Перейдите на страницу **Администрирование → Настройка активов → Учетные данные**.
    б. Нажмите (**Удалить**) напротив учетных данных, которые необходимо удалить.
    - **Результат шага:** появится окно ввода обоснования удаления учетных данных.

в. Введите обоснование удаления учетных данных и нажмите кнопку **Подтвердить**.

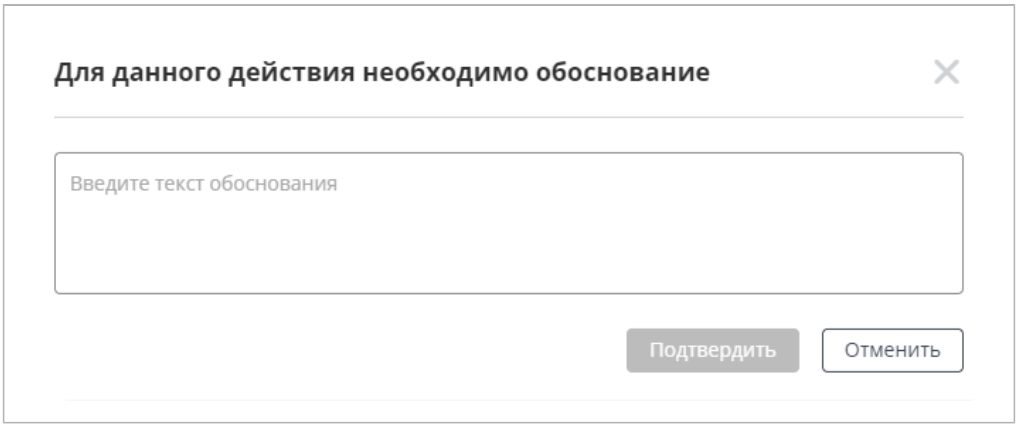


Рис. 190. Окно обоснования удаления учетных данных

4. Удаление учетных данных, отфильтрованных на странице **Учетные данные**. Для удаления:
   а. Перейдите на страницу **Администрирование → Настройка активов → Учетные данные**.
   б. Воспользуйтесь фильтрами для получения списка учетных данных, подлежащих удалению.
   в. В верхней части страницы нажмите (**Удалить учетные данные актива**).
   - **Результат шага:** появится окно ввода обоснования удаления учетных данных.

   г. Введите обоснование удаления учетных данных и нажмите кнопку **Подтвердить**.
5. Удаление учетной записи в карточке актива. Для удаления:
   а. Перейдите в карточку актива.
   б. Нажмите кнопку напротив блока **Учетные данные**.
   - **Результат шага:** откроется окно **Настройка учетных данных**.

   в. Нажмите (**Удалить**) напротив учетной записи, которую нужно удалить.
   - **Результат шага:** появится окно ввода обоснования удаления учетных данных.

   г. Введите обоснование удаления учетных данных и нажмите кнопку **Подтвердить**.

12.8.1.3. Импорт учетных данных активов

Для импорта списка учетных записей активов из файла формата `*.json` в Комплексе:

1. Перейдите на страницу **Администрирование → Основные настройки → Импорт и экспорт**.
2. На панели **Сбор данных** в строке **Учетные данные активов** нажмите кнопку (**Импортировать**).
3. В открывшемся окне укажите расположение импортируемого файла формата `*.json` и подтвердите выбор.
4. В открывшемся окне **Подготовка к импорту** выберите действие для элементов, которые отсутствуют в новом (загружаемом) справочнике:
   - **Оставить** — новые элементы будут добавлены к уже существующим;
   - **Удалить** — старые элементы будут удалены и добавлены новые.

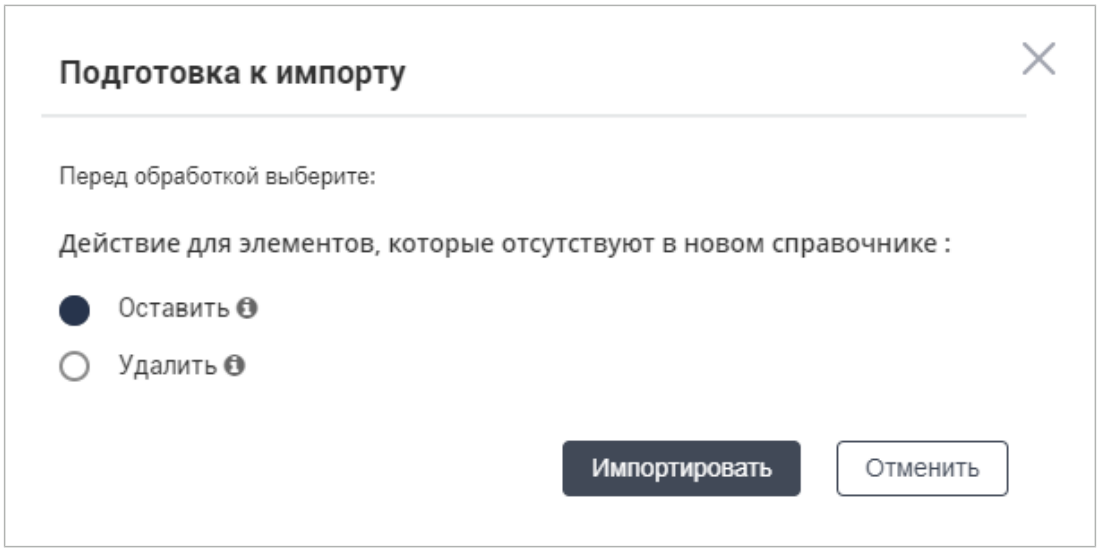


Рис. 191. Окно «Подготовка к импорту»

5. Нажмите кнопку **Импортировать** для выполнения импорта справочника.
6. Убедитесь, что список учетных данных был успешно загружен.

   ▸ **Результат шага:** сразу после загрузки файла в правом вернем углу страницы **Импорт и экспорт** появится уведомление: `Список «Учетные данные активов» успешно обновлен`, и на странице **Администрирование → Настройка активов → Учетные данные** появится импортированный список учетных записей.

12.8.2. Настройка классификаторов

Классификаторы активов загружаются в систему при первичной инсталляции. Некоторые из них доступны для редактирования и дополнения.

Информация о редактируемых классификаторах приведена в таблице ниже (Таблица 17. Редактируемые классификаторы Комплекса).

Табл. 17. Редактируемые классификаторы Комплекса

КЛАССИФИКАТОР	ХАРАКТЕРИСТИКА КЛАССИФИКАТОРА	ОТНОШЕНИЕ К АКТИВАМ
АСУ ТП	предустановленный редакти-руемый	необязательный атрибут классификации активов
OVAL	редактируемый	необязательный атрибут классификации активов
Метки	редактируемый	необязательный атрибут классификации активов

Классификаторы предназначены для фильтрации активов, их содержимое генерируется автоматически при появлении новых элементов в Комплексе. Информация о встроенных классификаторах приведена в таблице ниже.

Табл. 18. Встроенные классификаторы Комплекса

КЛАССИФИКАТОР	ХАРАКТЕРИСТИКА КЛАССИФИКАТОРА	ОТНОШЕНИЕ К АКТИВАМ
Комплекс	предустановленный, автоматически дополняемый с добавлением Комплексов нередактируемый	обязательный атрибут классификации активов, появляется при наличии иерархии Комплексов
Производители	предустановленный нередактируемый	обязательный атрибут классификации активов
Активы	предустановленный, автоматически дополняемый с добавлением Актив нередактируемый	обязательный атрибут классификации активов
Типы активов	предустановленный нередактируемый	обязательный атрибут классификации активов
Операционные системы, распознанные Комплексом	предустановленный, автоматически дополняемый нередактируемый	необязательный атрибут классификации активов; присваивается активам с операционной системой семейства Windows автоматически (при возможности получения информации от активов по протоколу Microsoft Windows Browser)

В Комплексе возможно автоматическое присваивание меток операционных систем для активов. При сканировании узлов контролируемой сети (на странице **Сенсоры**) метка CPE, полученная в результате сканирования актива и содержащая информацию об операционной системе актива и ее версии, сравнивается с метками CPE, присвоенными созданным ранее пользовательским меткам. В случае совпадения активу присваивается соответствующая метка.

Для поиска активов в списке на странице **Активы** используется фильтрация по реквизитам активов, в том числе с помощью встроенных и пользовательских классификаторов.

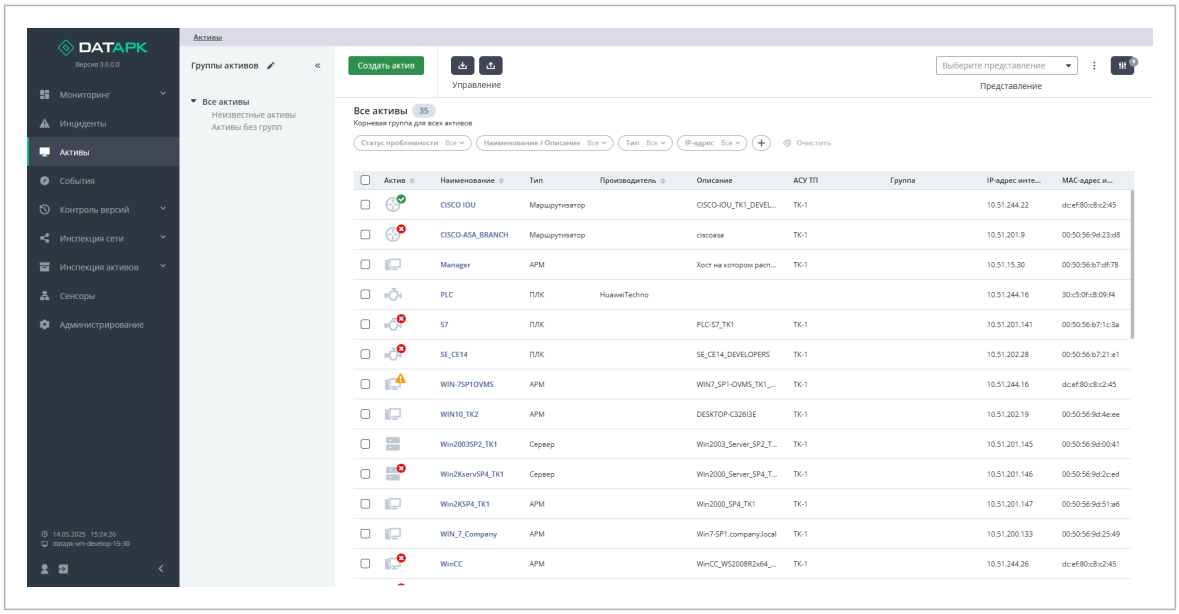


Рис. 192. Список активов с типом «Сервер» из классификатора «Типы активов»

12.8.2.1. Создание классификатора АСУ ТП

Для создания классификатора АСУ ТП:

> **Внимание:**
>
> Максимальная вложенность при создании дочерних классификаторов равна 10.

1. В веб-интерфейсе Комплекса перейдите на страницу **Активы → Настройка активов → Классификаторы**.

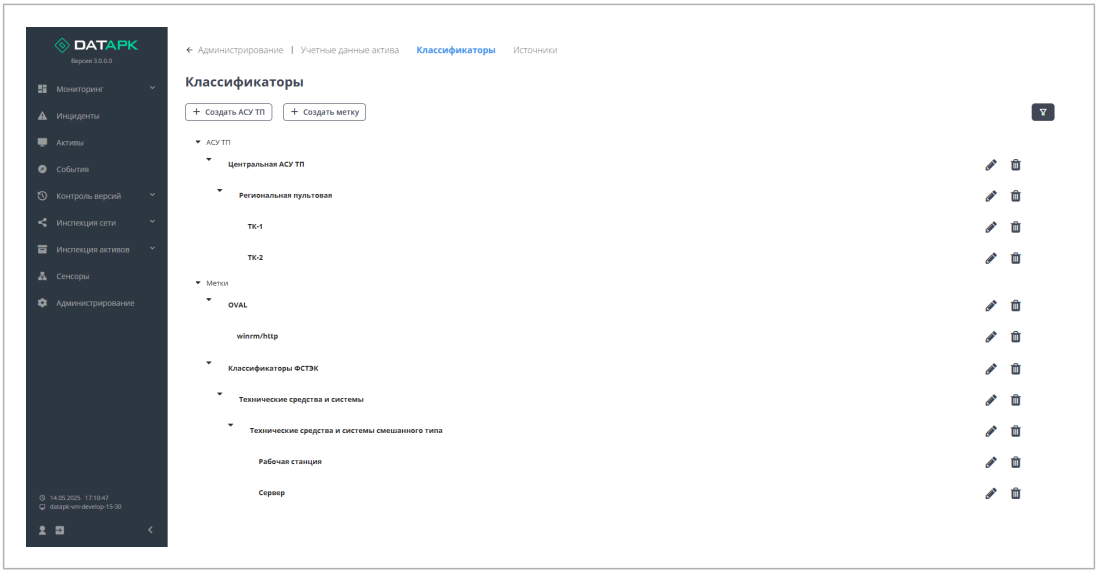


Рис. 193. Страница «Классификаторы»

2. Нажмите кнопку **Создать АСУ ТП**. В открывшемся окне **Создание АСУ ТП** задайте следующие параметры:
    a. наименование АСУ ТП;
    б. описание АСУ ТП;
    в. вышестоящую группу АСУ ТП.

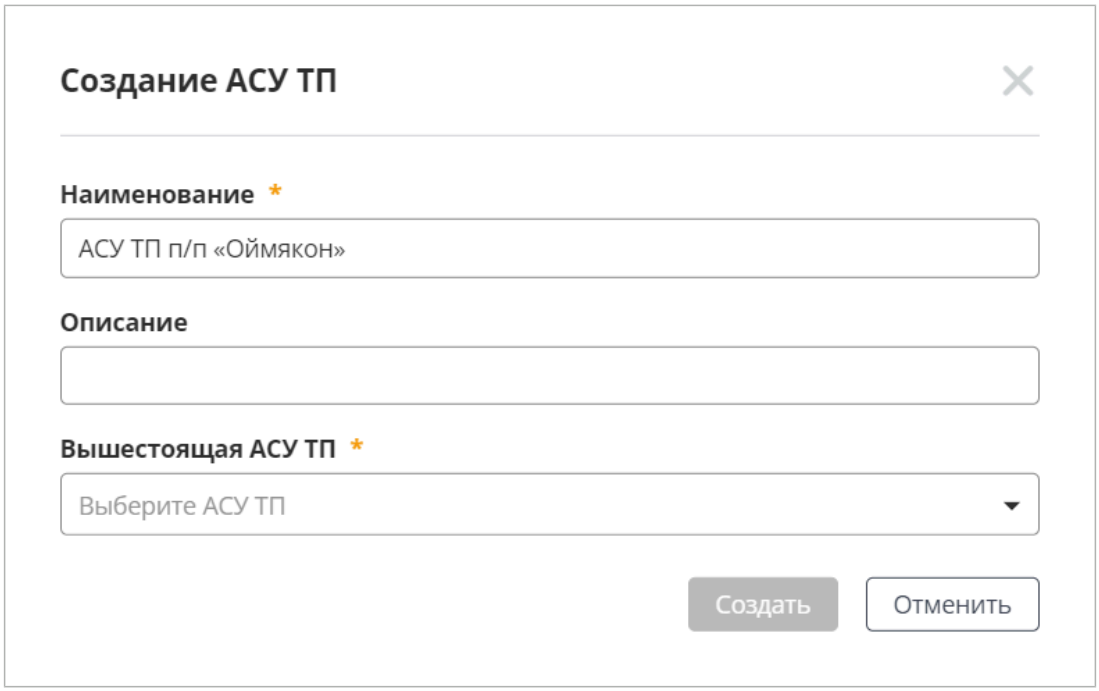


Рис. 194. Окно «Создание АСУ ТП»

3. Нажмите кнопку **Создать** для подтверждения изменений.

12.8.2.2. Создание метки

Для создания метки:

> Внимание:
>
> Максимальная вложенность при создании дочерних классификаторов равна 10.

1. Перейдите на страницу **Активы** → **Настройка активов** → **Классификаторы**.
2. Нажмите кнопку **Создать метку**. В открывшемся окне **Создание метки** задайте следующие параметры:
    a. наименование новой метки;
    б. вышестоящую метку.

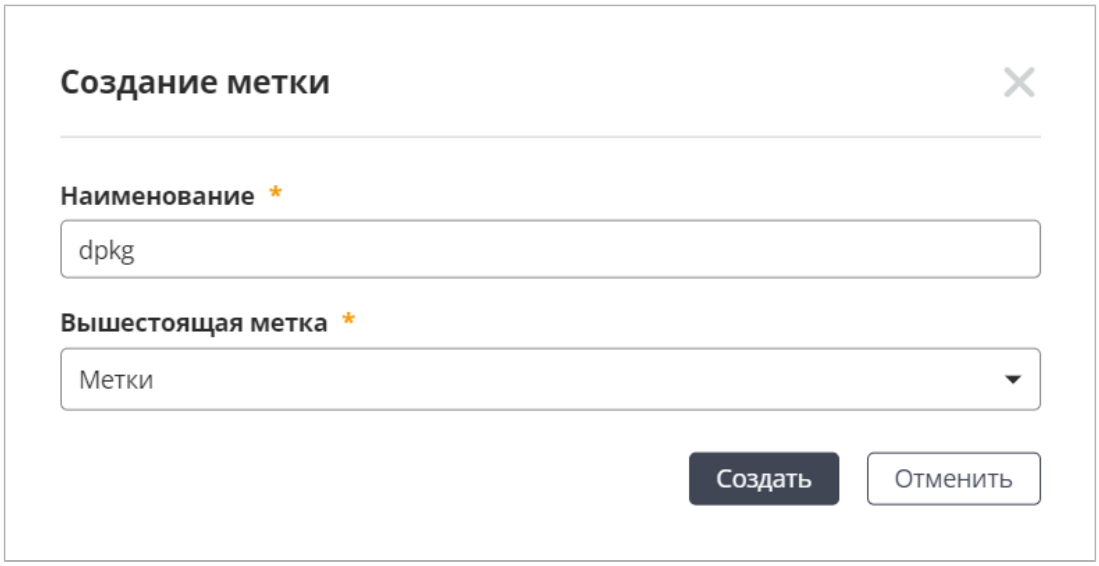


Рис. 195. Окно «Создание метки»

3. Нажмите кнопку **Создать** для подтверждения изменений.

12.8.2.3. Редактирование и удаление классификаторов

Для управления созданными ранее классификаторами доступны следующие возможности:

1. Редактирование. Для редактирования классификатора:
    a. Перейдите на страницу **Администрирование → Настройка активов → Классификаторы**.
    б. Напротив классификатора, который необходимо изменить, нажмите (**Редактировать**).

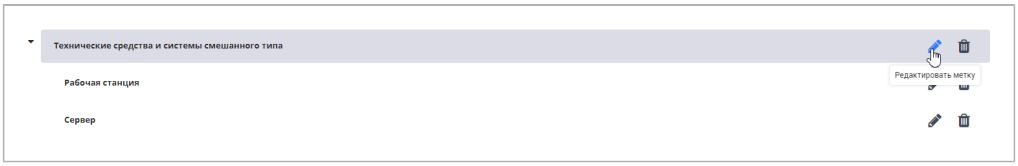


Рис. 196. Кнопка редактирования классификатора

- **Результат шага:** появится окно **Редактирование метки**, либо **Редактирование АСУ ТП**, в зависимости от выбора типа классификатора.

    в. В окне редактирования классификатора измените необходимые параметры.

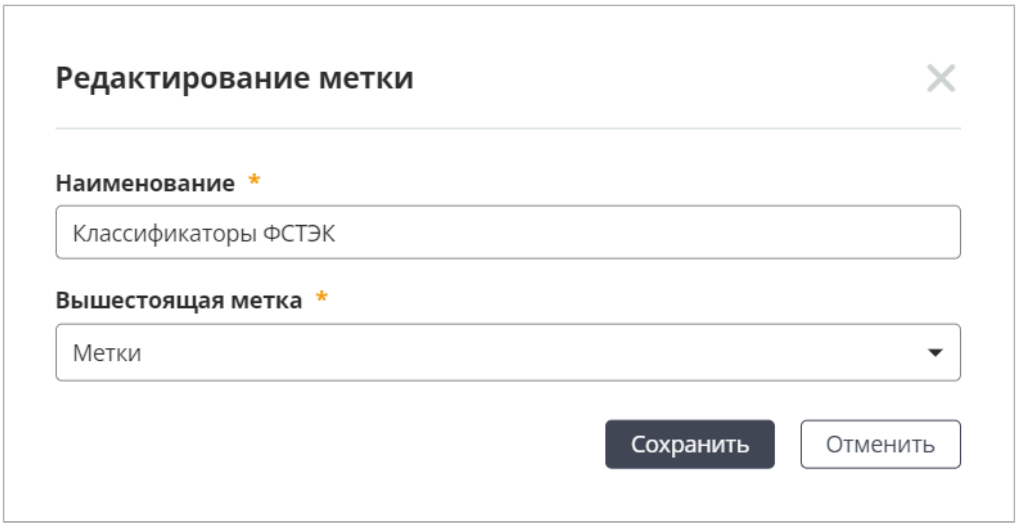


Рис. 197. Окно «Редактирование метки»

г. Нажмите **Сохранить**.

2. Удаление. Для удаления классификатора:

а. Перейдите на страницу **Классификаторы**.

б. Напротив классификатора, который необходимо удалить, нажмите (**Удалить**).

Результат шага:

появится окно подтверждения удаления АСУ ТП, либо метки, в зависимости от выбора типа классификатора.

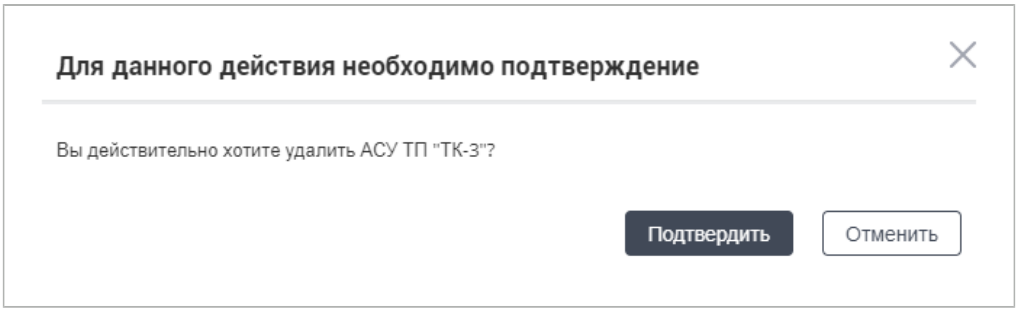


Рис. 198. Окно подтверждения удаления АСУ ТП

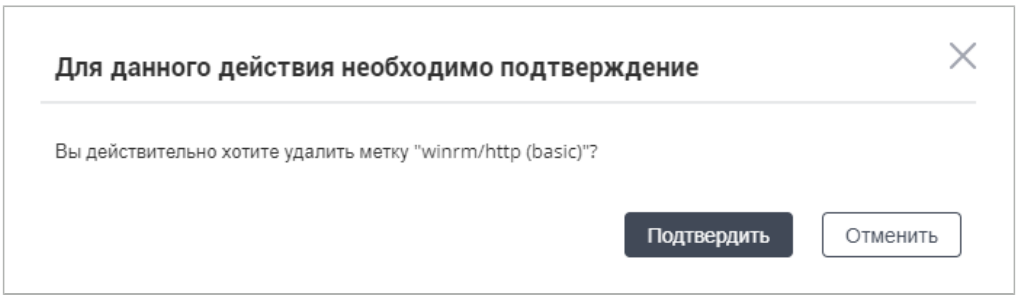


Рис. 199. Окно подтверждения удаления метки

в. Нажмите **Подтвердить**.

12.8.2.4. Экспорт и импорт классификаторов

В этом разделе:

- Экспорт справочника с классификаторами АСУ ТП
- Экспорт меток
- Импорт справочника с классификаторами АСУ ТП
- Импорт меток

Экспорт и импорт справочников с иерархической структурой, содержащих классификаторы осуществляется на странице **Администрирование** → **Основные настройки** → **Импорт и экспорт**.

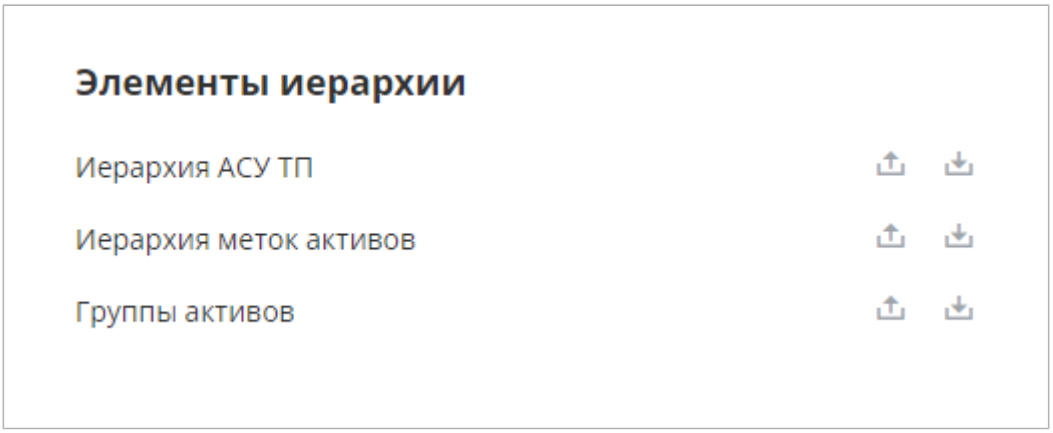


Рис. 200. Панель «Элементы иерархии» на странице «Импорт и экспорт»

12.8.2.4.1. Экспорт справочника с классификаторами АСУ ТП

Для экспорта справочника АСУ ТП с классификаторами и их иерархией в файл формата `*.json`:

1. Перейдите на страницу **Администрирование** → **Основные настройки** → **Импорт и экспорт**.
2. На панели **Элементы иерархии** в строке **Иерархия АСУ ТП** нажмите кнопку (**Экспортировать**).
   - **Результат шага:** файл со списком классификаторов АСУ ТП и их иерархией `ics_[дата_и_время].json` будет сформирован и доступен для скачивания в правом верхнем углу страницы **Импорт и экспорт** под заголовком **Результат последнего экспорта**.
3. Для скачивания файла нажмите на название сформированного файла под заголовком **Результат последнего экспорта**.
4. В открывшемся окне укажите расположение для экспортируемого файла, при необходимости изменив его название, и нажмите кнопку **Сохранить**.
   - **Результат шага:** файл `ics_[дата_и_время].json` будет загружен на компьютер.

12.8.2.4.2. Экспорт меток

Для экспорта справочника с метками и их иерархией в файл формата `*.json`:

1. Перейдите на страницу **Администрирование** → **Основные настройки** → **Импорт и экспорт**.
2. На панели **Элементы иерархии** в строке **Иерархия меток активов** нажмите кнопку (**Экспортировать**).
   - **Результат шага:** файл со списком меток и их иерархией `tags_[дата_и_время].json` будет сформирован и доступен для скачивания в правом верхнем углу страницы **Импорт и экспорт** под заголовком **Результат последнего экспорта**.
3. Для скачивания файла нажмите на название сформированного файла под заголовком **Результат последнего экспорта**.
4. В открывшемся окне укажите расположение для экспортируемого файла, при необходимости изменив его название, и нажмите кнопку **Сохранить**.
   - **Результат шага:** файл `tags_[дата_и_время].json` будет загружен на компьютер.

12.8.2.4.3. Импорт справочника с классификаторами АСУ ТП

> Внимание:
>
> Как правило, файлы в формате `*.json` не создаются вручную, а экспортируются из другого Комплекса.

Для импорта справочника с пользовательской иерархией АСУ ТП из файла формата `*.json` в Комплекс:

1. Перейдите на страницу **Администрирование → Основные настройки → Импорт и экспорт**.
2. На панели **Элементы иерархии** в строке Иерархия АСУ ТП нажмите кнопку (**Импортировать**).
3. В открывшемся окне укажите расположение импортируемого файла формата `*.json` и подтвердите выбор.
4. В открывшемся окне **Подготовка к импорту** выберите действие для элементов, которые отсутствуют в новом (загружаемом) справочнике:
   - **Оставить** — новые элементы будут добавлены к уже существующим;
   - **Удалить** — старые элементы будут удалены и добавлены новые.

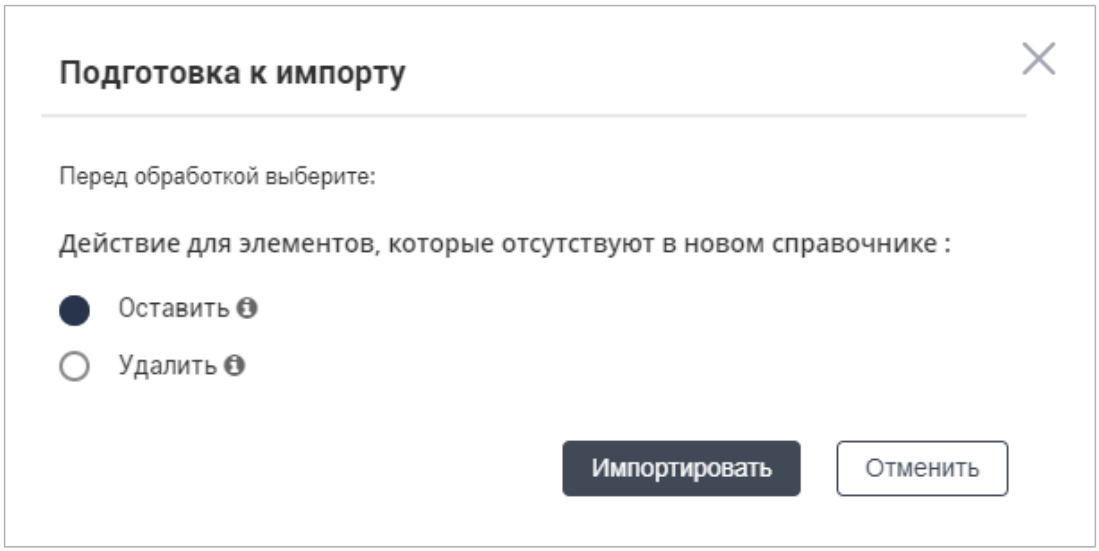


Рис. 201. Окно «Подготовка к импорту»

5. Нажмите кнопку **Импортировать**.
6. Убедитесь, что классификаторы АСУ ТП были успешно загружены.

   ▸ **Результат шага:** сразу после загрузки файла в правом вернем углу страницы **Импорт и экспорт** появится уведомление: `Список «Иерархия АСУ ТП» успешно обновлена`, и на странице **Активы → Настройка активов → Классификаторы** появится импортированный справочник.

12.8.2.4.4. Импорт меток

Для импорта справочника с пользовательской иерархией групп и меток из файла `*_tags_*.json` в Комплекс:

1. Перейдите на страницу **Администрирование → Основные настройки → Импорт и экспорт**.
2. На панели **Элементы иерархии** в строке **Иерархия меток активов** нажмите кнопку (**Импортировать**).
3. В открывшемся окне укажите расположение импортируемого файла формата `*.json` и подтвердите выбор.
4. В открывшемся окне **Подготовка к импорту** выберите действие для элементов, которые отсутствуют в новом (загружаемом) справочнике:

- **Оставить** — новые элементы будут добавлены к уже существующим;
- **Удалить** — старые элементы будут удалены и добавлены новые.

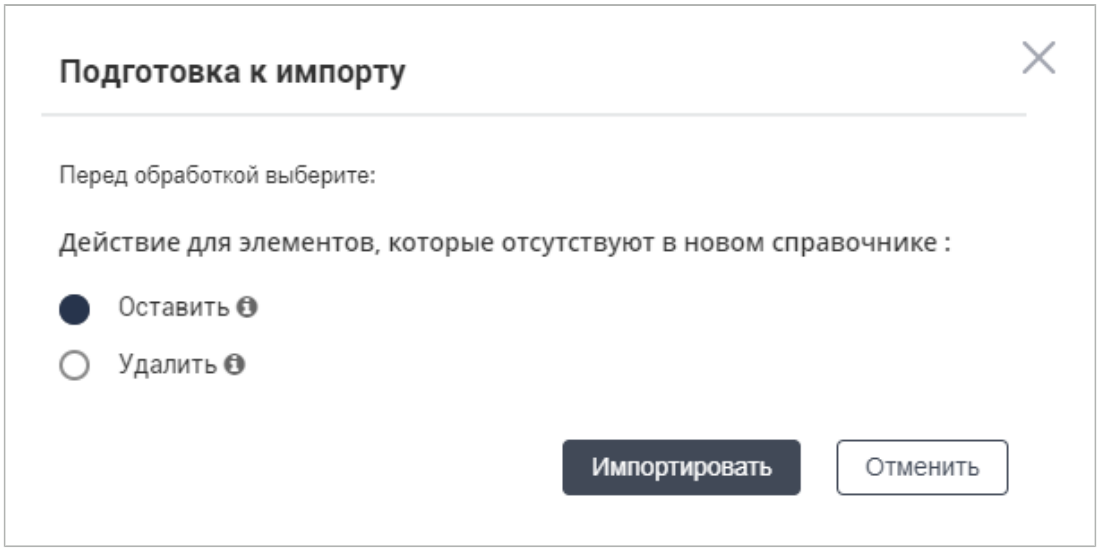


Рис. 202. Окно «Подготовка к импорту»

5. Убедитесь, что метки были успешно загружены.

   ▸ **Результат шага:** сразу после загрузки файла в правом вернем углу страницы **Импорт и экспорт** появится уведомление `Список «Иерархия меток активов» успешно обновлен`, и на странице **Активы → Настройка активов → Классификаторы** появится импортированный справочник.

13. Активный сбор данных с активов

В этом разделе:

1. **Просмотр сводки конфигураций**
2. **Настройка сбора конфигураций активов**
3. **Настройка активного сбора событий**
4. **Настройка сбора данных об операционной системе и установленном ПО**

В Комплексе доступен режим взаимодействия с активами «запрос-ответ», в результате использования которого полученные данные обрабатываются и могут быть интерпретированы как: конфигурации, события, информация об ОС или ПО или результаты проверок на соответствие требованиям ИБ. Такой режим называется активным сбором данных.

Активный сбор данных с актива предполагает, что Комплекс «посещает» актив от имени пользователя, чьи учетные данные привязаны к активу. Подробнее см. раздел «Настройка активов для сбора данных».

Для активного сбора доступны следующие данные:

- Конфигурации. См. подробнее в разделе «Настройка сбора конфигураций активов».
- События. См. подробнее в разделе «Настройка активного сбора событий».
- Параметры безопасности. См. подробнее в главе «Поиск уязвимостей и проверка соответствия требованиям информационной безопасности».
- Информация об ОС и ПО. См. подробнее в разделе «Настройка сбора данных об операционной системе и установленном ПО».

Настройка сбора осуществляется на страницах меню **Администрирование** → **Инспекция активов**.

Внимание:

Перед настройкой сбора данных необходимо ознакомиться с рекомендациями, приведенными в справочном разделе «Рекомендации по настройке сбора данных».

Просмотр результатов активного сбора данных и настройка сбора выполняются на страницах:

- **Конфигурации**, где отображается список последних данных, собранных в рамках задач сканерами сбора конфигураций.
- **События**, где среди прочих отображаются события, которые были загружены в результате работы сканеров сбора событий, входящих в задачи сбора данных.
- **Статус сбора**, где отображаются новейшие итоговые статусы выполнения всех сканеров сбора данных.
- **Результаты проверок**, где отображается список ранее созданных проверок на соответствие требованиям информационной безопасности — подобнее см. в главе «Поиск уязвимостей и проверка соответствия требованиям информационной безопасности».
- Вкладка **Перечень** ПО в **карточке актива**, где отображается список собранных с актива данных об установленном на нем ПО.

13.1. Просмотр сводки конфигураций

Используя страницу **Конфигурации**, можно оперативно получить сводку о последних собранных сканерами данных с активов, а также найти интересующие. Последними считаются новейшие просканированные конфигурации (подробнее см. раздел «Сбор данных с активов»).

Чтобы просмотреть последние конфигурации, перейдите на страницу **Инспекция активов** → **Конфигурации**. На странице конфигурации отображаются в виде таблицы, содержащей следующие данные:

- статус конфигурации;
- дата обновления конфигурации;
- название актива, с которого собиралась конфигурация;

> Подсказка:
>
> При нажатии на название актива, для которого была создана конфигурация, можно открыть окно **Информация об активе**, в котором будет отображаться краткая информация о выбранном активе.

- наименование конфигурации.

После подбора списка конфигураций содержимое таблицы можно сохранить в отчет.

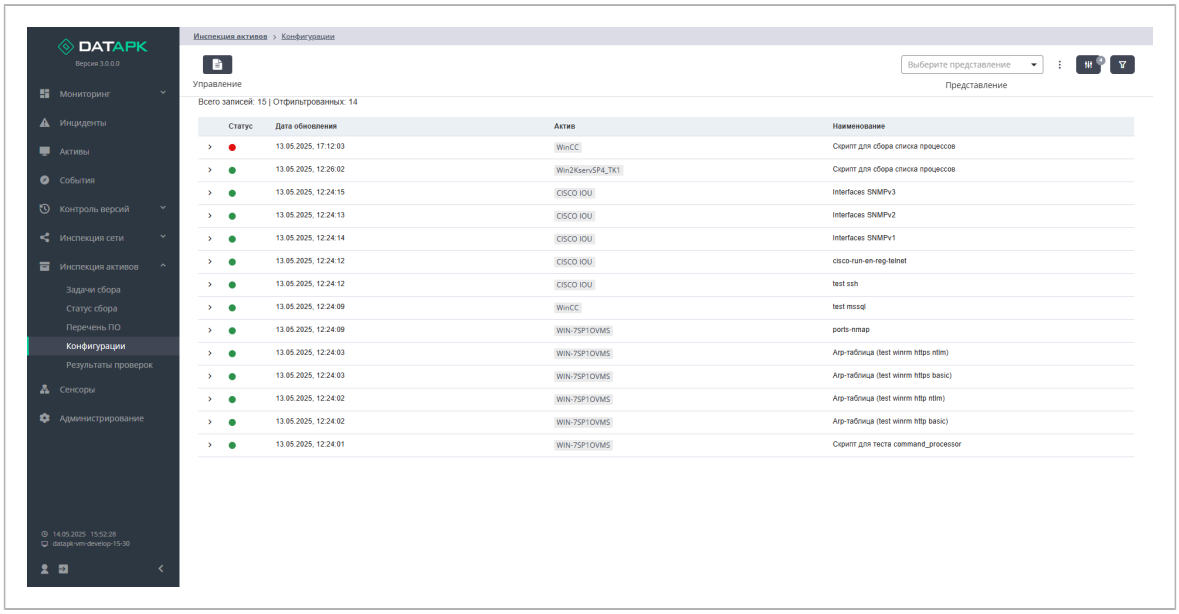


Рис. 203. Страница «Конфигурации»

Статусы конфигураций

Конфигурации могут иметь следующие статусы, которые отображаются при наведении на индикатор статуса:

- **Нет отклонений** — зеленый индикатор;
- **Были отклонения** — желтый индикатор;
- **Есть отклонения** — красный индикатор.

Отображение столбцов

При первом входе на страницу отображаются конфигурации за все время (без фильтров). Чтобы регулировать отображение столбцов, нажмите кнопку в правом верхнем углу. Содержание конфигураций по умолчанию

выводится в кратком (свернутом) виде. Для вывода подробностей воспользуйтесь соответствующим фильтром, либо нажмите слева от конфигурации.

Фильтры

Чтобы найти интересующие конфигурации, воспользуйтесь фильтрами. Доступны следующие фильтры:

- выпадающий список **Актив** — содержит список доступных для выбора активов;
- выпадающий список **Конфигурации** — содержит список доступных для выбора конфигураций;
- поле **Содержание конфигурации** — может быть заполнено любым текстом, который содержится в конфигурациях;
- поля **Дата и время обновления** — позволяет выбрать период с точностью до секунды, по которым необходимо отобразить конфигурации;
- чекбокс **Сравнить с эталонной** позволяет сравнить выбранные фильтром конфигурации с эталоном и вывести только те конфигурации, в которых были обнаружены отклонения от эталона;
- чекбокс **Только с отклонениями** позволяет вывести только те конфигурации, в которых были обнаружены отклонения от эталона, при этом сравнение с эталоном отображаться не будет.

Отчет

Чтобы сохранить отчет по выбранным конфигурациям, нажмите кнопку **Создать отчет** в верхней части страницы. Подробнее о выгрузке отчетов см. раздел «Выгрузка отчетов».

В отчете конфигурации отображаются подробно вне зависимости от того, был ли выбран подробный вывод конфигурации. В разделе отчета **Содержание конфигурации** содержится информация о том, является ли конфигурация эталонной.

Сравнение с эталоном

При выборе в фильтрах опции **Сравнить с эталонной** можно просматривать только конфигурации, у которых есть непроверенные изменения.

При просмотре в подробном виде доступны кнопки (**Показать еще по 5 окружающих строк**) и (**Скрыть по 5 окружающих строк**).

Просмотр конфигурации актива

Чтобы просмотреть архив конфигураций, полученных с актива, наведите курсор на строку с выбранным сканером и нажмите кнопку **Просмотреть конфигурацию актива**. Подробнее см. раздел «Просмотр архива конфигураций».

13.2. Настройка сбора конфигураций активов

В этом разделе:

- Цифровая подпись Python-скрипта
- Экспорт и импорт задач сбора данных, сканеров и их групп
- Настройка сканеров сбора данных
- Добавление сетевых атрибутов активу с помощью сканера сбора данных по SNMP
- Сбор данных с активов
- Просмотр статуса сбора данных
- Работа с архивом изменений конфигурации актива

Задача сбора данных — сущность, позволяющая при помощи групп сканеров собирать конфигурации и события с активов и их групп, в том числе с использованием расписания cron. Создание и управление задачами производится на странице **Инспекция активов** → **Задачи сбора** (подробнее см. разделы «Создание задачи сбора данных», «Управление задачами сбора данных»).

Сканер — исполняемый скрипт сбора данных. После импорта или создания сканеров их можно собрать в группы. Управление сканерами и их группами выполняется на странице **Администрирование** → **Инспекция активов** → **Сканеры** (подробнее см. разделы «Создание сканера сбора данных» и «Настройка сканеров сбора данных»).

Скрипт — это исполняемый файл, содержащий последовательность действий на скриптовом языке программирования Python. Предназначен для сбора данных с активов с помощью сканеров. Подробнее о содержании скриптов см. в разделе «Содержание Python-скриптов». Скрипты сбора данных доступны к импорту при создании сканера. Скрипт также можно экспортировать при редактировании сканера.

Для возможности сбора конфигурации с активов необходимо создать и настроить учетные записи на активах с соответствующими правами. Учетную запись, настроенную в операционной системе актива, необходимо добавить в список учетных данных в веб-интерфейсе Комплекса. Порядок настройки учетных данных в Комплексе приведен в разделе «Настройка учетных данных активов».

В результате выполнения отдельных сканеров, либо в составе задач сбора данных формируются конфигурации и события активов.

По умолчанию эталонной считается конфигурация, которая была получена первой в результате успешного сбора данных по расписанию, указанному в настройках задачи сбора данных актива.

Просмотреть последние собранные конфигурации можно на странице **Инспекция активов** → **Конфигурации** (подробнее см. раздел «Просмотр сводки конфигураций»).

Сбор информации о конфигурациях ведется при помощи задач сбора данных, он может быть разовым или периодическим, с отложенным временем запуска или начиная с момента сохранения.

> Внимание:
>
> Перед настройкой сбора данных необходимо ознакомиться с рекомендациями, приведенными в справочном разделе «Рекомендации по настройке сбора данных».

13.2.1. Экспорт и импорт задач сбора данных, сканеров и их групп

В этом разделе:

- Импорт сканеров и их групп
- Импорт задач сбора данных
- Экспорт сканеров и их групп
- Экспорт задач сбора данных

Экспорт и импорт задач сбора данных, сканеров и их групп осуществляется на странице **Администрирование** → **Основные настройки** → **Импорт и экспорт** на панели **Сбор данных**.

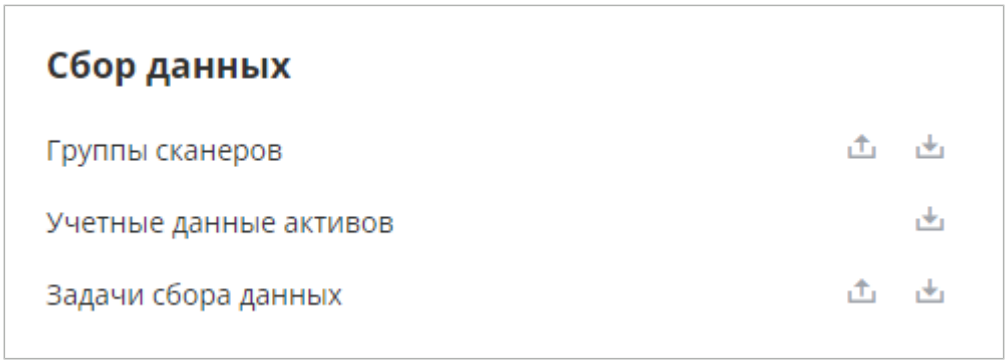


Рис. 204. Панель «Сбор данных» на странице «Импорт и экспорт»

13.2.1.1. Импорт сканеров и их групп

Для импорта сканеров из файла формата `*.json` в Комплекс:

1. Перейдите на страницу **Администрирование → Основные настройки → Импорт и экспорт**.
2. На панели **Сбор данных** в строке **Группы сканеров** нажмите кнопку (**Импортировать**).
3. В открывшемся окне укажите расположение импортируемого файла формата `*.json` и подтвердите выбор.
4. В открывшемся окне **Подготовка к импорту** выберите действие для элементов, которые отсутствуют в новом (загружаемом) справочнике:
   - **Оставить** — новые элементы будут добавлены к уже существующим;
   - **Удалить** — старые элементы будут удалены и добавлены новые.

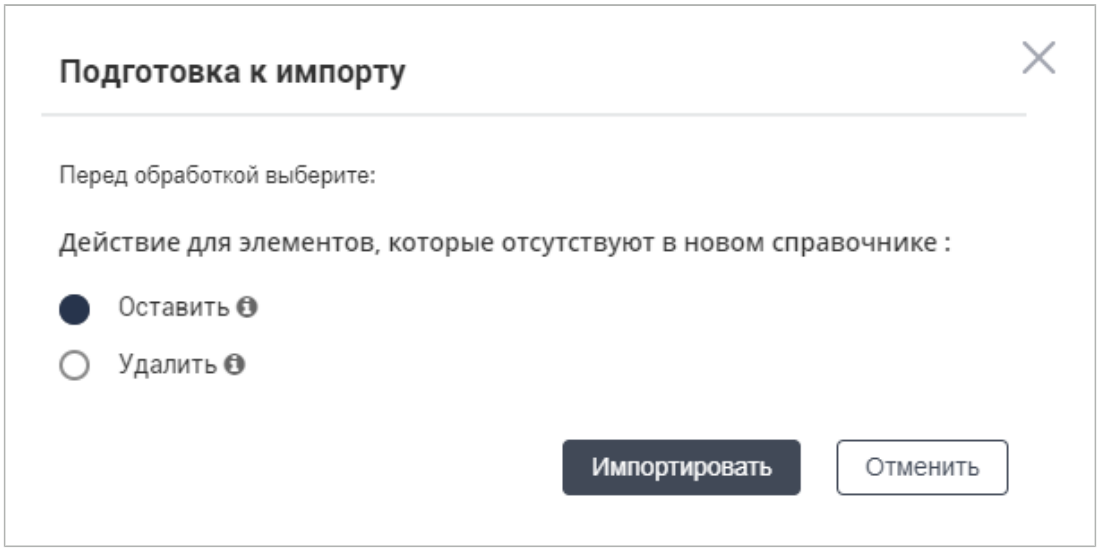


Рис. 205. Окно «Подготовка к импорту»

5. нажать кнопку **Импортировать** для выполнения импорта.
   - **Результат шага:** будет запущен процесс импорта: в правом верхнем углу появится уведомление `Запущен импорт справочника`, а под заголовком **Результат последнего импорта** будет символ `-`.

> Подсказка:
>
> Операции импорта являются фоновыми — со страницы можно безопасно уходить.

6. Убедитесь, что сканеры и их группы были успешно загружены. Для этого перейдите на страницу **Администрирование → Инспекция активов → Сканеры**.

13.2.1.2. Импорт задач сбора данных

Для импорта задач сбора данных из файла формата `*.json` в Комплекс:

1. Перейдите на страницу **Администрирование → Основные настройки → Импорт и экспорт**.
2. На панели **Сбор данных** в строке **Задачи сбора данных** нажмите кнопку **Импортировать**.
3. В открывшемся окне укажите расположение импортируемого файла формата `*.json` и подтвердите выбор.
4. В открывшемся окне **Подготовка к импорту** выберите действие для элементов, которые отсутствуют в новом (загружаемом) справочнике:
   - **Оставить** — новые элементы будут добавлены к уже существующим;
   - **Удалить** — старые элементы будут удалены и добавлены новые.

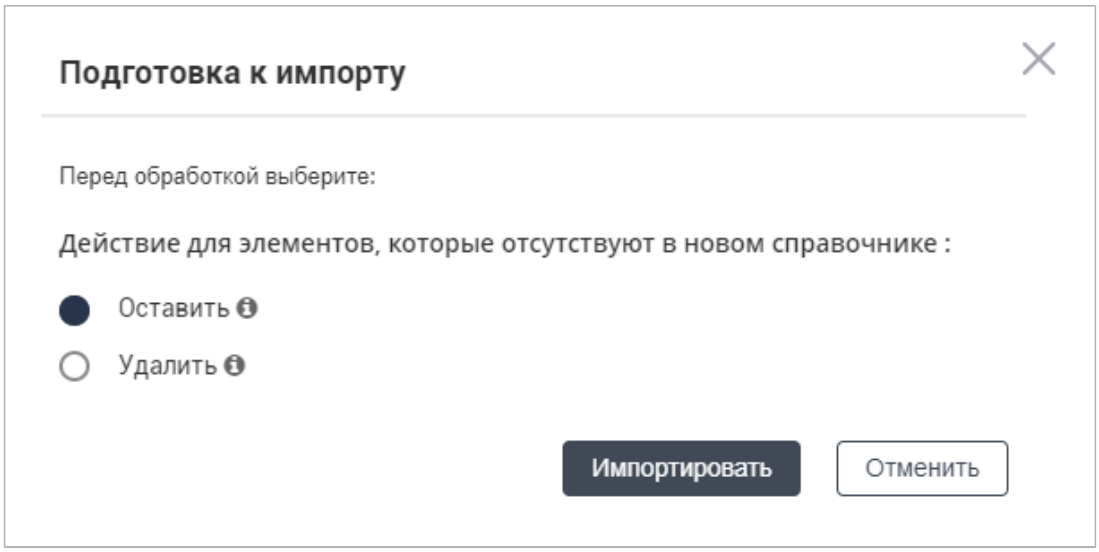


Рис. 206. Окно «Подготовка к импорту»

5. нажать кнопку **Импортировать** для выполнения импорта.
   - **Результат шага:** будет запущен процесс импорта: в правом верхнем углу появится уведомление `Запущен импорт справочника`, а под заголовком **Результат последнего импорта** будет символ `-`.

> Подсказка:
>
> Операции импорта являются фоновыми — со страницы можно безопасно уходить.

6. Убедитесь, что задачи были успешно загружены. Для этого перейдите на страницу **Инспекция активов → Задачи сбора**.

13.2.1.3. Экспорт сканеров и их групп

Для экспорта списка сканеров сбора данных и их групп в файл формата `*.json`:

1. Перейдите на страницу **Администрирование → Основные настройки → Импорт и экспорт**.
2. На панели **Сбор данных** в строке **Группы сканеров** нажмите кнопку (**Экспортировать**).
   - **Результат шага:** файл со списком сканеров и их групп `scanner_groups_[дата_и_время].json` будет сформирован и доступен для скачивания в правом верхнем углу страницы **Импорт и экспорт** под заголовком **Результат последнего экспорта**.

3. Для скачивания файла нажмите на его название в верхнем правом углу под заголовком **Результат последнего экспорта**.
4. В открывшемся окне укажите расположение для экспортируемого файла, при необходимости изменив его название, и нажмите кнопку **Сохранить**.
   - **Результат шага:** файл `scanner_groups_[дата_и_время].json` будет загружен на компьютер.

13.2.1.4. Экспорт задач сбора данных

Для экспорта списка задач сбора данных в файл формата `*.json`:

1. Перейдите на страницу **Администрирование → Основные настройки → Импорт и экспорт**.
2. На панели **Сбор данных** в строке **Задачи сбора данных** нажмите кнопку (**Экспортировать**).
   - **Результат шага:** файл со списком задач `collection_tasks_[дата_и_время].json` будет сформирован и доступен для скачивания в правом верхнем углу страницы **Импорт и экспорт** под заголовком **Результат последнего экспорта**.
3. Для скачивания файла нажмите на название сформированного файла под заголовком **Результат последнего экспорта**.
4. В открывшемся окне укажите расположение для экспортируемого файла, при необходимости изменив его название, и нажмите кнопку **Сохранить**.
   - **Результат шага:** файл `collection_tasks_[дата_и_время].json` будет загружен на компьютер.

13.2.2. Настройка сканеров сбора данных

В этом разделе:

- Создание сканера сбора данных
- Управление сканерами сбора данных
- Группировка сканеров сбора данных
- Настройка сканеров сбора данных с ПЛК Regul

В веб-интерфейсе Комплекса имеется возможность создания сканера для сбора данных с актива путем загрузки Python-скрипта сбора данных из файла в Комплекс. Создать сканер можно на странице **Сканеры**.

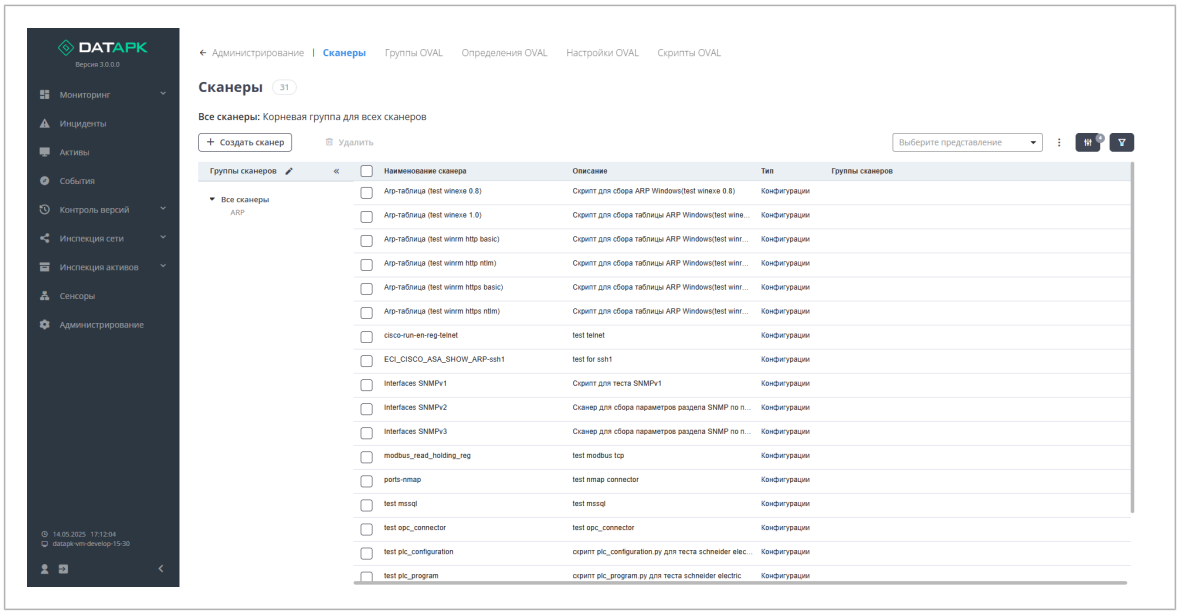


Рис. 207. Страница «Сканеры»

13.2.2.1. Создание сканера сбора данных

Для создания сканера вручную:

1. Создайте или получите от сервисного центра ООО «СайберЛимфа» файл формата `*.py`, содержащий скрипт для сбора необходимых данных. См. подробнее о содержании скрипта в разделе «Содержание Python-скриптов».
2. Если вы создали файл формата `*.py` вручную, обратитесь в сервисный центр ООО «СайберЛимфа» или к вашему администратору безопасности для получения закрытого ключа от сертификата `datapk_script.crt` и создайте цифровую подпись файла. См. подробнее о цифровой подписи в разделе «Цифровая подпись Python-скрипта».
3. Перейдите на страницу **Администрирование → Инспекция активов → Сканеры**.
4. Нажмите кнопку **Создать сканер**. В открывшемся окне **Настройки сканера** задайте следующие параметры:
    а. наименование и описание сканера;

> Внимание:
>
> Максимальная длина текста в поле **Наименование** — 255 символов. Максимальная длина текста в поле **Описание** — 100 символов.

    б. тип сканера (конфигурации, события, версия ОС или установленное ПО);
    в. группы сканеров (подробнее см. в разделе «Группировка сканеров сбора данных»);
    г. цифровую подпись (подробнее см. в разделе «Цифровая подпись Python-скрипта»);
    д. максимальное время ожидания выполнения задачи в минутах, при достижении которого сбор завершится ошибкой соединения;

> Внимание:
>
> Вводимое значение максимального времени ожидания выполнения задачи должно быть в диапазоне от 1 до 30.

e. нажмите кнопку **Импортировать** для загрузки скрипта из файла. В проводнике выберите и откройте подписанный ранее файл скрипта формата `*.py`;

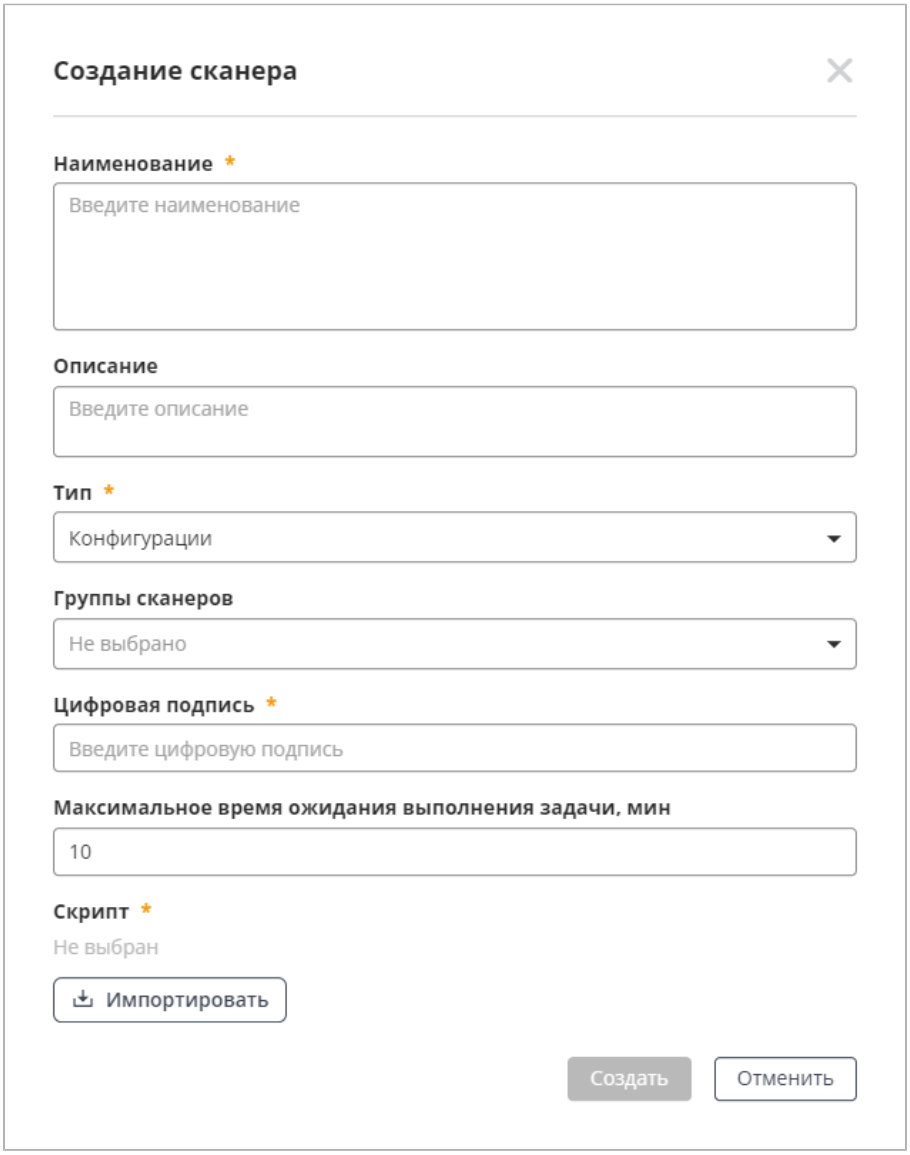


Рис. 208. Окно «Создание сканера»

5. Нажмите кнопку **Создать** для подтверждения изменений.

13.2.2.2. Управление сканерами сбора данных

13.2.2.2.1. Просмотр информации о сканере

Для просмотра:

1. Наведите курсор на строку со сканером, информацию о котором необходимо просмотреть.
2. Нажмите кнопку (**Просмотреть информацию о сканере**) напротив него.
   - **Результат шага:** появится окно **Просмотр информации о сканере**.

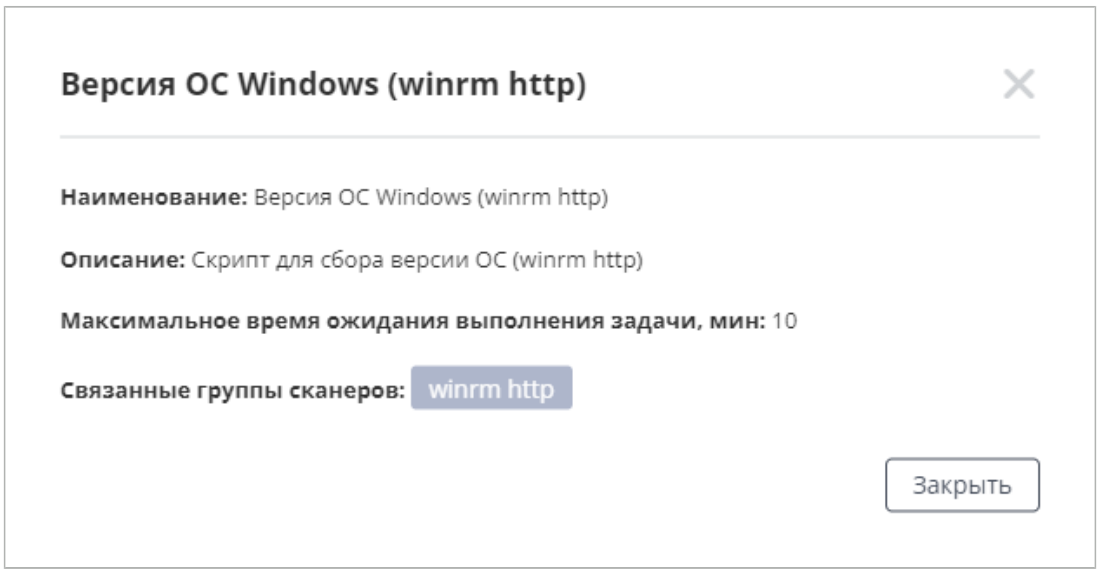


Рис. 209. Окно просмотра информации о сканере

3. Для выхода из окна нажмите **Закрыть**.

13.2.2.2.2. Запуск сканера

Для запуска:

1. Наведите курсор на строку со сканером, который необходимо запустить.
2. Нажмите кнопку (**Запустить сканирование**) напротив него.
   - **Результат шага:** появится окно **Запуск сканера**.
3. Выберите Комплекс и актив для сбора данных.

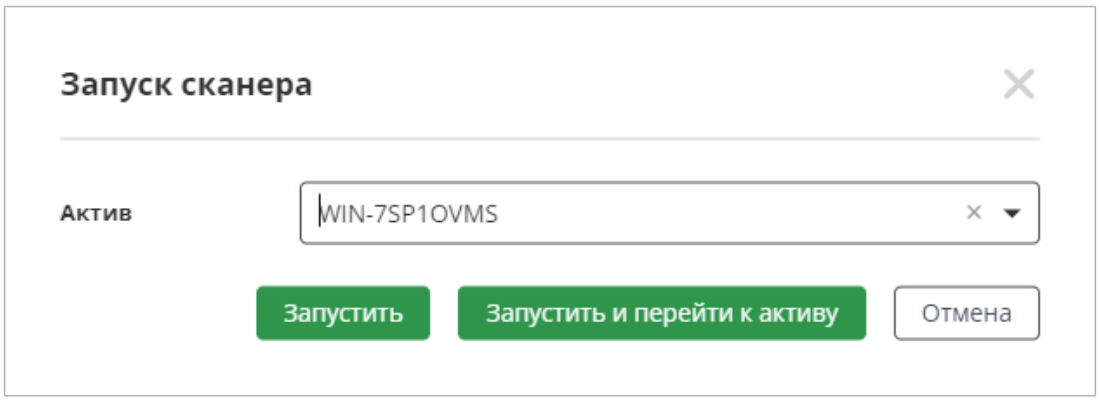


Рис. 210. Окно «Запуск сканера»

4. Нажмите **Запустить** или **Запустить и перейти к активу**.

13.2.2.2.3. Повторный запуск сканера

Для повторного запуска однократного сбора данных на активе:

1. Перейдите в раздел **Инспекция активов** -> **Статус сбора**.
   - **Результат шага:** откроется таблица **Статус сбора**.
2. При необходимости отфильтруйте список статусов, чтобы найти строку с требуемым активом и сканером, который ранее запускался на этом активе.
3. Нажмите кнопку (**Запустить сканирование повторно**) справа в выбранной строке таблицы.
   - **Результат шага:** появится уведомление об успешном запуске сканирования.

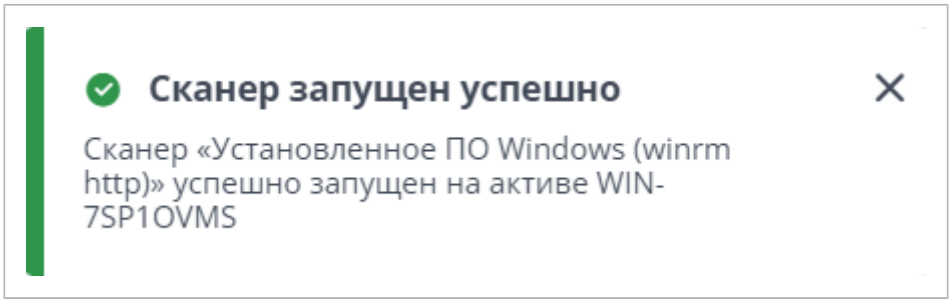


Рис. 211. Уведомление о запуске сканирования

13.2.2.2.4. Редактирование сканера

Для редактирования:

1. Наведите курсор на строку со сканером, который необходимо изменить.
2. Нажмите кнопку (**Редактировать**) напротив него.
   - **Результат шага:** появится окно **Редактирование сканера**.
3. Измените необходимые параметры сканера.

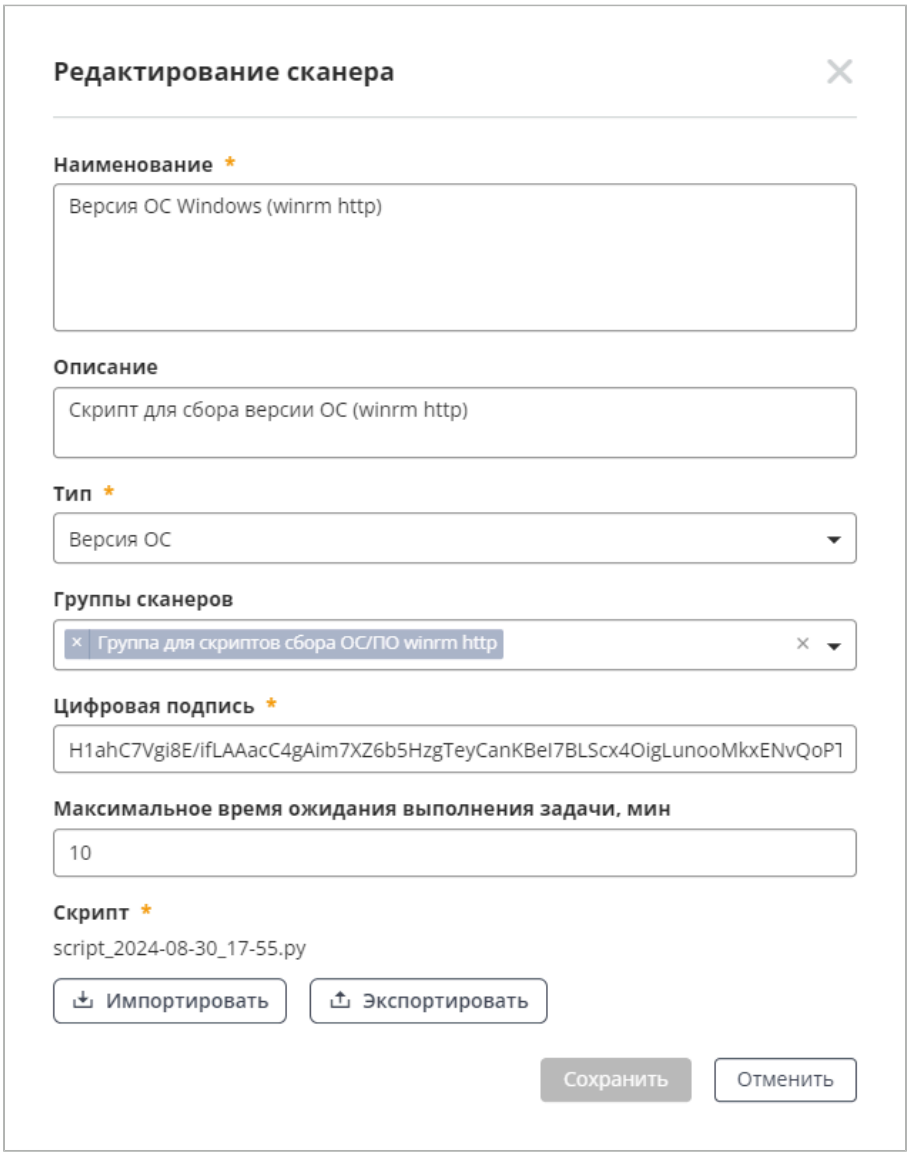


Рис. 212. Окно «Редактирование сканера»

4. Нажмите **Сохранить**.

13.2.2.2.5. Удаление сканера

Для удаления:

1. Наведите курсор на строку со сканером, который необходимо удалить.
2. Нажмите кнопку (**Удалить сканер**) напротив него.
   - **Результат шага:** появится окно предупреждения `При удалении сканера будут удалены конфигурации, собранные этим сканером.`

3. Введите обоснование удаление сканера и нажмите **Подтвердить**.

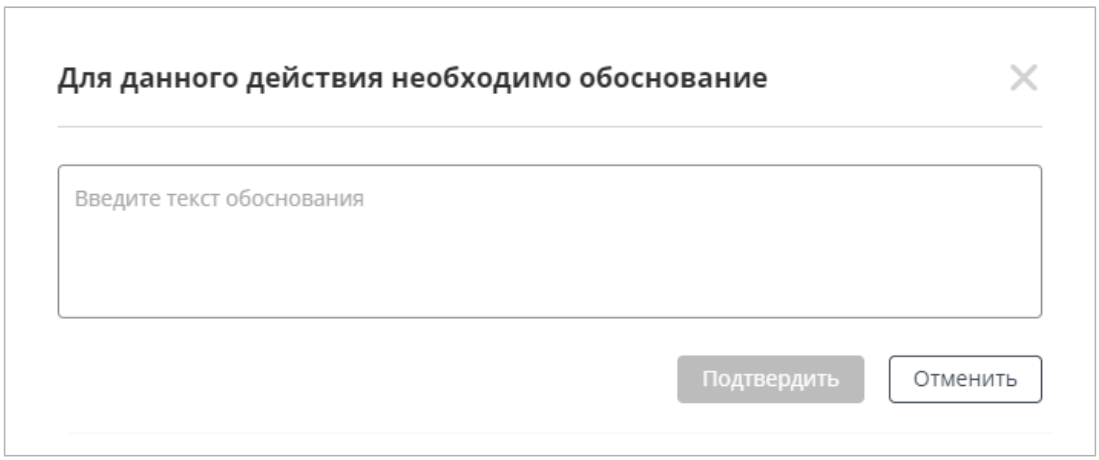


Рис. 213. Окно предупреждения и ввода обоснования удаления сканера

13.2.2.2.6. Групповое удаление сканеров

Для удаления группы сканеров:

1. Получите необходимую выборку сканеров:
   а. Выберите группу сканеров в левой части страницы.
   б. При необходимости отфильтруйте список сканеров: нажмите кнопку , выберите настройки фильтрации и нажмите кнопку **Применить**.
   в. Отметьте все отфильтрованные сканеры на удаление с помощью чекбокса в заголовке таблицы, либо отметьте отдельные сканеры с помощью чекбоксов рядом со сканерами.
2. Нажмите кнопку Удалить в верхней части страницы.
   ▸ **Результат шага:** появится окно предупреждения `При удалении сканеров будут удалены конфигурации, собранные этими сканерами.`
3. В открывшемся окне введите обоснование удаления сканеров и нажмите кнопку **Подтвердить**.

13.2.2.3. Группировка сканеров сбора данных

В этом разделе:

- Создание группы сканеров
- Добавление сканеров в группу
- Управление группами сканеров

Для использования сканеров в задачах необходима группировка существующих сканеров сбора данных. Группы сканеров отображаются на странице **Сканеры** в левой части страницы.

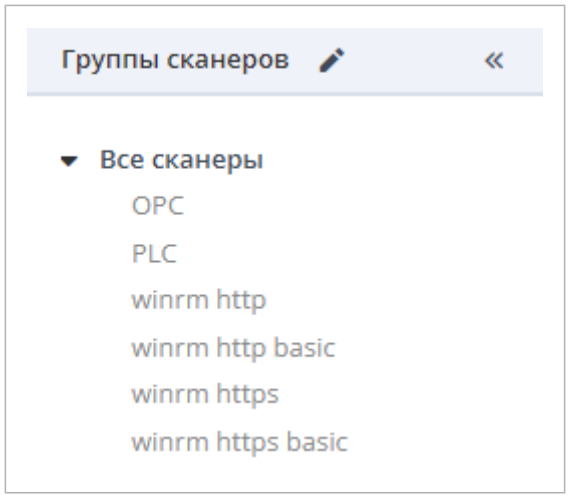


Рис. 214. Панель управления сканерами сбора данных

Если в списке выбрана конкретная группа сканеров, то фильтры будут применяться только для элементов этой группы.

13.2.2.3.1. Создание группы сканеров

Для создания группы сканеров:

1. Перейдите на страницу **Администрирование → Инспекция активов → Сканеры**.
2. Над панелью с группами сканеров в левой части страницы нажмите **Редактировать**.
   - **Результат шага:** появится окно **Редактирование групп сканеров**.
3. Нажмите кнопку ➕ напротив группы, которая будет вышестоящей для создаваемой.

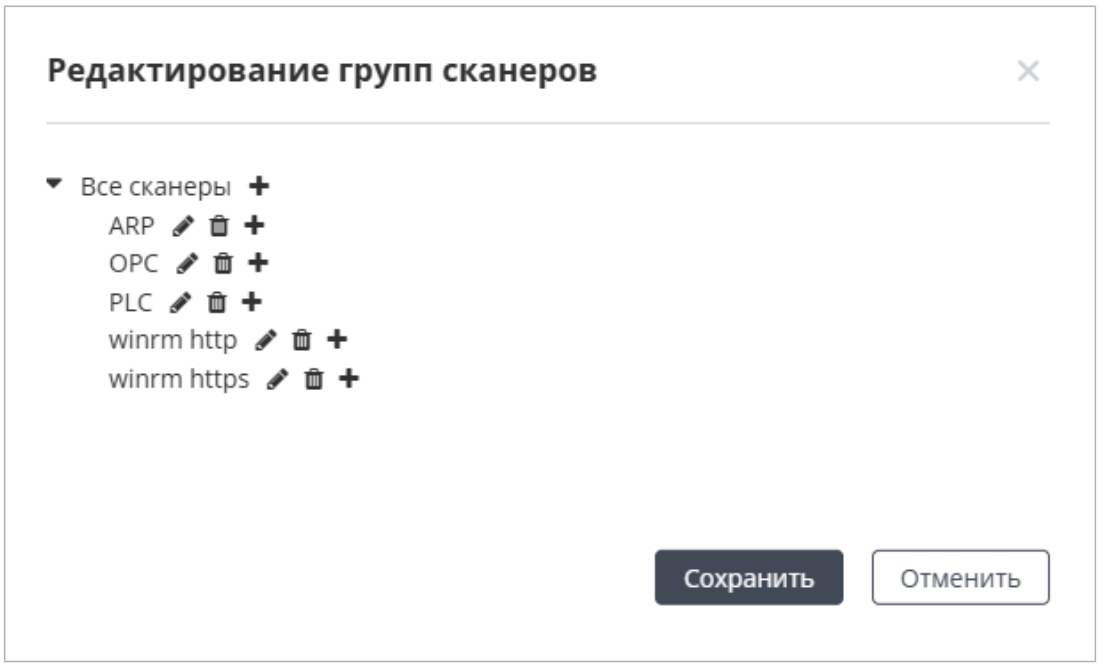


Рис. 215. Окно «Редактирование групп сканеров»

   - **Результат шага:** появится окно **Создание группы сканеров**.
4. В окне создания задайте наименование и описание новой группы. При необходимости выберите другую вышестоящую группу.

Внимание:

Наименование группы сканеров должно быть уникальным.

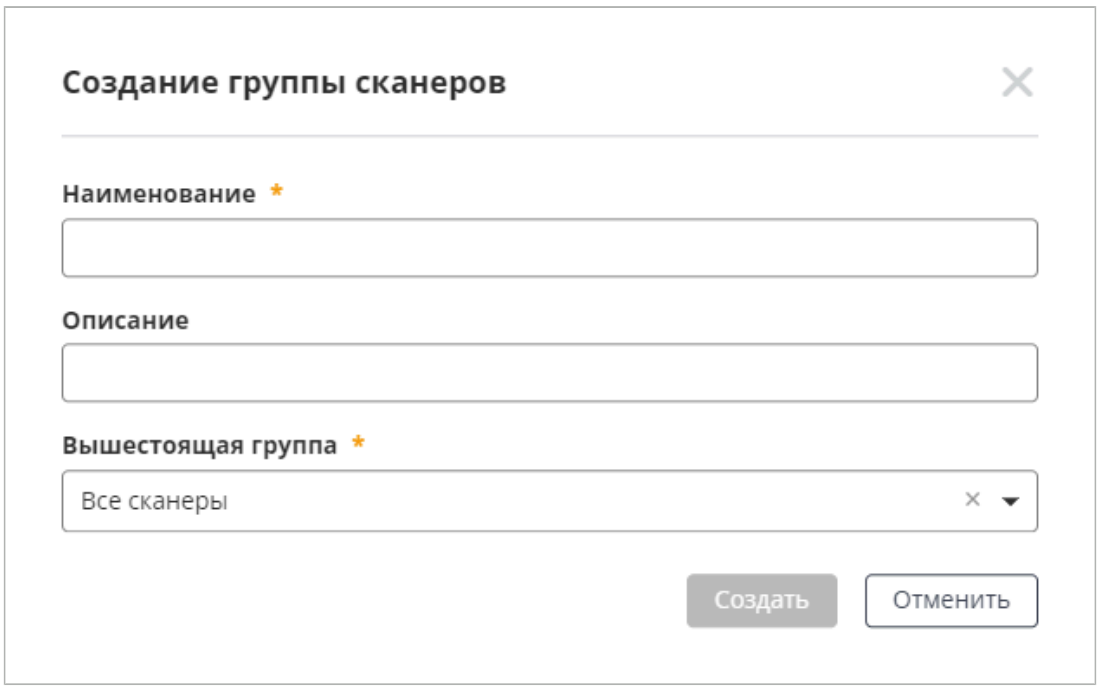


Рис. 216. Окно «Создание группы сканеров»

5. Нажмите кнопку **Сохранить** для подтверждения изменений.

Внимание:

Без сохранения всех изменений групп в в окне редактирования групп сканеров изменения не будут отражены в Комплексе.

- **Результат шага:** созданная группа появится в списке в окне **Редактирование групп сканеров**.

6. При необходимости добавьте другие группы сканеров.
7. В окне **Редактирование групп сканеров** нажмите **Сохранить**.
   - **Результат шага:** появится предупреждение о неизменности задач сбора данных в результате изменения состава групп.
8. Нажмите **Подтвердить** для сохранения изменения состава групп.
   - **Результат шага:** окно редактирования групп будет закрыто, изменения появятся в Комплексе.

Внимание:

В одну группу сканеров можно добавить до 10 групп. При попытке добавления более 10 групп сканеров возникнет предупреждение об ошибке `Уровень вложенности групп превышает максимальный (10)`

13.2.2.3.2. Добавление сканеров в группу

> Подсказка:
>
> Сканер может быть добавлен в несколько групп.

Для добавления сканеров в ранее созданную группу:

1. Перейдите на страницу **Администрирование → Инспекция активов → Сканеры**.
2. Добавьте сканеры в группу. Для этого:
   a. Выделите при помощи курсора сканеры, которые будут добавлены в группу.

> Подсказка:
>
> Для выделения множества строк выше или ниже выбранной нажмите клавишу **Shift** и выделите строку с последним сканером, который необходимо добавить в группу.

> Внимание:
>
> Рекомендуется добавлять в группу не более 30 сканеров сбора данных.

   б. Наведите курсор на один из выделенных сканеров и зажмите левую кнопку мыши.
   - **Результат шага:** появится полупрозрачный квадрат с количеством выделенных сканеров.

   в. Не отпуская левую кнопку мыши, перетащите сканеры в левую часть страницы так, чтобы курсор оказался на наименовании группы, в которую будут перемещены сканеры.
   г. Отпустите левую кнопку мыши.

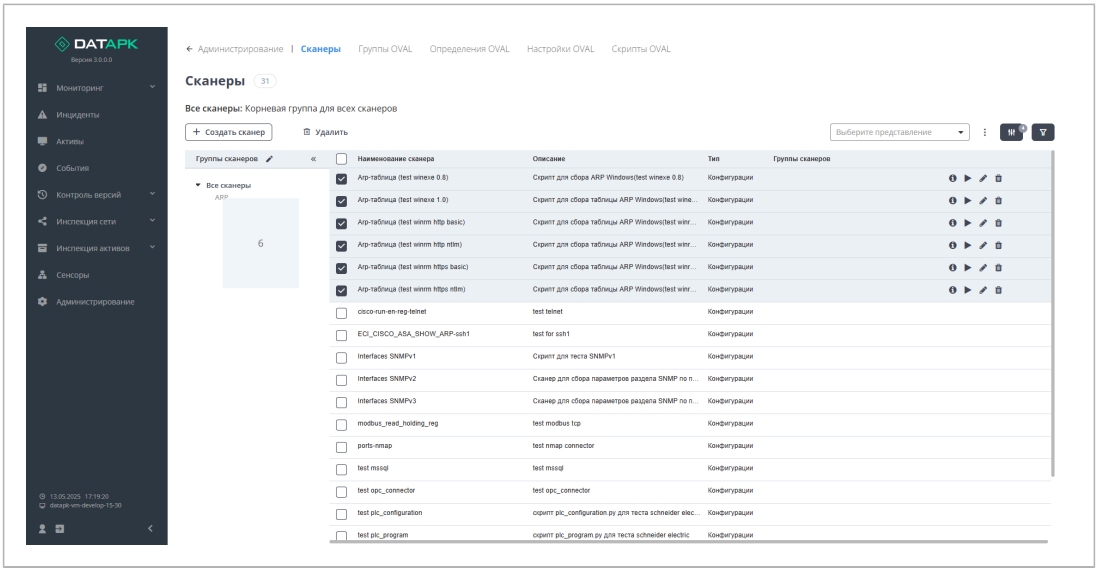


Рис. 217. Добавление сканеров в группу

   - **Результат шага:** появится окно подтверждения добавления сканеров в группу.
3. Для подтверждения переноса нажмите **Подтвердить**.

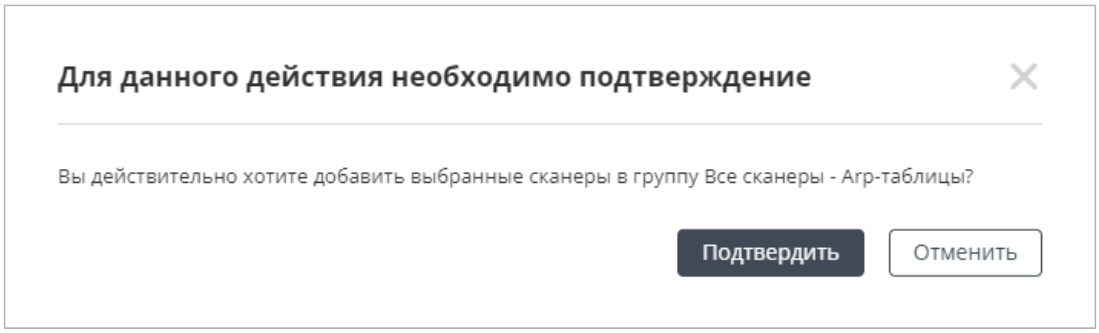


Рис. 218. Окно подтверждения перемещения сканеров

- **Результат шага:** в правом вернем углу появится уведомление: `Добавление в группу выбранных сканеров успешно завершено`, и сканеры будут добавлены в группу. Если некоторые сканеры уже были в выбранной группе, отобразится предупреждение: `Объект уже существует`, и в группу будут добавлены сканеры, которых не было в группе.

4. При необходимости изменить группу можно также в окне редактирования сканера. См. подробнее в разделе «Управление сканерами сбора данных».

Что дальше: Если необходимо исключить сканер из группы, измените соответствующее поле в окне **Редактирование сканера**.

13.2.2.3.3. Управление группами сканеров

На странице **Администрирование → Инспекция активов → Сканеры** предусмотрены следующие возможности для управления группами сканеров:

1. Изменение группы. Для изменения:
   a. Над панелью с группами сканеров в левой части страницы нажмите **Редактировать**.
   - **Результат шага:** появится окно **Редактирование групп сканеров**.

   б. Нажмите кнопку ✎ напротив группы, которую необходимо изменить.

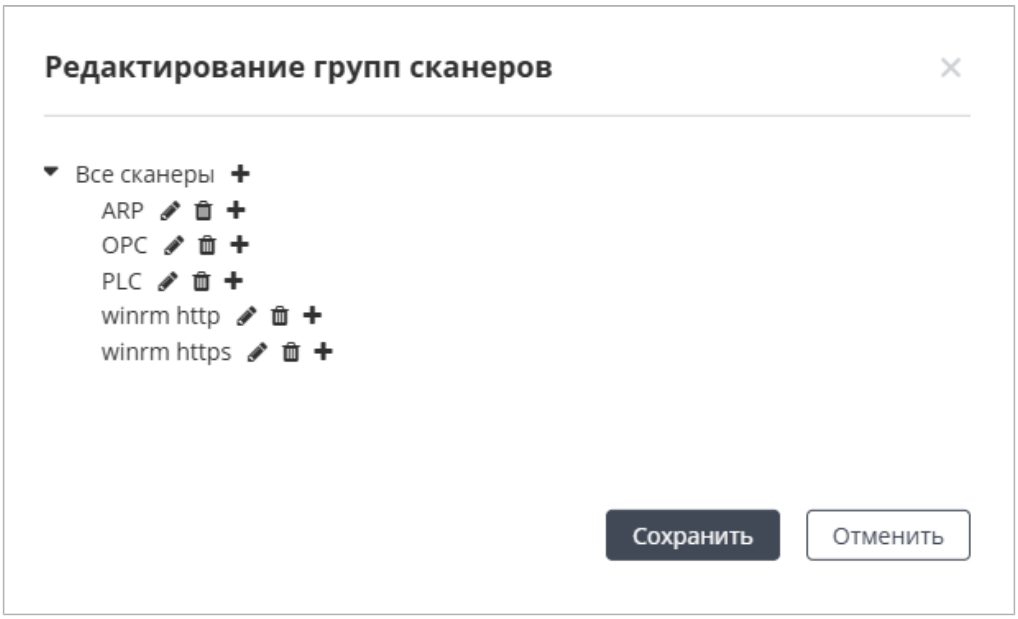


Рис. 219. Окно «Редактирование групп сканеров»

- **Результат шага:** появится окно **Редактирование группы сканеров**.

в. Измените необходимые параметры группы сканеров.

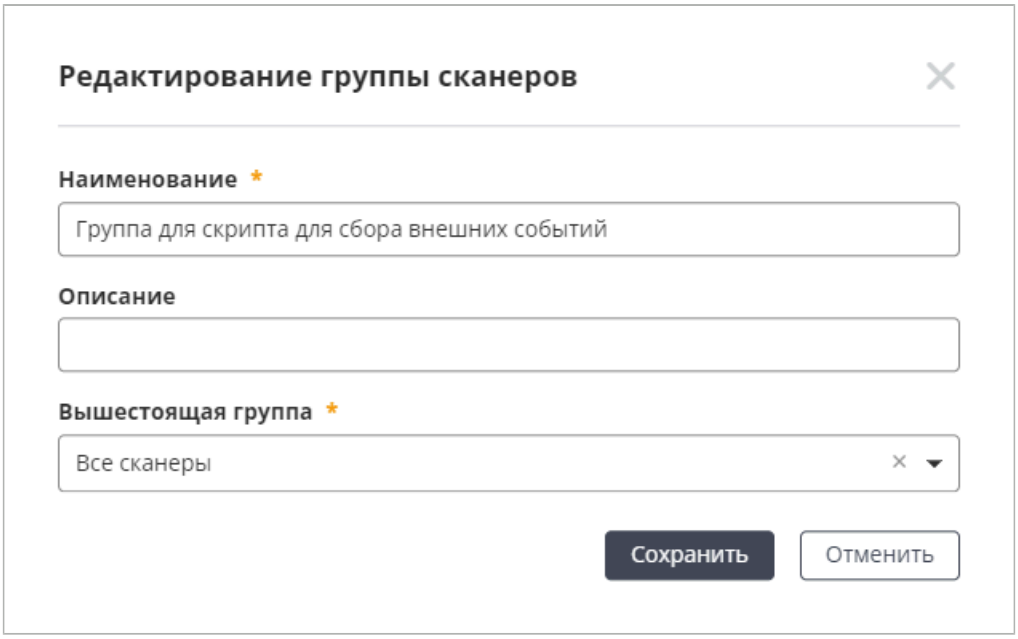


Рис. 220. Окно «Редактирование группы сканеров»

г. Нажмите кнопку **Сохранить** для подтверждения изменений.

> Внимание:
>
> Без сохранения всех изменений групп в в окне редактирования групп сканеров изменения не будут отражены в Комплексе.

- **Результат шага:** изменения названия группы появятся в окне **Редактирование групп активов**.

д. При необходимости измените другие группы сканеров.

е. В окне **Редактирование групп сканеров** нажмите **Сохранить**.

- **Результат шага:** появится предупреждение о неизменности задач сбора данных в результате изменения состава групп.

ж. Нажмите **Подтвердить** для сохранения изменения состава групп.

- **Результат шага:** окно редактирования групп будет закрыто, изменения появятся в Комплексе.

2. Удаление группы. Для удаления:

а. Над панелью с группами сканеров в левой части страницы нажмите **Редактировать**.

- **Результат шага:** появится окно **Редактирование групп сканеров**.

б. Нажмите кнопку напротив группы, которую необходимо удалить.

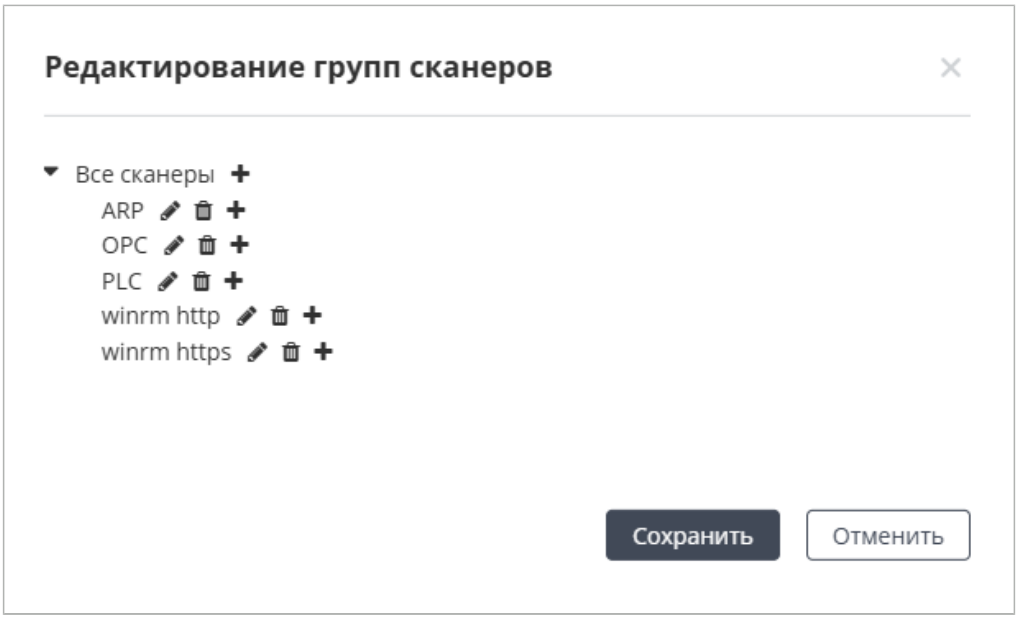


Рис. 221. Окно «Редактирование групп сканеров»

- **Результат шага:** группа сканеров будет удалена, но данные изменения не будут сохранены до нажатия **Сохранить** в окне редактирования групп сканеров.

в. При необходимости измените другие группы сканеров.

г. В окне «Редактирование групп сканеров» нажмите **Сохранить**.

- **Результат шага:** появится предупреждение о неизменности задач сбора данных в результате изменения состава групп. Это значит, что удаляемые группы останутся в задачах сбора данных, если такие были созданы. Для возобновления периодического сбора измените или создайте задачи заново, в том числе при помощи копирования.

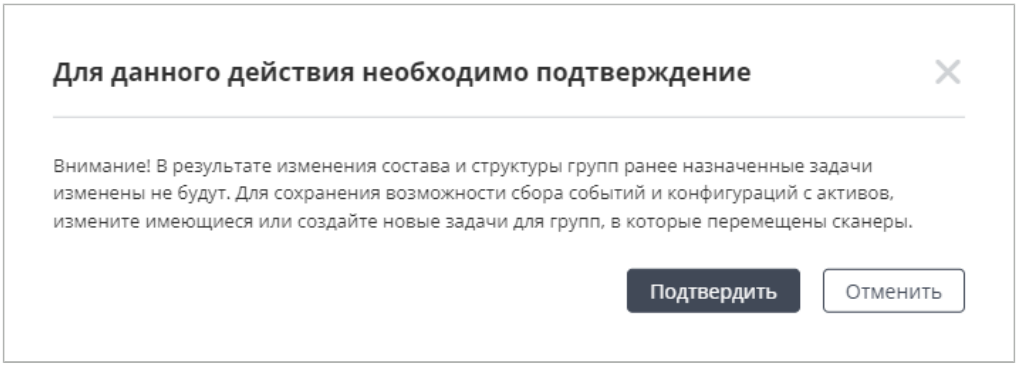


Рис. 222. Окно подтверждения изменений групп

д. Нажмите **Подтвердить** для сохранения изменения состава групп.

- **Результат шага:** окно редактирования групп будет закрыто, изменения появятся в Комплексе.

13.2.2.4. Настройка сканеров сбора данных с ПЛК Regul

Для сбора данных с ПЛК Regul необходимо настроить актив, с которого будут собираться данные. Способы настройки различаются в зависимости от протокола сбора данных. Ниже описаны способы настройки для протоколов OPC UA, SNMPv3 и FTP.

1. Для настройки сканера сбора контрольных сумм с ПЛК Regul по протоколу OPC UA:
    a. Активируйте и настройте сервер OPC UA на ПЛК.
    б. Создайте пользователя для подключения и назначьте ему права `ro`.
    в. Добавьте программу `CHECKSUM_PRG` в проект.
    г. Добавьте и настройте объект **Символьная конфигурация**.
    д. Установите тег `OPCUA` на активе.
    e. В настройках тега укажите логин и пароль ранее созданного пользователя.
2. Для настройки сканера сбора контрольных сумм с ПЛК Regul по протоколу SNMPv3:
    a. Активируйте SNMPv3 на ПЛК.
    б. Установите активу следующие теги и учетные данные:
        - тег `snmp3`, логин `Administrator`;
        - тег `auth`, логин `HMAC_SHA`, пароль `Administrator`;
        - тег `priv`, логин `AES_128`, пароль `Administrator`.
3. Для настройки сканера сбора контрольных сумм с ПЛК Regul по протоколу FTP:
    a. Активируйте и настройте сервер FTP на ПЛК.
    б. Создайте пользователя для подключения и назначьте ему права `rw`.
    в. В настройках сервера FTP добавьте IP-адрес Комплекса в доверенные.
    г. Установите тег `FTP` на активе.
    д. В настройках тега укажите логин и пароль ранее созданного пользователя.
    e. Установите тег `program_filename` на активе, в качестве логина установите название файла программы ПЛК.

13.2.3. Сбор данных с активов

В этом разделе:

- Настройка активов для сбора данных
- Создание задачи сбора данных
- Управление задачами сбора данных
- Однократный сбор данных

Для сбора конфигураций и событий в веб-интерфейсе Комплекса доступна настройка задач сбора данных. Задачи позволяют сбор событий и конфигураций. Настройка задач производится на странице **Задачи сбора**.

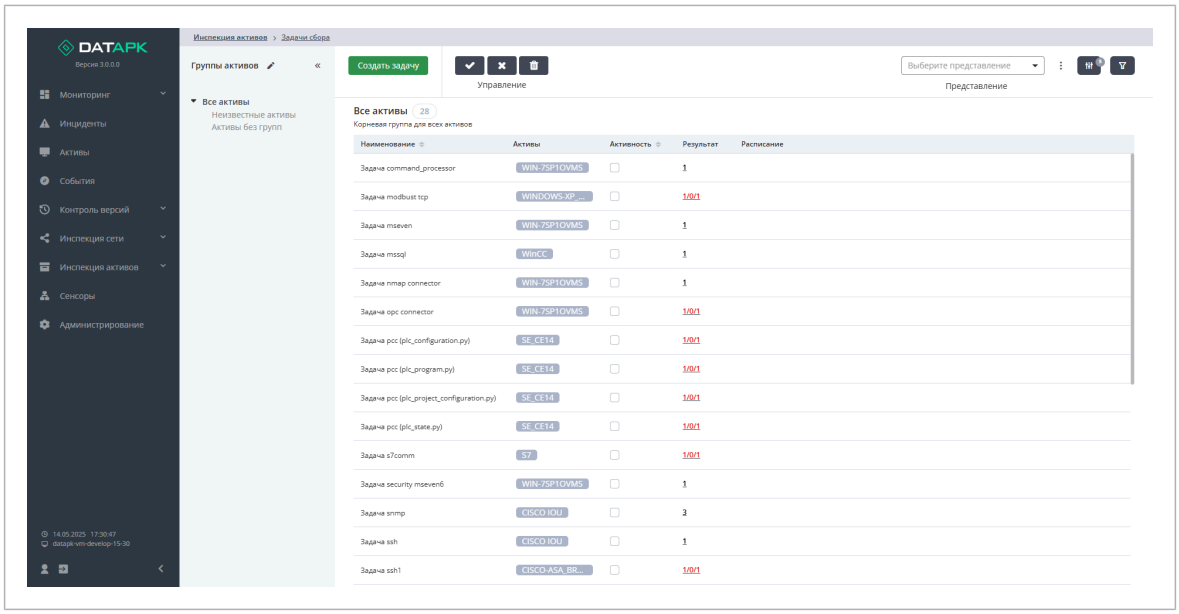


Рис. 223. Страница «Задачи сбора данных»

После выполнения задач доступен запуск сканеров в их составе по одному. Запуск сканеров осуществляется из карточки актива.

13.2.3.1. Настройка активов для сбора данных

Для сбора данных необходимо убедиться, что на активах добавлены и применены учетные данные и выбран сетевой интерфейс сбора данных.

Для подготовки актива к активному сбору данных:

1. Убедитесь, что учетные данные для доступа к активу были добавлены ранее. Для этого перейдите на страницу **Активы → Настройка активов→ Учетные данные**.

   > Подсказка:
   >
   > Подробнее о добавлении учетных данных см. в разделе «Добавление учетных данных актива».

2. Перейдите на страницу **Активы**.
3. Выберите из списка актив, для которого будет настроен сбор данных, и нажмите на его иконку или наименования.
   - **Результат шага:** откроется карточка актива.
4. Нажмите кнопку напротив блока **Учетные данные**.
5. Установите чекбокс рядом с добавленной ранее учетной записью для привилегированного доступа к активу и нажмите кнопку **Сохранить**.

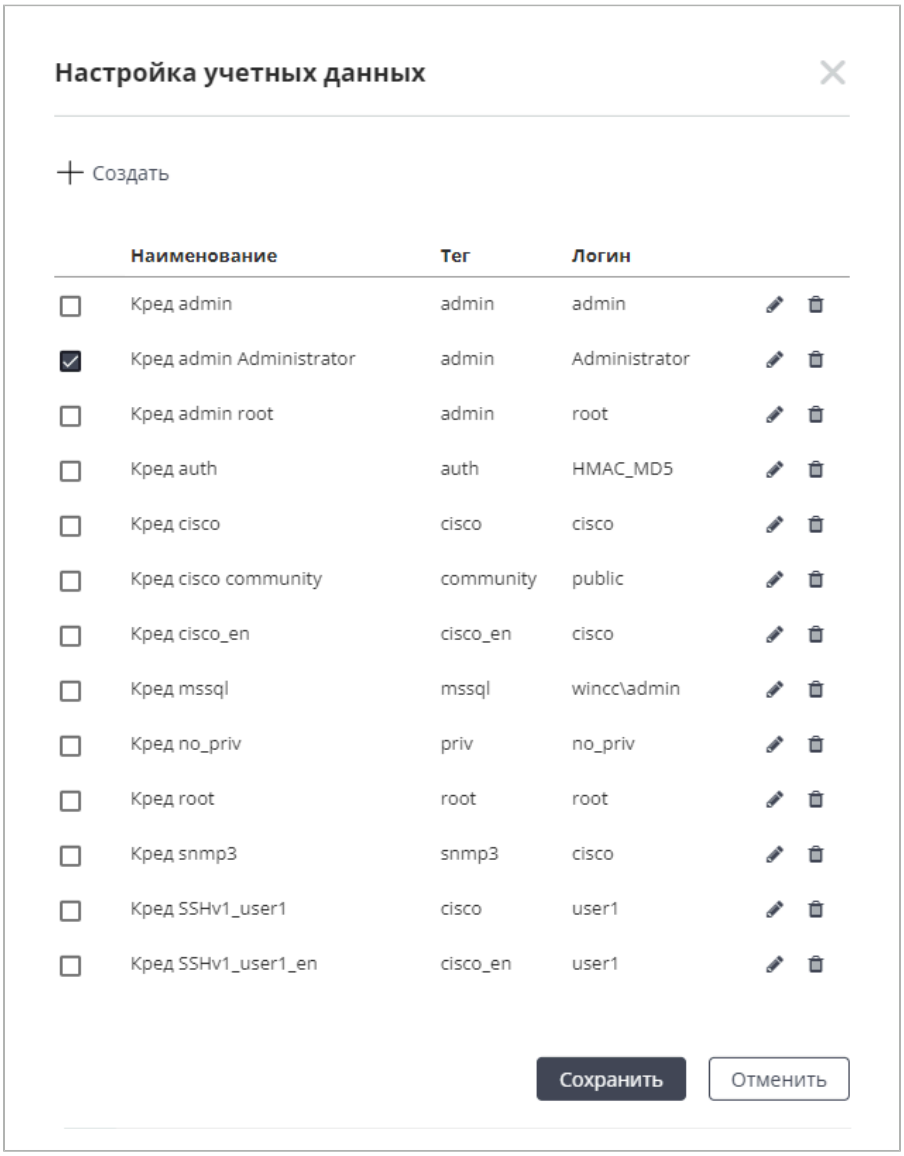


Рис. 224. Окно «Настройка учетных данных»

Внимание:

Невозможно назначить активу учетные записи с одинаковыми тегами. При попытке назначения активу учетных записей с одинаковыми тегами появится уведомление `Ошибка: Выбор нескольких учетных данных с одинаковым тегом запрещен`

6. Если интерфейс для сбора данных с актива не был выбран ранее:
    a. нажать ✎ напротив блока **Сетевые атрибуты**;
    б. В открывшемся окне **Редактирование сетевых атрибутов актива** Выбрать из списка интерфейс для сбора данных и отметьте параметр **Интерфейс для сбора данных** при помощи чекбокса в левой части таблицы.

> **Внимание:**
>
> - У актива всегда должен быть интерфейс сбора данных — при попытке сохранения сетевых атрибутов актива при условии, что ни один атрибут не выбран в качестве интерфейса сбора, появится предупреждение: `Ошибка! Не выбран интерфейс сбора данных. Установите чекбокс напротив сетевых атрибутов для их выбора в качестве интерфейса сбора данных.`
> - Только один сетевой атрибут актива может быть выбран в качестве интерфейса сбора данных.

в. нажать кнопку (**Сохранить изменения**) напротив редактируемого сетевого интерфейса.

13.2.3.2. Создание задачи сбора данных

Для создания задачи сбора данных:

1. Перейдите на страницу **Инспекция активов → Задачи сбора**.

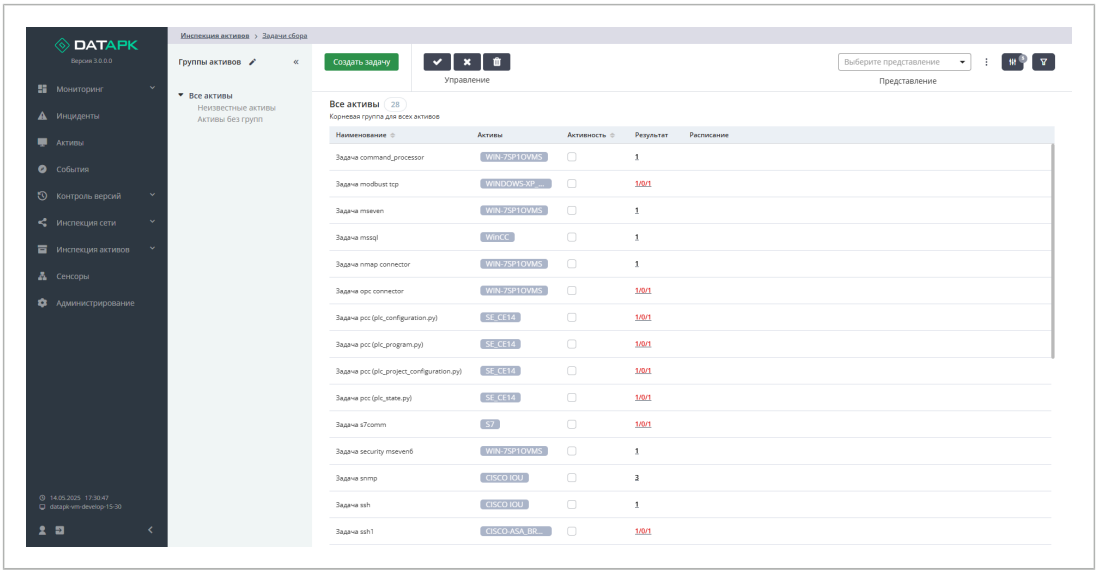


Рис. 225. Страница «Задачи сбора данных»

2. В верхней части страницы нажмите **Создать задачу**.
   - **Результат шага:** появится окно **Создание задачи**.
3. Задайте следующие параметры создаваемой задаче:
   - наименование;

> **Внимание:**
>
> Допускается вводить не более 255 символов.

   - описание;
   - чекбокс **Активность задачи** для запуска выполнения задачи по установленному расписанию;
   - дату и время начала отсчета расписания;

- тип запуска: однократный для сбора в указанную дату и время, либо периодический для повторяющегося многократного сбора после указанной даты и времени;

  > Внимание:
  >
  > При выборе периодического типа запуска первый сбор данных по задаче произойдет через указанный период в указанную дату. Например, если 01.01.2022 в 10.00 выбрать время запуска расписания `Сейчас` и периодический тип запуска с интервалом в один час (`0 * * * *`), то первый сбор данных произойдет 01.01.2022 в 11.00, второй — в 01.01.2022 в 12.00 и будет продолжаться, пока пользователь не удалит задачу.

- активы и (или) их группы;

  > Внимание:
  >
  > При использовании групп активов сбор производится для всех вложенных групп. Например, при использовании в задаче группы активов `Windows` сбор данных будет также производиться с вложенных групп `Windows 7` и `Windows 10`.

- группы сканеров.

  > Внимание:
  >
  > Не рекомендуется использовать группы, количество сканеров в которых превышает 30. Подробнее о группах сканеров см. в разделе «Группировка сканеров сбора данных».

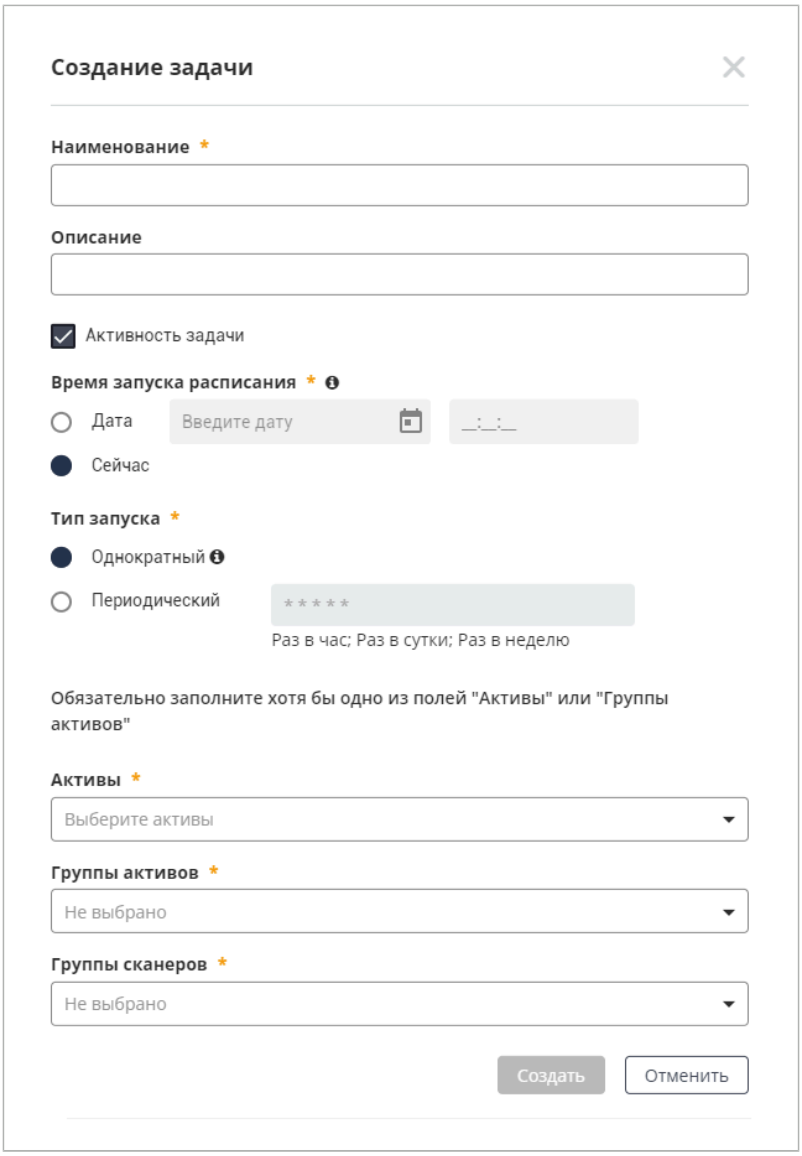


Рис. 226. Окно «Создание задачи»

4. Нажмите **Создать**.

   ▸ **Результат шага:** состояние сбора данных будет отображаться на странице **Статус сбора**, а также на странице **Задачи сбора**.

> Подсказка:
>
> При возникновении ошибок см. раздел «Просмотр статуса сбора данных».

13.2.3.3. Управление задачами сбора данных

Для управления задачами сбора конфигураций и событий веб-интерфейсе Комплекса предусмотрены следующие возможности:

1. Редактирование задачи сбора данных.

   > Внимание:
   >
   > Редактирование доступно только для задач, содержащих расписание. Для задач с однократным типом запуска воспользуйтесь возможностью копирования.

   Для изменения параметров задачи:

   а. Перейдите на страницу **Инспекция активов → Задачи сбора**.

   б. Наведите курсор на правую часть строки с задачей, которую необходимо изменить.

   в. Нажмите кнопку (**Редактировать**).

   - **Результат шага:** появится окно **Редактирование задачи**.

   г. Измените необходимые параметры задачи.

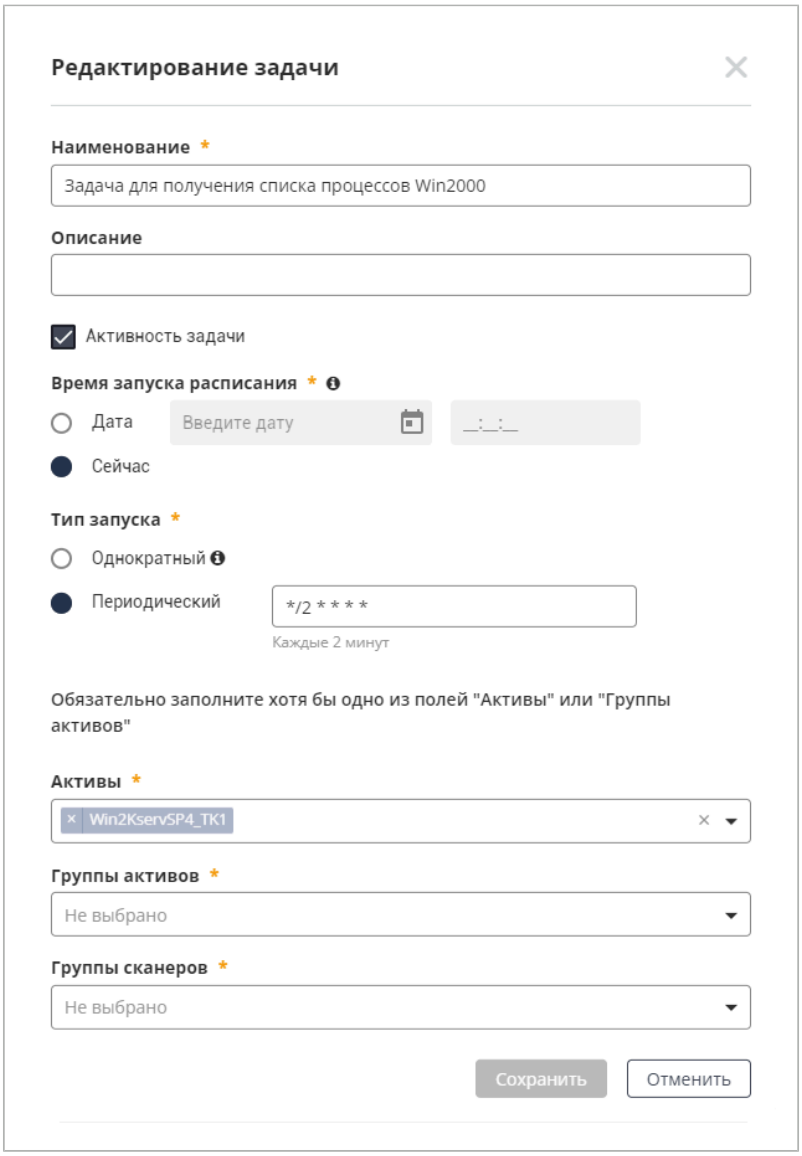


Рис. 227. Окно «Редактирование задачи»

д. Нажмите **Сохранить**.

2. Копирование задачи сбора данных. Для копирования:

   а. Перейдите на страницу **Инспекция активов** → **Задачи сбора**.

   б. Наведите курсор на правую часть строки с задачей, которую необходимо скопировать.

   в. Нажмите (**Копировать задачу**).

   ▸ **Результат шага:** появится окно **Копирование задачи**, в котором автоматически будет добавлена текущая дата и время в конце наименования задачи.

   г. При необходимости измените параметры задачи.

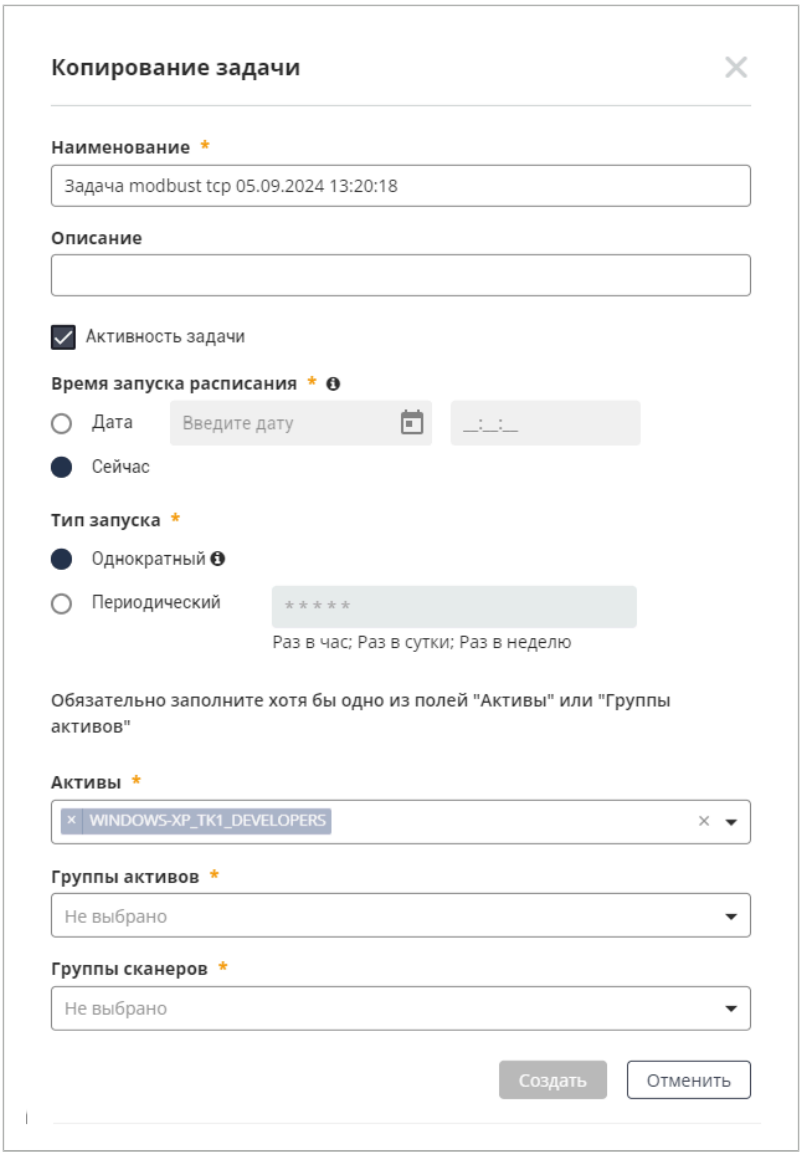


Рис. 228. Окно «Копирование задачи»

д. Нажмите **Создать**.

▸ **Результат шага:** задача будет запускаться с новыми параметрами. Если наименование задачи изменено, на странице **Статус сбора** новое наименование задачи будет отображаться только для новых процессов сбора.

3. Удаление задачи сбора данных. Для удаления:

   а. Перейдите на страницу **Инспекция активов → Задачи сбора**.

   б. Наведите курсор на правую часть строки с задачей, которую необходимо удалить.

   в. Нажмите кнопку (**Удалить задачу**).

   ▸ **Результат шага:** появится окно подтверждения удаления задачи.

г. Введите обоснование удаления задачи и нажмите **Подтвердить**.

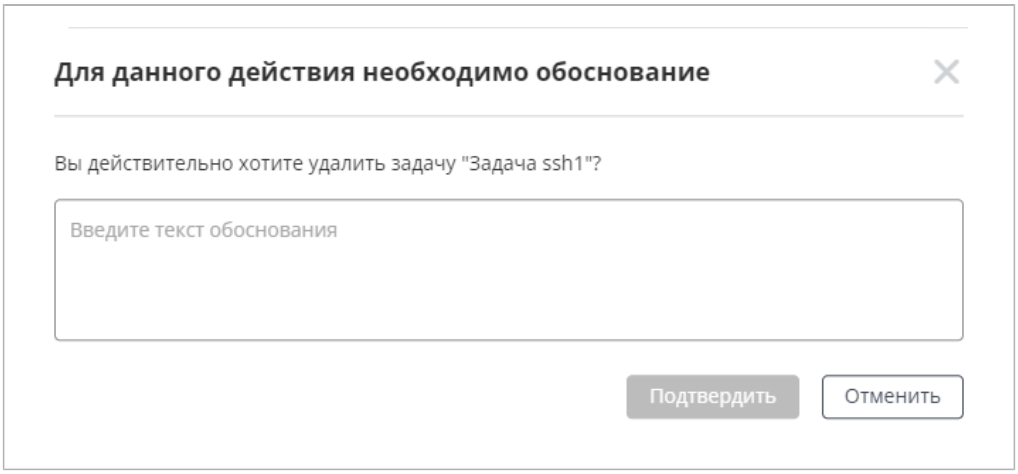


Рис. 229. Окно ввода обоснования удаления задачи

4. Групповое удаление задач сбора данных. Для удаления:
   a. Перейдите на страницу **Инспекция активов** → **Задачи сбора**.
   a. Нажмите кнопку (**Удалить**).
   - **Результат шага:** появится окно подтверждения удаления задач.
   б. Введите обоснование удаления задач и нажмите **Подтвердить**.

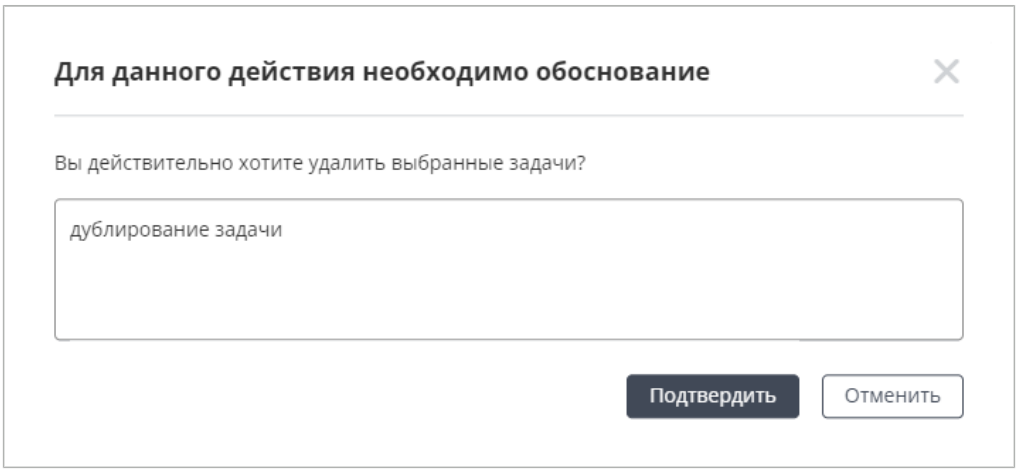


Рис. 230. Окно ввода обоснования удаления задачи

- **Результат шага:** задача будет удалена. На странице **Статус сбора** сохранятся записи о процессах, завершенных в рамках удаленной задачи.

13.2.3.4. Однократный сбор данных

Для однократного запуска сбора данных с актива:

1. Перейдите на страницу **Администрирование** → **Инспекция активов** → **Сканеры**.
2. Наведите курсор на сканер, который планируется запустить.
3. Нажмите кнопку (**Запустить сканирование**) справа от сканера.
   - **Результат шага:** появится окно **Запуск сканера**.
4. В открывшемся окне выберите актив, с которого необходимо собрать данные.

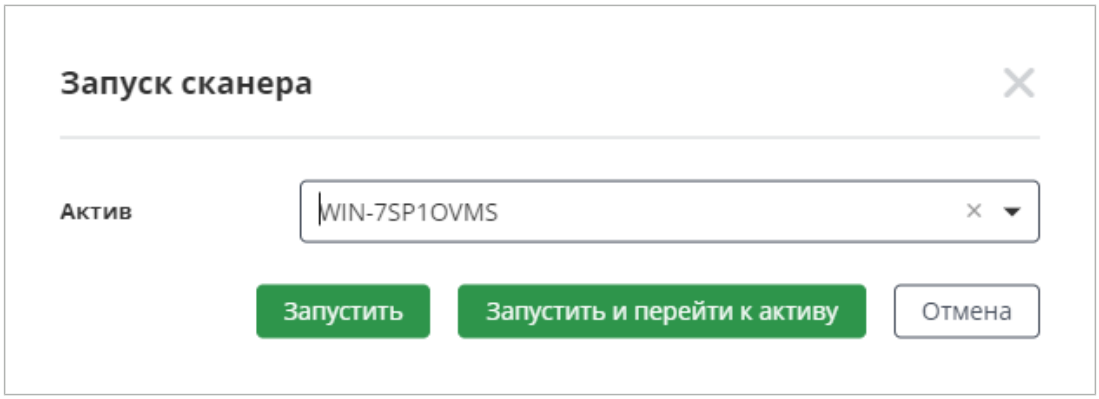


Рис. 231. Окно «Запуск сканера»

5. Нажмите **Запустить и перейти к активу**.
   - **Результат шага:** откроется карточка актива.
6. Нажмите на ссылку **Статус сбора данных** в разделе **Связанные данные**.
   - **Результат шага:** откроется страница **Статус сбора** с информацией о состоянии сбора данных выбранного актива.

> Подсказка:
>
> При возникновении ошибок сбора данных см. раздел «Просмотр статуса сбора данных».

13.2.4. Просмотр статуса сбора данных

Если на каком-то этапе выполнения задач сбора данных возникают ошибки или сбор данных завершается не так, как ожидалось, краткие результаты сбора можно просмотреть на странице **Задачи сбора** в колонке **Результат**.

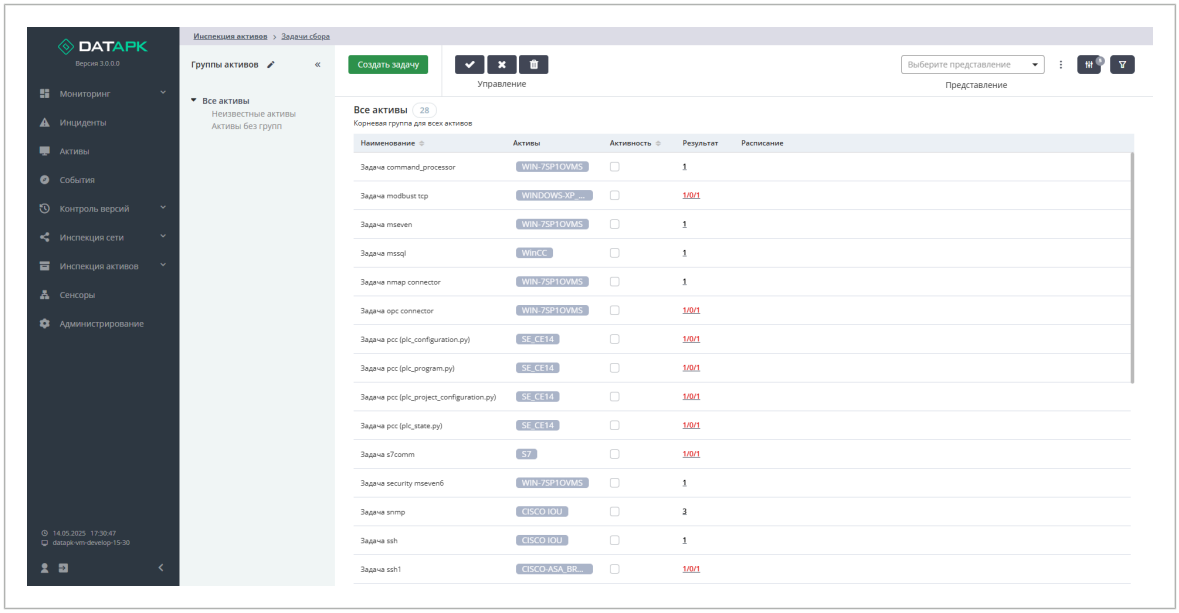


Рис. 232. Страница «Задачи сбора данных»

Значение, которое отображается в колонке, показывает, сколько было выполнено попыток сбора, и количество полученных результатов по типам. Подробнее см. в таблице ниже (Таблица 19. Обозначение цифр результатов задач).

Табл. 19. Обозначение цифр результатов задач

ПОРЯДКОВЫЙ НОМЕР ЦИФРЫ РЕЗУЛЬТАТА	НАЗВАНИЕ	ОБОЗНАЧЕНИЕ
1	Назначено	Общее количество процессов задачи сбора данных. Одним процессом задачи сбора данных считается пара сканер — актив
2	Ошибка соединения	Количество процессов, которые не удалось завершить из-за проблем с соединением
3	Ошибка сбора	Количество процессов, которые не удалось завершить из-за проблем со сканером или Комплексом

Пример

В качестве примера приведем результат сбора данных 4/1/2. Такой результат будет говорить о том, что в задаче есть 4 процесса, один из которых не удалось завершить вследствие потери соединения с активом, два — из-за проблем со сканером.

В таблице на странице **Активы** в столбце **Результаты сканирования** можно просматривать статистику по попыткам сбора данных с цветной индикацией для каждого актива. Подробнее см. раздел «Статусы активов».

При клике на результат происходит переход на страницу **Статус сбора**, где можно изучить подробности о статусах по каждому отдельному сканеру, который входит в задачу.

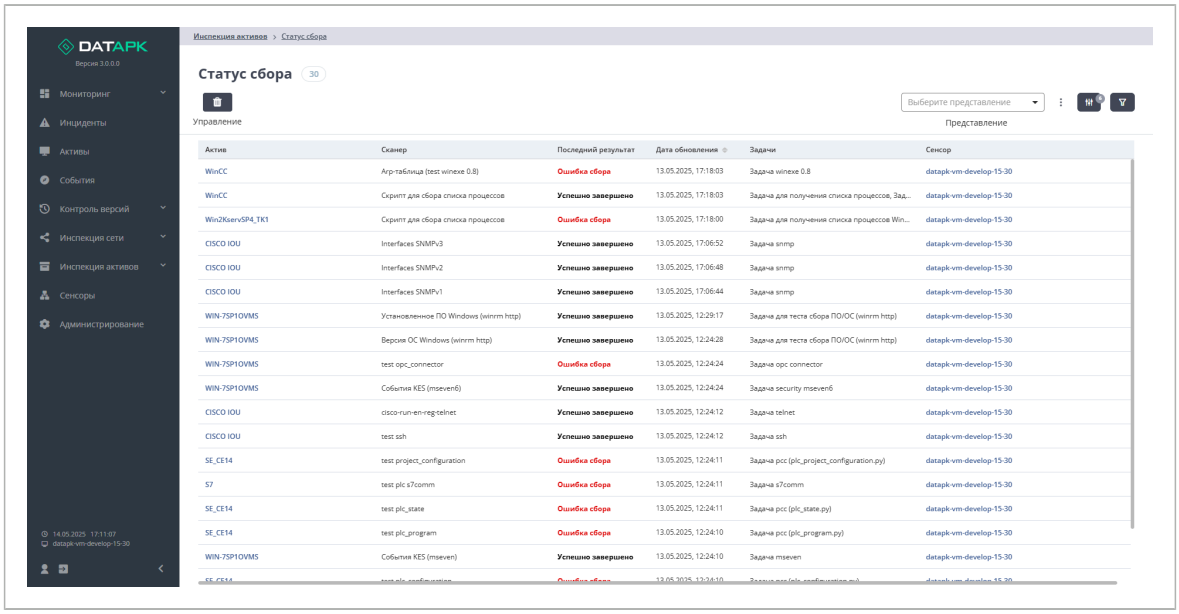


Рис. 233. Страница «Статус сбора»

На странице **Статус сбора** отображаются основные данные о попытке сбора: актив, сканер, последний результат, дата и время обновления, задачи, которым принадлежит сканер, сенсор, на котором выполняется сбор, время в очереди, длительность сбора.

По кнопке можно настроить отображение информации о сборе данных по следующим фильтрам:

- **Задача**
- **Сканер**
- **Актив**
- **Последний результат**
- **Сенсор**
- **Дата и время обновления**

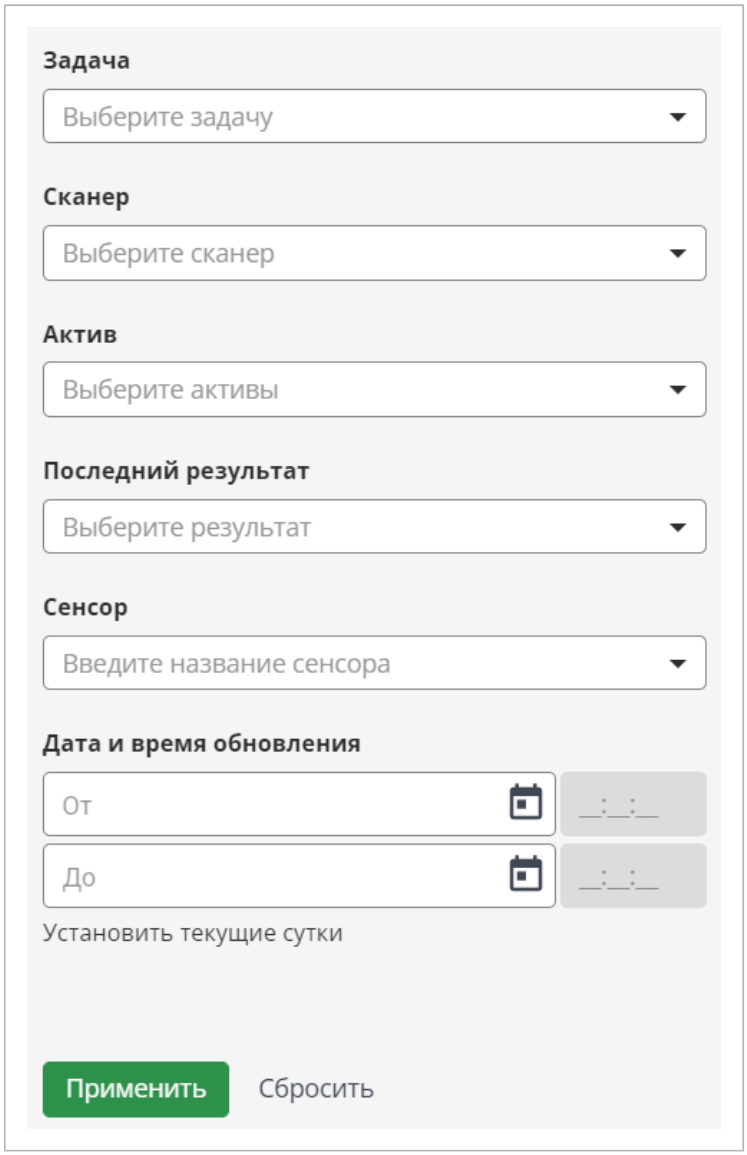


Рис. 234. Фильтры на странице «Статус сбора»

В колонке **Последний результат** отображаются статусы сбора по каждому запуску сканеров. Типы статусов совпадают с представленными в цифровом виде на странице **Задачи сбора**. Перечень статусов, их обозначение и причины получения см. в таблице ниже (Таблица 20. Результаты сбора данных).

Табл. 20. Результаты сбора данных

РЕЗУЛЬТАТ	ЦВЕТ	ОБОЗНАЧЕНИЕ	ОПИСАНИЕ	ВОЗМОЖНЫЕ ПРИЧИНЫ
Ошибка соединения	Оранжевый	Ошибка соединения	Не удалось подключиться к активу в течение периода, заданного в поле **Максимальное время ожидания** при создании сканера	• Скорость передачи данных в сети не позволяет получить результат за заданное в переменной время. • Актив недоступен: физически выключен, отсутствует доступ в сеть
Ошибка сбора	Оранжевый	Ошибка сбора	Не удалось завершить непосредственно сбор данных	• Не заданы корректные учетные данные. • Ошибки в сканерах. • Работоспособность Комплекса нарушена
Успешно завершено	Черный	Соответствует эталону	Соответствие собранной конфигурации эталонной	
		Успешный импорт событий	Обнаружены события	

При клике на результат, содержащий ошибки, открывается окно с описанием полученной ошибки.

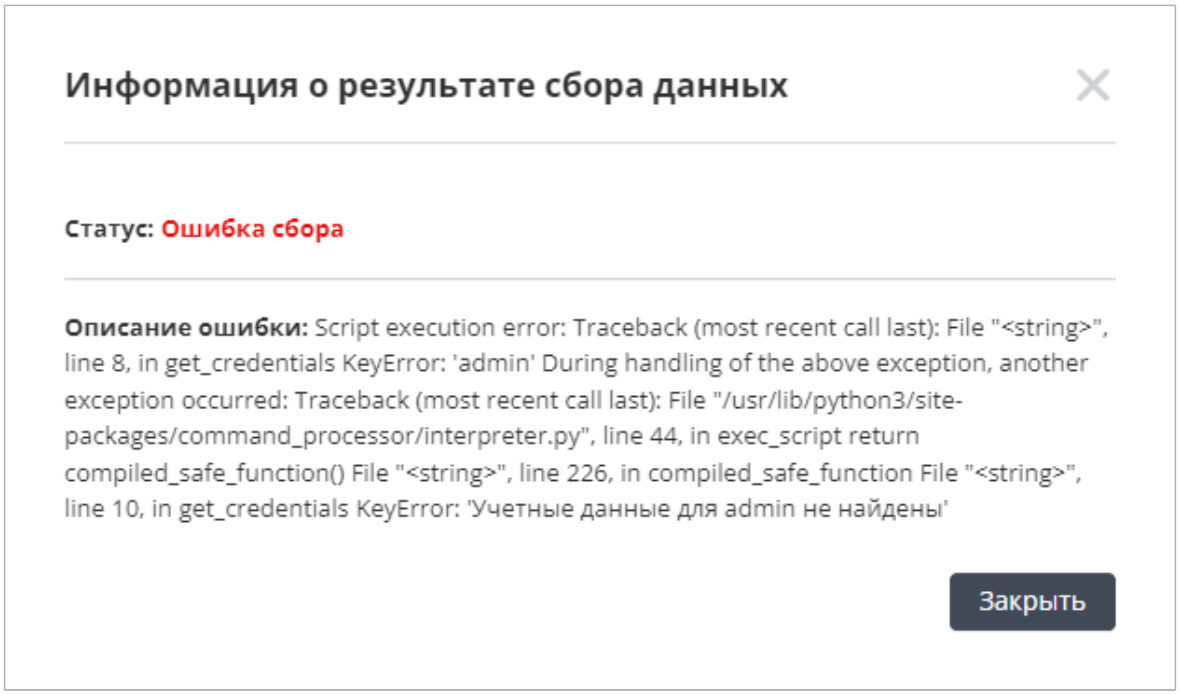


Рис. 235. Окно «Информация о результате сбора данных»

При необходимости неактуальные более результаты сбора данных можно удалить. Для группового удаления воспользуйтесь фильтрами и нажмите (**Удалить**) в верхней части страницы. Для удаления одного результата нажмите (**Удалить статус сбора**) в строке с удаляемым результатом.

13.2.5. Работа с архивом изменений конфигурации актива

В этом разделе:

- Просмотр сводки конфигураций
- Просмотр архива конфигураций
- Принятие конфигурации за эталонную
- Сравнение конфигурации с эталонной, принятие конфигурации за эталонную
- Удаление конфигураций

В результате выполнения сканеров, входящих в задачи сбора данных, формируются конфигурации. Просмотреть список таких сканеров можно при переходе из карточки актива на страницу **Активы → Конфигурации актива** (подробнее о задачах и результатах сбора данных см. в разделах «Сбор данных с активов» и «Просмотр статуса сбора данных»).

Конфигурации конкретных активов доступны к просмотру при переходе из карточки актива или со страницы **Инспекция активов → Конфигурации** (подробнее см. раздел «Просмотр архива конфигураций»).

Все последние собранные конфигурации доступны на странице **Инспекция активов → Конфигурации** (подробнее см. раздел «Просмотр сводки конфигураций»).

Список конфигураций пополняется в том случае, если вновь полученная конфигурация отличается от последней зафиксированной конфигурации.

13.2.5.1. Просмотр сводки конфигураций

Используя страницу **Конфигурации**, можно оперативно получить сводку о последних собранных сканерами данных с активов, а также найти интересующие. Последними считаются новейшие просканированные конфигурации (подробнее см. раздел «Сбор данных с активов»).

Чтобы просмотреть последние конфигурации, перейдите на страницу **Инспекция активов** → **Конфигурации**. На странице конфигурации отображаются в виде таблицы, содержащей следующие данные:

- статус конфигурации;
- дата обновления конфигурации;
- название актива, с которого собиралась конфигурация;

> Подсказка:
>
> При нажатии на название актива, для которого была создана конфигурация, можно открыть окно **Информация об активе**, в котором будет отображаться краткая информация о выбранном активе.

- наименование конфигурации.

После подбора списка конфигураций содержимое таблицы можно сохранить в отчет.

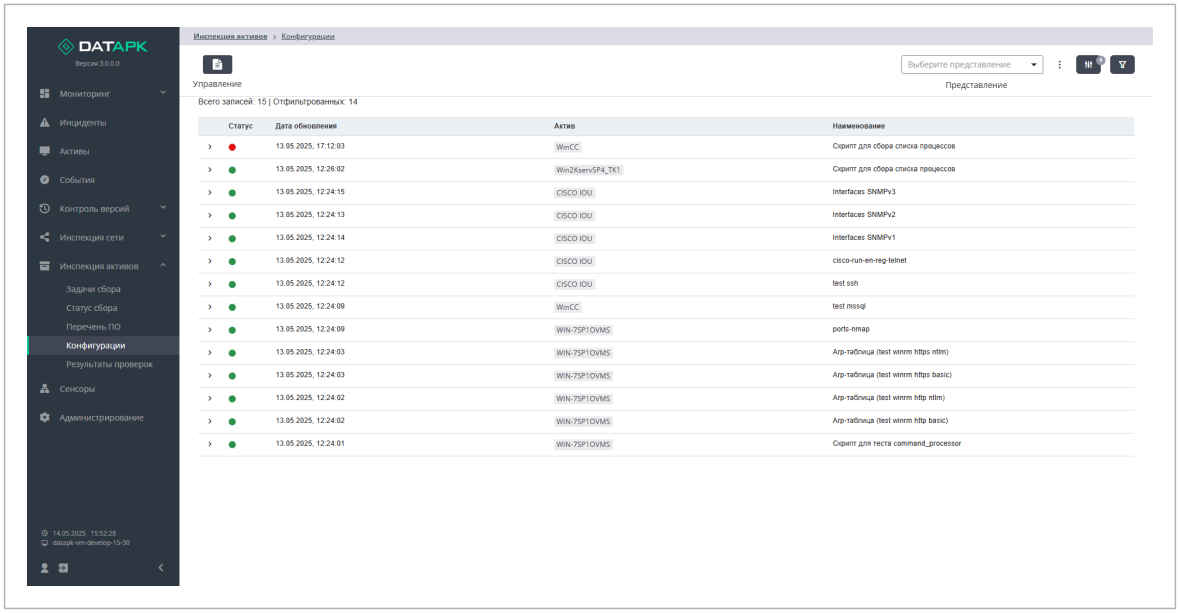


Рис. 236. Страница «Конфигурации»

Статусы конфигураций

Конфигурации могут иметь следующие статусы, которые отображаются при наведении на индикатор статуса:

- **Нет отклонений** — зеленый индикатор;
- **Были отклонения** — желтый индикатор;
- **Есть отклонения** — красный индикатор.

Отображение столбцов

При первом входе на страницу отображаются конфигурации за все время (без фильтров). Чтобы регулировать отображение столбцов, нажмите кнопку в правом верхнем углу. Содержание конфигураций по умолчанию

выводится в кратком (свернутом) виде. Для вывода подробностей воспользуйтесь соответствующим фильтром, либо нажмите слева от конфигурации.

Фильтры

Чтобы найти интересующие конфигурации, воспользуйтесь фильтрами. Доступны следующие фильтры:

- выпадающий список **Актив** — содержит список доступных для выбора активов;
- выпадающий список **Конфигурации** — содержит список доступных для выбора конфигураций;
- поле **Содержание конфигурации** — может быть заполнено любым текстом, который содержится в конфигурациях;
- поля **Дата и время обновления** — позволяет выбрать период с точностью до секунды, по которым необходимо отобразить конфигурации;
- чекбокс **Сравнить с эталонной** позволяет сравнить выбранные фильтром конфигурации с эталоном и вывести только те конфигурации, в которых были обнаружены отклонения от эталона;
- чекбокс **Только с отклонениями** позволяет вывести только те конфигурации, в которых были обнаружены отклонения от эталона, при этом сравнение с эталоном отображаться не будет.

Отчет

Чтобы сохранить отчет по выбранным конфигурациям, нажмите кнопку **Создать отчет** в верхней части страницы. Подробнее о выгрузке отчетов см. раздел «Выгрузка отчетов».

В отчете конфигурации отображаются подробно вне зависимости от того, был ли выбран подробный вывод конфигурации. В разделе отчета **Содержание конфигурации** содержится информация о том, является ли конфигурация эталонной.

Сравнение с эталоном

При выборе в фильтрах опции **Сравнить с эталонной** можно просматривать только конфигурации, у которых есть непроверенные изменения.

При просмотре в подробном виде доступны кнопки (**Показать еще по 5 окружающих строк**) и (**Скрыть по 5 окружающих строк**).

Просмотр конфигурации актива

Чтобы просмотреть архив конфигураций, полученных с актива, наведите курсор на строку с выбранным сканером и нажмите кнопку **Просмотреть конфигурацию актива**. Подробнее см. раздел «Просмотр архива конфигураций».

13.2.5.2. Просмотр архива конфигураций

Для просмотра архива конфигураций вы можете воспользоваться двумя представленными способами:

1. Просмотр архива конфигураций, полученных с определенного актива. Для просмотра:
    a. Перейдите на страницу **Активы** и нажмите на иконку или наименование актива.
    - **Результат шага:** Откроется карточка актива.

    б. В карточке актива нажмите на ссылку **Конфигурации** в разделе **Связанные данные**.
    - **Результат шага:** Откроется страница **Активы → Конфигурации актива**.

в. Выберите интересующую конфигурацию актива из списка в левой части страницы.

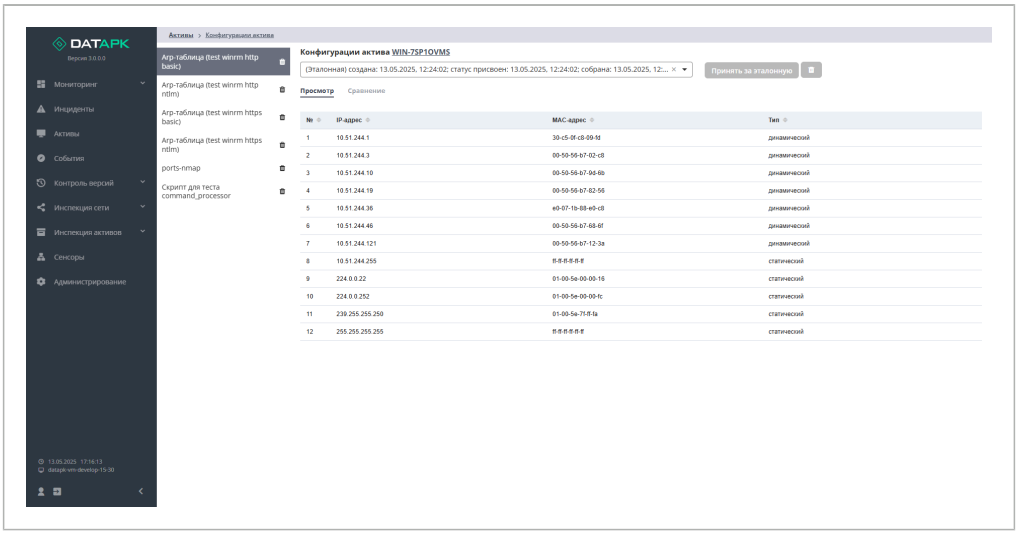


Рис. 237. Результат сбора данных с актива на странице «Конфигурации актива»

2. Просмотр конфигурации актива из списка всех конфигураций, собранных Комплексом. Для просмотра:

   а. Перейдите на страницу **Инспекция активов → Конфигурации**.

   б. Воспользуйтесь фильтрами в левой части страницы по кнопке для изменения выборки конфигураций.

   в. Наведите курсор на строку с выбранной конфигурацией и нажмите кнопку (**Просмотреть конфигурацию актива**).

   ▸ **Результат шага:** Откроется страница **Активы → Конфигурации актива** с выбранной конфигурацией актива.

13.2.5.3. Принятие конфигурации за эталонную

Для изменения эталонной конфигурации, полученной с помощью выбранного сканера:

1. Перейдите к конфигурациям актива со страницы **Активы** или из карточки актива. Для этого нажмите кнопку **Конфигурации** в строке с названием сканера на панели **Результаты сбора данных**.
2. В верхней части страницы напротив названия конфигурации нажмите кнопку **Принять за эталонную**.

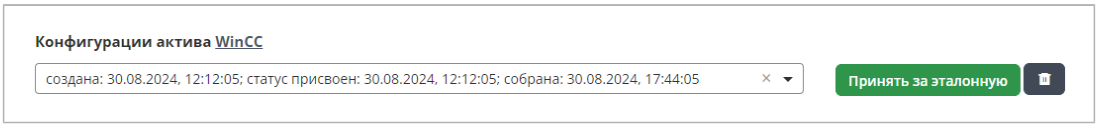


Рис. 238. Кнопка «Принять за эталонную» в списке конфигураций

3. Введите обоснование принятия конфигурации за эталонную и нажмите **Подтвердить**.

   ▸ **Результат шага:** после подтверждения под выпадающим списком конфигураций появится уведомление о принятии конфигурации за эталонную. Значок неэталонной конфигурации () перестанет отображаться возле названия сканера.

13.2.5.4. Сравнение конфигурации с эталонной, принятие конфигурации за эталонную

13.2.5.4.1. Сравнение конфигурации с эталонной

Для отслеживания изменений конфигурации актива, получаемой с помощью выбранного сканера:

1. Перейдите к конфигурациям актива из карточки актива. Для этого нажмите на ссылку **Конфигурации** в разделе **Связанные данные**.
2. Выберите из списка конфигурацию, которая не является эталонной.
3. Под строкой выбора конфигураций нажмите **Сравнение**.
4. Выберите одну из доступных опций:

НАЗВАНИЕ ОПЦИИ	ОПИСАНИЕ
Таблицей	Сравнение в виде таблицы: в верхней части отображаются изменения текущей конфигурации, в нижней части — сравниваемые строки эталонной конфигурации
Строка под строкой	Сравнение с подсветкой изменений по строкам и конкретным символам в них
Два экрана	Отображение всех строк сравниваемых файлов друг напротив друга с подсветкой добавленных и удаленных строк, а также символов в них

Подсказка:

Индикация изменений между версиями конфигурации:

- Элементы, отсутствующие в открытой на странице конфигурации, но присутствующие в эталонной, имеют красный цвет.
- Элементы, появившиеся в открытой конфигурации, но отсутствующие в эталонной, имеют зеленый цвет.

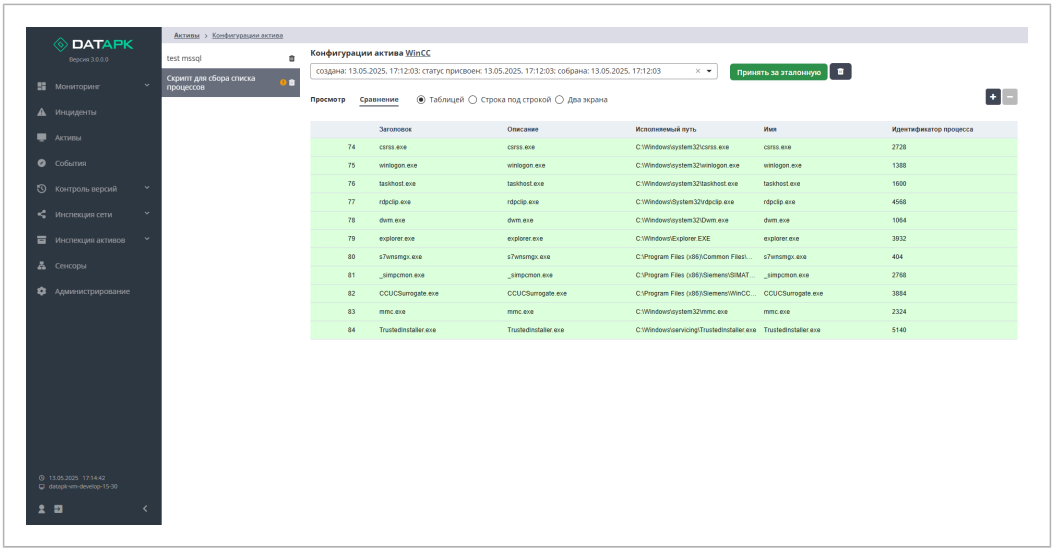


Рис. 239. Список изменений в конфигурации актива при сравнении с эталонной

5. Просмотрите список изменений в конфигурации.

> Прим.:
>
> При необходимости воспользуйтесь кнопками (**Показать еще по 5 окружающих строк**) и (**Скрыть по 5 окружающих строк**), а также возможностью отображения спецсимволов.

> ОСТОРОЖНО:
>
> Если вы увидите сообщение `Текущая конфигурация совпадает с эталонной. В период между получением эталонной конфигурации и текущей было обнаружено отклонение. Убедитесь в легитимности` изменений, убедитесь в том, что изменения не были произведены злоумышленником.

13.2.5.4.2. Принятие конфигурации за эталонную

Для изменения эталонной конфигурации, полученной с помощью выбранного сканера:

1. Перейдите к конфигурациям актива со страницы **Активы** или из карточки актива. Для этого нажмите кнопку **Конфигурации** в строке с названием сканера на панели **Результаты сбора данных**.
2. В верхней части страницы напротив названия конфигурации нажмите кнопку **Принять за эталонную**.

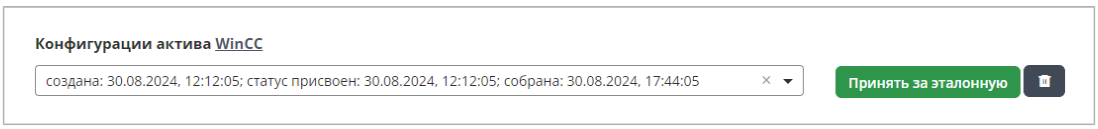


Рис. 240. Кнопка «Принять за эталонную» в списке конфигураций

3. Введите обоснование принятия конфигурации за эталонную и нажмите **Подтвердить**.
   - **Результат шага:** после подтверждения под выпадающим списком конфигураций появится уведомление о принятии конфигурации за эталонную. Значок неэталонной конфигурации ( ) перестанет отображаться возле названия сканера.

13.2.5.5. Удаление конфигураций

Для удаления конфигураций вы можете воспользоваться следующими возможностями:

1. Удаление одной конфигурации. Для удаления:

> Внимание:
>
> Удаление возможно только для тех конфигураций, которые не были приняты за эталонную.

   а. Перейдите к конфигурациям актива из карточки актива. Для этого нажмите на ссылку **Конфигурации** в разделе **Связанные данные**.

   б. В верхней части страницы напротив названия конфигурации нажмите кнопку (**Удалить**).

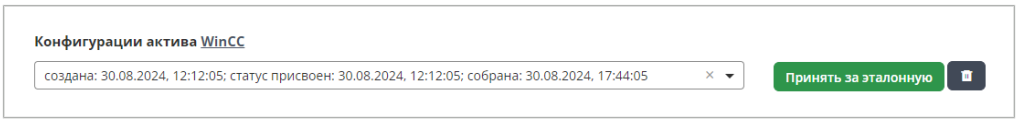


Рис. 241. Кнопка удаления неэталонной конфигурации

   ▸ **Результат шага:** появится окно ввода обоснования удаления конфигурации.

   в. Введите текст обоснования удаления неэталонной конфигурации.

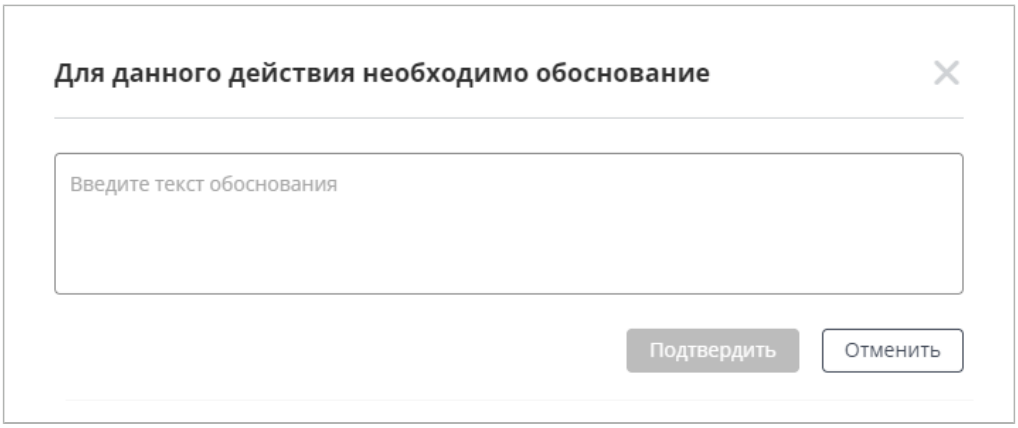


Рис. 242. Окно обоснования удаления неэталонной конфигурации

2. Удаление всех конфигураций, собранных сканером. Для удаления:

   а. Перейдите к конфигурациям актива из карточки актива. Для этого нажмите на ссылку **Конфигурации** в разделе **Связанные данные**.

   б. Нажмите (**Удалить конфигурации**) напротив названия сканера.

   ▸ **Результат шага:** появится окно ввода обоснования.

в. Введите обоснование удаления всех конфигураций, собранных сканером и нажмите **Подтвердить**.

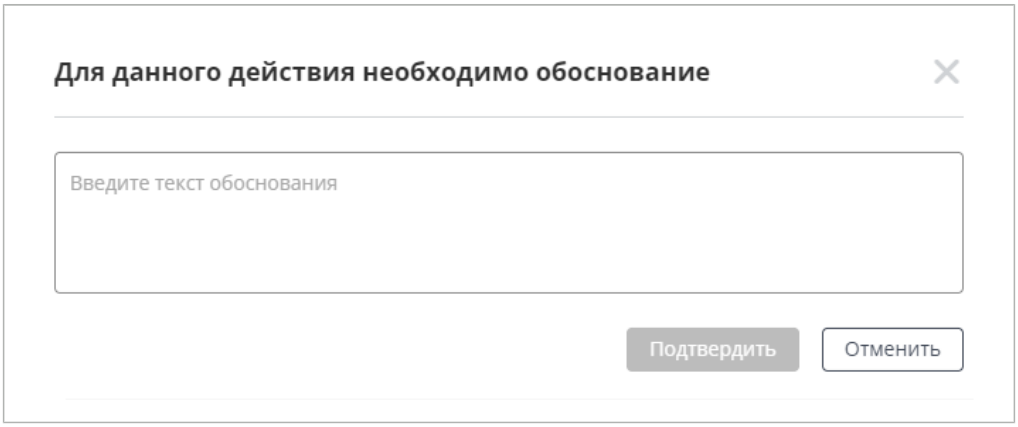


Рис. 243. Окно ввода обоснования удаления конфигураций актива

13.2.6. Добавление сетевых атрибутов активу с помощью сканера сбора данных по SNMP

Если на активе настроен доступ по протоколу SNMP, с него возможно получить конфигурацию подключенных сетевых интерфейсов. Полученную конфигурацию можно использовать, чтобы автоматически назначить активу новые сетевые атрибуты.

> Внимание:
>
> Чтобы Комплекс мог добавлять сетевые атрибуты из конфигурации, ее необходимо собрать сканерами SNMP, которые содержат Python-скрипты с ключами `ip_for_iface` и `mac_for_iface`.

Чтобы назначить активу сетевые атрибуты из конфигурации:

1. Убедитесь, что в операционной системе сенсора, который будет собирать данные с актива, присутствует директория `/usr/share/udv/snmp-connector/snmp_mibs` и она содержит необходимые MIB-словари.
2. Загрузите в Комплекс сканеры сбора конфигурации интерфейсов актива по протоколу SNMP и добавьте их в группу.

   > Подсказка:
   >
   > См. подробнее в разделах «Настройка сканеров сбора данных» и «Импорт сканеров и их групп».

3. Создайте и привяжите к активу учетные данные для сбора конфигурации по протоколу SNMP (в качестве тега укажите `community`, в качестве логина — значение параметра **community**).

   > Подсказка:
   >
   > См. подробнее в разделах «Добавление учетных данных актива» и «Импорт учетных данных активов».

4. Выполните однократный сбор данных с актива с помощью сканера SNMP или создайте задачу сбора данных для периодического сбора данных по расписанию.

> Подсказка:
>
> См. подробнее в разделах «Однократный сбор данных» и «Управление задачами сбора данных».

5. Дождитесь завершения сбора данных и откройте полученную конфигурацию в карточке актива. Подробнее см. в разделах «Карточка актива» и «Конфигурации актива».
6. На странице **Конфигурации актива** нажмите кнопку **Создать сетевые атрибуты**.

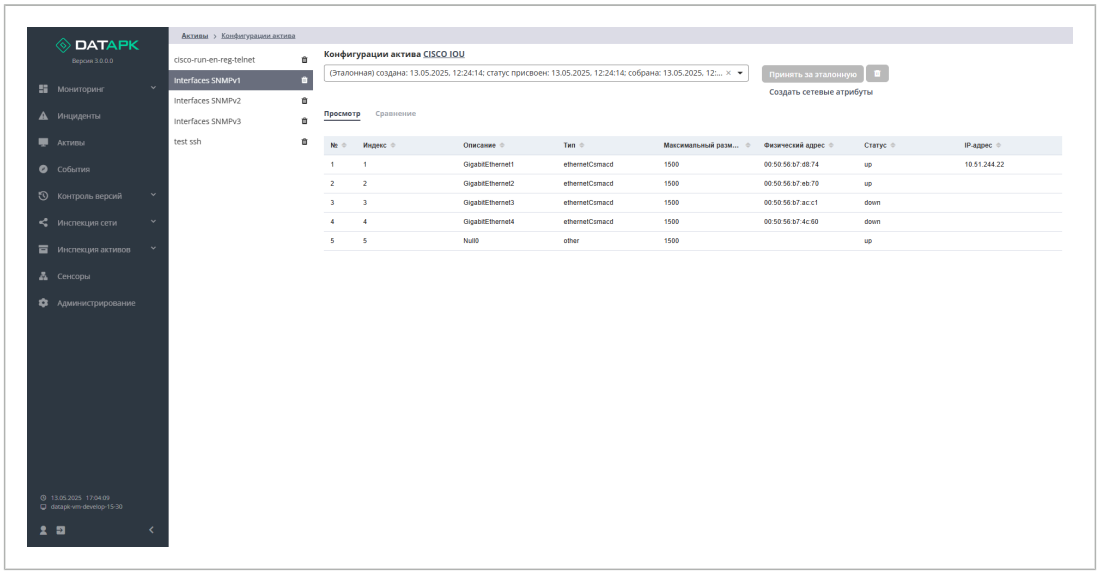


Рис. 244. Создание сетевых атрибутов со страницы конфигурации актива

- **Результат шага:**
  - В правом верхнем углу появится статус Сетевые атрибуты созданы.
  - Сетевые атрибуты, указанные в конфигурации, будут назначены текущему активу и удалены из других активов.

> **Внимание:**
>
> Если для активов удаленные сетевые атрибуты были единственными, такие активы будут удалены.

- Новым сетевым атрибутам актива будет назначен такой же сенсор, как у существующего интерфейса сбора данных. Присвоенный сенсор будет отображаться в поле **Сенсор** блока **Сетевые атрибуты** в **карточке актива**.

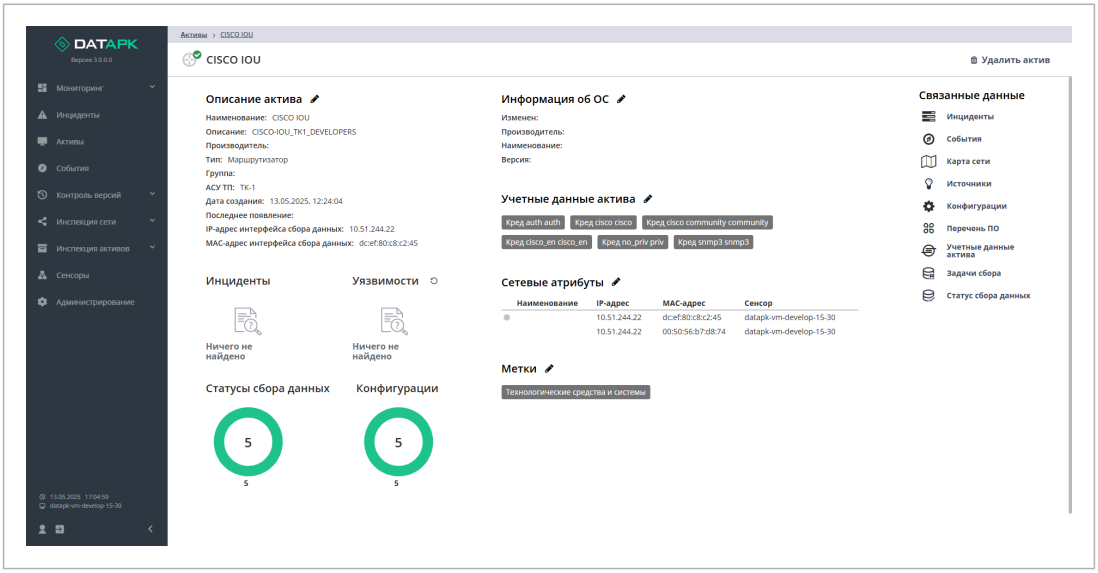


Рис. 245. Новые сетевые атрибуты в карточке актива

13.2.7. Цифровая подпись Python-скрипта

Для предотвращения запуска вредоносных исполняемых файлов в сети АСУ ТП все сканеры, создаваемые в Комплексе, должны иметь цифровую подпись импортируемых при их создании Python-файлов (скриптов). Возможность подписывать Python-файлы имеется у производителя Комплекса, а также у администратора безопасности или другого сотрудника при наличии закрытого ключа от сертификата. Подпись можно выполнять с помощью библиотеки OpenSSL. Комплекс верифицирует цифровую подпись Python-файла при создании сканера с помощью сертификата открытого ключа. Сертификат хранится в операционной системе Комплекса.

Для создания цифровой подписи Python-файла:

1. Запросите у поставщика закрытый ключ от сертификата `datapk-script.key`.
2. Подключитесь к операционной системе Комплекса по протоколу SFTP.
3. Скопируйте Python-файл в директорию `/usr/share/udv/scripts-certs`.

> **Подсказка:**
>
> Вы также можете скопировать Python-файл в директорию `scripts-certs` с помощью USB-носителя.

4. Подключитесь к операционной системе Комплекса или сенсора, который будет собирать данные.
5. Перейдите в директорию `/usr/share/udv/scripts-certs`. Для этого выполните команду:

```
cd /usr/share/udv/scripts-certs
```

6. Создайте цифровую подпись Python-файла с использованием закрытого ключа `datapk_script.key` (или ключа с другим названием, расположенного в директории `scripts-certs`). Для этого выполните команду:

```
openssl dgst -sha256 -sign datapk_script.key "[Наименование_Python-файла].py" | openssl
 enc -base64 -in /dev/stdin
```

7. Скопируйте полученную цифровую подпись в буфер обмена или в текстовый файл.

Что дальше: Используйте Python-файл и его цифровую подпись при создании или редактировании сканера сбора данных — подробнее см. раздел «Настройка сканеров сбора данных».

13.3. Настройка активного сбора событий

События — записи, которые Комплекс собирает из журналов актива. Например, из журналов Windows.

Просмотр событий, полученных в результате выполнения сканеров, доступен на странице **События** и на панели мониторинга «События активов». Подробнее см. в разделе «Просмотр событий и создание запросов в экспертном режиме».

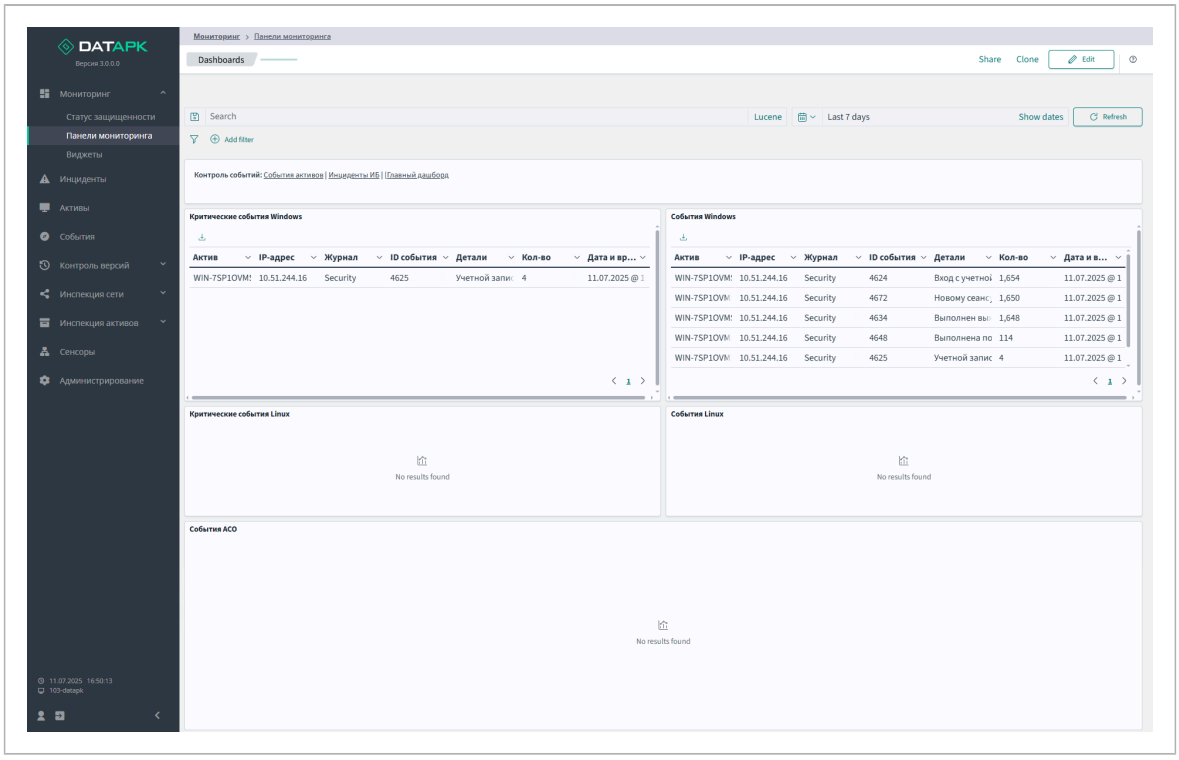


Рис. 246. Панель мониторинга «События активов»

Для настройки активного сбора событий с актива:

1. Импортируйте или создайте сканеры для сбора событий.

> Подсказка:
>
> См. подробнее в разделах «Импорт сканеров и их групп», «Создание сканера сбора данных», «Управление сканерами сбора данных».

2. Добавьте сканеры в группы.

> Подсказка:
>
> См. подробнее в разделе «Группировка сканеров сбора данных».

3. Убедитесь, что объектам защиты назначены учетные данные.

> Подсказка:
>
> См. подробнее в разделе «Настройка активов для сбора данных».

4. Выполните сбор данных одним из доступных способов:
   - однократный сбор сканером сбора данных;

     > Подсказка:
     >
     > См. подробнее в разделе «Однократный сбор данных».

   - сбор данных задачей сбора данных.

     > Подсказка:
     >
     > См. подробнее в разделах «Создание задачи сбора данных», «Управление задачами сбора данных».

5. Убедитесь, что сбор данных произведен успешно.

> Подсказка:
>
> См. подробнее в разделе «Просмотр статуса сбора данных».

6. Ознакомьтесь с результатами сбора. Сделать это можно на панели мониторинга События активов и на странице **События**.

13.4. Настройка сбора данных об операционной системе и установленном ПО

В веб-интерфейсе Комплекса доступен сбор данных о производителе актива и об установленных на активе операционной системе и программном обеспечении.

Сбор данных о производителе, операционной системе

Для сбора общей информации о производителе и операционной системе предусмотрены следующие возможности:

1. Автоматическое определение данных о производителе на основе первых трех октетов MAC-адреса. Собранная информация отображается в поле **Производитель** блока **Описание актива** карточки актива.

> Подсказка:
>
> Для ознакомления с возможностью определения производителя на основе трафика см. пункт 4.b раздела «Редактирование актива».

2. Определение производителя, названия операционной системы и ее версии по результатам работы сканеров. Собранная информация отображается в блоке **Информация об ОС** карточки актива.
3. Указание информации о производителе и операционной системе актива вручную.

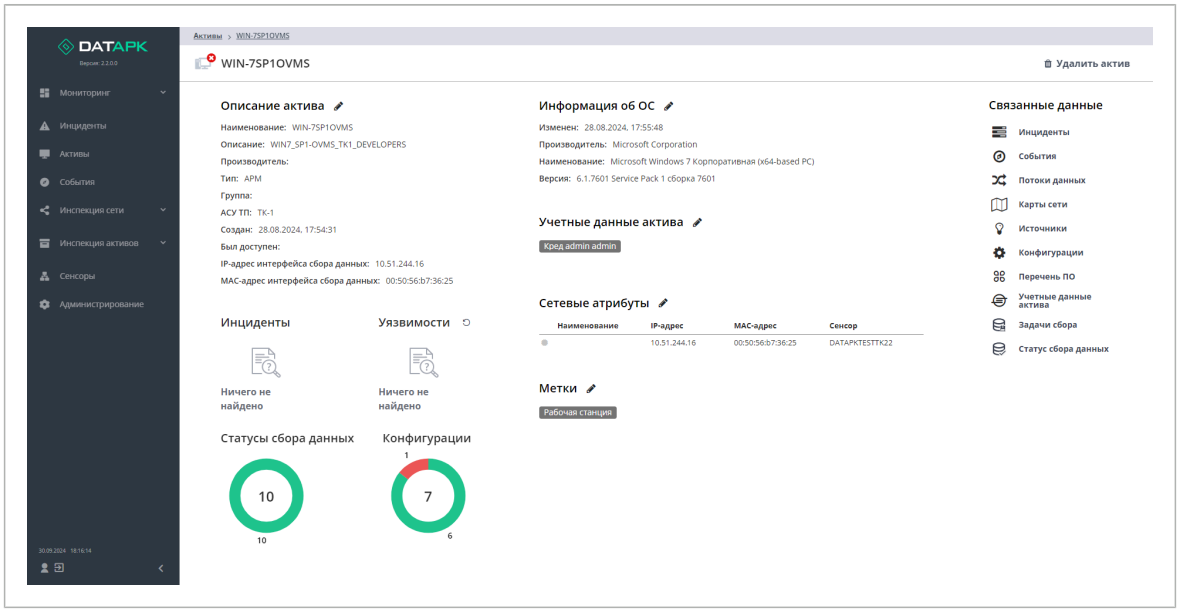


Рис. 247. Карточка актива

Тип информации, сохраняемой в блоке **Информация об ОС**, зависит от настроенного типа актива: для активов с типом `ПЛК` собирается и сохраняется информация о прошивке, для остальных активов — информация об операционной системе.

Тип актива и информация в блоке **Информация об ОС** влияют на список уязвимостей, которые возможно обнаружить на активе с помощью справочников CVE и CPE:

- для активов с типом `ПЛК` поиск уязвимостей выполняется только для прошивки. Поиск уязвимостей ПО и ОС не выполняется;
- для остальных активов поиск уязвимостей выполняется для ОС и ПО, но не выполняется для прошивки.

При изменении типа актива на `ПЛК` или обратно необходимо обновить информацию в блоке **Информация об ОС**.

При повторном сборе информации об ОС предыдущие данные удаляются и заменяются новыми. Автообновление данных об ОС можно отключить в карточке актива — см. пункт 6 раздела «Редактирование актива».

Сбор данных о программном обеспечении

Для сбора информации об установленном на активах программном обеспечении могут быть использованы сканеры сбора данных. После сбора перечень ПО отображается на странице **Перечень ПО**. Получить перечень ПО для определенного актива можно с помощью фильтра по наименованию актива, либо перейти к списку из карточки актива по ссылке **Перечень ПО**.

При повторном сборе информации о ПО предыдущие данные удаляются и заменяются новыми.

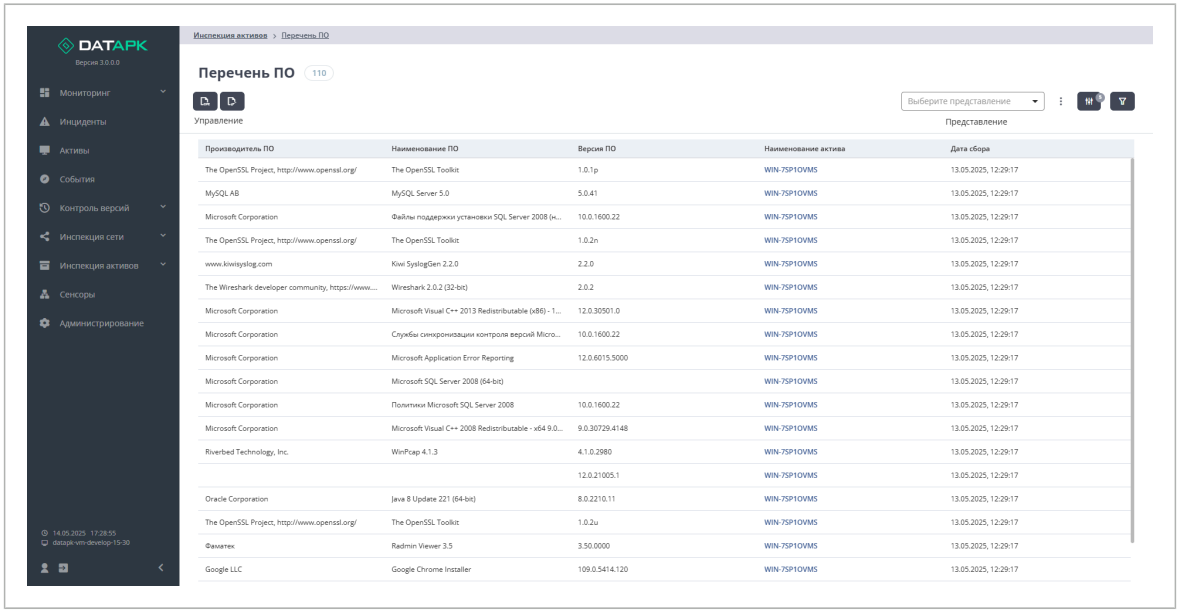


Рис. 248. Страница «Перечень ПО»

13.4.1. Запуск сбора данных об операционной системе и установленном ПО

Для настройки возможности сбора подробной информации об операционной системе и установленном ПО актива:

1. Импортируйте или создайте сканеры для сбора данных об ОС и ПО с типами `Версия ОС` и `Установленное ПО`.

   > Подсказка:
   >
   > См. подробнее в разделах «Импорт сканеров и их групп», «Создание сканера сбора данных», «Управление сканерами сбора данных».

   > Внимание:
   >
   > При повторном сборе информации об ОС или ПО предыдущие данные удаляются и заменяются новыми. Автообновление данных об ОС можно отключить в карточке актива — см. пункт 6 раздела «Редактирование актива».

2. Добавьте сканеры в группы.

   > Подсказка:
   >
   > См. подробнее в разделе «Группировка сканеров сбора данных».

3. Убедитесь, что объектам защиты назначены учетные данные.

> Подсказка:
>
> См. подробнее в разделе «Настройка активов для сбора данных».

4. Выполните сбор данных одним из доступных способов:
   - однократный сбор сканером сбора данных;

     > Подсказка:
     >
     > См. подробнее в разделе «Однократный сбор данных».

   - сбор данных задачей сбора данных.

     > Подсказка:
     >
     > См. подробнее в разделах «Создание задачи сбора данных», «Управление задачами сбора данных».

5. Убедитесь, что сбор данных произведен успешно.

   > Подсказка:
   >
   > См. подробнее в разделе «Просмотр статуса сбора данных».

6. Ознакомьтесь с результатами сбора.

   Результат шага:

   - Результаты сбора данных об ОС отобразятся в карточке актива в блоке **Информация об ОС**.
   - Результаты сбора данных об установленном ПО отобразятся на странице **Перечень ПО**.

14. Поиск уязвимостей и проверка соответствия требованиям информационной безопасности

В этом разделе:

1. Поиск уязвимостей ПО и ОС в базах CVE, CPE и БДУ ФСТЭК России
   Проверки на уязвимости и соответствие требованиям информационной безопасности с помощью
2. OVAL

С целью контроля и оценки состояния защищенности активов в Комплексе реализованы следующие функции:

1. Анализ уязвимостей активов. Реализуется двумя способами:
   - Проверка на уязвимости выбранной группы ПО с помощью загруженных в Комплекс справочников OVAL (OVAL). Предварительный сбор данных о ПО, установленном на активе, не требуется.
   - Предварительный сбор данных о ПО и ОС, установленных на активе, и проверка полученного списка на уязвимости с помощью загруженных в Комплекс справочников CVE (CVE), CPE (CPE) и БДУ ФСТЭК России (БДУ ФСТЭК России).
2. Контроль соответствия отдельных настроек и конфигураций активов требованиям информационной безопасности. Реализуется только с помощью OVAL.

Табл. 21. Сравнение функций поиска уязвимостей в Комплексе

СРАВНИВАЕМАЯ ХАРАКТЕРИСТИКА	CVE И CPE	OVAL
Возможности	Поиск уязвимостей	• Поиск уязвимостей • Контроль соответствия конфигураций активов требованиям информационной безопасности
Раздел документации	Поиск уязвимостей ПО и ОС в базах CVE, CPE и БДУ ФСТЭК России	Проверки на уязвимости и соответствие требованиям информационной безопасности с помощью OVAL
Страница запуска	• **Активы** • **Карточка актива**	**Результаты проверок**
Результат	• Отчет с результатами поиска уязвимостей формата `*.csv` в окне **Запуск поиска уязвимостей** • Диаграмма и список уязвимостей в **карточке актива**	На странице **Результаты проверки** напротив успешно выполненной проверки:

Табл. 21. Сравнение функций поиска уязвимостей в Комплексе

СРАВНИВАЕМАЯ ХАРАКТЕРИСТИКА	CVE И CPE	OVAL
	• Статистика по обнаруженным уязвимостям на странице **Активы** • Отчет сопоставления ОС и ПО со справочником CPE формата `*.csv` на странице **Перечень ПО** по кнопке	• таблица результатов проверок по кнопке (**Просмотреть результаты**) • отчет формата `html` или `xlsx` по кнопке (**Создать отчет**)
Ограничения по запуску	Нет ограничений — каждый актив опрашивается один раз для получения списка ОС или ПО, а поиск уязвимостей выполняется в Комплексе в фоновом режиме	Рекомендуется запускать в технологические окна — для выполнения проверки каждый актив опрашивается несколько раз, что может кратковременно влиять на его доступность и быстродействие

14.1. Поиск уязвимостей ПО и ОС в базах CVE, CPE и БДУ ФСТЭК России

Пользователь с ролью `Администратор` или `Инженер` может выполнить поиск уязвимостей активов с помощью справочников CVE и CPE в следующем порядке:

1. Убедиться в актуальности импортированных справочников CVE, CPE и БДУ ФСТЭК России — подробнее см. раздел «Проверка актуальности справочников поиска уязвимостей».
2. Импортировать справочники CVE, CPE — подробнее см. раздел «Импорт справочников CVE и CPE и файла сопоставления ПО с CPE».
3. При необходимости импортировать справочник БДУ ФСТЭК России — подробнее см. раздел «Импорт справочника БДУ ФСТЭК России».

   Подсказка:

   Импорт справочника БДУ ФСТЭК России позволяет добавить в отчеты о проверках дополнительную информацию об уязвимостях, но не обязателен для успешного выполнения проверок.

4. Получить с актива информацию об установленных на нем ОС и ПО с помощью сканеров с типами `Версия ОС` и `Установленное ПО` — подробнее см. раздел «Запуск сбора данных об операционной системе и установленном ПО».

   Внимание:

   Полученная информация об ОС сохраняется в блоке **Информация об ОС** **карточки актива** (подробнее см. раздел «Редактирование актива»).

   Тип информации, сохраняемой в блоке **Информация об ОС**, зависит от настроенного типа актива: для активов с типом `ПЛК` собирается и сохраняется информация о прошивке, для остальных активов — информация об операционной системе.

Тип актива и информация в блоке **Информация об ОС** влияют на список уязвимостей, которые возможно обнаружить на активе с помощью справочников CVE и CPE:

- для активов с типом `ПЛК` поиск уязвимостей выполняется только для прошивки. Поиск уязвимостей ПО и ОС не выполняется;
- для остальных активов поиск уязвимостей выполняется для ОС и ПО, но не выполняется для прошивки.

При изменении типа актива на `ПЛК` или обратно необходимо обновить информацию в блоке **Информация об ОС**.

5. Запустить поиск уязвимостей. Поиск уязвимостей можно запустить для одного или нескольких активов разными способами — подробнее см. раздел «Запуск поиска уязвимостей в базах CVE, CPE и БДУ ФСТЭК России». На данном этапе Комплекс:
   a. Сопоставляет наименования и версии ОС и ПО, полученные с актива, со справочником CPE.
   b. Сравнивает результаты сопоставления со справочниками CVE и БДУ ФСТЭК России.

Результаты поиска уязвимостей с помощью CVE, CPE и БДУ ФСТЭК России можно просмотреть в Комплексе несколькими способами:

- Скачать отчет формата `*.csv`, который будет содержать список уязвимостей активов, для которых выполнялся последний поиск. Подробнее см. раздел «Запуск поиска уязвимостей в базах CVE, CPE и БДУ ФСТЭК России».
- Просмотреть диаграмму и список уязвимостей **в карточке актива**, для которого когда-либо выполнялся поиск.
- Просмотреть статистику по обнаруженным уязвимостям для каждого актива. Статистика отображается на странице **Активы** в столбце **Уязвимости**. Подробнее см. раздел «Статусы активов».
- Скачать отчет формата `*.csv`, который будет содержать результаты сопоставления ОС и ПО со справочником CPE. Подробнее см. раздел «Выгрузка отчета по результатам сопоставления собранного ПО со справочником CPE».

ОСТОРОЖНО:

Точность, с которой для ПО подобран элемент CPE, указывается в отчете в виде относительного коэффициента **map_confidence** в диапазоне от 0 до 1.

Минимальное значение относительного коэффициента **map_confidence** для подбора элемента CPE = `60%` или `0,6`. При меньшем значении подбор CPE для ПО выполняться не будет.

Пороговые значения для сопоставления наименования, версии и поставщика ПО с элементами CPE задаются в переменных `CPE_PRODUCT_THRESHOLD`, `CPE_VENDOR_THRESHOLD` и `CPE_VERSION_THRESHOLD`.

См. также

Переменные Комплекса уровня Management

14.1.1. Проверка актуальности справочников поиска уязвимостей

Перед импортом справочников ПО и уязвимостей (CPE, CVE и БДУ ФСТЭК России) и файла сопоставления собранного ПО со справочником CPE проверьте актуальность загруженных справочников по дате их последнего обновления. Для этого:

1. Перейдите на страницу **Активы**.
2. При помощи чекбокса выберите любой актив.
3. Нажмите кнопку (**Запустить поиск уязвимостей**).
   - **Результат шага:** появится окно запуска поиска уязвимостей с датами последнего обновления баз.

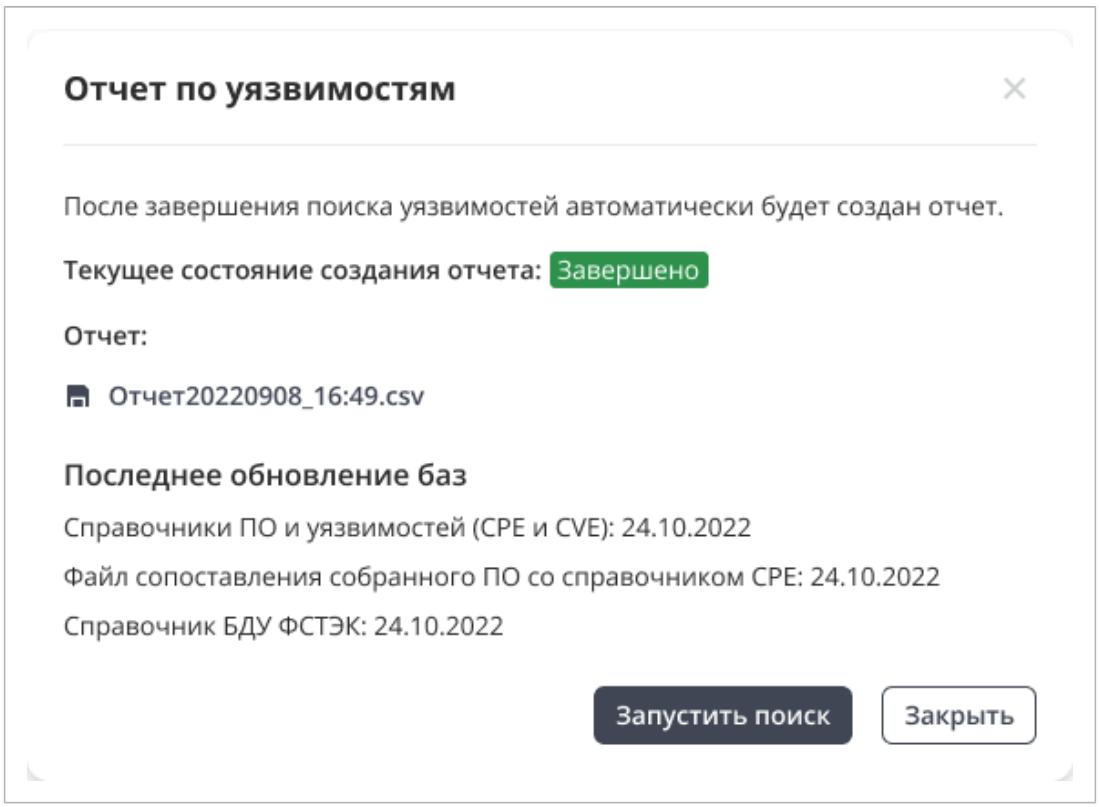


Рис. 249. Окно запуска поиска уязвимостей

Внимание:

Если справочник не был загружен ранее, вместо даты будет символ -.

14.1.2. Импорт справочников CVE и CPE и файла сопоставления ПО с CPE

> Внимание:
>
> Невозможно экспортировать справочники ПО и уязвимостей (CVE и CPE) и файл сопоставления собранного сканерами ПО со справочником CPE.

14.1.2.1. Импорт справочников ПО и уязвимостей (CPE и CVE)

Для импорта справочников CPE и CVE:

1. Перейдите на страницу **Администрирование → Основные настройки → Импорт и экспорт**.
2. На панели **Обнаружение уязвимостей (CVE)** в строке **Справочники ПО и уязвимостей (CPE и CVE)** нажмите кнопку (**Импортировать**).
3. В открывшемся окне укажите расположение импортируемого файла `cve_cpe_db_[дата].tar.bz` и подтвердите выбор.
   - **Результат шага:** будет запущен процесс импорта: в правом верхнем углу появится уведомление `Запущен импорт справочника`, а под заголовком **Результат последнего импорта** будет символ `-`.

   > Подсказка:
   >
   > Операции импорта являются фоновыми — со страницы можно безопасно уходить.

4. Дождитесь загрузки справочника и убедитесь, что файл был успешно загружен.
   - Если файл импортирован успешно, в правом вернем углу под заголовком **Результат последнего импорта** появится уведомление: `Успешно`.
   - Если произошла ошибка, в правом верхнем углу под заголовком **Результат последнего импорта** появится уведомление `Ошибка`. Для просмотра информации об ошибке нажмите ссылку **Подробнее** в подсказке рядом с уведомлением.

14.1.2.2. Импорт файла сопоставления собранного сканерами ПО со справочником CPE

Для импорта файла сопоставления собранного сканерами ПО со справочником CPE:

1. Перейдите на страницу **Администрирование → Основные настройки → Импорт и экспорт**.
2. На панели **Обнаружение уязвимостей (CVE)** в строке **Сопоставление собранного сканерами ПО со справочником CPE** нажмите кнопку (**Импортировать**).
3. В открывшемся окне укажите расположение импортируемого файла `mappings_[дата].tar.bz2` и подтвердите выбор.
   - **Результат шага:** будет запущен процесс импорта: в правом верхнем углу появится уведомление `Запущен импорт справочника`, а под заголовком **Результат последнего импорта** будет символ `-`.

   > Подсказка:
   >
   > Операции импорта являются фоновыми — со страницы можно безопасно уходить.

4. Убедитесь, что файл был успешно загружен.

- Если файл импортирован успешно, в правом вернем углу под заголовком **Результат последнего импорта** появится уведомление: `Успешно`.
- Если произошла ошибка, в правом верхнем углу под заголовком **Результат последнего импорта** появится уведомление `Ошибка`. Для просмотра информации об ошибке нажмите ссылку **Подробнее** в подсказке рядом с уведомлением.

14.1.3. Импорт справочника БДУ ФСТЭК России

> Подсказка:
>
> Актуальный справочник БДУ ФСТЭК России в формате *.xlsx можно скачать с сайта БДУ ФСТЭК России (см. ссылку **Скачать сведения об угрозах** внизу страницы).

> Внимание:
>
> Экспортировать справочник БДУ ФСТЭК России из Комплекса невозможно.

Для импорта справочника БДУ ФСТЭК России:

1. Перейдите на страницу **Администрирование → Основные настройки → Импорт и экспорт**.
2. На панели **Обнаружение уязвимостей (CVE)** в строке **Справочник БДУ ФСТЭК** нажмите кнопку (**Импортировать**).
3. В открывшемся окне укажите расположение импортируемого файла формата `*.xlsx` и подтвердите выбор.

   ▸ **Результат шага:** будет запущен процесс импорта: в правом верхнем углу появится уведомление `Запущен импорт справочника`, а под заголовком **Результат последнего импорта** будет символ `-`.

   > Подсказка:
   >
   > Операции импорта являются фоновыми — со страницы можно безопасно уходить.

4. Дождитесь загрузки справочника и убедитесь, что файл был успешно загружен.
   - Если файл импортирован успешно, в правом вернем углу под заголовком **Результат последнего импорта** появится уведомление: `Успешно`.
   - Если произошла ошибка, в правом верхнем углу под заголовком **Результат последнего импорта** появится уведомление `Ошибка`. Для просмотра информации об ошибке нажмите ссылку **Подробнее** в подсказке рядом с уведомлением.

14.1.4. Запуск поиска уязвимостей в базах CVE, CPE и БДУ ФСТЭК России

См. также

Выгрузка отчетов

Ошибки поиска уязвимостей в базах CVE, CPE и БДУ ФСТЭК России

14.1.4.1. Запуск поиска уязвимостей актива

Поиск уязвимостей для одного актива можно выполнить двумя равнозначными способами:

- со страницы **Активы**;
- из карточки актива.

1. Для поиска уязвимостей актива со страницы **Активы**:
   a. Перейдите на страницу **Активы**.
   б. При помощи чекбокса выберите актив.
   в. Нажмите кнопку (**Запустить поиск уязвимостей**).
   ▸ **Результат шага:** появится окно **Запуск поиска уязвимостей**.
   г. Нажмите **Запустить поиск**.

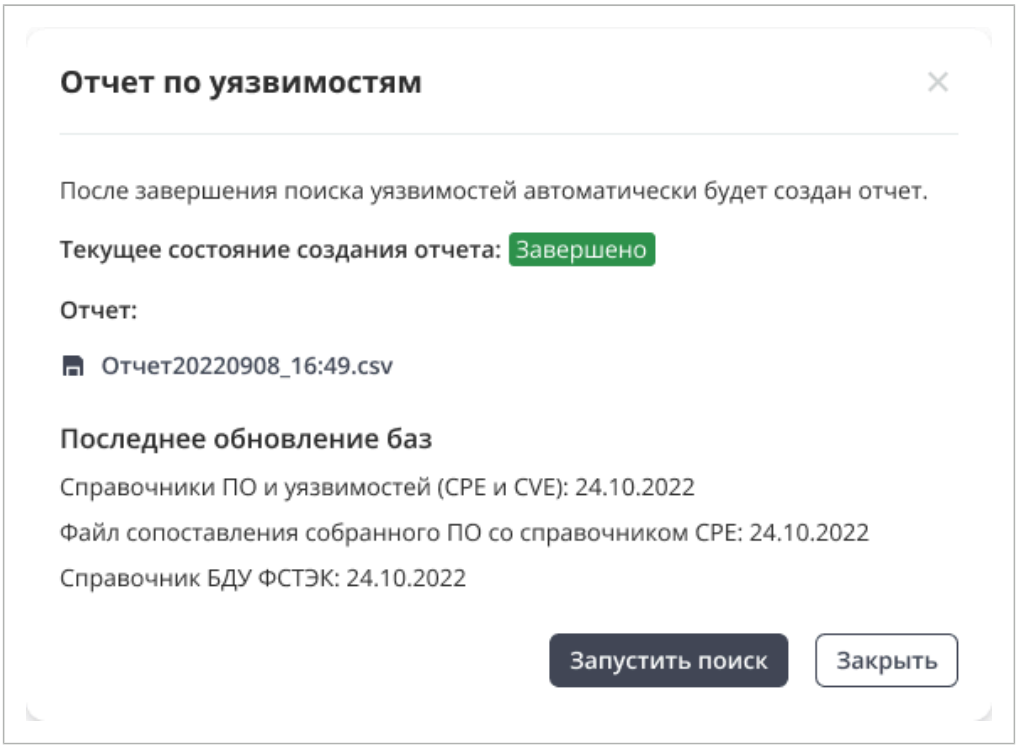


Рис. 250. Окно «Запуск поиска уязвимостей»

Подсказка:

Поиск уязвимостей и создание отчета может занять продолжительное время. Вы можете безопасно закрыть окно — поиск продолжится в фоновом режиме. Для просмотра статуса поиска уязвимостей заново откройте окно **Запуск поиска уязвимостей** — для этого на странице **Активы** выберите любой актив и нажмите кнопку .

Вы также можете отменить поиск уязвимостей, нажав кнопку **Остановить поиск** в окне **Запуск поиска уязвимостей**

д. Дождитесь завершения поиска.

- **Результат шага:** в окне **Запуск поиска уязвимостей** отобразится текущее состояние создания отчета: Завершено. В случае возникновения ошибки см. раздел «Ошибки поиска уязвимостей в базах CVE, CPE и БДУ ФСТЭК России».

2. Для поиска уязвимостей актива из карточки актива:

а. Перейдите в карточку актива.

б. Нажмите кнопку (**Запустить поиск уязвимостей**) рядом с заголовком **Уязвимости**.

- **Результат шага:** появится окно **Запуск поиска уязвимостей**.

в. Нажмите **Запустить поиск**.

> Подсказка:
>
> Поиск уязвимостей и создание отчета может занять продолжительное время. Вы можете безопасно закрыть окно — поиск продолжится в фоновом режиме. Для просмотра статуса поиска уязвимостей заново откройте окно **Запуск поиска уязвимостей** — для этого повторно нажмите кнопку в карточке актива, либо на странице **Активы** выберите любой актив и нажмите кнопку CVE.
>
> Вы также можете отменить поиск уязвимостей, нажав кнопку **Остановить поиск** в окне **Запуск поиска уязвимостей**

г. Дождитесь завершения поиска.

- **Результат шага:** в окне **Запуск поиска уязвимостей** отобразится текущее состояние создания отчета: Завершено. В случае возникновения ошибки см. раздел «Ошибки поиска уязвимостей в базах CVE, CPE и БДУ ФСТЭК России».

14.1.4.2. Запуск группового поиска уязвимостей активов

Для поиска уязвимостей нескольких активов:

1. Перейдите на страницу **Активы**.
2. При помощи чекбоксов выберите активы.
3. Нажмите кнопку CVE (**Запустить поиск уязвимостей**).
   - **Результат шага:** появится окно **Запуск поиска уязвимостей**.
4. Нажмите **Запустить поиск**.

> Подсказка:
>
> Поиск уязвимостей и создание отчета может занять продолжительное время. Вы можете безопасно закрыть окно — поиск продолжится в фоновом режиме. Для просмотра статуса поиска уязвимостей заново откройте окно **Запуск поиска уязвимостей** — для этого на странице **Активы** выберите любой актив и нажмите кнопку CVE.

Вы также можете отменить поиск уязвимостей, нажав кнопку **Остановить поиск** в окне **Запуск поиска уязвимостей**

5. Дождитесь завершения поиска.

   ▸ **Результат шага:** в окне **Запуск поиска уязвимостей** отобразится текущее состояние создания отчета: `Завершено`. В случае возникновения ошибки см. раздел «Ошибки поиска уязвимостей в базах CVE, CPE и БДУ ФСТЭК России».

14.1.4.3. Просмотр обнаруженных уязвимостей и рекомендаций по их устранению

Пользователь может просматривать уязвимости и рекомендации по их устранению следующими способами:

- в карточке актива;
- в отчете в формате `*.csv`.

1. Для просмотра уязвимостей и рекомендаций в карточке актива:

   а. Перейдите в карточку актива и нажмите на круговую диаграмму **Уязвимости**, либо перейдите на страницу **Активы** и в строке с активом в столбце **Уязвимости** нажмите на его статус.

   ▸ **Результат шага:** откроется окно **Просмотр уязвимостей** со списком уязвимостей, обнаруженных на активе.

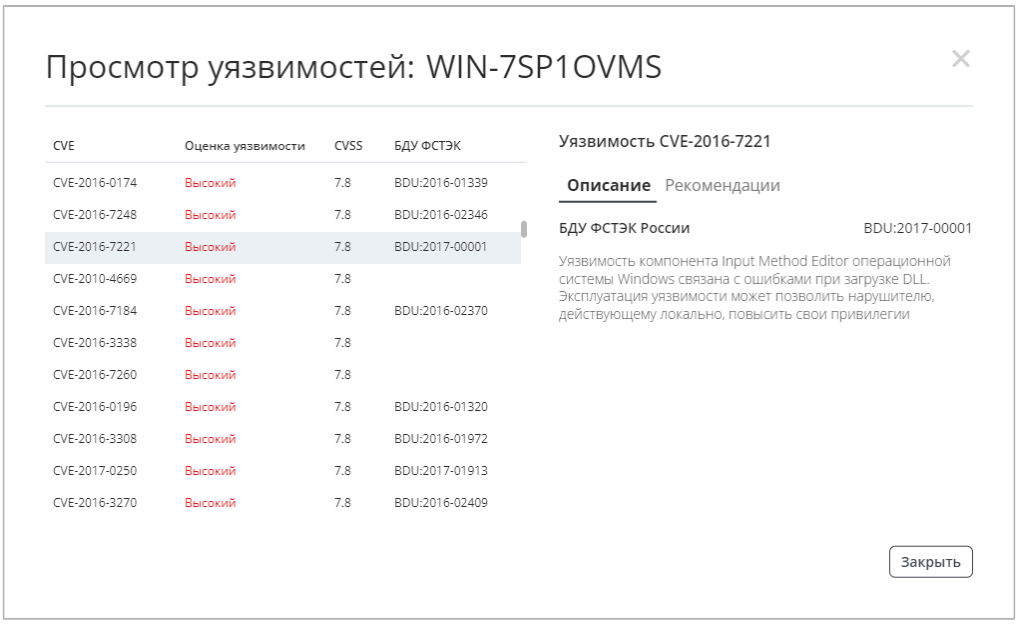


Рис. 251. Окно «Просмотр уязвимостей»

   б. Для просмотра рекомендаций выберите уязвимость из списка и откройте вкладку **Рекомендации**.

   ▸ **Результат шага:** отобразится текстовая ссылка на рекомендации производителя и кнопка **Ссылка на источник**, при нажатии которой откроется веб-страница с рекомендациями по устранению уязвимости.

> Внимание:
>
> Веб-страница с рекомендациями откроется только при наличии доступа в Интернет.

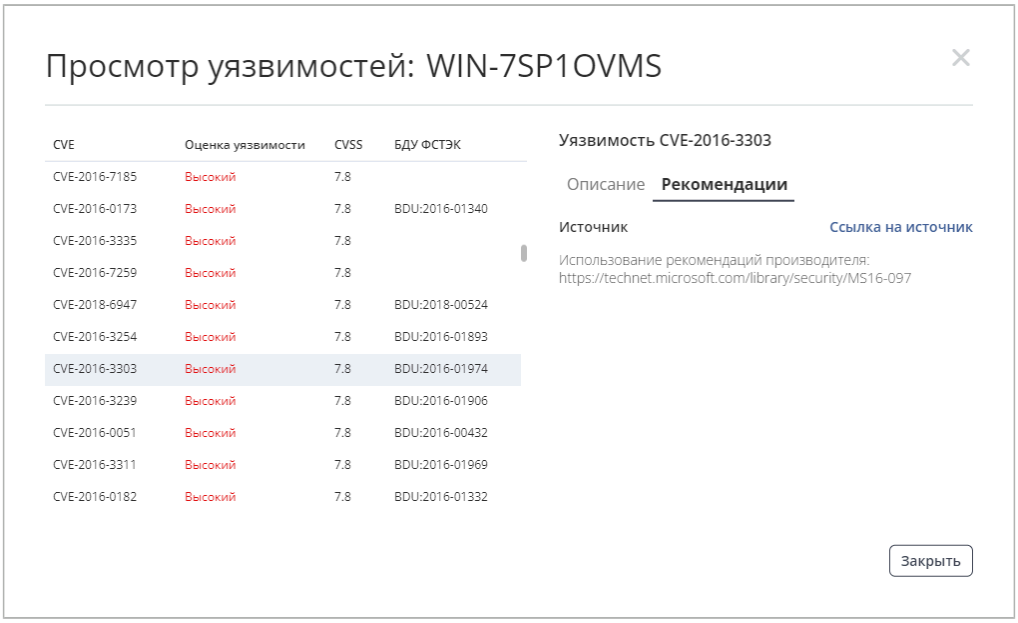


Рис. 252. Вкладка «Рекомендации»

2. Для просмотра уязвимостей в отчете формата `*.csv`:
   a. Перейдите в карточку актива, на котором выполнялся поиск уязвимостей, и откройте окно **Запуск поиска уязвимостей**.
   б. В открывшемся окне скачайте отчет формата `*.csv`.

   ▸ **Результат шага:** Файл с отчетом формата `*.csv` будет загружен на компьютер в директорию загрузки по умолчанию.

14.1.5. Выгрузка отчета по результатам сопоставления собранного ПО со справочником CPE

Для экспорта отчета, содержащего результаты сопоставления собранного сканерами ПО и ОС со справочником CPE всех активов, для которых когда-либо выполнялся поиск уязвимостей:

1. Перейдите на страницу **Инспекция активов → Перечень ПО**.
2. При необходимости очистите предыдущий файл отчета — для этого нажмите кнопку (**Очистить отчет по результатам сопоставления собранного ПО со справочником CPE**).
3. Запустите поиск уязвимостей на активах — подробнее см. раздел «Запуск поиска уязвимостей в базах CVE, CPE и БДУ ФСТЭК России».

> Подсказка:
>
> Отчет по результатам сопоставления собранного ПО со справочником CPE может содержать объединенный список ПО с нескольких активов — для этого перед выгрузкой отчета необходимо запустить и дождаться завершения поиска уязвимостей на всех требуемых активах.

4. Нажмите кнопку (**Экспортировать отчет по результатам сопоставления собранного ПО со справочником CPE**).
   - **Результат шага:** Файл с отчетом формата `*.csv` будет загружен на компьютер в директорию загрузки по умолчанию.
5. Заполните анкету, укажите в ней список ПО, для которого необходимо уточнить CPE, и отправьте с анкетой файл отчета на адрес сервисного центра ООО «СайберЛимфа»: support@cyberlympha.com

14.2. Проверки на уязвимости и соответствие требованиям информационной безопасности с помощью OVAL

В этом разделе приведен порядок настройки и выполнения проверок активов на уязвимости и соответствие требованиям информационной безопасности с помощью OVAL:

1. Импорт и экспорт скриптов, настроек, групп определений OVAL
2. Настройка OVAL-проверки актива на соответствие требованиям информационной безопасности
3. Запуск OVAL-проверки актива на соответствие требованиям информационной безопасности
4. Просмотр и выгрузка результатов проверки актива на соответствие требованиям информационной безопасности
5. Повторный запуск OVAL-проверки на соответствие требованиям ИБ
6. Удаление OVAL-проверок актива на соответствие требованиям информационной безопасности

Пример содержимого файла формата `*.xml`, содержащего OVAL-определения для оценки соответствия парольной политики Windows:

```
<?xml version="1.0" encoding="UTF-8"?>
<oval_definitions xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5" xmlns:oval="http://oval.mitre.org/XMLSchema/oval-common-5"  xmlns:oval-def="http://oval.mitre.org/XMLSchema/oval-definitions-5" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
 <generator>
 <oval:product_name>The CyberLympha OVAL Repository</oval:product_name>
 <oval:schema_version>5.10.1</oval:schema_version>
 <oval:timestamp>2018-05-14T14:06:41.489-04:00</oval:timestamp>
 </generator>
 <definitions>
 <definition class="compliance" id="oval:datapk.cyberlympha.ru:def:1" version="1">
 <metadata>
 <title>Password age check</title>
 <description>Password age check</description>
 </metadata>
 <criteria>
 <criterion comment="Password min age check" test_ref="oval:datapk.cyberlympha.ru:tst:1"/>
 <criterion comment="Password max age check" test_ref="oval:datapk.cyberlympha.ru:tst:2"/>
 </criteria>
 </definition>
 <definition class="compliance" id="oval:datapk.cyberlympha.ru:def:2" version="1">
 <metadata>
 <title>Password complexity check</title>
```

```
 <description>Password complexity check</description>
 </metadata>
 <criteria>
 <criterion comment="Password length check" test_ref="oval:datapk.cyberlympha.ru:tst:3"/>
 <criterion comment="Password complexity check" test_ref="oval:datapk.cyberlympha.ru:tst:4"/>
 <criterion comment="Password history size check" test_ref="oval:datapk.cyberlympha.ru:tst:5"/>
 </criteria>
 </definition>
 <definition class="compliance" id="oval:datapk.cyberlympha.ru:def:3" version="1">
 <metadata>
 <title>Password encryption check</title>
 <description>Password encryption check</description>
 </metadata>
 <criteria>
        <criterion        comment="Password        reversible        encryption        check"
 test_ref="oval:datapk.cyberlympha.ru:tst:6"/>
 </criteria>
 </definition>
 </definitions>
 <tests>
  <passwordpolicy_test  check="all"  check_existence="at_least_one_exists"  comment="Test  if  the
 min_passwd_age is compliant." id="oval:datapk.cyberlympha.ru:tst:1" version="1" xmlns="http://
oval.mitre.org/XMLSchema/oval-definitions-5#windows">
 <object object_ref="oval:datapk.cyberlympha.ru:obj:1"/>
 <state state_ref="oval:datapk.cyberlympha.ru:ste:1"/>
 </passwordpolicy_test>
  <passwordpolicy_test  check="all"  check_existence="at_least_one_exists"  comment="Test  if  the
 max_passwd_age is compliant." id="oval:datapk.cyberlympha.ru:tst:2" version="1" xmlns="http://
oval.mitre.org/XMLSchema/oval-definitions-5#windows">
 <object object_ref="oval:datapk.cyberlympha.ru:obj:1"/>
 <state state_ref="oval:datapk.cyberlympha.ru:ste:2"/>
 </passwordpolicy_test>
  <passwordpolicy_test  check="all"  check_existence="at_least_one_exists"  comment="Test  if  the
 min_passwd_len is compliant." id="oval:datapk.cyberlympha.ru:tst:3" version="1" xmlns="http://
oval.mitre.org/XMLSchema/oval-definitions-5#windows">
 <object object_ref="oval:datapk.cyberlympha.ru:obj:1"/>
 <state state_ref="oval:datapk.cyberlympha.ru:ste:3"/>
 </passwordpolicy_test>
   <passwordpolicy_test   check="all"   check_existence="at_least_one_exists"   comment="Test   if
   the   password_complexity   is   compliant."   id="oval:datapk.cyberlympha.ru:tst:4"   version="1"
 xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5#windows">
 <object object_ref="oval:datapk.cyberlympha.ru:obj:2"/>
 <state state_ref="oval:datapk.cyberlympha.ru:ste:4"/>
 </passwordpolicy_test>
  <passwordpolicy_test  check="all"  check_existence="at_least_one_exists"  comment="Test  if  the
 password_hist_len is compliant." id="oval:datapk.cyberlympha.ru:tst:5" version="1" xmlns="http:/
/oval.mitre.org/XMLSchema/oval-definitions-5#windows">
```

```
<object object_ref="oval:datapk.cyberlympha.ru:obj:2"/>
<state state_ref="oval:datapk.cyberlympha.ru:ste:5"/>
</passwordpolicy_test>
  <passwordpolicy_test check="all" check_existence="at_least_one_exists" comment="Test if
 the reversible_encryption is compliant." id="oval:datapk.cyberlympha.ru:tst:6" version="1"
xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5#windows">
<object object_ref="oval:datapk.cyberlympha.ru:obj:2"/>
<state state_ref="oval:datapk.cyberlympha.ru:ste:6"/>
</passwordpolicy_test>
</tests>
<objects>
       <passwordpolicy_object       comment="Retrieves       a       passwordpolicy_object."
 id="oval:datapk.cyberlympha.ru:obj:1" version="1" xmlns="http://oval.mitre.org/XMLSchema/oval-
definitions-5#windows"/>
       <passwordpolicy_object       comment="Retrieves       a       passwordpolicy_object."
 id="oval:datapk.cyberlympha.ru:obj:2" version="1" xmlns="http://oval.mitre.org/XMLSchema/oval-
definitions-5#windows"/>
</objects>
<states>
<passwordpolicy_state comment="This passwordpolicy_state represents a password policy that has
a min_passwd_age greater than or equal to 2." id="oval:datapk.cyberlympha.ru:ste:1" version="1"
xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5#windows">
<min_passwd_age datatype="int" operation="greater than or equal">2</min_passwd_age>
</passwordpolicy_state>
<passwordpolicy_state comment="This passwordpolicy_state represents a password policy that has
 a max_passwd_age less than or equal to 6." id="oval:datapk.cyberlympha.ru:ste:2" version="1"
xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5#windows">
<max_passwd_age datatype="int" operation="less than or equal">6</max_passwd_age>
</passwordpolicy_state>
<passwordpolicy_state comment="This passwordpolicy_state represents a password policy that has
a min_passwd_len greater than or equal to 6." id="oval:datapk.cyberlympha.ru:ste:3" version="1"
xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5#windows">
<min_passwd_len datatype="int" operation="greater than or equal">6</min_passwd_len>
</passwordpolicy_state>
 <passwordpolicy_state comment="This passwordpolicy_state represents a password policy that
 has a password_complexity equal to true." id="oval:datapk.cyberlympha.ru:ste:4" version="1"
xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5#windows">
<password_complexity datatype="boolean">true</password_complexity>
</passwordpolicy_state>
<passwordpolicy_state comment="This passwordpolicy_state represents a password policy that has a
password_hist_len greater than or equal to 2." id="oval:datapk.cyberlympha.ru:ste:5" version="1"
xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5#windows">
<password_hist_len datatype="int" operation="greater than or equal">2</password_hist_len>
</passwordpolicy_state>
 <passwordpolicy_state comment="This passwordpolicy_state represents a password policy that
has a reversible_encryption equal to false." id="oval:datapk.cyberlympha.ru:ste:6" version="1"
xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5#windows">
```

```
 <reversible_encryption datatype="boolean">false</reversible_encryption>
 </passwordpolicy_state>
 </states>
</oval_definitions>
```

14.2.1. Импорт и экспорт скриптов, настроек, групп определений OVAL

В этом разделе:

- Импорт групп OVAL-определений
- Импорт OVAL-определений
- Импорт скриптов OVAL
- Импорт настроек OVAL
- Экспорт групп OVAL-определений
- Экспорт скриптов OVAL
- Экспорт настроек OVAL

Экспорт и импорт OVAL-объектов осуществляется на странице **Администрирование** → **Основные настройки** → **Импорт и экспорт** в блоке **OVAL**.

Внимание:

Настройки OVAL — это связь меток активов, имеющих определенный идентификатор, со скриптами OVAL, у которых так же определен идентификатор. Поэтому перед выполнением импорта настроек OVAL необходимо предварительно импортировать следующие справочники, поставляемые в комплекте дистрибутива Комплекса:

- метки активов из файла `[version]_oval_tags.json`— подробнее см. «Импорт меток»;
- скрипты OVAL из файла `[version]_oval_scripts.json` — подробнее см. «Импорт скриптов OVAL».

Для того, чтобы механизм анализа уязвимостей смог определить, какой скрипт OVAL применять для выбранного актива при запуске проверки, необходимо присвоить активу необходимые метки. Наименования таких меток содержат наименование операционной системы или возможного механизма получения данных с активов, например: `winrm/http`, `dpkg`, `Windows NT 3.1`).

Рис. 253. Блок «OVAL» на странице «Импорт и экспорт»

14.2.1.1. Импорт групп OVAL-определений

Прим.:

Файл `[version]_oval_groups.json` с группами OVAL, поставляемый в комплекте дистрибутива Комплекса, уже содержит набор необходимых OVAL-определений для дальнейшего выполнения проверок активов на уязвимости и контроля соответствия ИБ, поэтому не требуется отдельно импортировать OVAL-определения.

Для импорта групп OVAL-определений из файла формата `*.json` в Комплекс:

1. Перейдите на страницу **Администрирование → Основные настройки → Импорт и экспорт**.
2. В блоке **OVAL** в строке **Группы OVAL-определений** нажмите кнопку .
3. В открывшемся окне укажите расположение импортируемого файла формата `*.xml` и подтвердите выбор.
4. В открывшемся окне **Подготовка к импорту** выберите действие для элементов, которые отсутствуют в новом (загружаемом) справочнике:
   - **Оставить** — новые элементы будут добавлены к уже существующим;
   - **Удалить** — старые элементы будут удалены и добавлены новые.

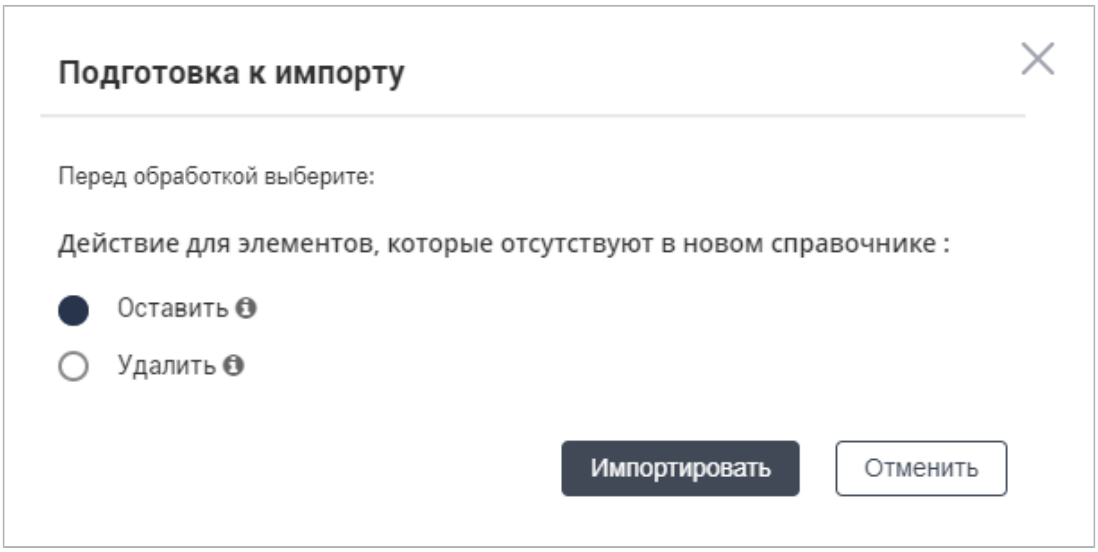


Рис. 254. Окно «Подготовка к импорту»

5. нажать кнопку **Импортировать** для выполнения импорта.

▸ **Результат шага:** будет запущен процесс импорта: в правом верхнем углу появится уведомление `Запущен импорт справочника`, а под заголовком **Результат последнего импорта** будет символ `-`.

> Подсказка:
>
> Операции импорта являются фоновыми — со страницы можно безопасно уходить.

6. Убедитесь, что группы OVAL-определений был успешно загружены.
   - Если файл импортирован успешно, в правом вернем углу под заголовком **Результат последнего импорта** появится уведомление: `Успешно`.
   - Если произошла ошибка, в правом верхнем углу под заголовком **Результат последнего импорта** появится уведомление `Ошибка`. Для просмотра информации об ошибке нажмите ссылку **Подробнее** в подсказке ℹ рядом с уведомлением.

▸ **Результат шага:** в результате успешного импорта на странице **Администрирование → Инспекция активов → Группы OVAL** появится импортированный справочник.

14.2.1.2. Импорт OVAL-определений

Для импорта OVAL-определений из файла формата `*.xml` в Комплекс:

1. Перейдите на страницу **Администрирование → Основные настройки → Импорт и экспорт**.
2. В блоке **OVAL** в строке **OVAL-определения** нажмите кнопку .
3. В открывшемся окне укажите расположение импортируемого файла формата `*.xml` и подтвердите выбор.

▸ **Результат шага:** будет запущен процесс импорта: в правом верхнем углу появится уведомление `Запущен импорт справочника`, а под заголовком **Результат последнего импорта** будет символ `-`.

> Подсказка:
>
> Операции импорта являются фоновыми — со страницы можно безопасно уходить.

4. Убедитесь, что OVAL-определения были успешно загружены.
   - Если файл импортирован успешно, в правом вернем углу под заголовком **Результат последнего импорта** появится уведомление: `Успешно`.
   - Если произошла ошибка, в правом верхнем углу под заголовком **Результат последнего импорта** появится уведомление `Ошибка`. Для просмотра информации об ошибке нажмите ссылку **Подробнее** в подсказке ℹ рядом с уведомлением.

▸ **Результат шага:** в результате успешного импорта на странице **Администрирование → Инспекция активов → Определения OVAL** появится импортированный справочник.

Что дальше: OVAL-определения применяются в OVAL-проверках только в составе OVAL-групп, поэтому перед запуском проверок необходимо добавить определения в группы — подробнее см. «Создание группы определений OVAL» и «Добавление и исключение OVAL-определений из групп».

14.2.1.3. Импорт скриптов OVAL

Для импорта скриптов OVAL из файла формата `*.json` в Комплекс:

1. Перейдите на страницу **Администрирование → Основные настройки → Импорт и экспорт**.
2. В блоке **OVAL** в строке **Скрипты OVAL** нажмите кнопку .
3. В открывшемся окне укажите расположение импортируемого файла формата `*.json` и подтвердите выбор.
4. В открывшемся окне **Подготовка к импорту** выберите действие для элементов, которые отсутствуют в новом (загружаемом) справочнике:
   - **Оставить** — новые элементы будут добавлены к уже существующим;
   - **Удалить** — старые элементы будут удалены и добавлены новые.

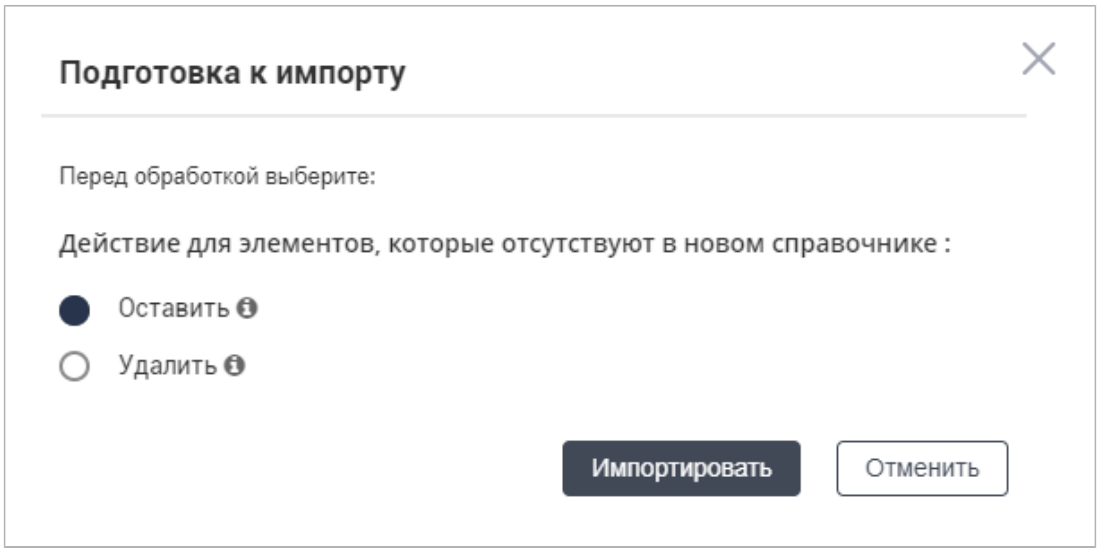


Рис. 255. Окно «Подготовка к импорту»

5. нажать кнопку **Импортировать** для выполнения импорта.

   ▸ **Результат шага:** будет запущен процесс импорта: в правом верхнем углу появится уведомление `Запущен импорт справочника`, а под заголовком **Результат последнего импорта** будет символ `-`.

> Подсказка:
>
> Операции импорта являются фоновыми — со страницы можно безопасно уходить.

6. Убедитесь, что скрипты OVAL были успешно загружены.
   - Если файл импортирован успешно, в правом вернем углу под заголовком **Результат последнего импорта** появится уведомление: `Успешно`.
   - Если произошла ошибка, в правом верхнем углу под заголовком **Результат последнего импорта** появится уведомление `Ошибка`. Для просмотра информации об ошибке нажмите ссылку **Подробнее** в подсказке рядом с уведомлением.

   ▸ **Результат шага:** в результате успешного импорта на странице **Администрирование → Инспекция активов → Скрипты OVAL** появится импортированный справочник.

14.2.1.4. Импорт настроек OVAL

Перед выполнением:

Убедитесь, что настройки OVAL в импортируемом файле подготовлены для корректной загрузки, а именно:

- В Комплекс уже импортированы скрипты OVAL, id которых указаны в каждой импортируемой настройке OVAL.

  > Подсказка:
  >
  > Подробнее об импорте OVAL скриптов см. раздел «Импорт скриптов OVAL».

- В каждой настройке OVAL указан хотя бы один из следующих параметров, который будет связывать скрипты OVAL с существующими активами:
  - id метки актива, уже существующей в Комплексе;
  - параметр **По умолчанию** (`is_default`);
  - список активов.

> ОСТОРОЖНО:
>
> Если в импортируемом файле присутствуют не все параметры (метка, параметр **По умолчанию**, список активов), настройка будет импортирована без них.

> Прим.:
>
> В комплекте дистрибутива Комплекса поставляются следующие файлы для импорта базовых настроек OVAL:
>
> - `[version]_oval_tags.json` — набор меток активов для более быстрой подготовки активов к сбору данных во время OVAL-проверок;
> - `[version]_oval_scripts.json` — набор скриптов OVAL, которые будут собирать определенные данные с активов во время OVAL-проверок.
>
> Файл с настройками OVAL `[version]_oval_host_script_relations.json`, поставляемый в комплекте дистрибутива, уже содержит набор связей скриптов OVAL из файла `[version]_oval_scripts.json`, с метками из файла `[version]_oval_tags.json`.

Для импорта настроек OVAL из файла формата `*.json` в Комплекс:

1. Перейдите на страницу **Администрирование → Основные настройки → Импорт и экспорт**.
2. В блоке **OVAL** в строке **Настройки OVAL** нажмите кнопку (**Импортировать**).
3. В открывшемся окне укажите расположение импортируемого файла формата `*.json` и подтвердите выбор.
4. В открывшемся окне **Подготовка к импорту** выберите действие для элементов, которые отсутствуют в новом (загружаемом) справочнике:
   - **Оставить** — новые элементы будут добавлены к уже существующим;
   - **Удалить** — старые элементы будут удалены и добавлены новые.

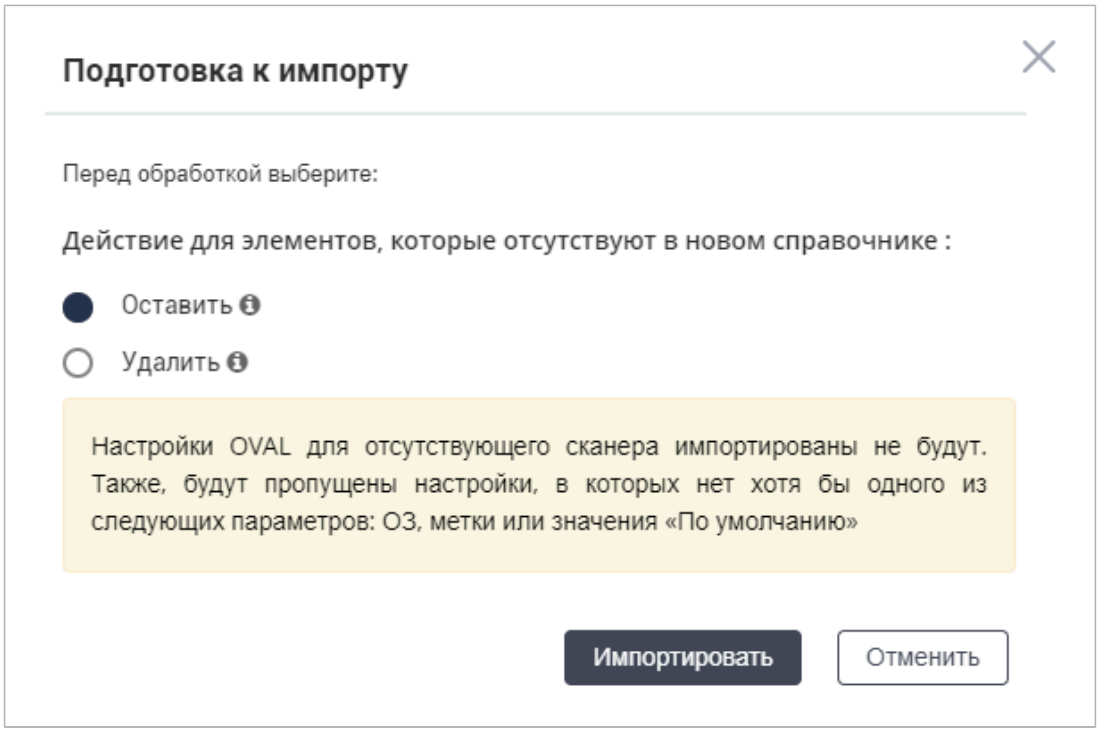


Рис. 256. Окно подготовки к импорту настроек OVAL

5. Нажмите кнопку **Импортировать** для выполнения импорта.
   - **Результат шага:** будет запущен процесс импорта: в правом верхнем углу появится уведомление `Запущен импорт справочника`, а под заголовком **Результат последнего импорта** будет символ `-`.

> Подсказка:
>
> Операции импорта являются фоновыми — со страницы можно безопасно уходить.

6. Убедитесь, что настройки OVAL были успешно загружены.
   - Если файл импортирован успешно, в правом вернем углу под заголовком **Результат последнего импорта** появится уведомление: `Успешно`.
   - Если произошла ошибка, в правом верхнем углу под заголовком **Результат последнего импорта** появится уведомление `Ошибка`. Для просмотра информации об ошибке нажмите ссылку **Подробнее** в подсказке рядом с уведомлением.
   - **Результат шага:** в результате успешного импорта на странице **Администрирование → Инспекция активов → Настройки OVAL** появится импортированный справочник.

14.2.1.5. Экспорт групп OVAL-определений

Для экспорта групп OVAL-определений вместе с OVAL-определениями в файл формата `*.json`:

1. Перейдите на страницу **Администрирование → Основные настройки → Импорт и экспорт**.
2. На панели **OVAL** в строке **Группы OVAL-определений** нажмите кнопку (**Экспортировать**).
   - **Результат шага:** файл со списком групп OVAL-определений `oval_groups_[дата_и_время].json` будет сформирован и доступен для скачивания в правом верхнем углу страницы **Импорт и экспорт** под заголовком **Результат последнего экспорта**.
3. Для скачивания файла нажмите на его название в верхнем правом углу под заголовком **Результат последнего экспорта**.

4. В открывшемся окне укажите расположение для экспортируемого файла, при необходимости изменив его название, и нажмите кнопку **Сохранить**.
   - **Результат шага:** файл `oval_groups_[дата_и_время].json` будет загружен на компьютер.

14.2.1.6. Экспорт скриптов OVAL

> Внимание:
>
> Экспорт OVAL-определений доступен только в составе групп OVAL-определений.

Для экспорта списка скриптов OVAL в файл формата `*.json`:

1. Перейдите на страницу **Администрирование → Основные настройки → Импорт и экспорт**.
2. На панели **OVAL** в строке **Скрипты OVAL** нажмите кнопку (**Экспортировать**).
   - **Результат шага:** файл со списком скриптов OVAL `oval_scripts_[дата_и_время].json` будет сформирован и доступен для скачивания в правом верхнем углу страницы **Импорт и экспорт** под заголовком **Результат последнего экспорта**.
3. Для скачивания файла нажмите на его название в верхнем правом углу под заголовком **Результат последнего экспорта**.
4. В открывшемся окне укажите расположение для экспортируемого файла, при необходимости изменив его название, и нажмите кнопку **Сохранить**.
   - **Результат шага:** файл `oval_scripts_[дата_и_время].json` будет загружен на компьютер.

14.2.1.7. Экспорт настроек OVAL

Для экспорта списка настроек OVAL в файл формата `*.json`:

1. Перейдите на страницу **Администрирование → Основные настройки → Импорт и экспорт**.
2. На панели **OVAL** в строке **Настройки OVAL** нажмите кнопку (**Экспортировать**).
   - **Результат шага:** файл со списком настроек OVAL `oval_settings_[дата_и_время].json` будет сформирован и доступен для скачивания в правом верхнем углу страницы **Импорт и экспорт** под заголовком **Результат последнего экспорта**.
3. Для скачивания файла нажмите на название сформированного файла под заголовком **Результат последнего экспорта**.
4. В открывшемся окне укажите расположение для экспортируемого файла, при необходимости изменив его название, и нажмите кнопку **Сохранить**.
   - **Результат шага:** файл `oval_settings_[дата_и_время].json` будет загружен на компьютер.

14.2.2. Настройка OVAL-проверки актива на соответствие требованиям информационной безопасности

Для запуска OVAL-проверок на соответствие требованиям ИБ пользователь Комплекса должен убедиться, что все необходимые для этого элементы были ранее настроены. Для настройки вы можете последовательно воспользоваться следующими разделами:

- Управление скриптами OVAL
- Настройка доступа к активу для сбора OVAL-объектов
- Проверка привязки OVAL-скрипта к активу

- Создание группы определений OVAL
- Добавление и исключение OVAL-определений из групп

14.2.2.1. Управление скриптами OVAL

Для работы со скриптами в веб-интерфейсе Комплекса доступны следующие возможности:

1. Создание скрипта. Для создания:

   а. Перейдите в подраздел **Инспекция активов → Результаты проверок → Инспекция активов → Скрипты OVAL**.

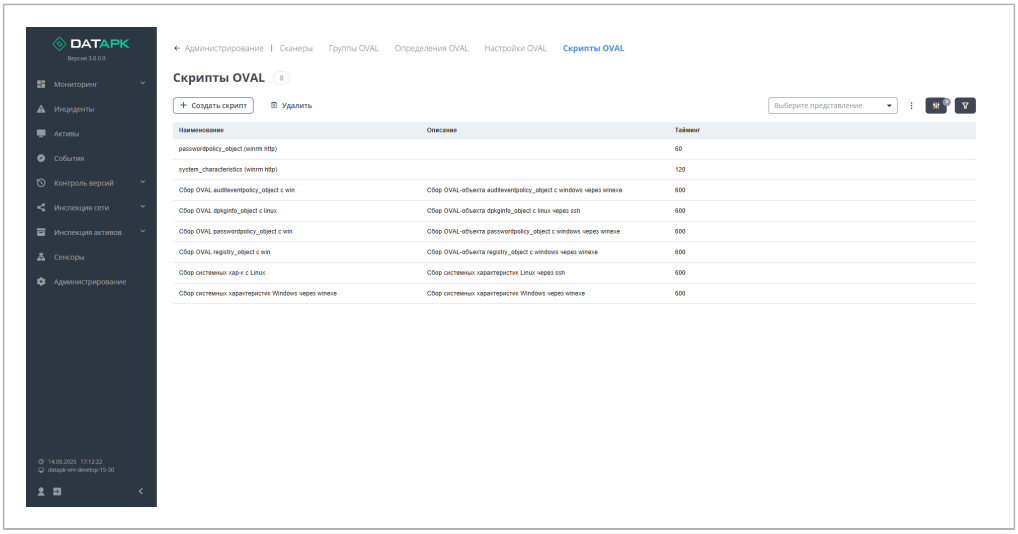


Рис. 257. Страница «Скрипты OVAL»

   б. Нажмите кнопку **Создать скрипт**. В открывшемся окне **Создание скрипта OVAL** задайте следующие параметры:

   - наименование и описание скрипта;
   - тип OVAL-объекта;
   - цифровую подпись скрипта (подробнее см. в разделе «Цифровая подпись Python-скрипта»);
   - при необходимости введите максимальное время ожидания выполнения задачи в секундах;
   - нажмите кнопку **Импортировать** для загрузки скрипта из файла. В проводнике выберите и откройте подписанный ранее файл скрипта формата `*.py`;

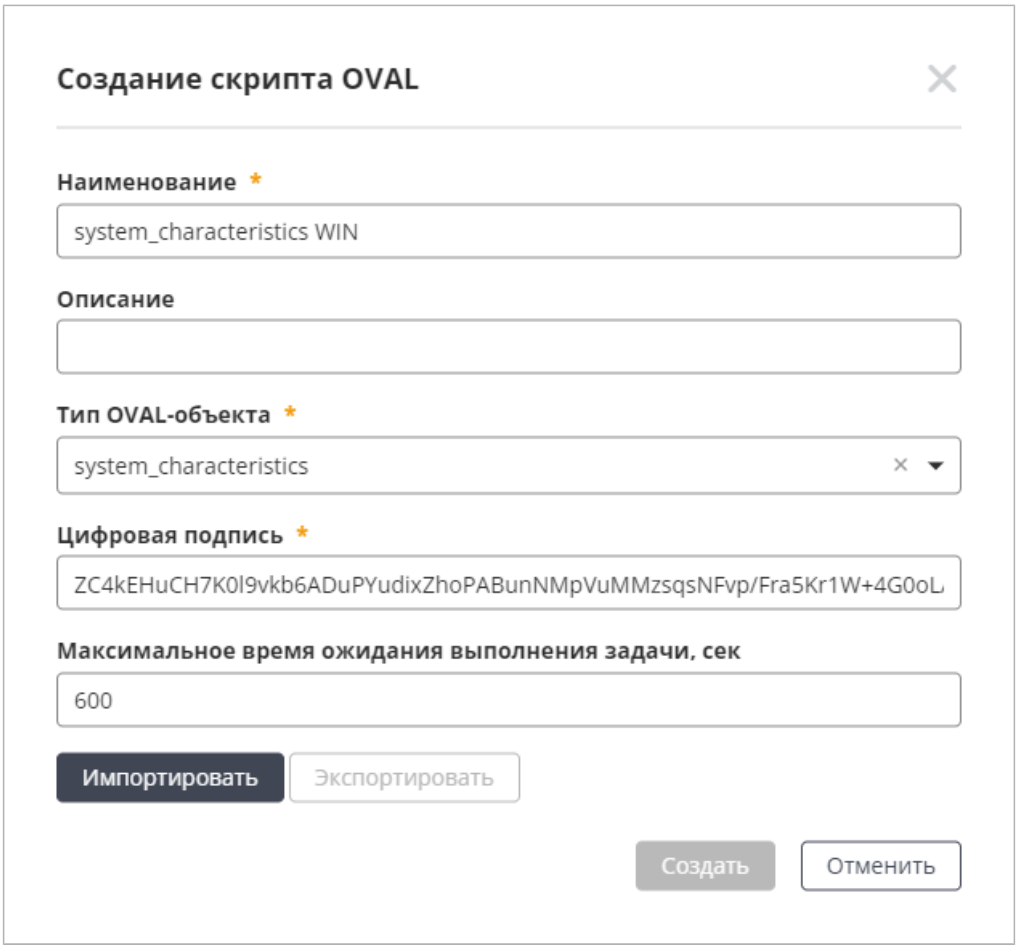


Рис. 258. Окно «Создание скрипта OVAL»

в. Нажмите кнопку **Создать** для подтверждения изменений.

2. Изменение скрипта. Для изменения:

а. Перейдите в подраздел **Инспекция активов → Результаты проверок → Инспекция активов → Скрипты OVAL**.

б. Наведите на правую часть строки изменяемого скрипта.

в. Нажмите кнопку (**Редактировать**).

- **Результат шага:** появится окно **Редактирование скрипта OVAL**

г. Измените необходимые параметры

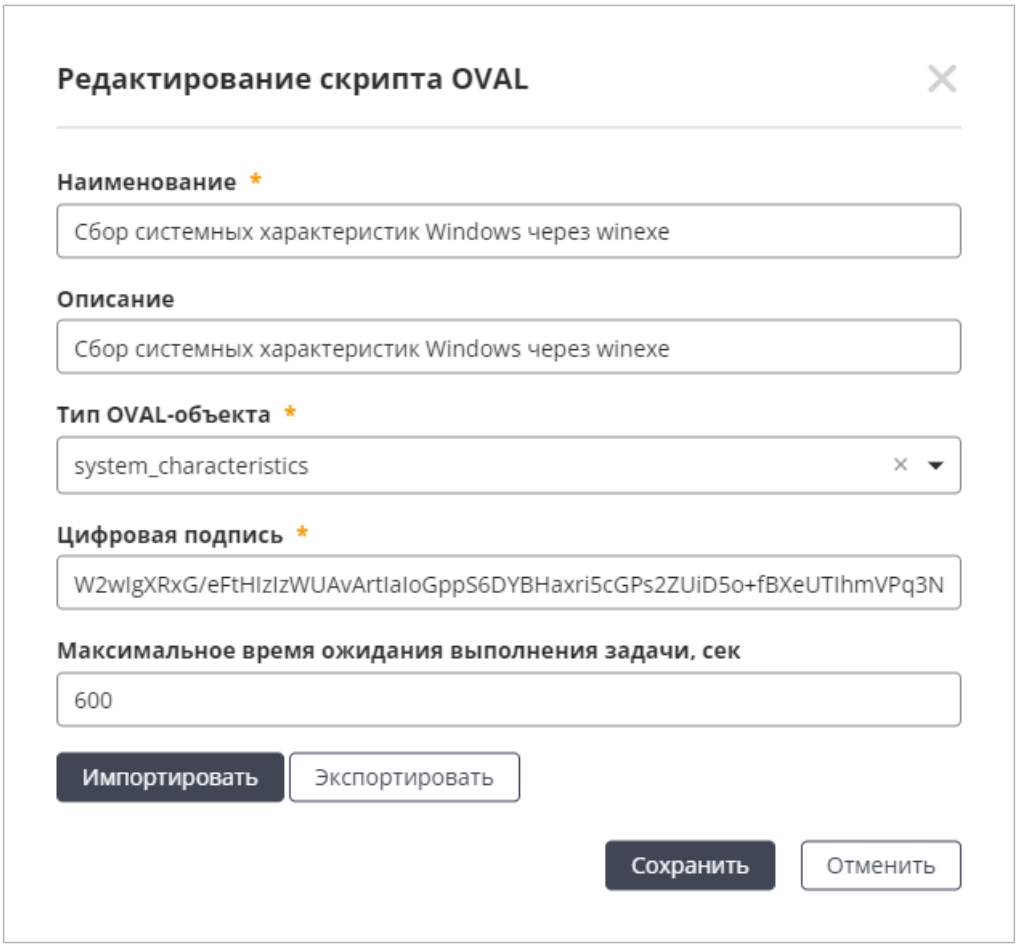


Рис. 259. Окно «Редактирование скрипта OVAL»

д. Нажмите кнопку **Сохранить** для подтверждения изменений.

3. Удаление скрипта. Для удаления:

   а. Наведите курсор на правую часть строки удаляемого скрипта.

   б. Нажмите кнопку (**Удалить скрипт**).

   - **Результат шага:** появится окно подтверждения удаления.

   в. Введите обоснование удаления скрипта и нажмите **Подтвердить**.

4. Удаление группы скриптов. Для удаления:

   а. При помощи фильтров отрегулируйте выборку так, чтобы отображались только скрипты, которые будут удалены.

   б. Нажмите (**Удалить скрипты**).

   - **Результат шага:** появится окно подтверждения удаления.

   в. Введите обоснование удаления скриптов и нажмите **Подтвердить**.

14.2.2.2. Настройка доступа к активу для сбора OVAL-объектов

Для настройки доступа к активу для сбора OVAL-объектов:

1. Добавьте, учетную запись актива (см. раздел «Настройка учетных данных активов»).
2. Привяжите учетную запись к активу. Для этого:

а. откройте окно **Карточка актива**;

б. на панели **Учетные данные** нажмите ✎.

▸ **Результат шага:** появится окно **Настройка учетных данных**.

в. выберите подходящие учетные данные из списка и нажмите **Сохранить**.

3. Убедитесь, что загружены скрипты для сбора OVAL-объектов на странице **Инспекция активов → Результаты проверок → Инспекция активов → Скрипты OVAL**.
4. Привяжите скрипты для сбора OVAL-объектов к активу. Для этого:

а. Перейдите на страницу **Инспекция активов → Результаты проверок → Инспекция активов → Настройки OVAL**.

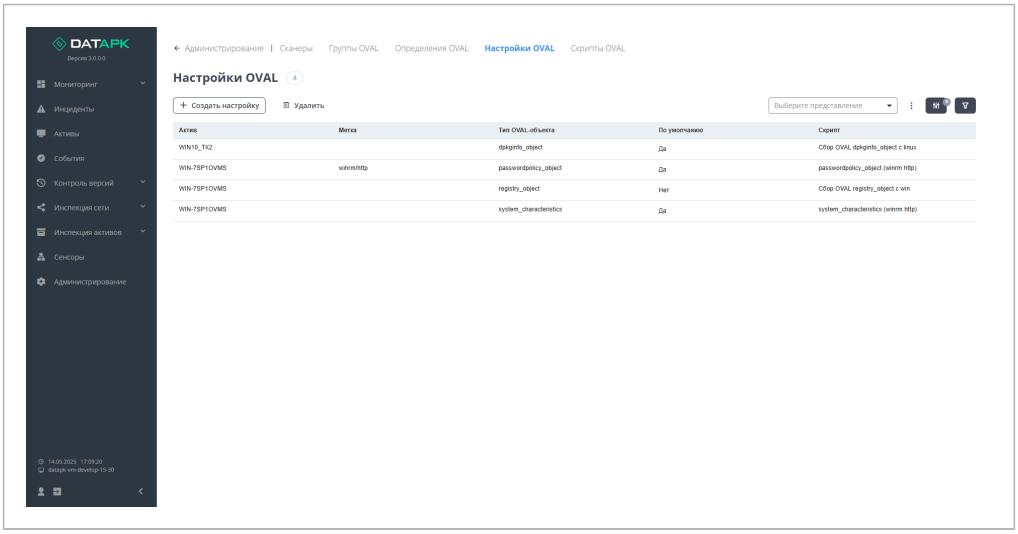


Рис. 260. Страница «Настройки OVAL»

б. Нажмите кнопку **Создать настройку**.

в. В открывшемся окне **Создание настройки OVAL** задайте следующие параметры для привязки скрипта к отдельным активам:

- в поле Скрипт выберите из списка скрипт для сбора выбранного OVAL-объекта.

> Подсказка:
>
> Тип OVAL-объекта будет отображен автоматически.

- в поле **Активы** выберите один или несколько активов, к которым будет привязан скрипт для выполнения OVAL-проверок;
- в поле **Метка** выберите из списка метку, к которой необходимо привязать скрипт для выполнения проверок на соответствие требованиям ИБ
- отметьте параметр **По умолчанию**, чтобы установить настройку для всех активов, которым не присвоена другая настройка.

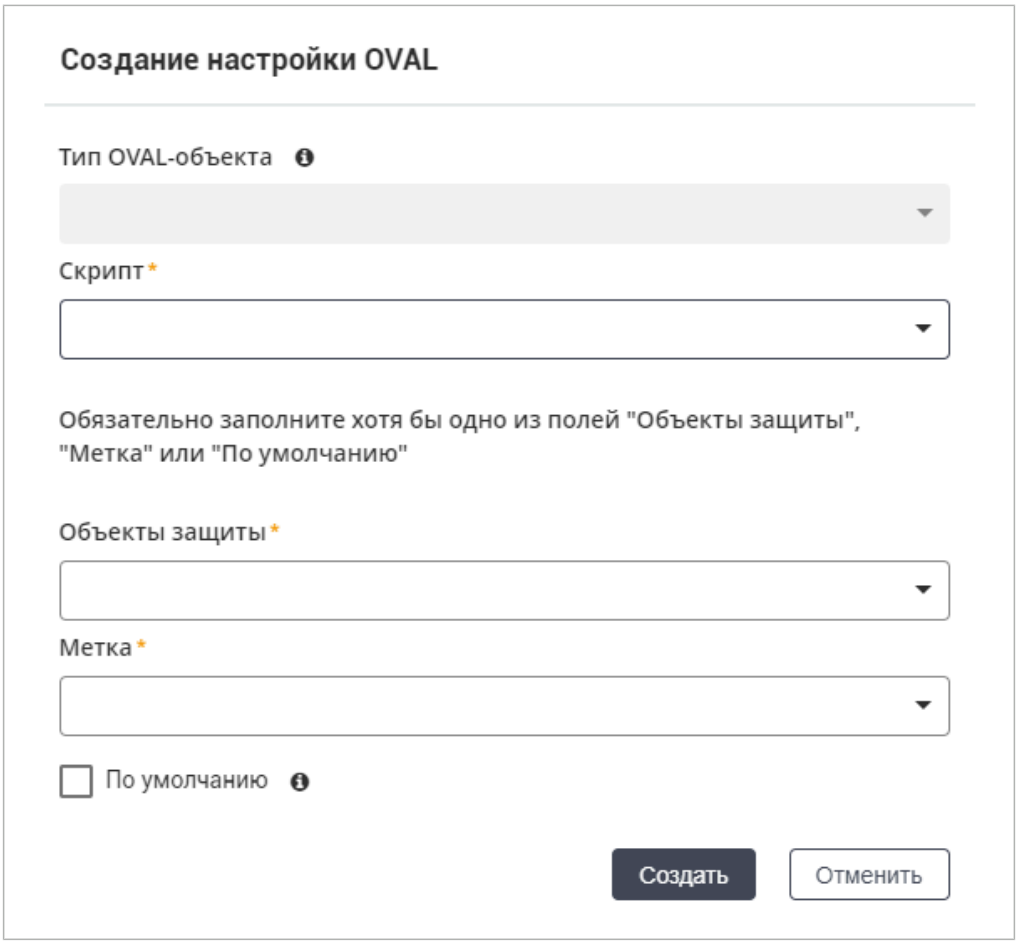


Рис. 261. Окно «Создание настройки OVAL»

г. Нажмите кнопку **Создать** для подтверждения изменений.

5. Повторите шаги из п. 4 для остальных OVAL-объектов.

14.2.2.3. Проверка привязки OVAL-скрипта к активу

Для проверки привязки (наличия OVAL-настройки) OVAL-скрипта к активу, в зависимости от используемого типа объекта:

1. Проверьте наличие персональной OVAL-настройки для актива по используемому типу OVAL-объекта.
2. Если для актива нет индивидуальных настроек по типу OVAL-объекта, проверьте наличие OVAL-настройки для меток, в которые входит актив. Если активу присвоено несколько групп, которые имеют OVAL-настройки для одного типа объекта, OVAL-настройка для актива выбирается случайным образом из настроек, назначенных меткам.
3. Если активу невозможно назначить OVAL-настройку исходя из меток, ему назначается настройка, указанная по умолчанию.

> Внимание:
>
> Если OVAL-настройки по умолчанию не заданы и активу не назначена индивидуальная настройка или настройка по меткам, в ходе выполнения OVAL-проверки для выбранного актива будет выведена ошибка.

14.2.2.4. Создание группы определений OVAL

Для создания группы определений OVAL:

1. Перейдите на страницу **Инспекция активов → Результаты проверок → Инспекция активов → Группы OVAL**.
2. Нажмите кнопку **Создать группу**. В открывшемся окне **Создание группы OVAL-определений** заполните следующие параметры:
    a. уникальное наименование группы OVAL определений;
    б. описание группы;
    в. в поле **OVAL-определения** выберите из списка импортированные определения, которые будут принадлежать новой группе.

> Подсказка:
>
> Добавить или исключить OVAL-определения из группы можно также на странице **Определения OVAL**. Подробнее см. в разделе «Добавление и исключение OVAL-определений из групп».

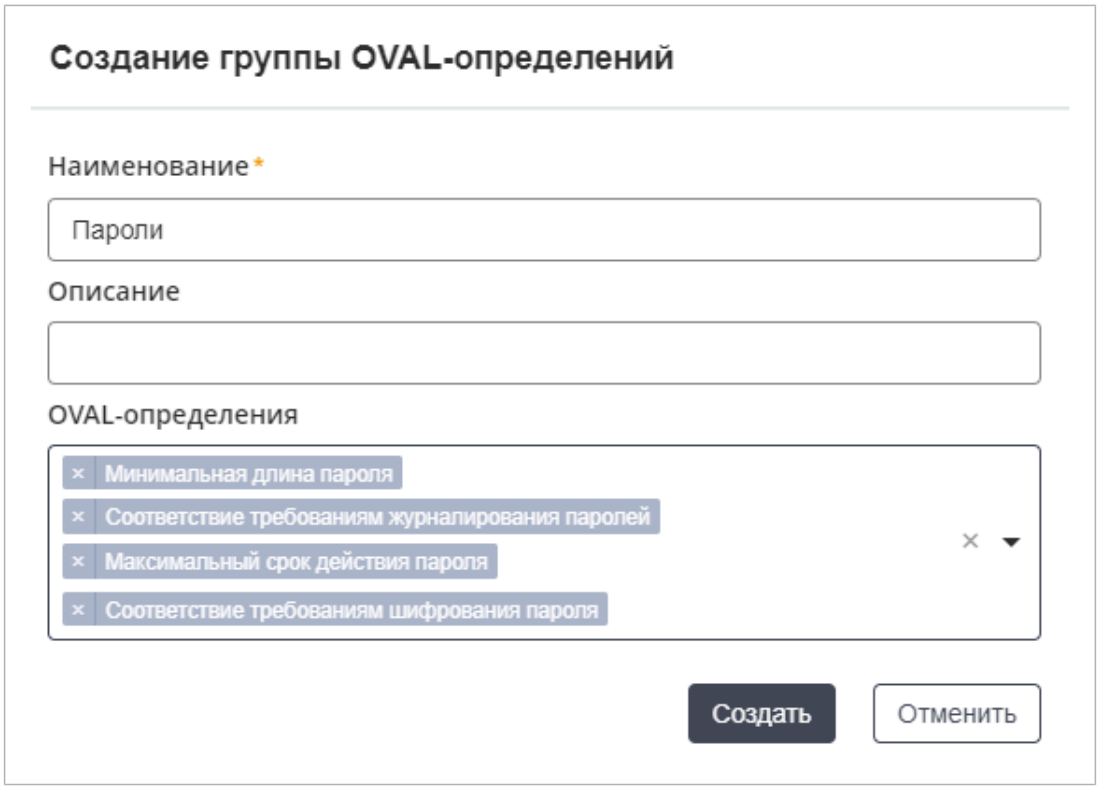


Рис. 262. Окно «Создание группы OVAL-определений»

3. Нажмите кнопку **Создать** для подтверждения изменений.

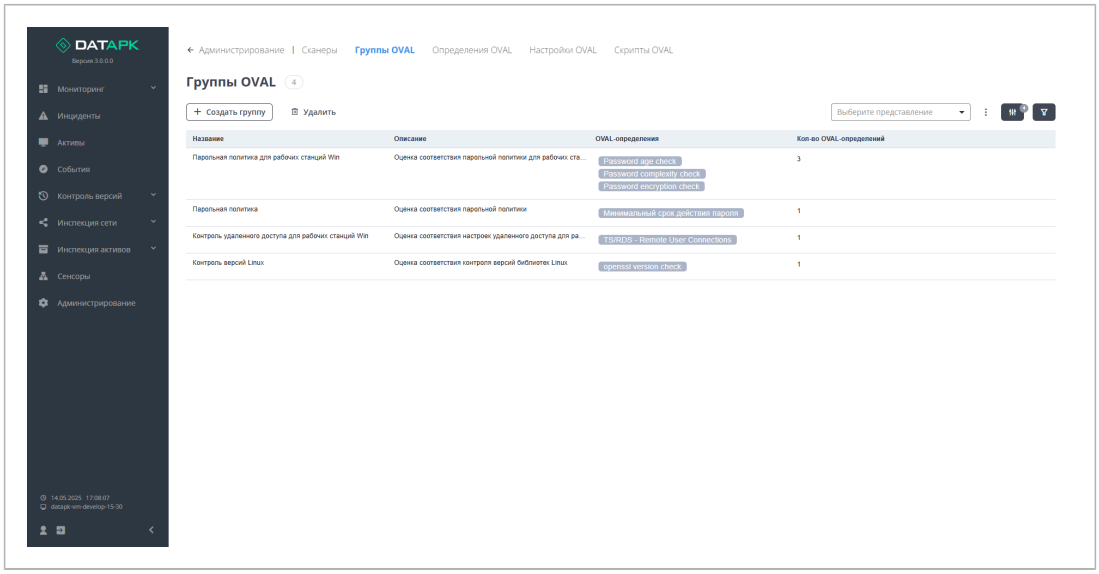


Рис. 263. Страница «Группы OVAL»

- **Результат шага:** созданная группа отобразится в списке на странице **Группы OVAL**.

14.2.2.5. Добавление и исключение OVAL-определений из групп

Для добавления или исключения OVAL-определений из созданной группы:

1. Перейдите на страницу **Инспекция активов → Результаты проверок → Инспекция активов → Определения OVAL**.
2. Выберите OVAL-определения, которые необходимо добавить в созданную группу или исключить из нее. Для этого вы можете воспользоваться следующими возможностями:

а. Выбор определений по одному. Для выбора одного определения нажмите кнопку ➕ (**Выбрать определение для добавления в группу**) в строке с требуемым OVAL-определением для выбора отдельных определений, либо установите чекбокс слева от OVAL-определения;

б. Выбор нескольких OVAL-определений. Для группового выбора OVAL-определений:

- выполните фильтрацию списка определений;
- нажмите кнопку (**Выбрать определения**) в верхней части списка определений для выбора всех определений, отображаемых в данный момент, либо установите чекбокс в заголовке таблицы;

> Подсказка:
>
> Доступен выбор до 300 определений за раз. Для изменения количества определений, которые можно выбрать, измените значения переменной `OVAL_DEFINITION_SELECT_MAX_LIMIT` в файле `manager.env`. Список всех переменных файла см. в разделе «Переменные Комплекса уровня Management».

в. Отмена выбора OVAL-определения. Для отмены нажмите ➖ (**Исключить определение из выбора**) напротив выбранного определения.

г. Отмена выбора нескольких OVAL-определений. Для групповой отмены выбора OVAL-определений:

- выполните фильтрацию списка определений;
- нажмите кнопку (**Отменить выбор**) в верхней части страницы для отмены выбора всех определений, отображаемых в данный момент;

3. Для добавления в группу:

а. Нажмите кнопку **Добавить в группу**.

б. В открывшемся окне **Добавление в группу OVAL-определений**:

- выберите из списка название созданной ранее группы;
- при необходимости измените состав OVAL-определений для добавления в группу.

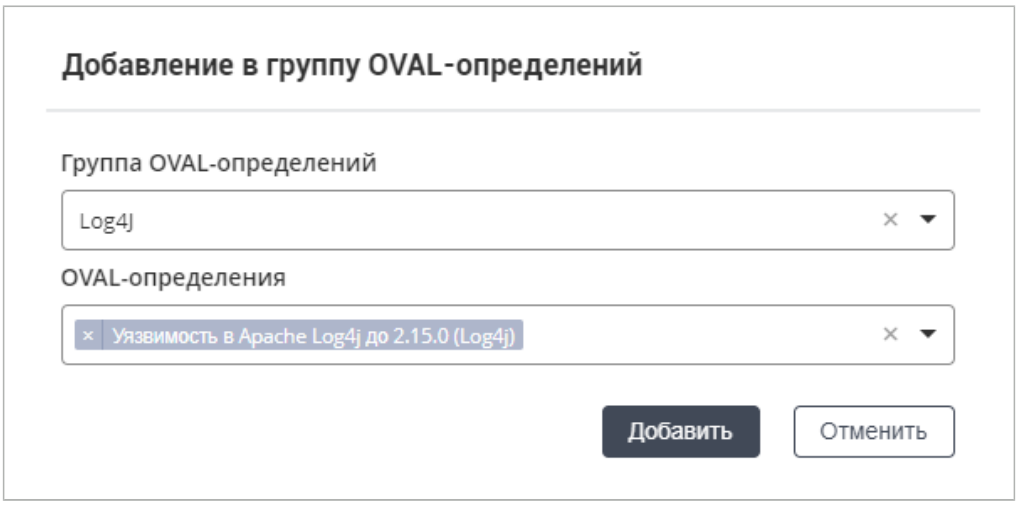


Рис. 264. Окно «Добавление в группу OVAL-определений»

в. Нажмите кнопку **Добавить**.

4. Для исключения из группы:

а. Нажмите кнопку **Исключить из группы**.

б. В открывшемся окне **Исключение OVAL-определений из групп**:

- выберите из списка название созданной ранее группы;
- при необходимости измените состав OVAL-определений для исключения из группы.

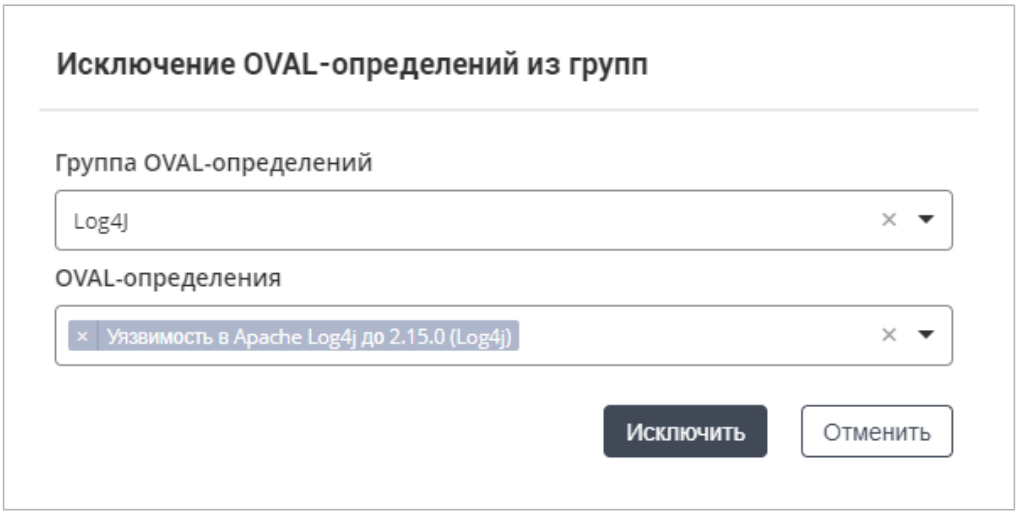


Рис. 265. Окно «Исключение OVAL-определений из групп»

в. Нажмите кнопку **Исключить**.

14.2.3. Запуск OVAL-проверки актива на соответствие требованиям информационной безопасности

Перед выполнением: Перед запуском OVAL-проверки актива на соответствие требованиям информационной безопасности убедитесь, что актив имеет сетевой атрибут. Для настройки сетевого атрибута выполните шаг 7 раздела Редактирование актива.

Для проверки актива на соответствие требованиям информационной безопасности с помощью OVAL:

1. Перейдите на страницу **Инспекция активов → Результаты проверок**.

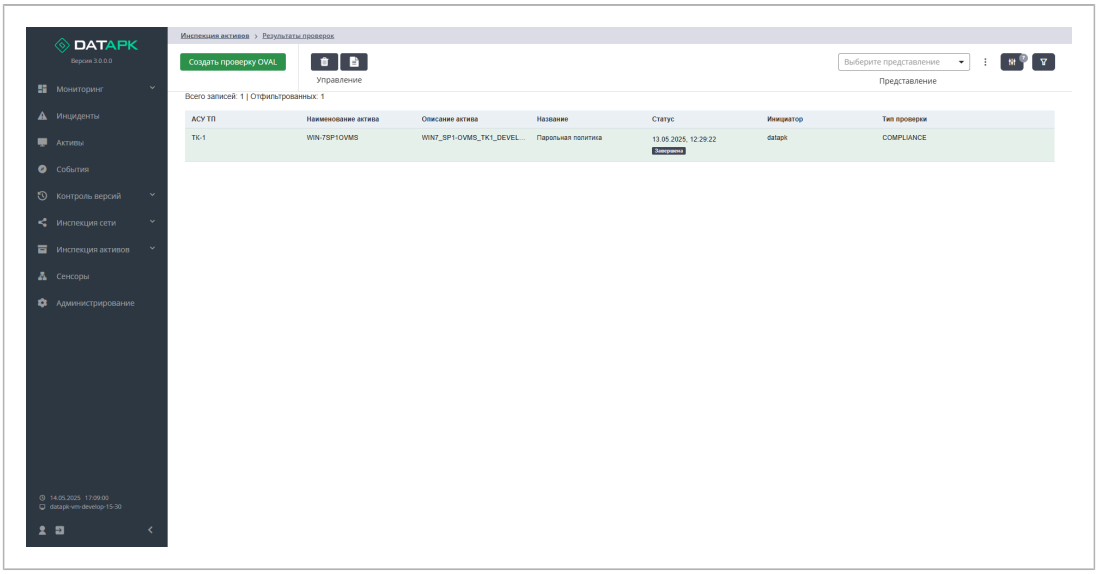


Рис. 266. Страница «Результаты проверок»

2. Нажмите кнопку **Создать проверку OVAL**. В открывшемся окне **Создание проверки OVAL-определений** настройте следующие параметры:
    а. группу OVAL-определений;
    б. наименование проверки;
    в. описание цели выполнения проверки;
    г. статус проверки;
    д. активы, к которым был настроен доступ.

> Внимание:
>
> Если поля **Цель проверки**, **Статус проверки** и **Наименование оставить** неизменными, то они будут заполнены автоматически. Поле **OVAL -определения** недоступно для редактирования и заполняется автоматически после выбора группы OVAL-определений.

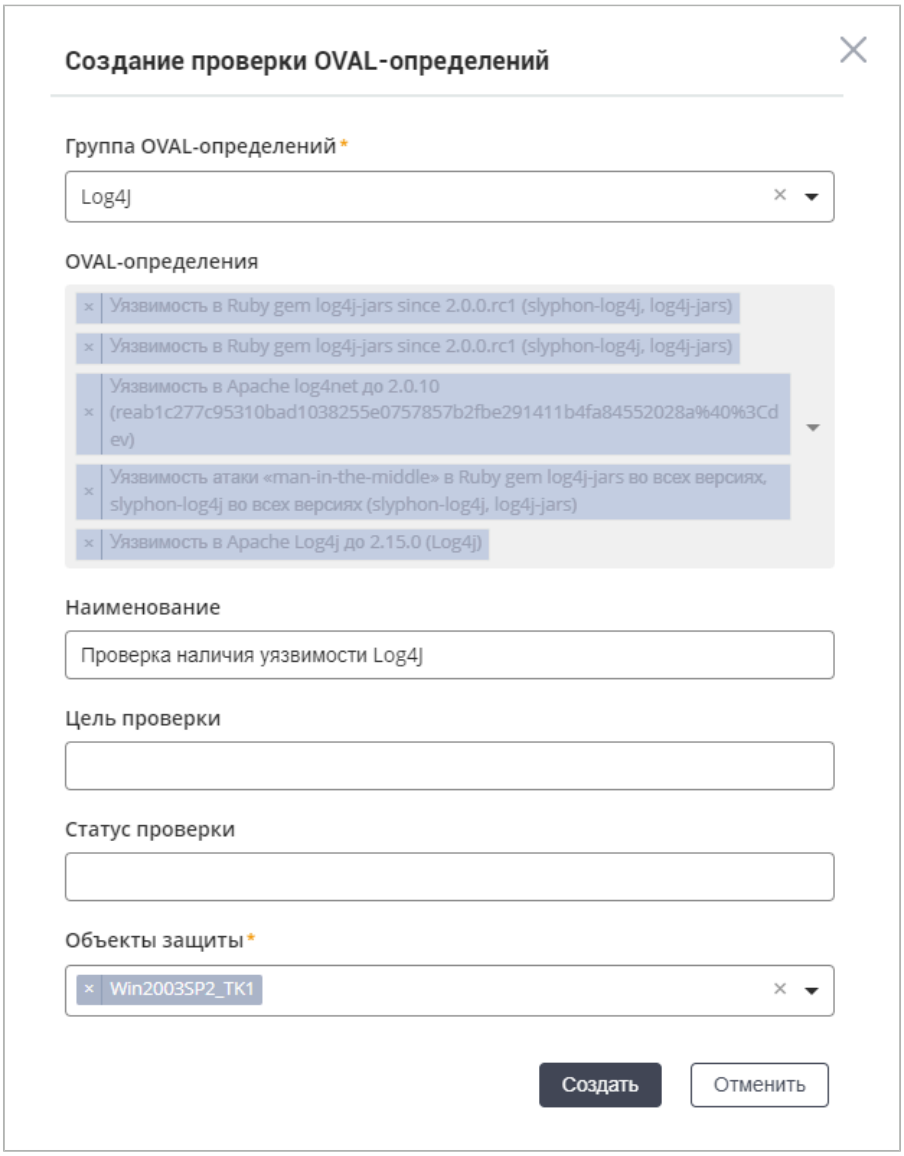


Рис. 267. Окно «Создание проверки OVAL-определений»

3. Нажмите кнопку **Создать** для подтверждения изменений.
   - **Результат шага:** выполнение проверки запустится автоматически.
4. Обновите страницу **Результаты проверок** для получения результата проверки.
   - **Результат шага:** на странице отобразятся результаты проверки с цветовой индикацией. Подробнее см. раздел «Просмотр и выгрузка результатов проверки актива на соответствие требованиям информационной безопасности».

14.2.4. Просмотр и выгрузка результатов проверки актива на соответствие требованиям информационной безопасности

Для просмотра результатов проверок на соответствие требованиям ИБ в веб-интерфейсе Комплекса:

1. Перейдите на страницу **Инспекция активов → Результаты проверок**.
2. Воспользуйтесь фильтрами по кнопке для получения необходимой выборки. При необходимости настройте отображение столбцов на странице. Подробнее см. раздел «Элементы управления таблицами».

Если проверка выполнена успешно и для актива не было обнаружено несоответствие по любому из критериев оценки соответствия (тип проверки: `COMPLIANCE`) либо ни одна из уязвимостей не была обнаружена (тип проверки: `VULNERABILITY`), в таблице результатов в строке **Статус** появится надпись `Завершена`, и строка таблицы будет выделена зеленым цветом.

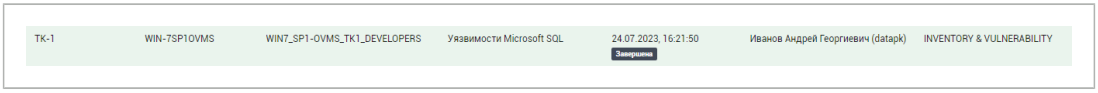


Рис. 268. Результат успешной проверки на соответствие требованиям ИБ в случае выполнения всех критериев оценки

Если проверка выполнена, но для актива обнаружено несоответствие хотя бы по одному из критериев оценки (тип проверки: `COMPLIANCE`) либо была обнаружена хотя бы одна из уязвимостей (тип проверки: `VULNERABILITY`), в таблице результатов в строке **Статус** появится статус: `Завершена`, а строка таблицы будет выделена красным цветом.

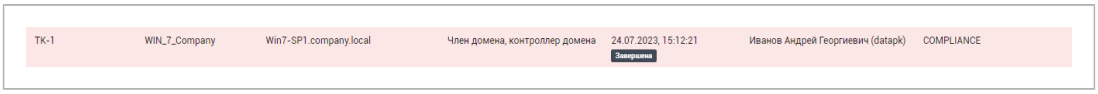


Рис. 269. Результат успешной проверки на соответствие требованиям ИБ в случае невыполнения критериев оценки

Если проверка не выполнена, в таблице результатов в столбце **Статус** появится статус: `Ошибка` с описанием ошибки.

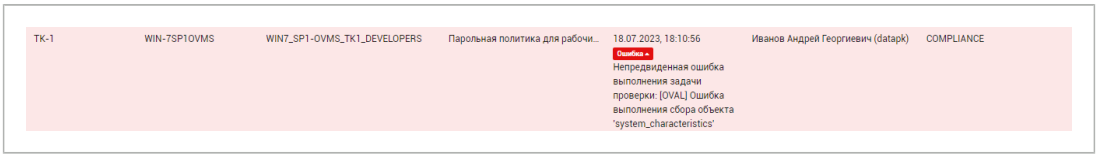


Рис. 270. Результат неуспешной проверки на соответствие требованиям ИБ

Результаты проверок будут выделены желтым цветом, если в случае проверок типа `COMPLIANCE` и `VULNERABILITY` хотя бы один критерий имеет результат, отличный от `true` и `false` (например, в случае ошибки или невозможности получить данные с актива).

Результаты проверок типа `INVENTORY` (проверка наличия установленного ПО и версий ПО) и `MISCELLANEOUS` (иные виды проверок) не выделяются цветом.

3. Нажмите кнопку ☰ (**Просмотреть результаты**) в строке с успешно выполненной проверкой на соответствие требованиям ИБ.

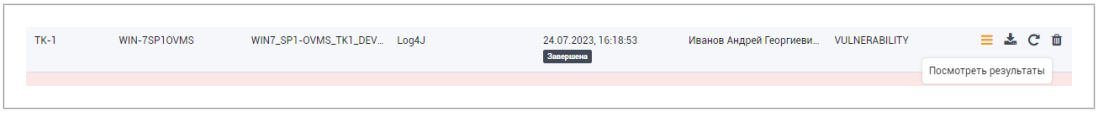


Рис. 271. Кнопка «Посмотреть результаты» в строке с проверкой на соответствие требованиям ИБ

> ⚠ Внимание:
>
> На странице **Результаты проверки** будут приведены результаты по каждому из критериев соответствия. Для критериев наличия уязвимости (с классом `VULNERABILITY`) в колонке **Меры по исправлению уязвимостей** приводятся рекомендации по устранению как для обнаруженных, так и не обнаруженных уязвимостей.

Рис. 272. Результаты успешной проверки на соответствие требованиям ИБ

4. Для выгрузки отчета по результатам проверок:

> Подсказка:
>
> Подробнее см. раздел «Выгрузка отчетов».

   а. Воспользуйтесь фильтрами по кнопке для получения необходимой выборки.

   б. В верхней части страницы нажмите кнопку (**Создать отчет**).

   в. В окне **Создание отчета** выберите формат файла (`html` или `xlsx`).

   г. Нажмите кнопку **Создать**.

   д. В открывшемся окне **Сохранение** выберите путь для сохранения файла.

   ▸ **Результат шага:** файл отчета `oval_assessments_[дата_и_время_в_формате_ДД.ММ.ГГГ_ЧЧ.ММ.СС]` выбранного формата будет загружен.

5. Для экспорта файла с результатами успешной проверки на соответствие требованиям ИБ:

   а. Нажмите кнопку (**Сохранить результаты в файл**) в строке с успешно выполненной проверкой на соответствие требованиям ИБ.

   б. В открывшемся окне **Сохранение результатов** выберите выберите формат файла (`html`, `xlsx` или `xml`).

   в. В открывшемся окне **Сохранение** выберите путь для сохранения файла.

   ▸ **Результат шага:** файл с результатом проверки `oval_assessment_results_[дата_и_время]` выбранного формата будет загружен.

14.2.5. Повторный запуск OVAL-проверки на соответствие требованиям ИБ

Для повторного запуска ранее выполненной проверки OVAL на соответствие требованиям ИБ (успешной или неуспешной):

1. Перейдите на страницу **Инспекция активов → Результаты проверок**.
2. Нажмите кнопку (**Перезапустить проверку**) в строке с проверкой OVAL, которую необходимо выполнить повторно.

> Подсказка:
>
> При необходимости остановки проверки нажать ■ (**Отменить проверку**) в строке с проверкой в статусе Выполняется.

3. Обновите страницу **Результаты проверок** для получения результата проверки.

14.2.6. Удаление OVAL-проверок актива на соответствие требованиям информационной безопасности

Если данных слишком много или они уже не нужны, их можно удалить.

Для удаления проверки:

1. Перейдите на страницу **Инспекция активов → Результаты проверок**.
2. Если необходимо удалить одну проверку, нажмите кнопку 🗑 (**Удалить**) в строке напротив нее.
3. Если необходимо удалить несколько проверок:
   a. отфильтруйте содержимое страницы так, чтобы отображались только удаляемые проверки;
   б. нажмите кнопку 🗑 (**Удалить проверки**).
4. Во всплывающем окне введите обоснование удаления.

> Внимание:
>
> Текст обоснования должен содержать минимум три символа. Без обоснования удалить проверку невозможно.

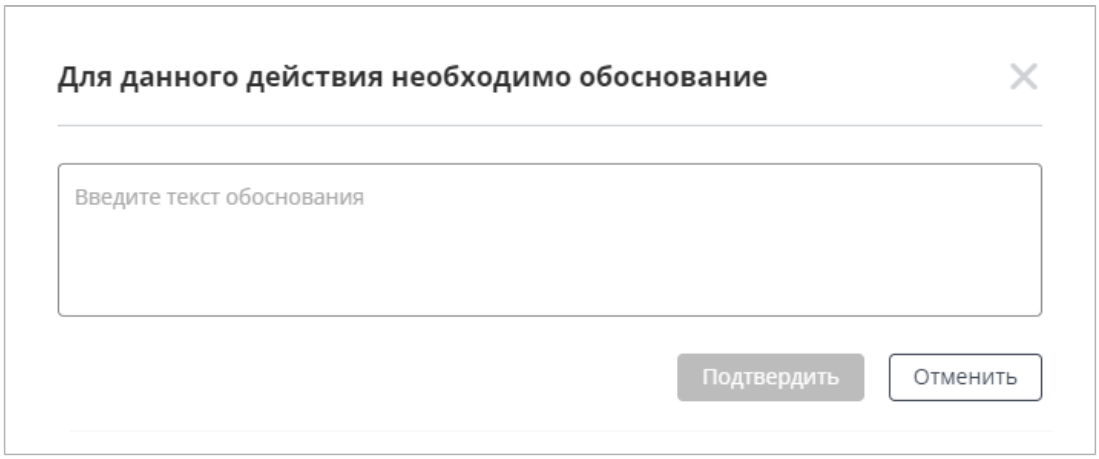


Рис. 273. Окно «Обоснование удаления проверки»

5. Нажмите **Подтвердить**.

▸ **Результат шага:** после удаления проверки будет зафиксировано соответствующее событие, в котором отображено обоснование удаления.

15. Анализ промышленного сетевого трафика

В этом разделе:

1. **Просмотр карты сети**
2. **Настройка представлений на карте**
3. **Управление сетевыми соединениями**
4. **Правила сессий**
5. **Правила контроля тегов**
6. **Контроль критичных функций технологического процесса**
7. **Служба обнаружения вторжений**

В Комплексе для отслеживания сетевых взаимодействий активов в контролируемой сети предусмотрены следующие возможности:

- просмотр активных и завершенных сетевых соединений (сессий), а также просмотр подробной информации об обнаруженных соединениях — доступно на вкладке **Сессии** страницы **Сетевые соединения**;
- просмотр информации о трафике, зафиксированном в рамках сессий, и сохранение трафика в файлы формата `pcap` — доступно на вкладке **Пакеты** страницы **Сетевые соединения**;
- анализ и сохранение файлов, передаваемых в рамках обнаруженных сессий — доступно на вкладке **Файлы** страницы **Сетевые соединения**;
- просмотр активов и соединений на странице **Карта сети**;
- просмотр событий и потенциальных инцидентов ИБ, зафиксированных по результатам анализа сетевой активности — доступно на страницах **События** и **Инциденты**;
- просмотр событий, генерируемых службой обнаружения вторжений — доступно на странице **События**.

Карта сети

На странице **Карта сети** отображается карта контролируемой сети Комплекса. На карте отображаются добавленные узлы, элементы глобальной и локальной сетей и соединения между ними. Для управления отображением используются представления. Подробнее см. в разделе «Настройка представлений на карте».

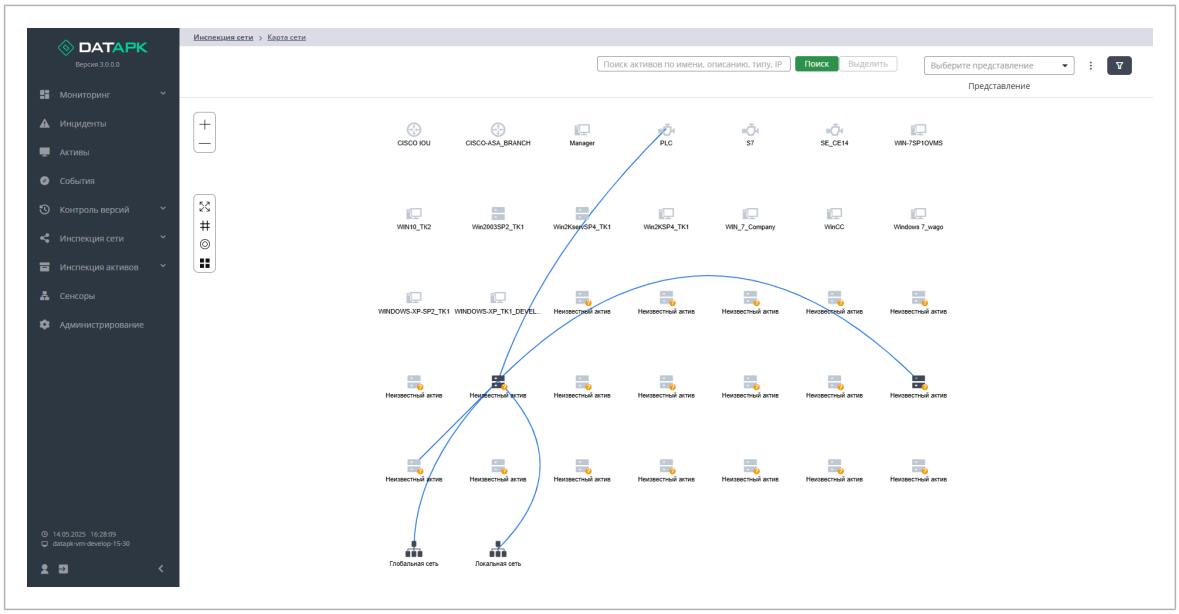


Рис. 274. Страница «Карта сети»

Сетевые соединения, пакеты, протоколы

Список обнаруживаемых сессий представлен в виде таблицы на вкладке **Сессии** страницы **Инспекция сети** → **Сетевые соединения**.

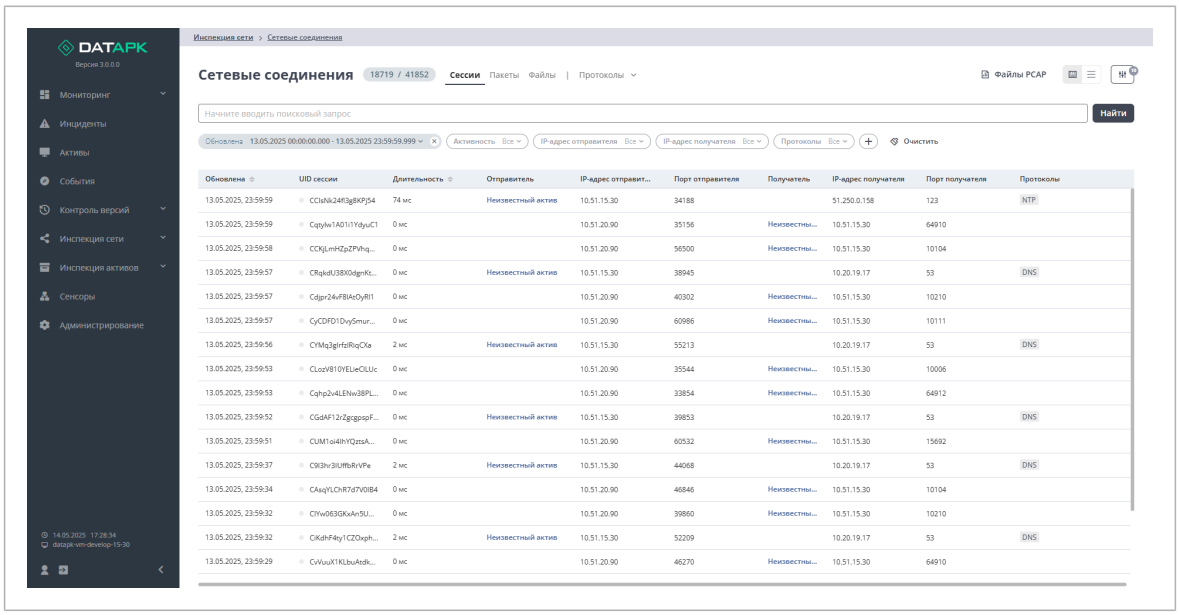


Рис. 275. Вкладка «Сессии» на странице «Сетевые соединения»

Для просмотра пакетов по всем протоколам отдельной сессии нажмите на ссылку **Перейти к пакетам** в карточке сессии.

Подробная информация о пакетах доступна на вкладке **Пакеты** по нажатию на строку с интересующей записью.

Записи о пакетах, для которых доступен глубокий анализ, также отображаются на отдельных вкладках, входящих в группу вкладок **Протоколы** на странице **Сетевые соединения**.

При обнаружении новой сессии необходимо подтверждать, является ли это разрешенной активностью в контролируемой сети. Новые неподтвержденные сессии имеют статус `Не разрешена` в столбце **Статус**.

В интерфейсе Комплекса возможно подтверждение сессий в ручном и автоматическом режимах.

Обнаружение вторжений

На странице **Правила обнаружения** отображаются правила, при помощи которых могут быть выявлены угрозы для локальной сети. Можно запускать, редактировать и удалять созданные правила.

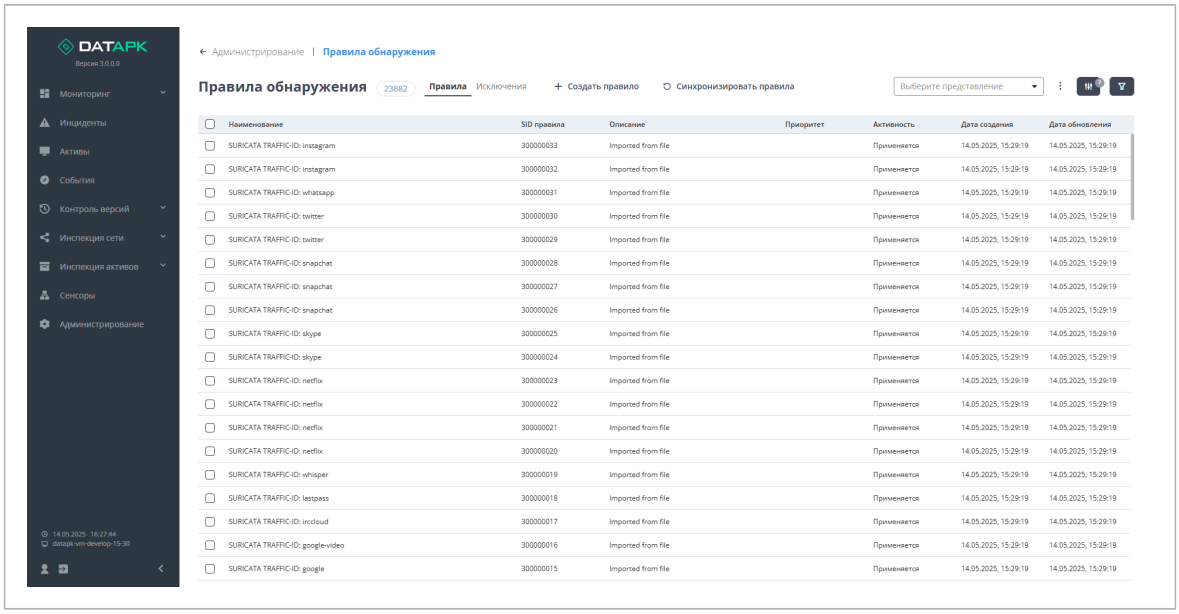


Рис. 276. Страница «Правила обнаружения»

15.1. Просмотр карты сети

Карта сети — модель, описывающая состав вычислительной сети предприятия: узлы и соединения между узлами на сетевом и канальном уровнях.

Узлы и соединения, обнаруженные в анализируемом трафике, добавляются на карту автоматически, после чего пользователь может менять их состав и отображение при помощи фильтров, кнопок настройки расположения и группировки.

Узел — это элемент сети предприятия, взаимодействующий с другими элементами сети.

На картах могут быть отображены узлы контролируемой сети (активы) и по одному элементу локальной и глобальной сетей.

> Внимание:
>
> Корректная работа карты сети возможна при выборе не более 500 активов для одновременного отображения. Отображение соединений для этого числа активов на карте также может занимать продолжительное время.

Расположение и группировка активов

Для регулировки отображения активов на карте воспользуйтесь следующими кнопками:

- (**Показать все узлы**) для сброса масштабирования;
- (**Расположить на сетке**) для расположения узлов на прямоугольной плоскости ровными рядами;
- (**Расположить по кругу**) для расположения узлов на круге;
- (**Сгруппировать по количеству сессий**) для группировки узлов в зависимости от соединений, относящихся к активам.

Для масштабирования карты воспользуйтесь кнопками в левом верхнем углу страницы.

Фильтрация активов и сессий

Для просмотра интересующих узлов и соединений воспользуйтесь фильтрами в правой части страницы по кнопке . Можно выбрать IP-адреса, типы активов, MAC-адреса отправителей и получателей, сеть отправителей и получателей, последние протоколы.

> Внимание:
>
> В поля IP-адресов допускается копирование из других источников списков IP-адресов, их диапазонов или подсетей. Элементы в исходном списке должны разделяться с помощью: **,**, **;**, **Tab**, **Enter**, **Space**. Подсети задаются в формате CIDR.

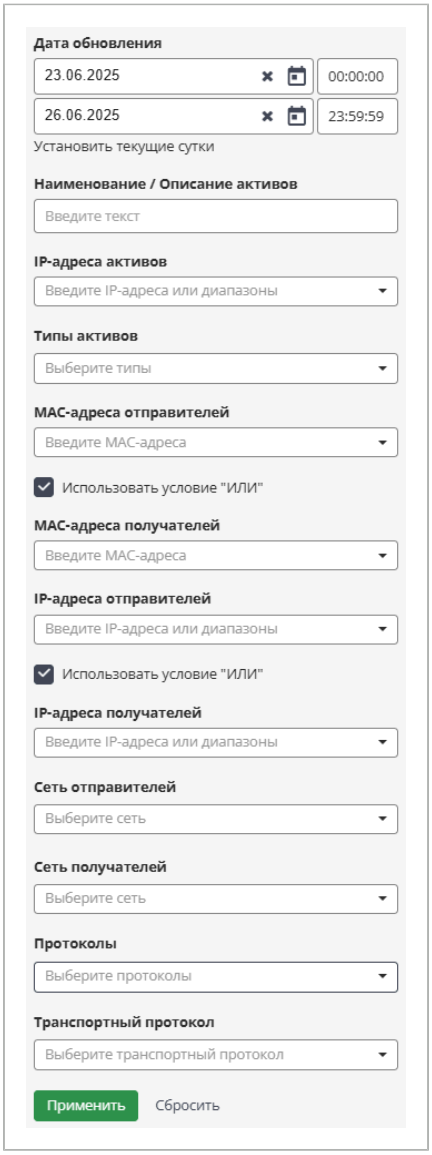


Рис. 277. Фильтры на странице «Карта сети»

Поиск на карте

Одним из способов выделения активов и сетевых соединений является поиск непосредственно на карте. Поиск расположен в верхней части страницы.

Для поиска активов или сетевых соединений введите IP-адрес, имя, описание или тип актива.

После того как актив найден, вы можете нажать **Выделить**, чтобы соединения, относящиеся к активу, были выделены и появились на соответствующей вкладке в правой части страницы.

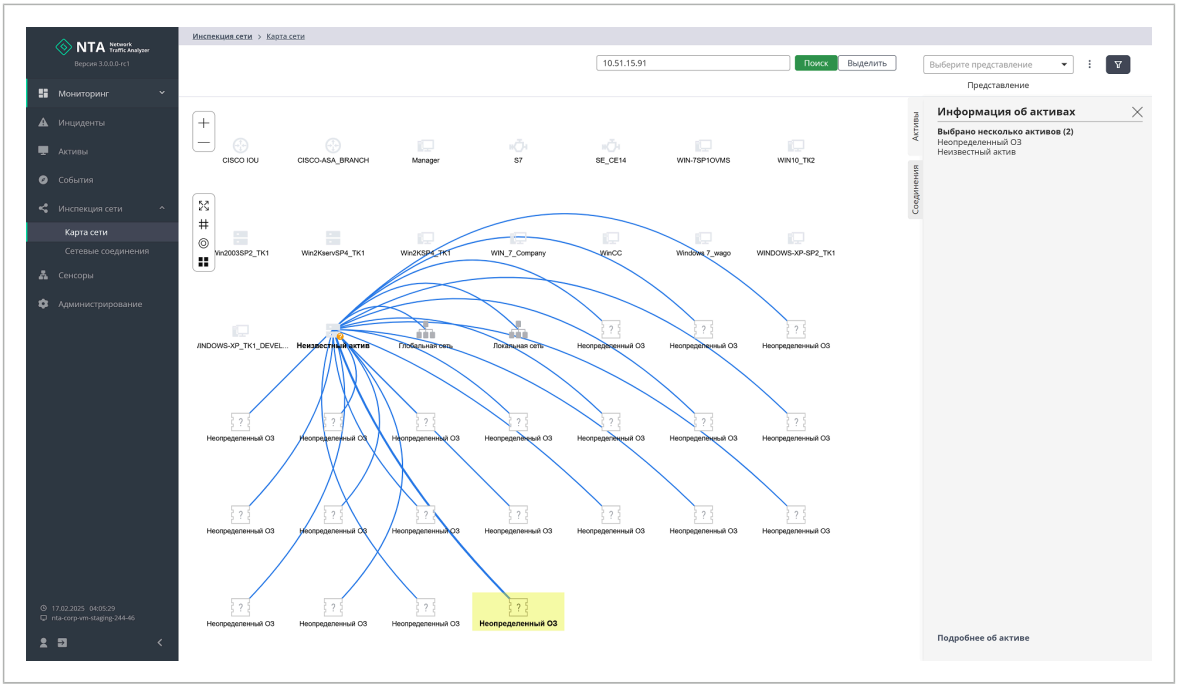


Рис. 278. Результат работы поиска и выделения

Выделение активов и сетевых соединений

На карте сети доступно выделение нескольких сетевых соединений и групп.

Для выделения активов или соединений по одному нажмите клавишу **Ctrl** и удерживайте ее во время выделения активов и (или) соединений. При таком типе выделения возможно как совместное, так и раздельное выделение активов с соединениями.

Для массового выделения активов нажмите клавишу **Shift** и удерживайте ее во время выделения активов.

Для снятия выделения с отдельных активов или соединений нажмите клавишу **Ctrl** и удерживайте ее во время выделения выбранных активов или соединений. Для снятия выделения со всех активов и соединений нажмите на пустую область на карте.

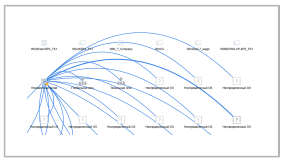


Рис. 279. Результат выделения при помощи Ctrl

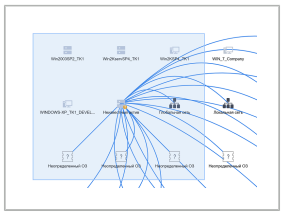


Рис. 280. Выделение при помощи Shift

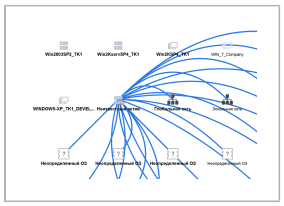


Рис. 281. Результат выделения при помощи Shift

Работа со вкладками

При выборе узлов и соединений в правой части страницы рядом с фильтрами появляются вкладки **Активы** и **Соединения**.

На вкладке **Активы** располагается общая информация об активе: наименование, тип, даты создания и появления, а также сетевые атрибуты и набор меток, присвоенных активу. В нижней части вкладки расположены кнопки:

- **Подробнее об активе** — при нажатии открывается страница актива, либо страница **Активы** с выбранными активами;
- **Подробнее о соединениях** — при нажатии открывается вкладка **Сессии** с сессиями выбранного соединения.

На вкладке **Соединения** располагается основная информация о выделенных соединениях либо о сессиях, относящихся к выделенным активам. При выделении актива, у которого есть сессии только с одним другим активом, на вкладке появится кнопка **Подробнее о соединениях**, при нажатии на которую открывается вкладка **Сессии** с сессиями выбранного соединения.

Рис. 282. Вкладка «Активы»

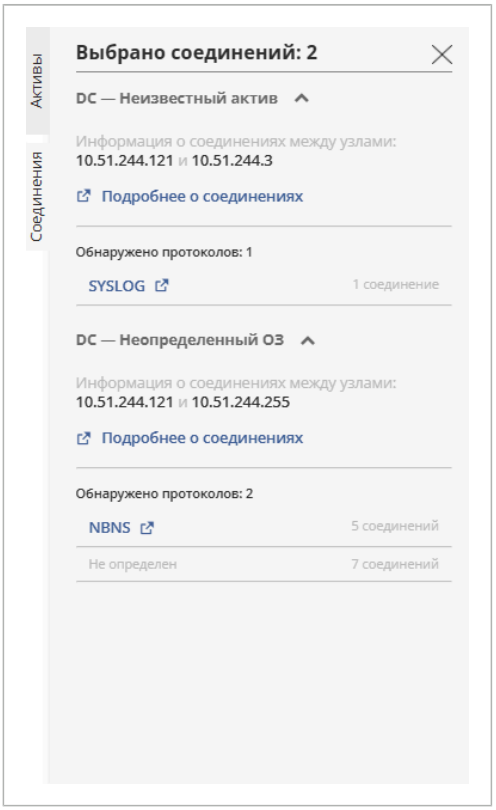


Рис. 283. Вкладка «Соединения»

Неопределенные активы

В результате удаления активов на карте могут отображаться неопределенные активы. Это узлы, для которых есть сессии, но отсутствуют сами активы. При необходимости создайте активы заново.

15.2. Настройка представлений на карте

На странице **Карта сети** вы можете создавать, редактировать и удалять представления.

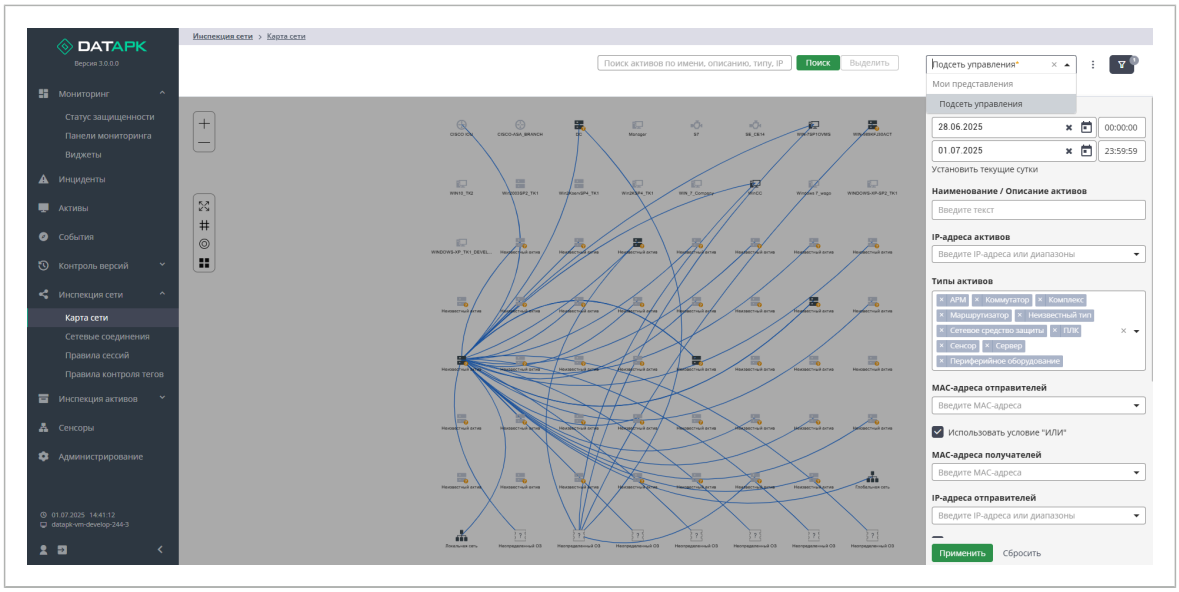


Рис. 284. Представления на странице Карта сети

К сохранению в составе представлений доступны:

- фильтры;
- группировка узлов по количеству соединений (**Сгруппировать по количеству сессий**);
- расположение элементов на карте (**Расположить на сетке**, **Расположить по кругу**).

В составе представлений не учитывается масштабирование, поиск и выделение по его результатам.

В качестве примера приводится изменение параметров фильтрации и отображения, последующее сохранение и изменение представления. Для работы с представлением на карте:

1. Измените необходимые параметры фильтров.

   Пример

   Например, выберите типы активов `APM`, `Маршрутизатор`, `Периферийное оборудование`, `ПЛК`, `Сервер`, `Сетевое средство защиты`, `Неизвестный тип`.

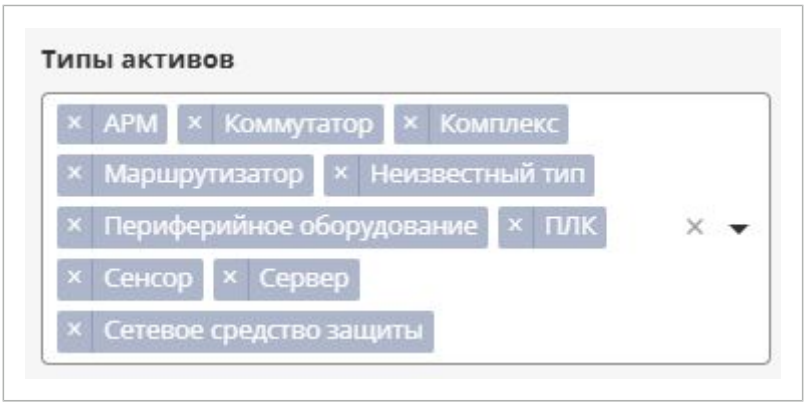


Рис. 285. Выбор типа отображаемых на карте активов

2. Измените параметры отображения узлов на карте.

   Пример

   Например, выберите группировку по количеству соединений (**Сгруппировать по количеству сессий**).

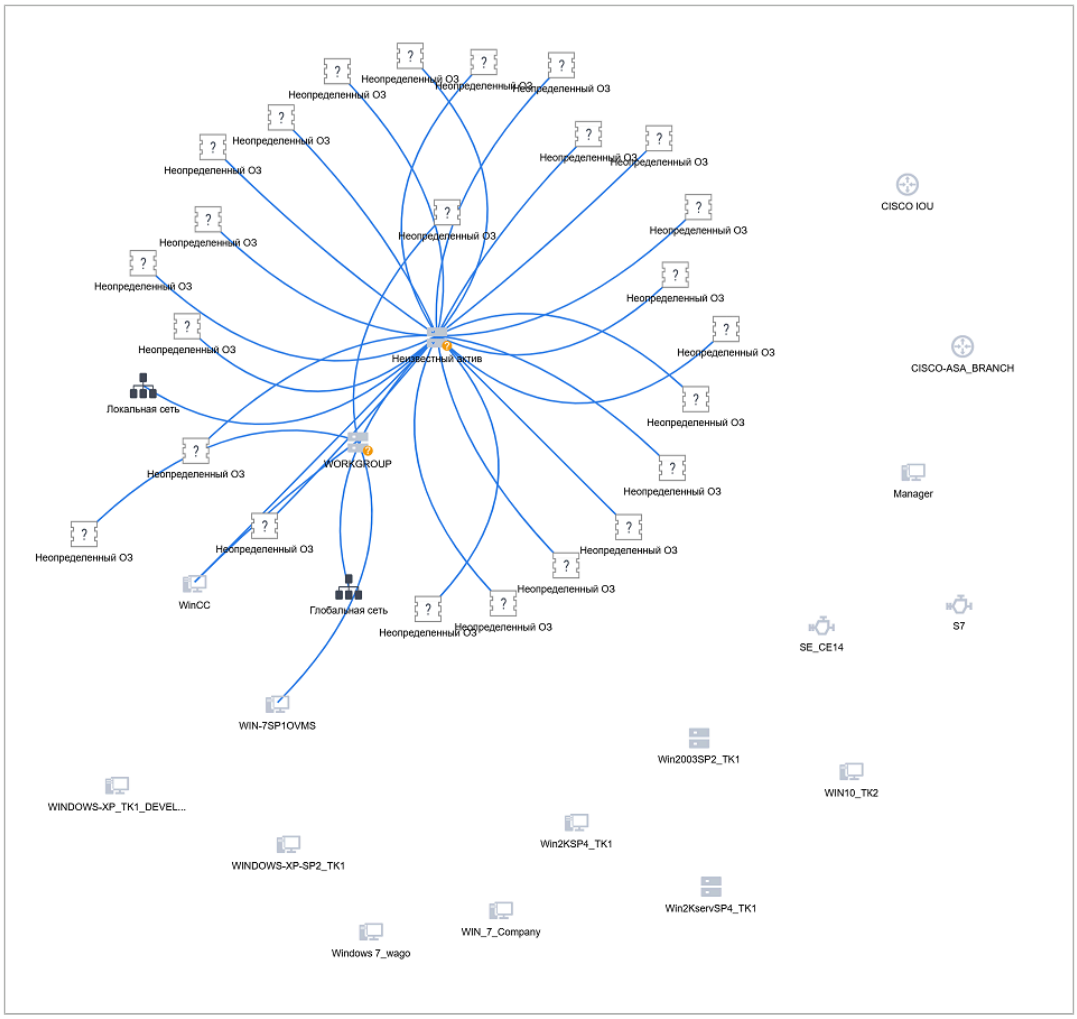


Рис. 286. Карта в результате фильтрации и изменения параметров отображения

3. В верхней правой части страницы нажмите ⋮;
4. В выпадающем меню выберите опцию **Сохранить как**;
   - **Результат шага:** появится окно сохранения представления.
5. В окне сохранения представления:
   - введите наименование;

     > Внимание:
     >
     > Имя не должно совпадать с уже существующим.

   - выберите, будет ли представление доступно для использования другими пользователями.

Пример

Например, введите название `Подсеть управления` и выберите тип использования `Только для меня`.

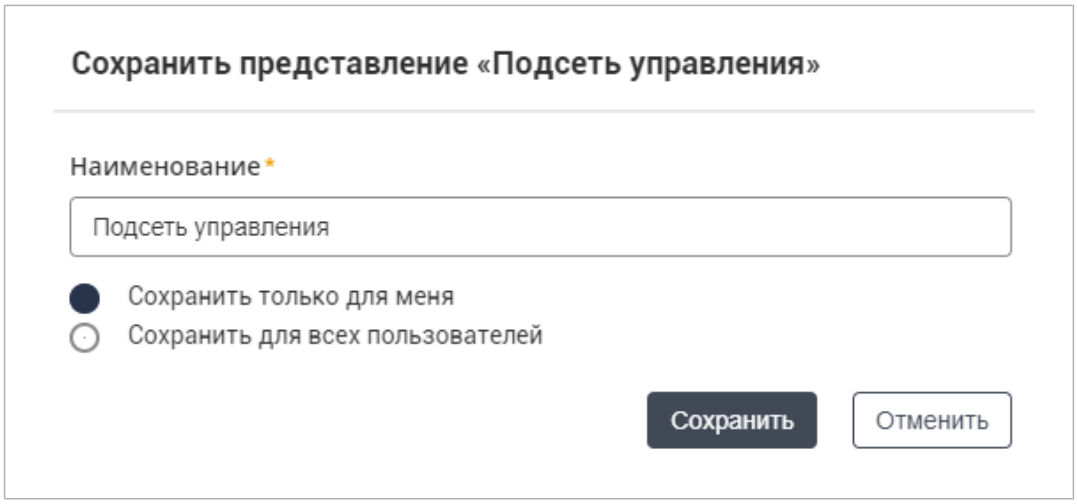


Рис. 287. Окно сохранения представления

6. Нажмите **Сохранить**.
   - **Результат шага:** новое представление станет доступно для выбора.
7. В верхней части панели фильтров выберите из выпадающего списка только что созданное представление.

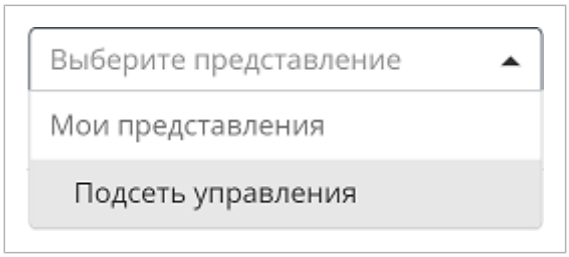


Рис. 288. Выпадающий список с доступными представлениями

8. Измените параметры фильтрации и отображение узлов на карте.

   Пример

   Например, выберите соединения за один месяц и расположение узлов по кругу.

   - **Результат шага:** возле названия представления в верхней части панели фильтров появится оранжевый символ `*`. Это означает, что есть несохраненные изменения представления.
9. Нажмите ⋮ в верхней правой части страницы.
10. В появившемся меню выберите **Редактировать**.

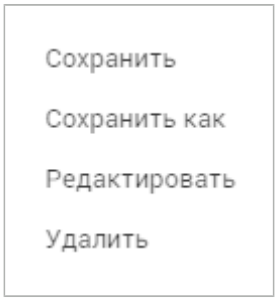


Рис. 289. Меню управления представлением

11. В окне сохранения представления введите новое имя представления.

    Пример

    Например, `Соединения за июль 2022`.

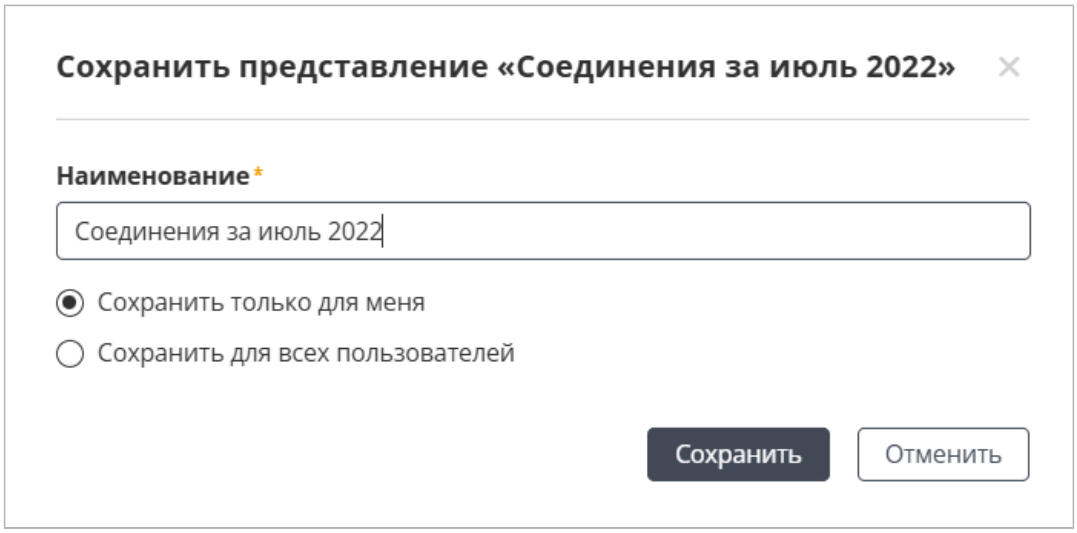


Рис. 290. Окно редактирования представления

12. Нажмите **Сохранить**.
    - **Результат шага:** сохраненное представление изменит название.

См. также

Представления

15.3. Управление сетевыми соединениями

В этом разделе:

- Просмотр сессий и пакетов
- Поиск по списку сессий
- Фильтрация списка сессий
- Экспорт копии сетевого трафика
- Экспорт файлов, обнаруженных в сетевом трафике

15.3.1. Просмотр сессий и пакетов

В этом подразделе:

- Просмотр вкладки «Сессии»
- Просмотр информации о пакетах сессии
- Просмотр информации о пакетах в группе вкладок «Протоколы»

Просмотр вкладки «Сессии»

Список обнаруживаемых сессий представлен в виде таблицы на вкладке **Сессии** страницы **Инспекция сети → Сетевые соединения**.

Для навигации по списку сессий используется область фильтров над таблицей. По умолчанию отображаются сессии, обнаруженные за текущие сутки.

> Подсказка:
>
> Для обновления данных на странице сбросьте вручную фильтр **Обновлена**.

Для настройки отображения столбцов используется кнопка в верхнем правом углу. Сессии по умолчанию или вручную можно сортировать по столбцу **Обновлена**.

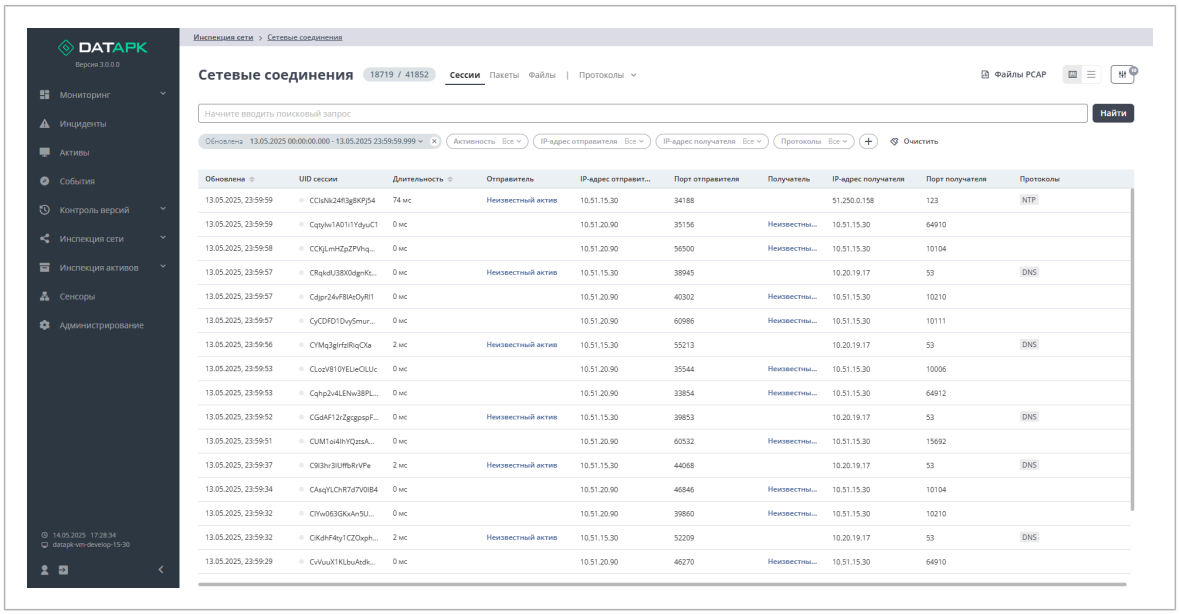


Рис. 291. Вкладка «Сессии» на странице «Сетевые соединения»

Модуль «Анализ промышленного сетевого трафика» определяет активность сессий в текущий момент. В столбце **UID сессии** активные сессии имеют иконку зеленого цвета, неактивные — серую. Неактивность сессии определяется по следующим признакам в пакетах протоколов транспортного и сетевого уровней:

- по стандартным флагам закрытия сессии, передаваемых в пакетах TCP, UDP и ICMP:
- по таймауту — при отсутствии трафика в рамках сессии в течение времени, определенного по умолчанию в модуле «Анализ промышленного сетевого трафика». Определены следующие таймауты в зависимости от протокола:
    - TCP — 5 минут;
    - UDP — 1 минута;
    - ICMP — 1 минута.

Подробнее о признаках неактивности см. справочный раздел «Признаки неактивности сессий».

Индивидуальным признаком сессии является поле **UID сессии** — идентификатор сессии, который используется также на других страницах модуля «Анализ промышленного сетевого трафика» для поиска информации, связанной с сессией.

Модуль «Анализ промышленного сетевого трафика» может разбирать протоколы на четырех уровнях:

- индикации;
- анализа событий ИБ;
- подробного анализа;
- извлечения файлов из трафика.

Модуль «Анализ промышленного сетевого трафика» разбирает большинство протоколов в пакетах на уровне индикации — это значит, что модуль отображает наименование протокола без дополнительной информации о содержании полей этого протокола. Протоколы, разбираемые на уровне индикации, можно увидеть только в столбце **Протоколы** вкладки **Сессии** и в поле **Протоколы** карточки сессии.

Для некоторых протоколов прикладного уровня модуль «Анализ промышленного сетевого трафика» также может выполнять подробный анализ и детализировать информацию о содержании полей. Список таких протоколов представлен в группе вкладок **Протоколы** на странице **Сетевые соединения**:

- **HTTP**
- **DNS**
- **SMB_CMD**
- **DCE_RPC**
- **NTLM**
- **SSH**
- **SSL**
- **Kerberos**
- **Modbus**
- **RDP**
- **SMTP**
- **OPC UA**
- **DELTAV**

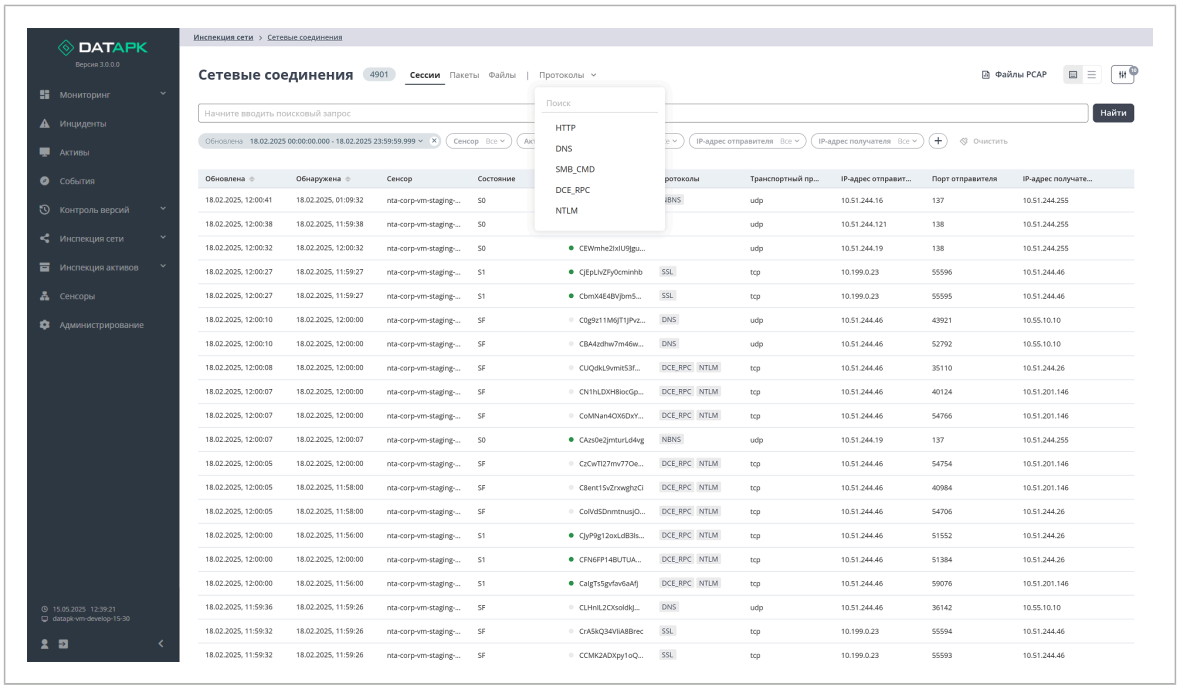


Рис. 292. Группа вкладок «Протоколы» на странице «Сетевые соединения»

При выборе сессии на вкладке **Сессии** открывается карточка сессии, которая содержит следующую информацию:

- Реквизиты отправителя и получателя сессии, количество переданных и полученных пакетов и байт, тип сети.
- Дата обнаружения, обновления и длительность сессии, идентификатор с расшифровкой состояния сессии. Перечень возможных состояний см. в справочном разделе «Признаки неактивности сессий»

- Информация о количестве переданных файлов в рамках сессии. Для просмотра и экспорта обнаруженных файлов см. инструкцию «Экспорт файлов, обнаруженных в сетевом трафике».
- Отдельные записи о пакетах, для которых выполнен подробный анализ. Записи о пакетах сгруппированы по протоколам, которые отображаются в поле **Протоколы**.

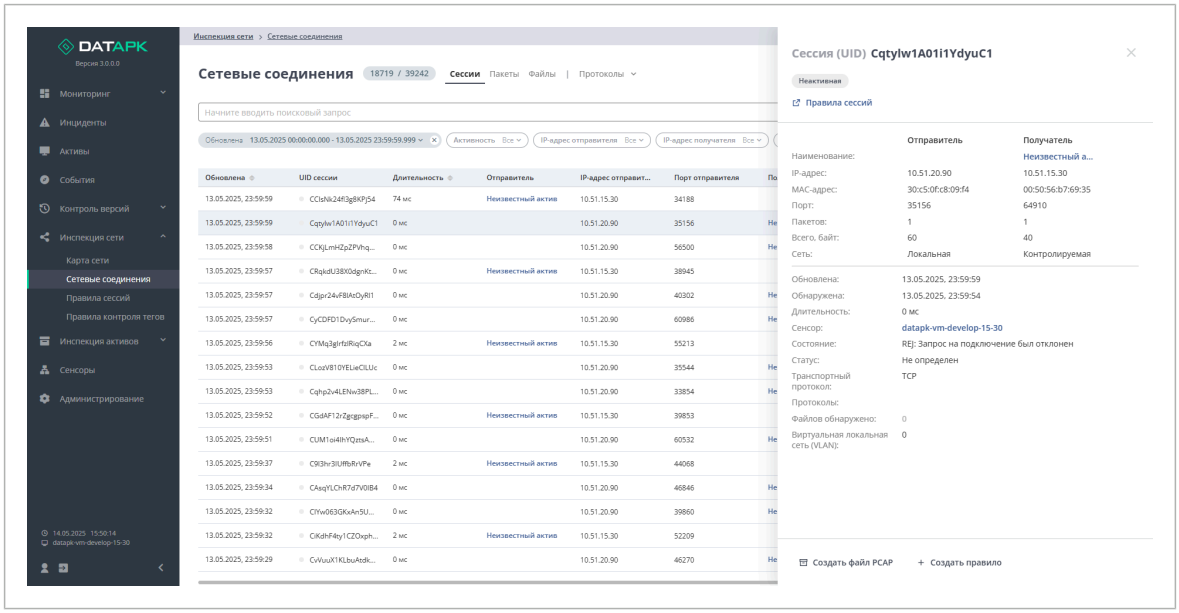


Рис. 293. Карточка сессии

> Подсказка:
>
> Описание всех сетевых протоколов, поддерживаемых модулем «Анализ промышленного сетевого трафика», вы можете найти в разделе «Поддерживаемые протоколы передачи данных».

Просмотр информации о пакетах сессии

В карточке сессии в поле **Протоколы** отображаются ссылки на отдельные записи о пакетах, сгруппированных по протоколам. При нажатии на протокол открывается вкладка **Пакеты** на странице **Сетевые соединения** с записями о пакетах.

> Прим.:
>
> Одна запись о пакетах содержит информацию о наборе пакетов, сгруппированных по протоколу и идентификатору сессии (UID).

Для просмотра пакетов по всем протоколам отдельной сессии нажмите на ссылку **Перейти к пакетам** в карточке сессии.

Подробная информация о пакетах доступна на вкладке **Пакеты** по нажатию на строку с интересующей записью.

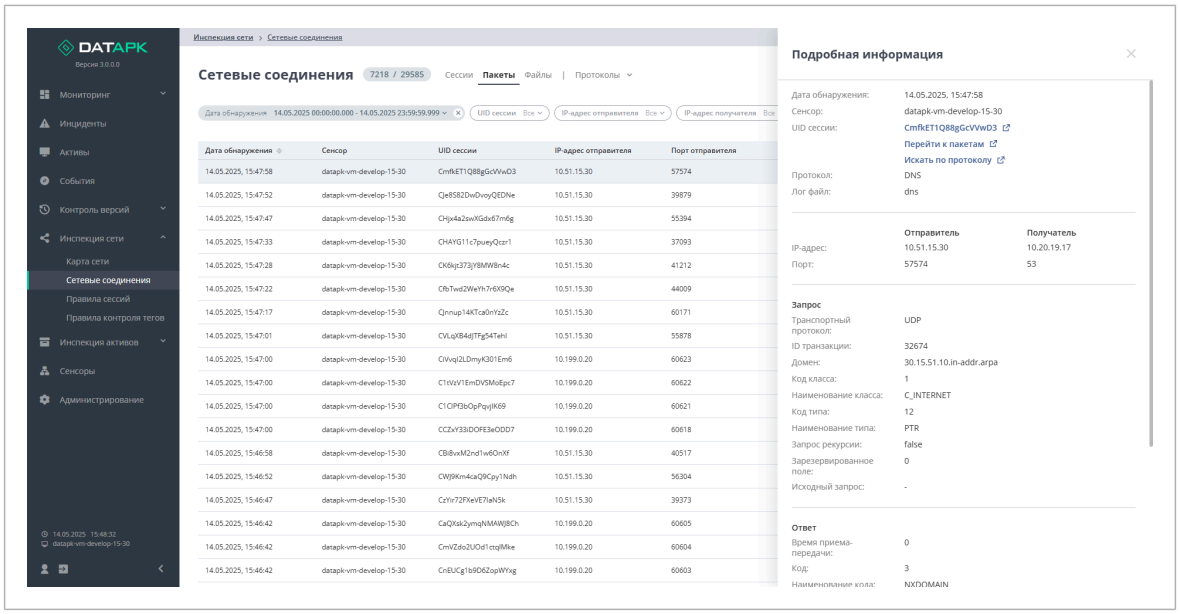


Рис. 294. Подробная информация о выбранных пакетах сессии на вкладке Пакеты

На вкладке **Пакеты** для навигации по записям используется область фильтров над таблицей. Для настройки отображения столбцов используется кнопка в верхнем правом углу.

Сенсоры модуля «Анализ промышленного сетевого трафика» по умолчанию сохраняют копию прослушиваемого трафика. По записям, отфильтрованным на вкладке **Пакеты**, возможен экспорт копии трафика в виде файла формата `.pcap`. Для подготовки и экспорта `.pcap`-файлов см. инструкцию «Экспорт копии сетевого трафика». Для управления сохранением трафика на сенсорах см. инструкцию «Первичная настройка модуля «Анализ промышленного сетевого трафика»».

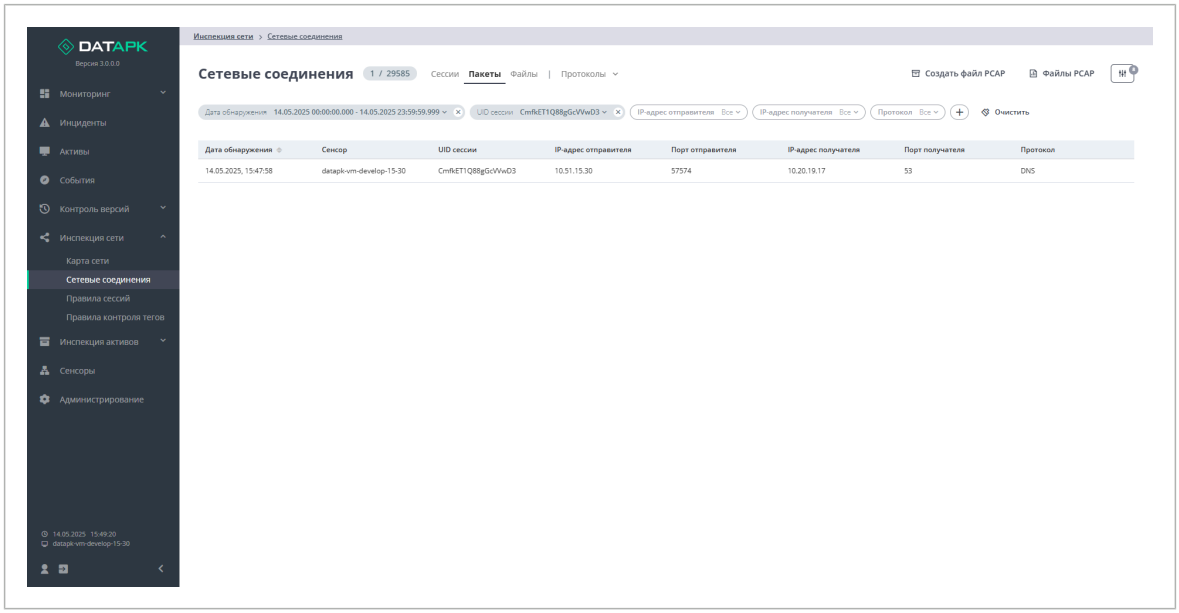


Рис. 295. Пакеты сессии на вкладке «Пакеты»

Для навигации по списку пакетов используется область фильтров над таблицей. По умолчанию отображаются пакеты, обнаруженные за текущие сутки.

Подсказка:

Для обновления данных на странице сбросьте вручную фильтр **Обновлена**.

При нажатии на запись о пакетах открывается карточка с той же информацией о пакетах, которую можно просматривать в карточке сессии.

Просмотр информации о пакетах в группе вкладок «Протоколы»

Записи о пакетах, для которых доступен глубокий анализ, также отображаются на отдельных вкладках, входящих в группу вкладок **Протоколы** на странице **Сетевые соединения**.

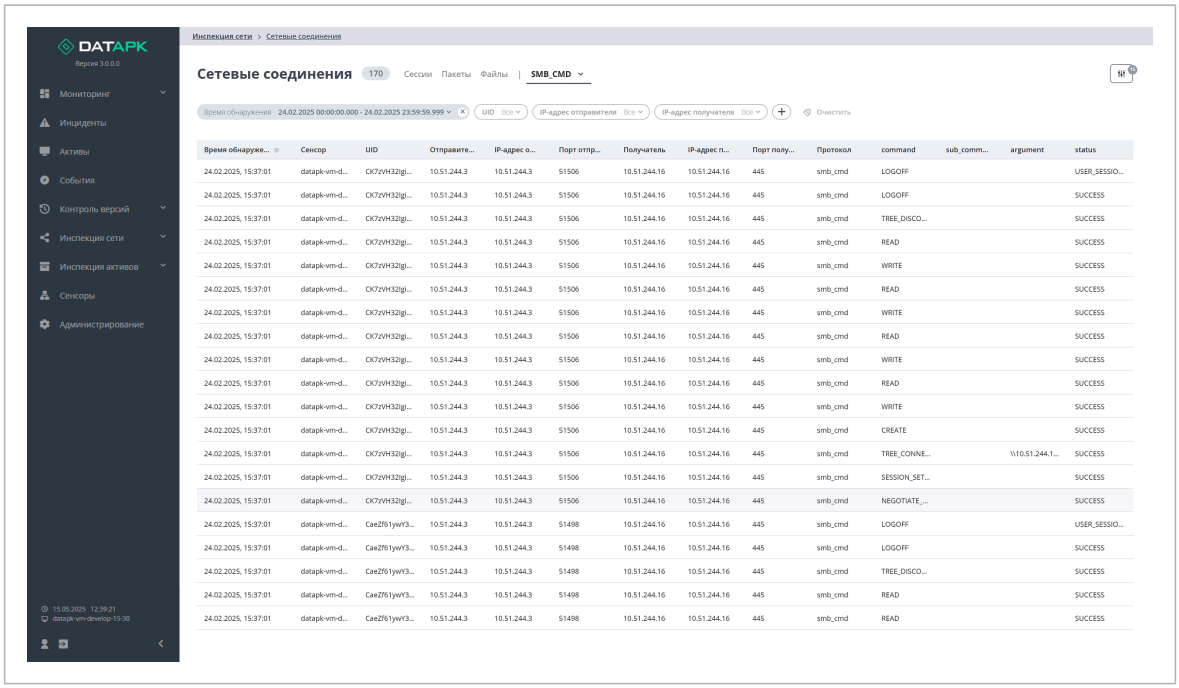


Рис. 296. Вкладка для протокола SMB_CMD на странице «Сетевые соединения»

Для навигации по списку пакетов используется область фильтров над таблицей. По умолчанию отображаются пакеты, обнаруженные за текущие сутки.

Подсказка:

Для обновления данных на странице сбросьте вручную фильтр **Обновлена**.

При нажатии на запись о пакетах открывается карточка с той же информацией о пакетах, которую можно просматривать в карточке на вкладке **Пакеты**.

15.3.2. Поиск по списку сессий

Для автоматического поиска с помощью строки поиска:

1. Установите курсор в строку поиска, расположенную вверху страницы.
   - **Результат шага:** отобразится выпадающий список с наименованиями доступных параметров сессии.

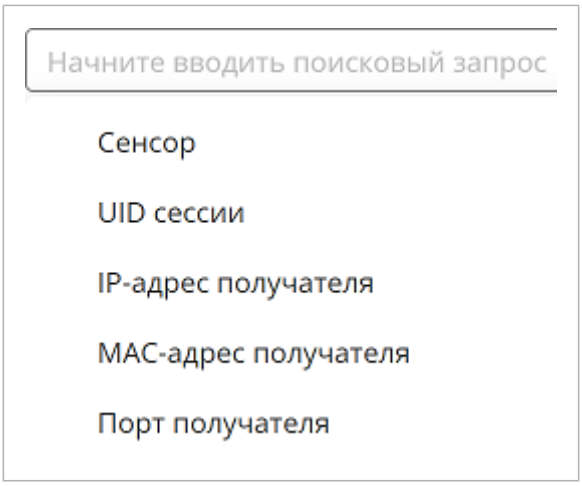


Рис. 297. Список доступных параметров сессии

2. Выберите параметр сессии из списка, либо начните вводить параметр вручную.

> Подсказка:
>
> При вводе поискового запроса в строке поиска будут появляться подсказки с доступными параметрами, условиями и значениями параметров.

3. Выберите условие параметра сессии из списка.

   Доступные условия для числовых данных:

   - `=` — равно;
   - `!=` — не равно;
   - `~~ ()` — равно одному из;
   - `!~~ ()` — не равно одному из;
   - `>` — больше;
   - `<` — меньше;
   - `>=` — больше или равно;
   - `<=` — меньше или равно.

   Доступные условия для текстовых данных:

   - `=` — равно;
   - `!=` — не равно;
   - `~~ ()` — равно одному из;
   - `!~~ ()` — не равно одному из;
   - `~` — содержит;
   - `!~` — не содержит;
   - `^` — начинается с;
   - `!^` — не начинается с.

4. Введите значение параметра.

> Подсказка:
>
> Допускается создавать сложные поисковые запросы, объединяя несколько запросов «параметр-условие-значение» с помощью логических условий `И`/`ИЛИ`. Данные условия также появляются в строке поиска в виде подсказок.

5. Нажмите кнопку Найти.
   - **Результат шага:** результаты поиска будут отображены на странице.

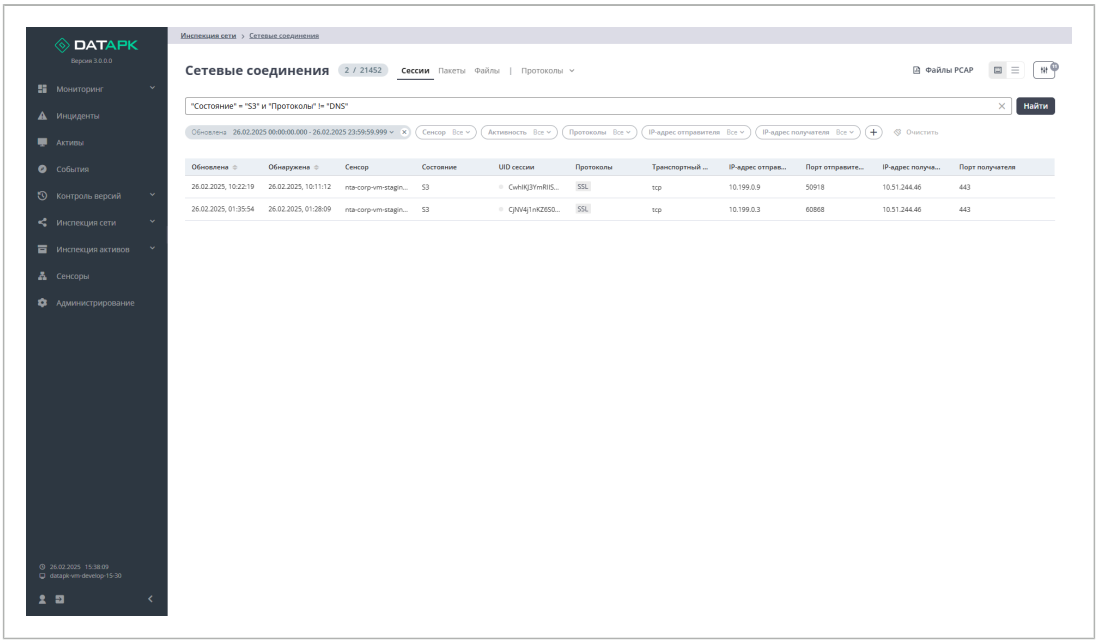


Рис. 298. Отображение результатов поиска в строке поиска на вкладке «Сессии»

15.3.3. Фильтрация списка сессий

Комплекс позволяет выполнять поиск обнаруженных сессий и фильтровать отображаемые сессии на вкладке **Сессии** страницы **Инспекция сети → Сетевые соединения**.

На панели фильтров под строкой поиска по умолчанию отображаются следующие фильтры:

- **Сенсор**. Фильтр содержит наименования сенсоров, подключенных к Комплексу. Можно выбирать несколько наименований. При применении фильтра отобразятся сессии, обнаруженные выбранными сенсорами.
- **Активность**. Фильтр содержит статусы состояния сессии. Можно выбрать одно из значений: `Активно`, `Неактивно`.
- **Протоколы**. Фильтрация выполняется по распознанному протоколу. Можно выбирать несколько значений. При применении фильтра отобразятся сессии с выбранными протоколами.
- **IP-адрес отправителя**. Фильтрация выполняется по распознанному IP-адресу отправителя сетевого пакета. Можно ввести только один адрес.
- **IP-адрес получателя**. Фильтрация выполняется по распознанному IP-адресу получателя сетевого пакета. Можно ввести только один адрес.

Также по нажатию кнопки ⊕ на панели фильтров доступно добавление и применение дополнительных фильтров:

- **Состояние**. Фильтр содержит список идентификаторов состояния сессии. Можно выбирать несколько идентификаторов. При применении фильтра отобразятся сессии с выбранными идентификаторами.
- **UID сессии**. Фильтрация выполняется по уникальному идентификатору сессии. Можно ввести только один идентификатор.

- **Транспортный протокол**. Фильтр содержит список протоколов транспортного уровня модели OSI, по которым выполнялись сетевые соединения. Можно выбирать несколько протоколов. При применении фильтра отобразятся сессии с выбранными протоколами.
- **Порт получателя**. Фильтрация выполняется по распознанным портам, к которым обращался получатель. Можно ввести только один порт.
- **Порт отправителя**. Фильтрация выполняется по распознанным портам, к которым обращался источник. Можно ввести только один порт.
- **Отправитель**. Фильтрация выполняется по наименованию актива, отправившего сетевой пакет.
- **Получатель**. Фильтрация выполняется по наименованию актива, получившего сетевой пакет.
- **Сеть отправителя**. Фильтрация выполняется по типу сети обнаруженной сессии. Можно выбрать одно из предлагаемых значений: `Контролируемая`, `Глобальная`, `Локальная`.

15.3.4. Экспорт копии сетевого трафика

На вкладке **Пакеты** страницы **Сетевые соединения** можно подготовить и экспортировать копию сетевого трафика в файл формата `.pcap`. Экспорт трафика выполняется по отфильтрованным записям.

Перед выполнением: Убедитесь, что на сенсорах включено сохранение копии трафика — подробнее см. инструкцию «Первичная настройка модуля «Анализ промышленного сетевого трафика»».

Доступен экспорт трафика не более 1 ГБ.

Для экспорта трафика из записей о пакетах:

1. Перейдите на вкладку **Пакеты** страницы **Сетевые соединения**. Откройте вкладку **Пакеты** с записями, отфильтрованными по определенной сессии. Для этого:
    a. Перейдите на вкладку **Сессии** страницы **Сетевые соединения**.
    б. Выберите сессию из списка.
    - **Результат шага:** откроется карточка сессии.

    в. В карточке сессии нажмите на ссылку **Перейти к пакетам**.
    - **Результат шага:** откроется вкладка **Пакеты** с записями о пакетах выбранной сессии (записи будут отфильтрованы по `UID сессии`).
2. На вкладке **Пакеты** нажмите кнопку (**Создать файл PCAP**) в правом верхнем углу страницы.
    - **Результат шага:** откроется окно **Фильтры создания файла PCAP** с предварительно настроенными фильтрами.

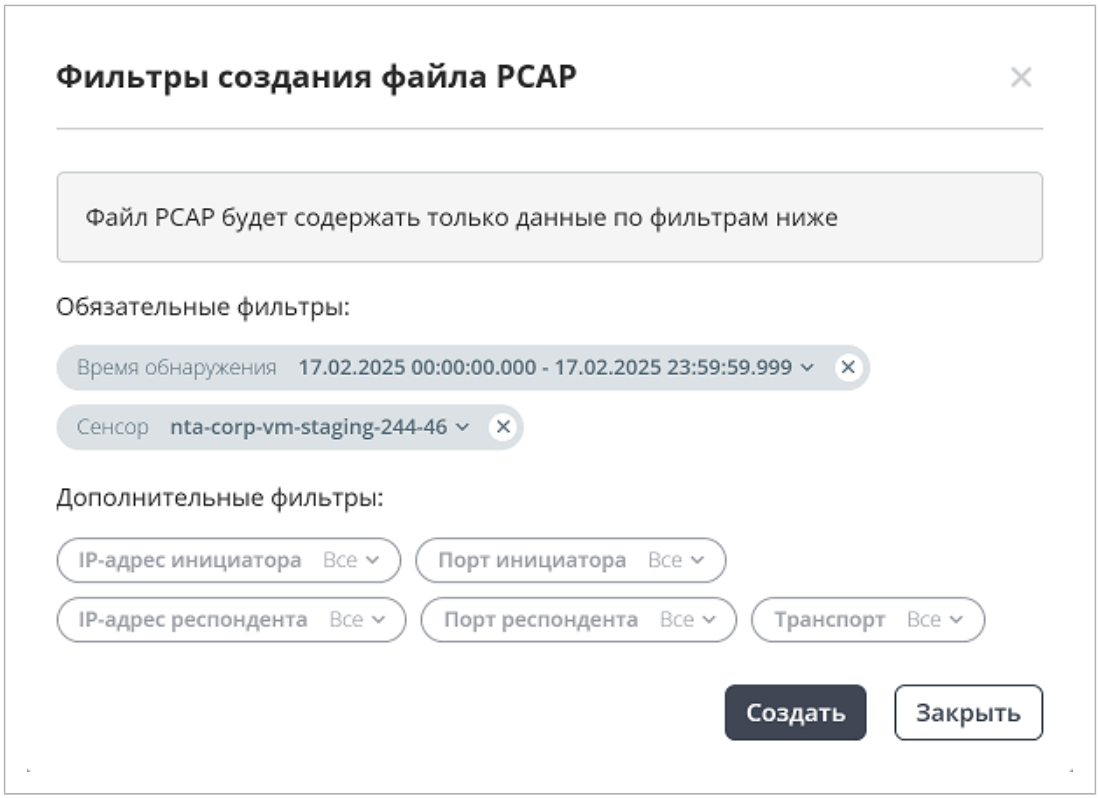


Рис. 299. Окно «Фильтры создания файла PCAP»

3. В открывшемся окне **Фильтры создания файла PCAP** при необходимости откорректируйте значения фильтров.
4. Нажмите кнопку **Создать**.
   - **Результат шага:** в правом верхнем углу появится уведомление `Запущено создание файла PCAP`, и начнется подготовка `pcap`-файла.
5. Дождитесь окончания подготовки файла.
   - **Результат шага:** в правом верхнем углу появится уведомление `Файл PCAP создан`.

> Внимание:
>
> Если файл будет иметь размер более 1 ГБ, отобразится ошибка `Файл слишком большой`, и файл не будет подготовлен. Уменьшите выборку пакетов с помощью фильтров на шаге 3 и повторите подготовку файла.

6. Нажмите кнопку (**Файлы PCAP**) в правом верхнем углу.
   - **Результат шага:** Откроется окно **Файлы PCAP**.
7. Нажмите на наименование файла со статусом загрузки `Готов к экспорту`.

> Прим.:
>
> В окне **Файлы PCAP** можно также экспортировать ранее подготовленные пакеты со статусом `Готов к экспорту`. Описание всех статусов файлов приведено в справочном разделе «Статусы подготовки файлов к экспорту».

8. В открывшемся окне укажите расположение для экспортируемого файла, при необходимости изменив его название, и нажмите кнопку **Сохранить**.
   - **Результат шага:** файл `traffic_[дата_и_время].pcap` будет загружен на компьютер.

15.3.5. Экспорт файлов, обнаруженных в сетевом трафике

15.3.5.1. Экспорт одного файла, обнаруженного в рамках сессии

Перед выполнением: Убедитесь, что на сенсорах включено сохранение файлов из трафика — подробнее см. инструкцию «Первичная настройка модуля «Анализ промышленного сетевого трафика»».

Для экспорта файла, обнаруженного в рамках сессии:

1. На странице **Файлы** отобразите файл, обнаруженный в рамках сессии. Для этого:
   а. Перейдите на вкладку **Сессии** страницы **Сетевые соединения**.
   б. Выберите сессию из списка.
   - **Результат шага:** откроется карточка сессии. Если в рамках сессии были обнаружены файлы, в поле **Файлов обнаружено** отобразится их количество.

   в. В карточке сессии нажмите на количество обнаруженных файлов.
   - **Результат шага:** откроется вкладка **Файлы** страницы **Сетевые соединения** со списком файлов из выбранной сессии (записи будут отфильтрованы по `UID сессии`).

   г. Нажмите на строку с файлом.
   - **Результат шага:** откроется карточка с подробной информацией о файле.
2. В карточке файла нажмите ссылку **Сформировать архив файлов**.
   - **Результат шага:** в правом верхнем углу появится уведомление `Запущена подготовка файлов к экспорту`, и начнется подготовка архива. По окончании формирования архива уведомление автоматически скроется.
3. Закройте карточку файла и нажмите кнопку Файлы для экспорта в правом верхнем углу страницы.
   - **Результат шага:** Откроется модальное окно **Файлы для экспорта**.

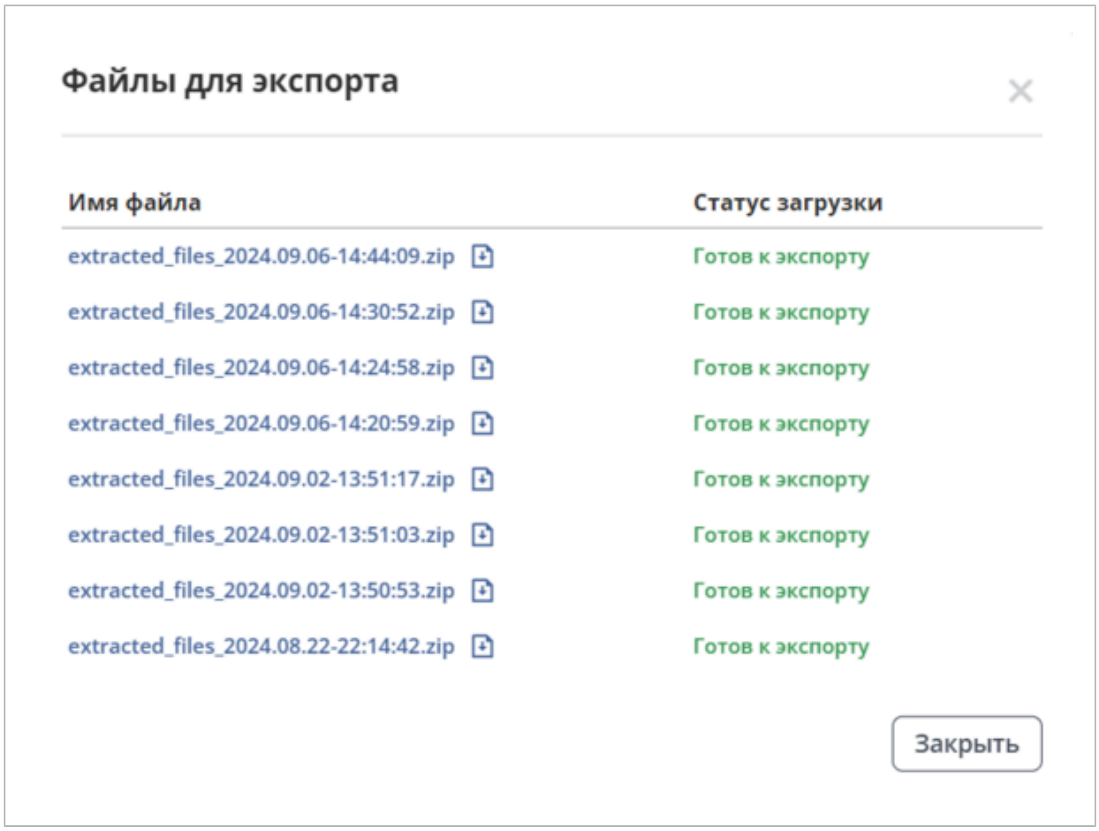


Рис. 300. Окно «Файлы для экспорта»

4. Нажмите на наименование подготовленного архива со статусом `Готов к экспорту`.

> Прим.:
>
> В окне **Файлы для экспорта** можно также экспортировать ранее подготовленные архивы со статусом `Готов к экспорту`. Описание всех статусов файлов приведено в справочном разделе «Статусы подготовки файлов к экспорту».

5. В открывшемся окне укажите расположение для экспортируемого файла, при необходимости изменив его название, и нажмите кнопку **Сохранить**.
   - **Результат шага:** архив `extracted_files_[дата_и_время].zip` будет загружен на компьютер.

> Внимание:
>
> Перед открытием файла убедитесь в его безопасности — файлы могут содержать вредоносное ПО.

15.3.5.2. Экспорт нескольких файлов

Перед выполнением: Убедитесь, что на сенсорах включено сохранение файлов из трафика — подробнее см. инструкцию «Первичная настройка модуля «Анализ промышленного сетевого трафика»».

Для экспорта нескольких файлов со страницы **Файлы**:

1. При необходимости отфильтруйте список всех обнаруженных файлов на странице **Файлы**.
2. Установите чекбоксы слева от файлов, которые нужно экспортировать.

3. Нажмите кнопку Подготовить к экспорту над списком файлов.
   - **Результат шага:** в правом верхнем углу появится уведомление `Запущена подготовка файлов к экспорту`, и начнется подготовка архива.
4. Дождитесь окончания подготовки архива.
   - **Результат шага:** в правом верхнем углу появится уведомление `Формирование архива завершено`.
5. Нажмите кнопку Файлы для экспорта в правом верхнем углу.
   - **Результат шага:** Откроется модальное окно **Файлы для экспорта**.

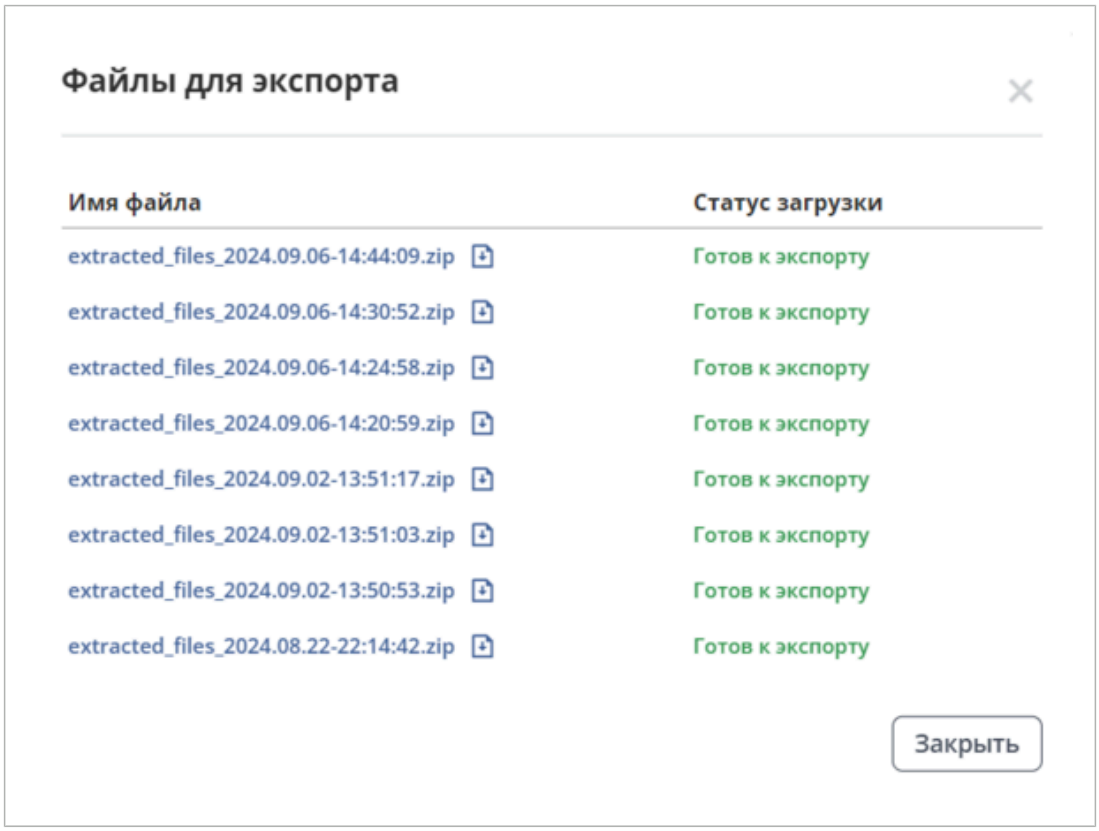


Рис. 301. Окно «Файлы для экспорта»

6. Нажмите на наименование подготовленного архива со статусом `Готов к экспорту`.

> Прим.:
>
> В окне **Файлы для экспорта** можно также экспортировать ранее подготовленные архивы со статусом `Готов к экспорту`. Описание всех статусов файлов приведено в справочном разделе «Статусы подготовки файлов к экспорту».

7. В открывшемся окне укажите расположение для экспортируемого файла, при необходимости изменив его название, и нажмите кнопку **Сохранить**.
   - **Результат шага:** архив `extracted_files_[дата_и_время].zip` будет загружен на компьютер.

> Внимание:
>
> Перед открытием файла убедитесь в его безопасности — файлы могут содержать вредоносное ПО.

15.4. Правила сессий

Для мониторинга наличия или отсутствия в контролируемой сети предприятия новых соединений Комплекс позволяет создавать и настраивать правила сессий.

Правило сессий — запись в Комплексе с набором критериев разрешенности сессии на основе заданных условий. Условия задаются для следующих обязательных параметров сессии:

- IP-адрес отправителя,
- IP-адрес получателя,
- порт получателя,
- транспортный протокол.

Если значения параметров в соединении совпадают с условиями в правиле (или входят в указанный диапазон — например, конкретный IP-адрес в соединении попадает в подсеть из правила), то сессии присваивается статус `Разрешенная`. Если значение хотя бы одного из параметров соединения не совпадает со значением в правиле, сессии присваивается статус `Неразрешенная`. При этом на странице **События** создается событие ИБ с кодом `1270001` об обнаружении неразрешенной сессии.

> Прим.:
>
> Для сессий с одинаковыми значениями обязательных параметров создается только одно событие в сутки во избежание дублирования и избыточного уведомления.

Статус `Не определен` присваивается всем обнаруженным сессиям в режиме обучения Комплекса.

15.4.1. Режим обучения

Режим обучения предназначен для формирования базы правил сессий для штатной работы Комплекса. На основе комбинаций уникальных значений обязательных параметров сессии Комплекс создает правило с наименованием `Автоматически созданное правило`. Пользователь может корректировать его параметры (см. инструкцию «Редактирование правил сессий») и управлять его активностью (см. инструкцию «Активация и деактивация правил сессий»). Продолжительность обучения Комплекса определяет пользователь с ролью `Администратор` или `Инженер`. Если новые правила прекратили появляться либо стали появляться очень редко, можно переводить Комплекс в режим обнаружения.

15.4.2. Режим обнаружения

Режим обнаружения предназначен для выявления во входящих соединениях отклонений от условий, установленных в правилах сессий. В режиме обнаружения пользователи создают правила сессий, настраивая их вручную (см. инструкцию «Создание правил сессий вручную») либо на основе зарегистрированных сессий (см. инструкцию «Создание правил сессий на основе зарегистрированных сессий»).

Изменить текущий режим контроля сессий можно в карточке сенсора в Комплексе уровня Sensor на странице **Сенсоры**, подробнее см. инструкции: «Автоматическое создание правил сессий», «Деактивация автоматического создания правил сессий».

В этом разделе:

- Просмотр правил сессий
- Управление правилами сессий

- Фильтрация списка правил сессий
- Создание правил сессий
- Активация и деактивация правил сессий
- Редактирование правил сессий
- Удаление правил сессий

15.4.3. Просмотр правил сессий

Правила сессий отображаются в виде таблицы на странице **Инспекция сети → Правила сессий**.

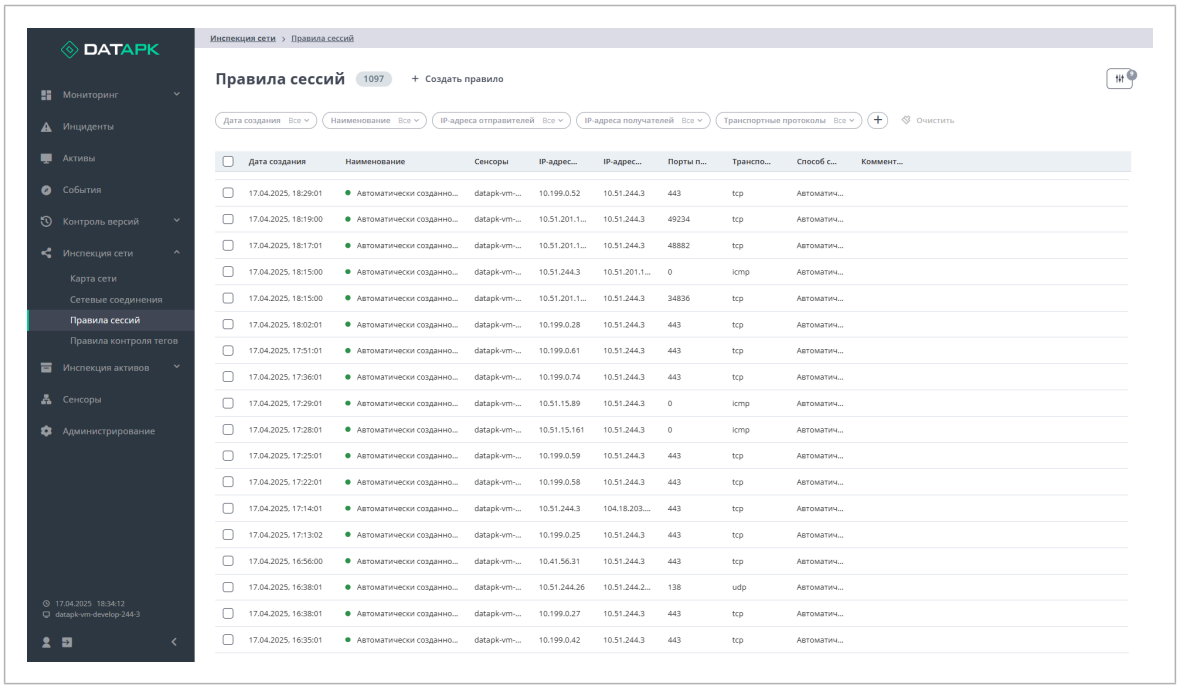


Рис. 302. Страница «Правила сессий»

Справа от заголовка страницы **Правила сессий** отображается количество созданных правил.

С помощью кнопки в правом верхнем углу страницы настраивается таблица правил сессий.

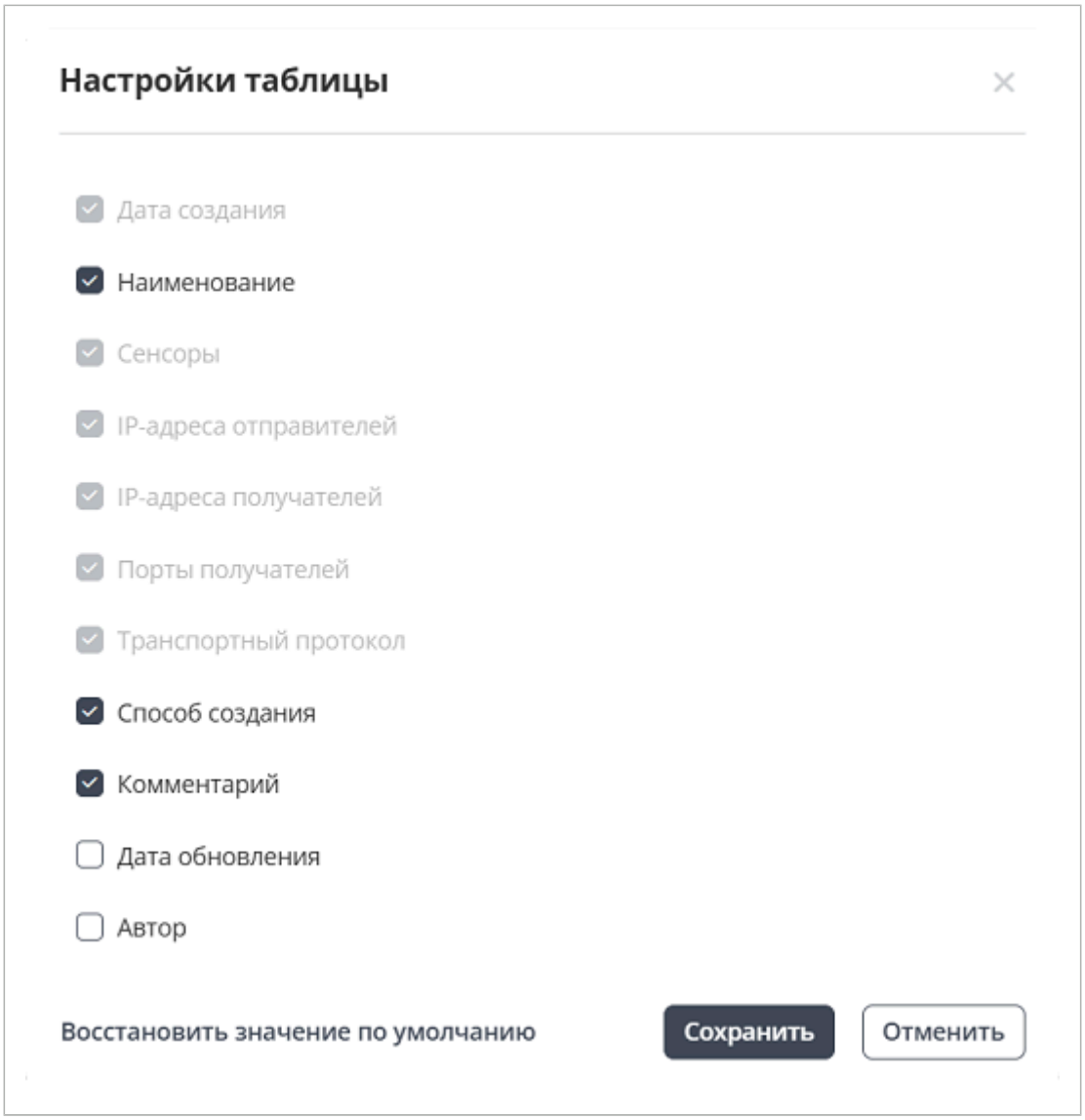


Рис. 303. Окно «Настройки таблицы»

В окне **Настройки таблицы** можно выбрать, какие столбцы и в каком порядке будут отображаться в таблице правил. Всегда отображаются столбцы **Дата создания**, **Сенсоры**, **IP-адреса отправителей**, **IP-адреса получателей**, **Порты получателей** и **Транспортный протокол** — их невозможно скрыть из таблицы. При необходимости можно восстановить вид таблицы по умолчанию. Подробнее о настройках таблицы см. в разделе «Элементы управления таблицами».

Под заголовком страницы расположена панель фильтров, подробнее о работе с ними см. в разделе «Фильтрация списка правил сессий».

При нажатии в таблице на правило сессий открывается карточка правила.

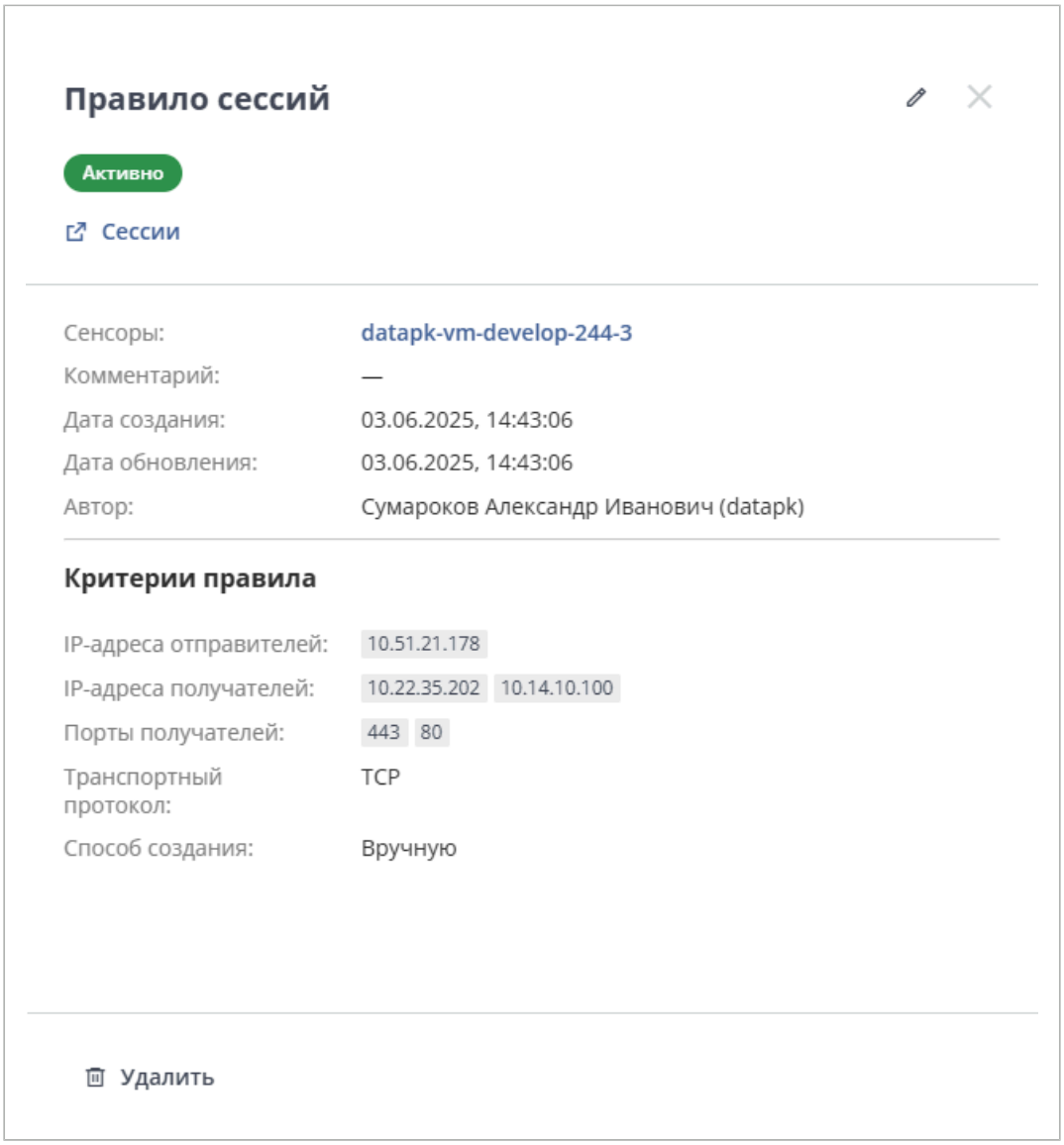


Рис. 304. Карточка правила сессии

В карточке представлена следующая информация:

- наименование правила сессий;
- индикатор активности правила — показывает одно из значений: `Активно` или `Неактивно`;

> Подсказка:
>
> Активность правила меняется вручную, подробнее см. в разделе «Активация и деактивация правил сессий».

- кнопка Сессии — предназначена для перехода к сессиям, удовлетворяющим критериям правила;
- **Сенсоры** — поле содержит наименования сенсоров, на которых применяется правило, при нажатии на наименование открывается карточка сенсора;
- **Комментарий** — поле содержит дополнительные сведения о правиле: например, для чего создано правило;
- **Дата создания** — поле содержит дату и время создания правила;
- **Дата обновления** — поле содержит дату и время последнего изменения правила;

- **Автор** — поле содержит Ф.И.О. пользователя, создавшего правило.

> Прим.:
>
> Для автоматически созданных правил в поле **Автор** отображается значение `Комплекс`.

- **Критерии правила** — блок содержит условия, при нарушении которых сессии присваивается статус `Не разрешена` и создается событие ИБ. Блок включает в себя поля:
  - **IP-адреса отправителей** — поле содержит IP-адреса, с которых отправлены сетевые пакеты;
  - **IP-адреса получателей** — поле содержит IP-адреса, на которые получены сетевые пакеты;
  - **Порты получателей** — поле содержит порты, на которые получены сетевые пакеты;
  - **Транспортный протокол** — поле содержит протокол транспортного уровня, использованный в сессии. Показывает одно из значений: `TCP`, `UDP`, `ICMP`;
  - **Способ создания** — поле показывает одно из значений: `Автоматически`, `Вручную`, `Из сессии`. Подробнее о способах создания правил сессий см. в разделе «Создание правил сессий».

При наведении курсора на строку в таблице правил отображаются кнопки (**Редактировать**) и (**Удалить**). С помощью них можно управлять правилами, подробнее см. в разделах «Редактирование правил сессий» и «Удаление правил сессий».

Если выбрать одно или несколько правил сессий с помощью чекбоксов слева от правил, внизу страницы отобразится меню управления правилами.

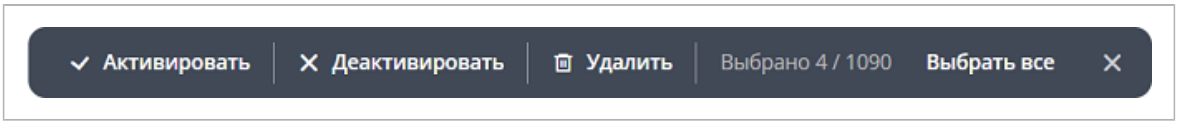


Рис. 305. Меню управления правилами сессий

Кнопки меню позволяют управлять как одним правилом, так и группой правил. Доступны следующие действия:

- **Активировать** — меняет активность выбранных правил на `Активно`.
- **Деактивировать** — меняет активность выбранных правил на `Неактивно`.

> Прим.:
>
> Активность меняется только у тех правил, текущий статус активности которых отличается от нового. Правила, уже имеющие выбранный статус, остаются без изменений.

- **Удалить** — удаляет выбранные правила из списка правил сессий и на сенсорах.
- **Выбрать все** — выбирает все созданные правила сессий для последующего выполнения действий с ними.

> Прим.:
>
> Если установить чекбокс в заголовке таблицы, будут выбраны только видимые в списке правила. Правила, подгружаемые при прокрутке списка, не будут выбраны автоматически — их можно выбрать повторной установкой чекбокса.

Также в меню управления отображается количество выбранных правил из их общего количества.

См. также

Фильтрация списка правил сессий

15.4.4. Управление правилами сессий

В этом подразделе:

- Фильтрация списка правил сессий
- Создание правил сессий
- Активация и деактивация правил сессий
- Редактирование правил сессий
- Удаление правил сессий

15.4.4.1. Фильтрация списка правил сессий

Комплекс позволяет фильтровать отображаемые правила сессий с помощью фильтров. Панель с фильтрами находится вверху страницы **Правила сессий**.

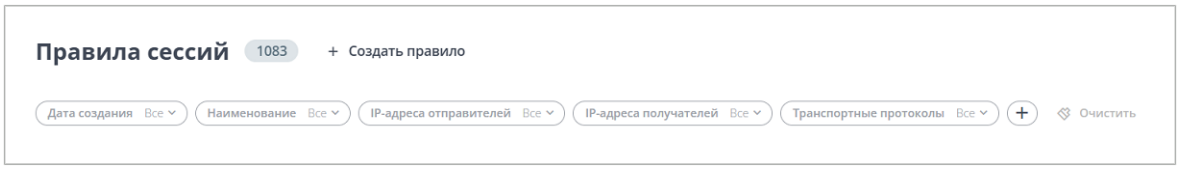


Рис. 306. Панель фильтров на странице «Правила сессий»

Для добавления фильтров на страницу нажмите кнопку ⊕, расположенную справа от последнего фильтра — отобразится выпадающий список с доступными фильтрами. Фильтры, уже выбранные для отображения на странице, имеют серый цвет и иконку ✔ слева от названия.

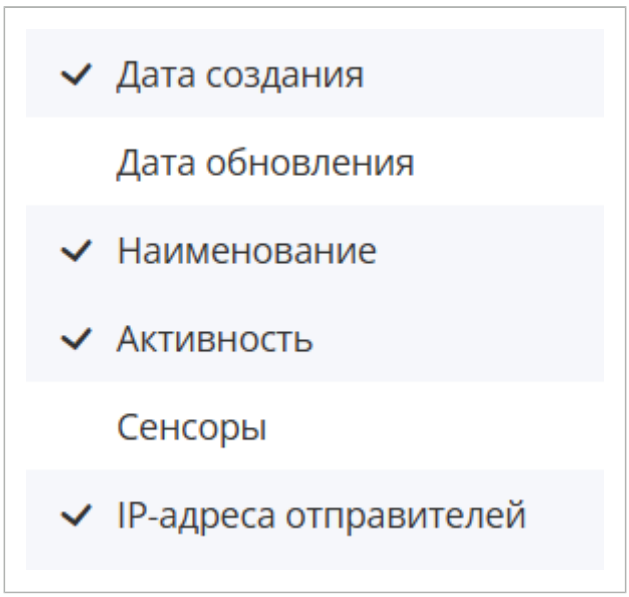


Рис. 307. Выпадающий список фильтров

Для настройки фильтра нажмите на него. Для сброса фильтра нажмите ✕ справа от него, либо нажмите **Снять выделение** в фильтрах с выбором нескольких значений. Для сброса результатов по всем фильтрам нажмите Очистить. Чтобы применить настройки фильтра, нажмите в нем ✔ или Применить либо клавишу **Enter**, в фильтрах **Дата создания** и **Дата обновления** нажмите на пустое пространство вне фильтра.

По умолчанию отображаются следующие фильтры:

1. **Дата создания** — фильтрация выполняется по правилам сессий, созданным в указанный временной период. Нажатием на число в календаре фильтра можно выбрать начальную и конечную даты. Также для фильтрации можно указать текущие сутки, нажав на текущую дату внизу календаря.
2. **Наименование** — фильтрация выполняется по полному и частичному названию правила.

   Подсказка:

   Поле **Наименование** является регистронезависимым.

3. **IP-адреса отправителей** — фильтрация выполняется по распознанным IP-адресам отправителей сетевых пакетов. IP-адрес, диапазон адресов или подсеть необходимо вводить полностью.
4. **IP-адреса получателей** — фильтрация выполняется по распознанным IP-адресам получателей сетевых пакетов. IP-адрес необходимо вводить полностью.

   Прим.:

   В поля IP-адресов допускается копирование из других источников списков IP-адресов, их диапазонов или подсетей. Элементы в исходном списке должны разделяться с помощью: **,**, **;**, **Tab**, **Enter**, **Space**. Подсети задаются в формате CIDR.

5. **Транспортные протоколы** — фильтрация выполняется по распознанным протоколам транспортного уровня: `TCP`, `UDP`, `ICMP`. Можно выбрать несколько протоколов.

Дополнительно можно добавить и настроить следующие фильтры:

1. **Активность** — фильтр позволяет отфильтровать правила сессий по статусу их работы, можно выбрать одно из значений: `Активно` или `Неактивно`.
2. **Сенсоры** — фильтр содержит наименования сенсоров, подключенных к Комплексу. Можно выбрать несколько наименований из списка. При применении фильтра отобразятся правила, применяемые на выбранных сенсорах.
3. **Порты получателей** — фильтрация выполняется по распознанным портам, на которые были получены сетевые пакеты. Можно ввести несколько портов, подтверждая ввод каждого нажатием клавиши **Enter** или **Tab**.
4. **Способ создания** — фильтр позволяет отобразить правила по способу их создания: `Автоматически`, `Вручную` или `Из сессии`. Можно выбрать несколько значений.
5. **Дата обновления** — фильтрация выполняется по указанному временному периоду последнего изменения правила сессий. Также для фильтрации можно указать текущие сутки, нажав на текущую дату внизу выпадающего окна фильтра.

Прим.:

При одновременном использовании двух и более фильтров будут отображены правила, удовлетворяющие всем заданным параметрам.

См. также

Просмотр правил сессий

15.4.4.2. Создание правил сессий

В этом подразделе:

- Автоматическое создание правил сессий
- Создание правил сессий вручную
- Создание правил сессий на основе зарегистрированных сессий
- Деактивация автоматического создания правил сессий

15.4.4.2.1. Автоматическое создание правил сессий

Переключение контроля сессий в режим обучения Комплекса для автоматического создания правил сессий на основе входящих соединений.

Прим.:

При первичном запуске Комплекса режим обучения активен по умолчанию.

Для активации автоматического создания правил сессий в режиме обучения Комплекса:

1. Перейдите на страницу **Сенсоры**.
2. Выберите сенсор, на котором необходимо создать правила.
   - **Результат шага:** справа откроется карточка сенсора.

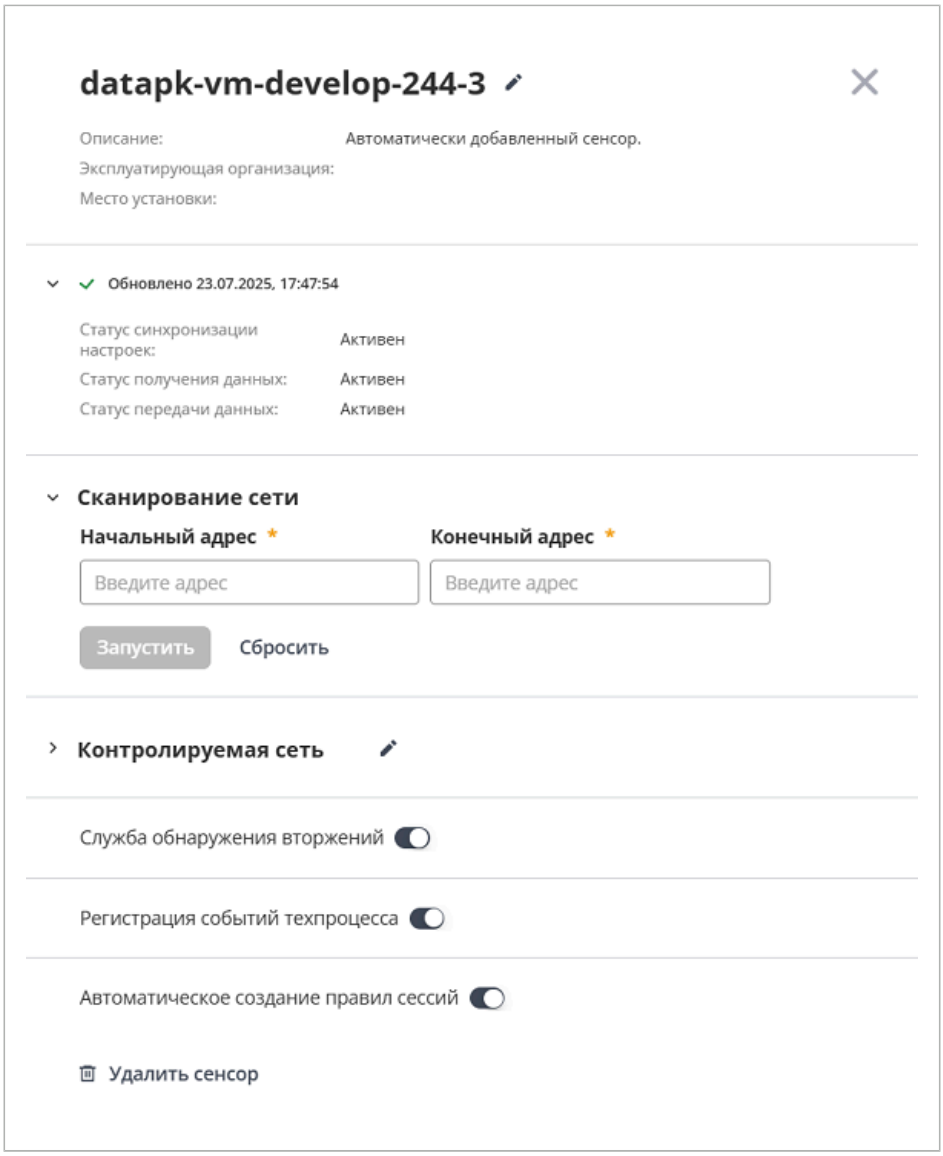


Рис. 308. Карточка сенсора

3. В открывшейся карточке в блоке **Контролируемая сеть** активируйте режим обучения Комплекса с помощью переключателя **Автоматическое создание правил сессий**: если переключатель в состоянии — режим обучения активен.

   ▸ **Результат шага:** на странице **События** отображается событие с кодом `1270002`: `Изменен режим работы контроля сессий`.

4. Перейдите на страницу **Инспекция сети → Правила сессий** и убедитесь, что в списке правил появляются новые правила с наименованием `Автоматически созданное правило`.

См. также

Правила сессий

Деактивация автоматического создания правил сессий

15.4.4.2.2. Создание правил сессий вручную

Для создания правила сессий:

1. Перейдите на страницу **Инспекция сети → Правила сессий**.

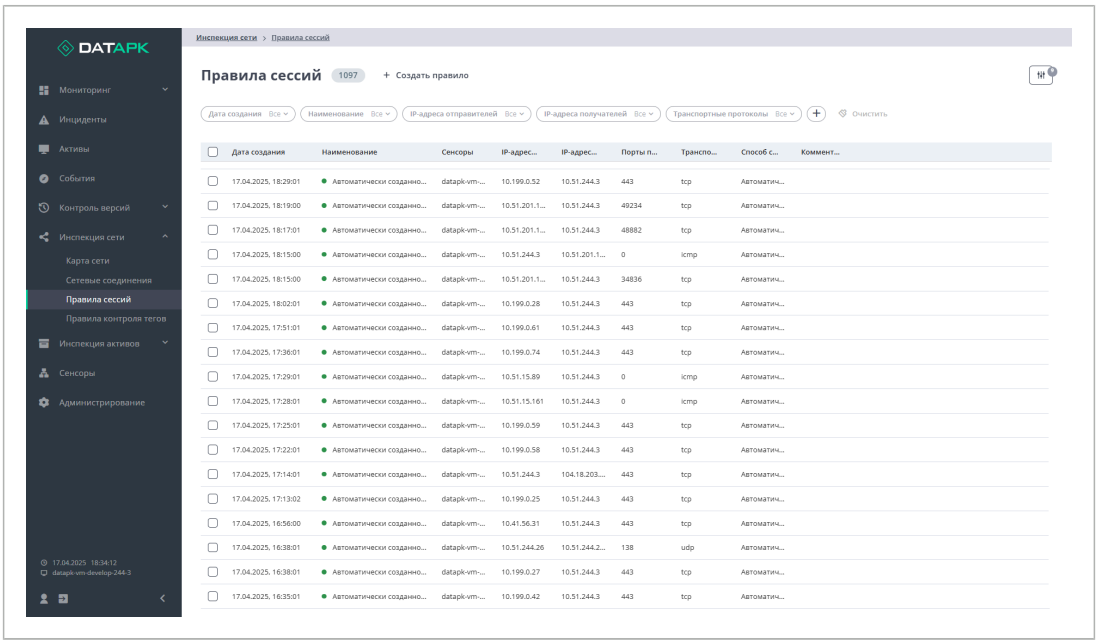


Рис. 309. Страница «Правила сессий»

2. Вверху страницы нажмите кнопку **Создать правило**.
   - **Результат шага:** справа откроется окно **Создание правила сессий**.
3. В открывшемся окне задайте следующие параметры:
   а. Введите наименование создаваемого правила.
   б. Настройте активность правила с помощью переключателя **Активность**: если он установлен вправо ( ) — правило активно, влево ( ) — неактивно.
   в. В поле **Сенсоры** выберите из списка сенсоры, на которых требуется применять правило.
   г. При необходимости заполните поле **Комментарий**, указав, например, описание или дополнительную информацию о правиле.
   д. В разделе **Критерии правила** задайте критерии для определения сессий, к которым требуется применять правило. Доступны следующие критерии:
      - IP-адреса отправителей;
      - IP-адреса получателей;

> Прим.:
>
> В поля IP-адресов допускается копирование из других источников списков IP-адресов, их диапазонов или подсетей. Элементы в исходном списке должны разделяться с помощью: „ ;, **Tab**, **Enter**, **Space**. Подсети задаются в формате CIDR.

- Порты получателей;
- Транспортный протокол.

> Прим.:
>
> Если поле какого-либо критерия оставить пустым, в правиле будет учтено любое значение этого критерия.

4. Нажмите кнопку **Создать** для подтверждения создания правила.
   - **Результат шага:** в правом верхнем углу страницы появится уведомление: `Правило сессий успешно создано`. Созданное правило отобразится в списке правил на странице **Правила сессий**.

15.4.4.2.3. Создание правил сессий на основе зарегистрированных сессий

Создание правил на основе зарегистрированных сессий со статусами «Не разрешена» и «Не определен».

Для создания правила на основе зарегистрированной сессии:

1. Перейдите на страницу **Инспекция сети** на вкладку **Сессии**.
2. Выберите из списка сессию.
   - **Результат шага:** справа откроется карточка сессии.

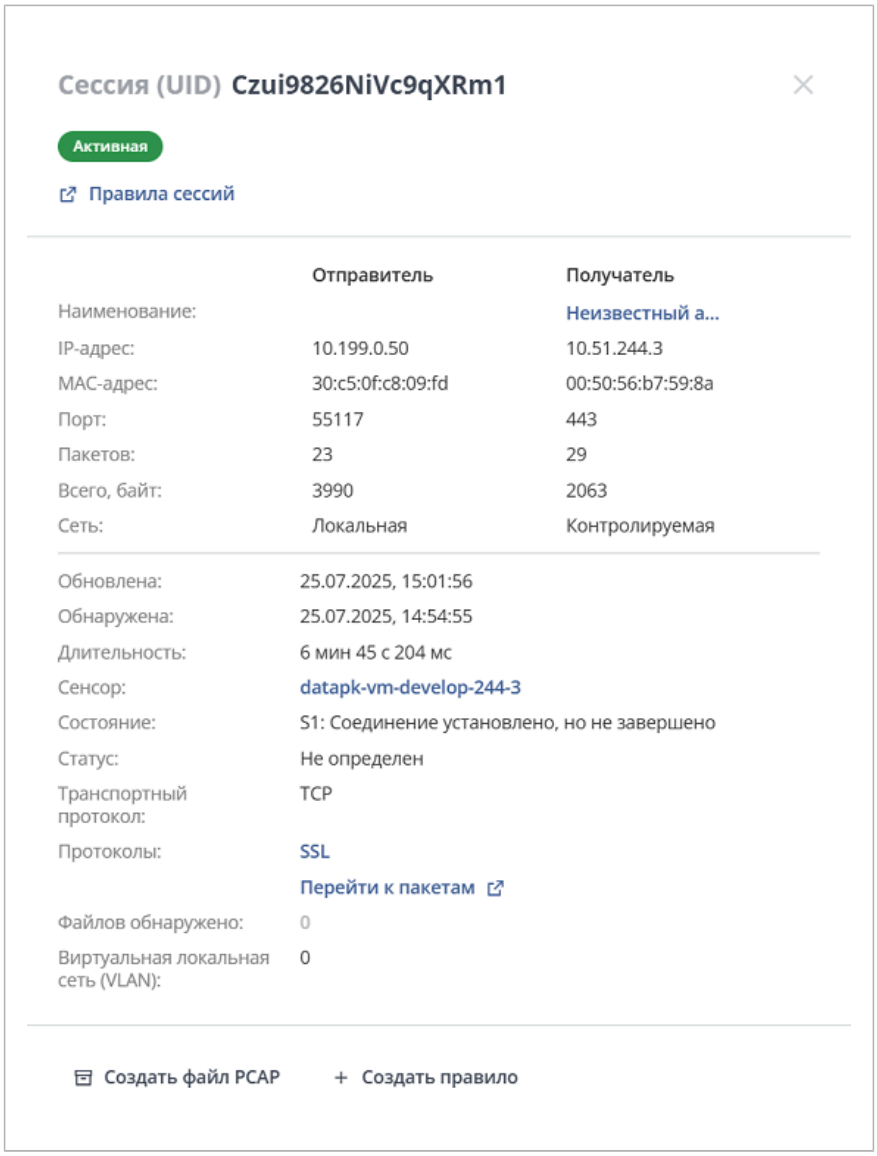


Рис. 311. Карточка сессии

3. В открывшейся карточке внизу нажмите **+ Создать правило**.
   - **Результат шага:** справа откроется окно **Создание правила сессий** с предзаполненными полями **Наименование**, **Сенсоры** и всеми полями подраздела **Критерии правила**.

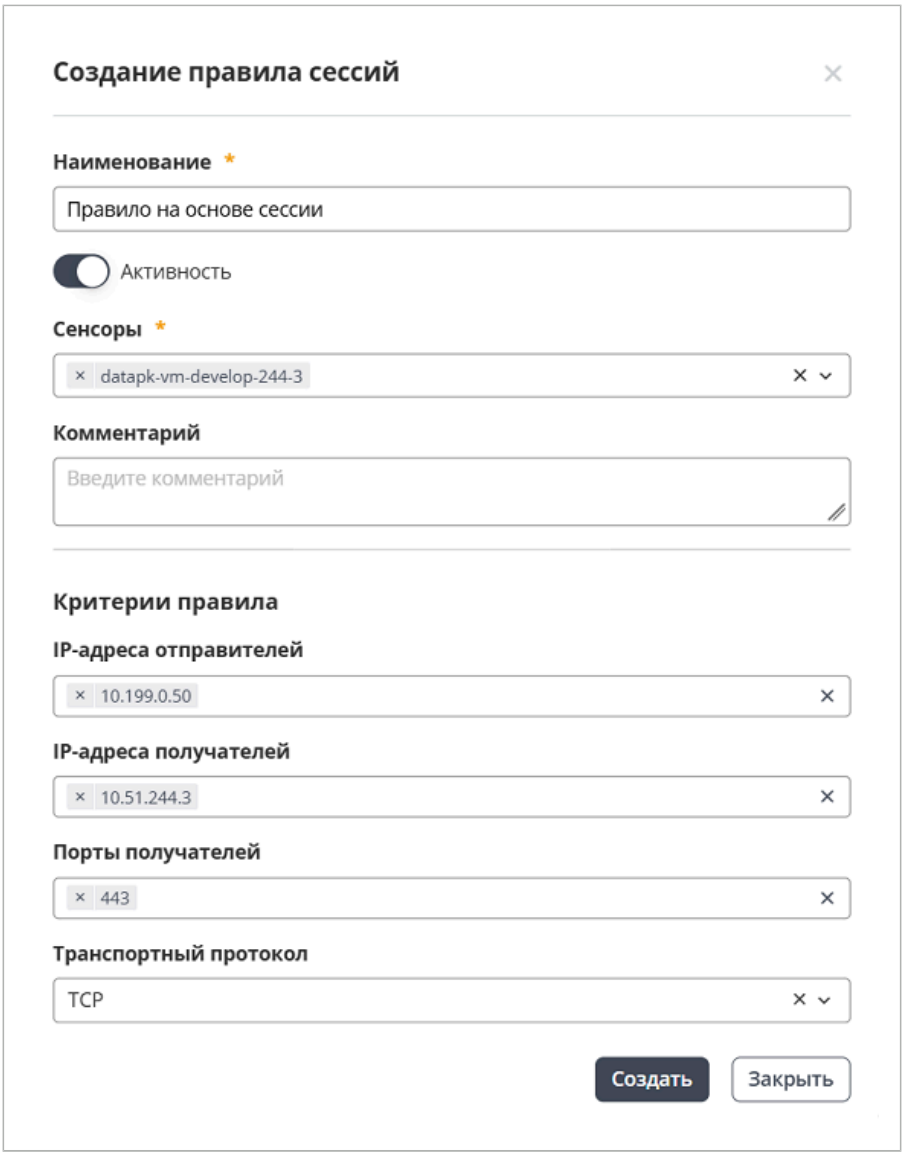


Рис. 312. Окно «Создание правила сессий»

4. В открывшемся окне задайте следующие параметры:
   а. При необходимости измените наименование правила.
   б. Настройте активность правила с помощью переключателя **Активность**: если он установлен вправо ( ) — правило активно, влево ( ) — неактивно.
   в. В поле **Сенсоры** выберите из списка сенсоры, на которых требуется применять правило.
   г. При необходимости заполните поле **Комментарий** и измените критерии создаваемого правила.

> Прим.:
>
> Если поле какого-либо критерия оставить пустым, в правиле будет учтено любое значение этого критерия.

5. Нажмите кнопку **Создать** для подтверждения создания правила.

▸ **Результат шага:** в правом верхнем углу страницы появится уведомление: `Правило сессий успешно создано`. Созданное правило отобразится в списке правил на странице **Правила сессий**.

15.4.4.2.4. Деактивация автоматического создания правил сессий

Переключение контроля сессий в режим обнаружения неразрешенных сессий.

Для деактивации автоматического создания правил сессий и активации режима обнаружения:

1. Перейдите на страницу **Сенсоры**.
2. Выберите сенсор, на котором хотите деактивировать автоматическое создание правил сессий.
   - **Результат шага:** справа откроется карточка сенсора.

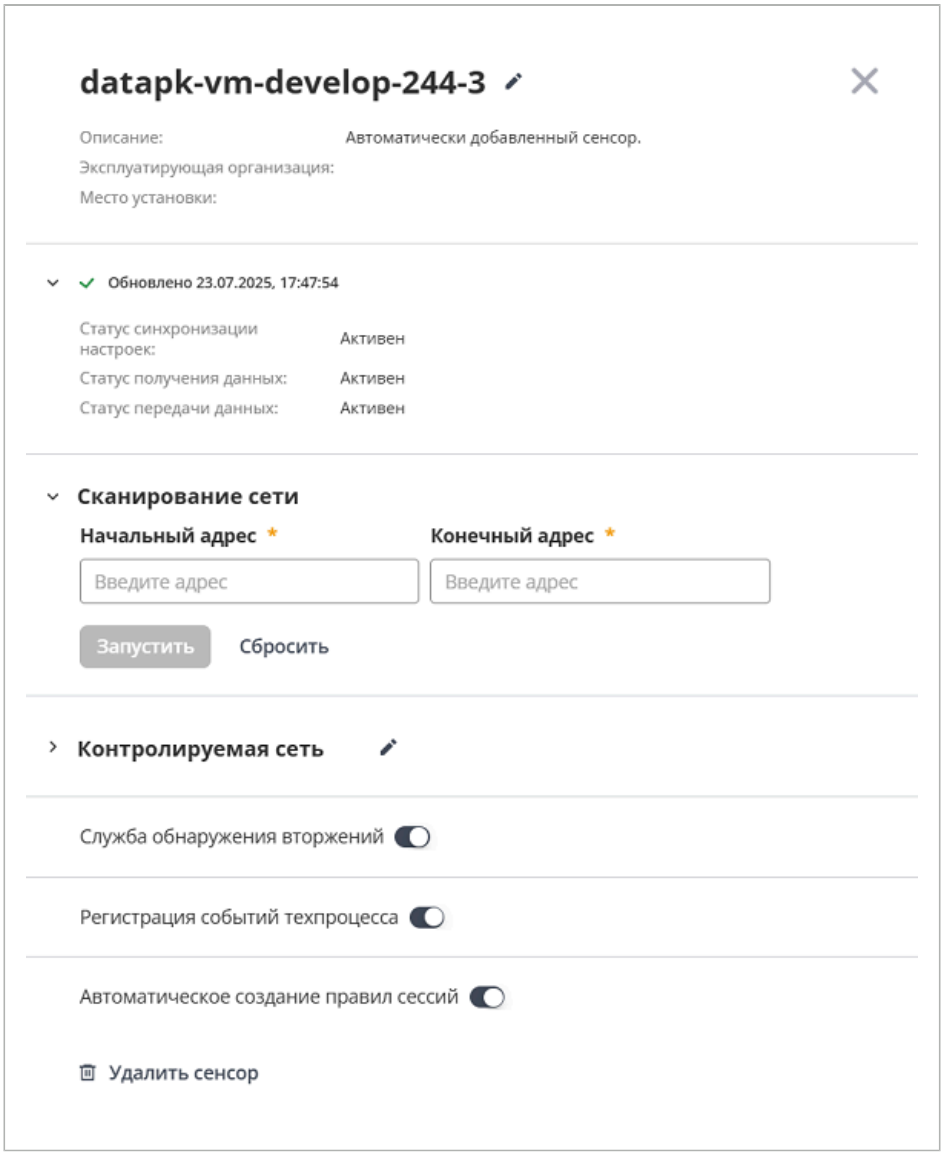


Рис. 313. Карточка сенсора

3. В открывшейся карточке в блоке **Контролируемая сеть** деактивируйте режим обучения Комплекса с помощью переключателя **Автоматическое создание правил сессий**: если переключатель в состоянии — режим обучения деактивирован, режим обнаружения активирован. Правила сессий не создаются автоматически.
4. Перейдите на страницу **Инспекция сети → Правила сессий** и убедитесь, что в списке правил не появляются новые правила с наименованием `Автоматически созданное правило`.

15.4.4.3. Активация и деактивация правил сессий

Деактивация позволяет приостановить работу правила, не удаляя его.

Доступна активация и деактивация как одного, так и нескольких правил сессий.

1. Для активации или деактивации одного правила:
    a. Перейдите на страницу **Инспекция сети → Правила сессий**.
    б. Выберите из списка правило, которое хотите активировать или деактивировать.

- **Результат шага:** справа откроется карточка правила сессий.

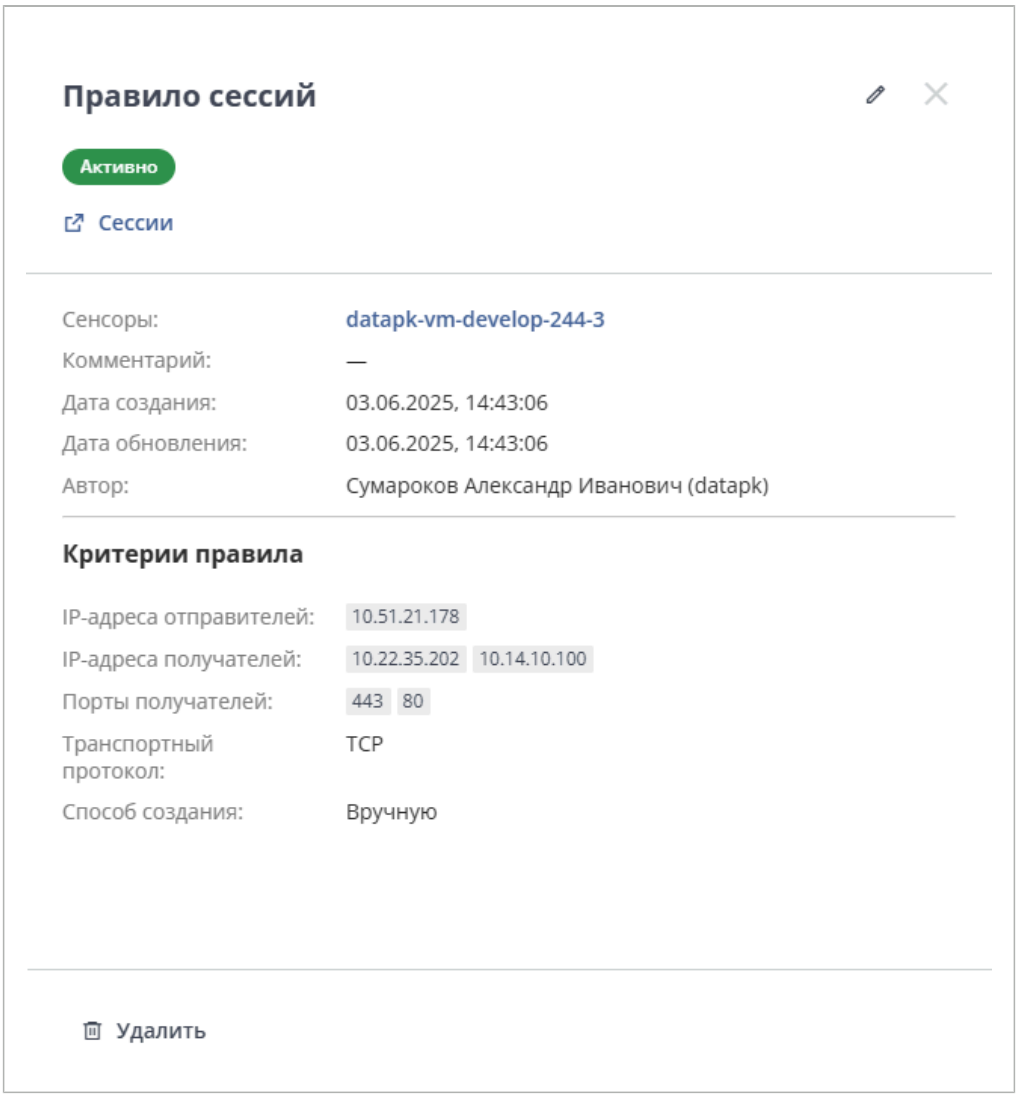


Рис. 314. Карточка правила сессий

в. Вверху карточки нажмите (**Редактировать**).

- **Результат шага:** откроется окно **Редактирование правила сессий**.

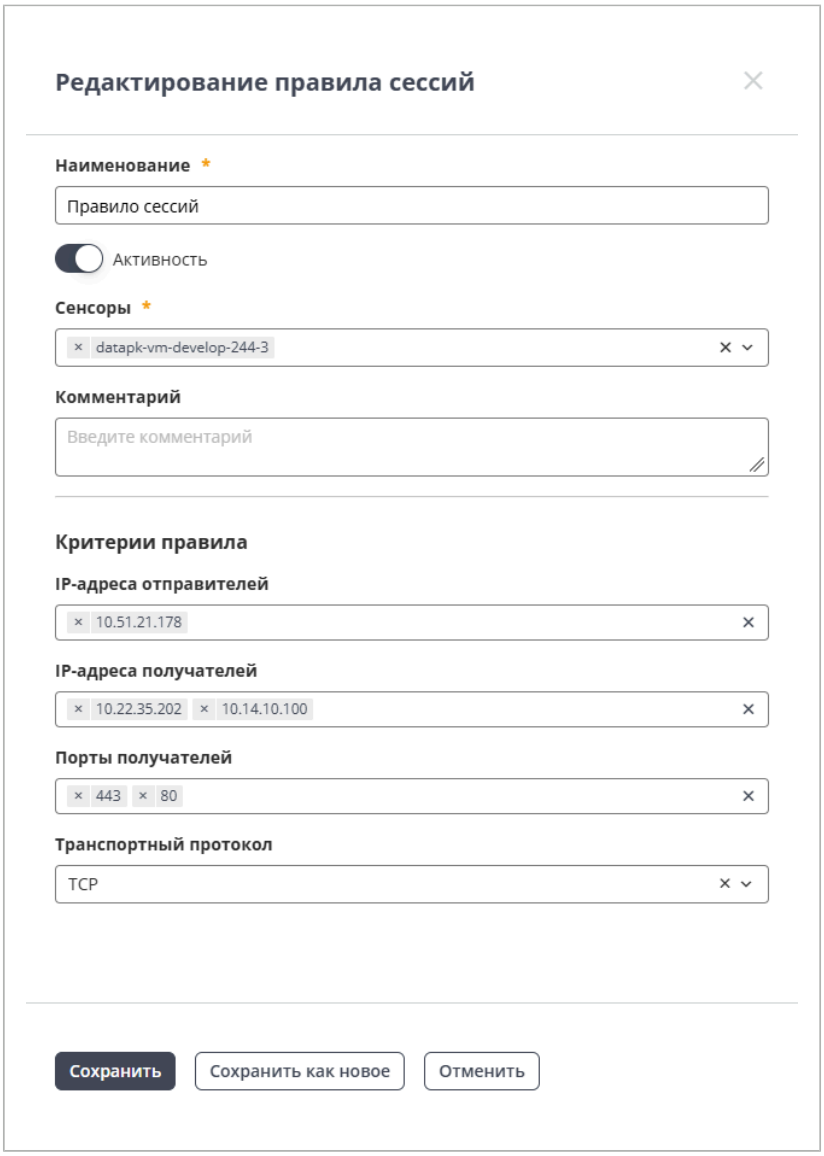


Рис. 315. Окно «Редактирование правила сессий»

г. В открывшемся окне активируйте или деактивируйте правило сессий с помощью переключателя **Активность**: если он установлен вправо ( ) — правило активно, влево ( ) — неактивно.

д. Нажмите **Сохранить** для подтверждения изменения активности правила.

Результат шага: при успешном изменении активности правила в правом верхнем углу страницы появится уведомление: Правило сессий успешно изменено. В карточке активированного правила отобразится иконка Активно, в карточке деактивированного правила — Неактивно

Подсказка:

Правило также можно активировать или деактивировать следующим способом:

- В списке правил установите чекбокс возле необходимого правила.
- В открывшемся внизу меню нажмите либо Деактивировать.

2. Для активации или деактивации нескольких правил:
    a. В списке правил на странице **Инспекция сети → Правила сессий** установите чекбоксы возле необходимых правил.
    б. В открывшемся внизу меню нажмите Активировать либо Деактивировать.

    ▸ **Результат шага:** в карточке активированного правила отобразится иконка Активно, в карточке деактивированного правила — Неактивно.

15.4.4.4. Редактирование правил сессий

Редактирование правила сессий позволяет:

- изменить правило без его удаления и повторного создания;
- создать новое правило на основе существующего.

1. Для изменения правила сессий:
    a. Выберите из списка правило, которое хотите изменить.

    ▸ **Результат шага:** справа откроется карточка правила сессий.

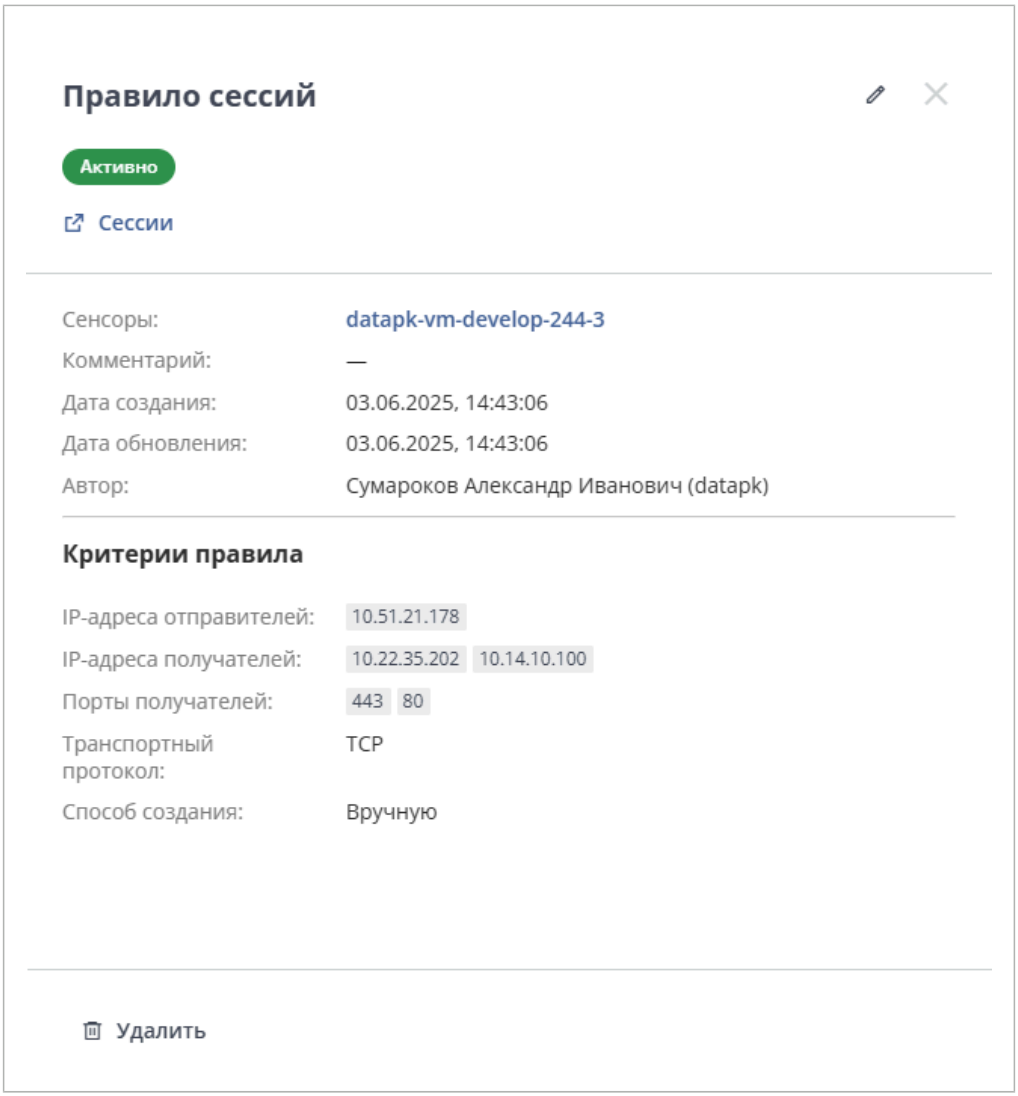


Рис. 316. Карточка правила сессий

б. Вверху карточки нажмите (**Редактировать**).

- **Результат шага:** откроется окно **Редактирование правила сессий**.

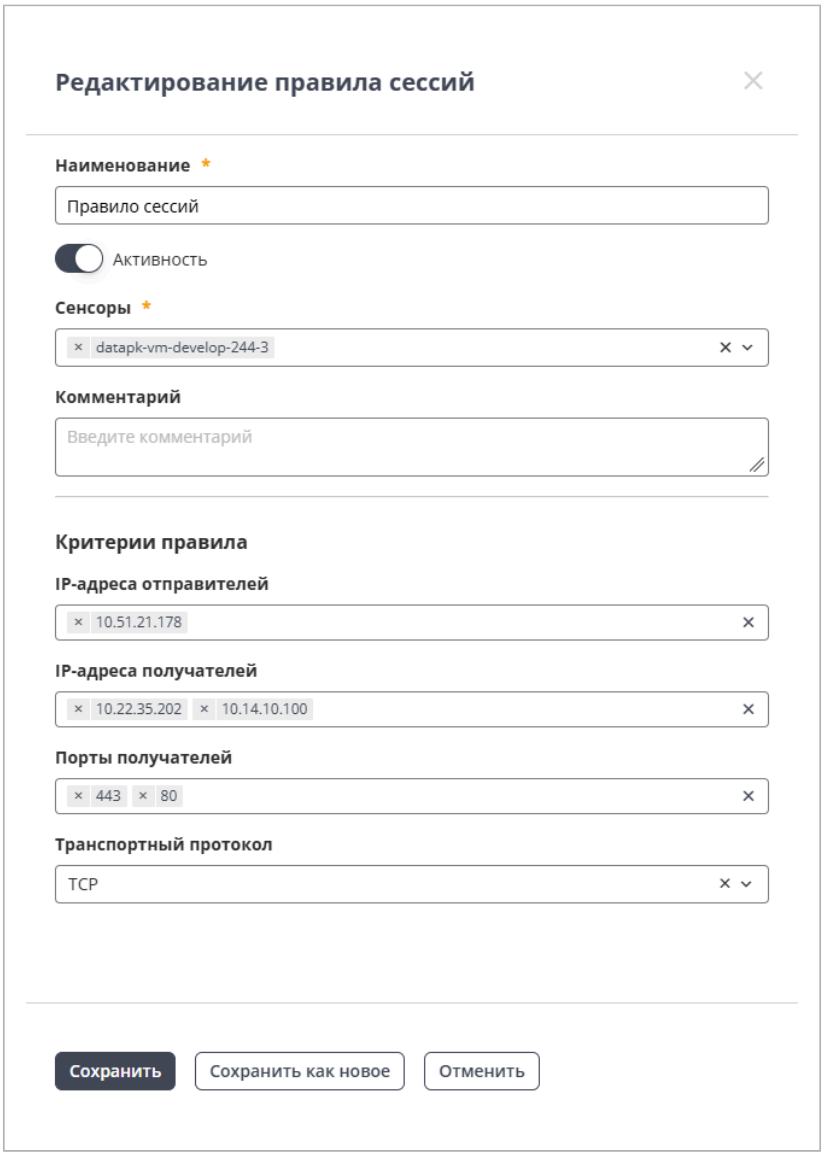


Рис. 317. Окно «Редактирование правила сессий»

в. В открывшемся окне измените необходимые параметры и нажмите **Сохранить** для подтверждения изменений.

- **Результат шага:** в правом верхнем углу страницы появится уведомление: Правило сессий успешно изменено.

2. Для создания нового правила на основе существующего:

а. Откройте существующее правило в режиме редактирования, повторив подшаги a-b из предыдущего шага.

б. Измените необходимые критерии в окне **Редактирование правила сессий** и нажмите **Сохранить как новое**.

- **Результат шага:** в правом верхнем углу страницы появится уведомление: Правило сессий успешно создано. Будет создано новое правило с выбранными критериями, при этом в существующем правиле критерии не изменятся. Новое правило отобразится в списке правил сессий.

15.4.4.5. Удаление правил сессий

Доступно удаление как одного, так и нескольких правил сессий.

Внимание:

Удаленное правило сессий невозможно восстановить. Перед удалением убедитесь, что правило больше не требуется.

1. Для удаления одного правила:
   a. В списке правил на странице **Инспекция сети → Правила сессий** выберите правило, которое хотите удалить.
   - **Результат шага:** справа откроется карточка правила сессий.

   б. Внизу открывшейся карточки нажмите Удалить.
   - **Результат шага:** откроется окно обоснования удаления правила сессий.

   в. Введите текст обоснования удаления правила и нажмите **Подтвердить**.

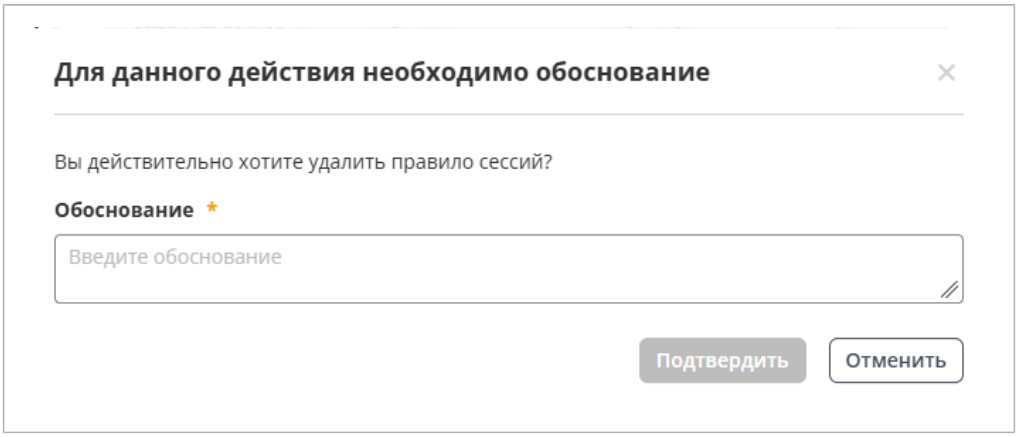


Рис. 318. Обоснование удаления правила сессий

- **Результат шага:** в правом верхнем углу страницы появится уведомление: Правило сессий успешно удалено. Правило удалится из списка правил сессий и на сенсоре.

Подсказка:

Правило также можно удалить следующим способом:
- В списке правил наведите курсор на правило, которое хотите удалить.
- Справа в строке с правилом нажмите на (**Удалить**).
- Введите текст обоснования удаления правила и нажмите **Подтвердить**.

2. Для удаления нескольких правил:
   a. В списке правил на странице **Инспекция сети → Правила сессий** установите чекбоксы возле необходимых правил.
   б. В открывшемся внизу меню нажмите
   - **Результат шага:** откроется окно обоснования удаления правил сессий.

   в. Введите текст обоснования удаления правил и нажмите **Подтвердить**.
   - **Результат шага:** правила удалятся из списка правил сессий и на сенсорах.

15.5. Правила контроля тегов

Контроль тегов обеспечивает мониторинг технологических параметров АСУ ТП в реальном времени. Это позволяет оперативно выявлять отклонения от заданных условий, предотвращать сбои и повышать стабильность технологических процессов.

Контроль тегов осуществляется с помощью правил, создаваемых пользователями с ролями `Администратор` и `Инженер`, на странице **Инспекция сети** → **Правила контроля тегов**.

При отклонении значения тега от условий, заданных в правиле, и при возвращении значения тега в норму создаются события на странице **События**.

Правила возможно создать для тегов следующих промышленных протоколов:

- Modbus;
- OPC UA;
- DeltaV.

В этом разделе:

- Просмотр правил контроля тегов
- Управление правилами контроля тегов
    - Фильтрация списка правил контроля тегов
    - Создание правил контроля тегов
    - Активация и деактивация правил контроля тегов
    - Редактирование правила контроля тегов
    - Удаление правила контроля тегов

15.5.1. Просмотр правил контроля тегов

Правила контроля тегов представлены в виде таблицы на странице **Инспекция сети** → **Правила контроля тегов**.

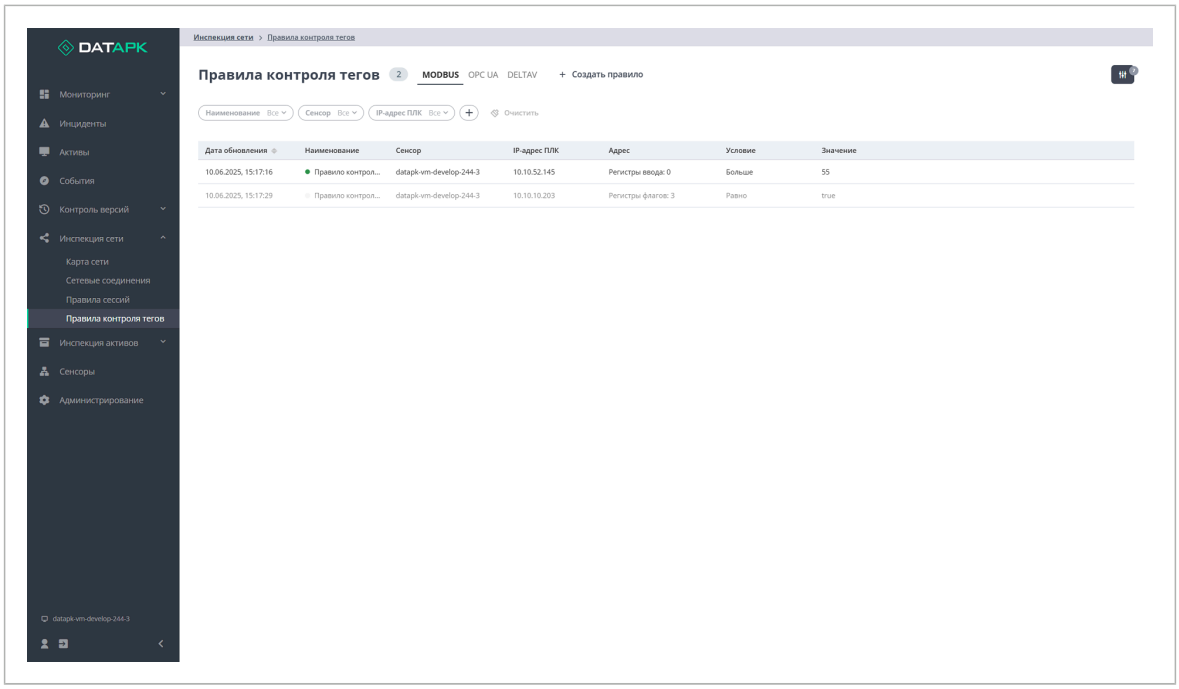


Рис. 319. Страница «Правила контроля тегов»

Справа от заголовка страницы **Правила контроля тегов** отображается количество созданных правил по выбранному протоколу.

Далее расположены вкладки протоколов:

- Modbus;
- OPC UA;
- DeltaV.

При выборе вкладки отображаются только правила, относящиеся к данному протоколу.

С помощью кнопки в правом верхнем углу страницы настраивается таблица правил контроля тегов.

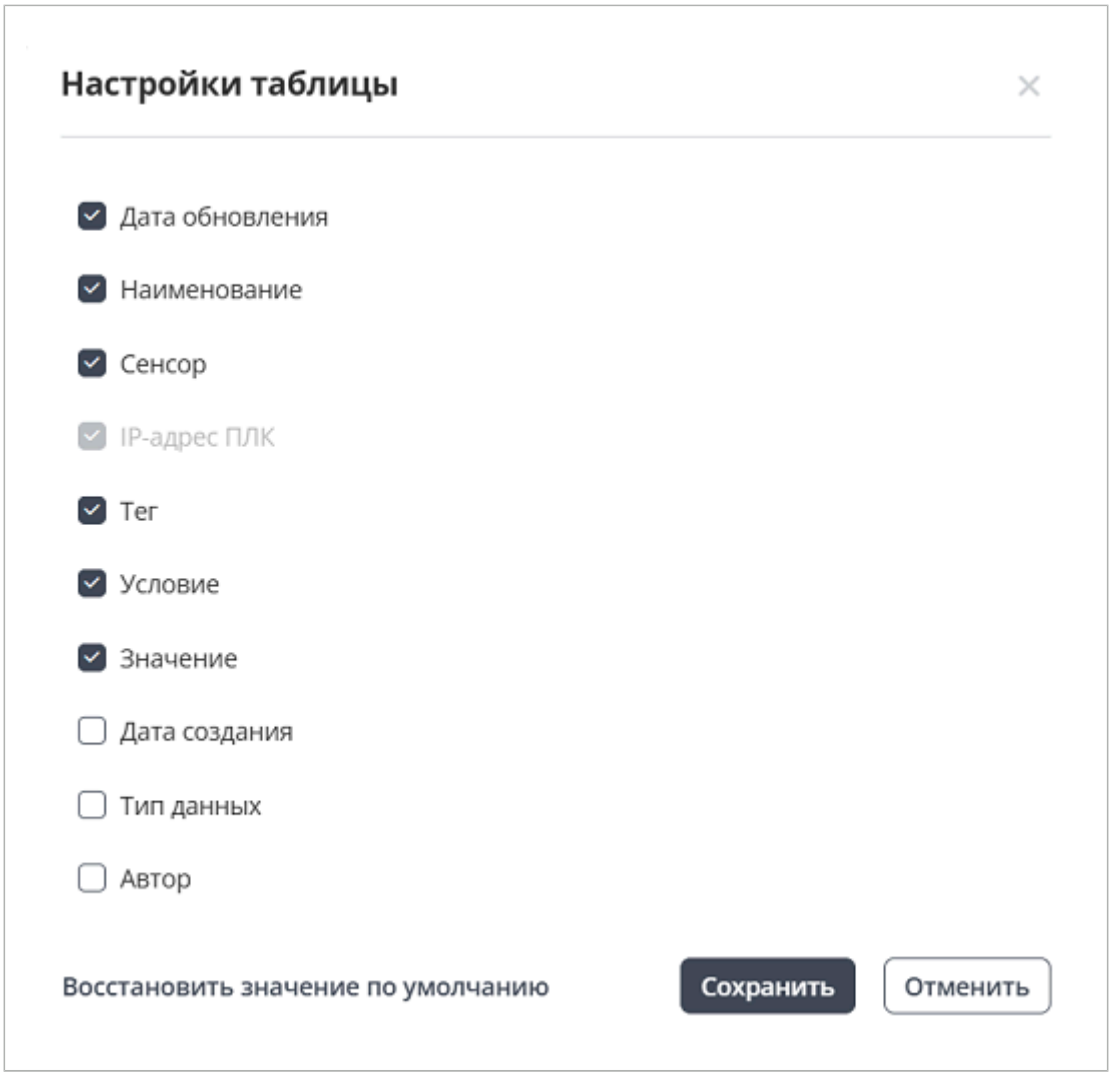


Рис. 320. Окно «Настройки таблицы»

В окне **Настройки таблицы** можно выбрать, какие столбцы и в каком порядке отображать в таблице. Столбец **IP-адрес ПЛК** невозможно скрыть из таблицы. При необходимости можно восстановить вид таблицы по умолчанию. Подробнее о настройках таблицы см. в разделе «Элементы управления таблицами».

Под заголовком страницы расположена панель фильтров, предназначенная для фильтрации и поиска нужных правил. Подробнее о работе с фильтрами см. в разделе «Фильтрация списка правил контроля тегов.

По умолчанию правила в таблице сортируются по дате создания: от новых вверху списка к старым. При нажатии справа от заголовка столбца **Дата создания** правила отобразятся в обратном порядке.

При наведении курсора на строку с правилом отображаются кнопки (**Редактировать**) и (**Удалить**). С помощью них можно управлять правилами, подробнее см. в разделах «Редактирование правила контроля тегов» и «Удаление правила контроля тегов».

При нажатии в таблице на правило контроля тегов открывается карточка правила.

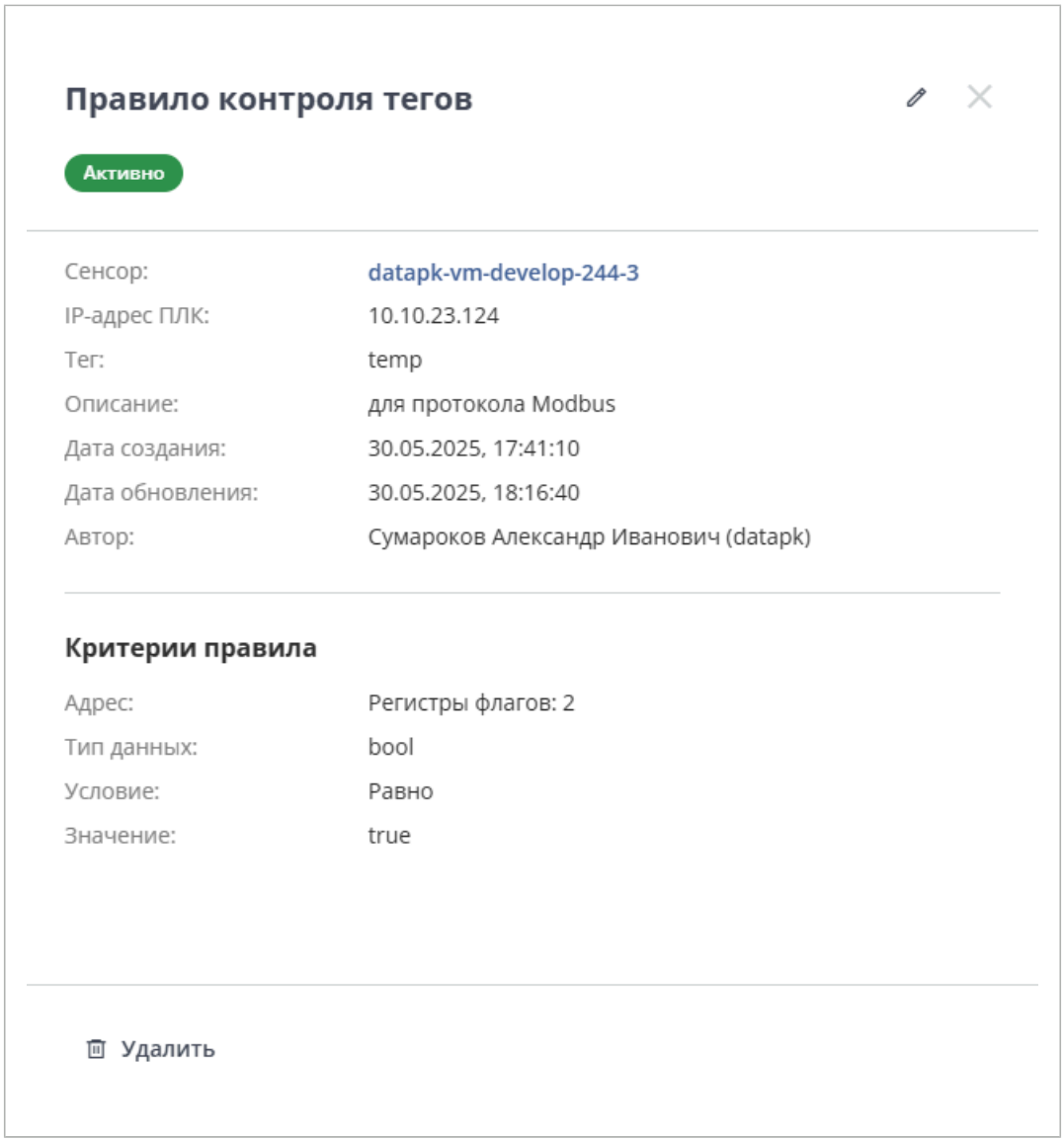


Рис. 321. Карточка правила контроля тегов

В ней представлена следующая информация:

- наименование правила;
- индикатор активности правила — показывает одно из значений: `Активно` или `Неактивно`;

> Подсказка:
>
> Активность правила меняется вручную, подробнее см. в разделе «Активация и деактивация правил контроля тегов»

- **Сенсор** — поле содержит наименование сенсора, на котором применяется правило, при нажатии на наименование открывается карточка сенсора;
- **IP-адрес ПЛК** — поле содержит IP-адрес устройства, на котором контролируется значение тега;
- **Тег** — поле содержит наименование тега, значение которого контролируется выбранным правилом;
- **Описание** — поле содержит дополнительную информацию о правиле: например, для чего создано правило;
- **Дата создания** — поле содержит дату и время создания правила;

- **Дата обновления** — поле содержит дату и время последнего изменения правила;
- **Автор** — поле содержит Ф.И.О. пользователя, создавшего правило.
- **Критерии правила** — блок содержит условия, при нарушении которых создается событие ИБ. Набор критериев отличается для каждого протокола.

15.5.2. Управление правилами контроля тегов

В этом разделе:

- Фильтрация правил контроля тегов
- Создание правил контроля тегов
- Активация и деактивация правил контроля тегов
- Редактирование правил контроля тегов
- Удаление правил контроля тегов

15.5.2.1. Фильтрация списка правил контроля тегов

Комплекс позволяет фильтровать отображаемые правила контроля тегов с помощью фильтров. Панель с фильтрами находится под заголовком страницы **Правила контроля тегов**.

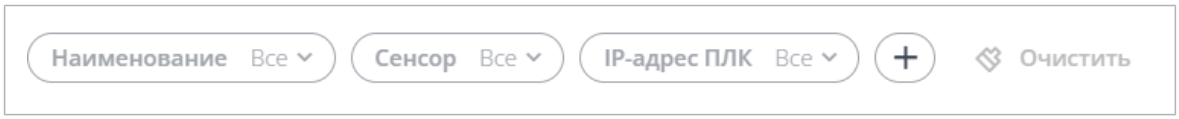


Рис. 322. Панель фильтров на странице «Правила контроля тегов»

Фильтры настраиваются отдельно для каждой вкладки протоколов, расположенных справа от заголовка страницы, и применяются только к правилам этой вкладки.

Для добавления фильтров на страницу нажмите кнопку , расположенную справа от последнего фильтра — отобразится выпадающий список с доступными фильтрами. Фильтры, уже выбранные для отображения на странице, имеют серый цвет и иконку слева от названия.

Для настройки фильтра нажмите на него. Для сброса фильтра нажмите справа от него, либо нажмите **Снять выделение** в фильтрах с выбором нескольких значений. Для сброса результатов по всем фильтрам нажмите Очистить. Чтобы применить настройки фильтра, нажмите в нем или Применить либо клавишу **Enter**, в фильтрах **Дата создания** и **Дата обновления** нажмите на пустое пространство вне фильтра.

По умолчанию отображаются следующие фильтры:

- **Наименование** — фильтрация выполняется по полному и частичному названию правила.

> Подсказка:
>
> Поле **Наименование** является регистронезависимым.

- **Сенсор** — фильтр содержит наименования сенсоров, подключенных к Комплексу. Можно выбрать несколько наименований из списка. При применении фильтра отобразятся правила, применяемые на выбранных сенсорах.
- **IP-адрес ПЛК** — фильтрация выполняется по IP-адресу ПЛК. IP-адрес необходимо вводить полностью.

Дополнительно можно добавить и настроить следующие фильтры:

- **Дата обновления** — фильтрация выполняется по указанному временному периоду последнего изменения правила контроля тегов. Нажатием на число в календаре фильтра можно выбрать начальную и конечную даты. Также для фильтрации можно указать текущие сутки, нажав на текущую дату внизу выпадающего окна фильтра.
- **Дата создания** — фильтрация выполняется по правилам контроля тегов, созданным в указанный временной период. Нажатием на число в календаре фильтра можно выбрать начальную и конечную даты. Также для фильтрации можно указать текущие сутки, нажав на текущую дату внизу календаря.
- **Тег** — фильтрация выполняется по полному и частичному наименованию тега. Можно ввести несколько наименований через запятую.

> Подсказка:
>
> Поле **Тег** является регистронезависимым.

> Прим.:
>
> При одновременном использовании двух и более фильтров будут отображены правила, удовлетворяющие всем заданным параметрам.

См. также

Просмотр правил контроля тегов

15.5.2.2. Создание правил контроля тегов

Для создания правила контроля тегов:

1. Перейдите на страницу **Инспекция сети → Правила контроля тегов**.
2. Вверху страницы выберите вкладку протокола, по которому будет передаваться значение тега:

Рис. 323. Вкладки протоколов

   - **Результат шага:** отобразится список правил контроля тегов для выбранного протокола.
3. Нажмите кнопку **Создать правило** рядом с вкладками протоколов.
   - **Результат шага:** справа откроется окно создания правила.
4. В открывшемся окне задайте следующие параметры:
   - наименование создаваемого правила;

     > Прим.:
     >
     > Наименование должно быть уникальным.

   - активность правила с помощью чекбокса **Активировать правило контроля тегов**: если чекбокс установлен (☑) — правило активно;
   - сенсор, на котором будет применяться правило;

- IP-адрес ПЛК;
- наименование тега;
- описание правила — например, дополнительная информация о правиле или рекомендации по его использованию;
- критерии правила.

> Прим.:
>
> Набор критериев зависит от выбранного протокола.

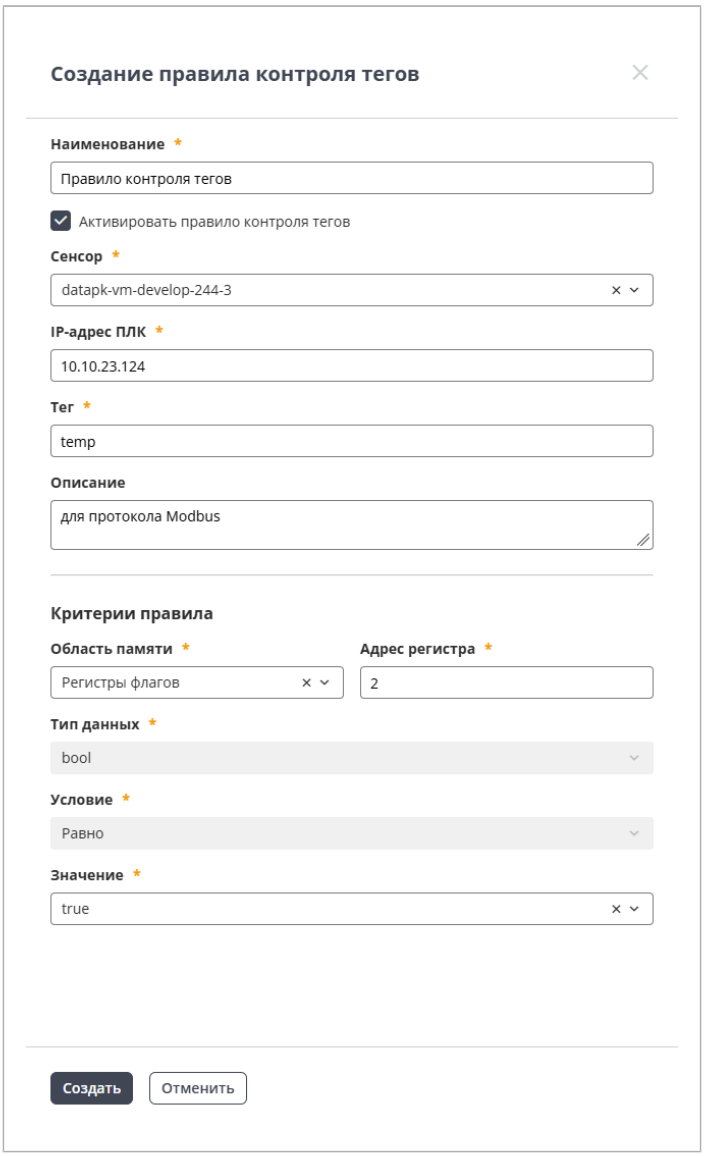


Рис. 324. Окно «Создание правила контроля тегов»

5. Нажмите кнопку **Создать** для подтверждения создания правила.
   - **Результат шага:** в правом верхнем углу страницы появится уведомление: `Правило контроля тегов успешно создано`. Созданное правило отобразится в списке правил на странице **Правила контроля тегов**.

15.5.2.3. Активация и деактивация правил контроля тегов

Деактивация позволяет приостановить работу правила, не удаляя его.

Для активации или деактивации правила:

1. Перейдите на страницу **Инспекция сети → Правила контроля тегов**.
2. Вверху страницы выберите вкладку протокола, к которому относится нужное правило.

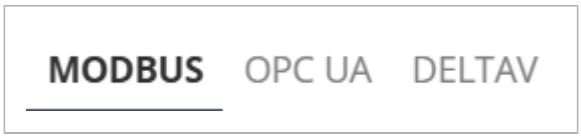


Рис. 325. Вкладки протоколов

- **Результат шага:** отобразится список правил контроля тегов для выбранного протокола.

3. Выберите из списка правило, которое хотите активировать или деактивировать.
   - **Результат шага:** справа откроется карточка правила контроля тегов.

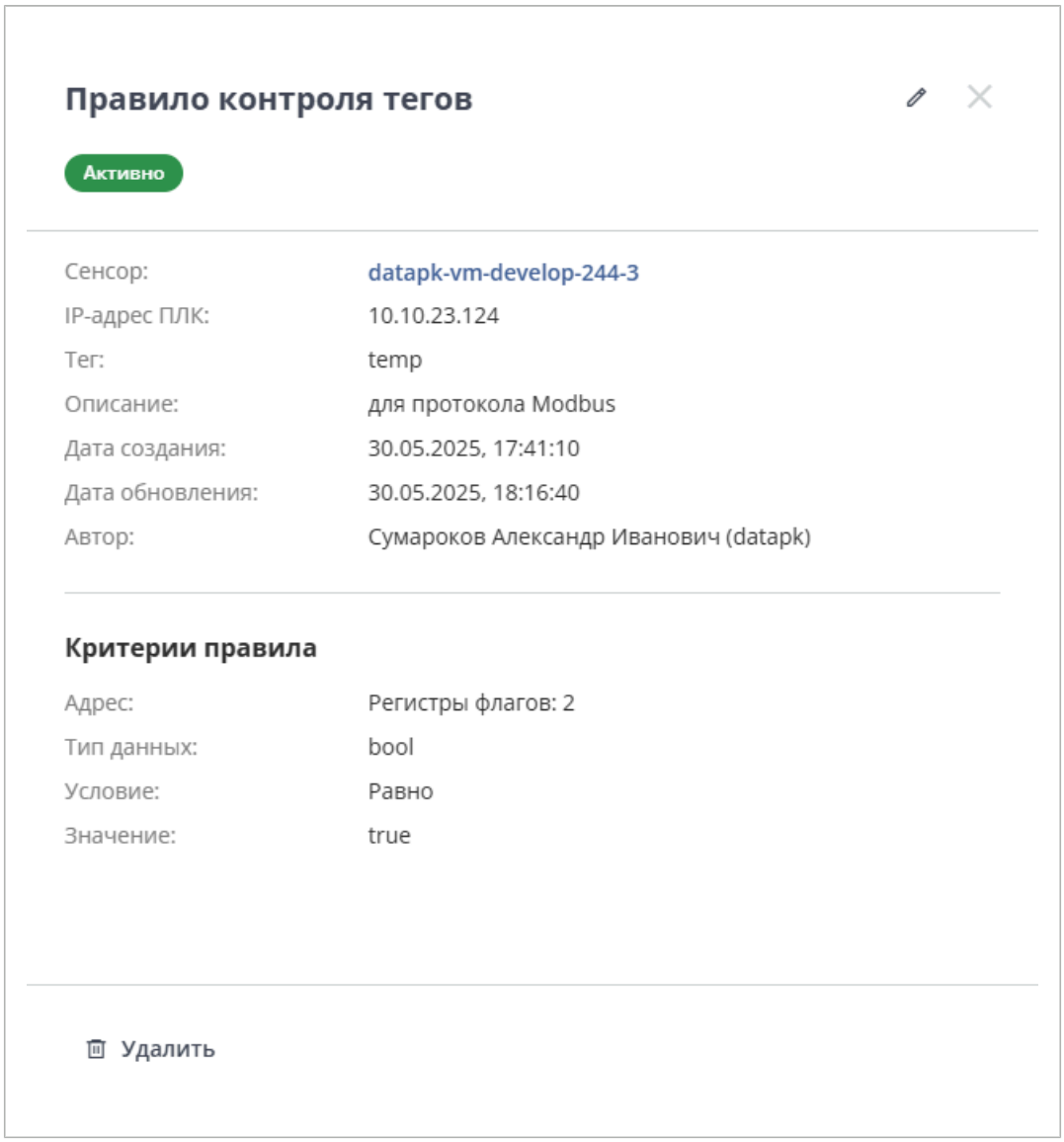


Рис. 326. Карточка правила контроля тегов

4. Вверху карточки нажмите (**Редактировать**).
   - **Результат шага:** откроется окно **Редактирование правила контроля тегов**.

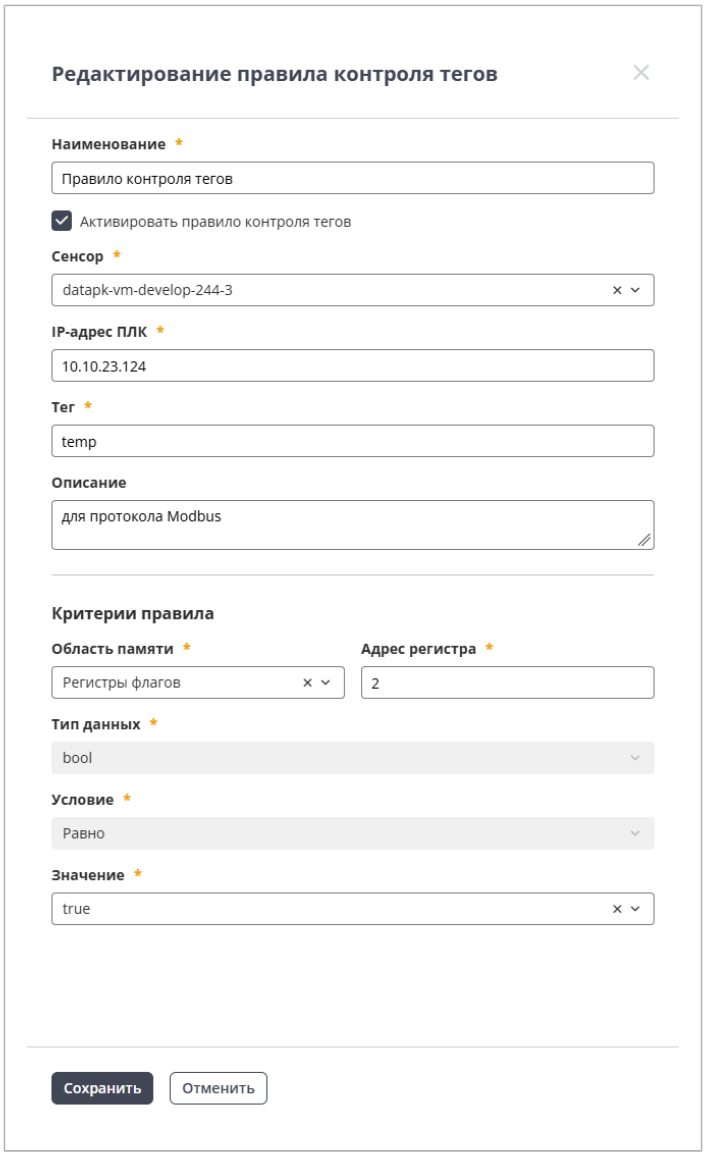


Рис. 327. Окно «Редактирование правила контроля тегов»

5. В открывшемся окне активируйте или деактивируйте правило контроля тегов с помощью чекбокса **Активировать правило контроля тегов**: если чекбокс установлен (☑) — правило активно; не установлен (☐) — правило неактивно.
6. Нажмите кнопку **Сохранить** для подтверждения изменения активности правила.
   - **Результат шага:** в правом верхнем углу страницы появится уведомление: `Правило контроля тегов успешно изменено`. В карточке активированного правила отобразится иконка Активно, деактивированного правила — Неактивно.

15.5.2.4. Редактирование правила контроля тегов

Редактирование позволяет изменить правило без его удаления и повторного создания.

Для редактирования правила контроля тегов:

1. Перейдите на страницу **Инспекция сети → Правила контроля тегов**.
2. Вверху страницы выберите вкладку протокола, к которому относится нужное правило.
   - **Результат шага:** отобразится список правил контроля тегов для выбранного протокола.

3. В списке правил нажмите на правило, которое хотите изменить.
   - **Результат шага:** справа откроется карточка правила.

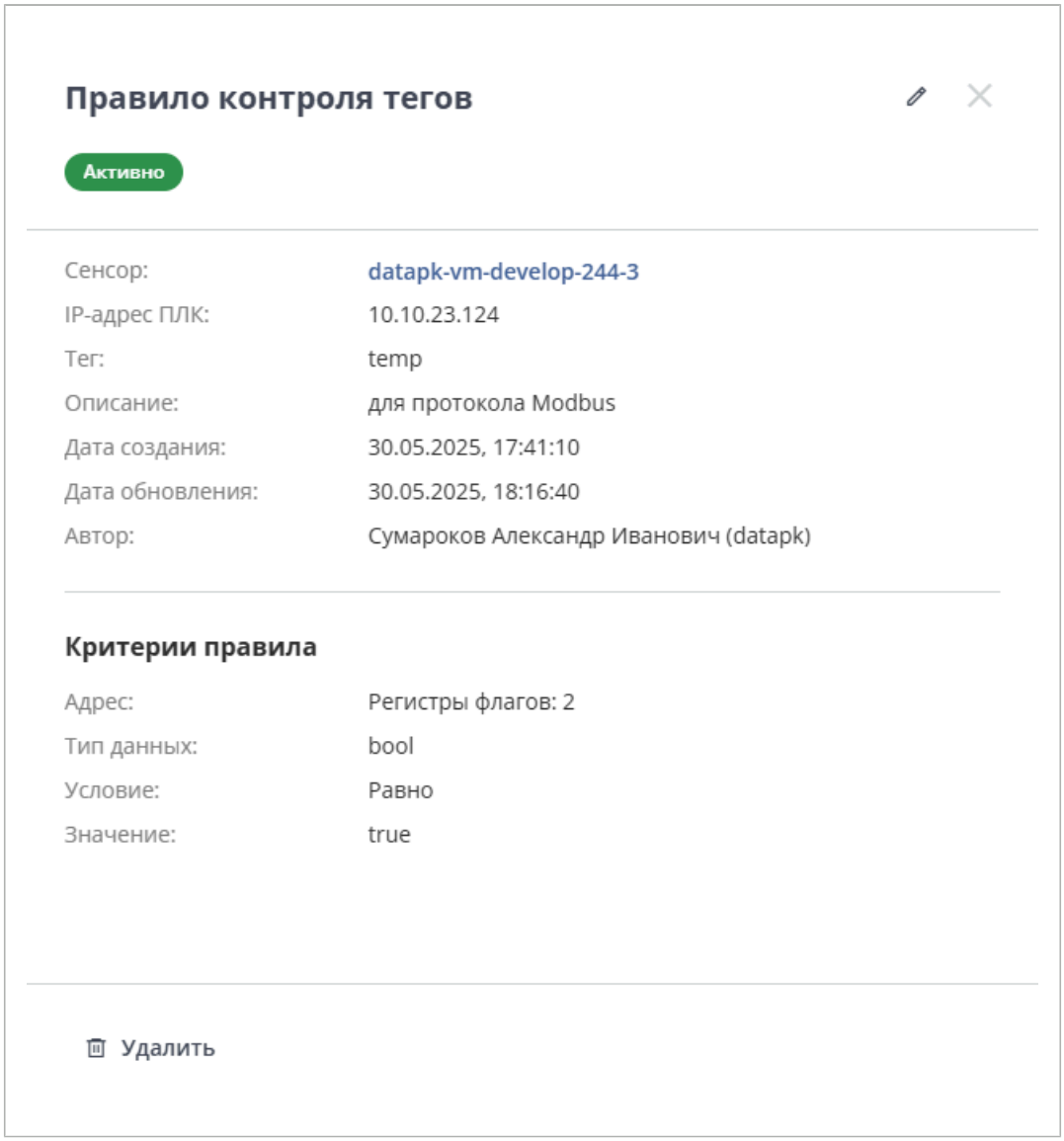


Рис. 328. Карточка правила контроля тегов

4. Вверху карточки нажмите (**Редактировать**).
   - **Результат шага:** откроется окно **Редактирование правила контроля тегов**.

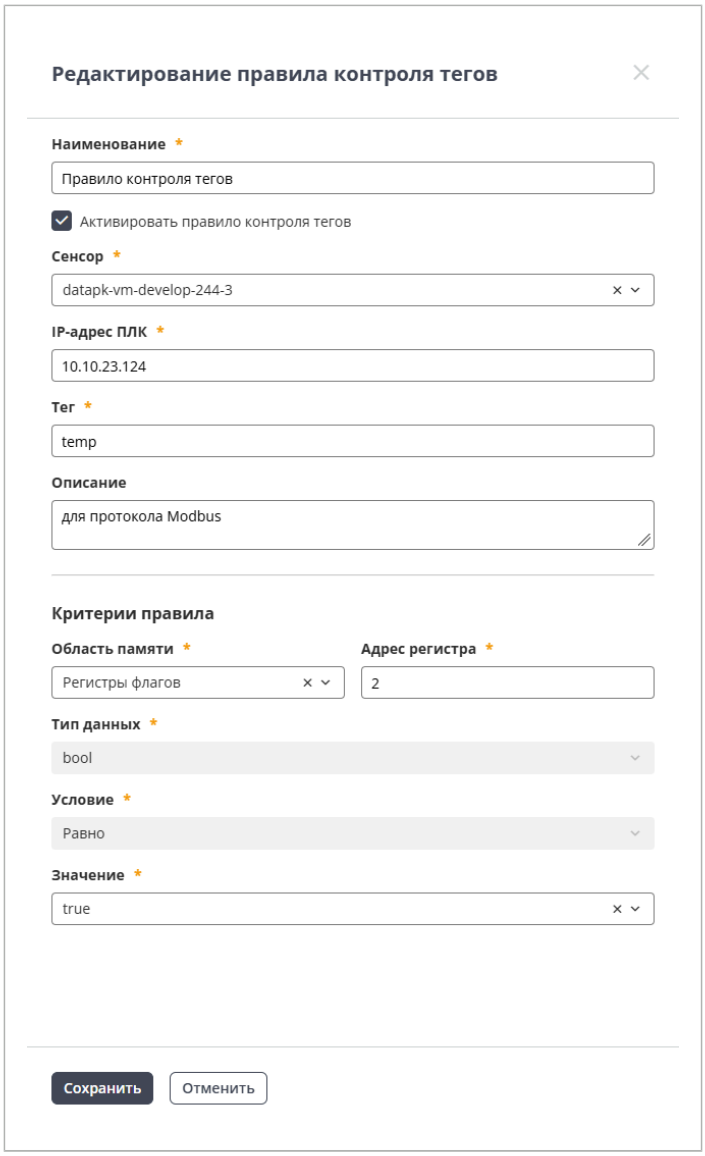


Рис. 329. Окно «Редактирование правила контроля тегов»

5. В открывшемся окне измените необходимые параметры и нажмите **Сохранить** для подтверждения внесенных изменений.
   - **Результат шага:** в правом верхнем углу страницы появится уведомление: `Правило контроля тегов успешно изменено`.

15.5.2.5. Удаление правила контроля тегов

> Внимание:
>
> Удаленное правило контроля тегов невозможно восстановить. Перед удалением убедитесь, что правило больше не требуется.

Для удаления правила контроля тегов:

1. Перейдите на страницу **Инспекция сети → Правила контроля тегов**.
2. В верхней панели страницы выберите протокол, к которому относится правило.
3. В появившемся списке нажмите на правило, которое хотите удалить.

- **Результат шага:** справа откроется карточка правила.

4. Внизу открывшейся карточки нажмите **Удалить** для подтверждения удаления правила.
5. Введите текст обоснования удаления правила и нажмите **Подтвердить**.

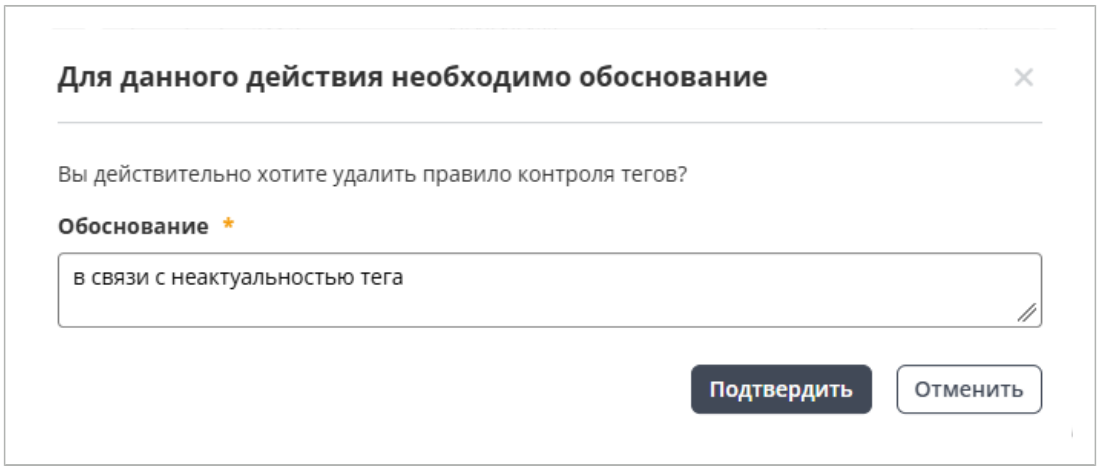


Рис. 330. Обоснование удаления правила контроля тегов

- **Результат шага:** в правом верхнем углу страницы появится уведомление: `Правило контроля тегов успешно удалено`. Правило удалится из списка правил контроля тегов и на сенсоре.

15.6. Контроль критичных функций технологического процесса

Критичные функции технологического процесса — это функции техпроцесса, изменение которых может привести к авариям, человеческим и финансовым потерям на производстве. К таким функциям можно отнести, например, запуск или останов ПЛК, загрузку или выгрузку ПО.

Преднастроенный список критичных функций расположен в файле `/usr/share/udv/zeek-wrapper/configs/ics-function.dat` Пользователь с ролью `Администратор` или `Инженер` может самостоятельно настраивать конфигурацию файла, указывая в нем, какие из выявляемых функций **модулю** считать критичными (см. инструкцию «Изменение списка критичных функций»). Со списком поддерживаемых функций вы можете ознакомиться в разделе «Поддерживаемые функции промышленных протоколов».

При обнаружении в контролируемой сети функций, заданных в конфигурационном файле `ics-function.dat`, создается событие с типом `dpi_notice` на странице **События**. Появлением событий можно управлять с помощью запуска и отключения сервиса регистрации событий техпроцесса, подробнее см. инструкцию «Управление сервисом регистрации событий техпроцесса».

В этом разделе:

- Управление сервисом регистрации событий техпроцесса
- Изменение списка критичных функций

15.6.1. Управление сервисом регистрации событий техпроцесса

Активация и деактивация сервиса, отвечающего за создание событий и оповещений при обнаружении критичных функций техпроцесса в контролируемой сети.

Для активации или деактивации сервиса регистрации событий техпроцесса:

1. Перейдите на страницу **Сенсоры**.
2. Выберите сенсор, на котором хотите активировать или деактивировать сервис регистрации событий техпроцесса.

- **Результат шага:** справа откроется карточка сенсора.

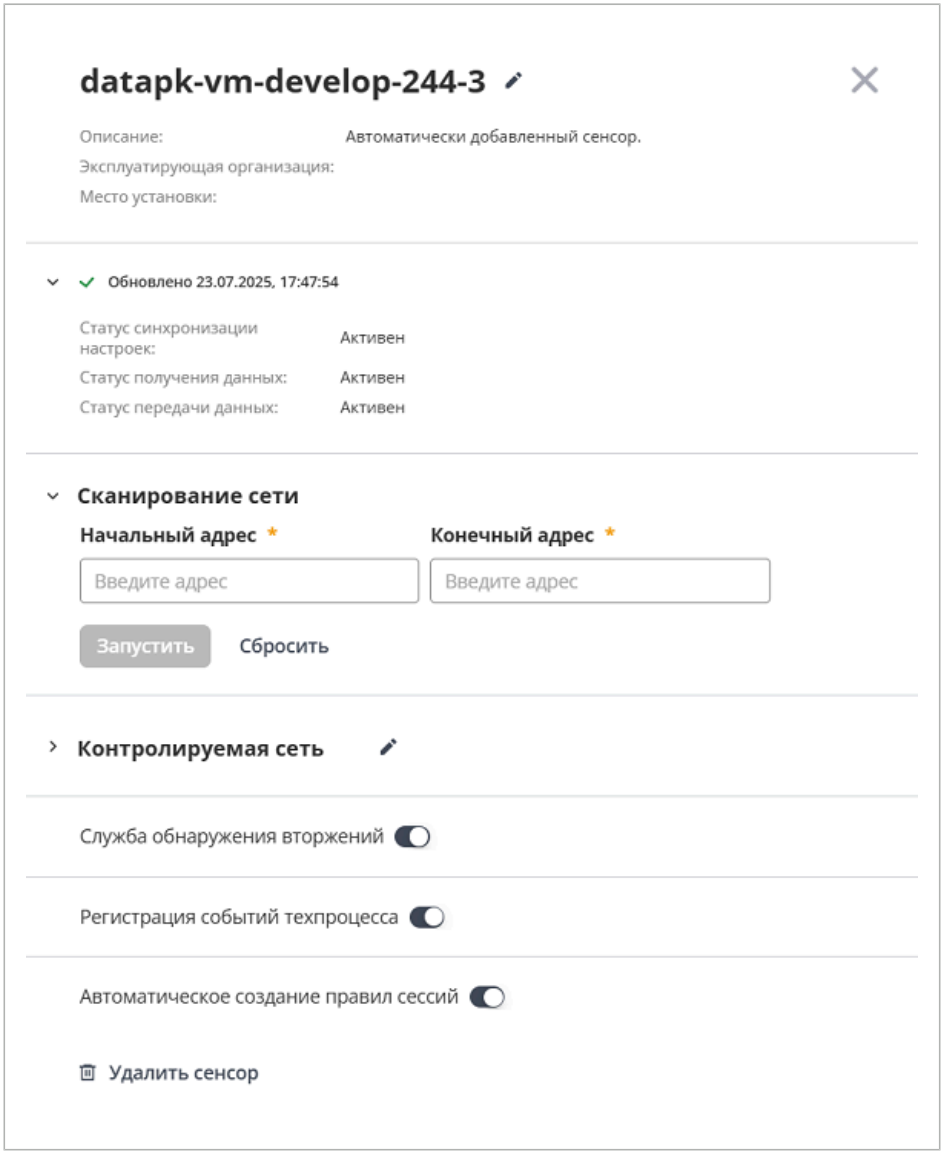


Рис. 331. Карточка сенсора

3. В открывшейся карточке в разделе **Контролируемая сеть** активируйте или деактивируйте сервис регистрации событий техпроцесса с помощью переключателя **Регистрация событий техпроцесса**: если он установлен вправо ( ) — сервис активен, влево ( ) — неактивен.

15.6.2. Изменение списка критичных функций

Любую поддерживаемую модулем функцию техпроцесса можно назначить критичной или управляющей, добавив или исключив из конфигурационного файла `ics-function.dat`. Функции, указываемые в этом файле, модуль определяет как критичные, и при их обнаружении в трафике промышленных протоколов создается событие ИБ. Функции из раздела «Поддерживаемые функции промышленных протоколов», не указанные в конфигурационном файле, считаются управляющими и при обнаружении не создают события ИБ.

Для изменения списка критичных функций:

1. Откройте на редактирование файл `ics-function.dat`:

```
mcedit /usr/share/udv/zeek-wrapper/configs/ics-function.dat
```

2. В открывшемся файле в строке с нужным протоколом добавьте или удалите функцию:
   a. При добавлении функций протокола `IEC104` соблюдайте формат записи:

```
IPAM: :[протокол]_critical_function [функция] [описание],[функция_2] [описание_2]
```

   При добавлении функций других протоколов соблюдайте формат записи:

```
IPAM: :[протокол]_critical_function [функция],[функция_2]
```

   Где:

   - `IPAM: :[протокол]_critical_function` — обязательный для каждого протокола префикс;
   - `[функция]`, `[описание]` — соответствующие значения из раздела «Поддерживаемые функции промышленных протоколов».

> Внимание:
>
> Регистр наименования функции и ее описания должен соответствовать регистру из указанного раздела.
>
> Между обязательным префиксом, функцией и ее описанием ставится пробел или табуляция.
>
> Если у протокола несколько функций, они разделяются запятой, без пробела.

   Примеры записей:

```
IPAM: :dnp3_critical_function ASSIGN_CLASS,UNSOLICITED_RESPONSE,FREEZE_AT_TIME_NR
IPAM: :iec104_critical_function C_BO_NA_1 bit string 32 bit,M_EP_TA_1 event of
 protection equipment with time tag
```

   б. Чтобы удалить функцию из файла, выделите ее (у протокола `IEC104` выделите функцию вместе с описанием) и нажмите клавишу **Delete**, **Del** или **Backspace**.

> ОСТОРОЖНО:
>
> Префикс и пробел после него в начале записи каждого протокола являются обязательными:
>
> ```
> IPAM: :[протокол]_critical_function
> ```
>
> Их изменение или удаление, даже при отсутствии функций, может привести к некорректной обработке конфигурационного файла.

3. Сохраните внесенные изменения, нажав клавишу **F10**, и подтвердите сохранение изменений, выбрав **Да** или **Yes**.

См. также

Поддерживаемые функции промышленных протоколов

Управление сервисом регистрации событий техпроцесса

15.7. Служба обнаружения вторжений

В этом разделе:

- Создание правил обнаружения вторжений
- Управление службой обнаружения вторжений
- Экспорт и импорт правил службы обнаружения вторжения
- Импорт правил обнаружения вторжений в формате *.json
- Импорт правил обнаружения вторжений в формате *.rules
- Экспорт правил службы обнаружения вторжений
- Создание исключений для правил обнаружения вторжений
- Удаление исключений для правил обнаружения вторжений

Правила обнаружения вторжений

Служба обнаружения вторжений позволяет обнаруживать подозрительную сетевую активность, сравнивая встроенные правила обнаружения вредоносного трафика с данными, проходящими по локальной сети.

Правила обнаружения вторжений расположены во вкладке **Правила** на странице **Правила обнаружения**.

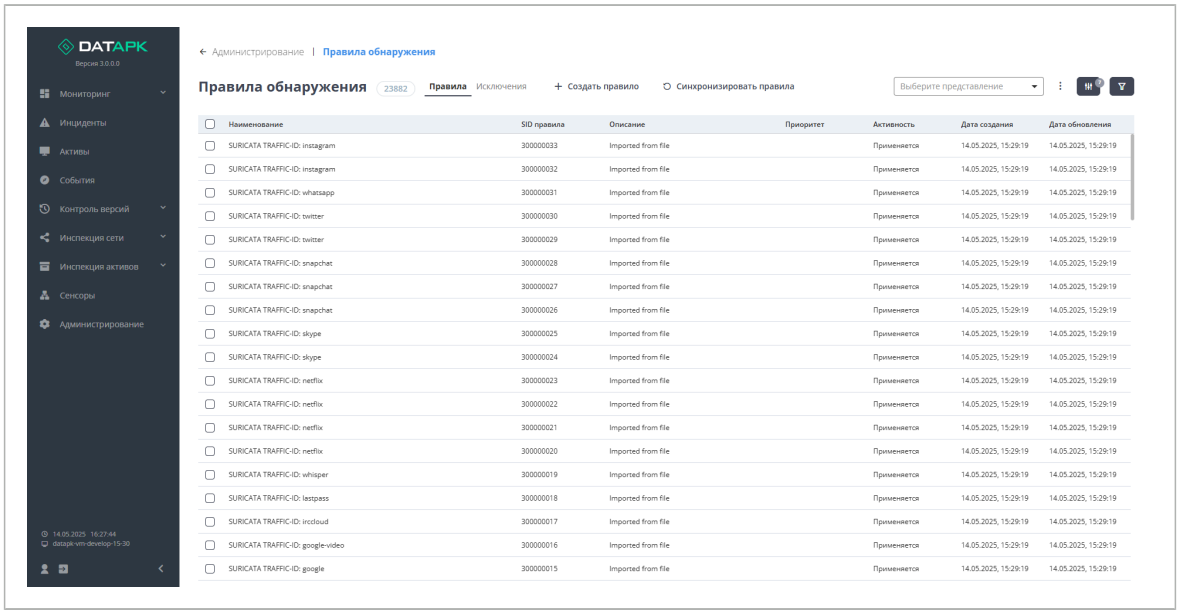


Рис. 332. Страница «Правила обнаружения»

Правила обнаружения состоят из заголовка и опций. Заголовок содержит следующую информацию:

- описание действия;
- протокол передачи данных;
- IP-адреса;
- сетевые маски;
- порты источника и назначения.

После заголовка правила следуют опции. Они включают определение дополнительных критериев выполнения правила и определение дополнительных реагирующих действий. Они используются для организации более направленной фильтрации трафика. Весь набор опций заключается в круглые скобки, сами опции отделяются друг от друга с помощью точки с запятой (последняя опция в списке тоже должна заканчиваться данным символом). Ключевые слова опций отделяются от своих аргументов двоеточием.

Синтаксис записи правил в формате Suricata:

```
[Действие] [Протокол] [IP-адреса отправителей] [Порты отправителей] [Оператор направления] [IP-адреса получателей] [Порты получателей] (ключ_1 : значение_1; ключ_2 : значение_2; ... ключ_N : значение_N;)
```

Пример содержимого файла с правилами обнаружения формата Suricata:

```
# test rule that catches all ICMP packets:
alert icmp any any -> any any (msg:"ICMP test detected"; GID:1; sid:11111111; rev:001; classtype:icmp-event;)
# rules for S7
alert tcp any any -> any 102 (msg:"Response (when error)"; content:"|02|"; offset:17; depth:1; sid:10000001; rev:001; priority:10;)
alert tcp any any -> any 102 (msg:"Read area"; content:"|04|"; offset:17; depth:1;sid:10000002; rev:001; priority:10;)
```

Веб-интерфейс Комплекса позволяет загрузить правила обнаружения несколькими способами:

- создавать запись о новом правиле вручную на странице **Правила обнаружения**;
- импортировать файл формата Suricata с расширением `*.rules`, содержащий список правил;
- импортировать файл формата `*.json`, содержащий список правил.

Зарегистрированные службой обнаружения вторжений события отображаются в списке событий на странице **События**, а также на панелях мониторинга. Подробнее см. раздел «Обнаружение вторжений».

Пользователь с ролью `Администратор` может фильтровать правила на странице **Правила обнаружения** по следующим признакам:

- статус активности — только активные или только неактивные правила;
- дата и время создания правила;
- дата и время обновления правила;
- тип правила — значение поля `classtype` (для правил без типа это поле имеет значение `Без типа`);
- приоритет — Очень низкий, Незначительный, Низкий, Средний, Высокий, Без приоритета.

> Внимание:
>
> В событиях от службы обнаружения вторжений (поле `event_type` в таких событиях имеет значение `ids_event`) Комплекс может менять местами IP-адреса отправителя и получателя. Корректный адрес можно посмотреть по ссылке **Сессия** вверху карточки интересующего события на странице **События**.

Исключения для правил обнаружения вторжений

Также пользователь с ролью `Администратор` может создавать исключения для правил обнаружения вторжений для того, чтобы исключить определенные правила, которые не должны работать на одном выбранном сенсоре.

Исключения для правил обнаружения вторжений расположены во вкладке **Исключения** на странице **Правила обнаружения**.

Исключения можно отфильтровать по следующим признакам:

- дата и время создания исключений;
- автор — пользователь, создавший исключения;
- сенсор — сенсор, на котором применяются исключения;

- SID правил — идентификаторы правил обнаружения вторжений, для которых были созданы исключения.

> Внимание:
>
> В фильтре **SID правил** можно указать как один идентификатор правила, так и определенный диапазон идентификаторов правил через тире.

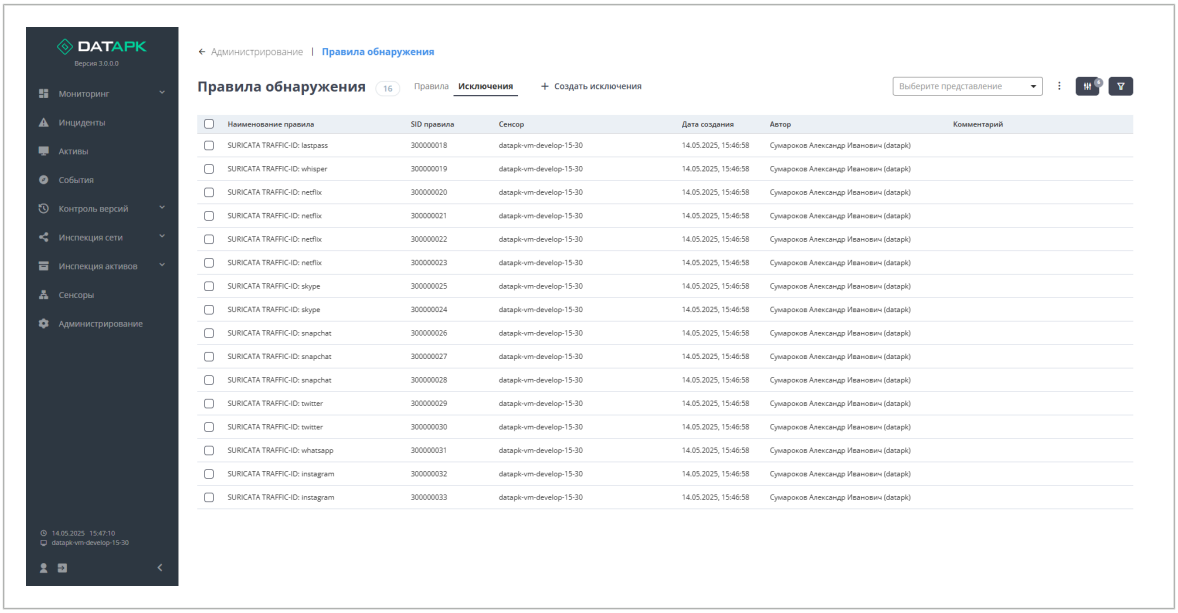


Рис. 333. Вкладка «Исключения» на странице «Обнаружение вторжений»

> Внимание:
>
> Для создания исключения с более точными сетевыми параметрами (например, с определенным IP-адресом) необходимо вручную создавать pass-правило обнаружения вторжений (подробнее см. в разделе «Создание исключения путем создания правила обнаружения вторжений на конкретные IP-адреса»).

15.7.1. Создание правил обнаружения вторжений

Для создания правил обнаружения в веб-интерфейсе Комплекса:

1. Перейдите на страницу **Администрирование → Правила обнаружения**.
2. Нажмите кнопку **Создать правило**. В открывшемся окне задайте следующие параметры:
   - наименование и описание создаваемого правила;
   - правило обнаружения в формате Suricata в поле **Условие**;

> Внимание:
>
> Убедитесь, что уникальный идентификатор сигнатуры (sid) не совпадает с sid других правил, загруженных ранее в Комплекс. Рекомендуемый диапазон пользовательских правил: от 94000000 до 94999999.

   - активность правила с помощью чекбокса **Активность**: если чекбокс установлен — правило активно.

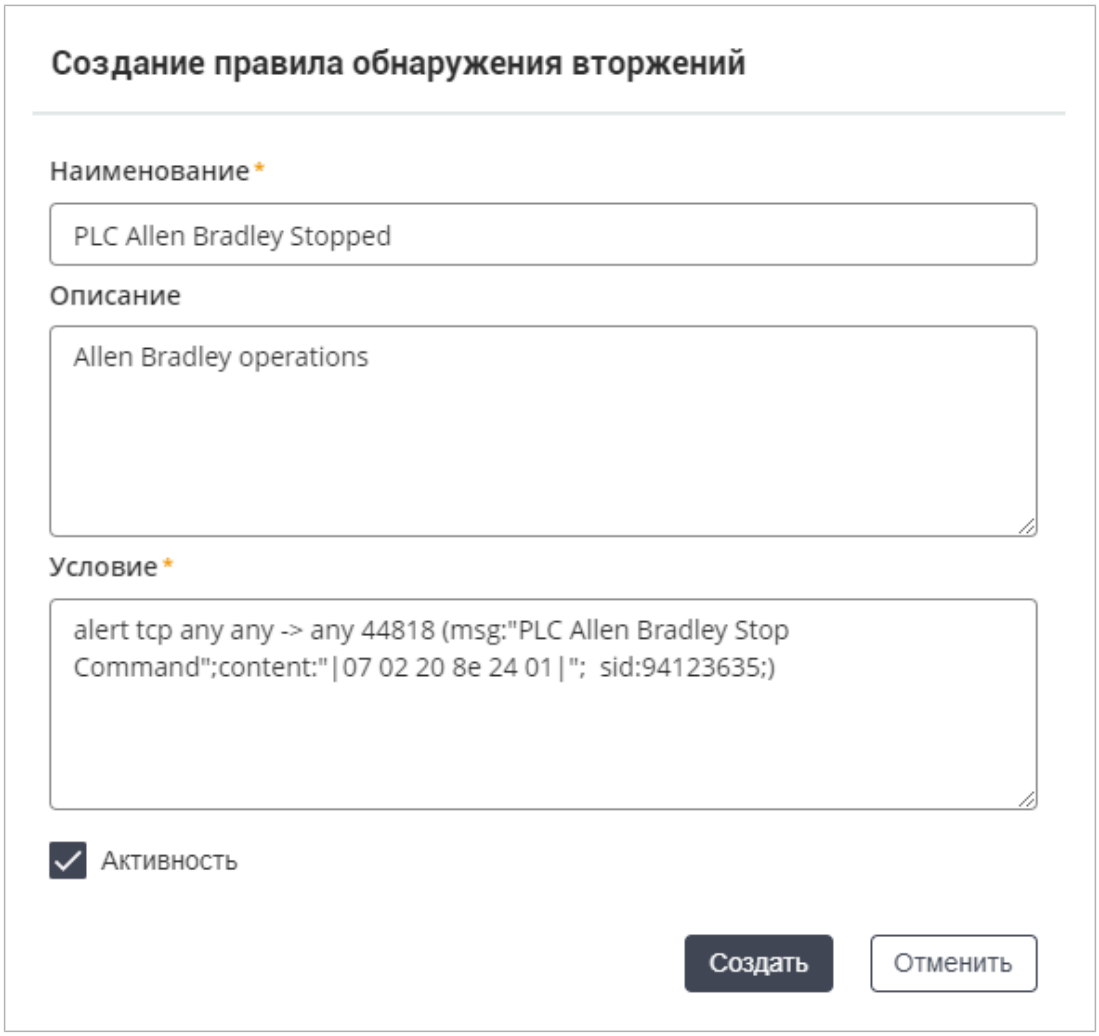


Рис. 334. Окно «Создание правила обнаружения вторжения»

3. Нажмите кнопку **Создать** для подтверждения создания правила.

15.7.2. Управление службой обнаружения вторжений

Доступны следующие действия со службой обнаружения вторжений:

- Запуск и остановка службы обнаружения вторжений на сенсорах
- Активация и деактивация правил обнаружения вторжений
- Редактирование правил обнаружения вторжений
- Изменение правила с SID в диапазоне, отличающемся от пользовательского
- Удаление правил обнаружения вторжений, синхронизация правил

Внимание:

При внесении изменений правила синхронизируются с сенсорами автоматически. При возникновении ошибки: `Не удалось автоматически синхронизировать правила на сенсорах. Синхронизируйте правила`

вручную по кнопке «Синхронизировать правила» нажмите кнопку Синхронизировать правила для принудительной синхронизации правил.

15.7.2.1. Запуск и остановка службы обнаружения вторжений на сенсорах

Для запуска или остановки службы на сенсорах:

1. Перейдите на страницу **Сенсоры**.
2. Нажмите на строку с сенсором, для которого нужно проверить статус службы обнаружения вторжений.
   - **Результат шага:** справа откроется карточка выбранного сенсора.
3. В открывшейся справа карточке включите или выключите службу обнаружения вторжений сенсора с помощью переключателя: если переключатель в состоянии — служба включена.

15.7.2.2. Активация и деактивация правил обнаружения вторжений

При работе с правилами обнаружения вторжений их можно активировать или деактивировать. Доступна активация и деактивация как одного, так и нескольких правил.

1. Для активации или деактивации одного правила:
   a. Перейдите на страницу **Администрирование → Правила обнаружения**.
   б. Для включения одного правила нажмите на необходимое правило из списка и в открывшейся справа карточке правила нажмите кнопку Активировать в левом верхнем углу.
   в. Для отключения одного правила нажмите на необходимое правило из списка и в открывшейся карточке правила нажмите кнопку Деактивировать в верхней части карточки правила.
2. Для активации или деактивации нескольких правил:
   a. Перейдите на страницу **Администрирование → Правила обнаружения**.
   б. Для включения нескольких правил установите чекбоксы возле необходимых правил и в открывшемся внизу меню нажмите кнопку Активировать
   в. Для выключения нескольких правил установите чекбоксы возле необходимых правил и в открывшемся внизу меню нажмите кнопку Деактивировать

15.7.2.3. Редактирование правил обнаружения вторжений

Для редактирования правила:

1. Нажмите на необходимое правило из списка.
2. Нажмите (**Редактировать**) в открывшейся карточке правила.
   - **Результат шага:** появится карточка **Редактирование правила обнаружения**.
3. Измените необходимые параметры в окне **Редактирование правила обнаружения вторжений** и нажмите **Сохранить**.

> **Внимание:**
>
> Не рекомендуется редактирование правил с SID в диапазоне, отличающемся от пользовательского (`94000000-94999999`), так как такие правила могут быть заменены при импорте.

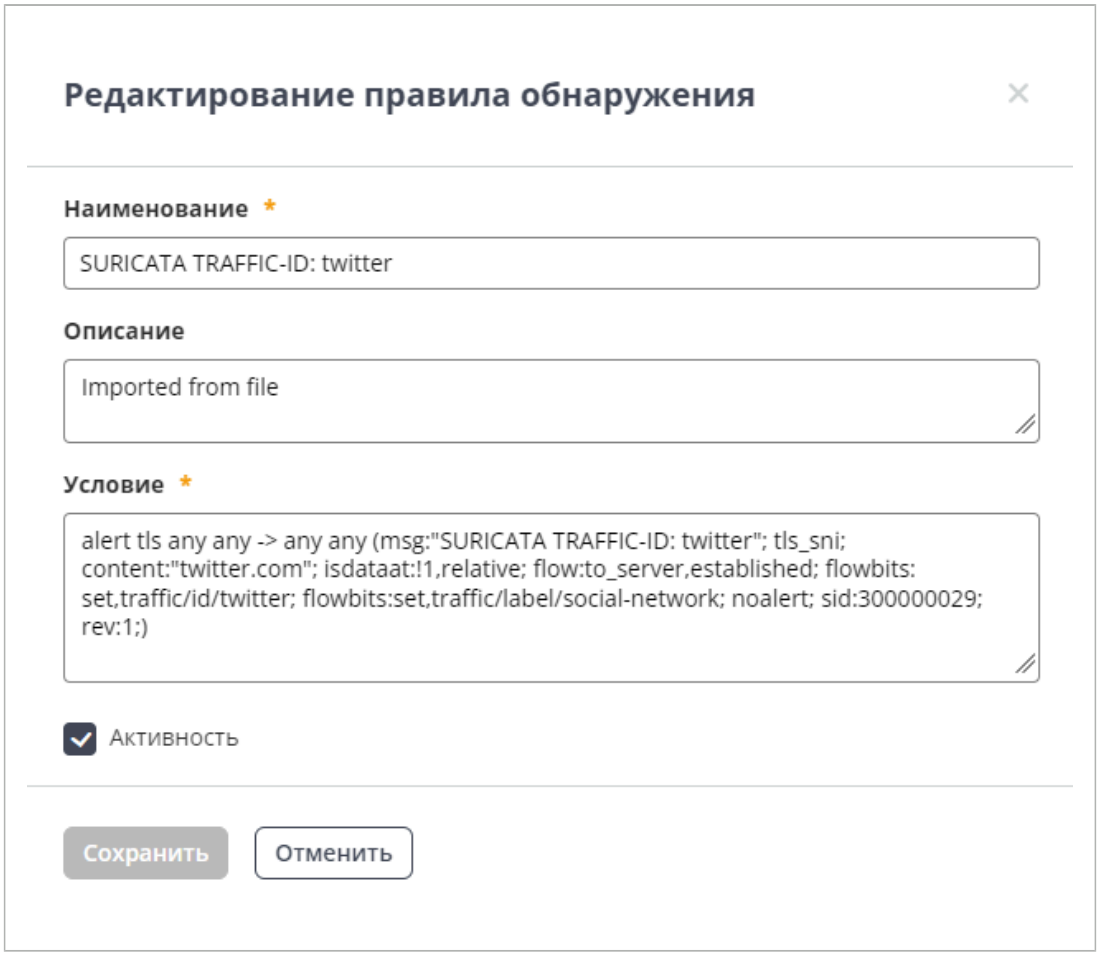


Рис. 335. Окно редактирования правила обнаружения вторжения

- **Результат шага:** отредактированное правило будет сохранено как новое правило обнаружения вторжений. Исходное правило также сохранится.

15.7.2.4. Изменение правила с SID в диапазоне, отличающемся от пользовательского

Для изменения правила с SID в диапазоне, отличающемся от пользовательского (`94000000-94999999`):

1. Нажмите на необходимое правило из списка.
2. Нажмите (**Редактировать**) в открывшейся карточке правила.
   - **Результат шага:** появится карточка **Редактирование правила обнаружения**.
3. Скопируйте значения полей окна.
4. При необходимости отмените выбор чекбокса **Активность** и нажмите **Сохранить**
5. Нажмите **Создать правило**
6. Вставьте скопированные ранее значения полей окна в соответствующие поля окна создания правила.
7. Измените sid так, чтобы он входил в пользовательский диапазон (`94000000-94999999`) и не совпадал с другими правилами.

8. Измените необходимые параметры правила.
9. Установите чекбокс **Активность**.
10. Нажмите **Создать**

    ▸ **Результат шага:** новое правило будет применяться для обнаружения вторжений. Старое правило останется в системе и может быть обновлено при импорте, но применяться не будет, если при импорте не будет активировано автоматически.

15.7.2.5. Удаление правил обнаружения вторжений, синхронизация правил

Возможно удаление как одного правила обнаружения вторжений, так и нескольких правил.

1. Для удаления одного правила:
    a. Нажмите на необходимое правило из списка.
    б. Внизу открывшейся карточки нажмите Удалить.
    в. Введите текст обоснования удаления правила и нажмите **Подтвердить**

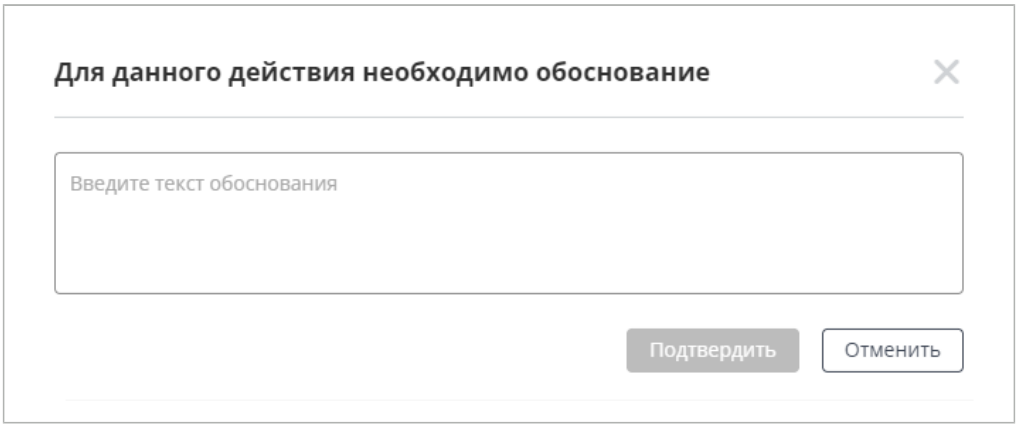


Рис. 336. Обоснование удаления правила обнаружения вторжений

▸ **Результат шага:** правило обнаружения вторжений будет удалено из сенсора.

> Подсказка:
>
> Правило также можно удалить следующим способом:
> - Установите чекбокс возле необходимого правила.
> - В открывшемся внизу меню нажмите ··· → **Удалить**.
> - Введите текст обоснования удаления правила и нажмите **Подтвердить**.

2. Для удаления нескольких правил:
    a. Установите чекбоксы возле необходимых правил.
    б. В открывшемся внизу меню нажмите ··· → (**Удалить**).
    в. Введите текст обоснования удаления правила и нажмите **Подтвердить**.

15.7.3. Экспорт и импорт правил службы обнаружения вторжения

В этом разделе:

- Импорт правил обнаружения вторжений в формате *.json
- Импорт правил обнаружения вторжений в формате *.rules
- Экспорт правил службы обнаружения вторжений

Экспорт и импорт правил обнаружения вторжений осуществляется на странице **Администрирование** → **Основные настройки** → **Импорт и экспорт** на панели **Обнаружение вторжений**.

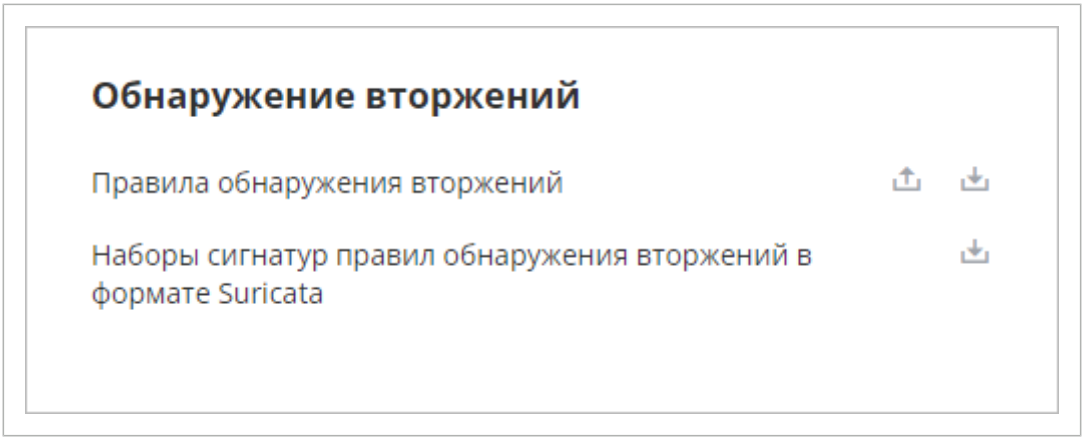


Рис. 337. Панель «Обнаружение вторжений» на странице «Импорт и экспорт»

15.7.3.1. Импорт правил обнаружения вторжений в формате *.json

Перед выполнением:

Перед импортом необходимо обратить внимание, что при импорте правил, чьи уникальные идентификаторы сигнатуры (sid) совпадают с уже загруженными правилами, будет проведена проверка на номер ревизии (rev), и возможны следующие варианты:

- если rev правила импортируемого меньше, чем в уже загруженном, новое правило не будет импортировано;
- если rev импортируемого правила больше, чем в уже загруженном, новое правило будет импортировано, старое правило будет заменено. Активность правила сохранится, если для параметра **Статус активности сигнатур после импорта** будет выбран вариант **Сохранить**.

При импорте группы правил уникальность проверяется для каждого отдельно, и неудачный импорт некоторых правил группы не повлияет на импорт других.

Для импорта файла формата `*.json` с правилами обнаружения:

1. Перейдите на страницу **Администрирование** → **Основные настройки** → **Импорт и экспорт**.
2. На панели **Обнаружение вторжений** в строке **Правила обнаружения вторжений** нажмите кнопку (**Импортировать**).
3. В открывшемся окне укажите расположение импортируемого файла формата `*.json` и подтвердите выбор.
4. В окне **Подготовка к импорту** Выбрать:

- действие для элементов, которые отсутствуют в новом (загружаемом) справочнике:
  - **Оставить** — новые элементы будут добавлены к уже существующим;

    Подсказка:

    Данный вариант рекомендован к выбору при наличии измененных правил.

  - **Удалить** — старые элементы будут удалены и добавлены новые.
- статус активности элементов справочника после импорта:
  - **Оставить как есть** — статус активности элементов справочника будет сохранен;

    Подсказка:

    Данный вариант рекомендован к выбору при наличии измененных правил.

  - **Присвоить старым статус, как в файле** — статус активности элементов справочника будет перезаписан в соответствии со значениями в импортируемом файле.

5. Нажмите **Импортировать** для запуска процедуры импорта.

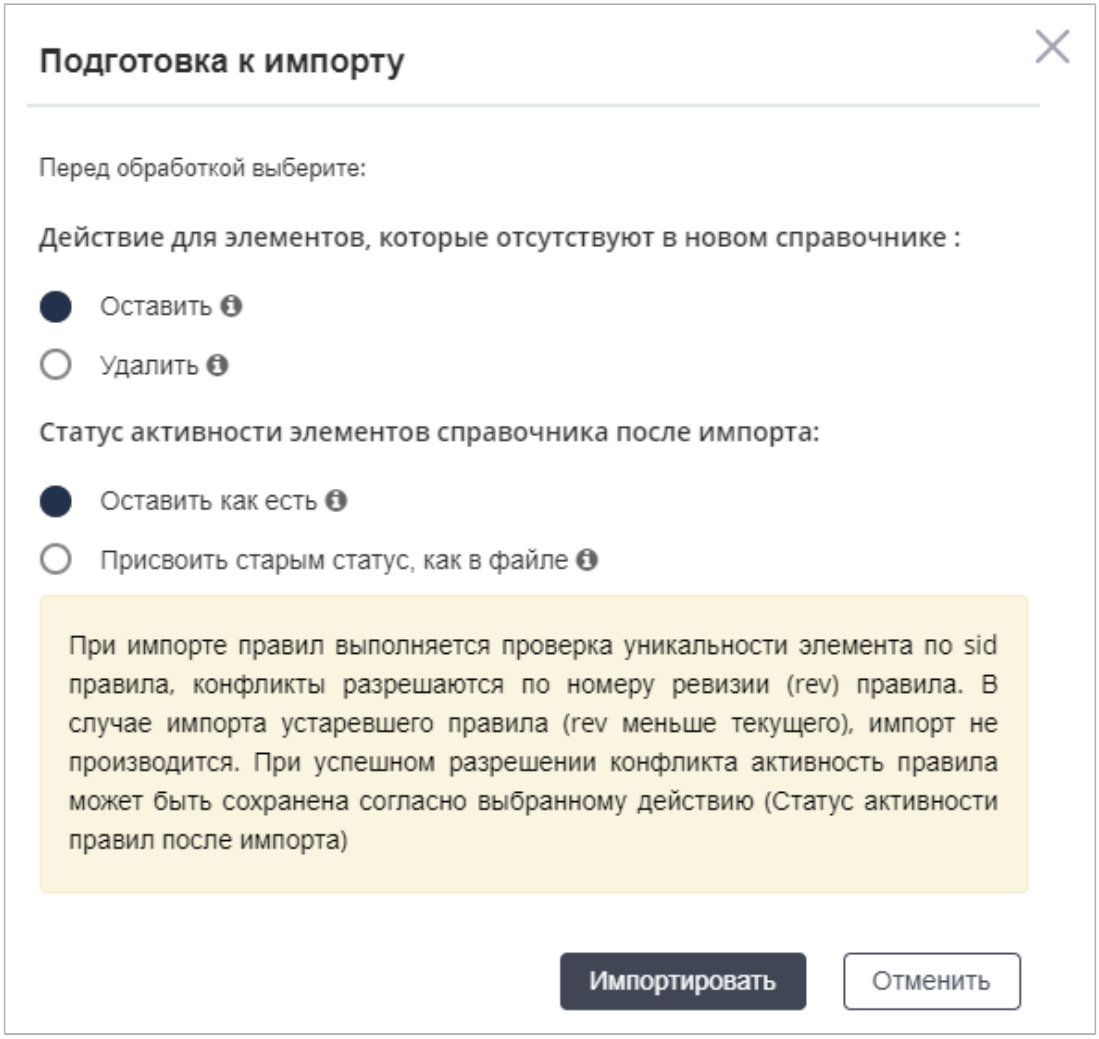


Рис. 338. Окно «Подготовка к импорту» при загрузке правил обнаружения вторжений

6. Дождитесь успешного результата импорта.

▸ **Результат шага:** сразу после загрузки файла в правом верхнем углу страницы в поле **Результат последнего импорта** появится статус `Успешно`, и правила будут загружены на страницу **Правила обнаружения**.

7. Перейдите на страницу **Правила обнаружения** и убедитесь, что правила были успешно загружены.

15.7.3.2. Импорт правил обнаружения вторжений в формате *.rules

Перед выполнением:

Перед импортом необходимо обратить внимание, что при импорте правил, чьи уникальные идентификаторы сигнатуры (sid) совпадают с уже загруженными правилами, будет проведена проверка на номер ревизии (rev), и возможны следующие варианты:

- если rev правила импортируемого меньше, чем в уже загруженном, новое правило не будет импортировано;
- если rev импортируемого правила больше, чем в уже загруженном, новое правило будет импортировано, старое правило будет заменено. Активность правила сохранится, если для параметра **Статус активности сигнатур после импорта** будет выбран вариант **Сохранить**.

При импорте группы правил уникальность проверяется для каждого отдельно, и неудачный импорт некоторых правил группы не повлияет на импорт других.

Для импорта файла формата Suricata (`*.rules`) с правилами обнаружения:

1. Перейдите на страницу **Администрирование → Основные настройки → Импорт и экспорт**.
2. На панели **Обнаружение вторжений** в поле Н**аборы сигнатур правил обнаружения вторжений в формате Suricata** нажмите кнопку (**Импортировать**).
3. В открывшемся окне укажите расположение импортируемого файла формата `*.rules` и подтвердите выбор.
   ▸ **Результат шага:** появится окно **Подготовка к импорту**.
4. В окне **Подготовка к импорту** Выбрать:
   - действие для элементов, которые отсутствуют в новом (загружаемом) справочнике:
     - **Оставить** — новые элементы будут добавлены к уже существующим;

       Подсказка:

       Данный вариант рекомендован к выбору при наличии измененных правил.

     - **Удалить** — старые элементы будут удалены и добавлены новые.
   - статус активности элементов справочника после импорта:
     - **Оставить как есть** — статус активности элементов справочника будет сохранен;

       Подсказка:

       Данный вариант рекомендован к выбору при наличии измененных правил.

     - **Присвоить старым статус, как в файле** — статус активности элементов справочника будет перезаписан в соответствии со значениями в импортируемом файле.

5. Нажмите **Импортировать** для запуска процедуры импорта.

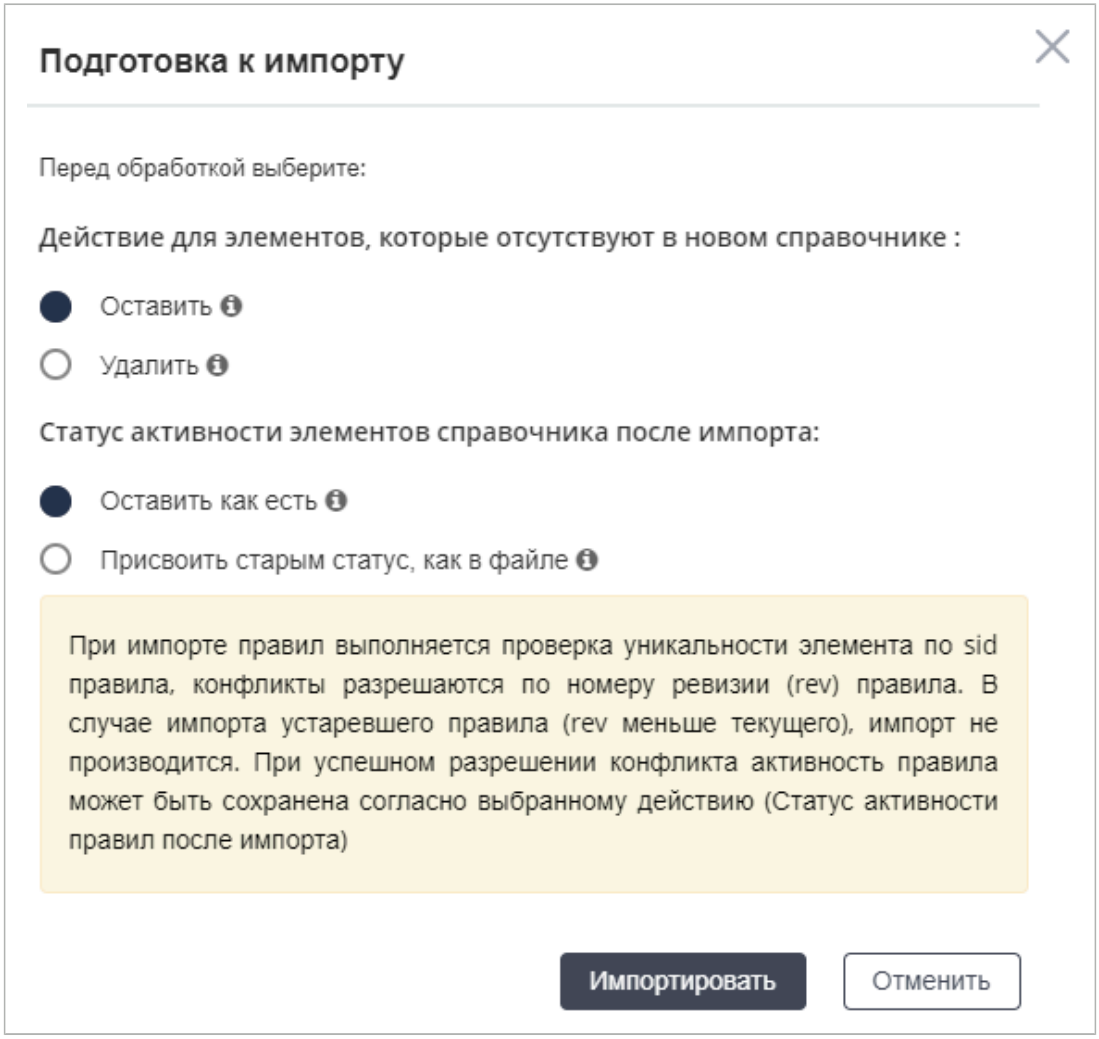


Рис. 339. Окно «Подготовка к импорту» при загрузке наборов сигнатур

▸ **Результат шага:** сразу после загрузки файла в правом верхнем углу страницы в поле **Результат последнего импорта** появится статус `Успешно`, и правила будут загружены на страницу **Правила обнаружения**.

6. Убедитесь, что правила были успешно загружены. Для этого перейдите на страницу **Правила обнаружения**.

15.7.3.3. Экспорт правил службы обнаружения вторжений

Для экспорта правил обнаружения вторжений в файл формата `*.json`:

1. Перейдите на страницу **Администрирование → Основные настройки → Импорт и экспорт**.
2. На панели **Обнаружение вторжений** в строке **Правила обнаружения вторжений** нажмите кнопку (**Экспортировать**).

   ▸ **Результат шага:** файл со списком правил `suricata_rules_[дата_и_время].zip` будет сформирован и доступен для скачивания в правом верхнем углу страницы **Импорт и экспорт** под заголовком **Результат последнего экспорта**.
3. Для скачивания файла нажмите на название сформированного файла под заголовком **Результат последнего экспорта**.

4. В открывшемся окне укажите расположение для экспортируемого файла, при необходимости изменив его название, и нажмите кнопку **Сохранить**.
   - **Результат шага:** файл `suricata_rules_[дата_и_время].zip` будет загружен на компьютер.

15.7.4. Создание исключений для правил обнаружения вторжений

Чтобы создать исключения для правил обнаружения вторжений, можно воспользоваться одним из следующих способов:

- создать исключение в карточке правила обнаружения вторжений;
- создать исключение во вкладке **Исключения** на странице **Правила обнаружения**;
- создать исключения для нескольких правил во вкладке **Правила** на странице **Правила обнаружения**;
- создать исключение для правила на конкретные IP-адреса.

15.7.4.1. Создание исключения в карточке правила обнаружения вторжений

Для создания исключения в карточке правила обнаружения вторжений:

1. Перейдите на страницу **Администрирование → Правила обнаружения**.
2. Откройте карточку создания исключения одним из способов:
   - Выберите необходимое правило обнаружения вторжений из списка правил во вкладке **Правила**.
   - Установите чекбокс возле правила в списке.
   - **Результат шага:** откроется карточка правила обнаружения вторжений.

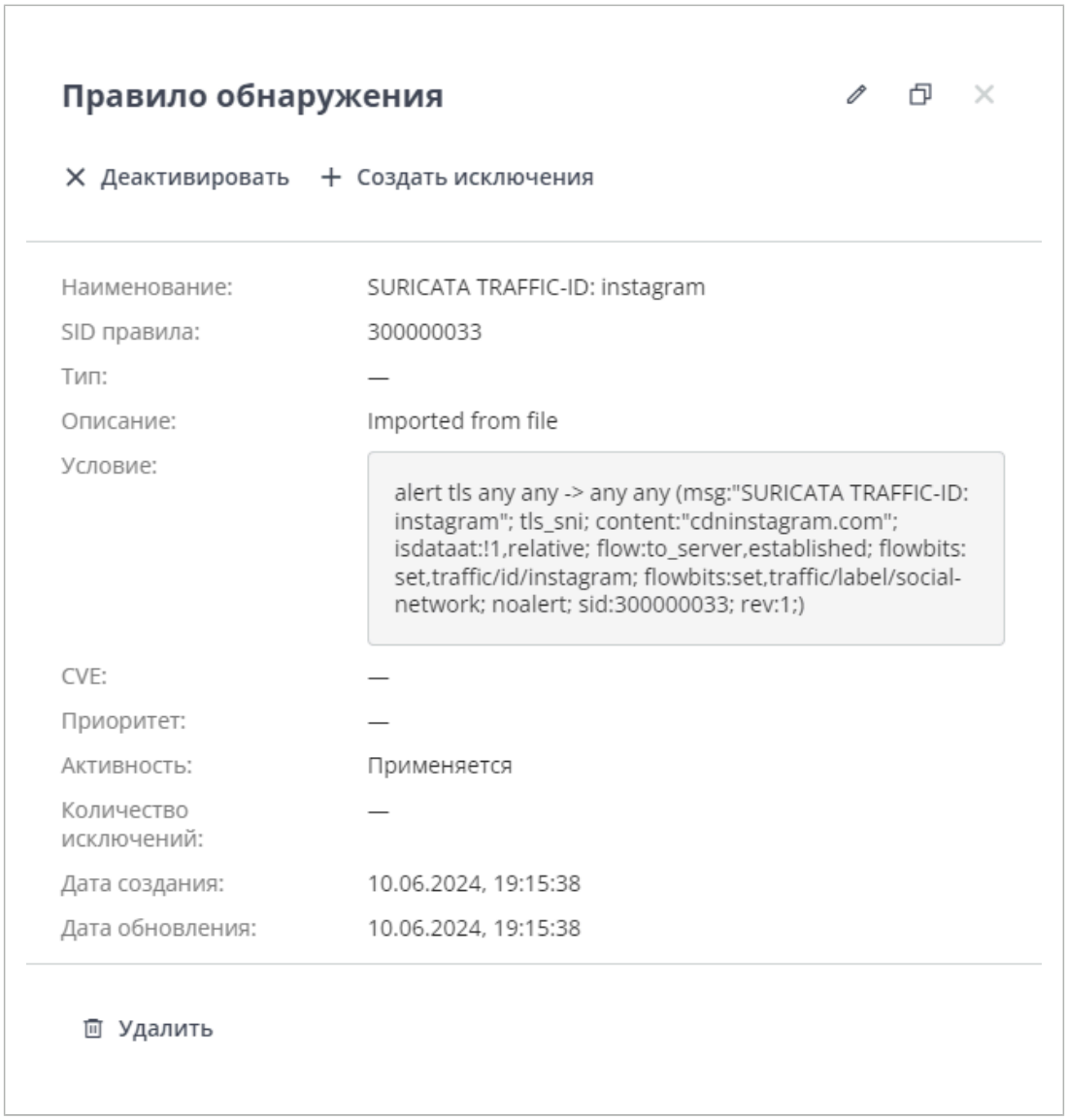


Рис. 340. Карточка правила обнаружения вторжений

3. Нажмите кнопку **Создать исключения**.
   - **Результат шага:** откроется окно создания исключений.

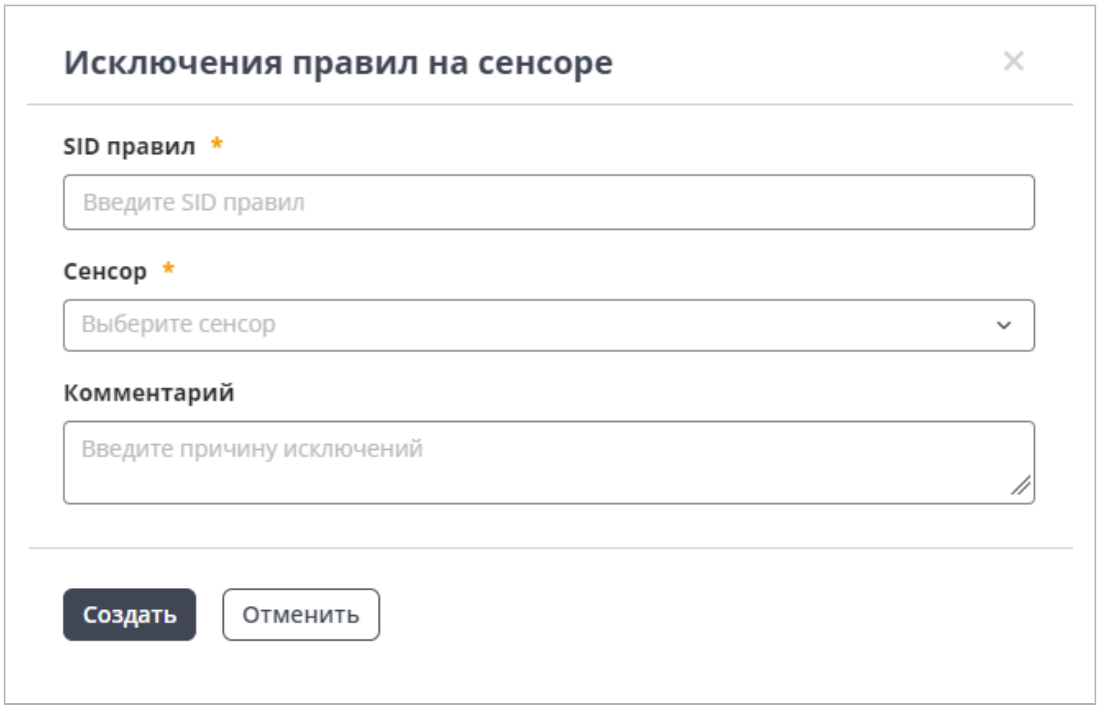


Рис. 341. Окно создания исключений

4. В окне создания исключений выберите сенсор, на котором будут созданы исключения, и введите комментарий к создаваемым исключениям.
5. После ввода данных нажмите кнопку **Создать**.
   - **Результат шага:** Созданные исключения будут отображаться в списке исключений во вкладке **Исключения**. В карточке правила обнаружения счетчик количества исключений в поле **Количество исключений** будет увеличен на 1.

15.7.4.2. Создание исключения во вкладке «Исключения»

Для создания исключения во вкладке **Исключения**:

1. Перейдите на страницу **Администрирование → Правила обнаружения**.
2. Во вкладке **Исключения** нажмите кнопку + Создать исключения.
   - **Результат шага:** откроется окно создания исключений.
3. В окне создания исключений введите SID правила и комментарий, а также выберите сенсор, на котором будут созданы исключения.
4. После ввода данных нажмите кнопку **Создать**.
   - **Результат шага:** Созданные исключения будут отображаться в списке исключений во вкладке **Исключения**.

15.7.4.3. Создание исключения для нескольких правил обнаружения вторжений

Для создания исключения для нескольких правил обнаружения вторжений:

1. Перейдите на страницу **Администрирование → Правила обнаружения**.
2. Установите чекбокс возле правил обнаружения вторжений из списка, либо установите чекбокс **Выбрать видимые строки**.

> Внимание:
>
> При установке чекбокса **Выбрать видимые строки** будет выбрано 100 правил.

- **Результат шага:** откроется меню выбора действий с правилами обнаружения вторжений.

3. В открывшемся меню выберите пункт **Создать исключения**.
   - **Результат шага:** откроется окно создания исключений.
4. В окне создания исключений выберите сенсор, на котором будет создано исключение, и введите комментарий к создаваемому исключению.
5. Нажмите кнопку **Создать**.
   - **Результат шага:** Созданное исключение будет отображаться в списке исключений во вкладке **Исключения**.

15.7.4.4. Создание исключения путем создания правила обнаружения вторжений на конкретные IP-адреса

Для ограничения срабатывания правила обнаружения вторжений на конкретные IP-адреса замените значение свойства `Action` с `alert` на `pass` и адреса отправителей и получателей.

Пример

Например, оригинальное правило с условием:

```
alert tcp any any -> any [139,445]
(msg:"ET NETBIOS Tree Connect AndX Request IPC$ Unicode";
flow:established,to_server; content:"|00|";
depth:1; content:"|FF|SMBu"; within:5; distance:3;
content:"| 00 5c 00 69 00 70 00 63 00 24 00 00 00|";
nocase; flowbits:set,smb.tree.connect.ipc; flowbits:noalert;
reference:cve,2006-4691;
classtype:protocol-command-decode; sid:2025090;
rev:1; metadata:created_at 2016_06_14, former_category NETBIOS,
updated_at 2020_08_20;)
```

После редактирования будет иметь следующий вид:

```
pass tcp 192.168.1.1 any -> 192.168.1.10 [139,445]
(msg:"ET NETBIOS Tree Connect AndX Request IPC$ Unicode";
flow:established,to_server; content:"|00|";
depth:1; content:"|FF|SMBu"; within:5; distance:3;
content:"| 00 5c 00 69 00 70 00 63 00 24 00 00 00|";
nocase; flowbits:set,smb.tree.connect.ipc; flowbits:noalert;
reference:cve,2006-4691;
classtype:protocol-command-decode; sid:94000000;
rev:1; metadata:created_at 2016_06_14, former_category NETBIOS,
updated_at 2020_08_20;)
```

В измененном правиле заменен `sid` на `94000000`, что соответствует пользовательскому диапазону, а значение свойства `Action` заменено на `pass`, что позволяет отключить срабатывание правила при получении на IP-адресе 192.268.1.10 пакетов от IP-адреса 192.268.1.1.

15.7.5. Удаление исключений для правил обнаружения вторжений

На Комплексе реализована возможность удаления как одного, так и нескольких исключений для правил обнаружения вторжений.

Для удаления нескольких исключений для правил обнаружения вторжений выполните следующие действия:

а. Установите чекбоксы возле необходимых исключений.

б. В открывшемся меню нажмите **Удалить**.

в. Введите текст обоснования удаления исключений и нажмите **Подтвердить**.

15.7.5.1. Удаление исключения для правила обнаружения вторжений

Для удаления исключения:

1. Выберите необходимое исключение из списка во вкладке **Исключения**.
   - **Результат шага:** откроется карточка исключения для правила обнаружения вторжений.

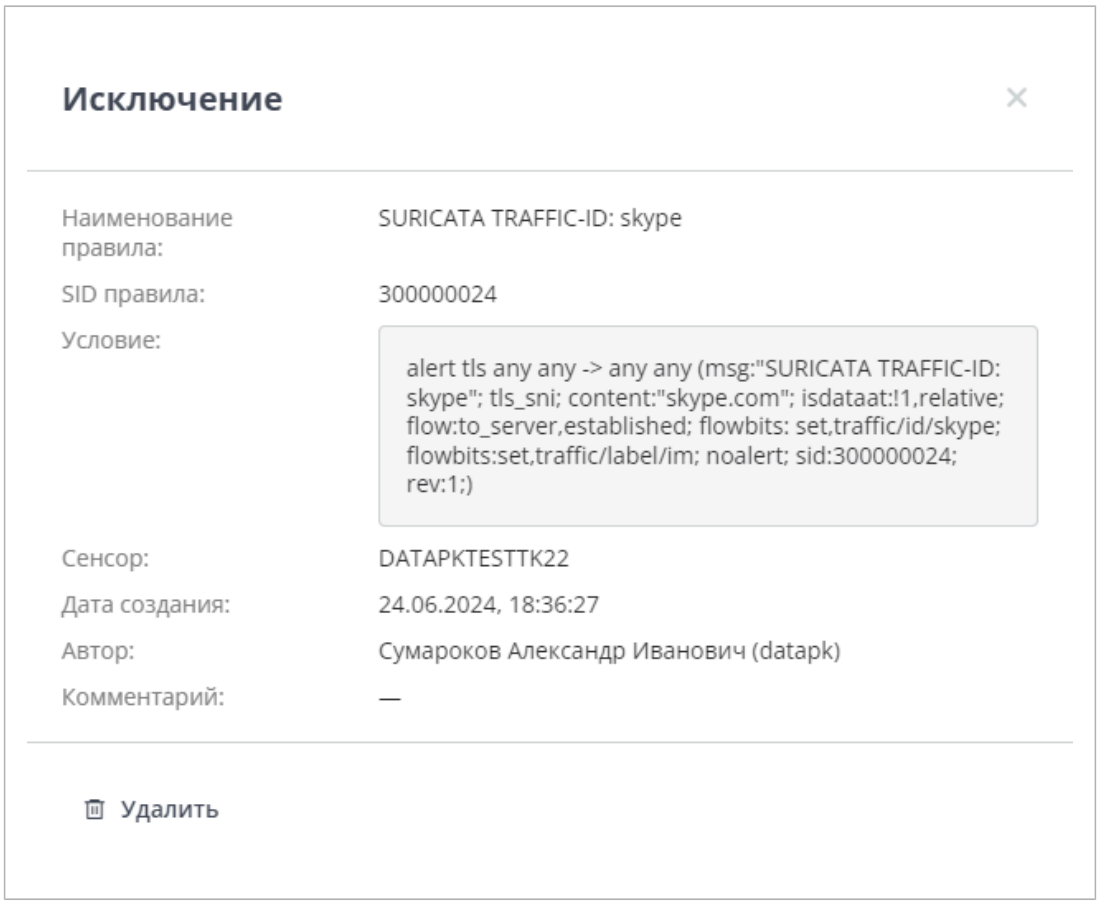


Рис. 342. Карточка исключения для правила обнаружения вторжений

2. Нажмите кнопку **Удалить**.
3. Введите текст обоснования удаления исключения и нажмите **Подтвердить**.

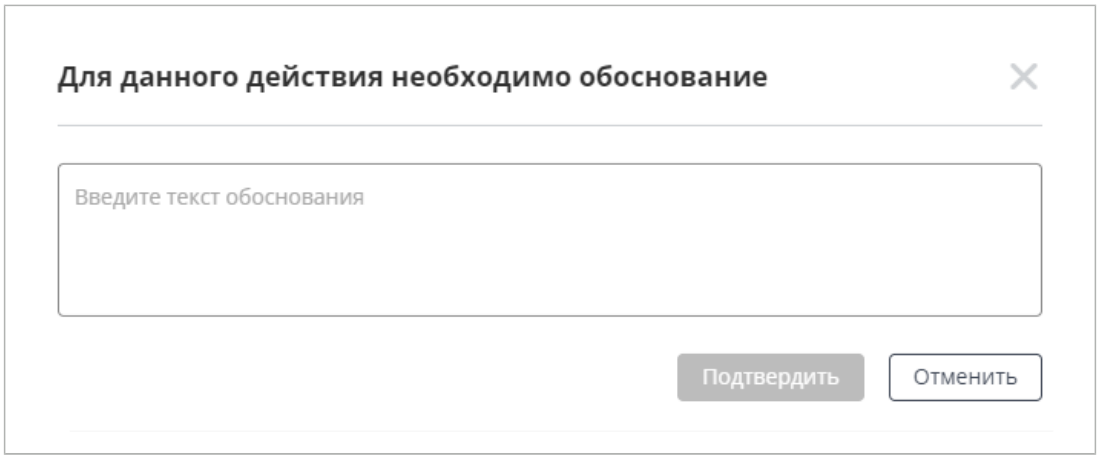


Рис. 343. Обоснование удаления исключения

- **Результат шага:** исключение будет удалено на сенсоре.

4. Вы также можете удалить исключение следующим способом:
    a. Установите чекбоксы возле необходимых исключений.
    - **Результат шага:** откроется меню выбора действий с правилами обнаружения вторжений.
    б. В открывшемся меню нажмите **Удалить**.
    в. Введите текст обоснования удаления исключения и нажмите **Подтвердить**.

15.7.5.2. Удаление нескольких исключений для правил обнаружения вторжений

Для удаления нескольких исключений:

1. Установите чекбоксы возле необходимых исключений.
2. В открывшемся меню нажмите **Удалить**.
3. Введите текст обоснования удаления и нажмите **Подтвердить**.
    - **Результат шага:** исключения будут удалены на сенсоре.

16. Управление проектами ПЛК

В этом разделе:

1. **Version Control Management**
2. **Version Control Desktop App**

См. также

Справочная информация о модуле «Управление проектами ПЛК»

16.1. Version Control Management

В этом разделе:

- Просмотр каталога репозиториев
- Управление группами
- Управление репозиториями
- Управление версиями проектов

16.2. Version Control Desktop App

В этом разделе:

- Системные требования
- Вход в систему Version Control Desktop App
- Использование Version Control Desktop App по назначению

16.2.1. Системные требования

Системные требования Version Control Desktop App:

- Операционная система:
  - Windows 7 SP1, 8.1, Windows 2012 R2 или новее;
  - РЕД ОС 7.3, 8 или новее;
  - Astra Linux 1.7, 1.8 или новее.

  Прим.:

  Для правильной работы Version Control Desktop App на Windows 7 SP1 необходимо установить:
  - обновление KB4474419;
  - Visual C++ версии 2015 Redistributable или выше.
- Оперативная память: не менее 4 ГБ.
- Дополнительное ПО: Git-клиент версии 2.37.0 или новее. Установка Git-клиента должна выполняться только пользователем с правами администратора.
  Каждый пользователь Version Control Desktop App перед началом работы с приложением должен отключить преобразование конца строк файлов, которые будет отслеживать Git:

```
git config --global core.autocrlf false
```

Внимание:

С открытой средой разработки возможно замедление при подключении к серверу Version Control Management.

16.2.2. Вход в систему Version Control Desktop App

В приложении Version Control Desktop App доступны два способа входа:

- Аутентификация с подключением к серверу — вход с подключением к серверу Version Control Management. В этом режиме доступны все функции Version Control Desktop App.
- Локальная аутентификация — вход без подключения к серверу Version Control Management. В этом режиме доступные следующие функции:
  - Просмотр каталога репозиториев.
  - Просмотр подключенных ранее репозиториев.
  - Скачивание файлов подключенных ранее репозиториев.
  - Отключение и подключение серверов.

Внимание:

С открытой средой разработки возможно замедление при подключении к серверу Version Control Management.

В этом разделе:

- Вход в Version Control Desktop App с подключением к серверу
- Локальный вход в Version Control Desktop App

16.2.2.1. Вход в Version Control Desktop App с подключением к серверу

Для входа с подключением к серверу:

1. Запустите приложение Version Control Desktop App.
   - **Результат шага:** Откроется страница аутентификации Version Control Desktop App.

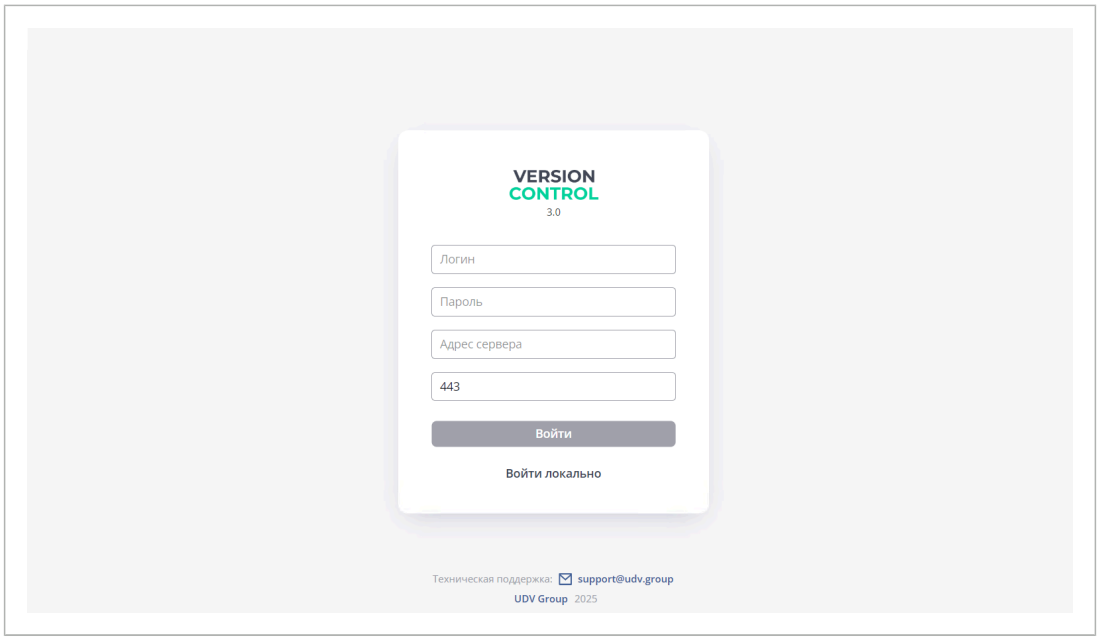


Рис. 344. Страница аутентификации Version Control Desktop App

2. Настройте параметры аутентификации:
   - **Логин** — имя пользователя для подключения к серверу Version Control Management;
   - **Пароль** — пароль для подключения к серверу Version Control Management;
   - **Адрес сервера** — IP-адрес сервера Version Control Management.
   - **Порт** — порт подключения. По умолчанию порт имеет значение 443.

   Если ранее уже выполнялось подключение к серверу, то в поле **Адрес сервера** можно выбрать сохраненный ранее сервер по его имени в выпадающем списке.

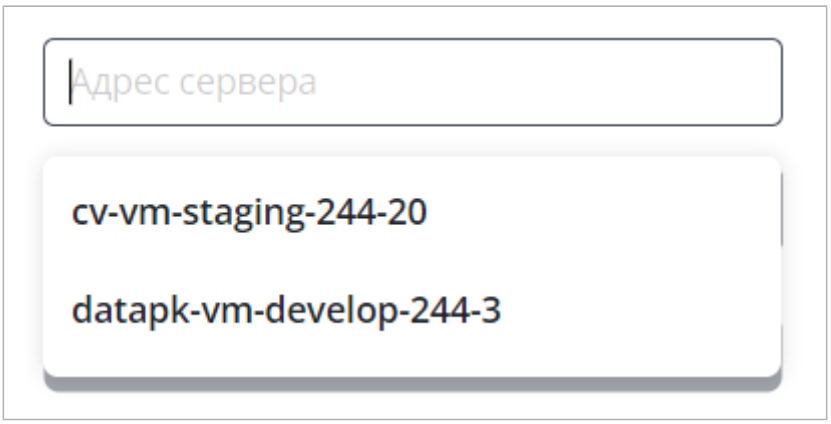


Рис. 345. Сохраненные ранее сервера

3. Нажмите кнопку **Войти**.

- **Результат шага:** отобразится главная страница с каталогом репозиториев.

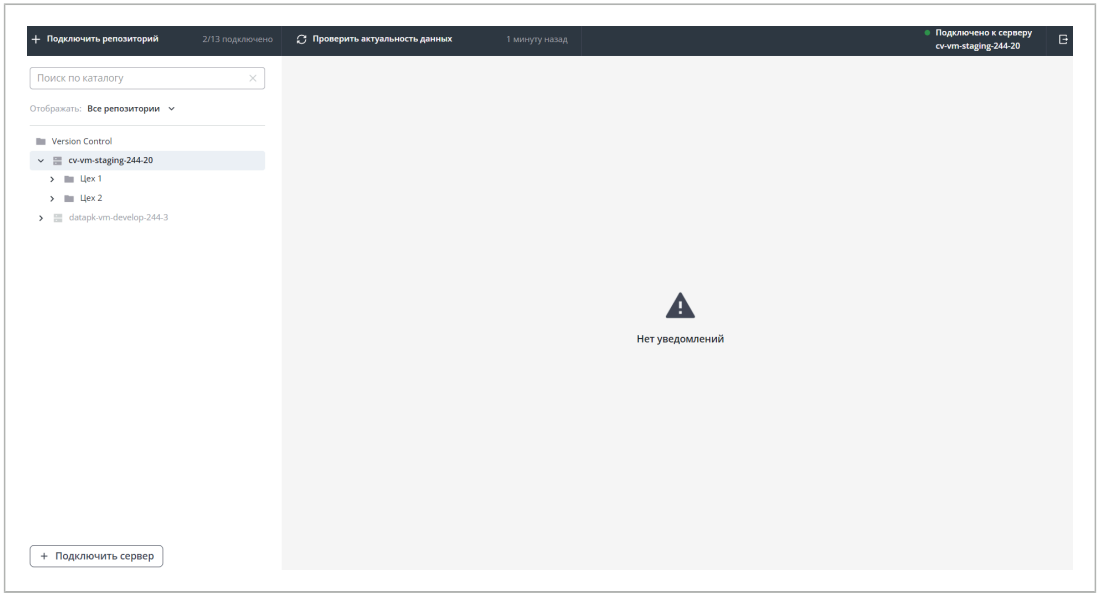


Рис. 346. Выполнена аутентификация с подключением к серверу

16.2.2.2. Локальный вход в Version Control Desktop App

Для локального входа:

1. Запустите приложение Version Control Desktop App.
   - **Результат шага:** Откроется страница аутентификации Version Control Desktop App.

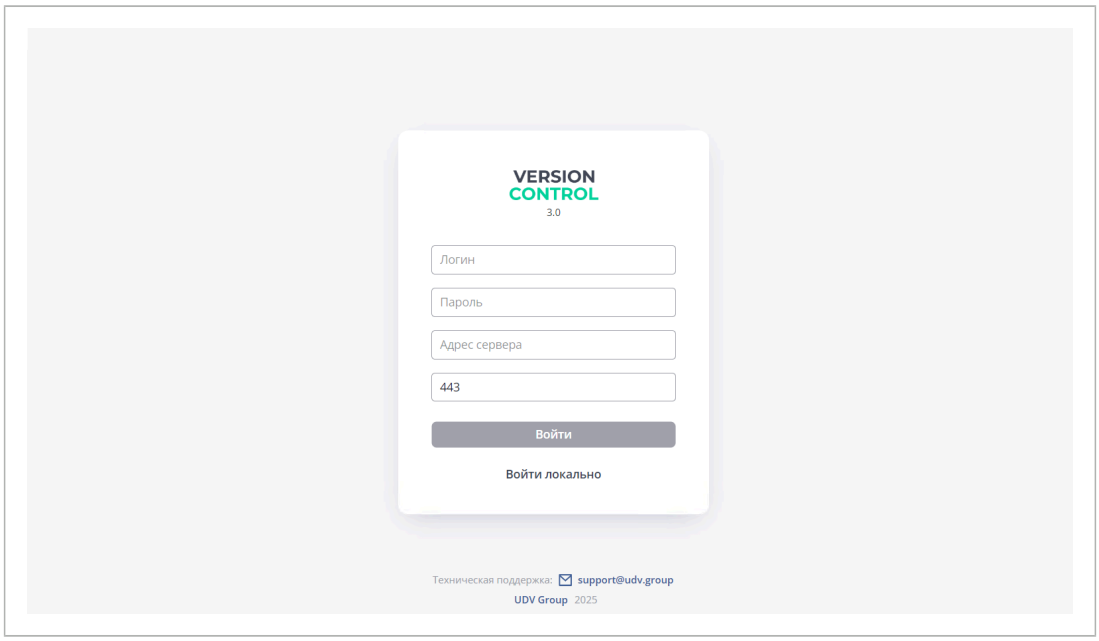


Рис. 347. Страница аутентификации Version Control Desktop App

2. Нажмите кнопку **Войти локально**.

- **Результат шага:** отобразится главная страница с каталогом репозиториев без подключения к серверу.

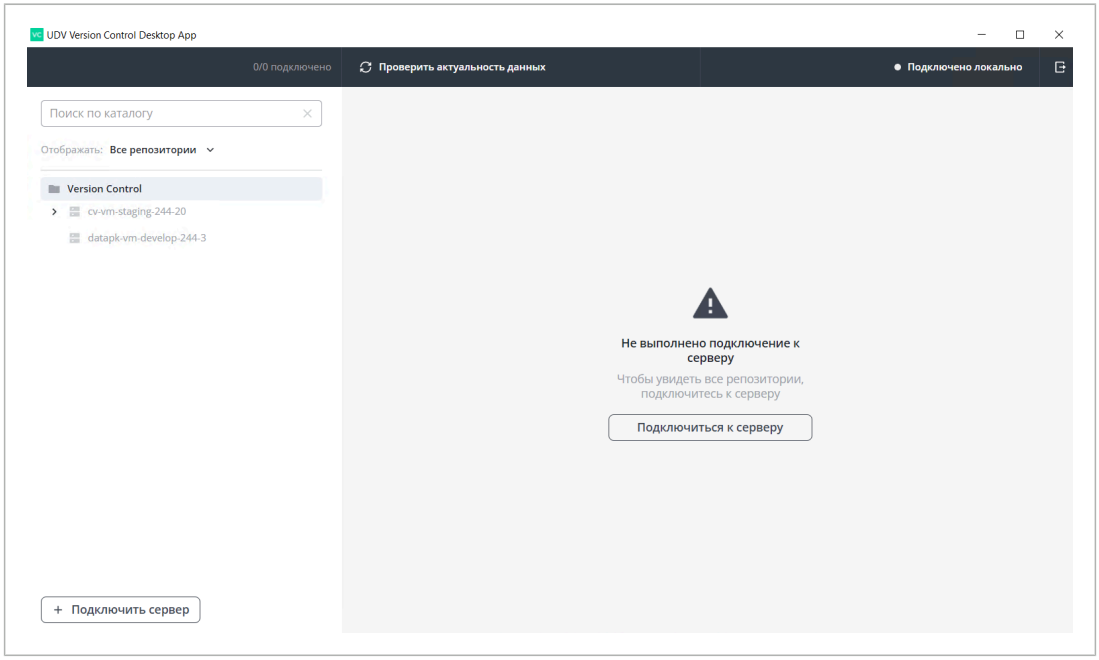


Рис. 348. Вход в систему выполнен локально

16.2.3. Использование Version Control Desktop App по назначению

В этом разделе:

- Просмотр каталога репозиториев
- Проверка актуальности данных
- Управление серверами
- Управление группами
- Управление репозиториями
- Управление версиями проектов

16.2.3.1. Просмотр каталога репозиториев

Каталог репозиториев отображается в левом боковом меню. Светло-серым цветом отображаются неподключенные сервера и репозитории.

Каталог имеет следующую иерархию:

- Сервер — может состоять из групп и репозиториев, отмечен символом .
- Группа — может состоять из групп и репозиториев, отмечена символом .
- Репозиторий — отмечен символом .

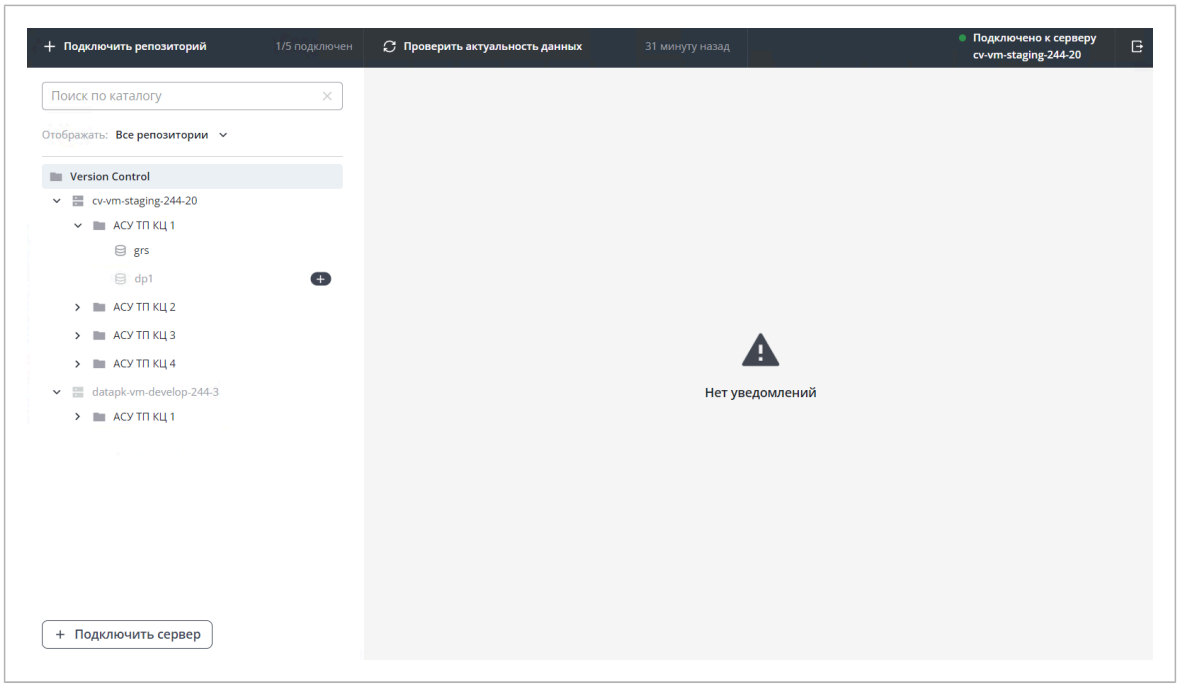


Рис. 349. Каталог репозиториев

В левом боковом меню возле имени репозитория может отображаться значок статуса репозитория. Перечень всех значков статусов репозитория см. в разделе Статусы репозиториев.

С помощью выпадающего списка **Отображать:** можно выбрать, отображать все репозитории или только подключенные. Если выбрать `Только подключенные`, то из каталога пропадут не только неподключенные репозитории, но и группы, в которых они состоят.

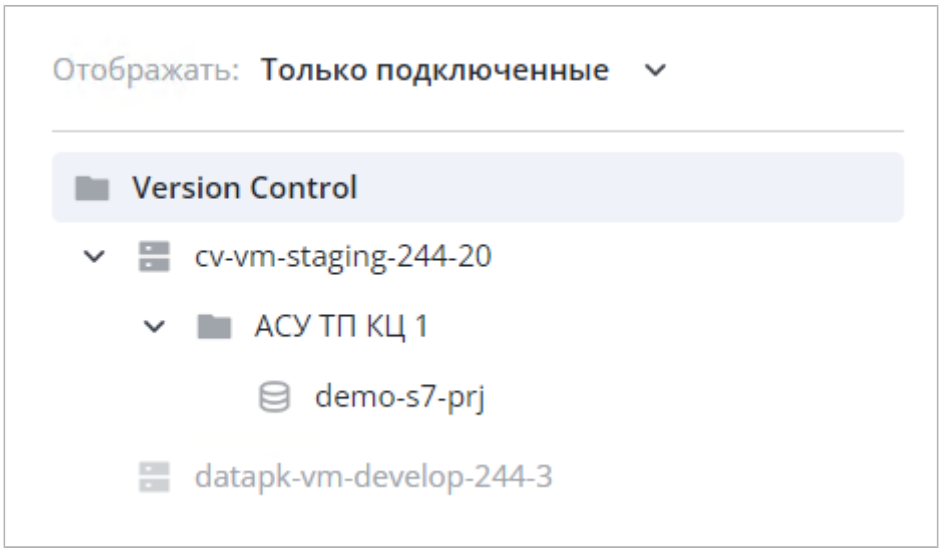


Рис. 350. Отображение только подключенных репозиториев

При нажатии правой кнопкой мыши по элементу каталога открывается меню для этого элемента.

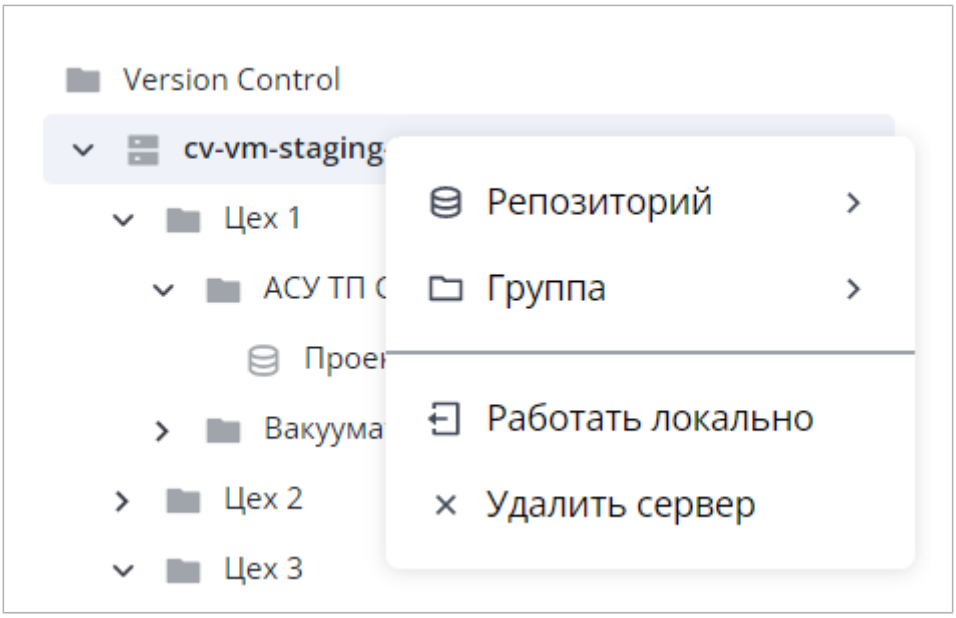


Рис. 351. Меню сервера

С помощью меню сервера можно:

- Подключиться к серверу.
- Создавать новые группы и репозитории.
- Перейти в режим локальной работы.
- Удалить сервер из каталога репозиториев.

С помощью меню группы можно:

- Создавать новые группы и репозитории.
- Удалить группу.
- Редактировать наименование группы.
- Подключить репозиторий.

С помощью меню репозитория можно:

- Подключить репозиторий.
- Редактировать наименование репозитория.
- Забыть проект.

16.2.3.2. Проверка актуальности данных

При подключении к серверу Version Control Management в приложении Version Control Desktop App проверяется актуальность данных приложения. Если версия проекта на сервере новее, чем в приложении, то на странице **Version Control** отображается уведомление об этом.

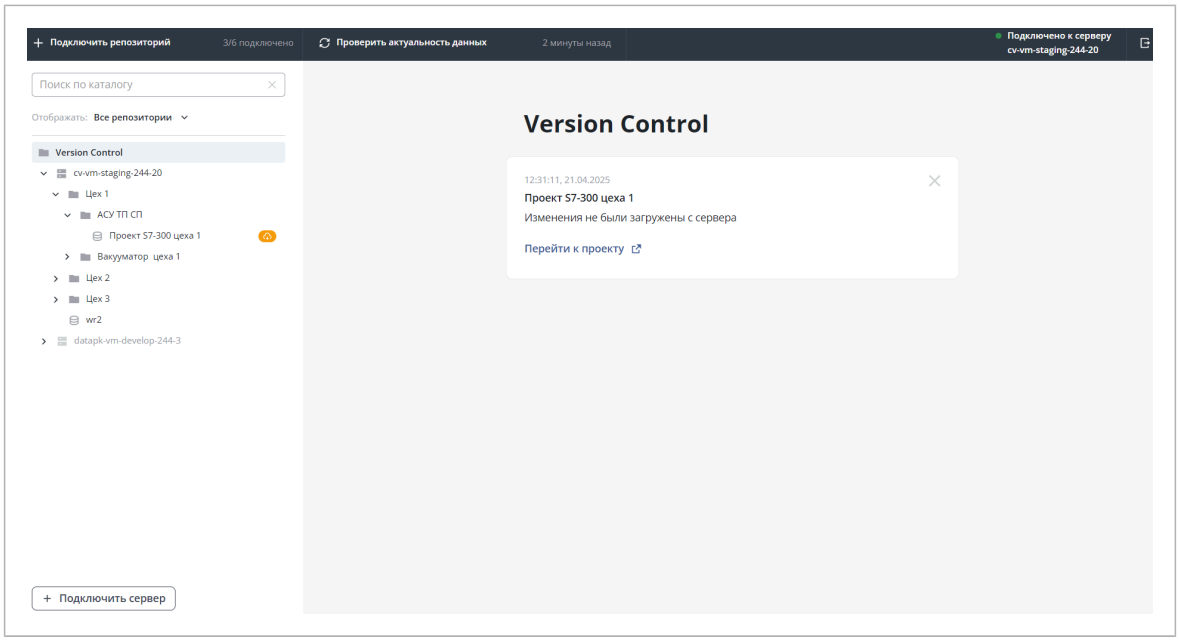


Рис. 352. Уведомление о новой версии проекта на сервере

Для корректной работы с проектами необходимо регулярно проверять актуальность данных вручную с помощью кнопки **Проверить актуальность данных**.

16.2.3.3. Управление серверами

В этом разделе:

- Подключение сервера
- Подключение нового сервера
- Удаление сервера

16.2.3.3.1. Подключение сервера

Есть несколько способов подключения сервера Version Control Management в Version Control Desktop App:

- Подключение сервера на странице аутентификации
- Подключение сервера
- Подключение определенного сервера через боковое меню
- Подключение определенного сервера на странице его репозитория

16.2.3.3.1.1. Подключение сервера на странице аутентификации

Для подключения к серверу Version Control Management:

1. Нажмите кнопку в правом верхнем углу, чтобы вернуться на страницу аутентификации.
   - **Результат шага:** откроется страница аутентификации Version Control Desktop App.

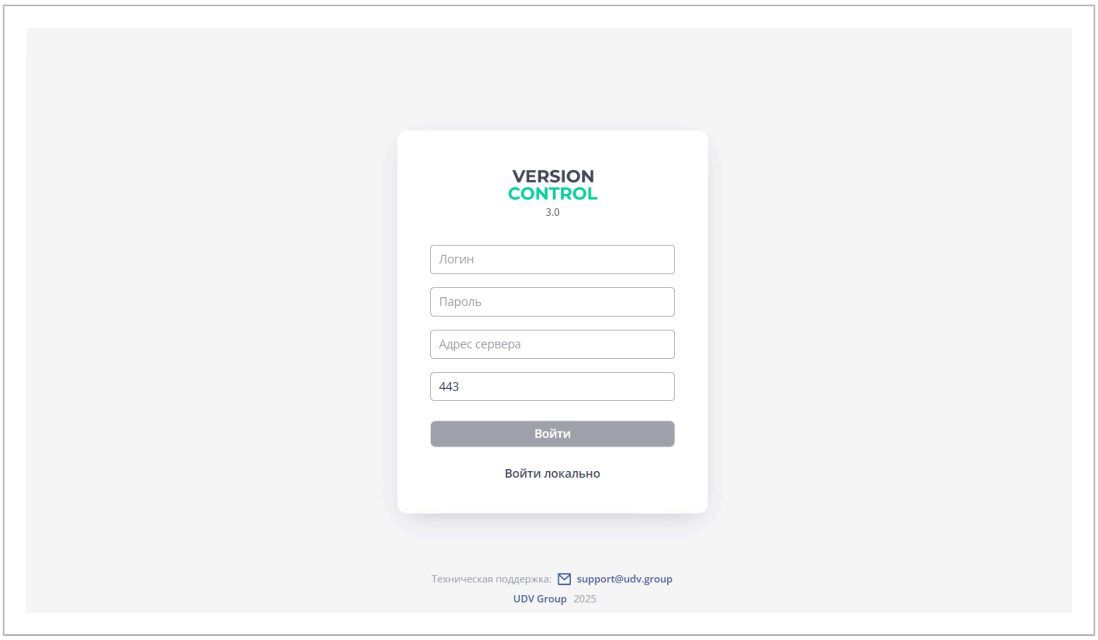


Рис. 353. Страница аутентификации Version Control Desktop App

2. Настройте параметры аутентификации:
   - **Логин** — имя пользователя для подключения к серверу Version Control Management;
   - **Пароль** — пароль для подключения к серверу Version Control Management;
   - **Адрес сервера** — IP-адрес сервера Version Control Management.
   - **Порт** — порт подключения. По умолчанию порт имеет значение 443.

   Если ранее уже выполнялось подключение к серверу, то в поле **Адрес сервера** можно выбрать сохраненный ранее сервер по его наименованию в выпадающем списке.

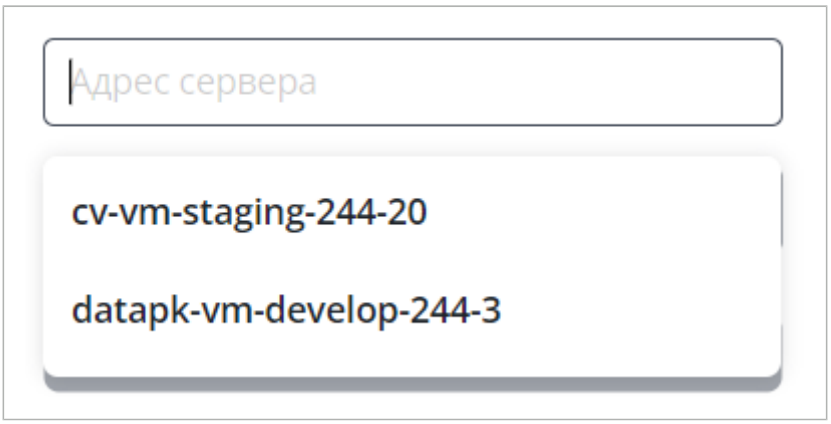


Рис. 354. Сохраненные ранее сервера

3. Нажмите кнопку **Войти**.

- **Результат шага:** сервер будет подключен.

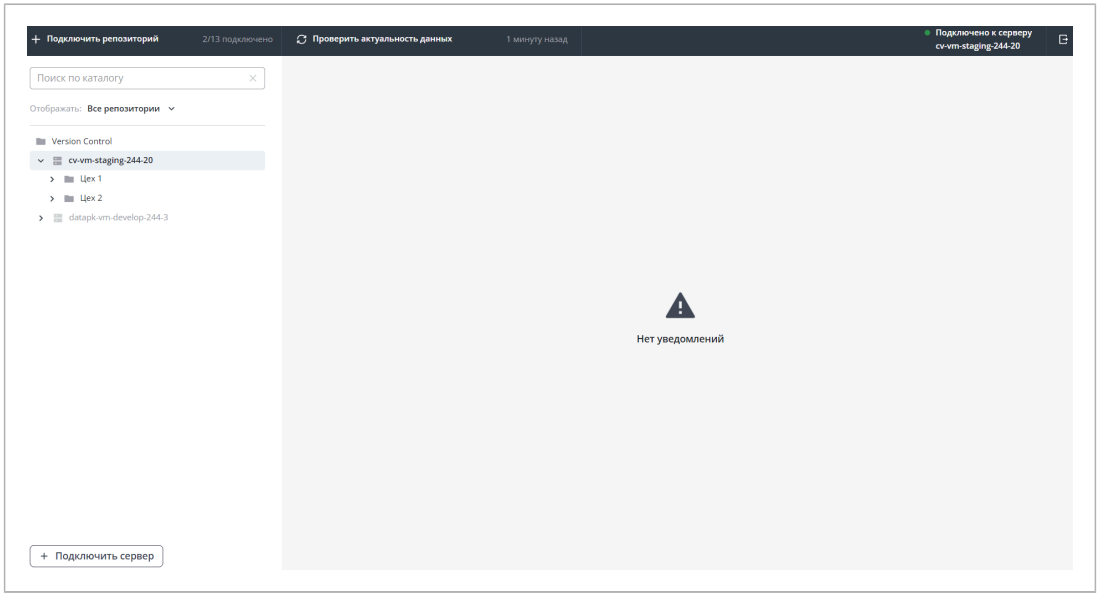


Рис. 355. Выполнена аутентификация с подключением к серверу

16.2.3.3.1.2. Подключение сервера

Для подключения к серверу Version Control Management:

1. Нажмите кнопку **Подключить сервер** в левом нижнем углу.
   - **Результат шага:** откроется окно аутентификации с подключением к серверу.

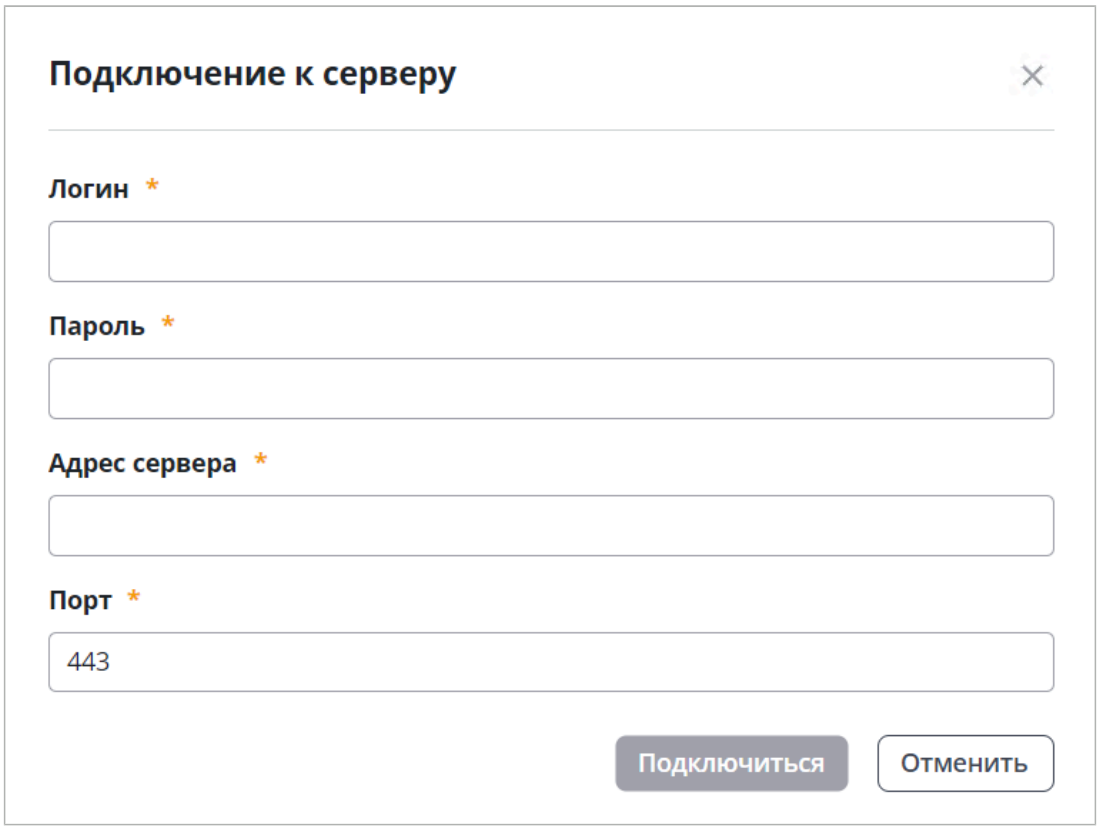


Рис. 356. Подключение к серверу

2. Настройте параметры аутентификации:

- **Логин** — имя пользователя для подключения к серверу Version Control Management;
- **Пароль** — пароль для подключения к серверу Version Control Management;
- **Адрес сервера** — IP-адрес сервера Version Control Management.
- **Порт** — порт подключения. По умолчанию порт имеет значение 443.

3. Нажмите кнопку **Подключиться**.
   - **Результат шага:** сервер будет подключен.

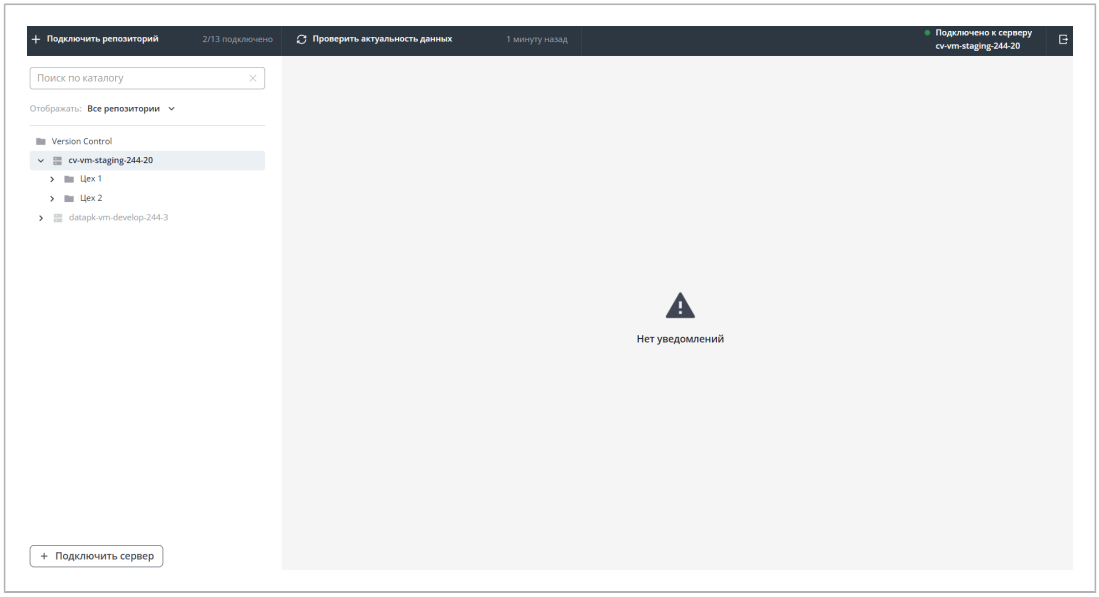


Рис. 357. Выполнена аутентификация с подключением к серверу

16.2.3.3.1.3. Подключение определенного сервера через боковое меню

Для подключения к серверу Version Control Management в каталоге репозиториев:

1. Нажмите правой кнопкой мыши в левом боковом меню на нужный сервер.
2. В открывшемся меню выберите **Подключиться к серверу**.
   - **Результат шага:** откроется окно аутентификации с подключением к серверу.

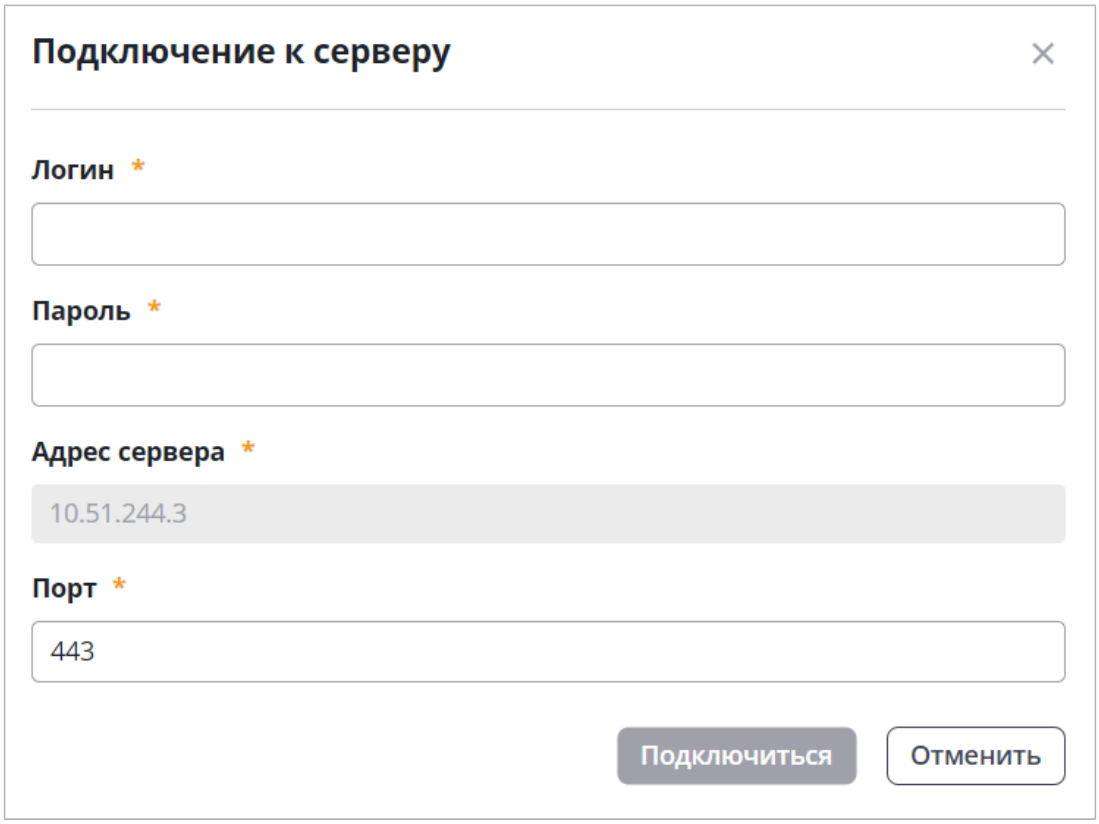


Рис. 358. Подключение к серверу

3. Настройте параметры аутентификации:
    - **Логин** — имя пользователя для подключения к серверу Version Control Management;
    - **Пароль** — пароль для подключения к серверу Version Control Management;
    - **Порт** — порт подключения. По умолчанию порт имеет значение 443.
4. Нажмите кнопку **Подключиться**.

- **Результат шага:** сервер будет подключен.

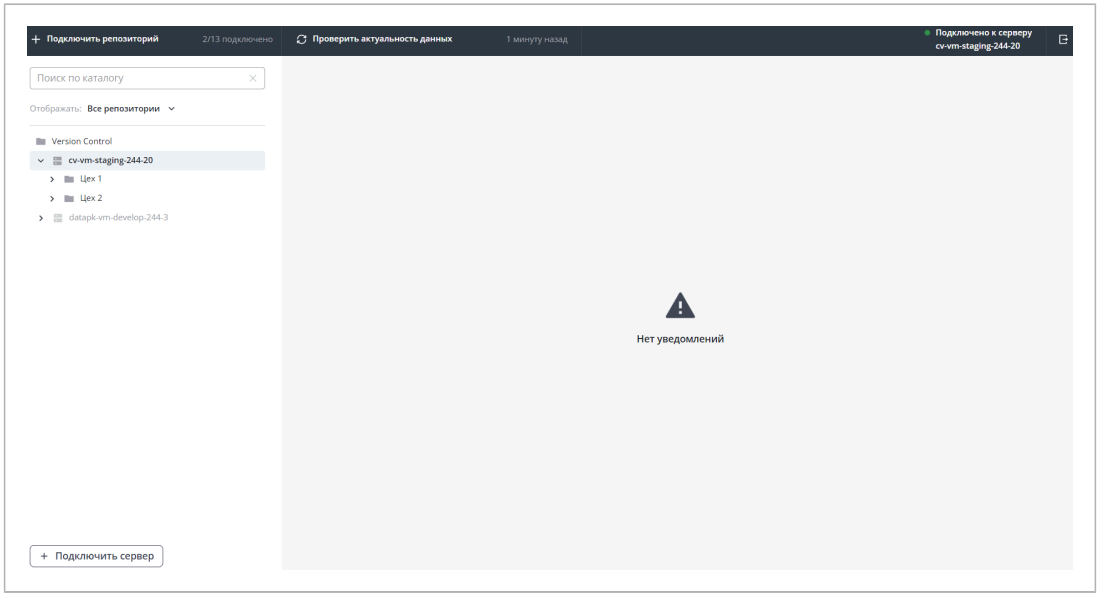


Рис. 359. Выполнена аутентификация с подключением к серверу

16.2.3.3.1.4. Подключение определенного сервера на странице его репозитория

Для подключения к серверу Version Control Management:

1. Нажмите на наименование репозитория неподключенного сервера в каталоге в левом боковом меню.
   - **Результат шага:** откроется страница репозитория неподключенного сервера.

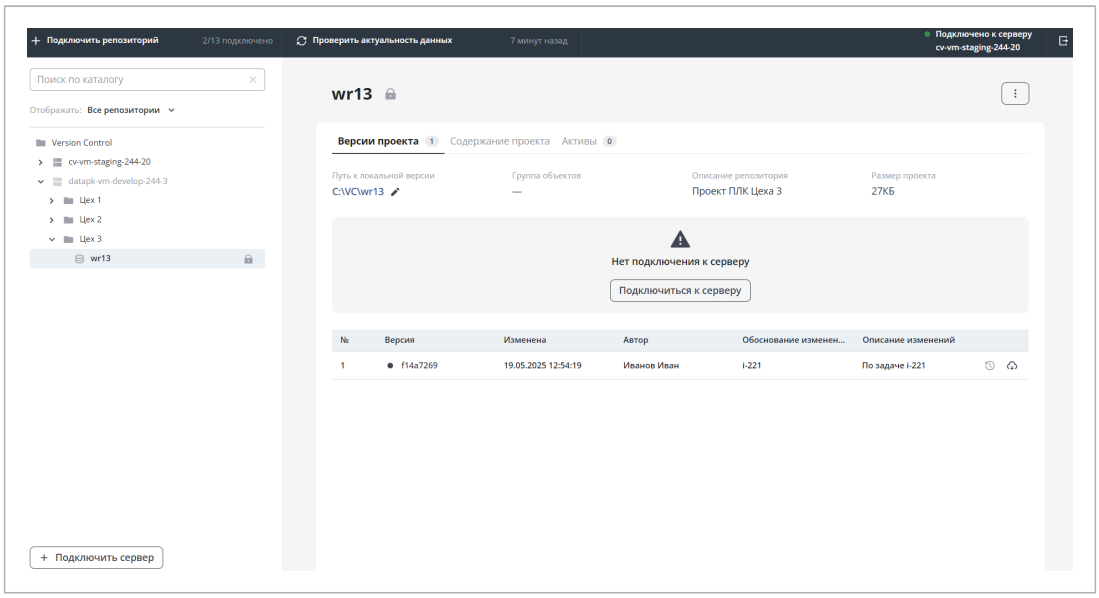


Рис. 360. Репозиторий, к серверу которого не было выполнено подключение

2. Нажмите кнопку **Подключиться к серверу**.
   - **Результат шага:** Откроется окно аутентификации с подключением к серверу.

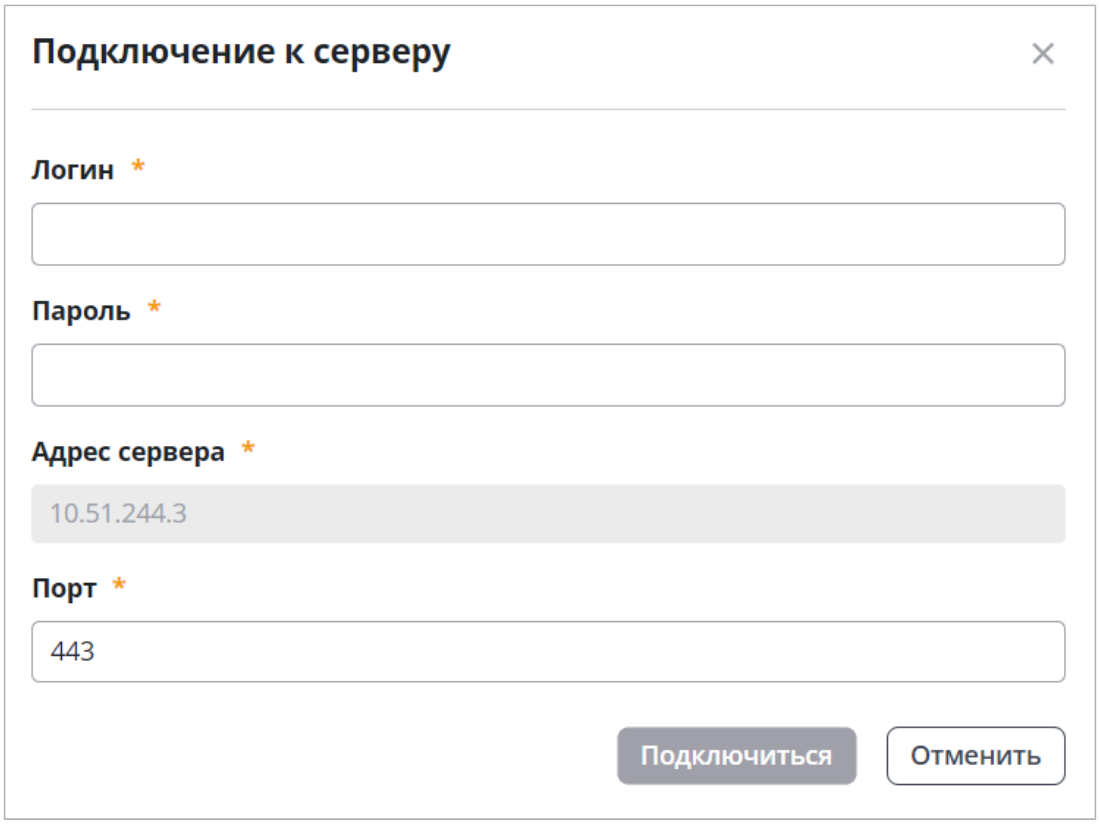


Рис. 361. Подключение к серверу

3. Настройте параметры аутентификации:
    - **Логин** — имя пользователя для подключения к серверу Version Control Management;
    - **Пароль** — пароль для подключения к серверу Version Control Management;
    - **Порт** — порт подключения. По умолчанию порт имеет значение 443.
4. Нажмите кнопку **Подключиться**.
    - **Результат шага:** сервер будет подключен.

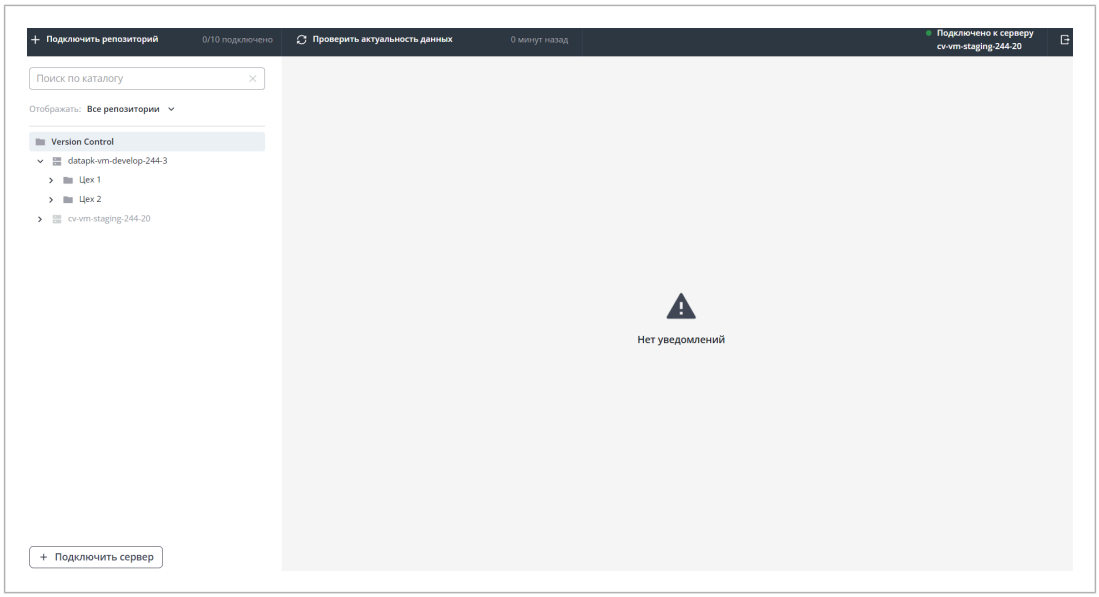


Рис. 362. Выполнена аутентификация с подключением к серверу

16.2.3.3.2. Подключение нового сервера

Есть несколько способов подключения нового сервера Version Control Management в Version Control Desktop App:

- Подключение нового сервера на странице аутентификации;
- Подключение нового сервера.

16.2.3.3.2.1. Подключение нового сервера на странице аутентификации

Для подключения к новому серверу Version Control Management:

1. Нажмите кнопку в правом верхнем углу, чтобы вернуться на страницу аутентификации.
   - **Результат шага:** откроется страница аутентификации Version Control Desktop App.

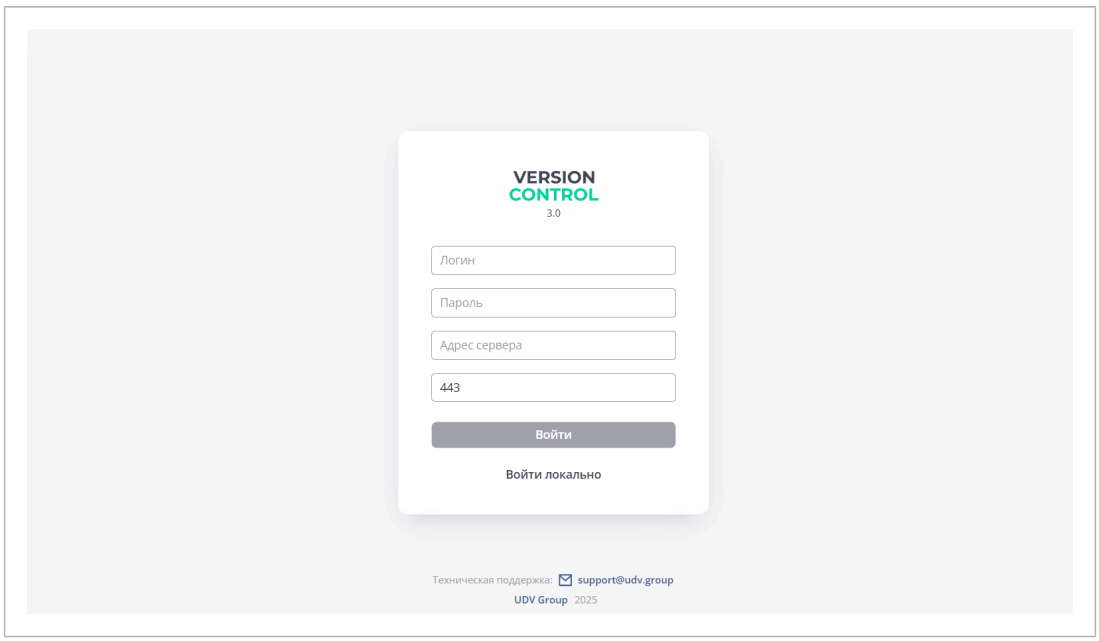


Рис. 363. Страница аутентификации Version Control Desktop App

2. Настройте параметры аутентификации:
   - **Логин** — имя пользователя для подключения к серверу Version Control Management;
   - **Пароль** — пароль для подключения к серверу Version Control Management;
   - **Адрес сервера** — IP-адрес сервера Version Control Management.
   - **Порт** — порт подключения. По умолчанию порт имеет значение 443.
3. Нажмите кнопку **Войти**.

- **Результат шага:** новый сервер будет подключен.

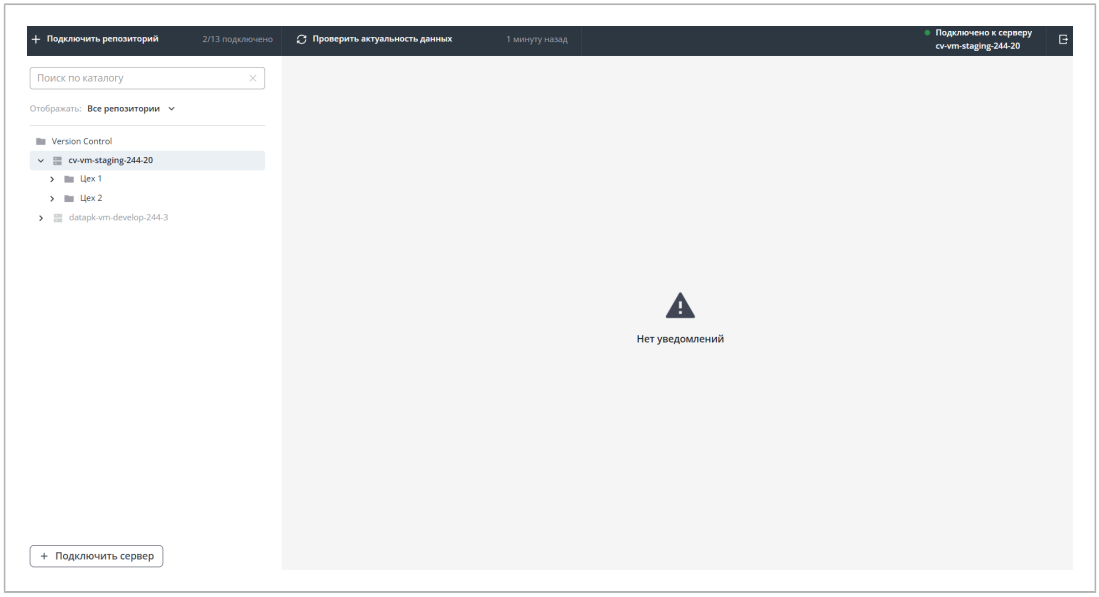


Рис. 364. Выполнена аутентификация с подключением к серверу

16.2.3.3.2.2. Подключение к новому серверу

Для подключения к новому серверу Version Control Management:

1. Нажмите кнопку **Подключить сервер** в левом нижнем углу.
   - **Результат шага:** откроется окно аутентификации с подключением к новому серверу.

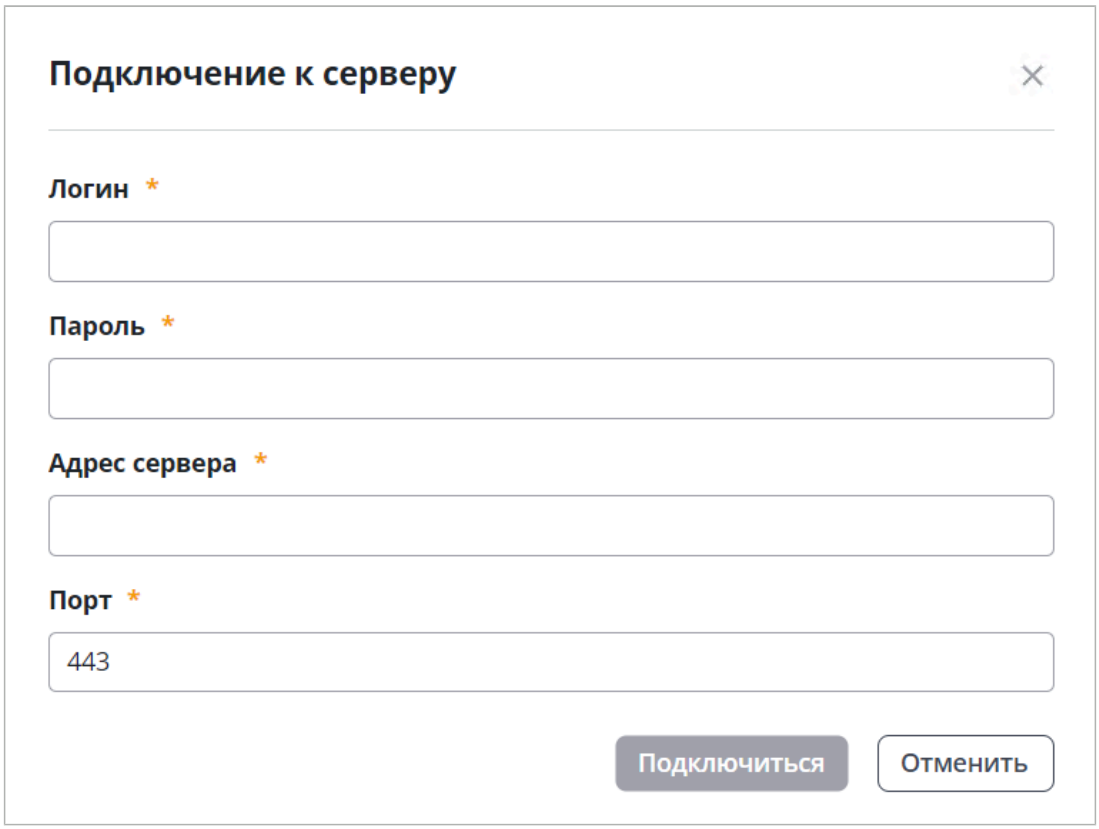


Рис. 365. Подключение к серверу

2. Настройте параметры аутентификации:

- **Логин** — имя пользователя для подключения к серверу Version Control Management;
- **Пароль** — пароль для подключения к серверу Version Control Management;
- **Адрес сервера** — IP-адрес сервера Version Control Management.
- **Порт** — порт подключения. По умолчанию порт имеет значение 443.

3. Нажмите кнопку **Подключиться**.
   - **Результат шага:** новый сервер будет подключен.

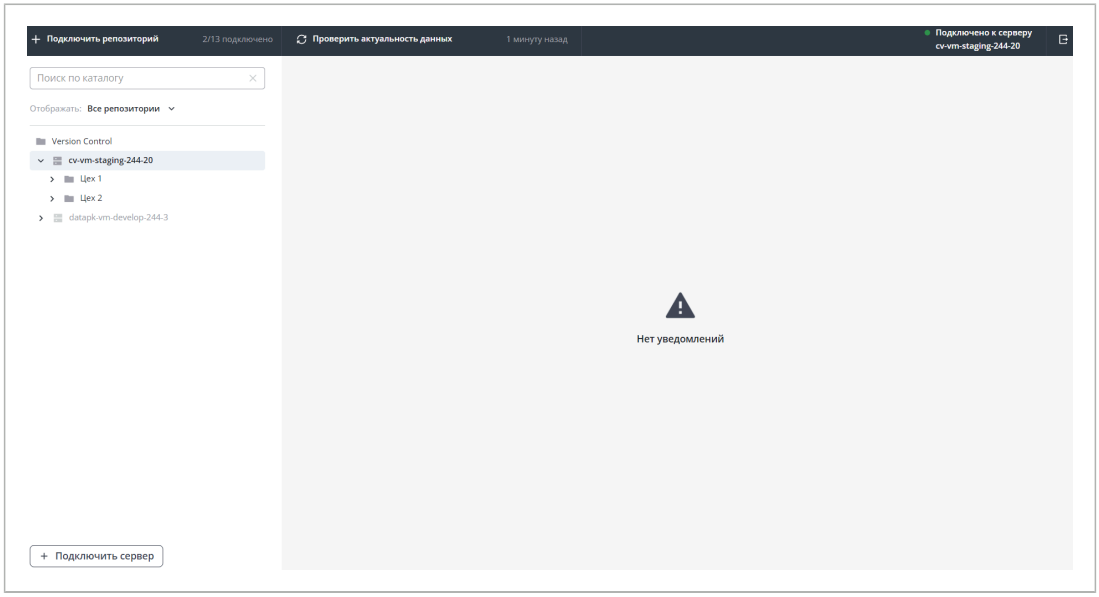


Рис. 366. Выполнена аутентификация с подключением к новому серверу

16.2.3.3.3. Удаление сервера

При удалении сервера удаляются связи между репозиториями сервера и локальными хранилищами. Сервер удаляется из каталога репозиториев. Все группы и репозитории сервера становятся недоступны.

Чтобы удалить сервер Version Control Management:

1. Нажмите правой кнопкой мыши в левом боковом меню на нужный сервер.
2. В открывшемся меню выберите **Удалить сервер**.
   - **Результат шага:** откроется окно подтверждения удаления сервера.

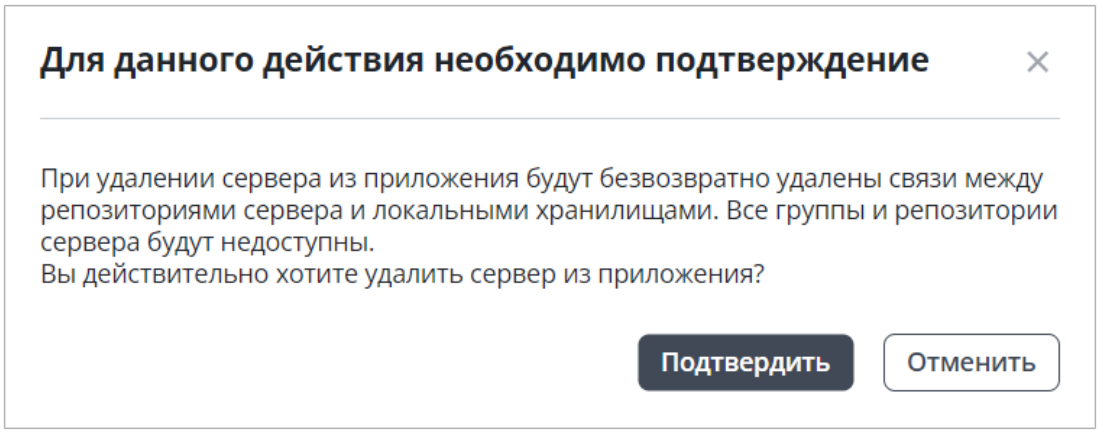


Рис. 367. Окно подтверждения

3. Нажмите кнопку **Подтвердить**.

16.2.3.4. Управление группами

Управление группами возможно только после входа в Version Control Desktop App с подключением к серверу Version Control Management.

В этом разделе:

- Создание группы
- Редактирование группы
- Удаление группы

16.2.3.4.1. Создание группы

Чтобы создать группу:

1. Нажмите правой кнопкой мыши в левом боковом меню на сервер или группу.
2. В открывшемся меню выберите **Группа → Создать**.
   - **Результат шага:** откроется окно создания группы.

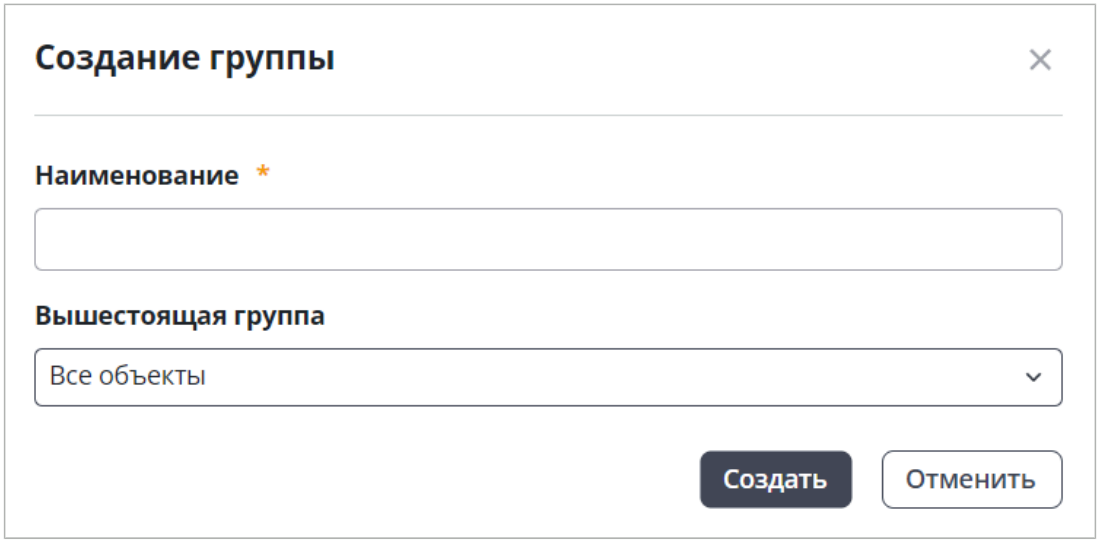


Рис. 368. Создание группы

3. Заполните поле **Наименование**.
4. В выпадающем списке **Вышестоящая группа** выберите подходящую группу для нового репозитория.
5. Нажмите кнопку **Создать**.

16.2.3.4.2. Редактирование группы

Чтобы редактировать группу:

1. Нажмите правой кнопкой мыши в левом боковом меню на нужную группу.
2. В открывшемся меню выберите **Группа → Редактировать**.
   - **Результат шага:** откроется окно редактирования группы.

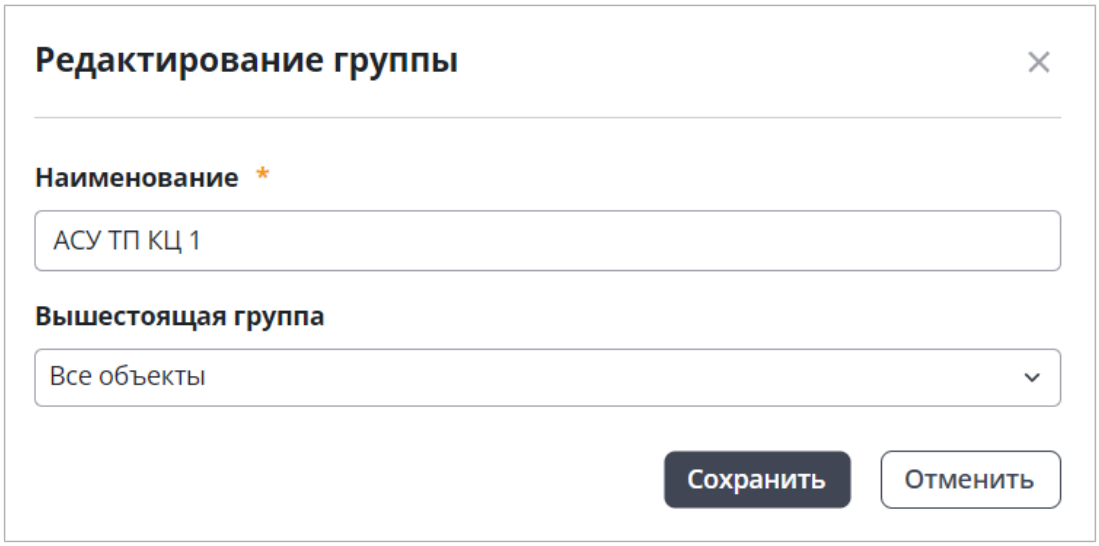


Рис. 369. Редактирование группы

3. Измените поле **Наименование** или группу в выпадающем списке **Вышестоящая группа**.
4. Нажмите кнопку **Сохранить**.

16.2.3.4.3. Удаление группы

При удалении группы ее объекты переносятся в вышестоящую группу.

Чтобы удалить группу:

1. Нажмите правой кнопкой мыши в левом боковом меню на нужную группу.
2. В открывшемся меню выберите **Группа → Удалить**.
   - **Результат шага:** откроется окно подтверждения удаления группы.

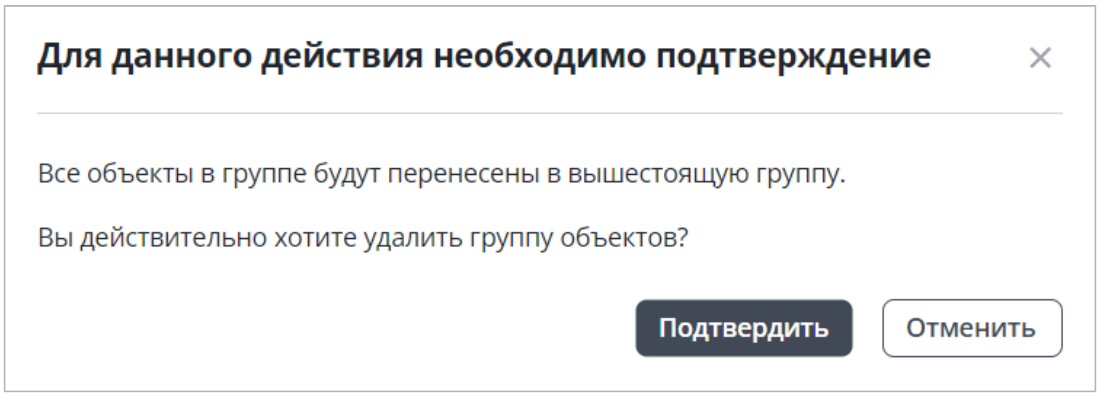


Рис. 370. Окно подтверждения

3. Нажмите кнопку **Подтвердить**.

16.2.3.5. Управление репозиториями

Управление репозиториями возможно только после входа в Version Control Desktop App с подключением к серверу Version Control Management.

В этом разделе:

- Просмотр репозиториев
- Создание репозитория

- Подключение репозитория
- Редактирование репозитория
- Удаление связи между локальным и серверным хранилищем
- Блокировка и разблокировка проекта
- Настройка исключений
- Изменение расположения локального хранилища

16.2.3.5.1. Просмотр репозиториев

Для просмотра репозитория нажмите на его наименование в левом боковом меню. По умолчанию открывается вкладка **Версии проекта**.

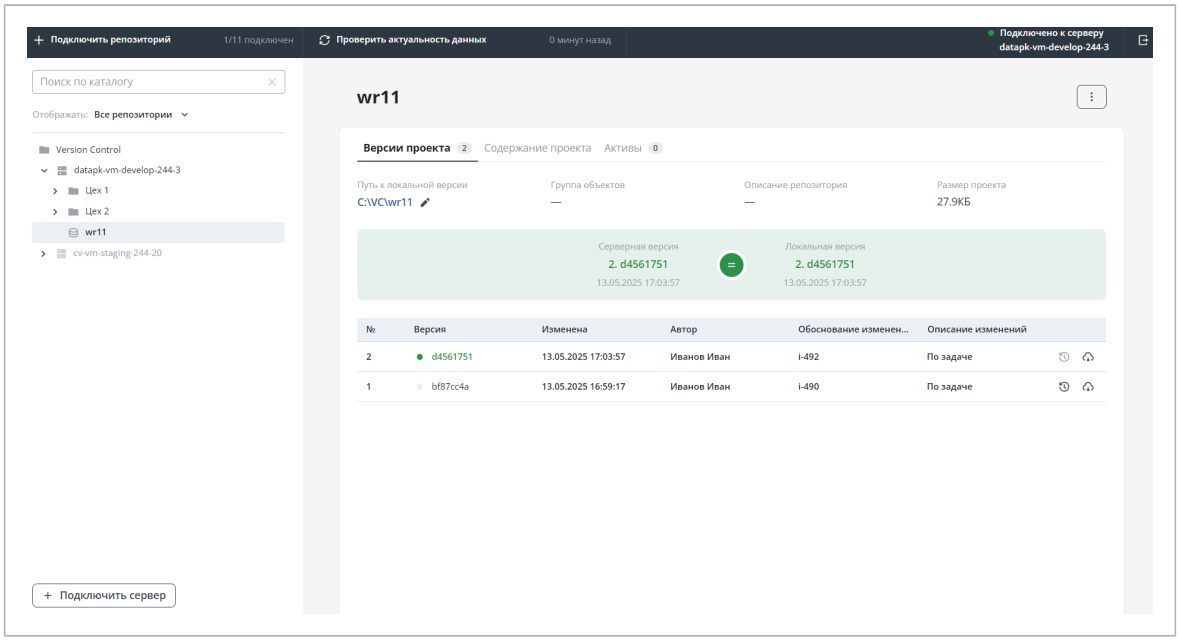


Рис. 371. Репозиторий

Страница репозитория имеет три вкладки: **Версии проекта**, **Содержание проекта** и **Активы**.

С помощью кнопки в правом верхнем углу можно выполнить следующие действия:

- Заблокировать репозиторий.
- Редактировать репозиторий.
- Настроить исключения.
- Забыть проект.

В этом разделе:

- Просмотр версий проекта
- Просмотр содержания проекта
- Просмотр активов

16.2.3.5.1.1. Просмотр версий проекта

На вкладке **Версии проекта** содержится информация о проекте и таблица версий проекта. Для каждой версии отображается:

- Порядковый номер.
- Наименование.
- Дата изменения.
- Пользователь, создавший версию.
- Основание для внесения изменений.
- Описание изменений версии проекта.

Версию проекта можно скачать с помощью кнопки в той же строке. Кнопка позволяет восстановить одну из предыдущих версий.

При нажатии на версию проекта открывается вкладка **Содержание проекта** и отображается содержимое выбранной версии.

С помощью кнопки можно изменить путь к локальному хранилищу репозитория. Нажатие на ссылку пути к файлу открывает локальное хранилище.

В левом боковом меню возле имени репозитория может отображаться значок статуса репозитория. Перечень всех значков статусов репозитория см. в разделе Статусы репозиториев.

Статус репозитория зависит от версии проекта и статуса подключения. Репозиторий может находиться в следующих статусах:

- Репозиторий подключен, серверная и локальная версии проекта совпадают.

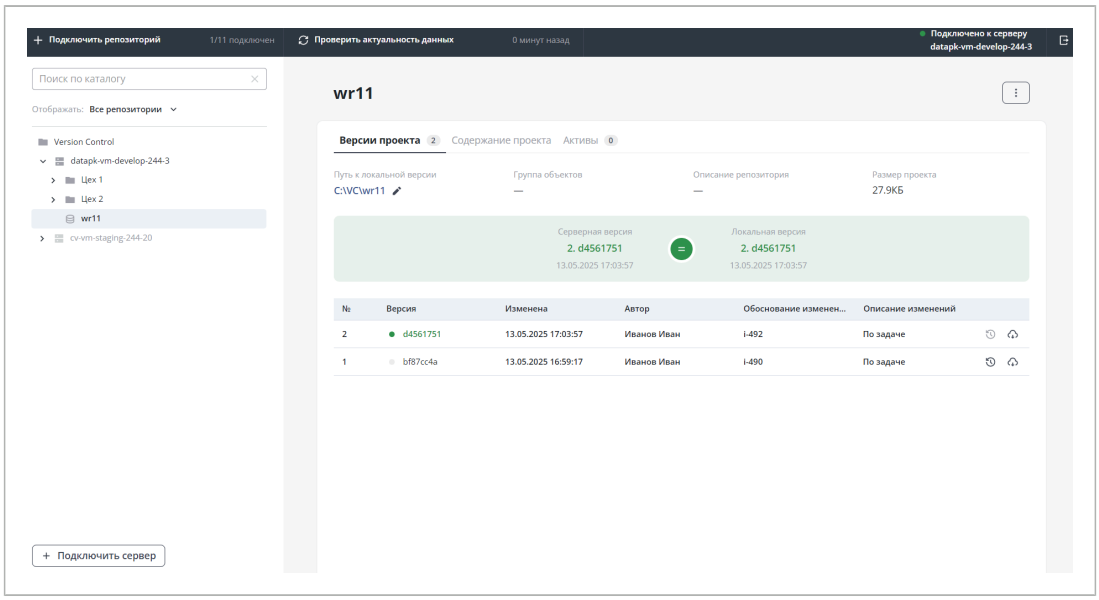


Рис. 372. Репозиторий, где серверная и локальная версии совпадают

- Репозиторий подключен, серверная версия проекта новее локальной.

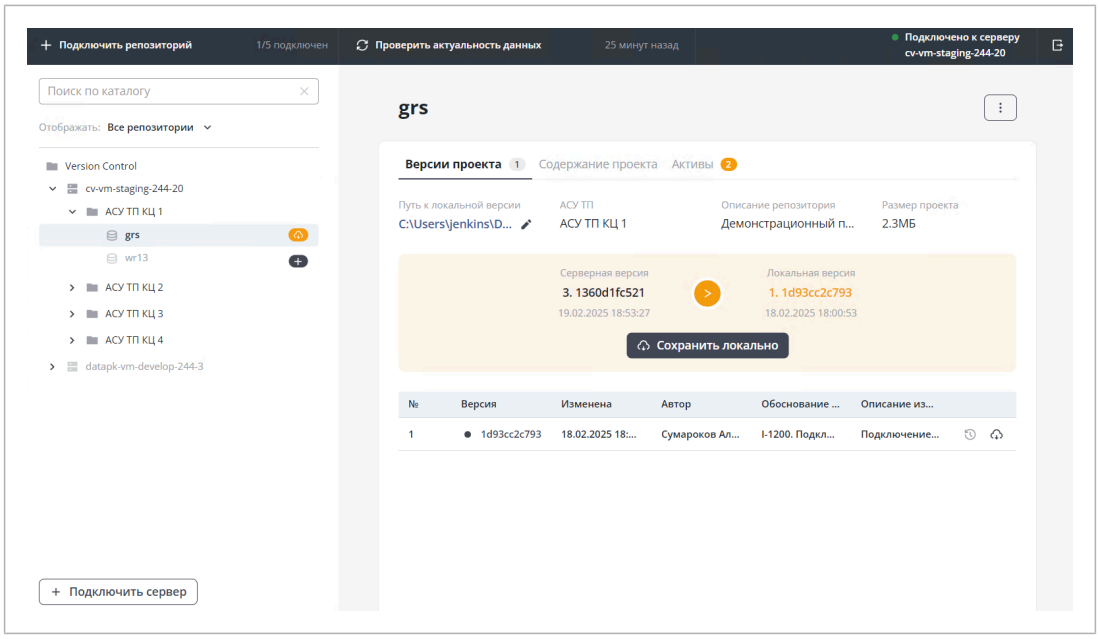


Рис. 373. Репозиторий, где серверная версия новее, чем локальная

- Репозиторий подключен, локальное хранилище изменено, новая версия не создана.

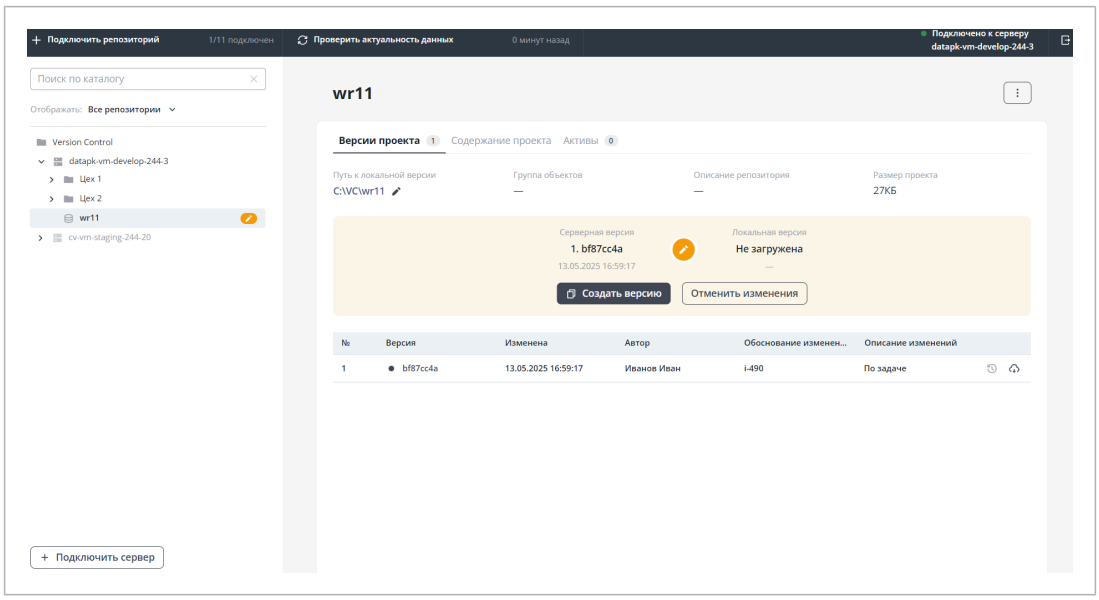


Рис. 374. Репозиторий, в котором изменили локального хранилища

- Репозиторий подключен, локальное хранилище изменено, новая версия создана, но еще не загружена на сервер.

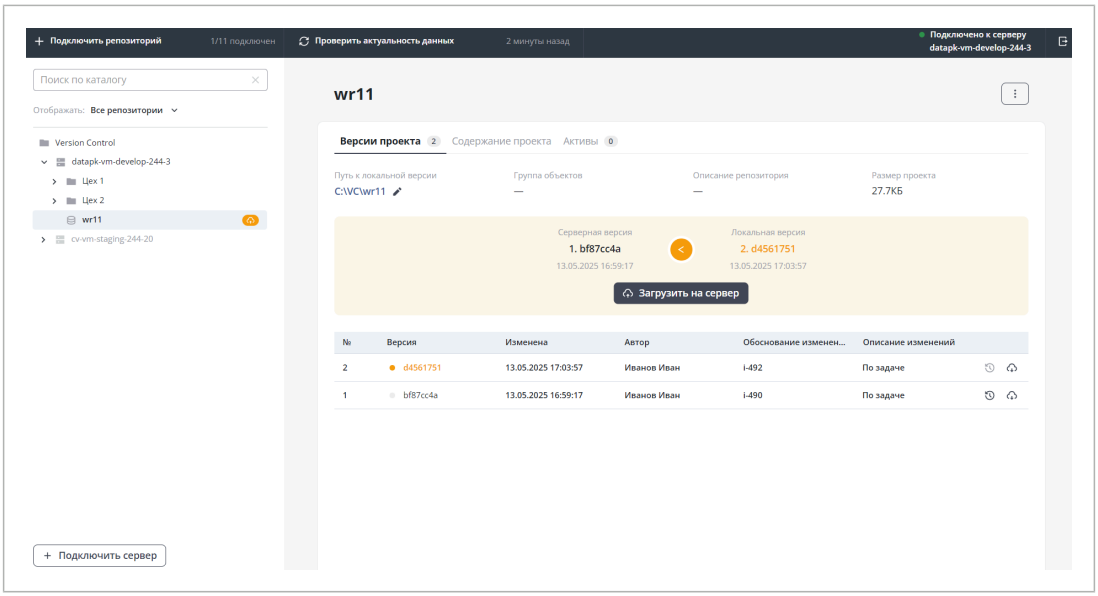


Рис. 375. Репозиторий, где локальная версия новее, чем серверная

- Репозиторий подключен, файлов и версий проекта в нем еще нет.

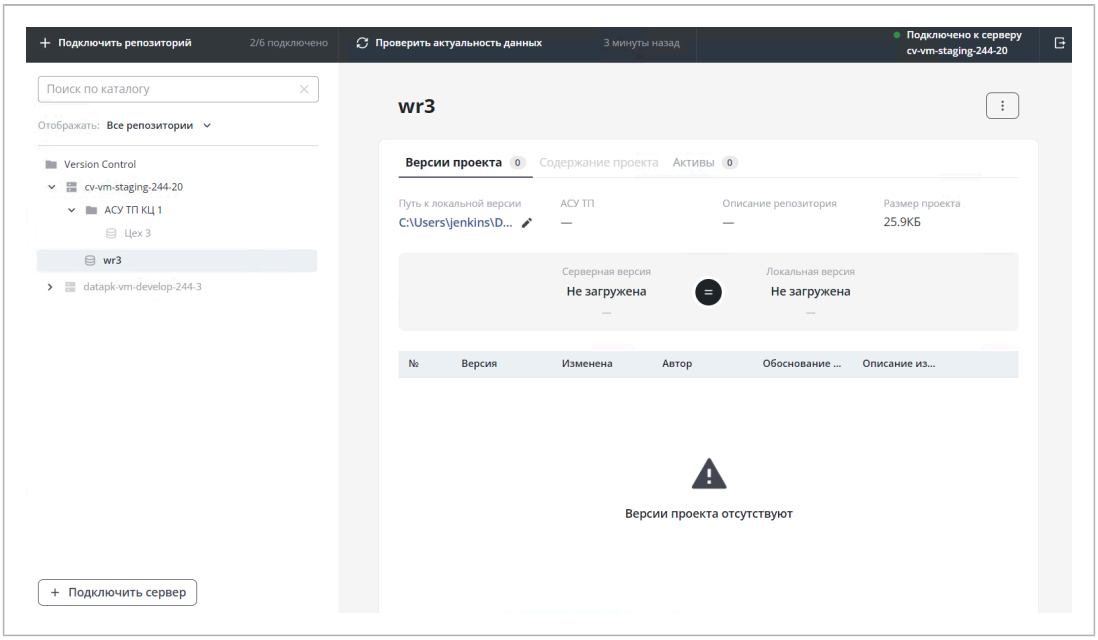


Рис. 376. Пустой репозиторий

- Репозиторий не подключен к локальному хранилищу.

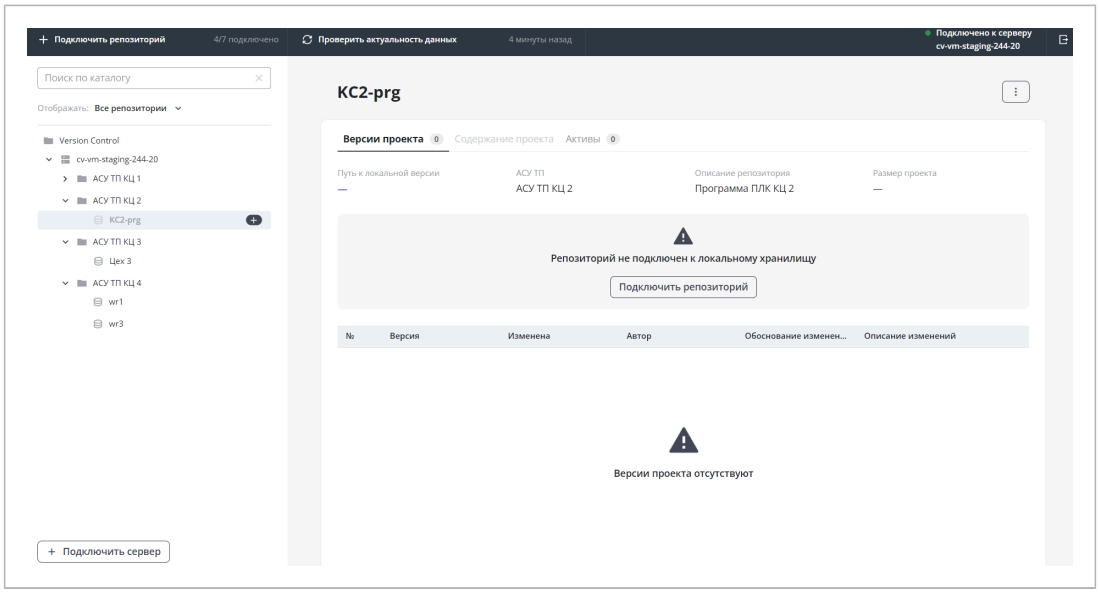


Рис. 377. Репозиторий, который не подключили к локальному хранилищу

- Сервер репозитория не подключен.

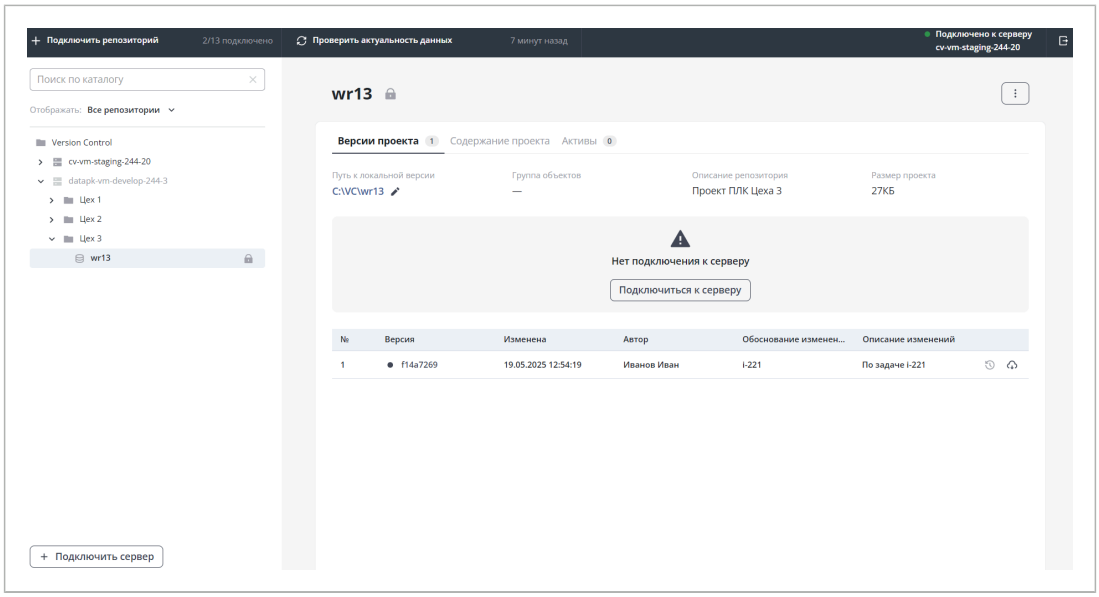


Рис. 378. Репозиторий, к серверу которого не было выполнено подключение

- Подключенный репозиторий был удален на сервере.

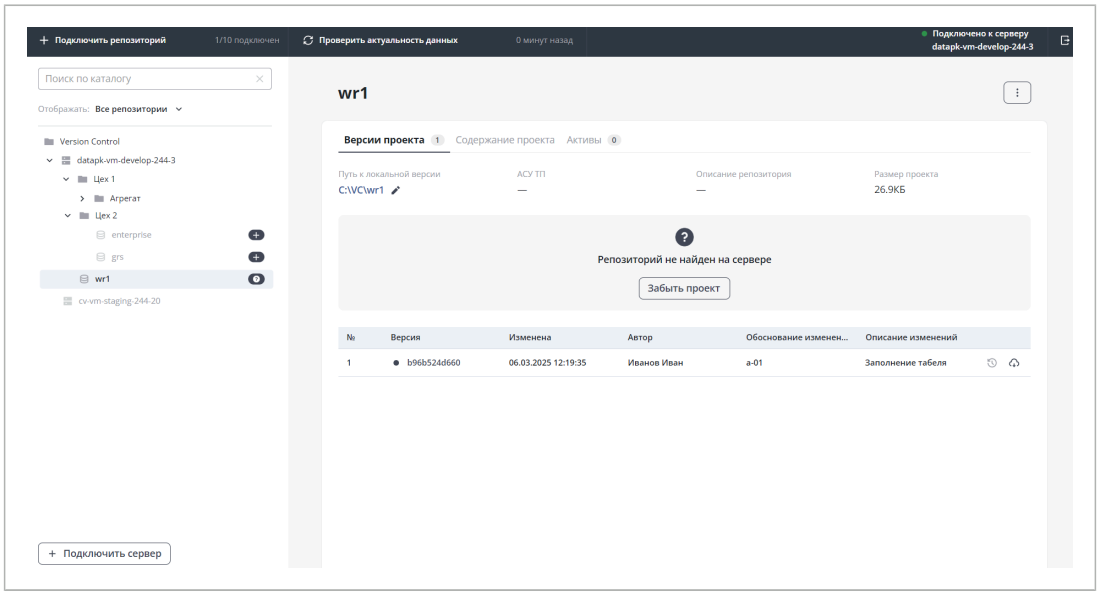


Рис. 379. Репозиторий не найден на сервере

Состояние репозитория также зависит от статуса блокировки проекта. Если проект был заблокирован, то репозиторий может находиться в следующих состояниях:

- Проект был заблокирован самим пользователем.

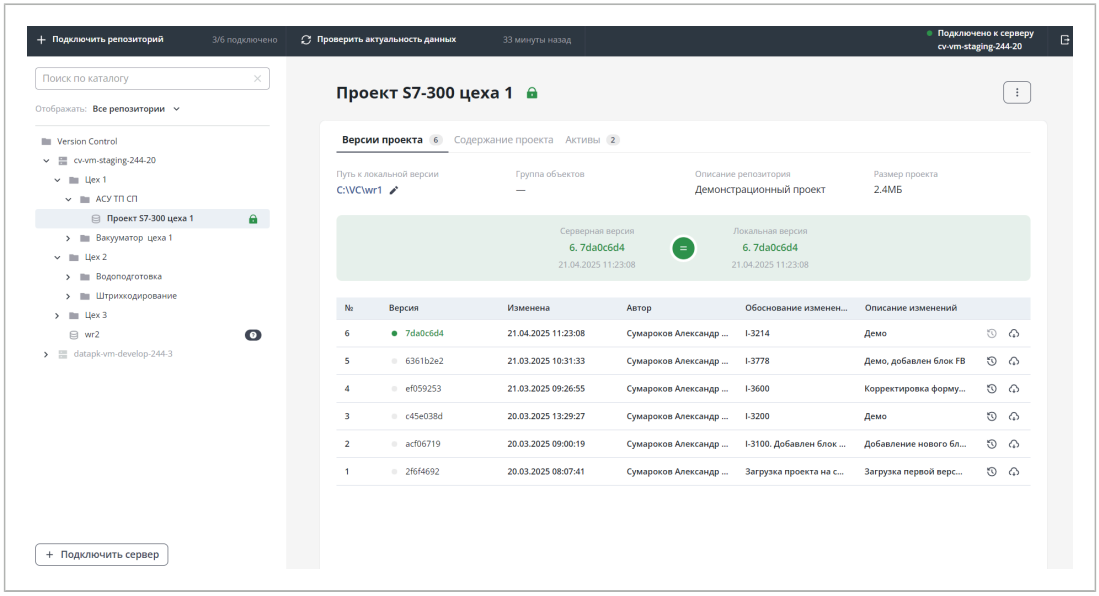


Рис. 380. Репозиторий заблокирован самим пользователем

- Проект был заблокирован другим пользователем.

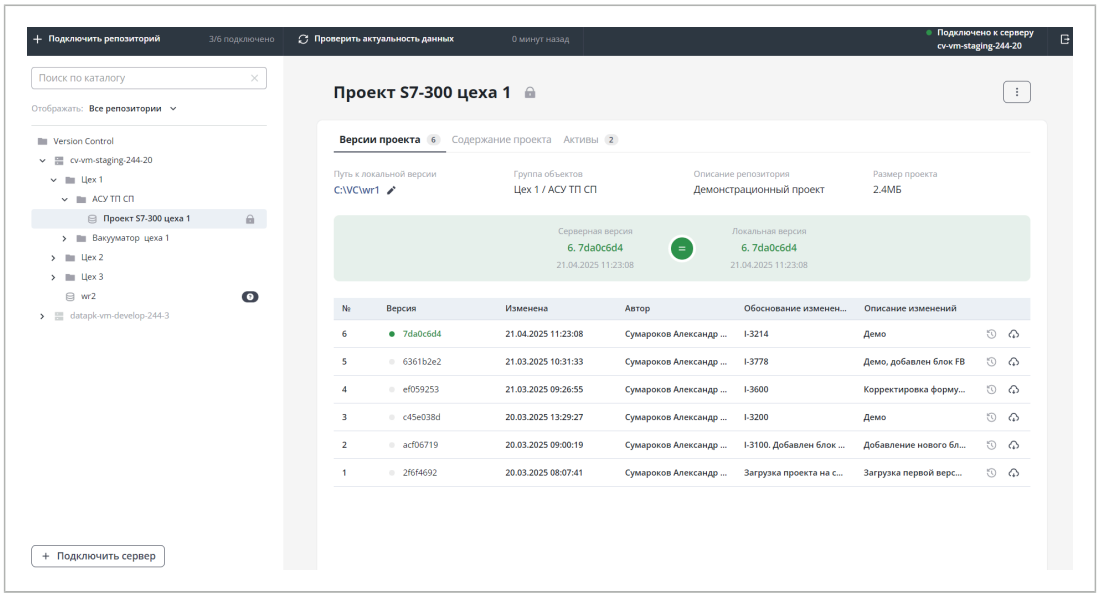


Рис. 381. Репозиторий заблокирован другим пользователем

16.2.3.5.1.2. Просмотр содержания проекта

На вкладке **Содержание проекта** можно изучить содержимое любой из версий проекта, для этого в выпадающем меню **Версия** нужно выбрать версию. В таблице отображается содержимое выбранной версии проекта. С помощью кнопки в правой части таблицы можно скачать соответствующий файл.

Кнопка **Скачать версию** скачивает все файлы выбранной версии проекта.

После выбора старой версии проекта появляется кнопка **Восстановить версию**. С ее помощью можно восстановить выбранную версию проекта в локальном хранилище и загрузить ее на сервер.

> **Внимание:**
>
> Для корректной работы приложения необходимо всегда закрывать среду разработки перед началом восстановления версии.

Возможна сортировка файлов по их автору изменения, дате изменения и их наименованию. По умолчанию выполнена сортировка по наименованию файлов в алфавитном порядке.

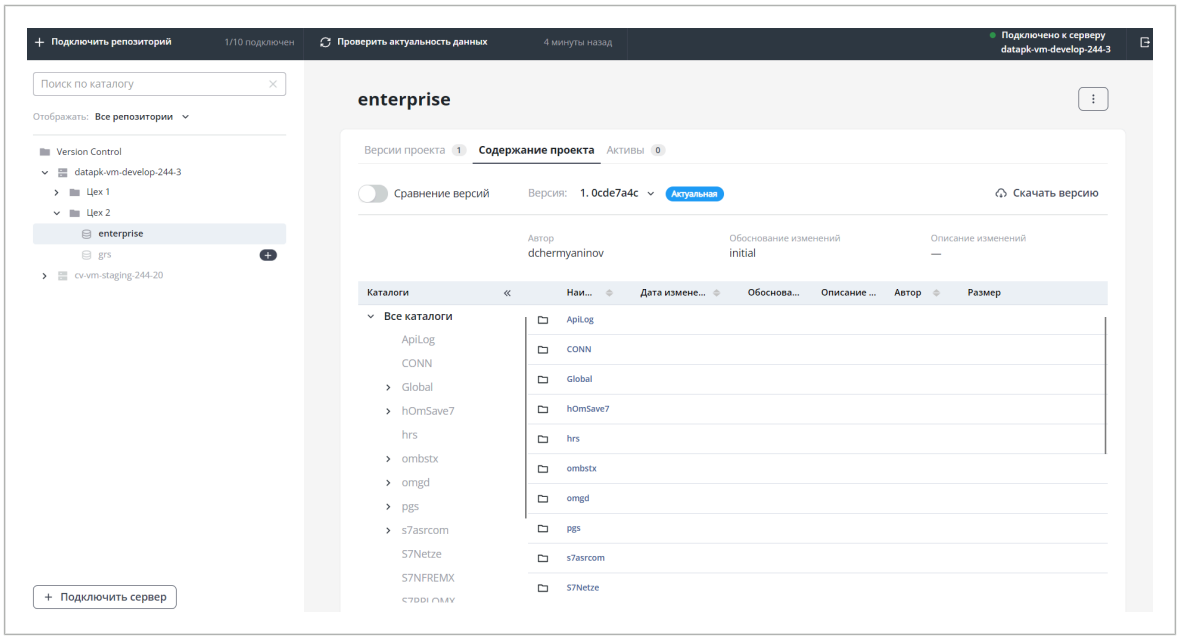


Рис. 382. Вкладка «Содержание проекта»

Просмотр содержимого файла

Для просмотра содержимого файла нужно нажать на него. После этого откроется окно, в котором отобразится информация о файле и его содержимое.

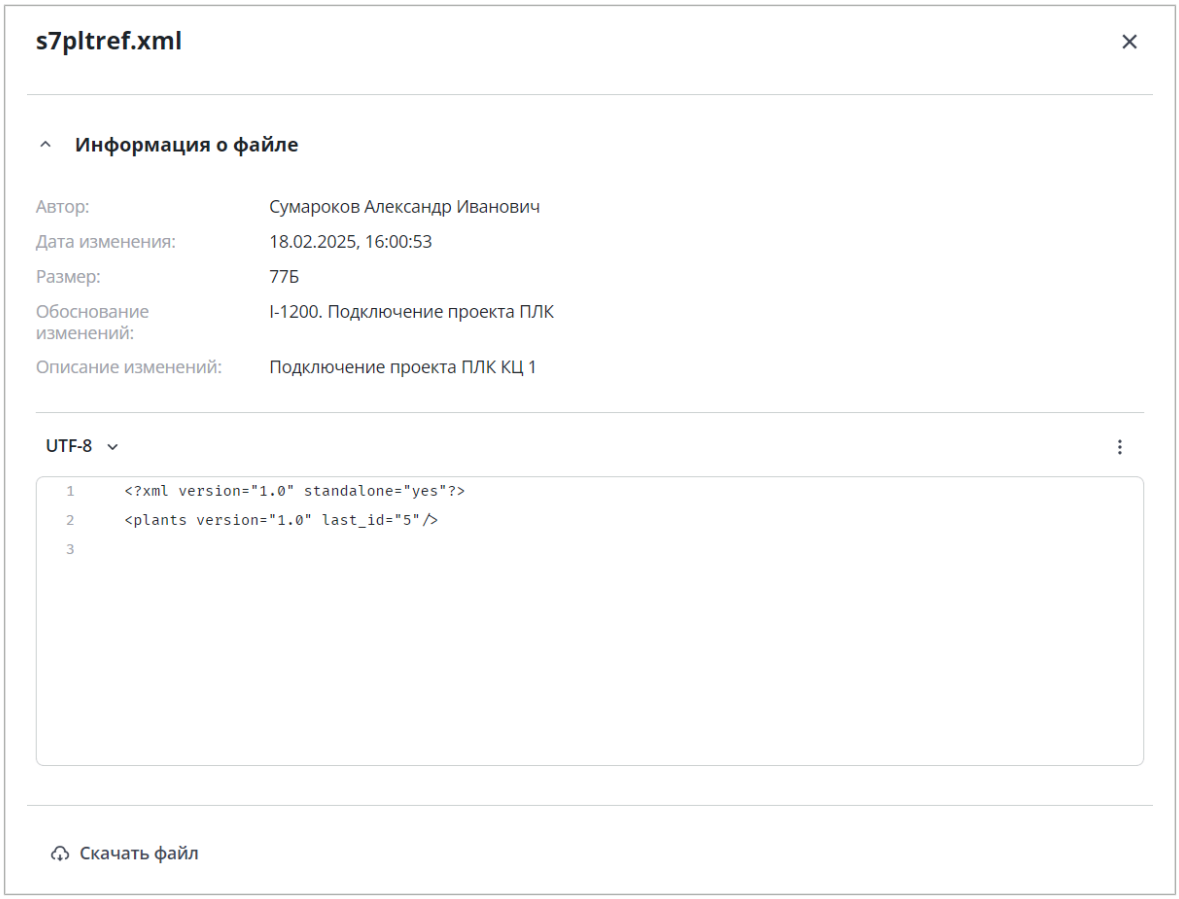


Рис. 383. Просмотр содержимого файла

Приложение автоматически определяет кодировку файла, при необходимости кодировку можно поменять в выпадающем меню над областью с содержимым файла. Доступные варианты кодировки:

- ASCII
- ISO-8859-1
- UTF-16
- UTF-8
- UTF-8-SIG
- WINDOWS-1251
- WINDOWS-1252

С помощью кнопки ⋮ можно включить отображение спецсимволов в области с содержимым файла. Подробнее о спецсимволах см. в разделе «Спецсимволы».

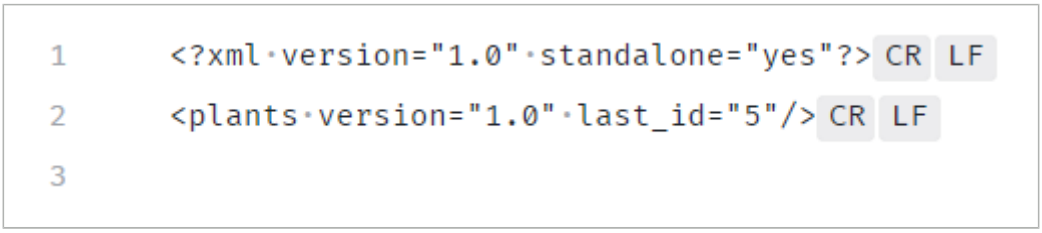


Рис. 384. Отображение спецсимволов включено

Посмотреть содержимое можно только у текстовых файлов. Для просмотра остальных файлов их необходимо скачать с помощью кнопки **Скачать файл** внизу окна.

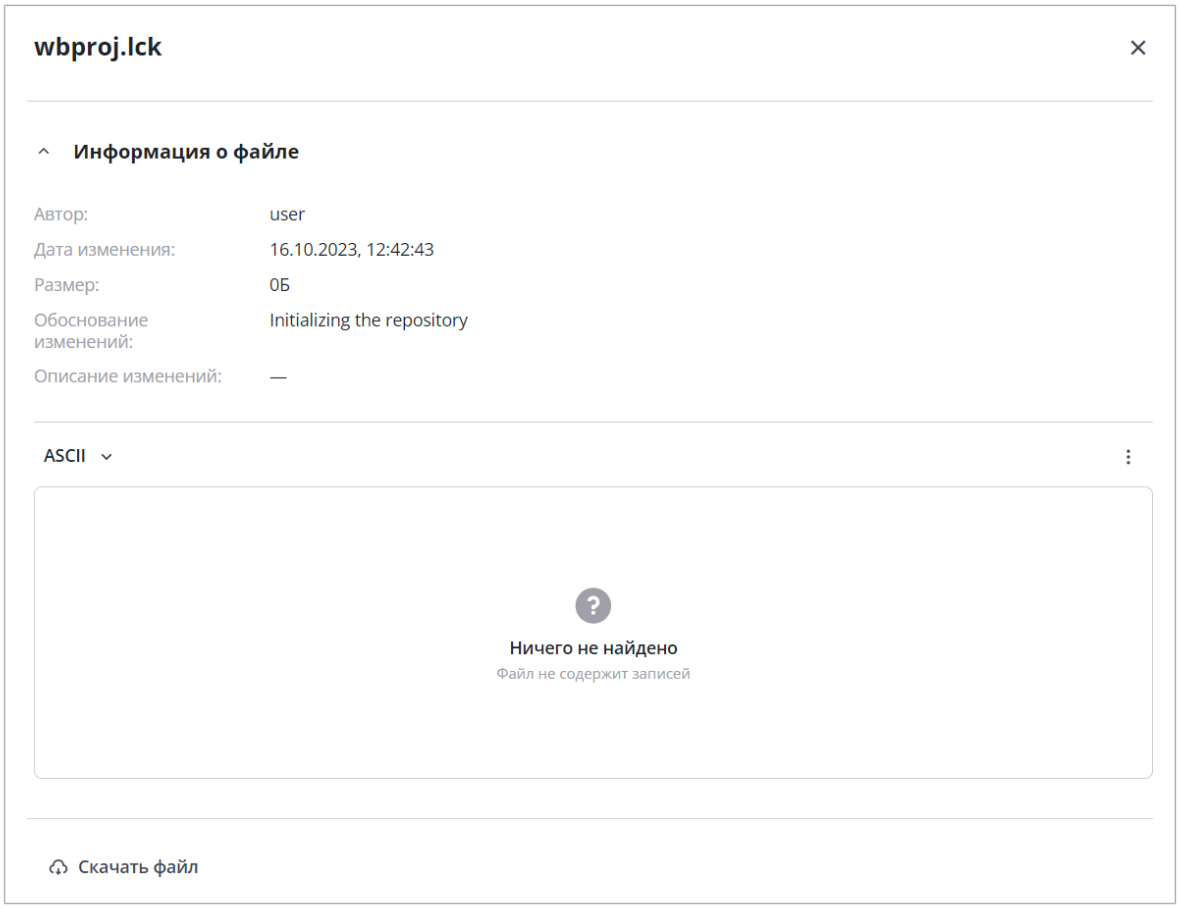


Рис. 385. Пустой файл

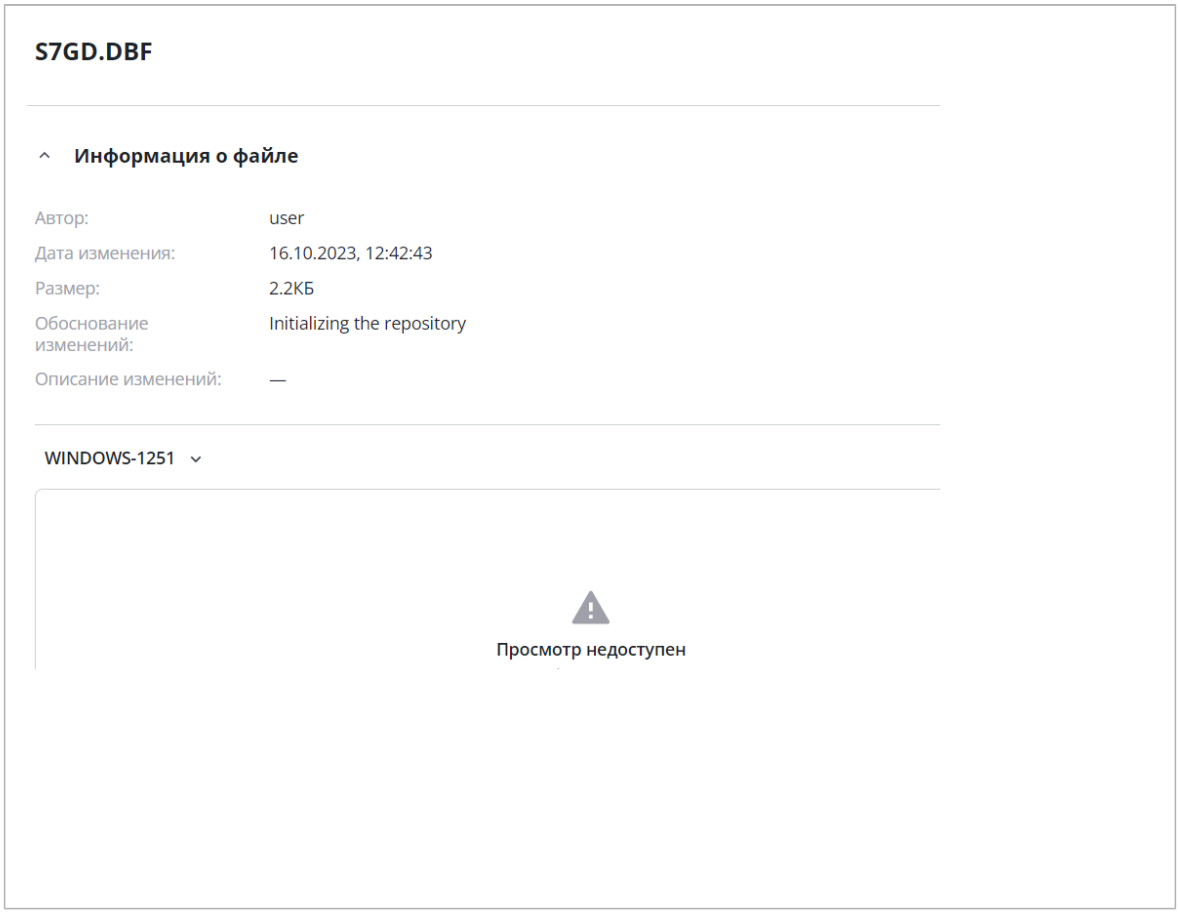


Рис. 386. Бинарный файл

Сравнение версий

Опция **Сравнение версий** позволяет сравнить изменения выбранной версии проекта и ее предыдущей версии.

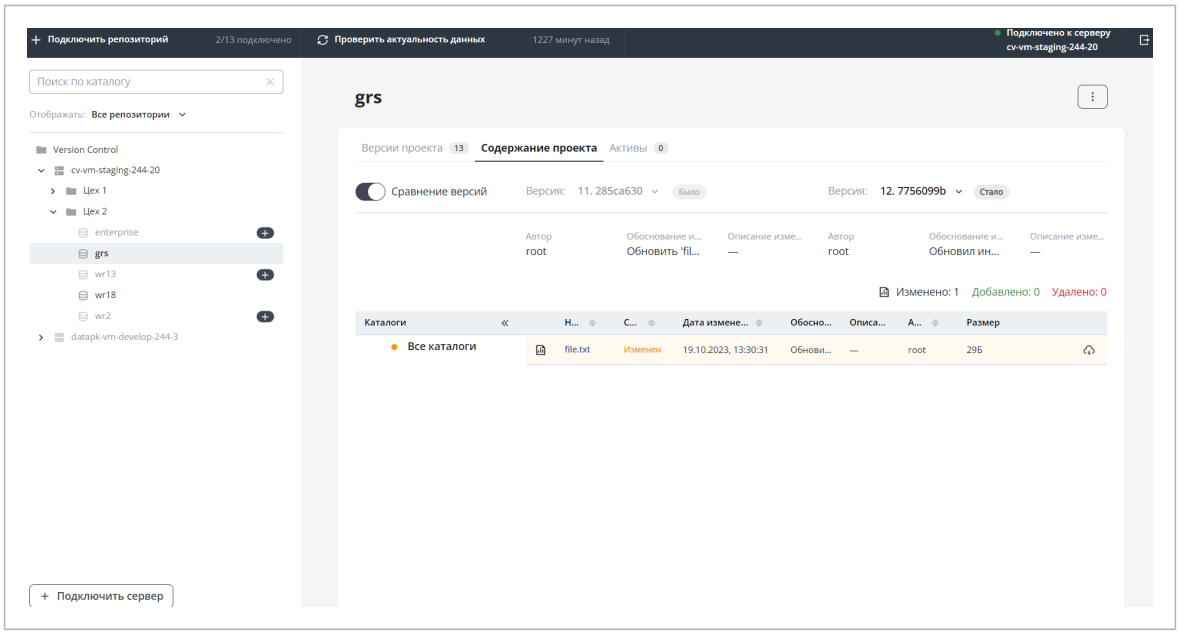


Рис. 387. Сравнение версий

Цветами отмечены изменения элементов проекта:

- Зеленый — элемент добавлен.
- Красный — элемент удален.
- Желтый — элемент изменен.

При нажатии на строку с файлом открывается окно с описанием изменений файла.

В режиме сравнения возможно скачивание файлов более новой версии с помощью кнопки справа от файлов.

Просмотр изменений в файле возможен лишь для текстовых файлов. Чтобы видеть только измененные данные, необходимо установить чекбокс **Только измененные**.

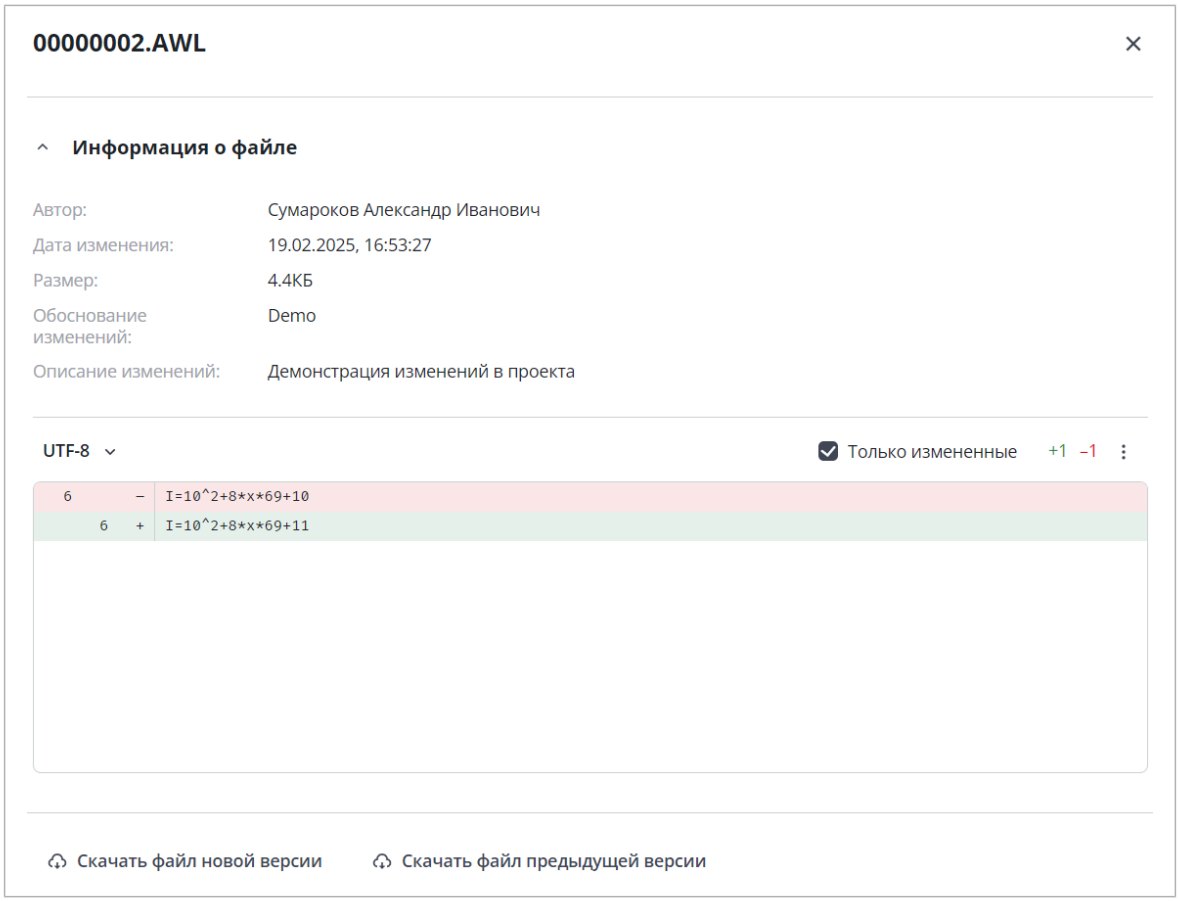


Рис. 388. Отображение только измененных данных файла

16.2.3.5.1.3. Просмотр активов

На вкладке **Активы** содержится информация о подключенных к репозиторию активах с типом ПЛК (подключение активов с другими типами также доступно). Подробнее о подключенных ПЛК см. в разделе «Подключенные активы».

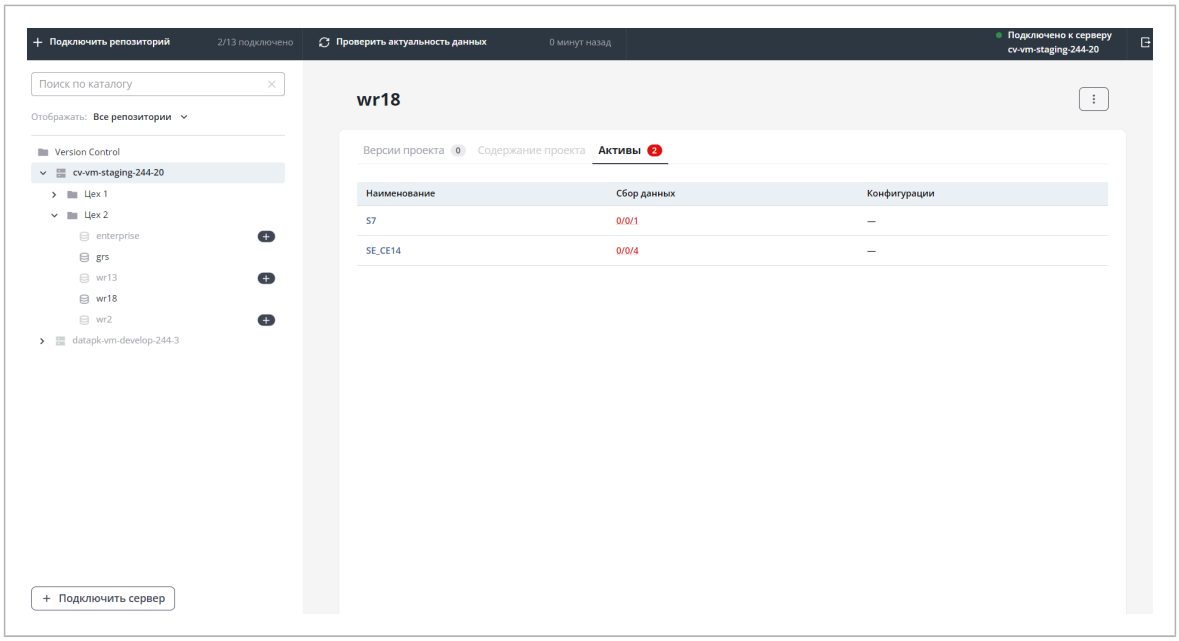


Рис. 389. Подключенные ПЛК

16.2.3.5.2. Создание репозитория

Чтобы создать репозиторий:

1. Нажмите правой кнопкой мыши в левом боковом меню на сервер или группу.
2. В открывшемся меню выберите **Репозиторий → Создать**.
   - **Результат шага:** откроется окно создания репозитория.

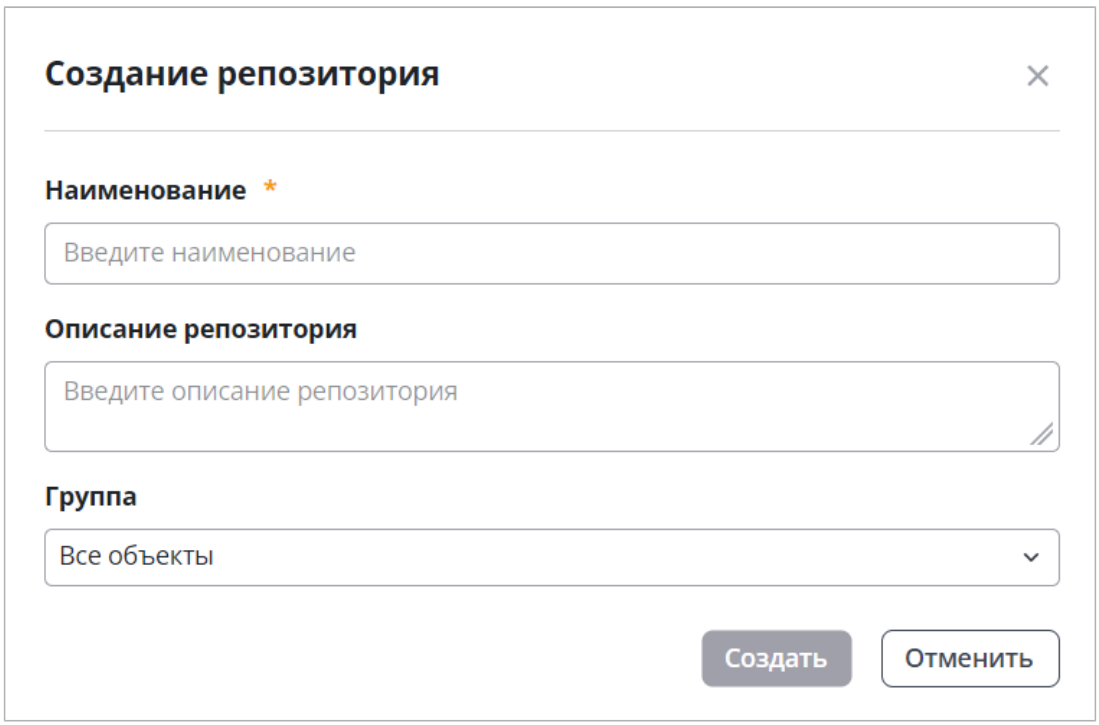


Рис. 390. Создание репозитория

3. Заполните поля **Наименование** и **Описание репозитория**.
4. В выпадающем списке **Группа** выберите подходящую группу для нового репозитория.
5. Нажмите кнопку **Создать**.

16.2.3.5.3. Подключение репозитория

> Внимание:
>
> Для подключения непустого репозитория можно выбрать только пустой каталог.

Есть несколько способов подключения репозитория в Version Control Desktop App:

- Подключение репозитория
- Подключение определенного репозитория на его странице
- Подключение определенного репозитория через боковое меню
- Подключение репозитория определенной группы

16.2.3.5.3.1. Подключение репозитория

1. Нажмите кнопку **Подключить репозиторий** в левом верхнем углу.
   - **Результат шага:** откроется окно подключения репозитория.

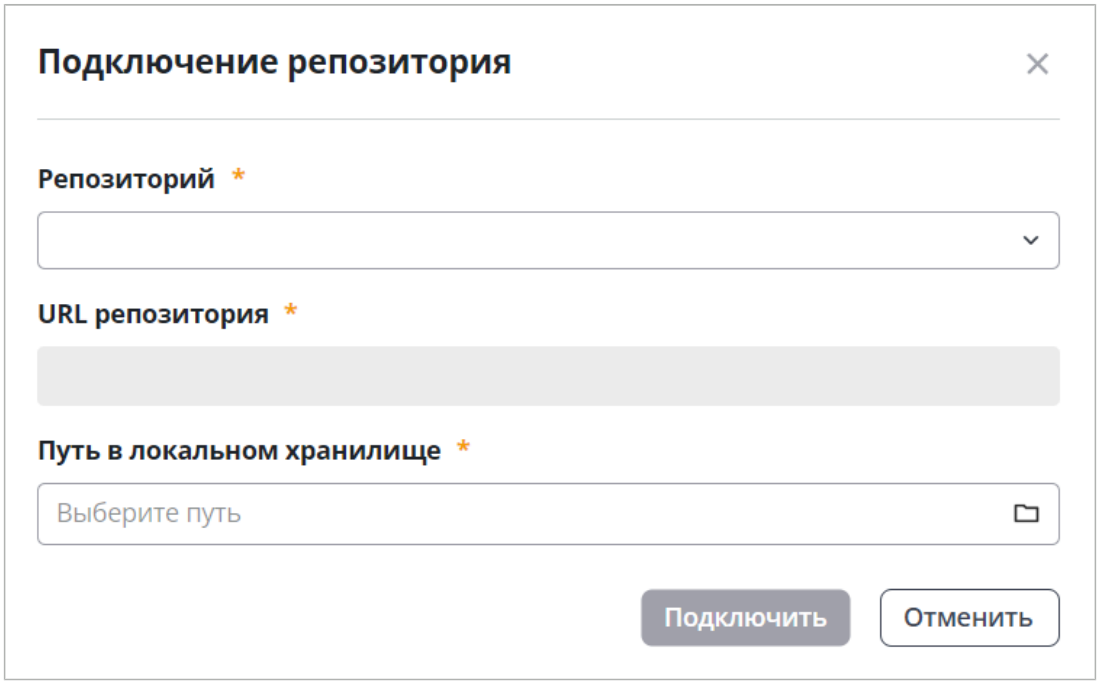


Рис. 391. Подключение репозитория

2. В выпадающем списке **Репозиторий** выберите нужный репозиторий.
3. Заполните поле **Путь в локальном хранилище** или выберите локальное хранилище с помощью кнопки
   - **Результат шага:** Станет активна кнопка **Подключить**.
4. Нажмите кнопку **Подключить**.

- **Результат шага:** репозиторий будет подключен.

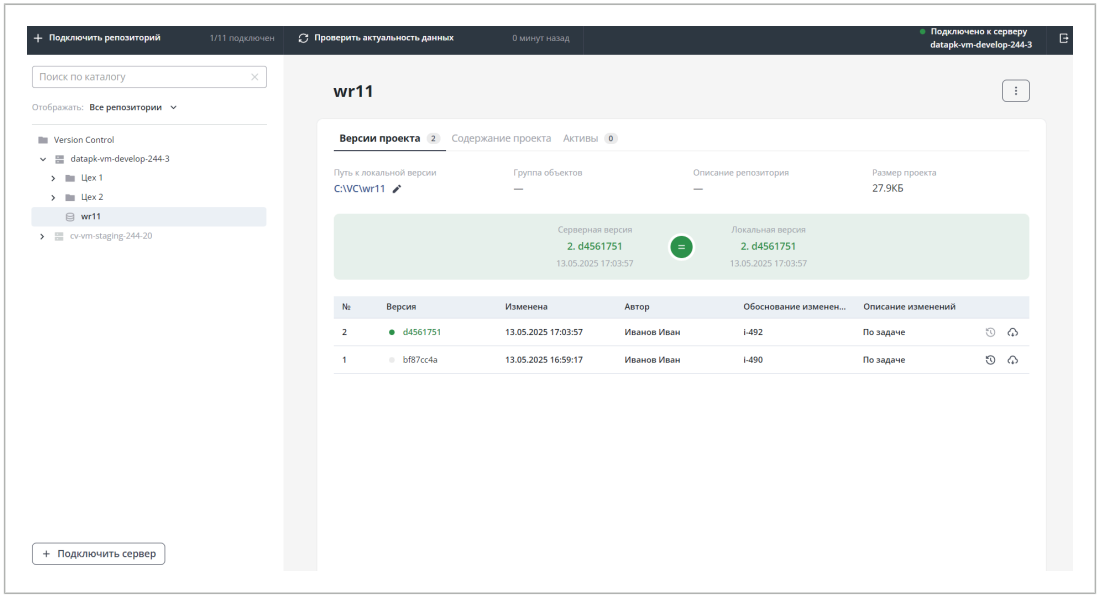


Рис. 392. Репозиторий подключен

16.2.3.5.3.2. Подключение определенного репозитория на его странице

1. Нажмите на наименование неподключенного репозитория в каталоге в левом боковом меню.
   - **Результат шага:** откроется страница неподключенного репозитория.

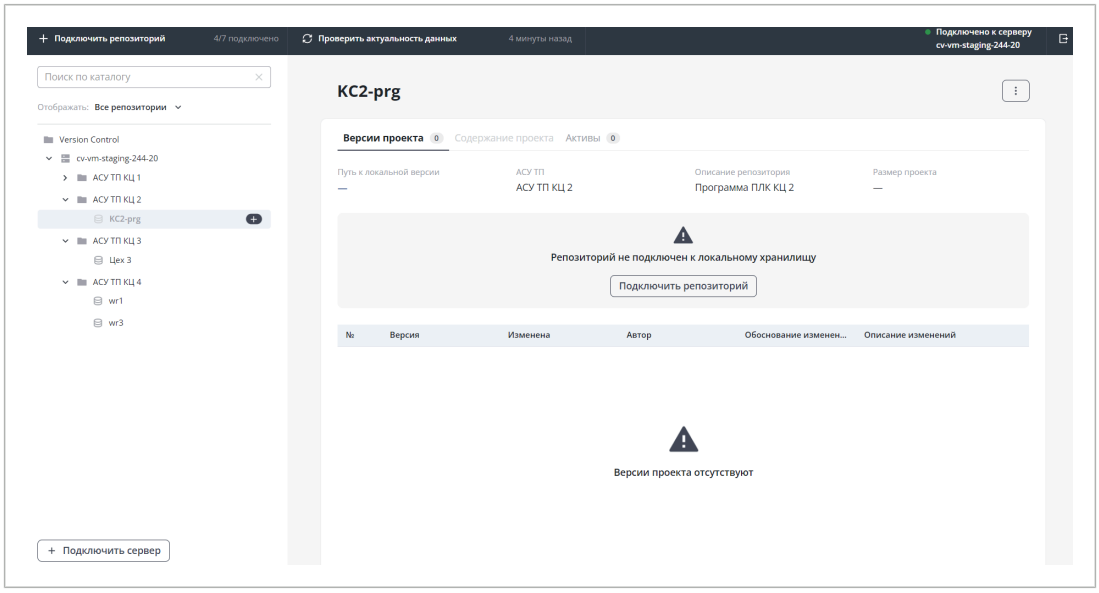


Рис. 393. Репозиторий не подключен

2. Нажмите кнопку **Подключить репозиторий** на странице неподключенного репозитория.
   - **Результат шага:** откроется окно подключения выбранного репозитория с уже заполненной информацией о нем.

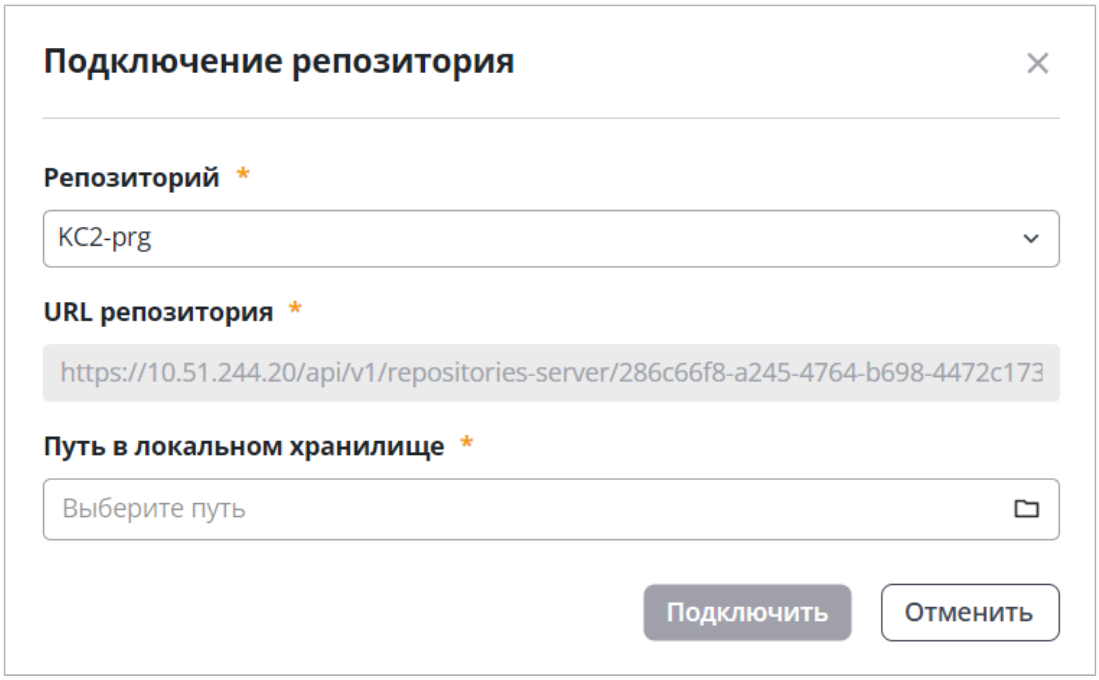


Рис. 394. Подключение выбранного репозитория

3. Заполните поле **Путь в локальном хранилище** или выберите локальное хранилище с помощью кнопки .
   - **Результат шага:** Станет активна кнопка **Подключить**.
4. Нажмите кнопку **Подключить**.
   - **Результат шага:** репозиторий будет подключен.

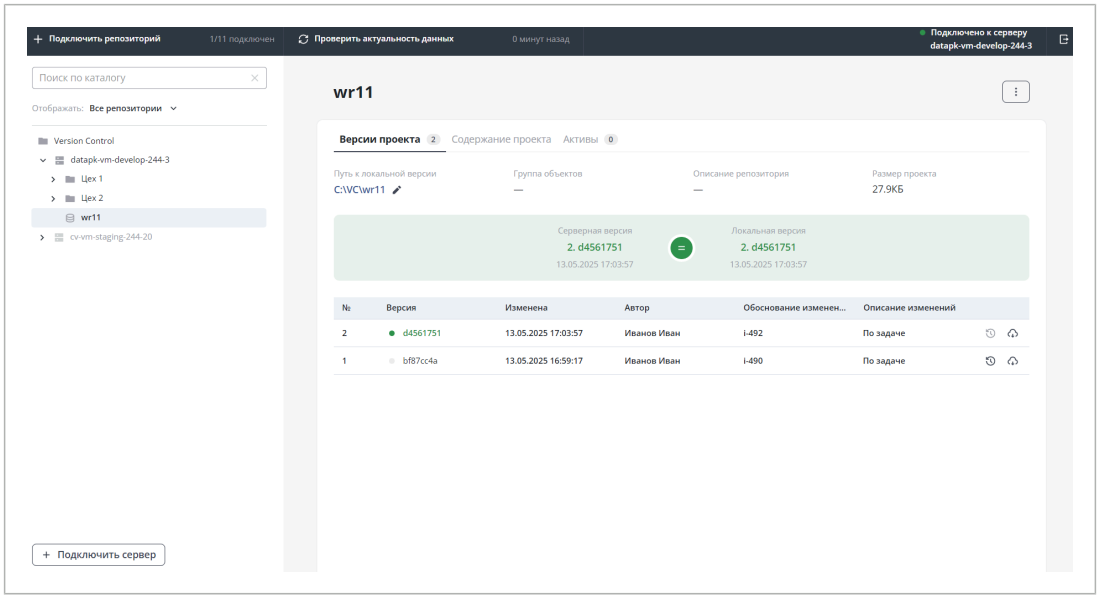


Рис. 395. Репозиторий подключен

16.2.3.5.3.3. Подключение определенного репозитория через боковое меню

1. Нажмите на значок статуса неподключенного репозитория в каталоге в левом боковом меню.
   - **Результат шага:** откроется окно подключения выбранного репозитория с уже заполненной информацией о нем.

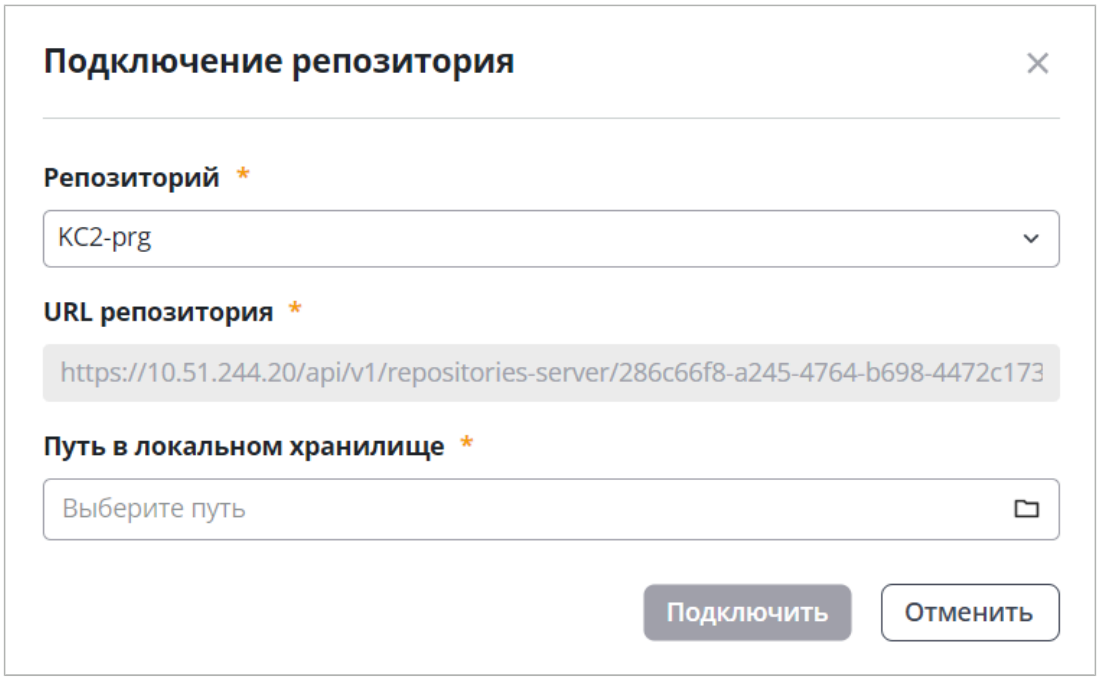


Рис. 396. Подключение выбранного репозитория

2. Заполните поле **Путь в локальном хранилище** или выберите локальное хранилище с помощью кнопки

   - **Результат шага:** Станет активна кнопка **Подключить**.

3. Нажмите кнопку **Подключить**.

   - **Результат шага:** репозиторий будет подключен.

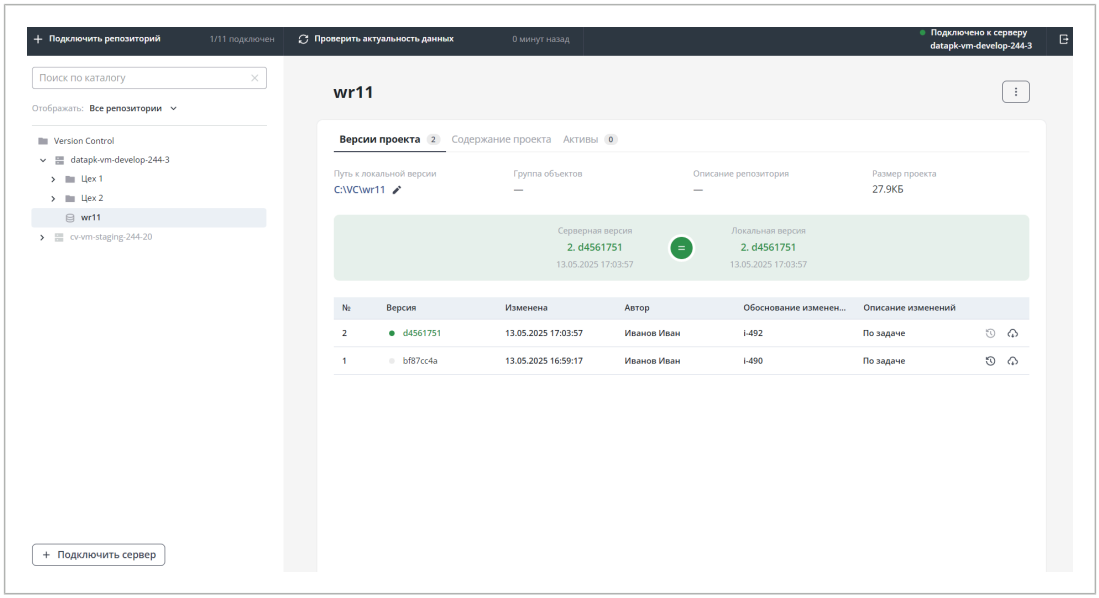


Рис. 397. Репозиторий подключен

16.2.3.5.3.4. Подключение репозитория определенной группы

1. Нажмите правой кнопкой мыши на наименование группы в левом боковом меню.
2. В открывшемся меню выберите **Репозиторий → Подключить**.

   - **Результат шага:** откроется окно подключения репозитория.

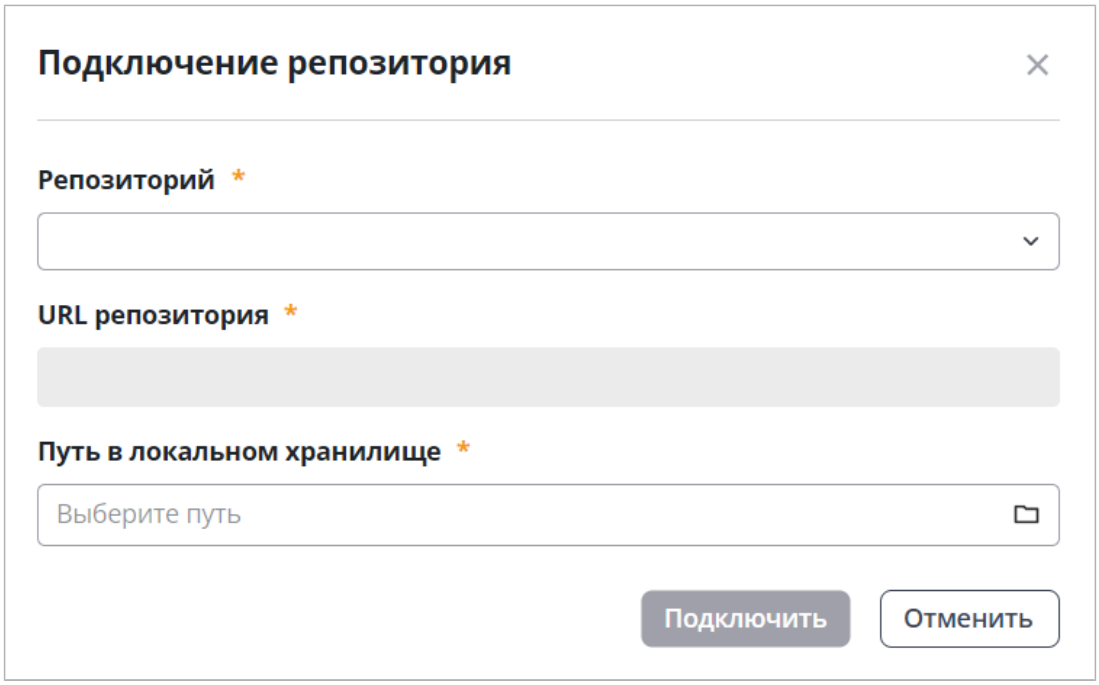


Рис. 398. Подключение репозитория

3. В выпадающем списке **Репозиторий** выберите нужный репозиторий.
4. Заполните поле **Путь в локальном хранилище** или выберите локальное хранилище с помощью кнопки

   - **Результат шага:** Станет активна кнопка **Подключить**.
5. Нажмите кнопку **Подключить**.
   - **Результат шага:** репозиторий будет подключен.

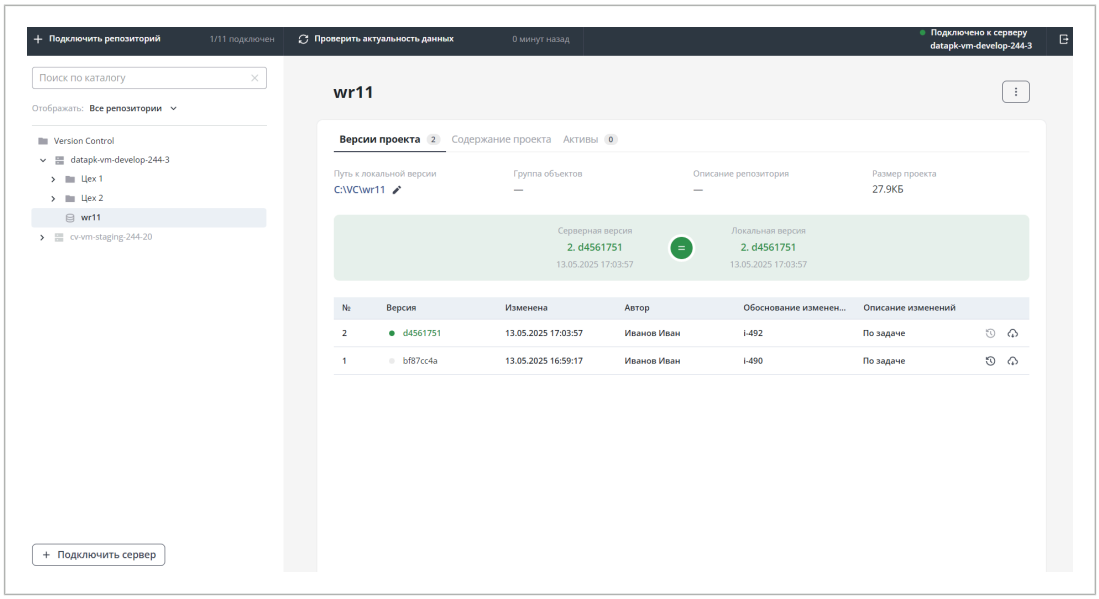


Рис. 399. Репозиторий подключен

16.2.3.5.4. Редактирование репозитория

Есть несколько способов редактировать репозиторий:

- Редактирование репозитория через боковое меню
- Редактирование репозитория на его странице

16.2.3.5.4.1. Редактирование репозитория через боковое меню

Чтобы редактировать репозиторий:

1. Нажмите правой кнопкой мыши в левом боковом меню на нужный репозиторий.
2. В открывшемся меню выберите **Репозиторий → Редактировать**.
   - **Результат шага:** откроется окно редактирования репозитория.

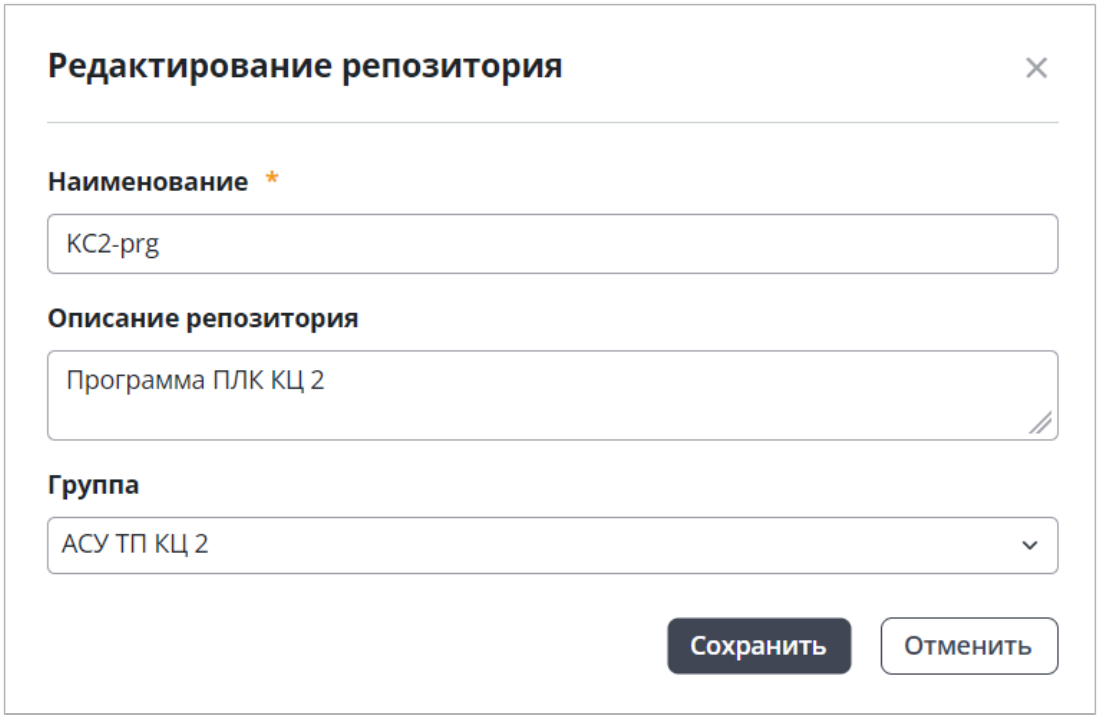


Рис. 400. Редактирование репозитория

3. Измените поля **Наименование**, **Описание репозитория** или группу в выпадающем списке **Группа**.
4. Нажмите кнопку **Сохранить**.

16.2.3.5.4.2. Редактирование репозитория на его странице

Чтобы редактировать репозиторий:

1. Нажмите на наименование нужного репозитория в каталоге в левом боковом меню.
   - **Результат шага:** откроется страница репозитория.

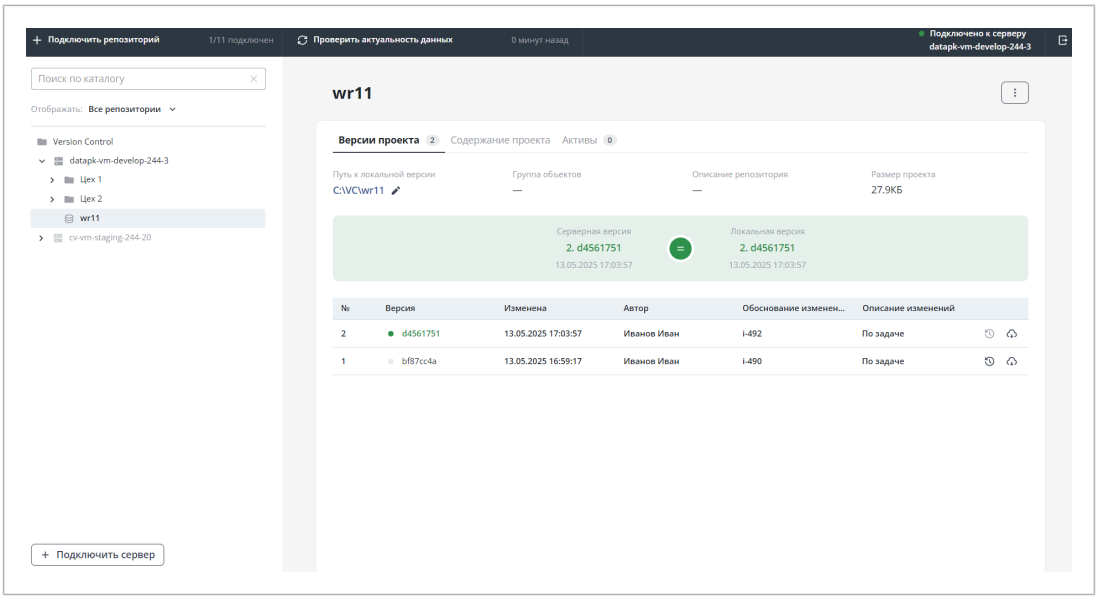


Рис. 401. Страница репозитория

2. Нажмите кнопку ⋮ в правом верхнем углу.
   - **Результат шага:** откроется меню репозитория.
3. Нажмите кнопку **Редактировать**.
   - **Результат шага:** откроется окно редактирования репозитория.

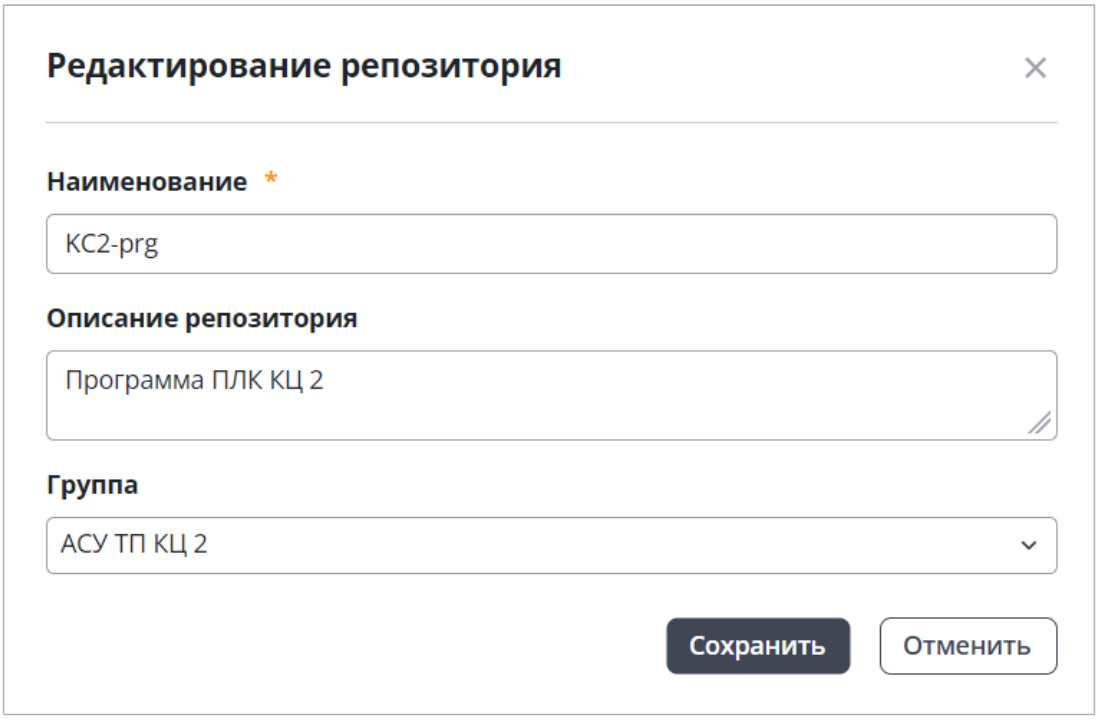


Рис. 402. Редактирование репозитория

4. Измените поля **Наименование**, **Описание репозитория** или группу в выпадающем списке **Группа**.
5. Нажмите кнопку **Сохранить**.

16.2.3.5.5. Удаление связи между локальным и серверным хранилищем

Удалить связь между локальным и серверным хранилищем можно с помощью функции **Забыть проект**, файлы проекта при этом сохраняются. История версий и информация о проекте удаляется из приложения Version Control Desktop App.

Забыть проект можно только у подключенного репозитория.

Есть несколько способов забыть проект:

- Забыть проект через боковое меню
- Забыть проект на его странице
- Забыть удаленный на сервере проект

16.2.3.5.5.1. Забыть проект через боковое меню

Чтобы забыть проект:

1. Нажмите правой кнопкой мыши в левом боковом меню на нужный репозиторий.
2. В открывшемся меню выберите **Репозиторий → Забыть**.

   ▸ **Результат шага:** откроется окно подтверждения удаления связи между локальным хранилищем и сервером.

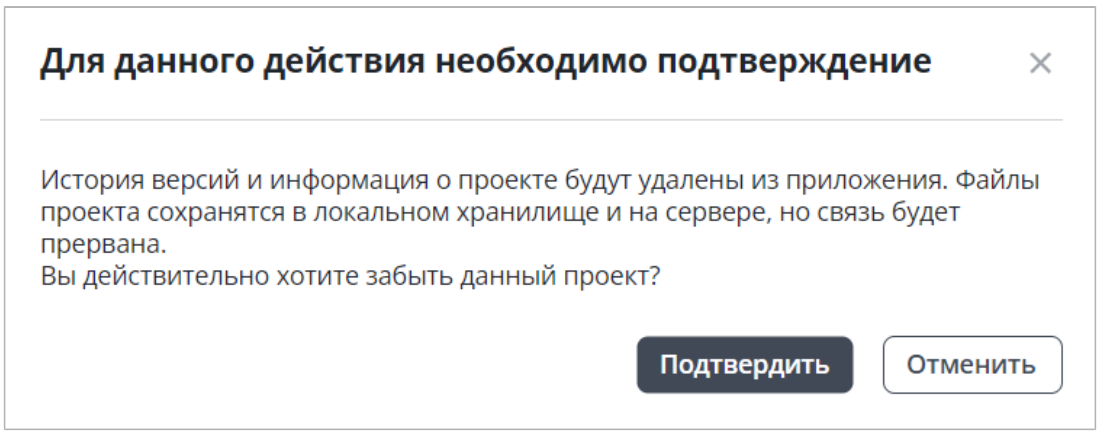


Рис. 403. Окно подтверждения

3. Нажмите на кнопку **Подтвердить**.

- **Результат шага:** связь между локальным и серверным хранилищами удалена.

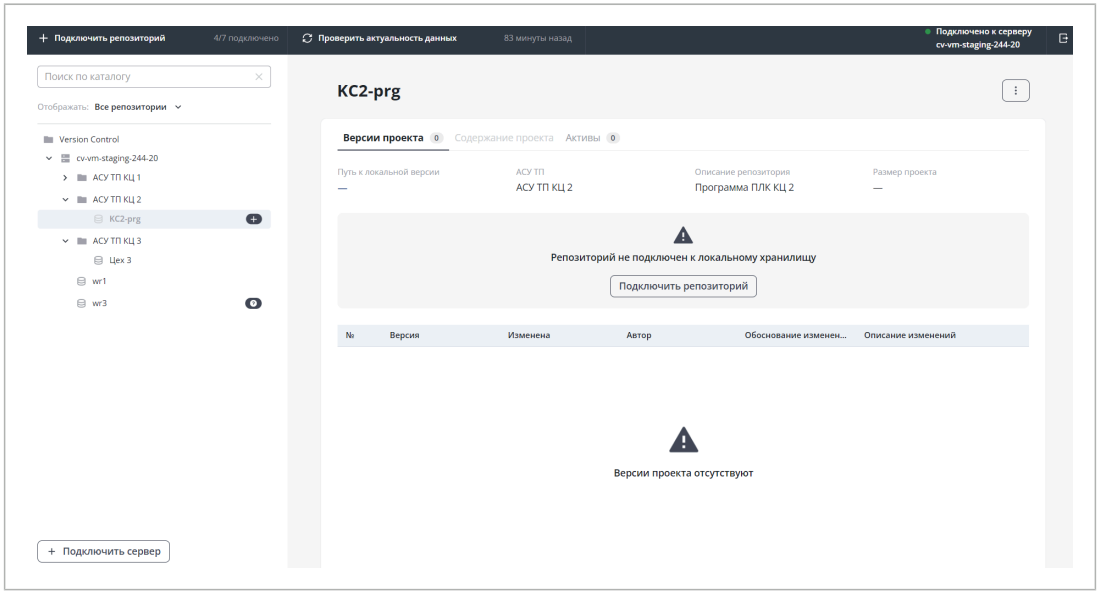


Рис. 404. Проект забыт

16.2.3.5.5.2. Забыть проект на его странице

Чтобы забыть проект:

1. Нажмите на наименование нужного репозитория в каталоге в левом боковом меню.
   - **Результат шага:** откроется страница репозитория.

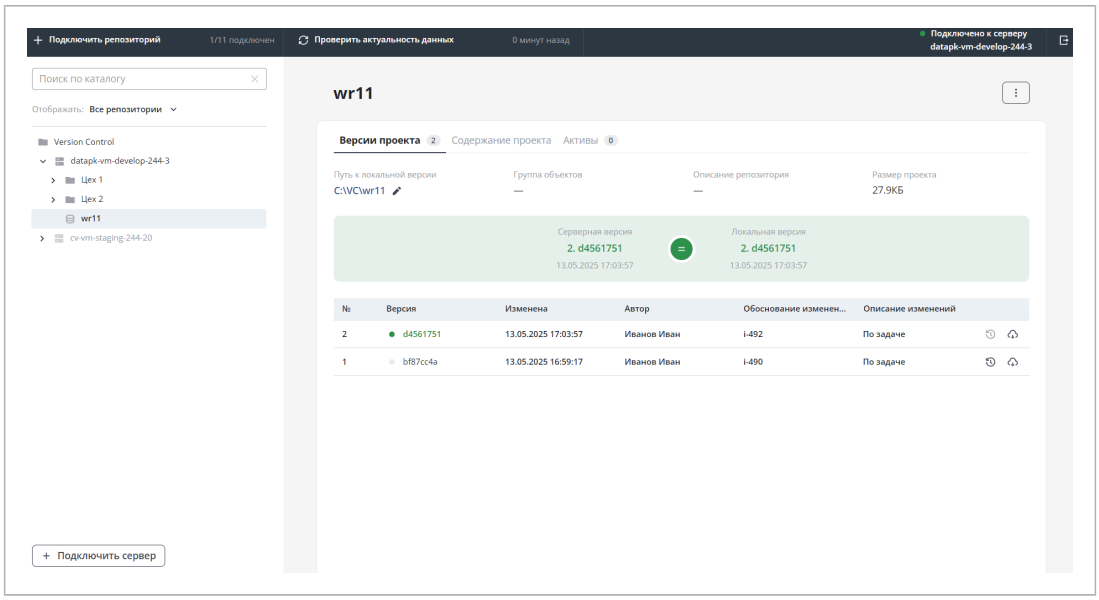


Рис. 405. Страница репозитория

2. Нажмите кнопку ⋮ в правом верхнем углу.
   - **Результат шага:** откроется меню репозитория.
3. Нажмите кнопку **Забыть**.
   - **Результат шага:** откроется окно подтверждения удаления связи между локальным хранилищем и сервером.

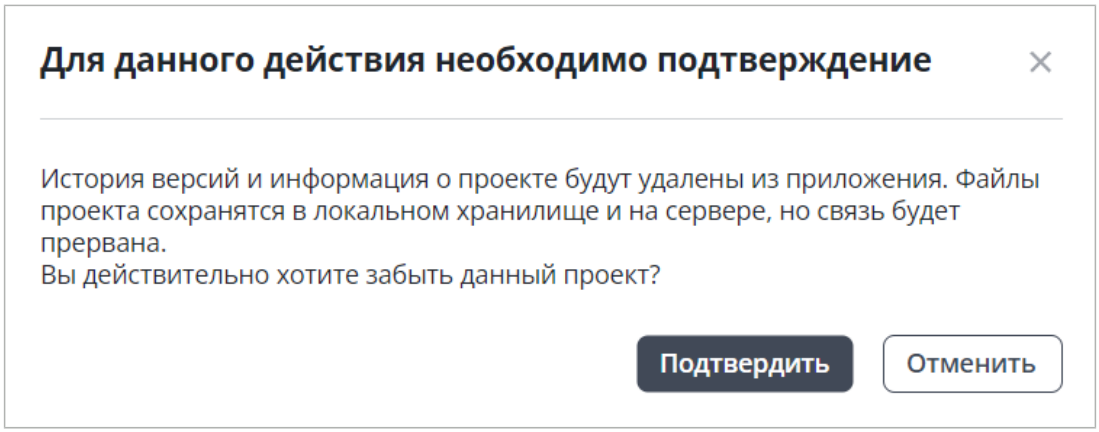


Рис. 406. Окно подтверждения

4. Нажмите на кнопку **Подтвердить**.
   - **Результат шага:** связь между локальным и серверным хранилищами удалена.

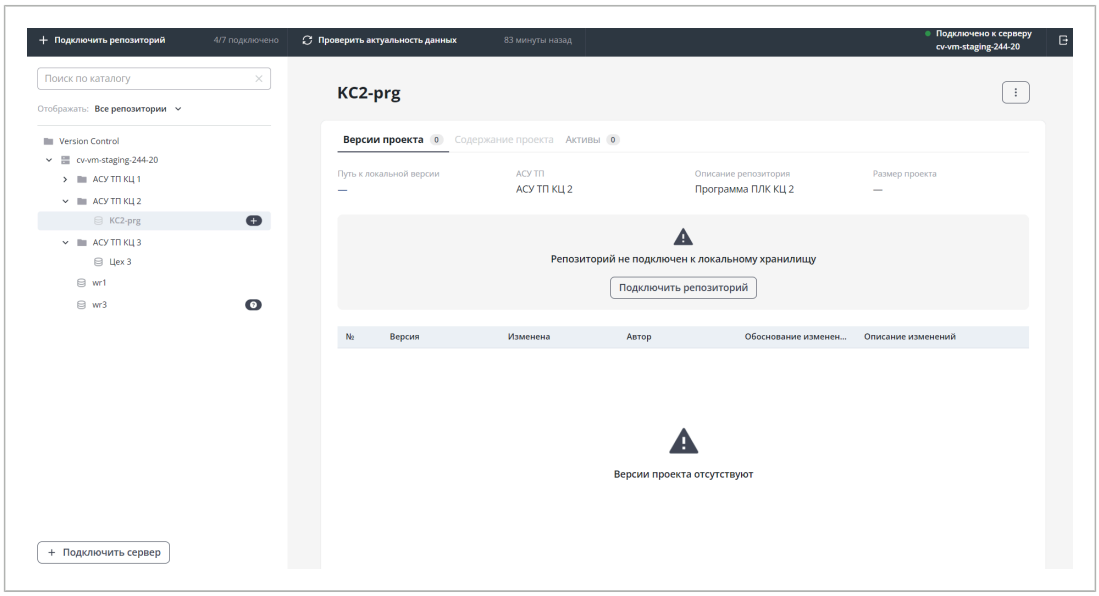


Рис. 407. Проект забыт

16.2.3.5.5.3. Забыть удаленный на сервере проект

В случае, когда подключенный репозиторий удаляют на сервере, его статус в приложении меняется на Репозиторий не найден на сервере. В таком случае необходимо забыть проект.

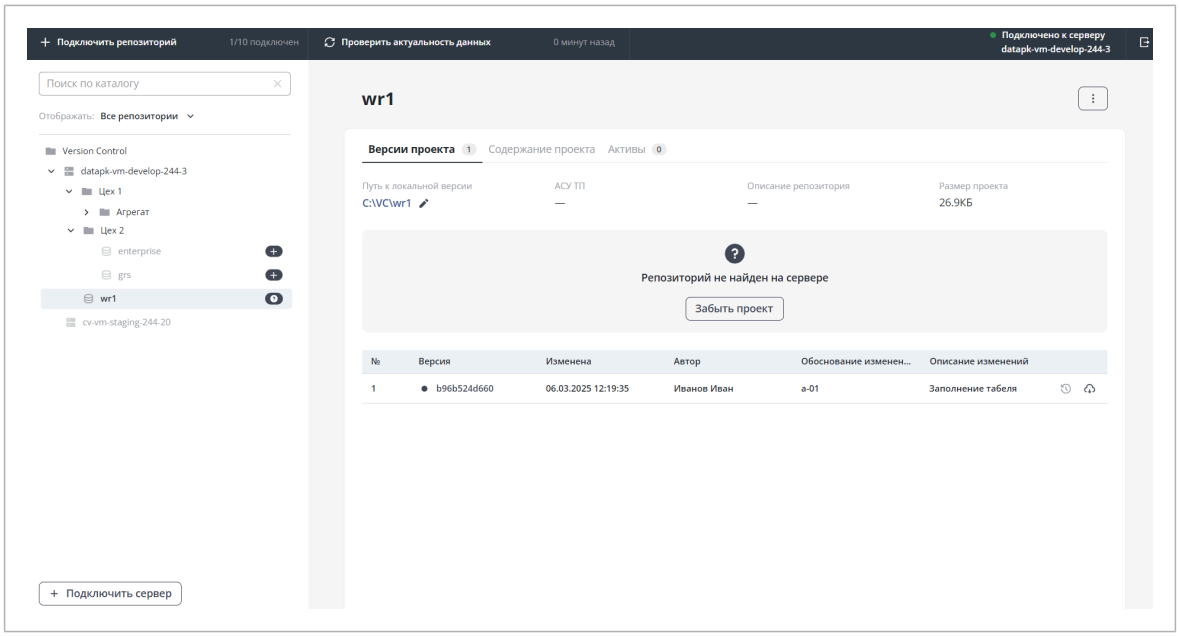


Рис. 408. Репозиторий не найден на сервере

Чтобы забыть проект:

1. Нажмите кнопку **Забыть проект**.
   - **Результат шага:** откроется окно подтверждения удаления связи между локальным хранилищем и сервером.

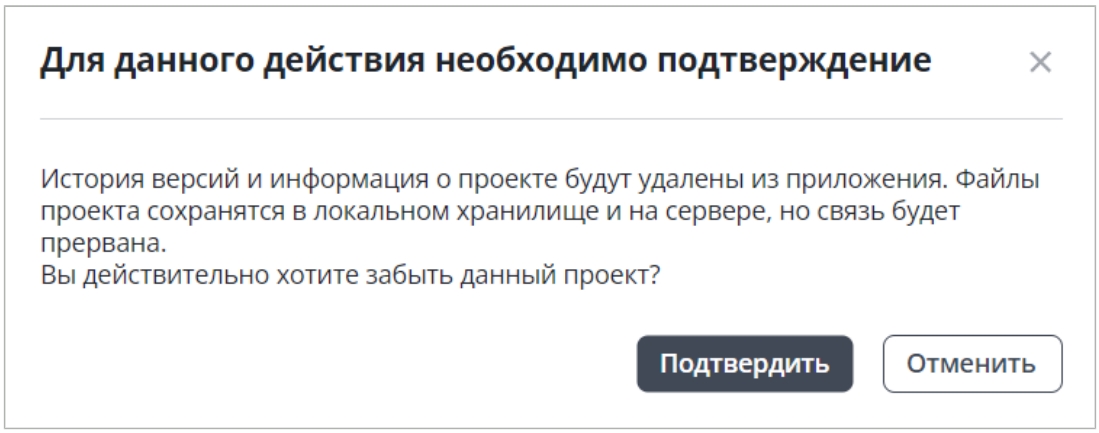


Рис. 409. Окно подтверждения

2. Нажмите на кнопку **Подтвердить**.

- **Результат шага:** связь между локальным и серверным хранилищами удалена.

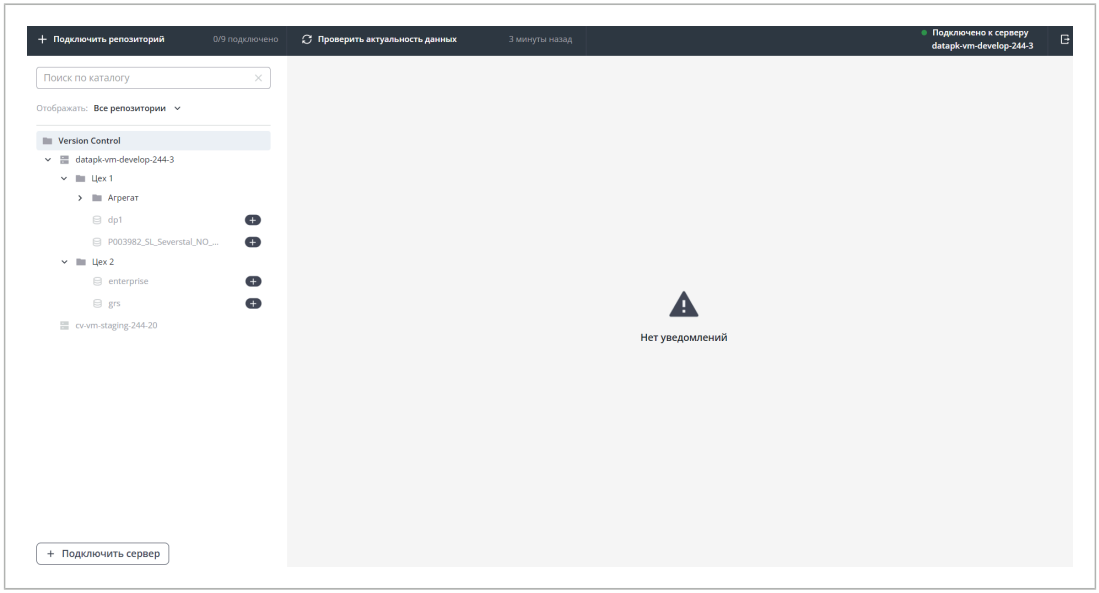


Рис. 410. Проект забыт

16.2.3.5.6. Блокировка и разблокировка проекта

> Внимание:
>
> Для корректной работы Version Control необходимо перед началом работы с файлами репозитория заблокировать проект и разблокировать после завершения работ.

Автор блокировки и причина отображаются при наведении курсора на значок статуса репозитория .

Подробнее об особенностях блокировки см. в разделе «Блокировка проекта».

В этом разделе:

- Блокировка проекта
- Разблокировка проекта

16.2.3.5.6.1. Блокировка проекта

1. Нажмите на наименование нужного репозитория в каталоге в левом боковом меню.
   - **Результат шага:** откроется страница репозитория.

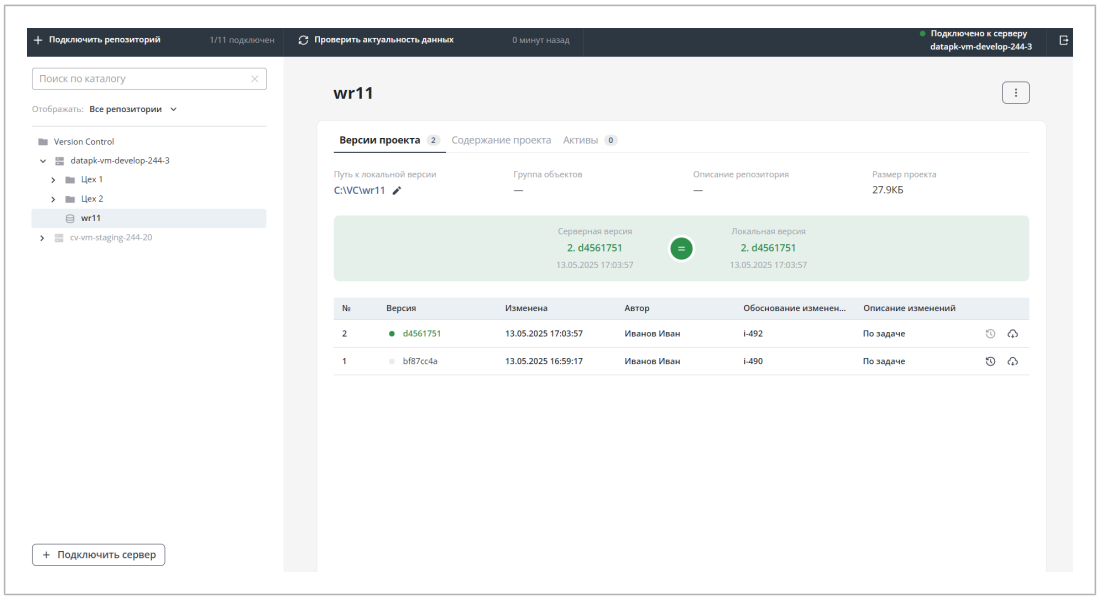


Рис. 411. Страница репозитория

2. Нажмите кнопку в правом верхнем углу.
   - **Результат шага:** откроется меню репозитория.
3. Нажмите кнопку **Заблокировать**.
   - **Результат шага:** откроется окно блокировки проекта.

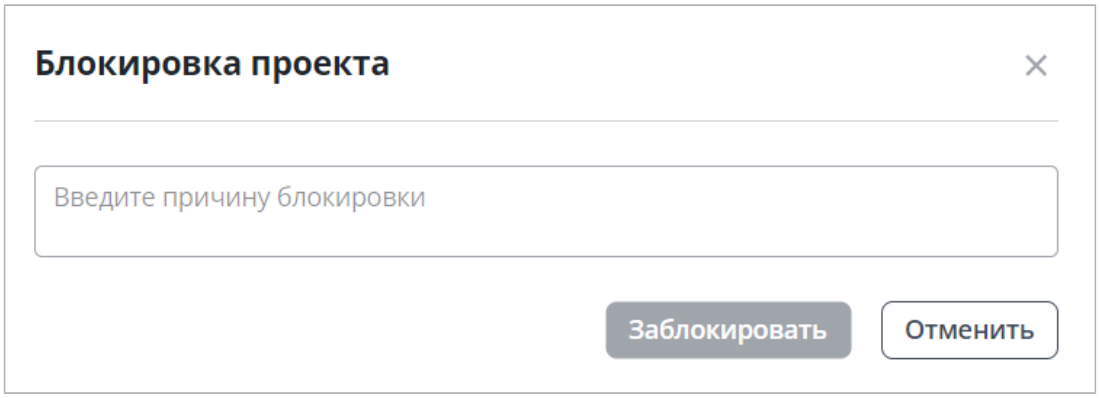


Рис. 412. Блокировка проекта

4. Укажите причину блокировки.
5. Нажмите кнопку **Заблокировать**.

- **Результат шага:** статус репозитория изменится на `Проект заблокирован`.

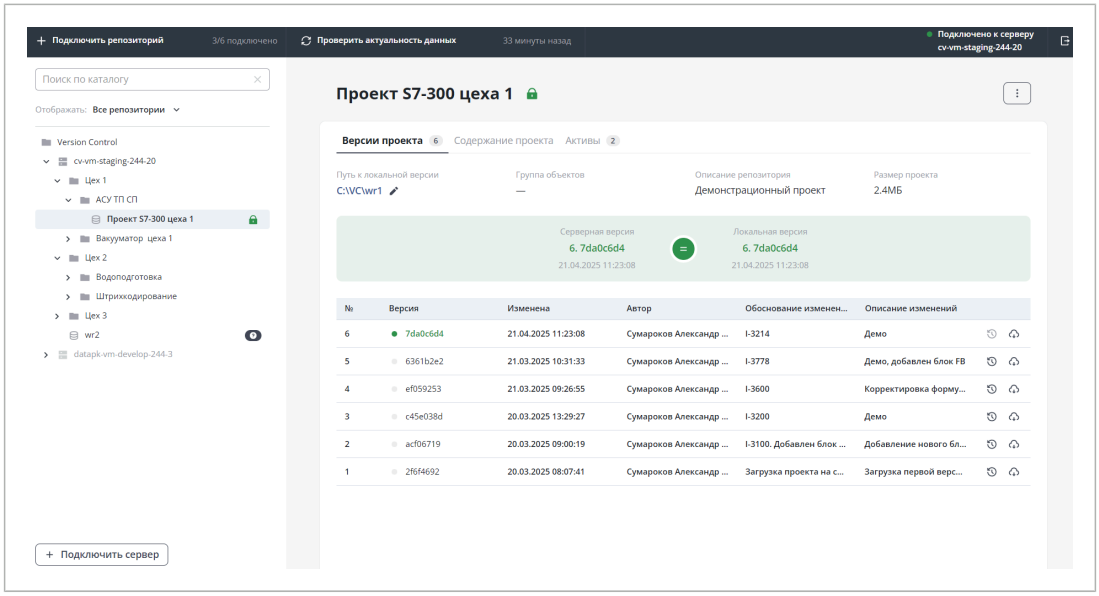


Рис. 413. Проект заблокирован

16.2.3.5.6.2. Разблокировка проекта

Для разблокировки проекта:

1. Нажмите на наименование нужного репозитория в каталоге в левом боковом меню.
   - **Результат шага:** откроется страница заблокированного проекта.

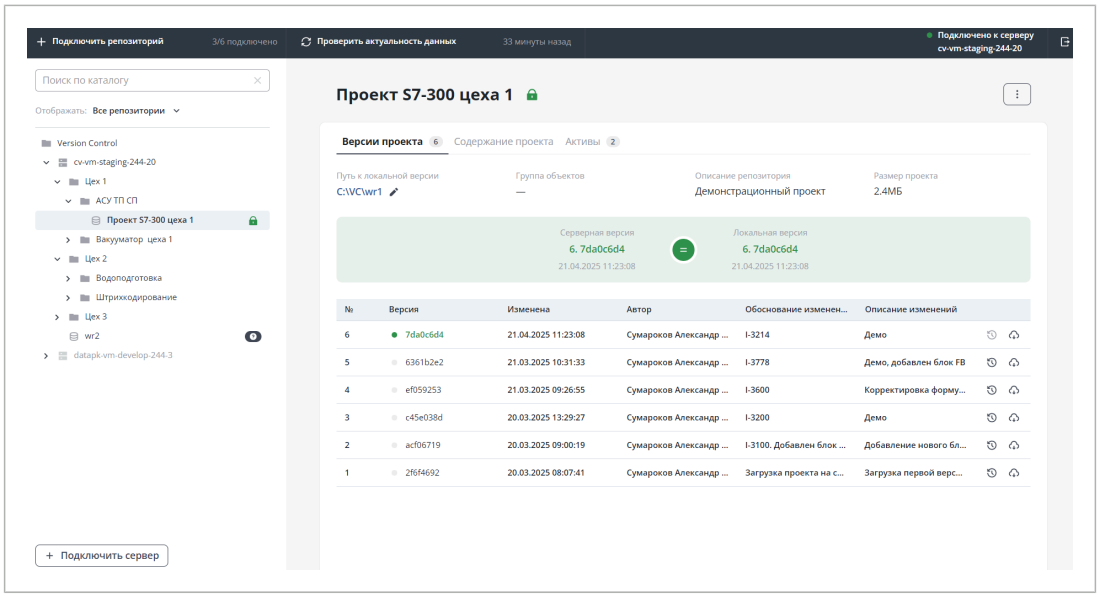


Рис. 414. Заблокированный проект

2. Нажмите кнопку в правом верхнем углу.
   - **Результат шага:** откроется меню репозитория.
3. Нажмите кнопку **Разблокировать**.
   - **Результат шага:** откроется окно подтверждения разблокировки проекта.

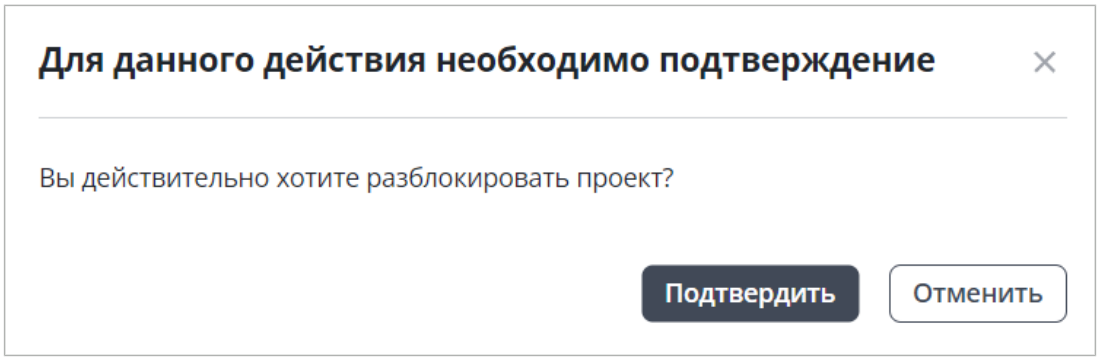


Рис. 415. Подтверждение разблокировки проекта

4. Нажмите кнопку **Подтвердить**.
   - **Результат шага:** проект будет разблокирован.

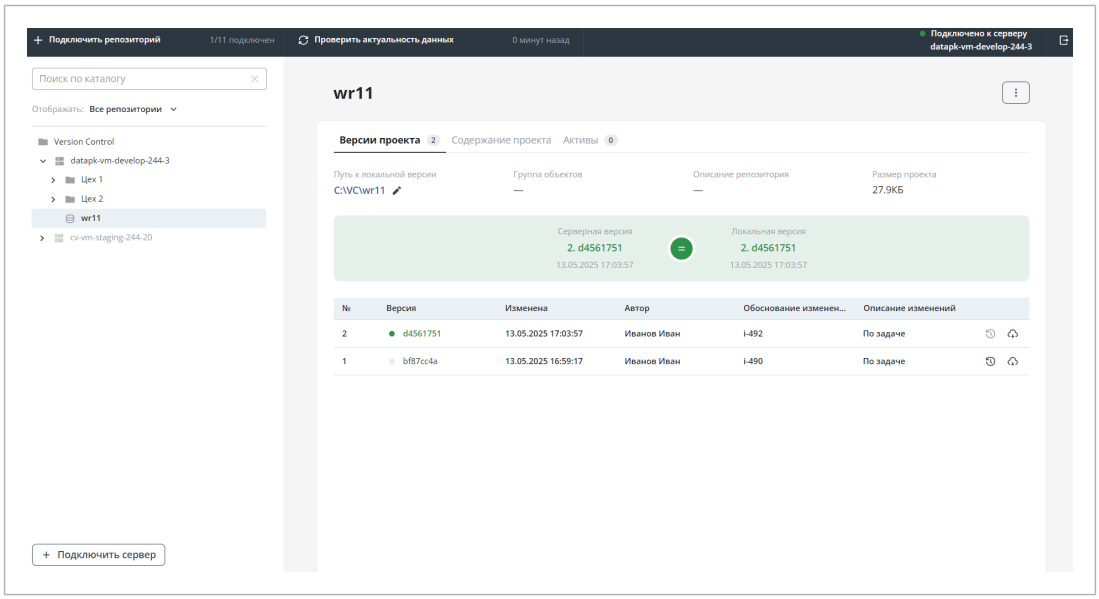


Рис. 416. Проект разблокирован

16.2.3.5.7. Настройка исключений

Заданные исключения хранятся в файле `.gitignore`, имеющем кодировку UTF-8.

Файл `.gitignore` создается в каталоге проекта после первой настройки исключений и удаляется, если в приложении удалить его содержимое и сохранить изменения.

Git по умолчанию не поддерживает исключение файлов с учетом регистра в файле `.gitignore`. Для каждого варианта регистра нужно создавать отдельное правило.

> **Пример**
> Чтобы исключить файлы `plan.txt`, `Plan.txt` и `PLAN.txt`, нужно указать в файле `.gitignore` следующие строки:
>
> ```
> plan.txt
> Plan.txt
> PLAN.txt
> ```

Исключения задаются относительно корневого каталога репозитория.

Табл. 22. Типовые шаблоны исключений

ШАБЛОН	ПОЯСНЕНИЕ
`folder_to_ignore/`	Исключение каталога из версионирования
`folder/file.txt`	Исключение определенного файла в каталоге из версионирования
`**/file.txt`	Исключение конкретного файла из версионирования вне зависимости от его местонахождения
`*.txt`	Исключение файлов с определенным расширением из версионирования
`my\ folder/`	Исключение каталога с пробелами в наименовании `my folder` из версионирования

Больше шаблонов исключений см. в разделе «Шаблоны для настройки исключений».

С помощью символа `#` в начале строки можно оставить комментарий в файле `.gitignore`:

```
# ignore all logs
*.log
```

Внимание:

После исключения каталога файлы внутри него нельзя версионировать.

Исключения нельзя применить к версионированным файлам. Для настройки исключений версионированных файлов используйте инструкцию «Настройка исключения версионированных файлов».

Если файлы для исключение еще не были созданы или версионированы, используйте инструкцию «Настройка исключения неверсионированных файлов».

16.2.3.5.7.1. Настройка исключения неверсионированных файлов

Прим.:

Подробнее о синтаксисе файла `.gitignore` см. в разделе «Шаблоны для настройки исключений».

Чтобы настроить исключение неверсионированных файлов или файлов, которые еще не были созданы:

1. Нажмите на наименование нужного репозитория в каталоге в левом боковом меню.
   - **Результат шага:** откроется страница репозитория.

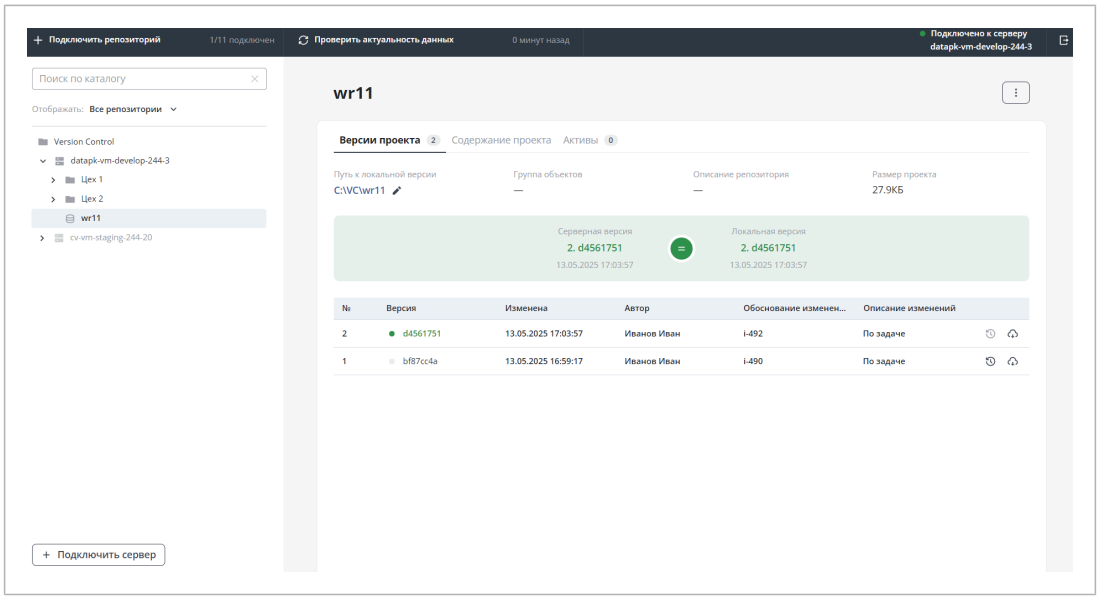


Рис. 417. Страница репозитория

2. Нажмите кнопку в правом верхнем углу.
   - **Результат шага:** откроется меню репозитория.
3. Нажмите кнопку **Настроить исключения**.
   - **Результат шага:** откроется окно редактирования исключений.

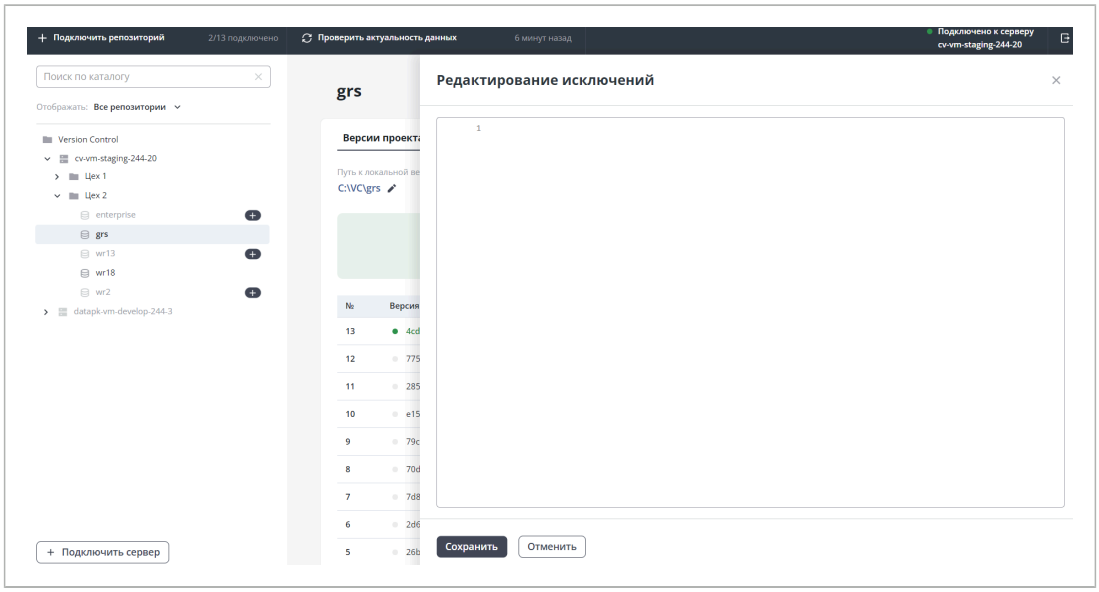


Рис. 418. Редактирование исключений

4. Укажите необходимые исключения.
5. Нажмите кнопку **Сохранить**.

> **Прим.:**
>
> Если необходимо продолжить редактирование исключений после сохранения файла `.gitignore`, нажмите на кнопку ✎ в верхнем правом углу.

6. Создайте новую версию проекта и загрузите ее на сервер, подробнее см. в разделе «Создание и загрузка версии проекта на сервер».

16.2.3.5.7.2. Настройка исключения версионированных файлов

> **Прим.:**
>
> Подробнее о синтаксисе файла `.gitignore` см. в разделе «Шаблоны для настройки исключений».

Чтобы настроить исключение версионированных файлов:

1. Перенесите выбранные для исключения файлы из локального хранилища репозитория в другую директорию.
2. Нажмите на наименование нужного репозитория в каталоге в левом боковом меню.
   - **Результат шага:** откроется страница репозитория.

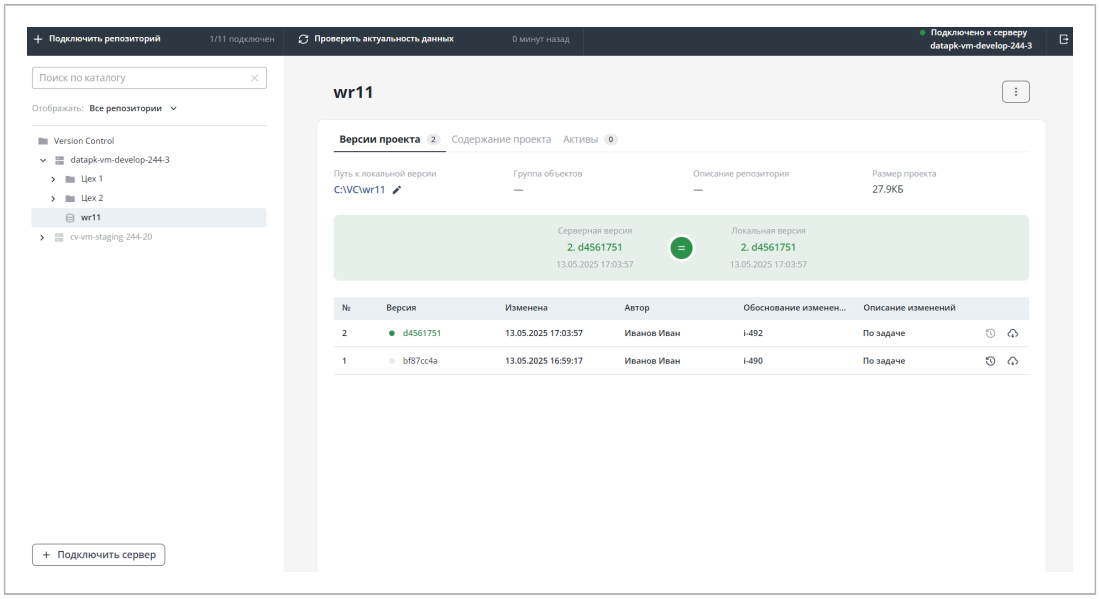


Рис. 419. Страница репозитория

3. Нажмите кнопку ⋮ в правом верхнем углу.
   - **Результат шага:** откроется меню репозитория.
4. Нажмите кнопку **Настроить исключения**.
   - **Результат шага:** откроется окно редактирования исключений.

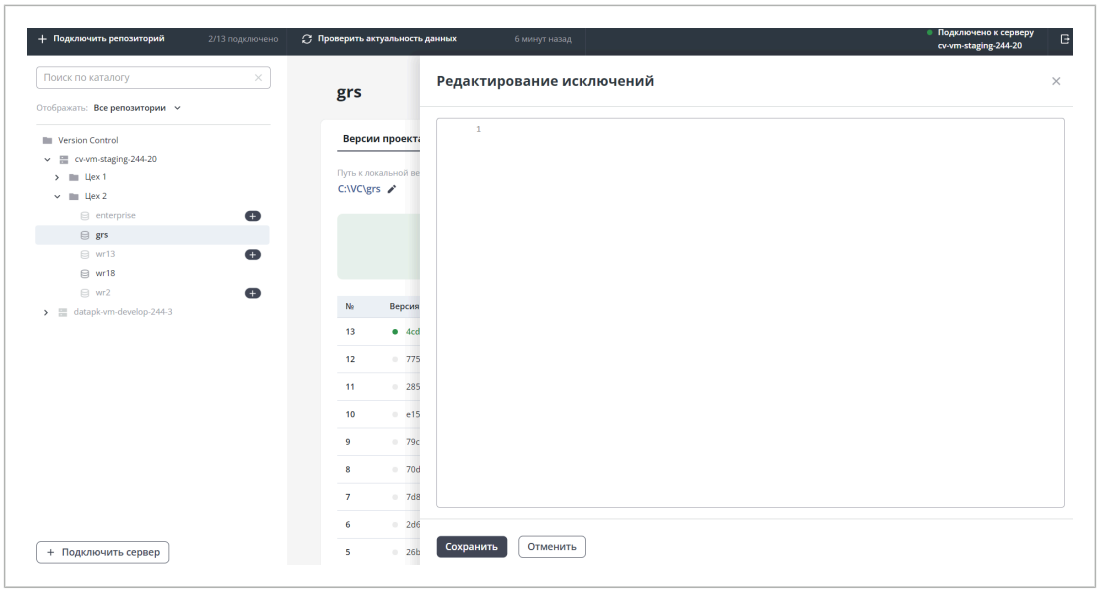


Рис. 420. Редактирование исключений

5. Укажите необходимые исключения.
6. Нажмите кнопку **Сохранить**.

> Прим.:
>
> Если необходимо продолжить редактирование исключений после сохранения файла `.gitignore`, нажмите на кнопку ✎ в верхнем правом углу.

7. Убедитесь, что все файлы, которые требуется исключить из версионирования, скопированы в другую директорию и удалены в локальном хранилище репозитория.
8. Создайте новую версию проекта и загрузите ее на сервер, подробнее см. в разделе «Создание и загрузка версии проекта на сервер».
9. Верните в локальное хранилище репозитория ранее перенесенные файлы.

16.2.3.5.8. Изменение расположения локального хранилища

При необходимости можно изменить расположение локального хранилища.

Чтобы изменить расположение локального хранилища:

1. Скопируйте каталог локального хранилища репозитория и вставьте его в выбранное место.

> Внимание:
>
> Не удаляйте каталог репозитория, пока не измените расположение локального хранилища.

2. Откройте вкладку **Версии проекта** нужного репозитория.
3. Нажмите кнопку ✎.
   - **Результат шага:** откроется окно редактирования пути репозитория.

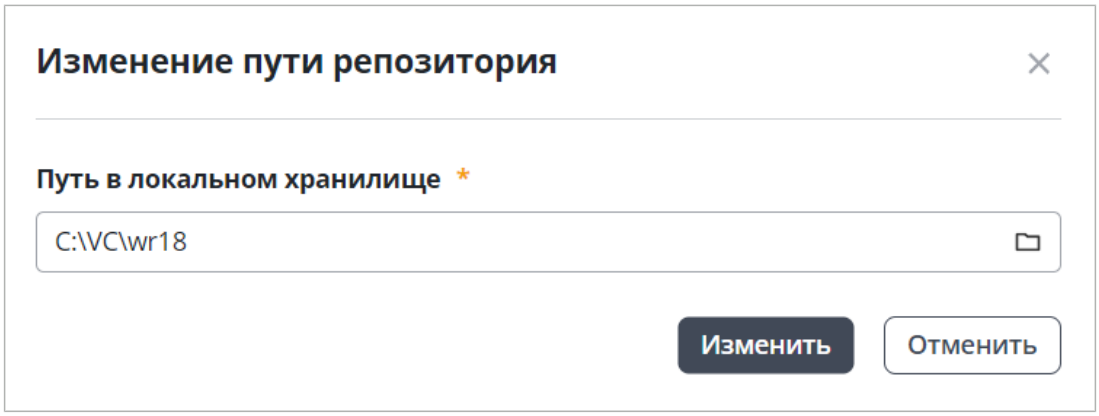


Рис. 421. Редактирование пути репозитория

4. Укажите новый путь к каталогу репозитория или выберите новый путь с помощью кнопки
5. Нажмите кнопку **Сохранить**.
   - **Результат шага:** расположение локального хранилища будет изменено.
6. Удалите файлы в старом локальном хранилище.

16.2.3.6. Управление версиями проектов

> Внимание:
>
> Для корректной работы Version Control необходимо заблокировать проект перед началом работы с файлами репозитория и разблокировать после завершения.

В этом разделе:

- Создание и загрузка версии проекта на сервер
- Создание версии проекта
- Загрузка версии проекта на сервер
- Восстановление версии проекта
- Отмена изменений

16.2.3.6.1. Создание и загрузка версии проекта на сервер

Создание и загрузка новой версии проекта на сервер Version Control Management возможно при выполнении следующих условий:

- На сервере Version Control Management существует репозиторий.
- В приложении Version Control Desktop App этот репозиторий подключен, его статус — `Локальное хранилище изменено` или `Серверная и локальная версии проекта равны`.
- В файлы локального хранилища репозитория были внесены изменения.
- Размер изменений не больше 2 ГБ.

1. Откройте вкладку **Версии проекта** нужного репозитория.
2. Нажмите кнопку **Проверить актуальность данных**.

> **Внимание:**
>
> Всегда нажимайте кнопку **Проверить актуальность данных** перед созданием новой версии и ее загрузкой на сервер. Это необходимо для предотвращения конфликтов версий.

- **Результат шага:** статус у репозитория должен быть `Локальное хранилище изменено`.

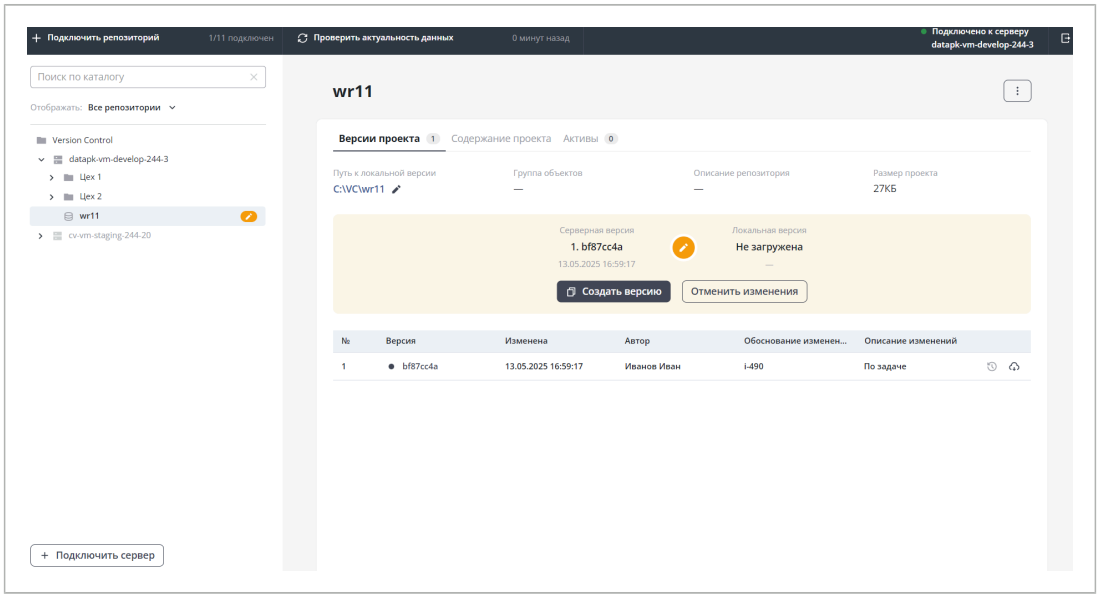


Рис. 422. Локальное хранилище изменено

3. Нажмите кнопку **Создать версию**.

- **Результат шага:** откроется окно **Создание версии**.

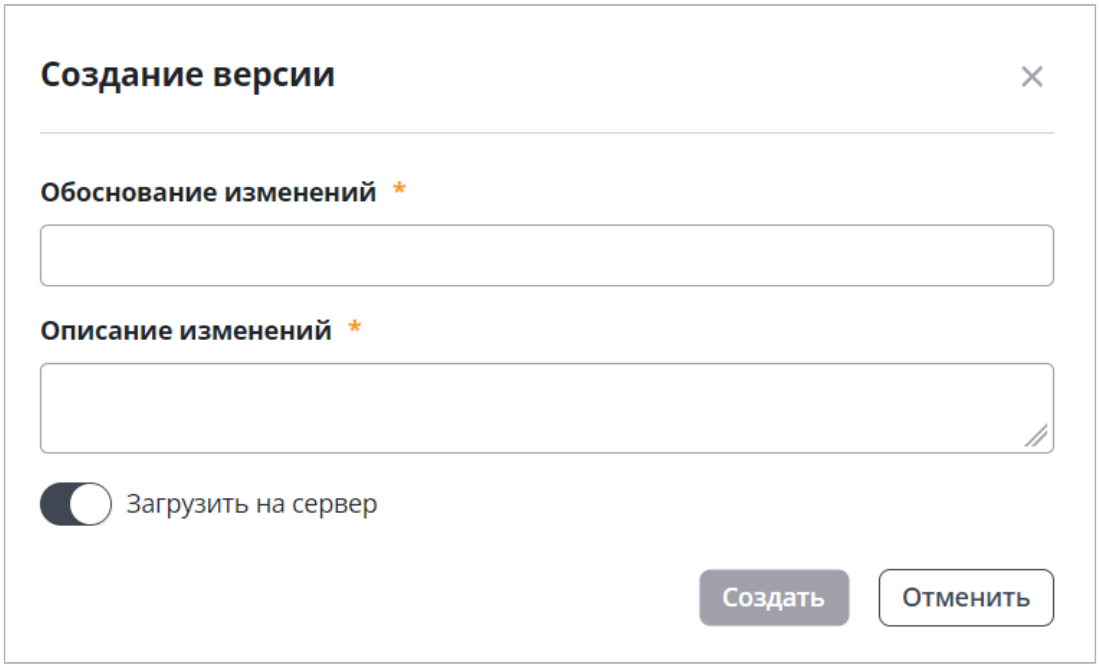


Рис. 423. Создание версии

4. Заполните следующие поля:
   - **Обоснование изменений** — укажите причину изменения файлов репозитория.
   - **Описание изменений** — подробно опишите изменения файлов репозитория.

- **Результат шага:** кнопка **Создать** станет активна.

5. Нажмите кнопку **Создать**.

   По умолчанию включена опция **Загрузить на сервер**, поэтому при создании новой версии проекта она будет загружена на сервер.

   - **Результат шага:** новая версия проекта будет создана и загружена на сервер Version Control Management. Статус репозитория изменится на `Серверная и локальная версии проекта равны`.

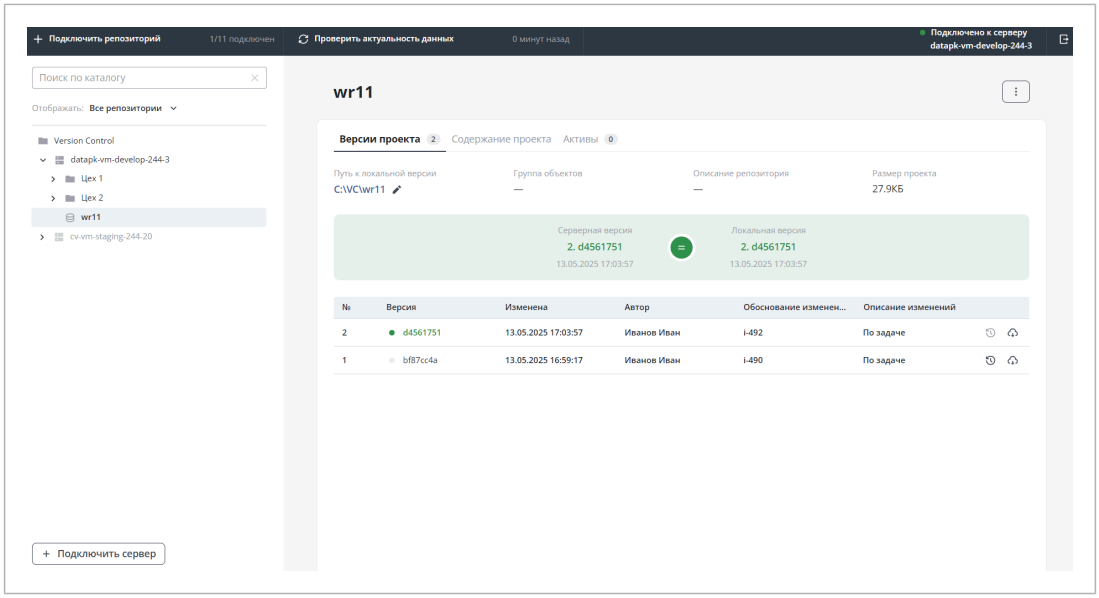


Рис. 424. Серверная и локальная версии проекта равны

6. После завершения работ с проектом разблокируйте его.

16.2.3.6.2. Создание версии проекта

Создание новой версии проекта возможно при выполнении следующих условий:

- На сервере Version Control Management существует репозиторий.
- В приложении Version Control Desktop App этот репозиторий подключен, его статус — `Локальное хранилище изменено` или `Серверная и локальная версии проекта равны`.
- В файлы локального хранилища репозитория были внесены изменения.
- Размер изменений не больше 2 ГБ.

При создании версии проекта с отключенной опцией **Загрузить на сервер** созданная версия проекта не будет автоматически загружена на сервер Version Control Management. Для загрузки созданной версии см. в разделе «Загрузка версии проекта на сервер».

1. Откройте вкладку **Версии проекта** нужного репозитория.
2. Нажмите кнопку **Проверить актуальность данных**.

> Внимание:
>
> Всегда нажимайте кнопку **Проверить актуальность данных** перед созданием новой версии. Это необходимо для предотвращения конфликтов версий.

- **Результат шага:** статус у репозитория должен быть `Локальное хранилище изменено`.

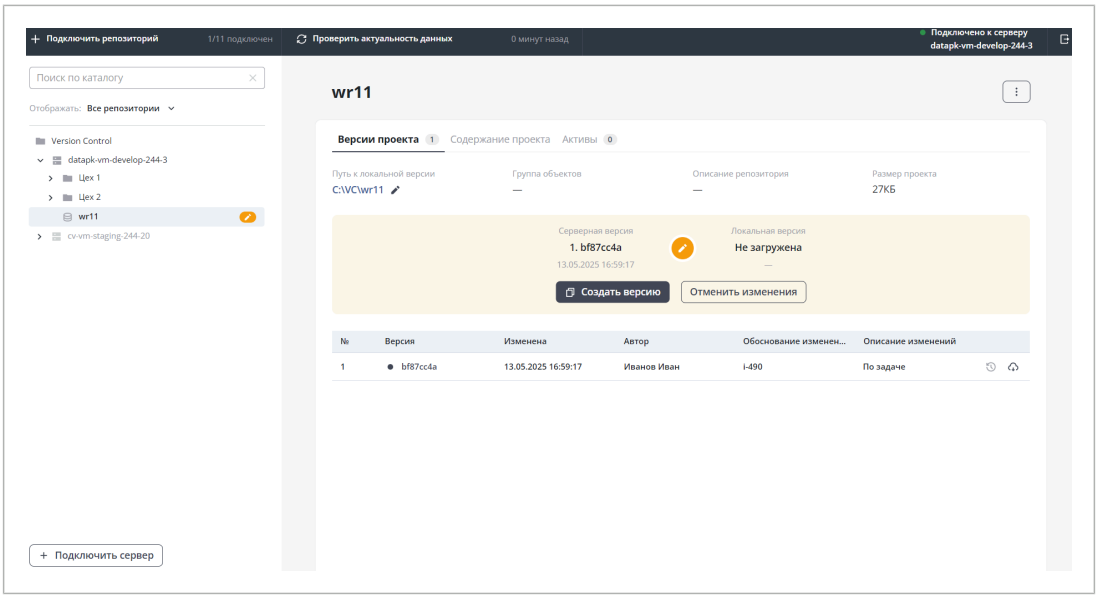


Рис. 425. Локальное хранилище изменено

3. Нажмите кнопку **Создать версию**.
   - **Результат шага:** откроется окно **Создание версии**.

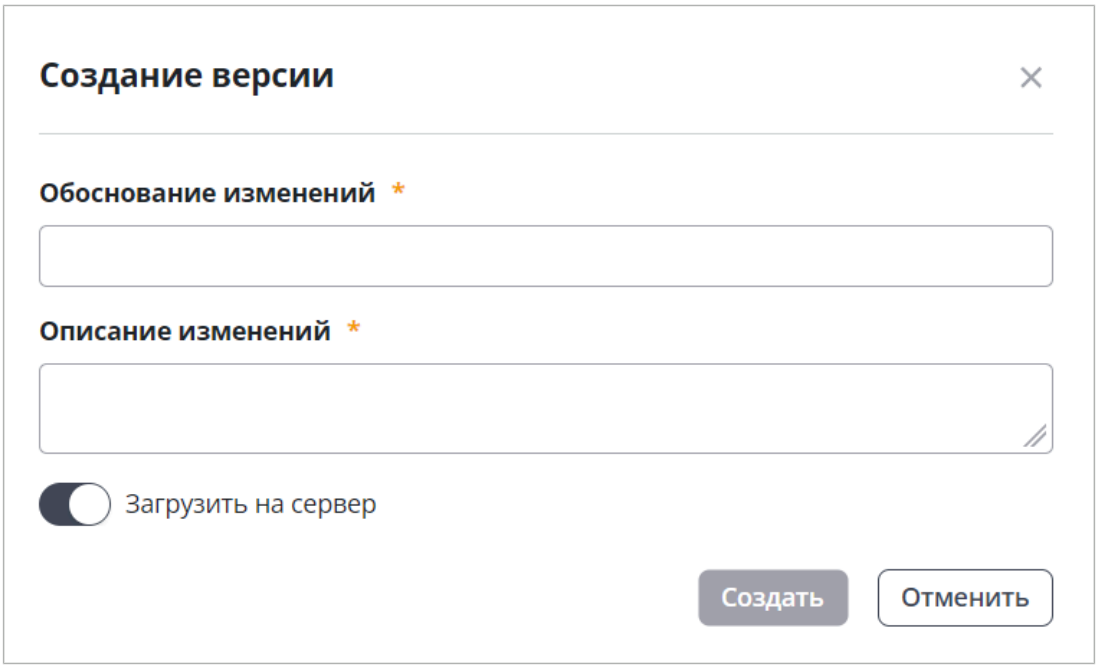


Рис. 426. Создание версии

4. Заполните следующие поля:
   - **Обоснование изменений** — укажите причину изменения файлов репозитория.
   - **Описание изменений** — подробно опишите изменения файлов репозитория.
   - **Результат шага:** кнопка **Создать** станет активна.
5. Отключите опцию **Загрузить на сервер**.
6. Нажмите кнопку **Создать**.

▸ **Результат шага:** новая версия проекта будет создана. Статус репозитория изменится на `Локальная версия проекта новее серверной`.

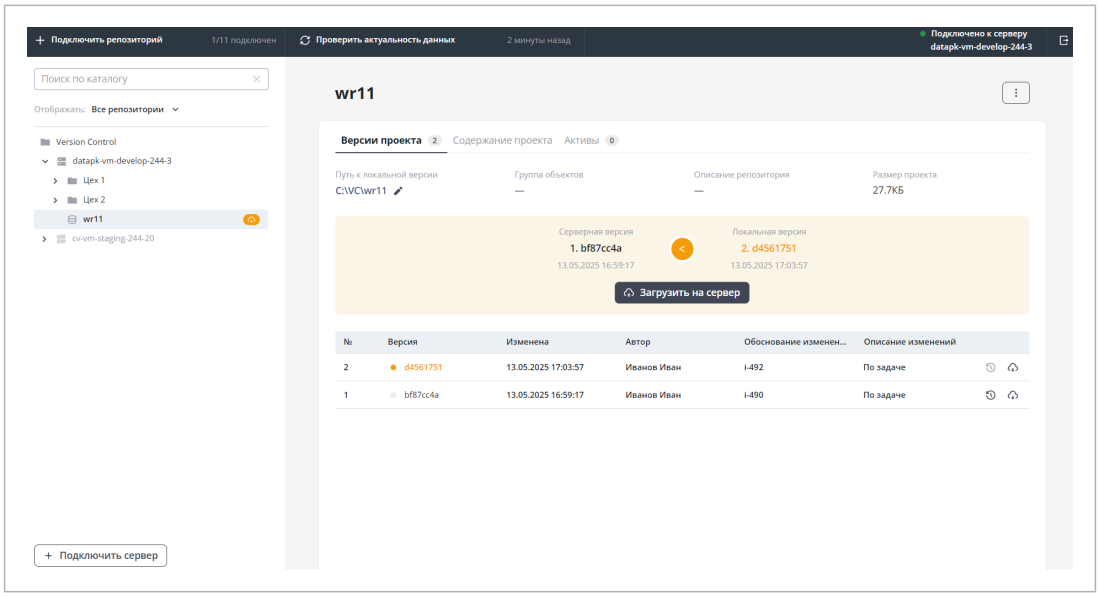


Рис. 427. Локальная версия проекта новее серверной

16.2.3.6.3. Загрузка версии проекта на сервер

Загрузка новой версии проекта на сервер Version Control Management возможна при выполнении следующих условий:

- На сервере Version Control Management существует репозиторий.
- В приложении Version Control Desktop App этот репозиторий подключен, его статус — `Локальная версия проекта новее серверной`.
- Размер новой версии проекта не больше 2ГБ.

1. Откройте вкладку **Версии проекта** нужного репозитория.
2. Нажмите кнопку **Проверить актуальность данных**.

> Внимание:
>
> Всегда нажимайте кнопку **Проверить актуальность данных** перед загрузкой новой версии на сервер. Это необходимо для предотвращения конфликтов версий.

▸ **Результат шага:** статус у репозитория должен быть `Локальная версия проекта новее серверной`.

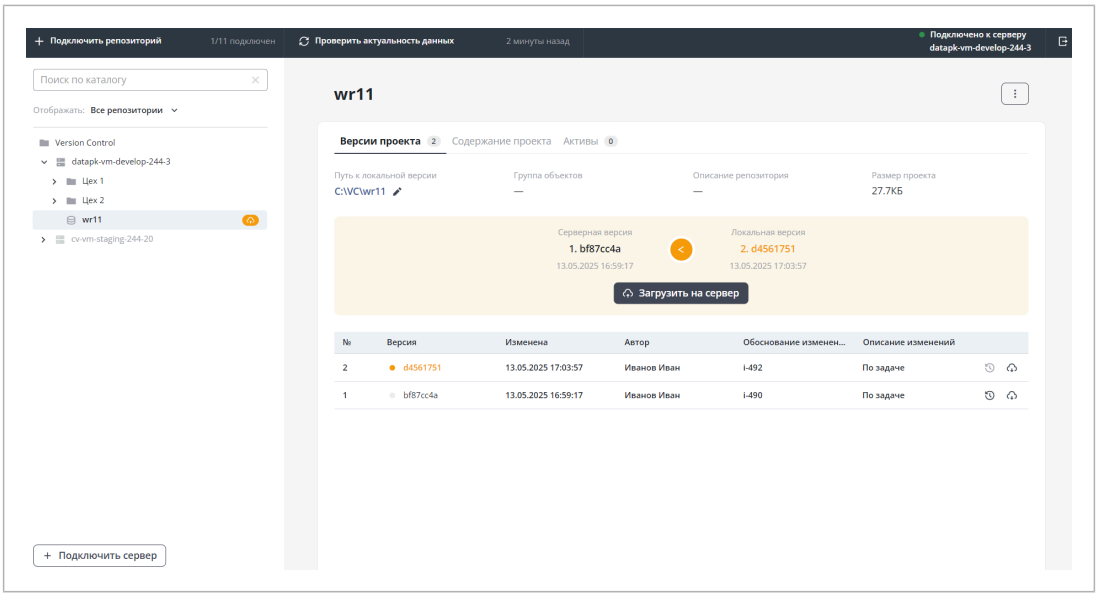


Рис. 428. Локальная версия проекта новее серверной

3. Нажмите кнопку **Загрузить на сервер**.
   - **Результат шага:** новая версия будет загружена на сервер Version Control Management. Статус репозитория изменится на `Серверная и локальная версии проекта равны`.

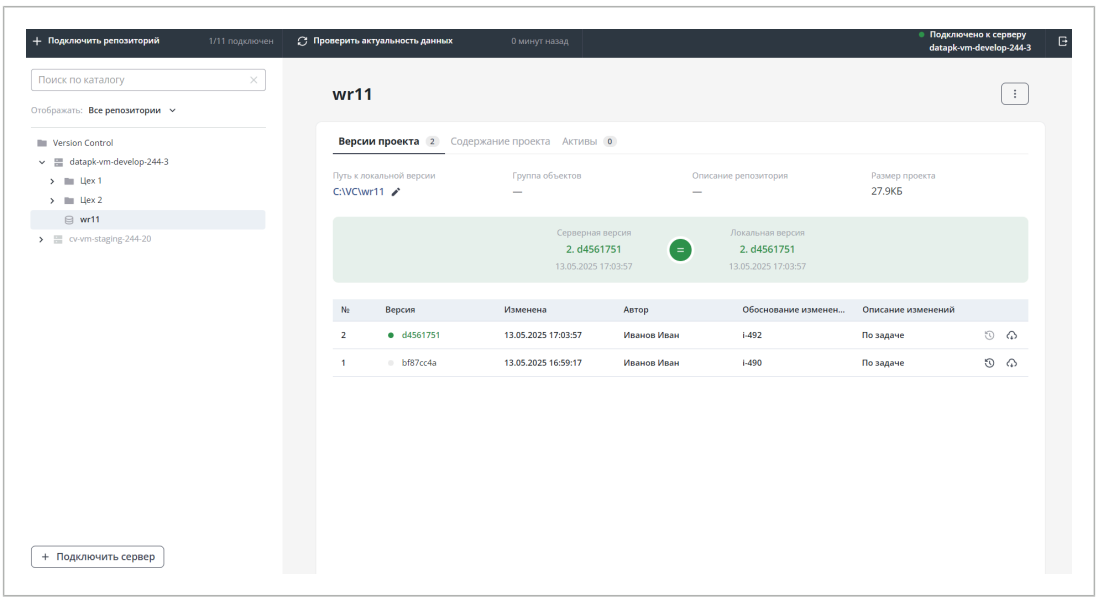


Рис. 429. Серверная и локальная версии проекта равны

4. После завершения работ с проектом разблокируйте его.

16.2.3.6.4. Восстановление версии проекта

Восстановление версии проекта возможно при выполнении следующих условий:

- У проекта больше одной версии.
- Последняя версия проекта отличается от выбранной для восстановления.

При восстановлении версии проекта создается новая версия проекта на основе восстановленной.

Чтобы восстановить версию проекта:

1. Закройте программы, работающие с файлами проекта.

> Внимание:
>
> С открытой средой разработки возможно замедление при подключении к серверу Version Control Management. Для корректной работы приложения необходимо всегда закрывать среду разработки.

2. Нажмите на наименование нужного репозитория в каталоге в левом боковом меню.
   - **Результат шага:** откроется страница репозитория, на которой отображаются версии проекта. Актуальная версия находится на верху таблицы и выделена зеленым цветом.

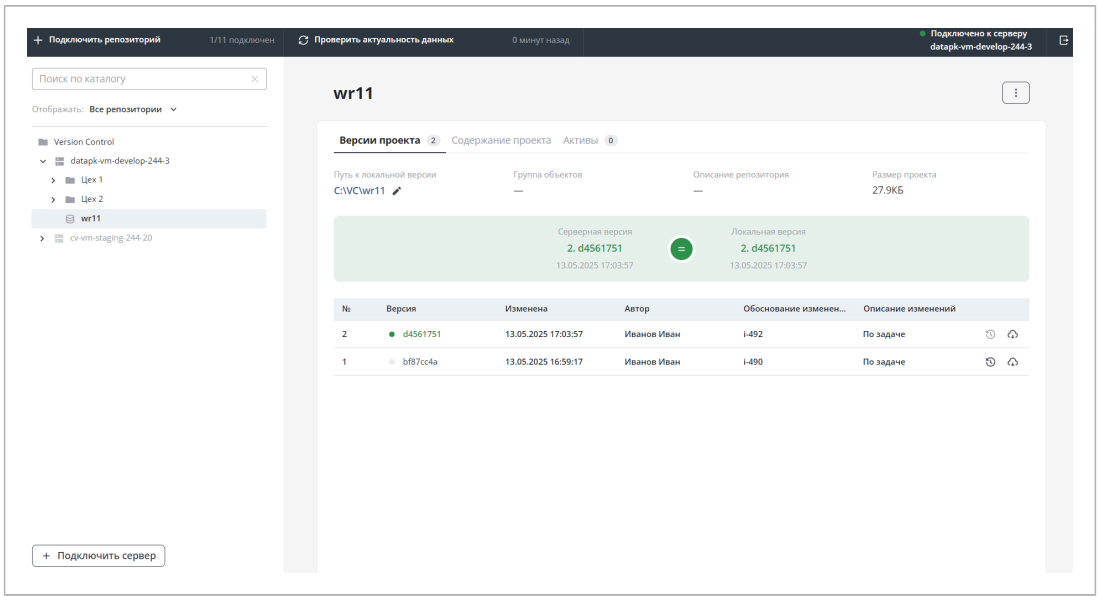


Рис. 430. Страница репозитория

3. Нажмите кнопку в строке с версией, которую нужно восстановить.
   - **Результат шага:** откроется окно восстановления версии

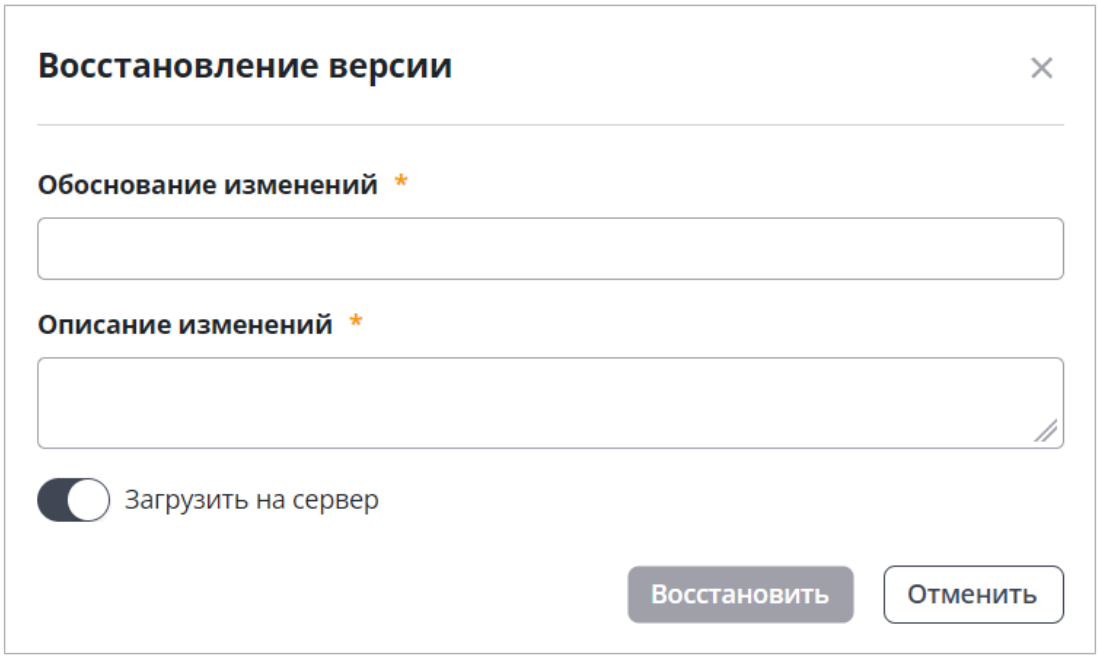


Рис. 431. Окно восстановления версии

4. Заполните поля **Обоснование изменений** и **Описание изменений**.
5. Нажмите кнопку **Восстановить**.
   - **Результат шага:** выбранная версия проекта будет восстановлена.

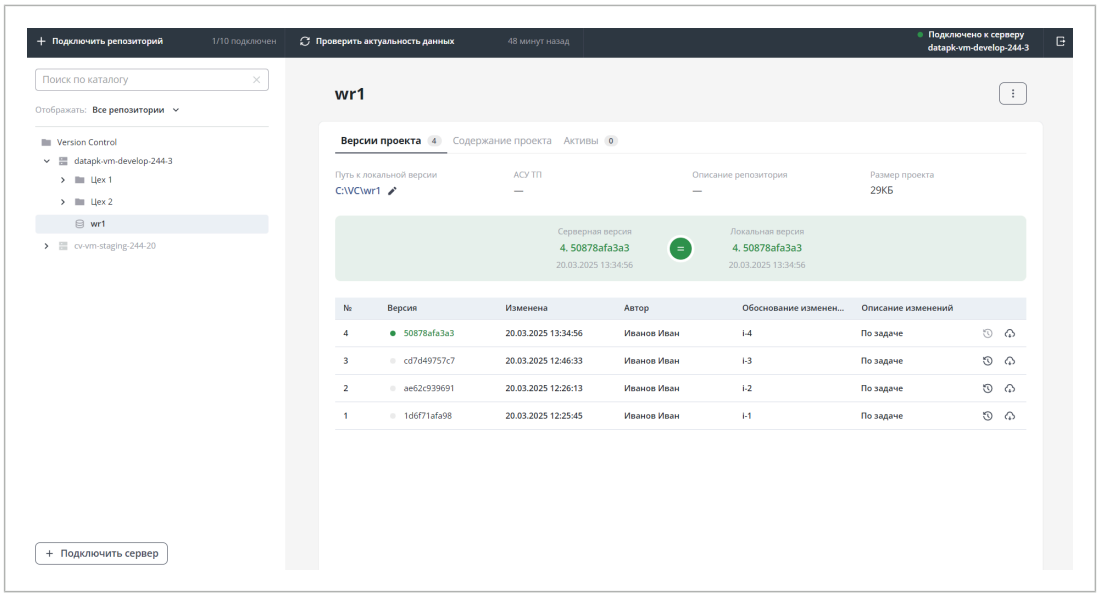


Рис. 432. Выбранная версия проекта восстановлена

6. После завершения работ с проектом разблокируйте его.

16.2.3.6.5. Отмена изменений

Отменить изменения возможно, когда файлы локального хранилища были изменены, но новая версия проекта еще не была создана.

Чтобы отменить изменения:

1. Закройте программы, работающие с файлами проекта.

> Внимание:
>
> С открытой средой разработки возможно замедление при подключении к серверу Version Control Management. Для корректной работы приложения необходимо всегда закрывать среду разработки.

2. Нажмите на наименование нужного репозитория в каталоге в левом боковом меню.
   - **Результат шага:** откроется страница репозитория.

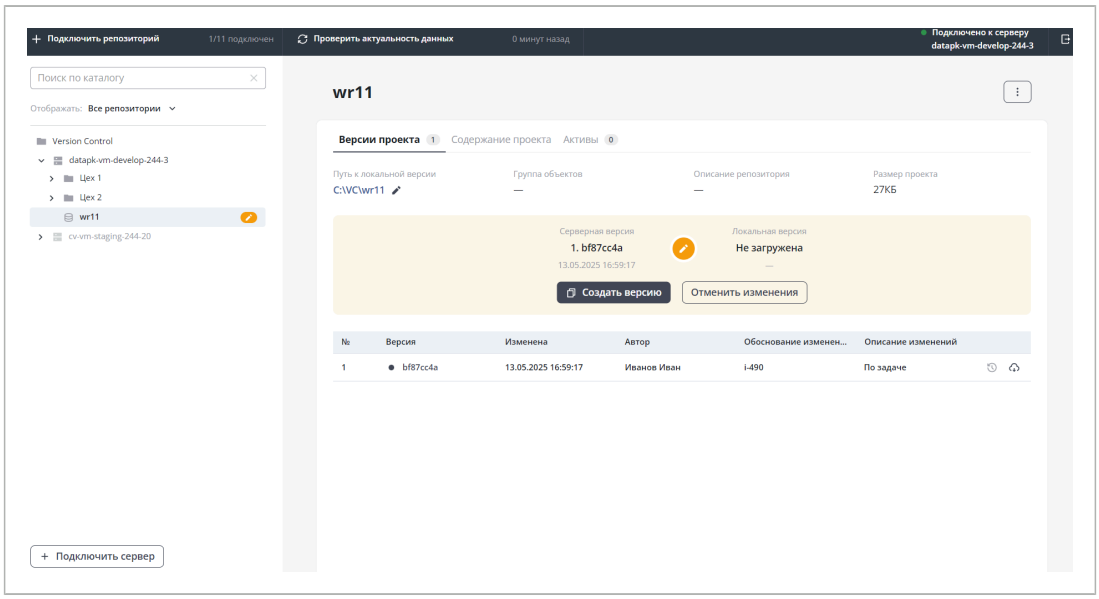


Рис. 433. Страница репозитория

3. Нажмите кнопку **Отменить изменения**.
   - **Результат шага:** откроется окно подтверждения отмены изменений.

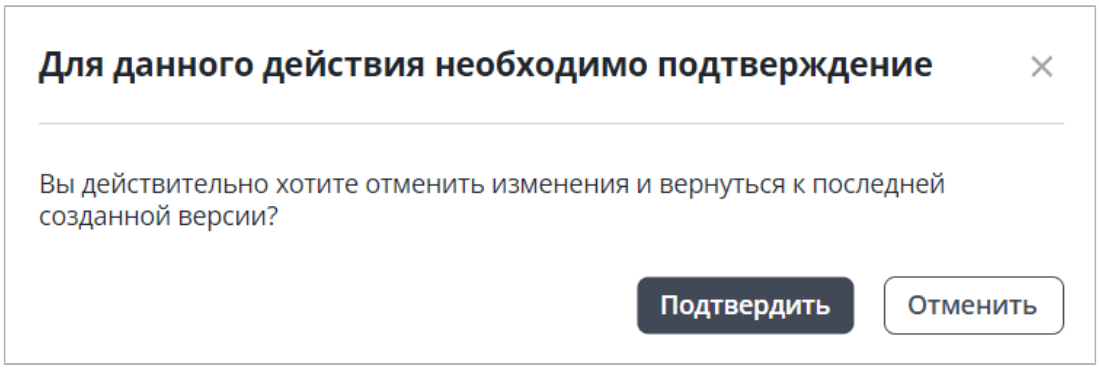


Рис. 434. Окно подтверждения

4. Нажмите кнопку **Подтвердить**.
   - **Результат шага:** последняя версия проекта будет восстановлена.

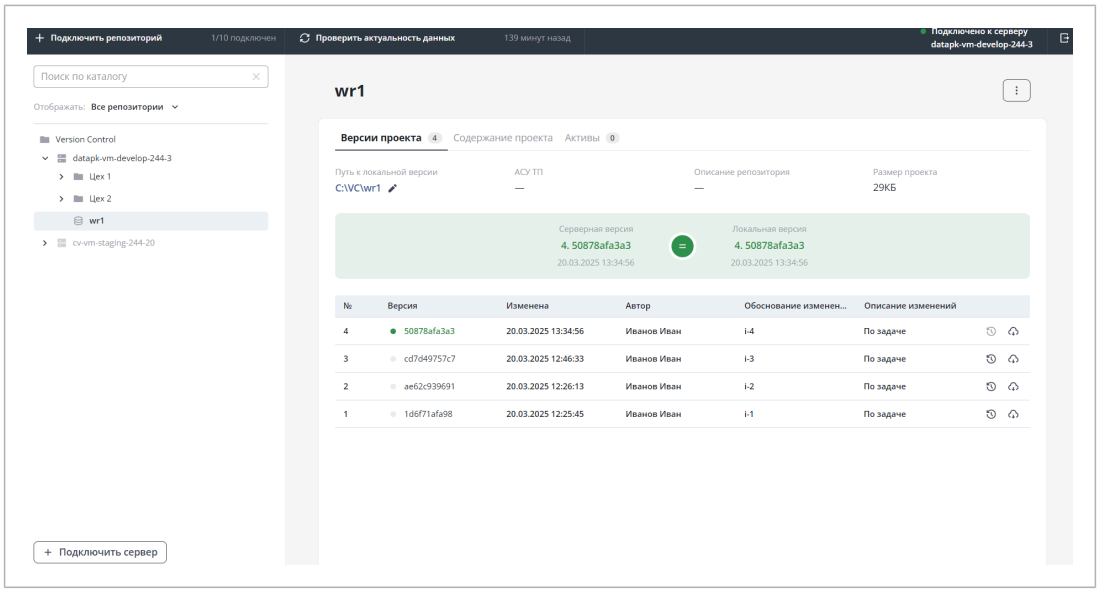


Рис. 435. Изменения отменены

5. После завершения работ с проектом разблокируйте его.

17. Управление модулем обнаружения и реагирования для ПЛК («EDR for PLC»)

В этом разделе:

1. **Выполнение операций с моделями**
2. **Получение информации об адресах по идентификаторам**
3. **Получение информации о сетевом узле по идентификатору**
4. **Получение списка сетевых узлов модуля «EDR for PLC»**
5. **Просмотр статистики по разбору сетевого трафика модулем «EDR for PLC»**
6. **Просмотр статуса активности формирования немодельных аномалий**
7. **Включение/отключение создания немодельных аномалий**
8. **Возможные ошибки API модуля «EDR for PLC»**

Управление модулем UDV DATAPK EDR for PLC и просмотр его состояния выполняются через API, которое доступно по адресу: `https://[IP-адрес Комплекса]:8081/docs`

Вид страницы API представлен на рисунке ниже.

Рис. 436. Страница API модуля «EDR for PLC»

Для выполнения операции:

1. Перейдите на страницу API.
2. Разверните необходимый блок.
3. Нажмите кнопку **Try it out**.

4. Нажмите кнопку **Execute**.

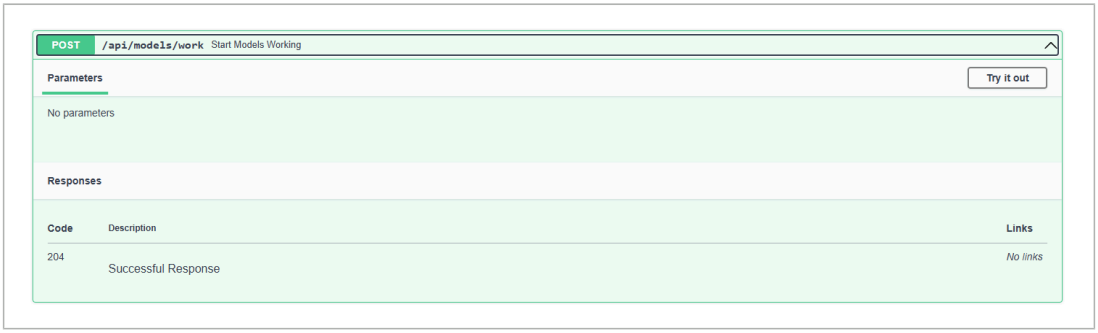


Рис. 437. Пример выполнения операции в API модуля «EDR for PLC»

17.1. Выполнение операций с моделями

В рамках модуля «EDR for PLC» пользователь может выполнять следующие операции с моделями:

- Получение списка всех моделей
- Перевод всех моделей в режим детектирования аномалий
- Перевод определенной модели в режим детектирования аномалий
- Удаление модели
- Постановка модели на паузу
- Продолжение функционирования модели
- Повторное обучение модели
- Принудительный расчет маски для всех моделей
- Принудительный расчет маски для определенной модели
- Просмотр информации о модели на основе иерархического словаря
- Просмотр информации о модели на основе временного автомата
- Просмотр информации о модели на основе гибридного автомата
- Запуск дообучения для модели на основе временного автомата
- Запуск дообучения модели на основе иерархического словаря
- Экспорт модели на основе гибридного автомата
- Получение информации об элементах словаря моделей по идентификатору

См. также

Модель на основе временного автомата

Модель на основе иерархического словаря

Модель на основе гибридного автомата

17.1.1. Получение списка всех моделей

Метод: `GET [IP-адрес Комплекса]:8081/api/models/`

Описание: Выводит информацию обо всех моделях, их типе, статусе, идентификаторе, адресной информации и краткую сводка по показателям. Кроме того, этот метод позволяет получить идентификатор любой модели, который в дальнейшем может быть использован для отправки различных команд конкретной модели.

Пример запроса:

```
curl -X 'GET' \
  'http://[IP-адрес Комплекса]:8081/api/models/' \
  -H 'accept: application/json'
```

17.1.1.1. Успешный ответ

Код ответа: `200`

Тип содержимого: `application/json`

Пример тела ответа:


```
[
  {
    "id": "0-bc00018f-f19d-4b07-b5e6-b98393261e25",
    "paused": false,
    "model_type": "HYBRID_AUTOMATON",
    "model_status": "LEARNING",
    "first_node": {
      "mode": "starts_with",
      "id": 1,
      "addresses_ids": [
        1
      ]
    },
    "second_node": {
      "mode": "starts_with",
      "id": 2,
      "addresses_ids": [
        2,
        3
      ]
    },
    "statistics": {
      "non_existent_transition_anomaly_count": "0",
      "prediction_error_in_state_anomaly_count": "0",
      "relative_prediction_error": "0",
      "checks_count": "0",
      "success_checks_number": "0",
      "anomalies_count": "0",
      "valid_packets_count": "0",
      "invalid_packets_count": "0",
      "probability_of_correct_prediction": "0"
    },
    "commands_stat": {
      "handled_commands_count": 8034,
      "unprocessed_commands": 0,
      "skipped_commands": 0
    },
```

```
    "separation_stat": []
  }
]
```

Табл. 23. Описание полей ответа на запрос

ПОЛЕ	ТИП	ОПИСАНИЕ
`id`	`string`	Идентификатор модели
`paused`	`boolean`	Признак того, что модель поставлена на паузу
`model_type`	`string`	Тип модели
`model_status`	`string`	Статус модели
`first_node`	`object`	Конфигурация первого узла
`first_node[].mode`	`string`	Режим
`first_node[].id`	`integer`	Идентификатор узла
`first_node[].addresses_ids`	`integer`	Идентификаторы адресов
`second_node`	`object`	Конфигурация второго узла
`statistics`	`object`	Статистика
`statistics[].non_existent_transition_-anomaly_count`	`integer`	Количество переходов между состояниями
`statistics[].prediction_error_in_state_-anomaly_count`	`integer`	Количество ошибок предсказания
`statistics[].relative_prediction_error`	`integer`	Относительная погрешность предсказания
`statistics[].checks_count`	`integer`	Общее количество проверок
`statistics[].success_checks_number`	`integer`	Количество успешных проверок
`statistics[].anomalies_count`	`integer`	Количество аномалий
`statistics[].valid_packets_count`	`integer`	Количество действительных пакетов

Табл. 23. Описание полей ответа на запрос

ПОЛЕ	ТИП	ОПИСАНИЕ
`statistics[].invalid_packets_count`	`integer`	Количество недействительных пакетов
`statistics[].probability_of_correct_-prediction`	`integer`	Вероятность корректного предсказания
`commands_stat`	`object`	Статистика по командам
`commands_stat[].handled_commands_count`	`integer`	Количество обработанных команд
`commands_stat[].unprocessed_commands`	`integer`	Количество необработанных команд
`commands_stat[].skipped_commands`	`integer`	Количество пропущенных команд
`separation_stat`	`array`	Статистика разделения

17.1.2. Перевод всех моделей в режим детектирования аномалий

Метод: `POST [IP-адрес Комплекса]:8081/api/models/work`

Описание: Переводит все модели в режим детектирования аномалий.

> Прим.:
>
> Если в момент выполнения команды модель находилась в процессе обучения, то она будет переведена в режим детектирования аномалий принудительно. Если модель находилась в режиме валидации, то процесс валидации завершается, а модель будет переведена в режим детектирования аномалий.
>
> Аналогичным способом происходит и перевод в режим детектирования аномалий для моделей, поставленных на паузу; при этом модель не снимается с паузы.

Пример запроса:

```
curl -X 'POST' \
  'http://[IP-адрес Комплекса]:8081/api/models/work' \
  -H 'accept: application/json'
```

17.1.2.1. Успешный ответ

Код ответа: `204`

Тип содержимого: Отсутствует (No Content).

17.1.3. Перевод определенной модели в режим детектирования аномалий

Метод: `POST [IP-адрес Комплекса]:8081/api/models/{model_id}/work`

Описание: Переводит в режим детектирования аномалий указанную модель по ее идентификатору.

Пример запроса:

```
curl -X 'POST' \
  'http://[IP-адрес Комплекса]:8081/api/models/{model_id}/work' \
  -H 'accept: application/json'
```

Табл. 24. Описание параметров запроса

ПОЛЕ	ТИП	ОПИСАНИЕ
`model_id`	`string`	Идентификатор модели

17.1.3.1. Успешный ответ

Код ответа: `204`

Тип содержимого: Отсутствует (No Content).

17.1.4. Удаление модели

Метод: `DELETE [IP-адрес Комплекса]:8081/api/models/{model_id}`

Описание: Удаляет определенную модель до следующего перезапуска.

> Прим.:
>
> Несмотря на удаление, модель останется в конфигурации модуля. Это может привести к тому, что при следующем запуске модуля модель будет снова запущена в режиме обучения.
> Для полного удаления модели:
>
> 1. Выполните данный метод.
> 2. Удалите строки с описанием удаленной модели из файла `configuration.yaml`.

Пример запроса:

```
curl -X 'DELETE' \
  'http://[IP-адрес Комплекса]:8081/api/models/{model_id}' \
  -H 'accept: application/json'
```

Табл. 25. Описание параметров запроса

ПОЛЕ	ТИП	ОПИСАНИЕ
`model_id`	`string`	Идентификатор модели

17.1.4.1. Успешный ответ

Код ответа: `204`

Тип содержимого: Отсутствует (No Content).

17.1.5. Постановка модели на паузу

Метод: `POST [IP-адрес Комплекса]:8081/api/models/{model_id}/pause`

Описание: Приостанавливает работу указанной модели.

> Прим.:
>
> Постановка модели на паузу сохраняет все данные модели. Фактически постановка модели на паузу означает, что контроллер модели перестает пересылать данные, извлекаемые из сетевого трафика, в саму модель.

Пример запроса:

```
curl -X 'POST' \
  'http://[IP-адрес Комплекса]:8081/api/models/{model_id}/pause' \
  -H 'accept: application/json'
```

Табл. 26. Описание параметров запроса

ПОЛЕ	ТИП	ОПИСАНИЕ
`model_id`	`string`	Идентификатор модели

17.1.5.1. Успешный ответ

Код ответа: `204`

Тип содержимого: Отсутствует (No Content).

17.1.6. Продолжение функционирования модели

Метод: `POST [IP-адрес Комплекса]:8081/api/models/{model_id}/pause`

Описание: Снимает указанную модель с паузы, после чего модель продолжит работу в режиме, в котором она находилась до постановки на паузу.

> Прим.:
>
> Фактически снятие модели с паузы означает, что контроллер модели вновь начнет пересылать данные, извлекаемые из сетевого трафика, в саму модель.

Пример запроса:

```
curl -X 'POST' \
  'http://[IP-адрес Комплекса]:8081/api/models/{model_id}/resume' \
  -H 'accept: application/json'
```

Табл. 27. Описание параметров запроса

ПОЛЕ	ТИП	ОПИСАНИЕ
`model_id`	`string`	Идентификатор модели

17.1.6.1. Успешный ответ

Код ответа: `204`

Тип содержимого: Отсутствует (No Content).

17.1.7. Повторное обучение модели

Метод: `POST [IP-адрес Комплекса]:8081/api/models/{model_id}/retrain`

Описание: Переводит указанную модель в режим обучения без учета ранее накопленных данных.

> Прим.:
>
> При выполнении этого метода модель будет переведена в исходное состояние, в котором она не имеет никакой приоритетной информации касательно данной инсталляции.

Пример запроса:

```
curl -X 'POST' \
  'http://[IP-адрес Комплекса]:8081/api/models/{model_id}/resume' \
  -H 'accept: application/json'
```

Табл. 28. Описание параметров запроса

ПОЛЕ	ТИП	ОПИСАНИЕ
`model_id`	`string`	Идентификатор модели

17.1.7.1. Успешный ответ

Код ответа: `204`

Тип содержимого: Отсутствует (No Content).

17.1.8. Принудительный расчет маски для всех моделей

Метод: `POST [IP-адрес Комплекса]:8081/api/models/calculate_masks`

Описание: Запускает расчет маски для всех моделей, у которых определена маска в конфигурации.

Пример запроса:

```
curl -X 'POST' \
  'http://[IP-адрес Комплекса]:8081/api/models/calculate_masks' \
  -H 'accept: application/json'
```

17.1.8.1. Успешный ответ

Код ответа: `204`

Тип содержимого: Отсутствует (No Content).

17.1.9. Принудительный расчет маски для определенной модели

Метод: `POST [IP-адрес Комплекса]:8081/api/models/{model_id}/calculate_mask`

Описание: Запускает расчет маски для определенной модели по ее идентификатору.

Пример запроса:

```
curl -X 'POST' \
  'http://[IP-адрес Комплекса]:8081/api/models/{model_id}/calculate_mask' \
  -H 'accept: application/json'
```

Табл. 29. Описание параметров запроса

ПОЛЕ	ТИП	ОПИСАНИЕ
`model_id`	`string`	Идентификатор модели

17.1.9.1. Успешный ответ

Код ответа: `204`

Тип содержимого: Отсутствует (No Content).

17.1.10. Просмотр информации о модели на основе иерархического словаря

Метод: `GET [IP-адрес Комплекса]:8081/api/models/qdict/{model_id}`

Описание: Выводит информацию о модели на основе иерархического словаря с указанным идентификатором в блоке `Server Response`.

Пример запроса:

```
curl -X 'GET' \
  'http://[IP-адрес Комплекса]:8081/api/models/qdict/{model_id}' \
  -H 'accept: application/json'
```

Табл. 30. Описание параметров запроса

ПОЛЕ	ТИП	ОПИСАНИЕ
`model_id`	`string`	Идентификатор модели

17.1.10.1. Успешный ответ

Код ответа: 200

Тип содержимого: `application/json`

Пример тела ответа:

```
{
  "statistics": {
    "checks_count": 36358,
    "success_checks_number": 36358,
    "anomalies_count": 0,
    "valid_packets_count": 72716,
    "invalid_packets_count": 0,
    "probability_of_correct_prediction": 100
```

```
  },
  "model_status": "WORKING",
  "qdict": {
    "(1,)": 2,
    "(3,)": 4,
    "(5,)": 6,
    "(7,)": 8,
    "(((7, 8),), 1)": 9,
    "(((3, 4),), 5)": 10,
    "(((5, 10), (7, 8)), 1)": 11,
    "(((3, 4), (5, 10), (7, 8)), 1)": 12,
    "(((1, 12), (3, 4), (5, 10), (7, 8)), 1)": 13,
    "(((1, 13), (3, 4), (5, 10), (7, 8)), 1)": 14,
    "(((1, 14), (3, 4), (5, 10), (7, 8)), 1)": 15,
    "(((1, 15), (3, 4), (5, 10), (7, 8)), 1)": 16,
    "(((1, 16), (3, 4), (5, 10), (7, 8)), 1)": 17,
    "(((1, 17), (3, 4), (5, 10), (7, 8)), 1)": 18,
    "(((1, 18), (3, 4), (5, 10), (7, 8)), 1)": 19,
    "(((1, 19), (3, 4), (5, 10), (7, 8)), 1)": 20,
    ...
  }
}
```


Табл. 31. Описание полей ответа на запрос

ПОЛЕ	ТИП	ОПИСАНИЕ
`statistics`	`object`	Статистика модели
`statistics.checks_count`	`integer`	Общее количество проверок
`statistics.success_checks_number`	`integer`	Количество успешных проверок
`statistics.anomalies_count`	`integer`	Количество аномалий
`statistics.valid_packets_count`	`integer`	Количество действительных пакетов
`statistics.invalid_packets_count`	`integer`	Количество недействительных пакетов
`statistics.probability_of_correct_-prediction`	`integer`	Вероятность корректного предсказания
`model_status`	`string`	Статус модели
`qdict`	`object`	Состав иерархического словаря

См. также

Модель на основе иерархического словаря

17.1.11. Просмотр информации о модели на основе временного автомата

Метод: `GET [IP-адрес Комплекса]:8081/api/models/otala/{model_id}`

Описание: Выводит информацию о модели на основе временного автомата с указанным идентификатором в блоке `Server Response`.

Пример запроса:

```
curl -X 'GET' \
  'http://[IP-адрес Комплекса]:8081/api/models/otala/{model_id}' \
  -H 'accept: application/json'
```

Табл. 32. Описание параметров запроса

ПОЛЕ	ТИП	ОПИСАНИЕ
`model_id`	`string`	Идентификатор модели

17.1.11.1. Успешный ответ

Код ответа: 200

Тип содержимого: `application/json`

Пример тела ответа:

```
{
  "first_node_conf": {
    "mode": "starts_with",
    "layers": [
      {
        "value": "11:11:11:11:11",
        "protocol": "ethernet",
        "format": "mac",
        "_hex_value": "31313a31313a31313a31313a3131"
      },
      {
        "value": "1.1.1.1",
        "protocol": "ip",
        "format": "ip",
        "_hex_value": "312e312e312e31"
      }
    ],
    "_id": 1,
    "_addresses": [
      1,
      2
    ]
```

```
  },
  "second_node_conf": {
    "mode": "starts_with",
    "layers": [
      {
        "value": "22:22:22:22:22",
        "protocol": "ethernet",
        "format": "mac",
        "_hex_value": "32323a32323a32323a32323a3232"
      },
      {
        "value": "2.2.2.2",
        "protocol": "ip",
        "format": "ip",
        "_hex_value": "322e322e322e32"
      }
    ],
    "_id": 2,
    "_addresses": [
      3,
      4
    ]
  },
  "_id": "0-5962b271-a934-435a-b906-69bb5fe5c2e9",
  "_paused": false,
  "configuration": {
    "separation": {
      "enabled": true,
      "max_group_commands_count": 100,
      "entropy_threshold": 0.5
    },
    "convergence_number_max": null
  },
  "_alphabet": {
    "_input": [
      "0"
    ],
    "_output": [
      "0"
    ],
    "_id": "952e4aae-b628-46bc-b1d2-9c186bf95c5f"
  },
  "_timed_automation": {
    "transitions": []
  },
  "type": "OTALA"
}
```

Табл. 33. Описание полей ответа на запрос

ПОЛЕ	ТИП	ОПИСАНИЕ
`first_node_conf`	`object`	Конфигурация первого узла
`first_node_conf.mode`	`string`	Режим работы узла
`first_node_conf.layers`	`array`	Список слоев (протоколов) с описанием параметров
`layers[].value`	`string`	Значение (например, MAC-адрес "11:11:11:11:11" или IP "1.1.1.1")
`layers[].protocol`	`string`	Протокол (например, "ethernet", "ip")
`layers[].format`	`string`	Формат значения (например, "mac", "ip")
`layers[]._hex_value`	`string`	HEX-представление значения
`first_node_conf._id`	`integer`	Уникальный идентификатор узла
`first_node_conf._addresses`	`array`	Список связанных адресов
`second_node_conf`	`object`	Конфигурация второго узла. Аналогично `first_node_conf`
`_id`	`string`	Уникальный идентификатор модели
`_paused`	`boolean`	Признак того, что модель поставлена на паузу
`configuration`	`object`	Дополнительные настройки модели
`configuration.separation`	`object`	Параметры разделения
`separation.enabled`	`boolean`	Признак активности разделения
`separation.max_group_commands_count`	`integer`	Максимальное количество команд в группе
`separation.entropy_threshold`	`float`	Порог энтропии для разделения
`configuration.convergence_number_max`	`null | integer`	Максимальное число сходимости
`_alphabet`	`object`	Алфавит входных/выходных символов
`_alphabet._input`	`array`	Список входных символов

Табл. 33. Описание полей ответа на запрос

ПОЛЕ	ТИП	ОПИСАНИЕ
`_alphabet._output`	`array`	Список выходных символов
`_alphabet._id`	`string`	Уникальный идентификатор алфавита
`_timed_automation`	`object`	Описание временного автомата
`_timed_automation.transitions`	`array`	Список переходов
`type`	`string`	Тип модели (например, "OTALA")

См. также

Модель на основе временного автомата

17.1.12. Просмотр информации о модели на основе гибридного автомата

Метод: `GET [IP-адрес комплекса]:8081/api/models/hybrid_automaton/{model_id}`

Описание: Выводит информацию о модели на основе гибридного автомата с указанным идентификатором в блоке `Server Response`.

Пример запроса:

```
curl -X 'GET' \
  'http://[IP-адрес Комплекса]:8081/api/models/hybrid_automaton/{model_id}' \
  -H 'accept: application/json'
```

Табл. 34. Описание параметров запроса

ПОЛЕ	ТИП	ОПИСАНИЕ
`model_id`	`string`	Идентификатор модели

17.1.12.1. Успешный ответ

Код ответа: `200`

Тип содержимого: `application/json`

Пример тела ответа:

```
{
  "statistics": {
    "non_existent_transition_anomaly_count": 0,
    "prediction_error_in_state_anomaly_count": 0,
    "relative_prediction_error": 1.9716408563249292,
    "checks_count": 9882,
    "success_checks_number": 9482,
    "anomalies_count": 40,
```

```
    "valid_packets_count": 9482,
    "invalid_packets_count": 40,
    "probability_of_correct_prediction": 0.9595223638939486
  },
  "commands_stat": {
    "handled_commands_count": 3341368,
    "unprocessed_commands": 0,
    "skipped_commands": 0
  },
  "model_status": "WORKING"
}
```


Табл. 35. Описание полей ответа на запрос

ПОЛЕ	ТИП	ОПИСАНИЕ
`statistics`	`object`	Статистика модели
`statistics.non_existent_-transition_anomaly_count`	`integer`	Количество аномалий, связанных с попыткой перехода по несуществующему переходу в автомате
`statistics.prediction_error_-in_state_anomaly_count`	`integer`	Количество аномалий, вызванных ошибками предсказания внутри состояния
`statistics.relative_-prediction_error`	`integer`	Относительная ошибка предсказания
`statistics.checks_count`	`integer`	Общее количество проверок
`statistics.success_checks_-number`	`integer`	Количество успешных проверок
`statistics.anomalies_count`	`integer`	Количество аномалий
`statistics.valid_packets_-count`	`integer`	Количество действительных пакетов
`statistics.invalid_packets_-count`	`integer`	Количество недействительных пакетов
`statistics.probability_of_-correct_prediction`	`integer`	Вероятность корректного предсказания
`commands_stat`	`object`	Статистика по командам

Табл. 35. Описание полей ответа на запрос

ПОЛЕ	ТИП	ОПИСАНИЕ
`commands_stat.handled_-commands_count`	`integer`	Количество обработанных команд
`commands_stat.unprocessed_-commands`	`integer`	Количество необработанных команд
`commands_stat.skipped_-commands`	`integer`	Количество пропущенных команд
`model_status`	`string`	Статус модели

См. также

Модель на основе гибридного автомата

17.1.13. Запуск дообучения для модели на основе временного автомата

Метод: `POST [IP-адрес Комплекса]:8081/api/models/otala/{model_id}`

Описание: Запускает процесс дообучения модели в соответствии с введенными данными.

Пример запроса:

```
curl -X 'POST' \
  'http://[IP-адрес Комплекса]:8081/api/models/otala/{model_id}' \
  -H 'accept: application/json' \
  -H 'Content-Type: application/json' \
  -d '{
    "first_request_command": 9,
    "first_response_command": 10,
    "second_request_command": 1,
    "second_response_command": 2,
    "time_interval": 160
  }'
```

Табл. 36. Описание параметров запроса

ПОЛЕ	ТИП	ОПИСАНИЕ
`model_id`	`string`	Идентификатор модели

Табл. 37. Тело запроса

ПОЛЕ	ТИП	ОПИСАНИЕ
`first_request_command`	`integer`	Количество команд при первом запросе

Табл. 37. Тело запроса

ПОЛЕ	ТИП	ОПИСАНИЕ
`first_response_command`	`integer`	Количество команд при первом ответе
`second_request_command`	`integer`	Количество команд при втором запросе
`second_response_command`	`integer`	Количество команд при втором ответе
`time_interval`	`integer`	Временной интервал

17.1.13.1. Успешный ответ

Код ответа: `200`

Тип содержимого: `application/json`

Пример тела ответа:


```
{
  "source": {
    "input_indexes": [
      1
    ],
    "output_indexes": [
      1
    ],
    "time": 0
  },
  "destination": {
    "input_indexes": [
      2
    ],
    "output_indexes": [
      2
    ],
    "time": 0
  },
  "time": 160,
  "_max_time": 160,
  "_min_time": 160
}
```

Табл. 38. Описание полей ответа на запрос

ПОЛЕ	ТИП	ОПИСАНИЕ
`source`	`integer`	Информация об источнике
`source[].input_indexes`	`integer`	Входные индексы
`source[].output_indexes`	`integer`	Выходные индексы
`destination`	`integer`	Информация о получателе
`destination[].input_indexes`	`integer`	Входные индексы
`destination[].output_indexes`	`integer`	Выходные индексы
`time`	`integer`	Время
`_max_time`	`integer`	Максимальное время
`_min_time`	`integer`	Минимальное время

См. также

Модель на основе временного автомата

17.1.14. Запуск дообучения модели на основе иерархического словаря

Метод: `POST [IP-адрес Комплекса]:8081/api/models/qdict/{model_id}`

Описание: Запускает процесс дообучения модели в соответствии с введенными данными.

Пример запроса:

```
curl -X 'POST' \
  'http://[IP-адрес Комплекса]:8081/api/models/qdict/{model_id}' \
  -H 'accept: application/json' \
  -H 'Content-Type: application/json' \
  -d '{
    "response_command_id": 1,
    "request_response_chain": [
      [[8, 12], [8, 13]],
      8
    ]
  }'
```

Табл. 39. Описание параметров запроса

ПОЛЕ	ТИП	ОПИСАНИЕ
`model_id`	`string`	Идентификатор модели

Табл. 40. Тело запроса

ПОЛЕ	ТИП	ОПИСАНИЕ
`response_command_id`	`integer`	Идентификатор команды ответа
`request_response_chain`	`array`	Цепочка запросов и ответов

17.1.14.1. Успешный ответ

Код ответа: `204`

Тип содержимого: Отсутствует (No Content).

См. также

Модель на основе иерархического словаря

17.1.15. Экспорт модели на основе гибридного автомата

Метод: `GET [IP-адрес комплекса]:8081/api/models/hybrid_automaton/{model_id}/unload`

Описание: Выводит информацию о гибридном автомате в формате JSON.

Пример запроса:

```
curl -X 'GET' \
  'http://[IP-адрес Комплекса]:8081/api/models/hybrid_automaton/{model_id}/unload?pretty=true' \
  -H 'accept: application/json'
```

Табл. 41. Описание параметров запроса

ПОЛЕ	ТИП	ОПИСАНИЕ
`model_id`	`string`	Идентификатор модели
`pretty`	`boolean`	Признак форматированого вывода информации

17.1.15.1. Успешный ответ

Код ответа: `200`

Тип содержимого: `application/json`

Пример тела ответа:

```
{
    "modes": {},
    "polynomial_model": {},
    "transitions": {},
    "max_normal_ape": [],
    "another_HA_params": {},
    "standard_scaler": {},
```

```
    "svc_model": {}
}
```

Табл. 42. Описание полей ответа на запрос

ПОЛЕ	ТИП	ОПИСАНИЕ
`modes`	`object`	Список состояний гибридного автомата
`polynomial_model`	`object`	Информация о модели аппроксимирующего полинома
`transitions`	`object`	Список переходов гибридного автомата
`max_normal_ape`	`array`	Допустимая величина ошибки предсказания по каждому значению анализируемых регистров
`another_HA_params`	`object`	Список служебных параметров гибридного автомата
`standard_scaler`	`object`	Параметры масштабирования данных
`svc_model`	`object`	Параметры для метода опорных векторов

См. также

Модель на основе гибридного автомата

17.1.16. Получение информации об элементах словаря моделей по идентификатору

Метод: `GET [IP-адрес Комплекса]:8081/api/commands`

Описание: Выводит список запрашиваемых элементов словаря моделей.

Пример запроса:

```
curl -X 'GET' \
  'http://[IP-адрес Комплекса]:8081/api/commands?ids=1&ids=2' \
  -H 'accept: application/json'
```

Табл. 43. Описание параметров запроса

ПОЛЕ	ТИП	ОПИСАНИЕ
`ids`	`array`	Список идентификаторов элементов

17.1.16.1. Успешный ответ

Код ответа: `200`

Тип содержимого: `application/json`

Пример тела ответа:


```
[
  {
    "id": 1,
    "payload": [
      {
        "value": "1",
        "name": "unit_id",
        "protocol_name": "modbus_detailed"
      },
      {
        "value": "READ_INPUT_REGISTERS",
        "name": "func",
        "protocol_name": "modbus_detailed"
      },
      {
        "value": "0",
        "name": "request_address",
        "protocol_name": "modbus_detailed"
      },
      {
        "value": "7",
        "name": "request_quantity",
        "protocol_name": "modbus_detailed"
      }
    ],
    "protocol": "modbus_detailed"
  },
  {
    "id": 2,
    "payload": [
      {
        "value": "1",
        "name": "unit_id",
        "protocol_name": "modbus_detailed"
```

```
      },
      {
        "value": "READ_INPUT_REGISTERS",
        "name": "func",
        "protocol_name": "modbus_detailed"
      },
      {
        "value": "7",
        "name": "response_quantity",
        "protocol_name": "modbus_detailed"
      },
      {
        "value": [
          "0",
          "0",
          "243",
          "0",
          "0",
          "0",
          "243"
        ],
        "name": "response_registers",
        "protocol_name": "modbus_detailed"
      }
    ],
    "protocol": "modbus_detailed"
  }
]
```


Табл. 44. Описание полей ответа на запрос

ПОЛЕ	ТИП	ОПИСАНИЕ
`id`	`integer`	Уникальный идентификатор элемента
`payload`	`array`	Массив объектов, содержащих параметры элемента
`payload[].value`	`string | array`	Значение параметра
`payload[].name`	`string`	Название параметра
`payload[].protocol_name`	`string`	Название протокола, к которому относится параметр
`protocol`	`string`	Общее название протокола

17.2. Получение информации об адресах по идентификаторам

Метод: `GET [IP-адрес Комплекса]:8081/api/addresses`

Описание: Возвращает детальную информацию о запрашиваемых адресах.

Пример запроса:

```
curl -X 'GET' \
  'http://[IP-адрес Комплекса]:8081/api/addresses?ids=1&ids=2' \
  -H 'accept: application/json'
```

Табл. 45. Описание параметров запроса

ПОЛЕ	ТИП	ОПИСАНИЕ
`ids`	`array`	Список идентификаторов адресов (опционально)

17.2.1. Успешный ответ

Код ответа: `200`

Тип содержимого: `application/json`

Пример тела ответа:

```
{
  "1": {
    "id": 1,
    "protocol": "ip",
    "value": "3139322e3136382e302e34"
  },
  "2": {
    "id": 2,
    "protocol": "ip",
    "value": "3139322e3136382e302e33"
  }
}
```

Табл. 46. Описание полей ответа на запрос

ПОЛЕ	ТИП	ОПИСАНИЕ
`id`	`integer`	Идентификатор адреса
`protocol`	`string`	Протокол
`value`	`string`	Значение адреса

17.3. Получение информации о сетевом узле по идентификатору

Метод: `GET [IP-адрес Комплекса]:8081/api/nodes/{node_id}`

Описание: Возвращает информацию о сетевом узле по его идентификатору.

Пример запроса:

```
curl -X 'GET' \
  'http://[IP-адрес Комплекса]:8081/api/nodes/{node_id}?mode=equal' \
  -H 'accept: application/json'
```

Табл. 47. Описание параметров запроса

ПОЛЕ	ТИП	ОПИСАНИЕ
`node_id`	`integer`	Идентификатор сетевого узла
`mode`	`string`	Режим поиска (`equal` или `starts_with`)

17.3.1. Успешный ответ

Код ответа: `200`

Тип содержимого: `application/json`

Пример тела ответа:

```
{
  "id": 1,
  "address": [1, 2],
  "child_nodes": [
    {
      "id": 2,
      "address": [3],
      "child_nodes": []
    }
  ]
}
```

Табл. 48. Описание полей ответа на запрос

ПОЛЕ	ТИП	ОПИСАНИЕ
`id`	`integer`	Идентификатор сетевого узла
`address`	`array`	Список адресов сетевого узла
`child_nodes`	`array`	Дочерние сетевые узлы

17.4. Получение списка сетевых узлов модуля «EDR for PLC»

Метод: `GET [IP-адрес Комплекса]:8081/api/nodes`

Описание: Возвращает список идентификаторов выявленных сетевых узлов, а также структуру адресов, из которых они сформированы.

Пример запроса:

```
curl -X 'GET' \
  'http://[IP-адрес Комплекса]:8081/api/nodes' \
  -H 'accept: application/json'
```

17.4.1. Успешный ответ

Код ответа: `200`

Тип содержимого: `application/json`

Пример тела ответа:

```
{
  "id": 1,
  "address": [1, 2],
  "child_nodes": [
    {
      "id": 2,
      "address": [3],
      "child_nodes": []
    }
  ]
}
```

Табл. 49. Описание полей ответа на запрос

ПОЛЕ	ТИП	ОПИСАНИЕ
`id`	`integer`	Идентификатор сетевого узла
`address`	`array`	Список адресов сетевого узла
`child_nodes`	`array`	Дочерние сетевые узлы

17.5. Просмотр статистики по разбору сетевого трафика модулем «EDR for PLC»

Метод: `GET [IP-адрес Комплекса]:8081/api/services/info`

Описание: Выводит основную информацию о работе сервиса анализа сетевого трафика.

Пример запроса:

```
curl -X 'GET' \
  'http://[IP-адрес Комплекса]:8081/api/services/info' \
  -H 'accept: application/json'
```

17.5.1. Успешный ответ

Код ответа: `200`

Тип содержимого: `application/json`

Пример тела ответа:

```
{
  "commands_saver": {
    "enabled": true,
    "alive": true,
    "statistic": {
      "handled_packets": 594114,
      "skipped_packets": 0
    }
  },
  "models_controller": {
    "enabled": true,
    "alive": null,
    "statistic": null,
    "models_count": 1
  }
}
```


Табл. 50. Описание полей ответа на запрос

ПОЛЕ	ТИП	ОПИСАНИЕ
`commands_saver`	`object`	Информация о сервисе сохранения команд
`commands_saver.enabled`	`boolean`	Признак состояния сервиса сохранения команд
`commands_saver.alive`	`boolean`	Признак активности сервиса сохранения команд
`commands_saver.statistics`	`object`	Статистика по пакетам
`commands_saver.statistics.handled_packets`	`number`	Количество обработанных пакетов
`commands_saver.statistics.skipped_packets`	`number`	Количество пропущенных пакетов
`models_controller`	`object`	Информация о контроллере моделей
`models_controller.enabled`	`boolean`	Признак состояния контроллера моделей
`models_controller.alive`	`boolean`	Признак активности контроллера моделей

Табл. 50. Описание полей ответа на запрос

ПОЛЕ	ТИП	ОПИСАНИЕ
`models_controller.statistics`	`object | null`	Статистика по пакетам
`models_controller.models_count`	`number`	Количество моделей

17.6. Просмотр статуса активности формирования немодельных аномалий

Метод: `GET [IP-адрес Комплекса]:8081/api/anomalies/generation_not_from_models`

Описание: Отображает текущее состояние активности формирования немодельных аномалий (`true` — активно, `false` — не активно).

Пример запроса:

```
curl -X 'GET' \
  'http://[IP-адрес Комплекса]:8081/api/anomalies/generation_not_from_models' \
  -H 'accept: application/json'
```

17.6.1. Успешный ответ

Код ответа: `200`

Тип содержимого: `application/json`

Пример тела ответа:

```
true
```

17.7. Включение/отключение создания немодельных аномалий

Метод: `PATCH [IP-адрес Комплекса]:8081/api/anomalies/generation_not_from_models`

Описание: Активирует или деактивирует создание немодельных аномалий.

Пример запроса:

```
curl -X 'PATCH' \
  'http://[IP-адрес Комплекса]:8081/api/anomalies/generation_not_from_models?new_value=true' \
  -H 'accept: application/json'
```

Табл. 51. Описание параметров запроса

ПОЛЕ	ТИП	ОПИСАНИЕ
`new_value`	`boolean`	Новый признак активности/неактивности создания немодельных аномалий

17.7.1. Успешный ответ

Код ответа: `204`

Тип содержимого: Отсутствует (No Content).

17.8. Возможные ошибки API модуля «EDR for PLC»

При работе с API модуля UDV DATAPK EDR for PLC могут возникать ошибки, описание которых представлено в таблице ниже.

Табл. 52. Возможные ошибки

HTTP-КОД	ЗНАЧЕНИЕ	ОПИСАНИЕ	ПРИМЕР ТЕЛА ОТВЕТА
422	Validation Error	Ошибка валидации данных	`{ "detail": [ { "loc": ["field"], "msg": "error", "type": "type" } ] }`
404	Not Found	Не найдено	`{ "detail": "Not Found" }`
500	Internal Server Error	Внутренняя ошибка сервера	`{ "detail": "Internal Server Error" }`

18. Управление Комплексом

В этом разделе:

1. **Изменение сведений о Комплексе и сенсорах**
2. **Сканирование сети и определение интерфейсов активного сетевого оборудования**
3. **Настройка контролируемой сети**
4. **Управление пользователями**
5. **Экспорт отдельных справочников**
6. **Диагностика состояния системы Комплекса**
7. **Диагностика состояния сенсора**
8. **Удаление сенсора**

На страницах управления выполняется настройка параметров использования Комплекса: сведения о текущем Комплексе, контролируемая сеть, пользователи, экспорт данных и диагностика.

18.1. Изменение сведений о Комплексе и сенсорах

18.1.1. Изменение сведений о текущем Комплексе

1. Перейдите на страницу **Администрирование → Основные настройки → О системе**.
2. В блоке **Сведения о Комплексе** введите описание Комплекса, наименование эксплуатирующей организации и место установки. Наименование Комплекса настраивается автоматически.

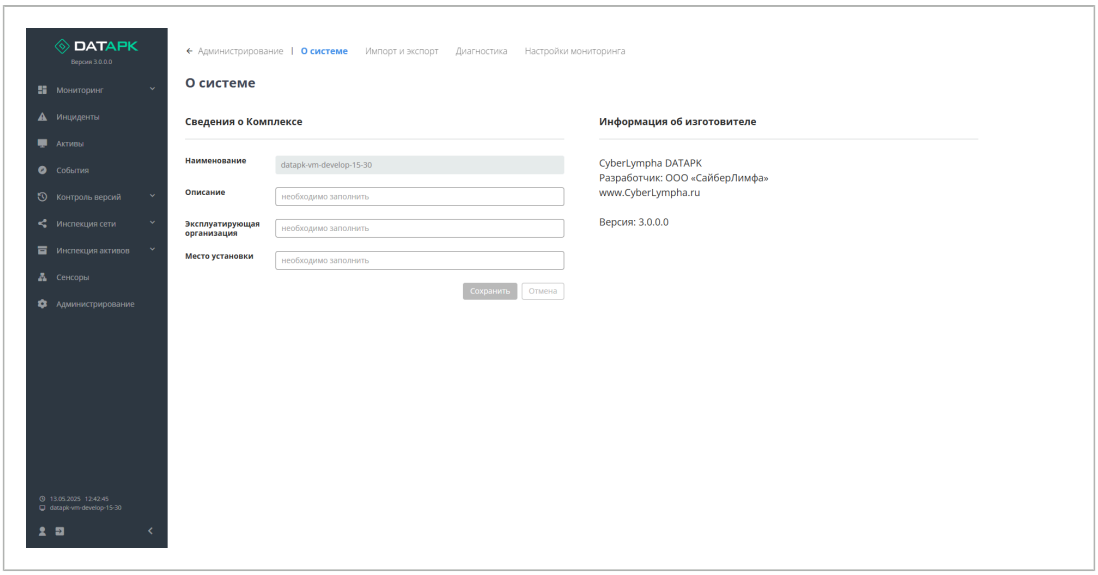


Рис. 438. Страница «О системе»

3. Нажмите кнопку **Сохранить** для подтверждения изменений.

18.1.2. Изменение сведений о сенсорах, подключенных к Комплексу

1. Перейдите на страницу **Сенсоры**.
2. Выберите сенсор из списка.
   - **Результат шага:** справа откроется карточка выбранного сенсора.

3. В открывшейся панели нажмите кнопку (**Редактировать**) напротив наименования сенсора.

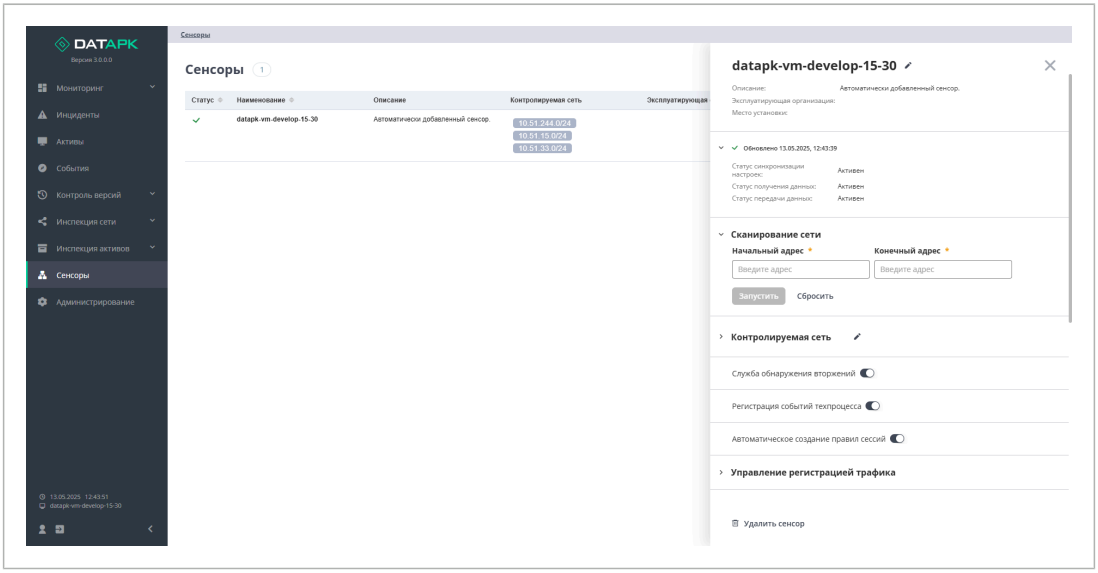


Рис. 439. Страница «Сенсоры»

4. Введите описание сенсора, наименование эксплуатирующей организации и место установки.

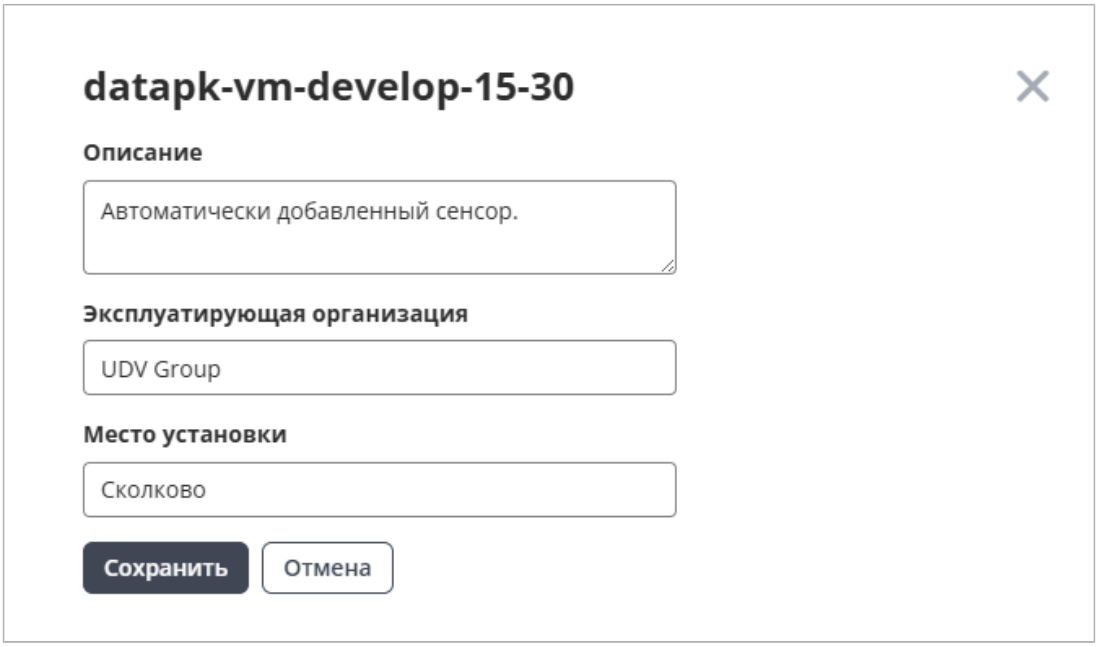


Рис. 440. Блок редактирования информации о сенсоре

5. Нажмите кнопку **Сохранить** для подтверждения изменений.

18.2. Сканирование сети и определение интерфейсов активного сетевого оборудования

Комплекс обнаруживает новые активы в автоматическом режиме, выполняя активное сканирование сети через активный интерфейс сенсоров, а также дополняя полученные данные за счет пассивного анализа трафика, поступающего на прослушивающий интерфейс. Такими данными могут быть IP-адреса источников или получателей пакетов.

Для некоторых активов возможно определение дополнительной информации об операционной системе: версии ОС, NetBIOS и сетевого имени. Вся полученная информация об активах отображается на странице **Активы**. Если сетевое имя актива удастся определить, его наименование в Комплексе автоматически меняется на сетевое имя.

> Прим.:
>
> Комплекс не сможет обнаружить актив, если до него нет доступа из-за особенностей настроек межсетевого экрана в сети предприятия.
>
> Сетевое имя актива возможно определить, только если в ОС Комплекса настроен DNS.

Способ обнаружения активов по MAC-адресу и их отображение зависит от значения переменной `AUTOMATIC_HOST_CREATION_BY_MAC` в конфигурационном файле `manager.env`:

- Если переменная имеет значение `true`, либо она не задана в файле `manager.env`, Комплекс фиксирует активы только по MAC-адресу независимо от наличия у них IP-адреса. В списке активов отображаются все найденные активы (до настройки контролируемой сети активы отображаются только с MAC-адресами).
- Если переменная имеет значение `false`, Комплекс фиксирует активы по MAC-адресу (если IP-адрес не обнаружен) и по связке MAC-адреса и IP-адреса. В списке активов будут отображаться только активы, IP-адреса которых входят в контролируемую сеть, а также активы, IP-адреса которых не обнаружены.

Сканирование определяет новые доступные сетевые узлы. Также возможно определение их IP-адреса, MAC-адреса и сетевого имени (если данная информация доступна в режиме быстрого сканирования).

Для сканирования сети:

1. Перейдите на страницу **Сенсоры**.
2. Выберите сенсор.
   - **Результат шага:** справа откроется карточка с описанием и настройками выбранного сенсора.
3. На панели **Сканирование сети** введите начальный и конечный адреса для сканирования.

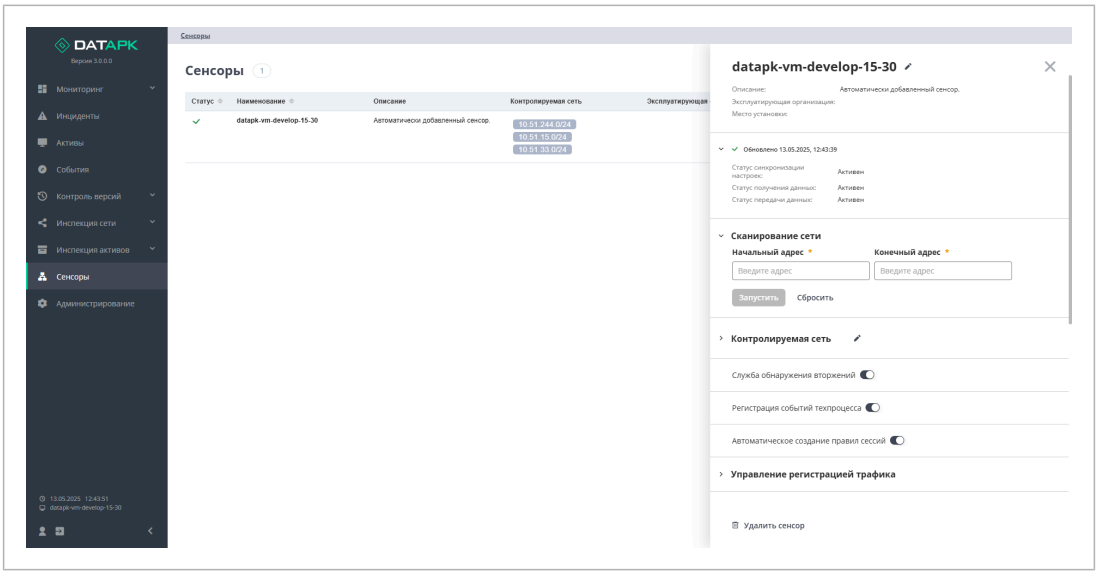


Рис. 441. Панель «Сканирование сети»

4. Нажмите кнопку **Запустить**.

> Внимание:
>
> При уменьшении количества IP-адресов, входящих в контролируемую подсеть (при изменении подсети в меньшую сторону), активы с типом `Неизвестный тип`, IP-адреса которых больше не входят в нее, будут удалены даже при наличии сетевого имени.

▸ **Результат шага:** появится уведомление `Запущено сканирование контролируемой сети`. По завершении сканирования сети на странице **Активы** будут отображаться новые неизвестные активы.

18.2.1. Интерпретация результатов пассивного сканирования сети

В процессе пассивного сканирования сети в Комплексе могут быть получены следующие результаты на странице **Активы**, которые необходимо проверить:

- Активу может быть присвоен дополнительный интерфейс с таким же IP-адресом, как у одного из его интерфейсов, но с другим MAC-адресом. Это может произойти из-за того, что в сетевых пакетах, отправленных с IP-адреса этого актива, был указан MAC-адрес интерфейса маршрутизатора. Тогда Комплекс в первую очередь проверяет принадлежность MAC-адреса одному из интерфейсов маршрутизатора, к которому подключен Комплекс. Если MAC-адрес принадлежит маршрутизатору, Комплекс автоматически присваивает новый интерфейс активу, который уже имеет интерфейс с таким же IP-адресом, и дополнительный интерфейс получает отметку `with_router_mac`. Если автоматическое присвоение интерфейса выполнено по ошибке, создайте вручную новый актив и присвойте ему найденный интерфейс — тогда он будет автоматически удален из списка интерфейсов исходного актива.
- На странице **Активы** могут присутствовать несколько активов с разными интерфейсами, хотя они должны принадлежать одному активу (часто такие активы являются активным сетевым оборудованием). Если на таком активе открыт доступ по протоколу SNMP, то есть возможность привязать к нему необходимые интерфейсы и удалить лишние активы с помощью специального сканера сбора данных. Подробнее см. в разделе «Добавление сетевых атрибутов активу с помощью сканера сбора данных по SNMP».

18.3. Настройка контролируемой сети

Настройка контролируемой сети необходима для отображения на странице **Активы** активов, IP-адреса которых входят в контролируемую сеть, а также для обнаружения сетевых соединений в контролируемой сети и отображения информации о них на страницах раздела **Сетевые соединения**. До выполнения настройки контролируемой сети, в зависимости от настроек Комплекса, в списке активов отображаются все активы, найденные только по MAC-адресу, независимо от наличия у них IP-адреса, либо только активы, у которых не определен IP-адрес (подробнее см. раздел «Сканирование сети и определение интерфейсов активного сетевого оборудования»).

Для настройки контролируемой сети Комплекса:

1. Перейдите на страницу **Сенсоры**.
2. Выберите сенсор из списка.
   ▸ **Результат шага:** справа откроется карточка выбранного сенсора.

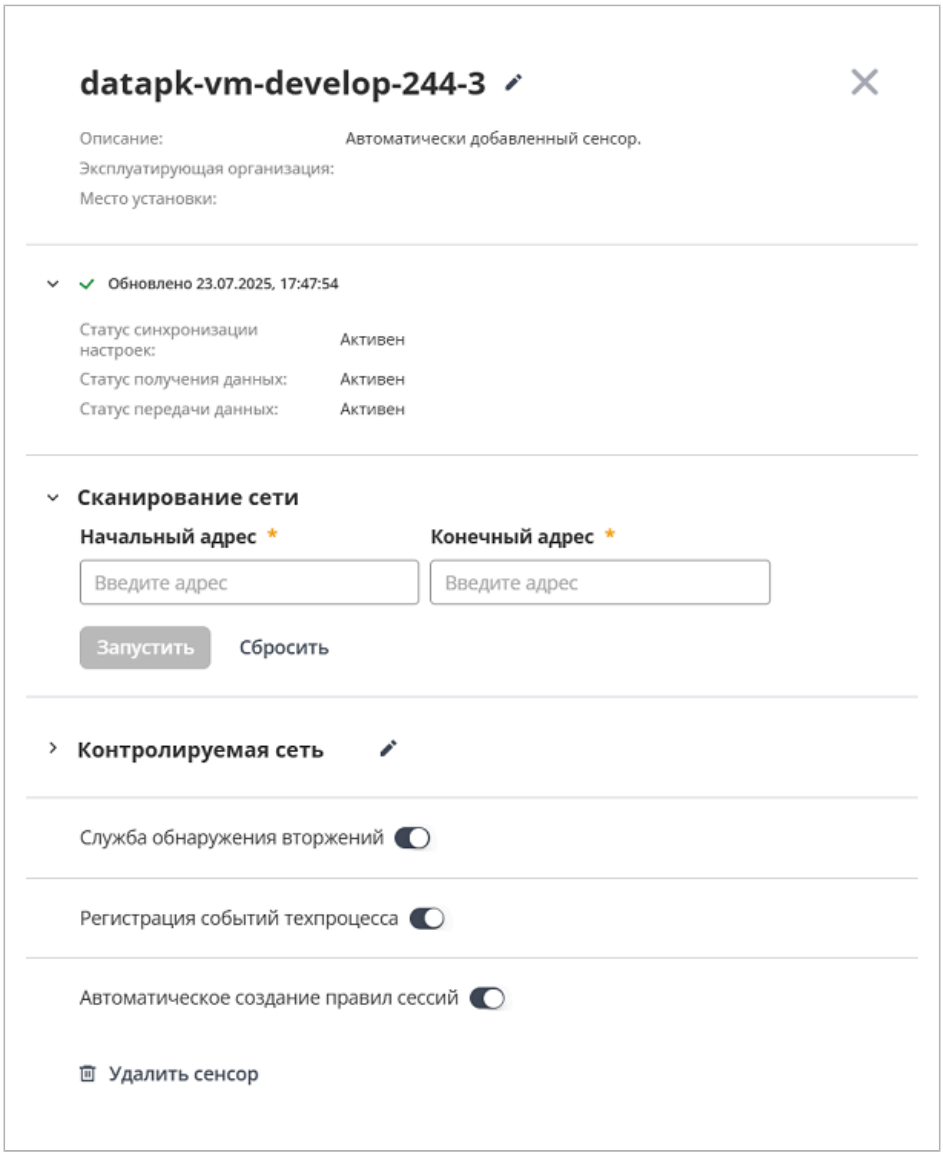


Рис. 442. Карточка сенсора

3. В открывшейся карточке в блоке **Контролируемая сеть** нажмите на (**Редактировать сеть**) для входа в режим редактирования.

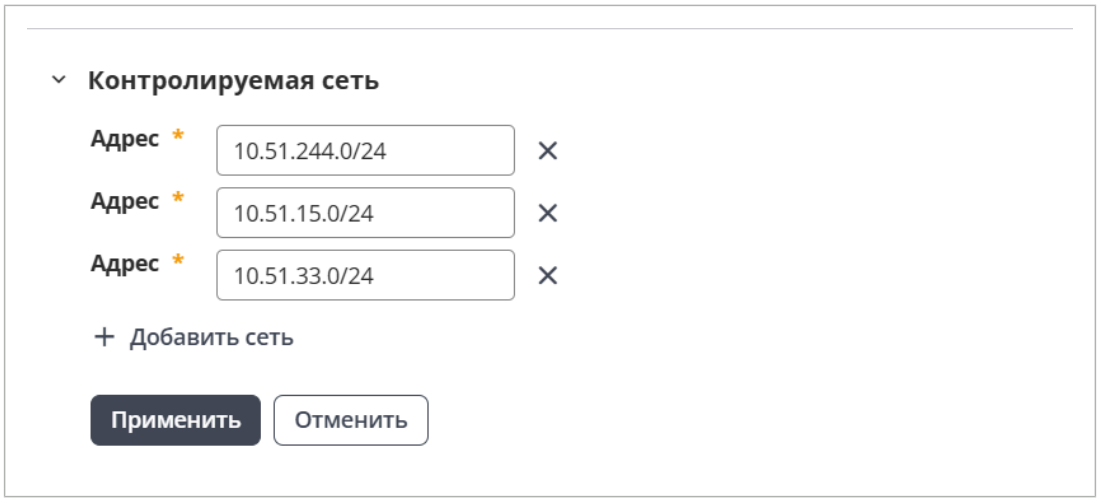


Рис. 443. Блок настроек сенсора «Контролируемая сеть» в режиме редактирования

4. Нажмите кнопку **+ Добавить сеть** и введите IP-адрес и маску подсети управляющего контура в качестве контролируемой подсети. Если требуется удалить добавленную ранее подсеть из списка, нажмите кнопку ✕ (**Удалить сеть**).
5. Нажмите кнопку **Применить** для сохранения внесенных изменений.

> ОСТОРОЖНО:
>
> Внесенные изменения в блоках **Контролируемая сеть** и **Управление файлами, извлеченными из трафика** сохраняются также при закрытии карточки сенсора, если в окне **Несохраненные данные** нажать кнопку **Закрыть**. Чтобы изменения не сохранились, нажмите **Отменить** в каждом измененном блоке, затем закройте карточку сенсора.

▸ **Результат шага:** Появится окно с предупреждением: `При смене контролируемой сети активы и сессии, не входящие в новую сеть, будут удалены.`

6. Нажмите **Подтвердить** для подтверждения всех изменений и запуска обновления списка активов в соответствии с указанными контролируемыми сетями.
7. Выполните шаги 2 - 6 для всех подключенных сенсоров, для которых нужно настроить контролируемую сеть.

▸ **Результат шага:**

- В список активов на странице **Активы** будут добавлены обнаруженные активы, IP-адреса которых входят в настроенные контролируемые сети.
- Каждому сетевому атрибуту обнаруженного актива будет присвоен сенсор, в чью контролируемую сеть входит IP-адрес атрибута. Присвоенный сенсор будет отображаться в поле **Сенсор** блока **Сетевые атрибуты** в **карточке актива**.
- На страницах раздела **Сетевые соединения** отображается информация о сетевых соединениях, обнаруживаемых в контролируемой сети.

18.4. Управление пользователями

В этом разделе:

- Управление учетными записями пользователей
    - Создание локальной учетной записи
    - Создание учетной записи службы каталогов
    - Редактирование учетных записей пользователей
- Настройка парольной политики

Об учетных записях

Учетная запись — хранимая в компьютерной системе совокупность данных о пользователе, необходимая для его опознавания (аутентификации) и предоставления доступа к его личным данным и настройкам.

Управление учетными записями осуществляется на странице **Администрирование → Пользователи**. При создании учетной записи, помимо стандартной пары логин-пароль, необходимо задать тип учетной записи и ее роль.

Вход и выход из Комплекса доступны всем пользователям, кроме заблокированных. Подробнее о блокировке см. раздел Блокировка и удаление учетной записи.

По умолчанию в веб-интерфейсе Комплекса разрешена только одна активная сессия для каждой учетной записи. При успешном входе пользователя с нового устройства предыдущая сессия завершится. Отключить ограничение на количество сессий можно в файле `manager.env` (подробнее см. раздел «Отключение ограничения на количество сессий пользователей»).

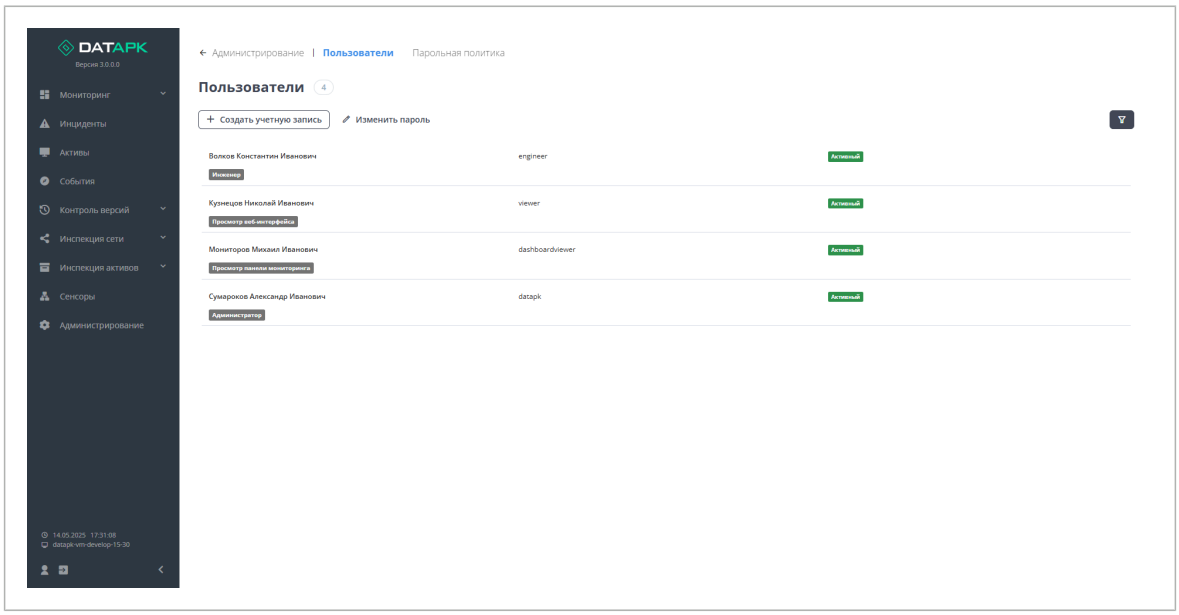


Рис. 444. Страница «Пользователи»

О ролях

Роль пользователя — это совокупность возможностей, которые получает пользователь Комплекса, входящий в определенное множество встроенных групп доступа и оперирующий с заданными наборами возможностей.

Каждая пользовательская роль связывается с набором разрешений. При создании пользователя и назначении ему роли пользователь становится обладателем набора разрешений роли.

В Комплексе есть встроенный набор пользовательских ролей, представленный в таблице ниже (Таблица 53. Пользовательские роли по умолчанию). Для роли `Администратор` указаны дополнительные функции, которые ему доступны помимо функций роли `Инженер`. Данные роли соответствуют разделению функций пользователей, предложенному в разделе «Разделение функций по администрированию» настоящего руководства.

Табл. 53. Пользовательские роли по умолчанию

ФУНКЦИОНАЛЬНАЯ ОБЛАСТЬ / РАЗДЕЛ ВЕБ-ИНТЕРФЕЙСА	ДЕЙСТВИЯ			
	АДМИНИСТРАТОР	ИНЖЕНЕР	ПРОСМОТР ВЕБ-ИНТЕРФЕЙСА	ПРОСМОТР ПАНЕЛИ МОНИТОРИНГА
Раздел **Мониторинг**	Просмотр виджетов и дашбордов, переход на страницы **Активы**, **Инциденты**, **Сессии**, **События** для получения подробной информации			
Пользователи	Создание, удаление, редактирование учетной записи и пароля	Просмотр списка учетных записей	Просмотр всех страниц Комплекса	–
Сканеры	Создание, редактирование, удаление	Запуск		
Поиск уязвимостей в базах CPE и CVE	Удаление результатов	Запуск		
Справочники OVAL (определения, группы, настройки) и проверки OVAL	Создание, удаление группы OVAL-определений; удаление OVAL-определений из группы	Добавление OVAL-определений в группу		
	Создание, редактирование, удаление настроек OVAL	Просмотр		
	Создание, редактирование, удаление скриптов OVAL	Просмотр		
Оповещения	Создание, редактирование, удаление	Просмотр		

Табл. 53. Пользовательские роли по умолчанию

ФУНКЦИОНАЛЬНАЯ ОБЛАСТЬ / РАЗДЕЛ ВЕБ-ИНТЕРФЕЙСА	ДЕЙСТВИЯ			
	АДМИНИСТРАТОР	ИНЖЕНЕР	ПРОСМОТР ВЕБ-ИНТЕРФЕЙСА	ПРОСМОТР ПАНЕЛИ МОНИТОРИНГА
Справочники	Импорт	Экспорт		
Служба корреляции	Запуск, перезапуск, остановка	Просмотр состояния		
Правила корреляции	Создание, редактирование, удаление, создание копии	Просмотр		
Схема корреляции	Создание, редактирование, удаление	Просмотр, проверка		
Служба обнаружения вторжений	Активация и деактивация			
Правила обнаружения вторжений	Создание, редактирование, импорт, удаление, активация и деактивация	Просмотр		
	Создание, редактирование, удаление исключений для правил	Просмотр исключений		
Правила сессий	Удаление	Просмотр, создание, редактирование, активация, деактивация		

Табл. 53. Пользовательские роли по умолчанию

ФУНКЦИОНАЛЬНАЯ ОБЛАСТЬ / РАЗДЕЛ ВЕБ-ИНТЕРФЕЙСА	ДЕЙСТВИЯ			
	АДМИНИСТРАТОР	ИНЖЕНЕР	ПРОСМОТР ВЕБ-ИНТЕРФЕЙСА	ПРОСМОТР ПАНЕЛИ МОНИТОРИНГА
Режим автоматического создания правил	Активация и деактивация			
Правила контроля тегов	Просмотр, создание, редактирование, удаление			
Режим регистрации событий техпроцесса	Активация и деактивация			
Активы	Удаление конфигурации	Настройка конфигурации; редактирование учетных данных актива; создание, изменение, удаление, экспорт и импорт; запуск поиска уязвимостей		
Источники	Создание, остановка, запуск, редактирование, удаление			
Инциденты и их статусы	Изменение параметров и удаление инцидента или группы инцидентов			
	Создание статуса	Просмотр списка статусов		
Индексы	Архивирование, удаление	Просмотр		
Задачи сбора данных	Импорт	Создание, редактирование, удаление, экспорт		

Табл. 53. Пользовательские роли по умолчанию

ФУНКЦИОНАЛЬНАЯ ОБЛАСТЬ / РАЗДЕЛ ВЕБ-ИНТЕРФЕЙСА	ДЕЙСТВИЯ			
	АДМИНИСТРАТОР	ИНЖЕНЕР	ПРОСМОТР ВЕБ-ИНТЕРФЕЙСА	ПРОСМОТР ПАНЕЛИ МОНИТОРИНГА
Сканирование сети	Запуск	Просмотр списка подсетей		
Сенсоры, иерархия	Управление сенсором	Перезапуск синхронизации		
События	Запуск текущего и ретроспективного анализа событий	Просмотр событий и создание запросов в экспертном режиме		
Карта сети	Просмотр соединений и активов			
Сессии	Создание и экспорт файла PCAP		Просмотр	
Пакеты	Создание и экспорт файла PCAP			
Файлы	Создание и экспорт архива с файлами			
Представление	Сохранение для всех пользователей	Настройка, редактирование, удаление, сохранение для текущего пользователя		
Отчет	Создание		—	
Репозитории	Управление репозиториями: • блокировка репозиториев • настройка исключения • проверка актуальности данных • создание версии проекта		Просмотр всех страниц Version Control Management	

Табл. 53. Пользовательские роли по умолчанию

ФУНКЦИОНАЛЬНАЯ ОБЛАСТЬ / РАЗДЕЛ ВЕБ-ИНТЕРФЕЙСА	ДЕЙСТВИЯ			
	АДМИНИСТРАТОР	ИНЖЕНЕР	ПРОСМОТР ВЕБ-ИНТЕРФЕЙСА	ПРОСМОТР ПАНЕЛИ МОНИТОРИНГА
	• загрузка версии проекта на сервер • скачивание новой версии Version Control Desktop App • открытие локального хранилища • удаление связи между локальным и серверным хранилищем (действие «Забыть проект») • отмена изменений			
	Управление репозиториями: • создание и редактирование • разблокировка любых репозиториев	Управление репозиториями: • разблокировка репозиториев, заблокированных текущим пользователем		
Заблокированные репозитории	Управление всеми заблокированными репозиториями: • редактирование репозиториев, заблокированных текущим пользователем • разблокировка репозиториев • удаление связи между локальным и серверным хранилищем • настройка исключения • отмена изменений	Управление заблокированными текущим пользователем репозиториями: • редактирование репозиториев • разблокировка репозиториев • настройка исключения • создание версии проекта • загрузка версии проекта на сервер • отмена изменений		

Табл. 53. Пользовательские роли по умолчанию

ФУНКЦИОНАЛЬНАЯ ОБЛАСТЬ / РАЗДЕЛ ВЕБ-ИНТЕРФЕЙСА	ДЕЙСТВИЯ			
	АДМИНИСТРАТОР	ИНЖЕНЕР	ПРОСМОТР ВЕБ-ИНТЕРФЕЙСА	ПРОСМОТР ПАНЕЛИ МОНИТОРИНГА
	• создание версии проекта • загрузка версии проекта на сервер			
Группа репозиториев	Создание, редактирование и удаление	—		

18.4.1. Управление учетными записями пользователей

В этом разделе:

- Создание локальной учетной записи
- Создание учетной записи службы каталогов
- Редактирование учетных записей пользователей

Веб-интерфейс Комплекса предоставляет возможность управления учетными записями пользователей. При создании пользователя и назначении ему роли пользователь станет обладать набором разрешений роли.

Перейдите на страницу **Администрирование** → **Пользователи** → **Пользователи**, чтобы просмотреть список учетных записей пользователей Комплекса.

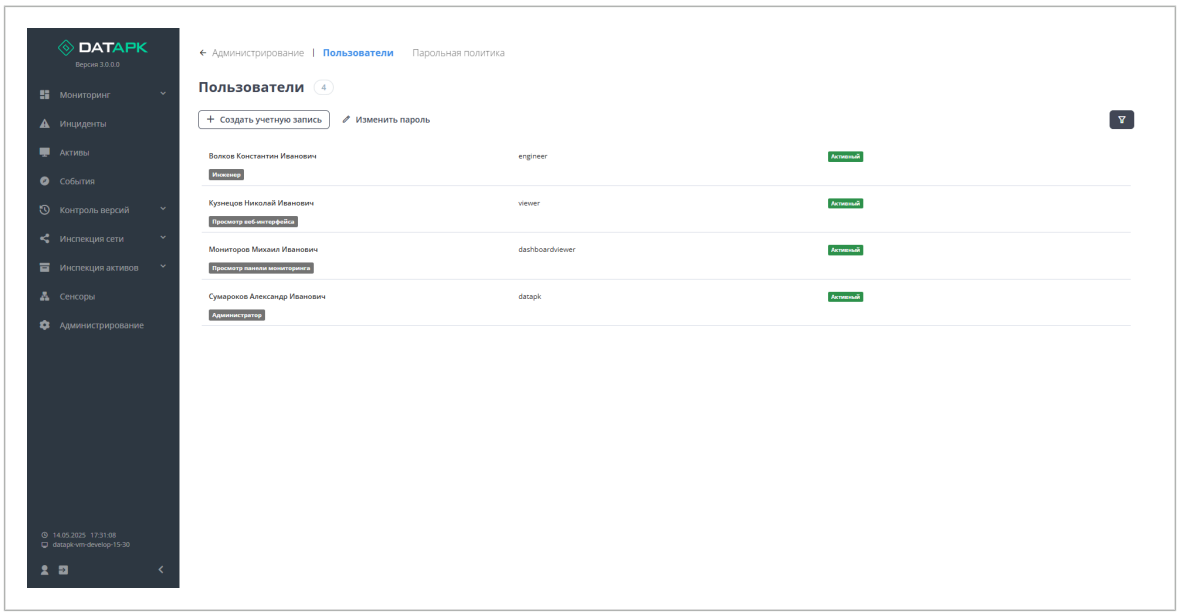


Рис. 445. Страница «Пользователи»

Для фильтрации списка учетных записей пользователей веб-интерфейс Комплекса предоставляет возможность использования предустановленных фильтров активности учетной записи.

В списке учетных записей выводится наименование, описание, роль пользователя, а также статус активности.

Предусмотрено создание локальных учетных записей и учетных записей службы каталогов. При выборе типа `Локальная` аутентификация происходит локально на Комплексе. При выборе типа `Служба каталогов` аутентификация происходит с использованием службы каталогов, а создаваемой учетной записи сопоставляется учетная запись из службы каталогов.

18.4.1.1. Создание локальной учетной записи

Для создания локальной учетной записи:

1. Перейдите на страницу **Администрирование → Пользователи**.
2. Нажмите кнопку **Создать учетную запись**.
3. В открывшемся окне **Создание учетной записи** задайте следующие параметры:
    - тип учетной записи — `Локальная`;
    - логин;
    - пароль;
    - фамилию, имя и отчество пользователя;

- роль;
- чекбокс Учетная запись **пользователя активна**;

> ОСТОРОЖНО:
>
> При отмене выбора данного параметра учетная запись пользователя будет заблокирована.

- при необходимости отметьте чекбокс **Сменить пароль при входе**.

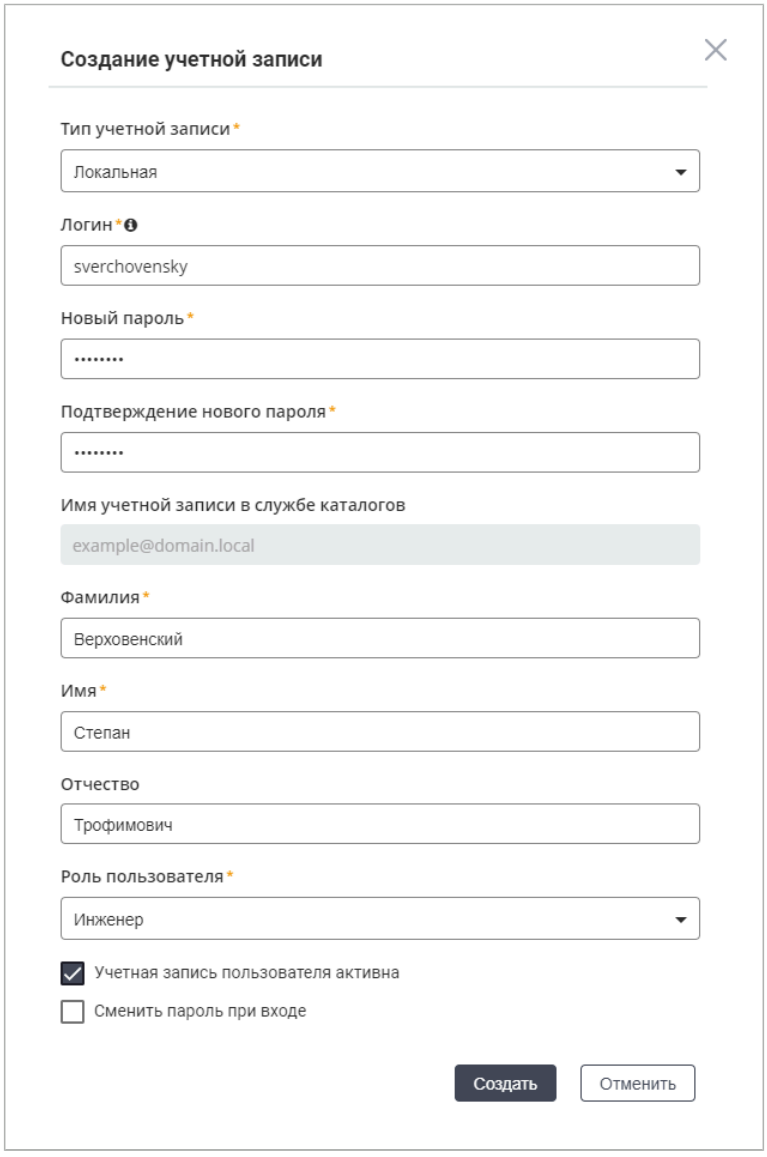


Рис. 446. Окно «Создание учетной записи» при создании локальный учетной записи

4. Нажмите кнопку **Создать** для подтверждения изменений.

18.4.1.2. Создание учетной записи службы каталогов

Для создания учетной записи службы каталогов:

1. Подключитесь к операционной системе Комплекса.
2. Перейдите в рабочую директорию Комплекса (по умолчанию путь к рабочей директории Комплекса — `/usr/share/udv/datapk`):

```
cd /usr/share/udv/datapk
```

3. Остановите работу сервисов следующей командой:

```
systemctl stop udv-* --all
```

4. Дождитесь остановки работы всех сервисов.
5. Для подключения по протоколу LDAPS добавьте в файл `manager.env` переменную `LDAP_TLS` и присвойте ей значение `true`.
6. Добавьте в конфигурационный файл `manager.env` переменную `LDAP_CONNECTION_STRING`:

```
LDAP_CONNECTION_STRING=[protocol]://[domain_or_IP-address]:[port]
```

где `[protocol]` — протокол для соединения с сервером, `[domain_or_IP-address]` — доменное имя или IP-адрес сервера службы каталогов, `[port]` — порт назначения (при необходимости).

> Подсказка:
>
> Если в вашей сети настроена служба DNS, разрешающая адреса внутри домена, то вы можете указать полное имя домена в качестве адреса для соединения со службой каталогов. В этом случае Комплекс будет перебирать все контроллеры домена, пока не найдет доступный.
>
> Например, для подключения по протоколу LDAPS с использованием доменного имени `udv.dev` через порт `636` значение переменных будет следующим:
>
> ```
> LDAP_TLS=true
> LDAP_CONNECTION_STRING=ldaps://udv.dev:636
> ```
>
> Для подключения по протоколу LDAPS с использованием IP-адреса `192.168.0.110` значение переменных будет следующим:
>
> ```
> LDAP_TLS=true
> LDAP_CONNECTION_STRING=ldaps://192.168.0.110
> ```

7. Запустить работу сервисов командой:

```
systemctl start udv-* --all
```

8. Дождитесь запуска работы всех сервисов.
9. Откройте веб-интерфейс Комплекса.
10. Перейдите на страницу **Администрирование → Пользователи**.
11. Нажмите кнопку **Создать учетную запись**.
12. В открывшемся окне **Создание учетной записи** задайте следующие параметры:
    - тип учетной записи — `Служба каталогов`;
    - логин;
    - имя учетной записи в службе каталогов в формате `[логин]@[доменное_имя_нижнего_уровня].[...].[доменное_имя_верхнего_уровня]`, где вместо `[...]` укажите промежуточные доменные имена, если доменных имен больше двух;
    - фамилию, имя, отчество пользователя;
    - роль;

- для изменения активности учетной записи выберите или отмените выбор параметра Учетная запись **пользователя активна**.

> Внимание:
>
> При отмене выбора данного параметра учетная запись пользователя будет заблокирована.

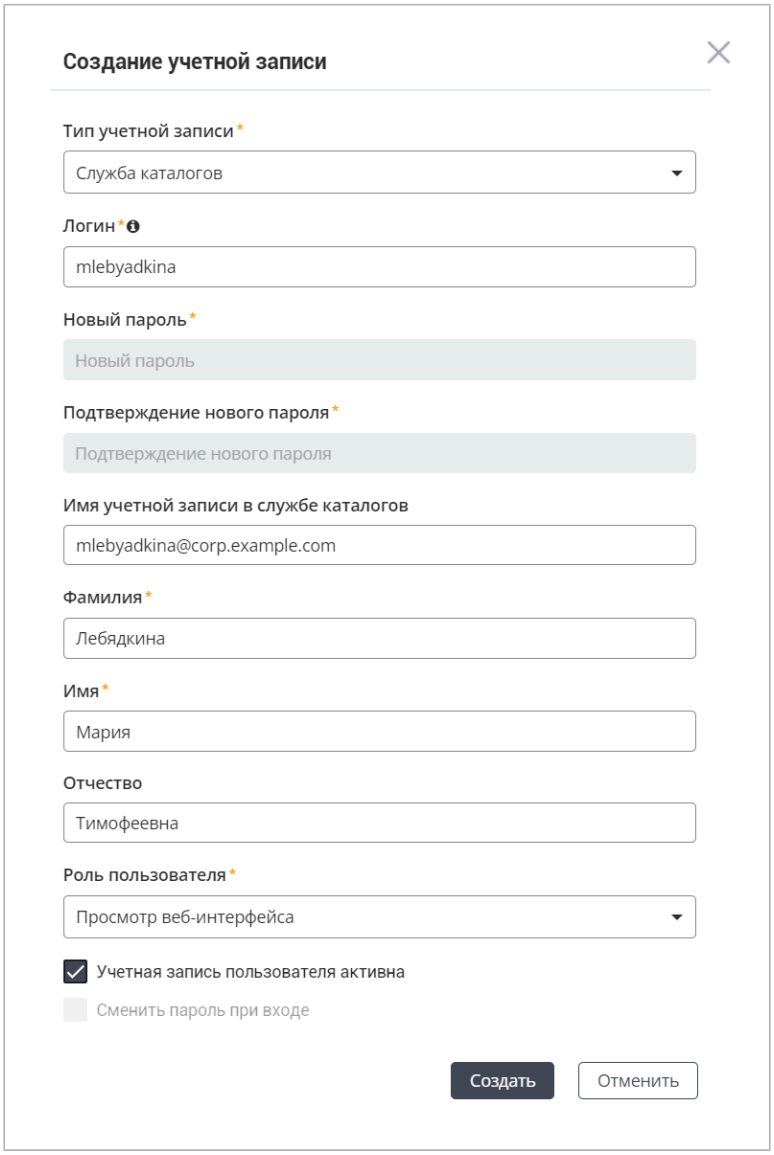


Рис. 447. Окно «Создание учетной записи» при создании учетной записи службы каталогов

13. Нажмите кнопку **Создать** для подтверждения изменений.

18.4.1.3. Редактирование учетных записей пользователей

Для редактирования учетных записей пользователей в интерфейсе Комплекса предусмотрены следующие возможности:

- Изменение учетных записей
- Смена пароля учетной записи
- Блокировка и удаление учетной записи

18.4.1.3.1. Изменение учетных записей

Для изменения настроек учетной записи пользователя:

1. Перейдите на страницу **Администрирование → Пользователи**.
2. Выберите учетную запись в списке пользователей и нажмите кнопку (**Редактировать учетную запись**).
   - **Результат шага:** появится окно **Редактирование учетной записи**.
3. Измените необходимые параметры учетной записи и нажмите кнопку **Сохранить**.

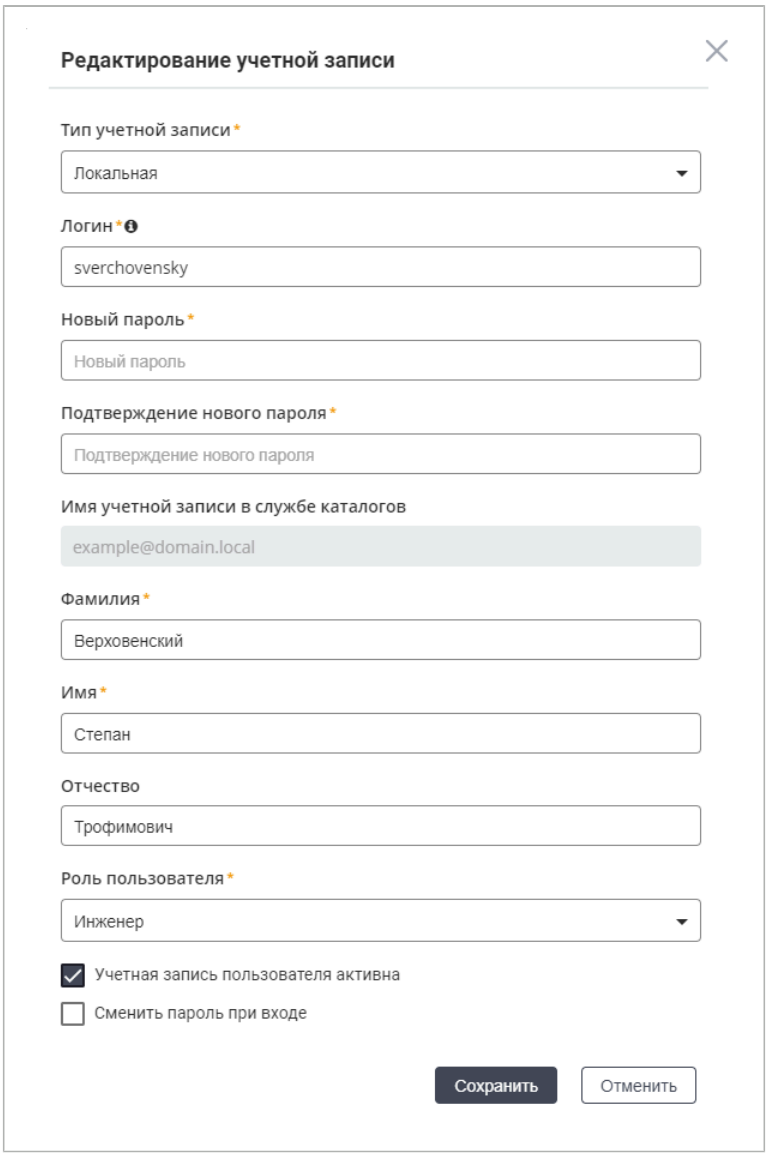


Рис. 448. Окно «Редактирование учетной записи»

4. Для применения изменений выполните повторный вход в веб-интерфейс Комплекса:
   a. Нажмите кнопку (**Выход**) в верхнем правом углу страницы веб-интерфейса.
   б. Выполните повторный вход в систему с измененной учетной записью.

18.4.1.3.2. Смена пароля учетной записи

Для смены пароля текущего пользователя:

1. Перейдите на страницу **Администрирование → Пользователи**.
2. Нажмите кнопку **Изменить пароль**.
   - **Результат шага:** появится окно **Изменение пароля учетной записи**.
3. Введите текущий пароль, новый пароль и подтверждение нового пароля.

> Внимание:
>
> Требования к паролю устанавливаются парольной политикой (подробнее см. в подразделе «Настройка парольной политики»). Парольная политика по умолчанию имеет следующие параметры:
>
> - длина пароля — не менее 6 и не более 128 символов;
> - содержание пароля — не менее одного буквенного и не менее одного числового символа;
> - пароль не должен содержать логин учетной записи.

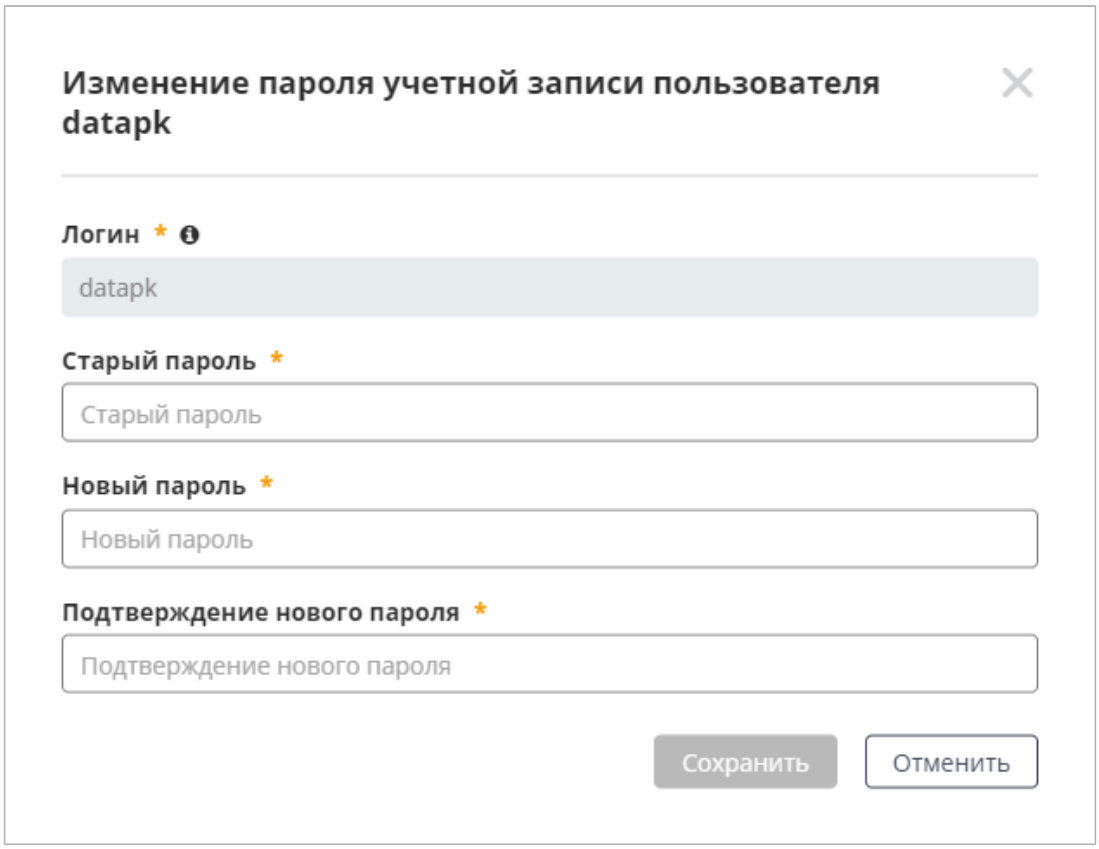


Рис. 449. Окно «Изменение пароля учетной записи»

4. Для применения изменений выполните повторный вход в веб-интерфейс Комплекса:
   a. Нажмите кнопку (**Выход**) в верхнем правом углу страницы веб-интерфейса.
   б. Выполните повторный вход в систему с измененной учетной записью.

18.4.1.3.3. Блокировка и удаление учетной записи

В случае обнаружения несанкционированных действий пользователя (подробнее см. раздел «Действия в случаях несанкционированного доступа к данным») или в иных случаях, интерфейс Комплекса предоставляет возможность бессрочно заблокировать или удалить учетную запись пользователя.

1. Перейдите на страницу **Администрирование → Пользователи**.
2. Для блокировки учетной записи пользователя Комплекса:
    a. Наведите курсор на запись, которую хотите заблокировать и нажмите кнопку (**Редактировать учетную запись**). Появится окно **Редактирование учетной записи**.
    б. Отмените выбор чекбокса **Учетная запись пользователя активна**.
3. Для удаления учетной записи пользователя Комплекса:

> Внимание:
>
> Удаленную учетную запись невозможно восстановить. Перед удалением убедитесь, что она больше не требуется.

    a. Наведите курсор на учетную запись, утратившую актуальность, и нажмите кнопку (**Удалить учетную запись**).
    б. Во всплывающем окне введите текст обоснования удаления и нажмите **Подтвердить**.

18.4.2. Настройка парольной политики

Для настройки единой парольной политики для всех пользователей:

1. Перейдите на страницу **Администрирование → Пользователи → Парольная политика**.

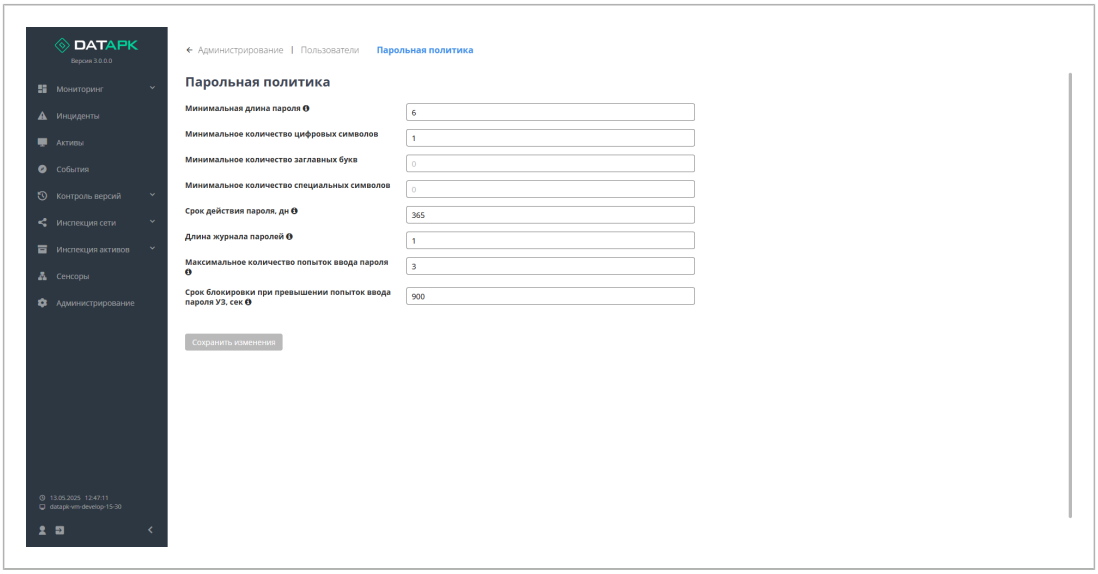


Рис. 450. Страница «Парольная политика»

2. Настройте следующие параметры парольной политики:

- общее минимальное количество символов, которое должен содержать пароль;

> Внимание:
>
> Доступен ввод значений в диапазоне от 6 до 128. Суммарное количество цифровых символов, заглавных букв и спецсимволов не должно превышать это значение.

- минимальное количество цифровых символов, которое должен содержать пароль;
- минимальное количество символов в верхнем регистре, которое должен содержать пароль;
- минимальное количество специальных символов, которое должен содержать пароль;
- максимальное количество дней, в течение которых может действовать пароль (во время или до окончания указанного срока действия пароля его необходимо будет заменить);

> Внимание:
>
> Доступен ввод значений в диапазоне от `0` до `998`. Чтобы сделать все пароли бессрочными, введите значение `0`.

- количество последних паролей пользователя, сохраняемых в Комплексе, которые нельзя будет использовать повторно;

> Внимание:
>
> Доступен ввод значений в диапазоне от `1` до `24`.

- максимальное количество попыток ввода пароля, после которых пользователь автоматически блокируется;

> Внимание:
>
> Доступен ввод значений в диапазоне от `0` до `12`. Чтобы отменить ограничение на количество попыток, введите значение `0`.

- срок автоматической блокировки пользователя при превышении попыток ввода пароля в секундах.

> Внимание:
>
> Чтобы отключить автоматическую блокировку, введите значение `0`.

3. Нажмите кнопку **Сохранить изменения**.

▸ **Результат шага:** в правом верхнем углу страницы появится уведомление: `Парольная политика успешно обновлена`. Настроенная парольная политика начнет действовать для новых паролей (при изменении текущих паролей существующих учетных записей и при создании новых учетных записей).

18.4.3. Отключение ограничения на количество сессий пользователей

Чтобы отключить ограничение на количество одновременных сессий пользователя в веб-интерфейсе Комплекса уровня Management:

1. Подключитесь к операционной системе Комплекса.
2. Перейдите в рабочую директорию Комплекса (по умолчанию `/usr/share/udv/datapk`):

   ```
   cd /usr/share/udv/datapk
   ```

3. Остановите работу сервисов следующей командой:

   ```
   systemctl stop udv-* --all
   ```

4. Дождитесь остановки работы всех сервисов.
5. Откройте конфигурационный файл `manager.env` в режиме редактирования.
6. Добавьте в файл `manager.env` переменную `LIMIT_USER_SESSIONS` и присвойте ей значение `false`:

   ```
   LIMIT_USER_SESSIONS=false
   ```

7. Сохраните и закройте файл `manager.env`.
8. Запустить работу сервисов командой:

   ```
   systemctl start udv-* --all
   ```

9. Дождитесь запуска работы всех сервисов.

18.5. Экспорт отдельных справочников

В качестве дополнительного способа создания резервных копий в веб-интерфейсе можно выгружать справочники объектов в файлы и сохранять их. В таблице ниже (Таблица 54. Ссылки на разделы документа с описанием экспорта объектов Комплекса) приведены ссылки на разделы с описанием выполнения резервных копий объектов Комплекса путем экспорта.

Табл. 54. Ссылки на разделы документа с описанием экспорта объектов Комплекса

НАИМЕНОВАНИЕ	ССЫЛКА	ФОРМАТ
Правила разбора событий	Экспорт правил разбора событий	`zip`
Правила обогащения событий	Экспорт правил обогащения событий	`zip`
Схема событий	Экспорт схемы событий	`zip`
Иерархия АСУ ТП	Экспорт справочника с классификаторами АСУ ТП	`json`
Иерархия меток активов	Экспорт меток	`json`
Группы активов (без активов)	Экспорт групп активов	`json`
Политика корреляции	Экспорт политики корреляции	`json`

Табл. 54. Ссылки на разделы документа с описанием экспорта объектов Комплекса

НАИМЕНОВАНИЕ	ССЫЛКА	ФОРМАТ
Сканеры в составе групп сканеров	Экспорт сканеров и их групп	`json`
Задачи сбора данных	Экспорт задач сбора данных	`json`
Статусы инцидентов	Экспорт статусов инцидентов	`json`
Правила службы обнаружения вторжений	Экспорт правил службы обнаружения вторжений	`json`
Группы OVAL-определений	Экспорт групп OVAL-определений	`json`
Скрипты OVAL	Экспорт скриптов OVAL	`json`
Настройки OVAL	Экспорт настроек OVAL	`json`
Источники событий	Экспорт источников событий	`json`
Сохраненные запросы, визуализации, панели мониторинга	Экспорт сохраненных объектов в экспертном режиме просмотра событий	`json`
Активы	Экспорт активов	`json`

Внимание:

Экспорт следующих справочников недоступен в веб-интерфейсе:

- справочники ПО и уязвимостей (CPE и CVE) и база сопоставления собранного сканерами ПО со справочником CPE. Экспорт этих справочников доступен только в операционной системе Комплекса путем копирования директории `/cve` вместе с содержимым (по умолчанию расположена в директории `/usr/share/udv/vulnerability-backend`);
- правила корреляции и схема корреляции — экспорт доступен только в составе политики корреляции;
- наборы сигнатур правил обнаружения вторжений в формате Suricata — экспорт доступен только в составе правил обнаружения вторжений;
- OVAL-определения — экспорт доступен только в составе групп OVAL-определений;
- учетные данные активов.

18.6. Диагностика состояния системы Комплекса

На странице **Администрирование** → **Диагностика** вы можете ознакомиться с графиками нагрузки компонентов системы, на которой функционирует текущий Комплекс.

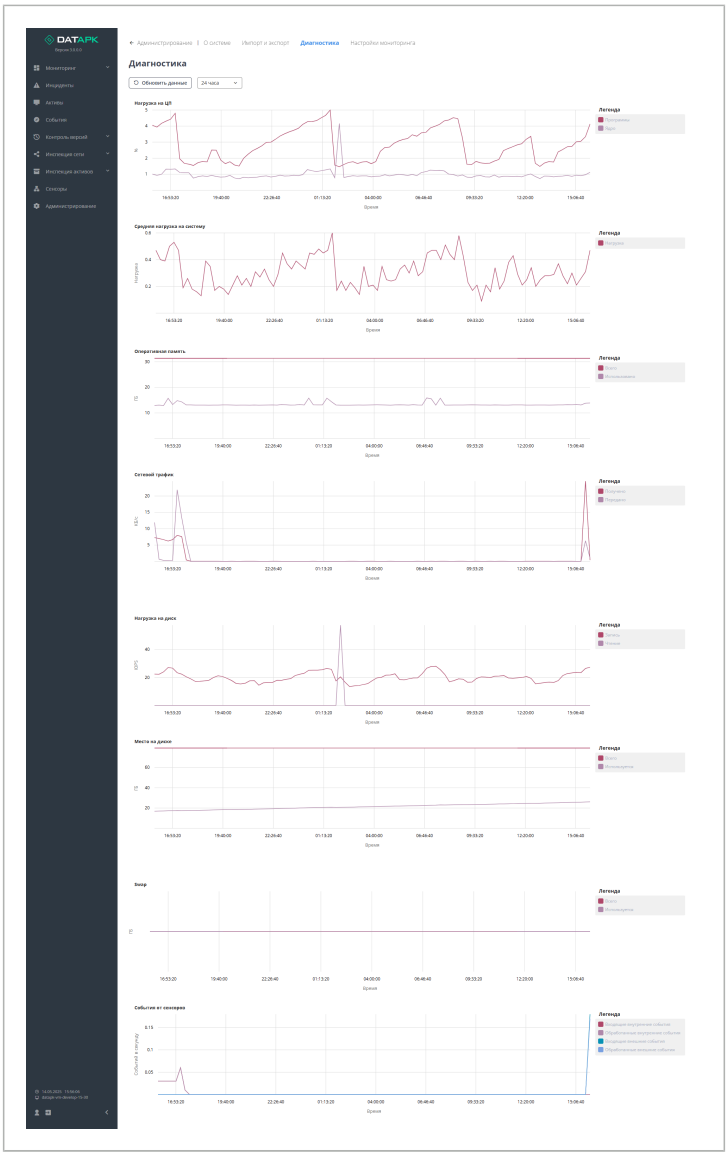


Рис. 451. Страница «Диагностика»

Для просмотра доступны следующие временные периоды:

- `1 час`;
- `24 часа`;
- `7 дней`.

Для выбора периода воспользуйтесь выпадающим списком в верхней части страницы и нажмите **Обновить данные.**

На странице представлены следующие графики:

- **Нагрузка на ЦП** — показывает загруженность центрального процесса за выбранное время. На графике отображаются две линии: программы и ядро. Таким образом можно точно определить, что нагружает систему.

  > Подсказка:
  >
  > При превышении заданного в переменной `MAX_CPU_LOAD_CONSUMED_PERCENTAGE` лимита, а также последующей нормализации значения нагрузки на центральный процессор будет получено соответствующее событие.

- **Средняя нагрузка на систему** — сводный коэффициент нагрузки на основные компоненты.

  > Подсказка:
  >
  > При превышении заданного в переменной `DATAPK_MAX_LA` лимита, а также последующей нормализации значения средней нагрузки (LA) будет получено соответствующее событие.

- **Оперативная память** — график показывает общее доступное количество оперативной памяти и занятое количество.

  > Подсказка:
  >
  > При превышении заданного в переменной `DATAPK_MAX_RAM_PERCENTAGE_CONSUMED` лимита оперативной памяти будет получено соответствующее событие.

- **Сетевой трафик** — отображает все сетевые интерфейсы и объем данных, которые они передают.
- **Нагрузка на диск** — показывает то, насколько занят жесткий диск во времени. На графике присутствуют две линии: чтение и запись.
- **Место на диске** — отображает занятое пространство относительно всего доступного для каждого диска.

  > Подсказка:
  >
  > При превышении заданного в переменной `MAX_DISK_SPACE_CONSUMED_PERCENTAGE` лимита, а также последующей нормализации значения нагрузки на диск будет получено соответствующее событие.

- **Swap** — график отражает место на жестком диске, которое используется для «выгрузки» в него неиспользуемых страниц из оперативной памяти.
- **События от сенсоров** — отображает количество внешних и внутренних событий, которые поступают с сенсоров.

Справа от каждого графика можно увидеть легенду, где указано, какие параметры используются на этом графике, и цвет их линий.

18.7. Диагностика состояния сенсора

На странице **Сенсоры** вы можете ознакомиться с графиками нагрузки сенсоров, действующих на текущем Комплексе и доступных в списке на этой странице.

Рис. 452. Страница «Сенсоры»

Для просмотра доступны следующие временные периоды:

- `1 час`;
- `24 часа`;
- `7 дней`.

Для выбора периода воспользуйтесь выпадающим списком в верхней части страницы и нажмите **Обновить данные.**

На странице представлены следующие графики:

- **Нагрузка на ЦП** — показывает загруженность центрального процесса за выбранное время. На графике отображаются две линии: программы и ядро. Таким образом можно точно определить, что нагружает систему.
- **Средняя нагрузка на систему** — сводный коэффициент нагрузки на основные компоненты.
- **Оперативная память** — график показывает общее доступное количество оперативной памяти и занятое количество.
- **Сетевой трафик** — отображает все сетевые интерфейсы и объем данных, которые они передают.
- **Нагрузка на диск** — показывает то, насколько занят жесткий диск во времени. На графике присутствуют две линии: чтение и запись.
- **Место на диске** — отображает занятое пространство относительно всего доступного для каждого диска.
- **Swap** — график отражает место на жестком диске, которое используется для «выгрузки» в него неиспользуемых страниц из оперативной памяти.
- **События от сенсора к Комплексу** — отображает количество внешних и внутренних событий, которые поступают с сенсора на Комплекс.
- **Обработанные события** — отображает количество событий, которые поступили с сенсора и были обработаны Комплексом.
- **Обработанные сетевые пакеты** — отображает количество сетевых пакетов, которые были обработаны Комплексом.

При наведении на график можно увидеть легенду, где указано, какие параметры используются на этом графике, и цвет их линий.

18.8. Удаление сенсора

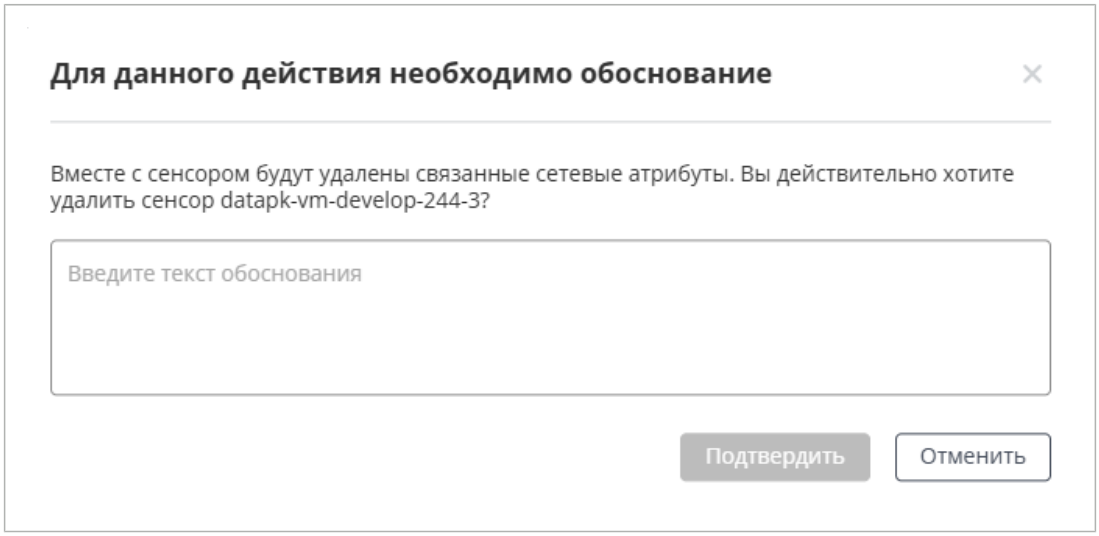
Для удаления сенсора и связанной с ним информации из Комплекса:

1. Перейдите на страницу **Сенсоры** веб-интерфейса Комплекса уровня Management.
2. Выберите сенсор из списка.
   - **Результат шага:** справа откроется карточка выбранного сенсора.
3. В открывшейся панели нажмите внизу кнопку **Удалить сенсор**.
   - **Результат шага:** Появится окно с предупреждением: `Вместе с сенсором будут удалены связанные сетевые атрибуты. Вы действительно хотите удалить сенсор [имя]?`

4. ОСТОРОЖНО:

   - При удалении сенсора будут удалены связанные с ним данные: сетевые атрибуты активов, конфигурации, статусы сбора.
   - Если при удалении связанных сетевых атрибутов актива будет удален его интерфейс сбора данных, то новым интерфейсом сбора данных станет случайный из оставшихся сетевых атрибутов.
   - Актив не будет удален, если у него не останется ни одного сетевого атрибута после удаления сенсора. При необходимости измените или удалите такие активы вручную.

   Введите обоснование удаления сенсора и нажмите кнопку **Подтвердить**.



   - **Результат шага:** сенсор и связанные с ним данные будут удалены из Комплекса уровня Management.

Что дальше: Если необходимо подключить сенсор к другому Комплексу уровня Management, выполните шаги 6-12 инструкции «Подключение сенсора к другому Комплексу уровня Management» Руководства по внедрению и поддержке.

19. Интеграция Комплекса с другими системами

В этом разделе:

1. **Интеграция Комплекса с ПО InfoWatch ARMA Industrial Firewall**
2. **Работа с REST API Комплекса**

В этом разделе:

- Интеграция Комплекса с ПО InfoWatch ARMA Industrial Firewall
- Работа с REST API Комплекса

19.1. Интеграция Комплекса с ПО InfoWatch ARMA Industrial Firewall

InfoWatch ARMA Industrial Firewall (ARMA FW) представляет собой промышленный межсетевой экран нового поколения, который обеспечивает обнаружение и блокировку атак на промышленные сети, а также защиту от несанкционированного доступа. Подробная информация о решении ARMA FW представлена на сайте производителя.

Интеграция DATAPK Industrial Kit с ARMA FW реализует следующие возможности:

- Сбор, обработка и отображение событий безопасности, генерируемых решением ARMA FW, средствами DATAPK Industrial Kit, например:
  - события аудита;
  - события системы обнаружения вторжений;
  - события межсетевого экрана;
  - события планировщика заданий;
  - события работы внутренних служб.
- Сбор, обработка и контроль конфигураций ARMA FW средствами DATAPK Industrial Kit, например:
  - правила межсетевого экрана;
  - системные настройки;
  - системные переменные;
  - учетные записи пользователей;
  - группы пользователей;
  - сетевые интерфейсы;
  - версия ОС;
  - установленное ПО;
  - статистическая информация по сетевым протоколам.
- Контроль сетевого трафика между ARMA FW и компонентами DATAPK Industrial Kit.

19.1.1. Предварительная настройка взаимодействия с ПО InfoWatch ARMA Industrial Firewall

Для сбора событий и конфигураций необходимо предварительно настроить взаимодействие Комплекса с ARMA FW[3].

3. Используемая версия ARMA FW — 3.10.2

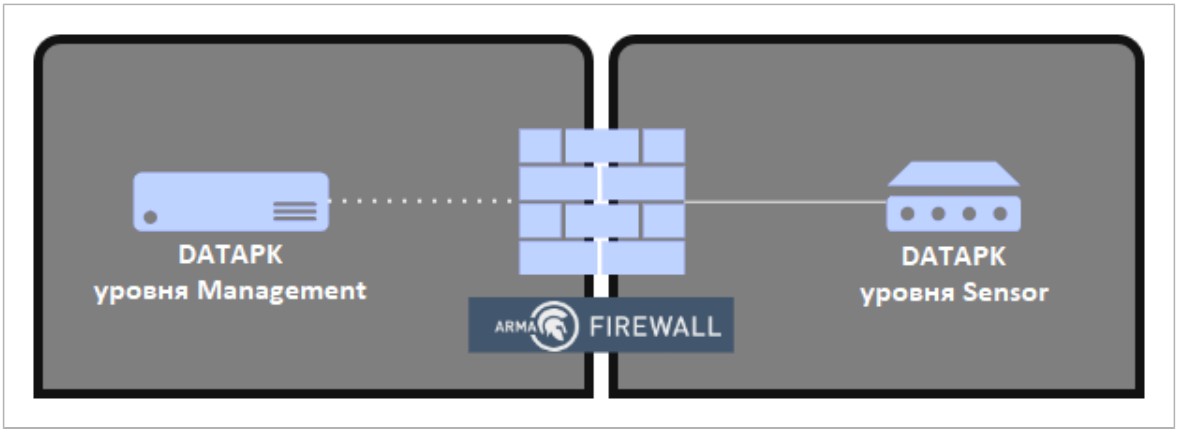


Рис. 453. Схема взаимодействия Комплекса с ARMA FW

Для настройки взаимодействия:

1. Разрешите на ARMA FW взаимодействие от Комплекса уровня Sensor до Комплекса уровня Management по следующим TCP-портам:
   - 15673;
   - 16379;
   - 19091.

   > Подсказка:
   >
   > Подробнее о настройке взаимодействия см. в документе «Руководство пользователя по эксплуатации» для ARMA FW в разделе «Настройка правил МЭ».

2. Перейдите на страницу **Сенсоры** веб-интерфейса Комплекса уровня Management и убедитесь, что сенсор доступен.

   > Подсказка:
   >
   > Подробнее о проверке доступности сенсора см. в разделе «Проверка работоспособности системы передачи данных по иерархии».

3. Настройте обнаружение ARMA FW среди ОЗ Комплекса. Для этого в веб-интерфейсе Комплекса:
   a. Перейдите на страницу **Сенсоры** и настройте на сенсоре контролируемую сеть ARMA FW.

      > Подсказка:
      >
      > Подробнее о настройке контролируемой сети см. в разделе «Настройка контролируемой сети».

   б. Перейдите на страницу **Активы** и выполните поиск ARMA FW по его IP-адресу.

   в. Нажмите на найденный ОЗ, чтобы перейти в его **карточку**.

г. В блоке **Описание ОЗ** отредактируйте наименование ОЗ, назначьте ему тип и сохраните изменения.

> Подсказка:
>
> Подробнее о настройке ОЗ см. в разделе «Редактирование актива».

- **Результат шага:** ARMA FW будет отображаться в списке известных ОЗ на странице **Активы**.

19.1.2. Сбор событий ПО InfoWatch ARMA Industrial Firewall

Перед выполнением: Перед началом настройки запросите у разработчика Комплекса конфигурационный файл `12-syslog-event-filter.conf`, содержащий фильтры для нормализации событий от ARMA FW.

Для настройки сбора событий:

1. Разрешите отправку Syslog-событий с ARMA FW на Комплекс уровня Sensor. Для этого на ARMA FW задайте следующие настройки экспорта событий:
   - транспортный протокол — UDP(4);
   - формат сообщения — Syslog;
   - имя хоста — IP-адрес Комплекса уровня Sensor;
   - порт — 514;
   - установите чекбокс **Включен**;
   - при необходимости введите описание получателя.

> Подсказка:
>
> Подробнее о настройке отправки Syslog-событий см. в документе «Руководство пользователя по эксплуатации» ARMA FW в разделе «Настройка экспорта событий syslog».

2. На Комплексе уровня Management создайте источник Syslog для ОЗ ARMA FW.

> Подсказка:
>
> Подробнее о создании источников см. в разделе «Создание источника событий».

3. Замените в Комплексе уровня Management конфигурационный файл `12-syslog-event-filter.conf` на новый, полученный ранее от разработчика Комплекса. Для этого:
   а. Подключитесь к Комплексу по протоколам SCP/SFTP с помощью FTP-клиента.
   б. Скопируйте с заменой конфигурационный файл `12-syslog-event-filter.conf`, полученный ранее от разработчика Комплекса, в директорию `/opt/datapk/logstash/config/plugins/pipeline`
   в. Авторизуйтесь в терминале Комплекса под логином `root`
   г. Перезапустите сервис `udv-logstash` командой:

```
systemctl restart udv-logstash
```

4. Перейдите в раздел **События** или **События → Экспертный режим** веб-интерфейса Комплекса.

5. Отфильтруйте события по типу `event_type = armaif_event`

> Подсказка:
>
> Подробнее о категориях событий ARMA FW, доступных для просмотра по фильтру `category` в **экспертном режиме просмотра событий**, см. в разделе «События ARMA FW».

- **Результат шага:** появятся события, отфильтрованные по типу `armaif_event`.

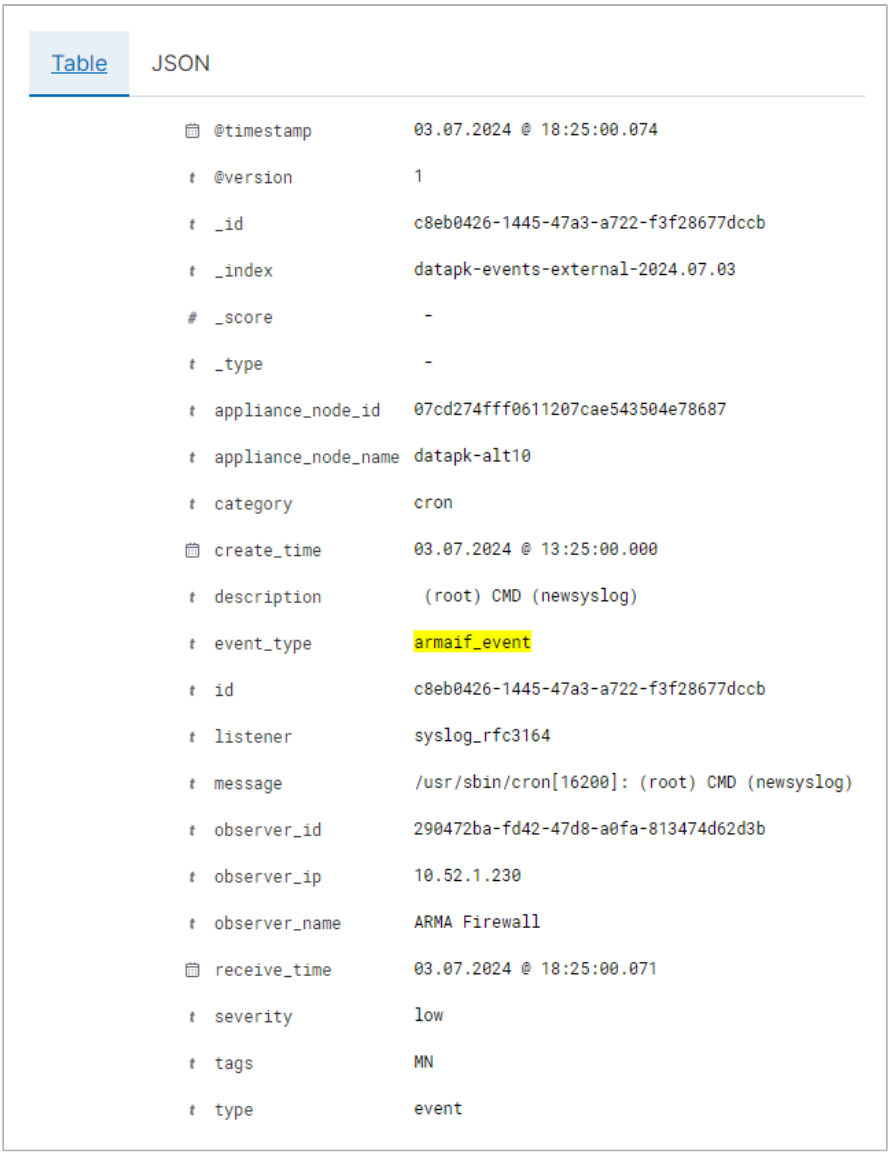


Рис. 454. Пример события с типом armaif_event на странице События → Экспертный режим

19.1.3. Сбор конфигураций ПО InfoWatch ARMA Industrial Firewall по протоколу SSH

Перед выполнением: Перед началом настройки запросите у разработчика Комплекса набор сканеров сбора данных с ARMA FW по протоколу SSH.

Для настройки сбора конфигураций ARMA FW по протоколу SSH:

1. Активируйте сервис SSH в ARMA FW.

   > Подсказка:
   >
   > Подробнее об активации сервиса SSH см. в документе «Руководство пользователя по эксплуатации» ARMA FW в разделе «SSH-сервер».

2. Добавьте в ARMA FW следующее правило межсетевого экрана:

   ```
   pass IPv4 tcp keep state any [IP-адрес Комплекса уровня Sensor] \
   any [IP-адрес ARMA FW] 22
   ```

   > Подсказка:
   >
   > Подробнее о добавлении правил межсетевого экрана см. в документе «Руководство пользователя по эксплуатации» ARMA FW в разделе «Настройка правил МЭ».

3. Создайте в ARMA FW пользовательскую учетную запись. При создании установите чекбокс «Доступ к консольному интерфейсу».

   > Подсказка:
   >
   > Подробнее о добавлении правил межсетевого экрана см. в документе «Руководство пользователя по эксплуатации» ARMA FW в разделе «Создание пользовательских учетных записей и их привилегий».

4. Добавьте созданную учетную запись ARMA FW в группу, которая была указана в поле **Группа логина** при активации SSH на шаге 1.

   > Подсказка:
   >
   > Подробнее о добавлении учетных записей в группы см. в документе «Руководство пользователя по эксплуатации» ARMA FW в разделе «Назначение привилегий пользовательской УЗ».

5. На Комплексе уровня Management перейдите на страницу **Администрирование** → **Настройка активов** → **Учетные данные** и добавьте учетные данные для ОЗ ARMA FW со следующими параметрами:
   - логин и пароль должны соответствовать учетной записи, созданной в ARMA FW на шаге 3;
   - тег — `admin`

   > Подсказка:
   >
   > Подробнее о создании и добавлении учетных данных для ОЗ см. в разделе «Добавление учетных данных актива».

6. На странице **Активы** найдите ОЗ ARMA FW, перейдите в карточку ОЗ и в блоке **Учетные данные** назначьте ему созданные учетные данные с тегом `admin`.

> Подсказка:
>
> Подробнее о настройке ОЗ для сбора данных см. в разделе «Настройка активов для сбора данных».

7. Перейдите на страницу **Администрирование → Основные настройки → Импорт и экспорт** и импортируйте сканеры сбора данных, полученные от разработчика Комплекса.

> Подсказка:
>
> Подробнее об импорте сканеров см. в разделе «Импорт сканеров и их групп».

8. Запустите необходимые сканеры одним из следующих способов:
   - запустите сканер однократно на странице **Администрирование → Инспекция активов → Сканеры**;
   - создайте задачу сбора данных для периодического запуска сканера или группы сканеров на странице **Инспекция активов → Задачи сбора**. Подробнее о создании задач сбора данных см. в разделе «Создание задачи сбора данных».
9. Убедитесь, что сбор данных выполнен успешно, на странице **Инспекция активов → Задачи сбора**.
10. Перейдите в раздел **Инспекция активов → Конфигурации** для просмотра результатов сбора данных в виде конфигураций, полученных с ARMA FW по SSH.

№	Действие	Протокол	Состояние	Направление	IP источника	Порт источника	IP получателя	Порт получателя	Создатель	Последнее обновление	Журналирование
1	pass	IPv4 tcp	keep state	in	10.52.2.200	any	10.52.1.231	15673	root@10.41.80.90	root@10.199.2.11	1
2	pass	IPv4 tcp	keep state	in	10.52.2.200	any	10.52.1.231	16379	root@10.199.2.11	root@10.199.2.11	None
3	pass	IPv4 tcp	keep state	in	10.52.2.200	any	10.52.1.231	19091	root@10.199.2.11	root@10.199.2.11	None
4	pass	IPv4 udp	keep state	in	10.52.2.10	any	10.52.2.200	514	root@10.199.1.0	root@10.199.1.80	None
5	pass	IPv4 tcp	keep state	any	10.52.2.200	any	10.52.2.10	22	root@10.199.1.80	root@10.199.1.80	None
6	pass	IPv4 udp	keep state	any	10.52.2.200	any	10.52.2.10	161-162	root@10.199.1.80	root@10.199.0.217	1
7	block	IPv4 any	keep state	in	10.52.2.0/24	any	any	any	root@10.199.0.128	root@10.199.2.247	None
8	block	IPv4 any	keep state	in	any	any	10.52.2.0/24	any	root@10.199.0.128	root@10.199.2.247	None
9	pass	IPv4 any	None	None	LAN сеть	any	any	any	None	None	None
10	pass	IPv6 any	None	None	LAN сеть	any	any	any	None	None	None
11	pass	IPv4 udp	keep state	in	any	any	Этот межсетево...	161	root@10.41.56.91	root@10.41.56.91	None
12	pass	IPv4 icmp	keep state	in	any	any	Этот межсетево...	any	root@10.41.56.91	root@10.41.56.91	None

Рис. 455. Результат выполнения задачи сбора конфигураций по протоколу SSH

19.1.4. Сбор конфигураций ПО InfoWatch ARMA Industrial Firewall по протоколу SNMP

Перед выполнением: Перед началом настройки запросите у разработчика Комплекса следующие файлы:

- набор сканеров сбора данных с ARMA FW по протоколу SNMP.
- MIB-словарь для сбора данных с ARMA FW по протоколу SNMP.

Для настройки сбора конфигураций ARMA FW по протоколу SNMP:

1. В ARMA FW активируйте сервис SNMP и создайте нового пользователя для подключения по SNMP.

   > Подсказка:
   >
   > Подробнее об активации сервиса SNMP и создаии пользователя SNMP см. в документе «Руководство пользователя по эксплуатации» ARMA FW в разделе «SNMP».

2. Добавьте в ARMA FW следующие правила межсетевого экрана:

   ```
   pass IPv4 udp keep state any [IP-адрес Комплекса уровня Sensor] \
   any [IP-адрес ARMA FW] 161
   ```

   ```
   pass IPv4 udp keep state in any any (self) 161
   ```

   > Подсказка:
   >
   > Подробнее о добавлении правил межсетевого экрана см. в документе «Руководство пользователя по эксплуатации» ARMA FW в разделе «Настройка правил МЭ».

3. Скопируйте на Комплекс уровня Sensor MIB-словарь для ARMA FW, полученный ранее от разработчика Комплекса. Для этого:
   a. Подключитесь к Комплексу уровня Sensor по протоколам SCP/SFTP с помощью FTP-клиента.
   б. Поместите MIB-словарь, полученный ранее от разработчика Комплекса, в директорию `/var/backups/snmp_mibs`
4. На Комплексе уровня Management перейдите на страницу **Администрирование → Настройка активов → Учетные данные** и добавьте учетные данные для ОЗ ARMA FW со следующими параметрами:
   - логин и пароль должны соответствовать имени пользователя SNMP и его паролю, настроенным в ARMA FW на шаге 1;
   - тег — `snmp3`

   > Подсказка:
   >
   > Подробнее о создании и добавлении учетных данных для ОЗ см. в разделе «Добавление учетных данных актива».

5. На странице **Активы** найдите ОЗ ARMA FW, перейдите в карточку ОЗ и в блоке **Учетные данные** назначьте ему созданные учетные данные с тегом `snmp3`.

   > Подсказка:
   >
   > Подробнее о настройке ОЗ для сбора данных см. в разделе «Настройка активов для сбора данных».

6. Перейдите на страницу **Администрирование → Основные настройки → Импорт и экспорт** и импортируйте сканеры сбора данных, полученные от разработчика Комплекса.

> Подсказка:
>
> Подробнее см. в разделе «Импорт сканеров и их групп».

7. Запустите необходимые сканеры одним из следующих способов:
   - запустите сканер однократно на странице **Администрирование** → **Инспекция активов** → **Сканеры**;
   - создайте задачу сбора данных для периодического запуска сканера или группы сканеров на странице **Инспекция активов** → **Задачи сбора**. Подробнее о создании задач сбора данных см. в разделе «Создание задачи сбора данных».
8. Убедитесь, что сбор данных выполнен успешно, на странице **Инспекция активов** → **Задачи сбора**.
9. Перейдите в раздел **Инспекция активов** → **Конфигурации** для просмотра результатов сбора данных в виде конфигураций, полученных с ARMA FW по SNMPv3.

Индекс	Описание	Тип	Максимальный размер пакета	Физический адрес	Статус
1	igb0	ethernetCsmacd	1500	6c:b3:11:39:fc:fc	up
2	igb1	ethernetCsmacd	1500	6c:b3:11:39:fc:fd	up
3	igb2	ethernetCsmacd	1500	6c:b3:11:39:fc:fe	down
4	igb3	ethernetCsmacd	1500	6c:b3:11:39:fc:ff	up
5	igb4	ethernetCsmacd	1500	6c:b3:11:39:c8:34	up
6	igb5	ethernetCsmacd	1500	6c:b3:11:39:c8:35	down
7	igb6	ethernetCsmacd	1500	6c:b3:11:39:c8:36	down
8	igb7	ethernetCsmacd	1500	6c:b3:11:39:c8:37	down
9	bge0	ethernetCsmacd	1500	3c:ec:ef:72:a4:22	down
10	bge1	ethernetCsmacd	1500	3c:ec:ef:72:a4:23	down
11	enc0	wwanPP2	1536		down
12	lo0	softwareLoopback	16384		up
13	pfsync0	ilan	1500		down
14	pflog0	ifPwType	33160		down
15	ue0	ethernetCsmacd	1500	be:3a:f2:b6:05:9f	down

Рис. 456. Результат выполнения задачи сбора конфигурационных данных по протоколу SNMP

19.2. Работа с REST API Комплекса

В этом разделе:

- Установка Swagger UI
- Конечные точки REST API Комплекса

19.2.1. Установка Swagger UI

Swagger UI предназначен для проектирования, документирования и тестирования API в средах разработки, тестирования и промышленной эксплуатации.

Swagger UI корректно функционирует при использовании в средах, соответствующих следующим требованиям:

- поддерживаемые операционные системы: Windows, Linux, macOS;
- доступ к сети Интернет для взаимодействия с API-серверами;
- совместимость с веб-браузерами (Chrome, Firefox, Edge, Safari) при работе с пользовательским интерфейсом;
- наличие среды выполнения для языков программирования.

19.2.1.1. Установка Swagger UI

Для установки Swagger UI:

1. Войдите в терминал Комплекса под учетной записью `root`.
2. Выполните команду для установки и запуска сервиса `udv-swagger-ui`:

   ```
   apt-get install udv-swagger-ui && systemctl start udv-swagger-ui.service
   ```

3. Перезапустите сервис `udv-nginx` командой:

   ```
   systemctl restart udv-nginx.service
   ```

4. Введите в адресной строке браузера следующий адрес:

   ```
   https://[IP-адрес Комплекса]/api/
   ```

   - **Результат шага:** В браузере будет отображаться актуальная спецификация REST API Комплекса.

19.2.1.2. Авторизация в Swagger UI

Перед выполнением: Авторизация в Swagger UI выполняется в два этапа:

- первый этап — авторизация с помощью логина и пароля Комплекса;
- второй этап — получение токена доступа к Swagger UI.

Перед авторизацией в Swagger UI убедитесь, что на Комплексе установлен и запущен сервис `udv-swagger-ui`.

19.2.1.2.1. Авторизация с помощью логина и пароля Комплекса

Для авторизации с помощью логина и пароля:

1. Введите в адресной строке браузера следующий адрес:

   ```
   https://[IP-адрес Комплекса]/api/
   ```

   - **Результат шага:** В браузере будет отображаться спецификация REST API Комплекса.
2. Нажмите кнопку **Authorize**.
   - **Результат шага:** В браузере будет отображаться окно авторизации в Swagger UI.

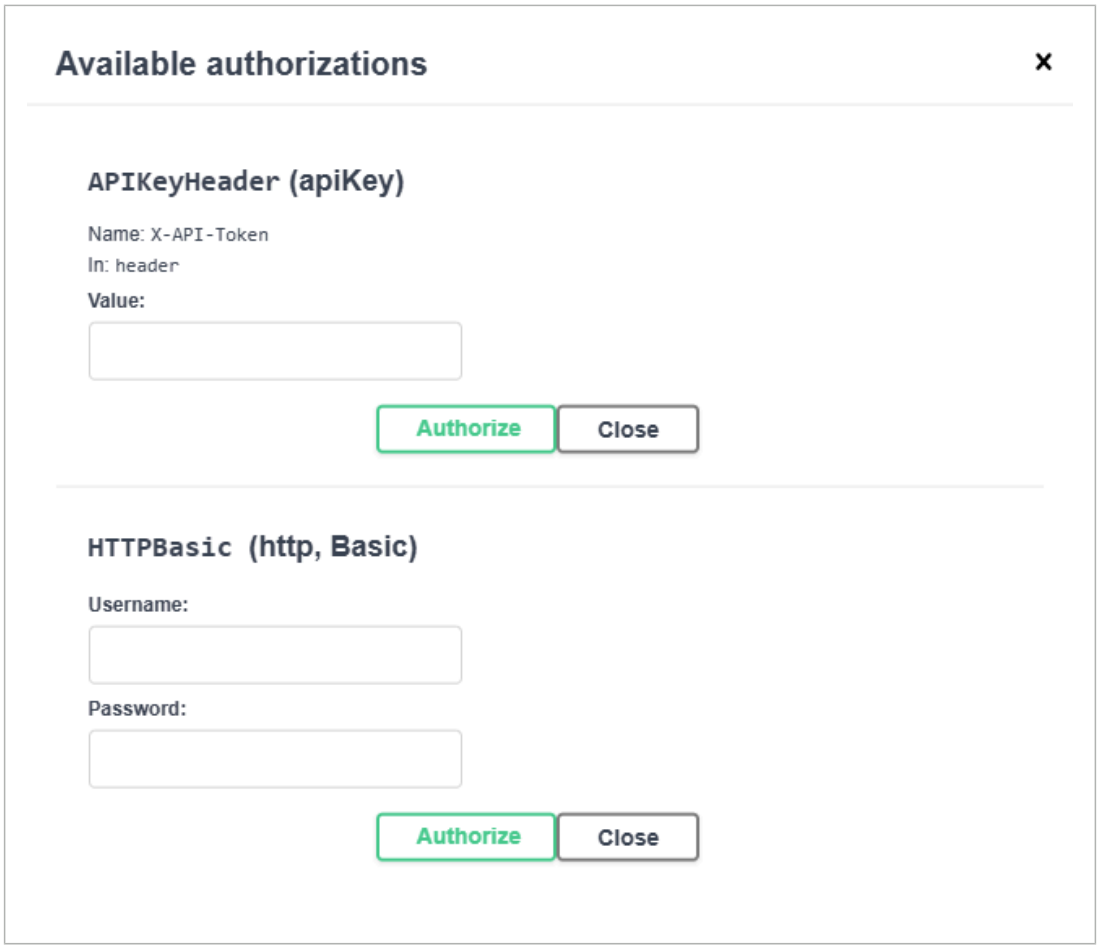


Рис. 457. Окно авторизации в Swagger UI

3. Введите логин и пароль для авторизации в Комплексе в блоке **HTTPBasic**.
4. Нажмите кнопку **Authorize**, затем нажмите кнопку **Close**.
   - **Результат шага:** Логин и пароль Комплекса успешно введены.

19.2.1.2.2. Получение токена доступа к Swagger UI

Для получения токена доступа:

1. На странице спецификации выберите конечную точку **Get Access Token**.
2. В развернутом окне нажмите кнопку **Try it out**, затем нажмите кнопку **Execute**.
   - **Результат шага:** В блоке **Response body** будет отображаться токен доступа (`access_token`).
3. Скопируйте токен доступа и вставьте его в поле **Value** в блоке **APIKeyHeader**.
4. Нажмите кнопку **Authorize**, затем нажмите кнопку **Close**.
   - **Результат шага:** Авторизация в Swagger UI будет успешно завершена.

19.2.1.2.3. Отзыв токена доступа к Swagger UI

Для отзыва токена доступа:

1. На странице спецификации выберите конечную точку **Revoke Access Token**.
2. В развернутом окне нажмите кнопку **Try it out**, затем нажмите кнопку **Execute**.
   - **Результат шага:** Токен доступа к Swagger UI будет успешно отозван. При попытке ввода отозванного токена будет отображаться ошибка авторизации.

19.2.2. Конечные точки REST API Комплекса

В этом разделе описываются конечные точки, с помощью которых выполняются следующие действия:

- получение информации обо всех активах или определенном активе по его идентификатору;
- получение информации о Комплексе;
- получение информации о типах активов;
- получение информации о сетевых интерфейсах;
- получение информации об инцидентах, зарегистрированных Комплексом, или определенном инциденте;
- получение информации о статусах инцидентов;
- обновление статуса определенного инцидента;
- получение сетевой информации о Комплексе;
- получение информации обо всех конфигурациях или определенной конфигурации;
- установка конфигурации в качестве эталонной;
- получение списка установленного ПО;
- получение информации о сенсорах;
- получение информации о контролируемых сетях всех подключенных сенсоров или определенного сенсора по его идентификатору;
- получение информации о сетевых соединениях;
- получение списка протоколов из сетевого трафика;
- получение списка правил сессий;
- получение правил контроля тегов;
- получение списка сканеров;
- получение информации об определенном сканере по его идентификатору;
- получение списка OVAL-проверок;
- получение информации об определенной OVAL-проверке по ее идентификатору.

19.2.2.1. Авторизация

Для авторизации в Swagger UI пользователю необходимо получить токен доступа. Кроме того, пользователь может в любое время отозвать полученный токен доступа.

Для выполнения вышеуказанных действий доступны следующие конечные точки:

- `GET [IP-адрес Комплекса]/API/v1/token`;
- `POST [IP-адрес Комплекса]/API/v1/token/revoke`.

19.2.2.1.1. Получение токена доступа

19.2.2.1.1.1. Запрос

URL: `GET [IP-адрес Комплекса]/API/v1/token`

Описание: С помощью этой конечной точки пользователь может получить токен доступа к спецификации API Комплекса. Без токена доступа авторизация в Swagger UI и выполнение действий с конечными точками невозможны.

Пример запроса:

```
curl -i -X GET \
'https://[IP-адрес Комплекса]/api/v1/token' \
```

```
-H 'accept: application/json' \
-H 'Authorization: Basic ZGF0YXBrOmRhdGFwaw=='
```

19.2.2.1.1.2. Успешный ответ

Код ответа: `200 OK`

Тип содержимого: `application/json`

Пример тела ответа:

```
{
  "access_token": ["токен доступа"]
}
```

Заголовки ответа:

```
 connection: keep-alive
content-encoding: gzip
content-type: application/json
date: Mon,05 May 2025 11:08:01 GMT
public-key-pins: pin-sha256="base64+info1="; max-age=31536000
server: nginx
strict-transport-security: max-age=31536000
transfer-encoding: chunked
x-content-type-options: nosniff
x-frame-options: DENY
x-xss-protection: 1; mode=block
```

19.2.2.1.1.3. Возможные ошибки

Информация о возможных ошибках представлена в таблице ниже.

Табл. 55. Возможные ошибки при выполнении запроса GET [IP-адрес Комплекса]/API/v1/token

HTTP-КОД	ЗНАЧЕНИЕ	ОПИСАНИЕ	ПРИМЕР ТЕЛА ОТВЕТА
`403`	`Forbidden`	Ошибка доступа	`{ "detail": "Not authenticated" }`

19.2.2.1.2. Отзыв токена доступа

19.2.2.1.2.1. Запрос

URL: `POST [IP-адрес Комплекса]/API/v1/token/revoke`

Описание: С помощью этой конечной точки пользователь может отозвать ранее полученный токен доступа к спецификации API Комплекса.

Пример запроса:

```
curl -X 'POST' \
'https://[IP-адрес Комплекса]/api/v1/token/revoke' \
```

```
-H 'accept: application/json' \
-H 'X-API-Token: [токен доступа]'
-d ''
```

19.2.2.1.2.2. Успешный ответ

Код ответа: `200 OK`

Тип содержимого: `application/json`

Пример тела ответа:

Заголовки ответа:

```
connection: keep-alive
content-encoding: gzip
content-type: application/json
strict-transport-security: max-age=31536000
x-content-type-options: nosniff
x-frame-options: DENY
x-xss-protection: 1; mode=block
```

19.2.2.1.2.3. Возможные ошибки

Информация о возможных ошибках представлена в таблице ниже.

Табл. 56. Возможные ошибки при выполнении запроса POST [ip-адрес Комплекса]/API/v1/token/revoke

HTTP-КОД	ЗНАЧЕНИЕ	ОПИСАНИЕ	ПРИМЕР ТЕЛА ОТВЕТА
`204`	`No Content`	Отсутствует содержимое ответа	
`403`	`Forbidden`	Ошибка доступа	`{ "detail": "Not authenticated" }`
`404`	`Not Found`	Запись не найдена	`{ "message": "Request failed", "errors": [ "{\"message\":\"Запись не найдена\", \"errors\":[\"No row was found when one was required\"]}" ] }`
`422`	`Validation Error`	Ошибка валидации	`{ "detail": [ { "loc": [`

Табл. 56. Возможные ошибки при выполнении запроса POST [ip-адрес Комплекса]/API/v1/token/revoke

HTTP-КОД	ЗНАЧЕНИЕ	ОПИСАНИЕ	ПРИМЕР ТЕЛА ОТВЕТА

			<pre>"string"
			],
			"msg": "string",
			"type": "string"
			}
			]
			}</pre>

19.2.2.2. Активы и сетевые интерфейсы

Для выполнения операций с активами и сетевыми интерфейсами доступны следующие конечные точки:

- `GET [IP-адрес Комплекса]/API/v1/inventory/assets` — конечная точка для получения данных обо всех активах;
- `GET [IP-адрес Комплекса]/API/v1/inventory/assets/{asset_id}` — конечная точка для получения данных об активе по его идентификатору;
- `GET [IP-адрес Комплекса]/API/v1/inventory/asset_types` — конечная точка для получения списка всех типов активов;
- `GET [ip-адрес Комплекса]/API/v1/inventory/interfaces` — конечная точка для получения информации о сетевых интерфейсах.

19.2.2.2.1. Получение информации обо всех активах

19.2.2.2.1.1. Запрос

URL: `GET [ip-адрес Комплекса]/API/v1/inventory/assets`

Описание: С помощью этой конечной точки пользователь может получить информацию об активах на Комплексе.

Авторизация: Требуется передача заголовка X-API-Token с действительным токеном доступа.

Пример запроса :

```
curl -X 'GET' \
'https://[IP-адрес Комплекса]/API/v1/inventory/assets' \
-H 'accept: application/json' \
-H 'X-API-Token: [токен доступа]' \
-H 'Content-Type: application/json' \
-d '{
  "limit": 1000,
  "asset_types": [
    "string"
  ],
  "vendors": [
    "string"
  ],
  "asset_ids": [
    "3fa85f64-5717-4562-b3fc-2c963f66afa6"
```

```
  ],
  "sensor_ids": [
    "3383113bf1eb1e069ac958e53bd0a3ed"
  ],
  "ics_ids": [
    "3fa85f64-5717-4562-b3fc-2c963f66afa6"
  ],
  "ip_addresses": [
    "string"
  ],
  "mac_address": "24:f3:5c:fb:bc:23",
  "labels_ids": [
    "3fa85f64-5717-4562-b3fc-2c963f66afa6"
  ],
  "asset_groups_ids": [
    "3fa85f64-5717-4562-b3fc-2c963f66afa6"
  ],
  "only_known_assets": true,
  "asset_hostname_search": "string",
  "without_asset_groups": true,
  "operating_system_name_search": "string",
  "operating_system__vendor_search": "string",
  "operating_system__version_search": "string",
  "status": [
    "EMPTY"
  ],
  "pagination_sort_field": "netbios_name",
  "pagination_sort_direction": "asc",
  "pagination_last_id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
  "pagination_sort_field_last_value": "string"
}'
```

Табл. 57. Параметры запроса GET [IP-адрес Комплекса]/API/v1/inventory/assets

ПОЛЕ	ТИП	ОПИСАНИЕ
`limit`	`integer`	Предельное количество активов, для которых необходимо получить данные
`asset_types`	`array`	Типы активов
`vendors`	`array`	Поставщики
`asset_ids`	`array`	Идентификаторы активов
`sensor_ids`	`array`	Идентификаторы сенсоров

Табл. 57. Параметры запроса GET [IP-адрес Комплекса]/API/v1/inventory/assets

ПОЛЕ	ТИП	ОПИСАНИЕ
`ics_ids`	`array`	Идентификаторы АСУ ТП, к которым принадлежат активы
`ip_addresses`	`array`	IP-адреса
`mac_address`	`string`	MAC-адрес
`labels_ids`	`array`	Идентификаторы меток
`asset_groups_ids`	`array`	Идентификаторы групп активов
`only_known_assets`	`boolean`	Поиск только среди известных активов
`asset_hostname_search`	`string`	Поиск по наименованию хоста
`without_asset_groups`	`boolean`	Поиск среди активов без группы
`operating_system_name_search`	`string`	Поиск по наименованию операционной системы
`operating_system_vendor_-search`	`string`	Поиск по наименованию поставщика операционной системы
`operating_system_version_-search`	`string`	Поиск по версии операционной системы
`status`	`string`	Статус. Доступны следующие значения: • `EMPTY`; • `OK`; • `WARNING`; • `CRITICAL`.
`pagination_sort_field`	`string`	Поле, по которому должна выполняться сортировка активов. Доступны следующие значения: • `netbios_name`; • `vendor`; • `problematic`; • `incidents_stat`;

Табл. 57. Параметры запроса GET [IP-адрес Комплекса]/API/v1/inventory/assets

ПОЛЕ	ТИП	ОПИСАНИЕ
		• `configurations_stat`; • `data_collection_logs_stat`; • `vulnerability_stat`.
`pagination_sort_direction`	`string`	Направление сортировки. Доступны следующие значения: • `asc` — по возрастанию; • `desc` — по убыванию.
`pagination_last_id`	`string`	Последний идентификатор
`pagination_sort_field_last_-value`	`string`	Последнее значение поля

19.2.2.2.1.2. Успешный ответ

Код ответа: `200 OK`

Тип содержимого: `application/json`

Пример тела ответа:


```
{
  "data": [
    {
      "asset_name": "string",
      "id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
      "type": "APPLIANCE",
      "description": "string",
      "vendor": "string",
      "operating_system": {
        "asset_id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
        "created_at": "2025-04-29T11:42:08.432Z",
        "updated_at": "2025-04-29T11:42:08.432Z",
        "product": "string",
        "version": "string",
        "vendor": "string"
      },
      "status": "EMPTY",
      "created_at": "2025-04-29T11:42:08.432Z",
      "updated_at": "2025-04-29T11:42:08.432Z",
      "ics_id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
      "asset_group_id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
      "sensor_id": "47a690981c082cb63c21e771292b728a",
      "ics": {
```

```
      "name": "string",
      "id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
      "description": "string",
      "parent_id": "3fa85f64-5717-4562-b3fc-2c963f66afa6"
    },
    "asset_group": {
      "id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
      "name": "string",
      "description": "string",
      "parent_id": "3fa85f64-5717-4562-b3fc-2c963f66afa6"
    },
    "labels": [
      {
        "name": "string",
        "id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
        "parent_id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
        "is_system": true
      }
    ],
    "network_interfaces": [
      {
        "name": "string",
        "id": "string",
        "description": "string",
        "ip_v4_address": "198.51.100.42",
        "mac_address": "string",
        "status": true,
        "last_network_activity": "2025-04-29T11:42:08.432Z",
        "created_at": "2025-04-29T11:42:08.432Z",
        "updated_at": "2025-04-29T11:42:08.432Z",
        "asset_id": "string",
        "network_switch_interface_id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
        "sensor_id": "d0124dbae72f2202a7d40d215793a93c",
        "default": true
      }
    ],
    "default_interface": {
      "name": "string",
      "id": "string",
      "description": "string",
      "ip_v4_address": "198.51.100.42",
      "mac_address": "string",
      "status": true,
      "last_network_activity": "2025-04-29T11:42:08.432Z",
      "created_at": "2025-04-29T11:42:08.432Z",
      "updated_at": "2025-04-29T11:42:08.432Z",
      "asset_id": "string",
```

```
        "network_switch_interface_id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
        "sensor_id": "bc2b9a1e700db641ebab4a8d05f2715a",
        "default": true
      }
    }
  ],
  "total_count": 0,
  "filtered_count": 0
}
```


Табл. 58. Описание полей ответа на запрос GET [IP-адрес Комплекса]/API/v1/inventory/assets

ПОЛЕ	ТИП	ОПИСАНИЕ
`data`	`array`	Информация по полученным активам
`asset_name`	`string`	Наименование актива
`type`	`string`	Тип актива. Доступны следующие значения: • `APPLIANCE`; • `IDS`; • `PERIFERY`; • `PLC`; • `ROUTER`; • `SENSOR`; • `SERVER`; • `SWITCH`; • `UNKNOWN`; • `WORKSTATION`.
`description`	`string`	Описание актива
`vendor`	`string`	Поставщик
`operating_system`	`object`	Информация об операционной системе актива
`asset_id`	`string`	Идентификатор актива
`created_at`	`string`	Дата и время создания ОС
`updated_at`	`string`	Дата и время обновления ОС
`product`	`string`	Описание продукта

Табл. 58. Описание полей ответа на запрос GET [IP-адрес Комплекса]/API/v1/inventory/assets

ПОЛЕ	ТИП	ОПИСАНИЕ
`version`	`string`	Версия продукта
`vendor`	`string`	Поставщик
`status`	`string`	Статус. Доступны следующие значения: • `EMPTY`; • `OK`; • `WARNING`; • `CRITICAL`.
`created_at`	`string`	Дата и время создания актива
`updated_at`	`string`	Дата и время обновления актива
`ics_id`	`string`	Идентификатор АСУ ТП, к которой принадлежит актив
`asset_group_id`	`string`	Идентификатор группы актива
`sensor_id`	`string`	Идентификатор сенсора
`ics`	`array`	Информация об АСУ ТП, к которой принадлежит актив
`name`	`string`	Наименование АСУ ТП, к которой принадлежит актив
`id`	`string`	Идентификатор АСУ ТП, к которой принадлежит актив
`description`	`string`	Описание АСУ ТП, к которой принадлежит актив
`parent_id`	`string`	Идентификатор родительского актива
`asset_group`	`array`	Группа актива
`id`	`string`	Идентификатор группы актива
`name`	`string`	Наименование группы актива

Табл. 58. Описание полей ответа на запрос GET [IP-адрес Комплекса]/API/v1/inventory/assets

ПОЛЕ	ТИП	ОПИСАНИЕ
`description`	`string`	Описание группы активов
`parent_id`	`string`	Идентификатор родительского актива
`labels`	`array`	Метка актива
`name`	`string`	Наименование метки актива
`id`	`string`	Идентификатор метки актива
`parent_id`	`string`	Идентификатор родительского актива
`is_system`	`boolean`	Признак того, что актив является системой
`network_interfaces`	`array`	Сетевые интерфейсы
`name`	`string`	Наименование сетевого интерфейса
`id`	`string`	Идентификатор сетевого интерфейса
`description`	`string`	Описание сетевого интерфейса
`ip_v4_address`	`string`	Адрес IPv4
`mac_address`	`string`	MAC-адрес
`status`	`boolean`	Статус сетевого интерфейса
`last_network_activity`	`string`	Дата и время последней сетевой активности
`created_at`	`number`	Дата и время создания сетевого интерфейса
`updated_at`	`number`	Дата и время обновления сетевого интерфейса
`asset_id`	`string`	Идентификатор актива

Табл. 58. Описание полей ответа на запрос GET [IP-адрес Комплекса]/API/v1/inventory/assets

ПОЛЕ	ТИП	ОПИСАНИЕ
`network_switch_interface_id`	`string`	Идентификатор интерфейса сетевого переключателя
`sensor_id`	`string`	Идентификатор сенсора
`default`	`boolean`	Сетевой интерфейс установлен по умолчанию
`default_interface`	`array`	Сетевой интерфейс, установленный по умолчанию
`name`	`string`	Наименование сетевого интерфейса, установленного по умолчанию
`id`	`string`	Идентификатор сетевого интерфейса, установленного по умолчанию
`description`	`string`	Описание сетевого интерфейса, установленного по умолчанию
`ip_v4_address`	`string`	Адрес IPv4 интерфейса, установленного по умолчанию
`mac_address`	`string`	MAC-адрес интерфейса, установленного по умолчанию
`status`	`boolean`	Статус сетевого интерфейса, установленного по умолчанию
`last_network_activity`	`string`	Дата и время последней сетевой активности сетевого интерфейса, установленного по умолчанию
`created_at`	`number`	Дата и время создания сетевого интерфейса сетевого интерфейса, установленного по умолчанию
`updated_at`	`number`	Дата и время обновления сетевого интерфейса сетевого ин-

Табл. 58. Описание полей ответа на запрос GET [IP-адрес Комплекса]/API/v1/inventory/assets

ПОЛЕ	ТИП	ОПИСАНИЕ
		терфейса, установленного по умолчанию
`asset_id`	`string`	Идентификатор актива
`network_switch_interface_id`	`string`	Идентификатор интерфейса сетевого переключателя
`sensor_id`	`string`	Идентификатор сенсора
`default`	`boolean`	Сетевой интерфейс установлен по умолчанию
`total_count`	`integer`	Общее количество активов
`filtered_count`	`integer`	Количество активов, соответствующих указанным параметрам

Заголовки ответа:

```
connection: keep-alive
content-encoding: gzip
content-type: application/json
strict-transport-security: max-age=31536000
x-content-type-options: nosniff
x-frame-options: DENY
x-xss-protection: 1; mode=block
```

19.2.2.2.1.3. Возможные ошибки

Информация о возможных ошибках представлена в таблице ниже.

Табл. 59. Возможные ошибки при выполнении запроса GET [ip-адрес Комплекса]/API/v1/inventory/assets

HTTP-КОД	ЗНАЧЕНИЕ	ОПИСАНИЕ	ПРИМЕР ТЕЛА ОТВЕТА
`401`	`Unauthorized`	Ошибка авторизации	`{ "detail": "Could not validate credentials" }`
`403`	`Forbidden`	Ошибка доступа	`{ "detail": "Not authenticated" }`

Табл. 59. Возможные ошибки при выполнении запроса GET [ip-адрес Комплекса]/API/v1/inventory/assets

HTTP-КОД	ЗНАЧЕНИЕ	ОПИСАНИЕ	ПРИМЕР ТЕЛА ОТВЕТА
`404`	`Not Found`	Запись не найдена	`{ "message": "Request failed", "errors": [ "{\"message\":\"Запись не найдена\", \"errors\":[\"No row was found when one was required\"]}" ] }`
`422`	`Validation Error`	Ошибка валидации	`{ "detail": [ { "loc": [ "string" ], "msg": "string", "type": "string" } ] }`

19.2.2.2.2. Получение информации об определенном активе

19.2.2.2.2.1. Запрос

URL: `GET [ip-адрес Комплекса]/API/v1/inventory/assets/{asset_id}`

Описание: С помощью этой конечной точки пользователь может получить информацию об определенном активе по его идентификатору.

Авторизация: Требуется передача заголовка X-API-Token с действительным токеном доступа.

Пример запроса:

```
curl -i -X GET \
'https://[IP-адрес Комплекса]/API/v1/inventory/assets/{asset_id}' \
-H 'accept: application/json' \
-H 'X-API-Token: [токен доступа]'
-H 'Content-Type: application/json'
```

19.2.2.2.2.2. Успешный ответ

Код ответа: `200 OK`

Тип содержимого: `application/json`

Пример тела ответа:

```
{
  "asset_name": "string",
  "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
  "type": "APPLIANCE",
  "description": "string",
  "vendor": "string",
  "operating_system": {
    "asset_id": "b4695157-0d1d-4da0-8f9e-5c53149389e4",
    "created_at": "2019-08-24T14:15:22Z",
    "updated_at": "2019-08-24T14:15:22Z",
    "product": "string",
    "version": "string",
    "vendor": "string"
  },
  "status": "EMPTY",
  "created_at": "2019-08-24T14:15:22Z",
  "updated_at": "2019-08-24T14:15:22Z",
  "ics_id": "90672151-3d1f-407a-bf67-470401c9673c",
  "asset_group_id": "46dc71b5-e085-4acb-aff0-f9d50bed21ce",
  "sensor_id": "string",
  "ics": {
    "name": "string",
    "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
    "description": "string",
    "parent_id": "1c6ca187-e61f-4301-8dcb-0e9749e89eef"
  },
  "asset_group": {
    "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
    "name": "string",
    "description": "string",
    "parent_id": "1c6ca187-e61f-4301-8dcb-0e9749e89eef"
  },
  "labels": [
    {
      "name": "string",
      "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
      "parent_id": "1c6ca187-e61f-4301-8dcb-0e9749e89eef",
      "is_system": true
    }
  ],
  "network_interfaces": [
    {
      "name": "string",
      "id": "string",
      "description": "string",
      "ip_v4_address": "192.168.0.1",
      "mac_address": "string",
```

```
      "status": true,
      "last_network_activity": "2019-08-24T14:15:22Z",
      "created_at": "2019-08-24T14:15:22Z",
      "updated_at": "2019-08-24T14:15:22Z",
      "asset_id": "string",
      "network_switch_interface_id": "e581646c-8b41-487d-93b5-ce6a709b439d",
      "sensor_id": "string",
      "default": true
    }
  ],
  "default_interface": {
    "name": "string",
    "id": "string",
    "description": "string",
    "ip_v4_address": "192.168.0.1",
    "mac_address": "string",
    "status": true,
    "last_network_activity": "2019-08-24T14:15:22Z",
    "created_at": "2019-08-24T14:15:22Z",
    "updated_at": "2019-08-24T14:15:22Z",
    "asset_id": "string",
    "network_switch_interface_id": "e581646c-8b41-487d-93b5-ce6a709b439d",
    "sensor_id": "string",
    "default": true
  }
}
```


Табл. 60. Описание полей ответа на запрос GET [ip-адрес Комплекса]/API/v1/inventory/assets/{asset_id}

ПОЛЕ	ТИП	ОПИСАНИЕ
`asset_name`	`string`	Наименование актива
`id`	`string`	Идентификатор актива
`type`	`string`	Тип актива. Доступны следующие значения: • `APPLIANCE`; • `IDS`; • `PERIFERY`; • `PLC`; • `ROUTER`; • `SENSOR`; • `SERVER`; • `SWITCH`;

Табл. 60. Описание полей ответа на запрос GET [ip-адрес Комплекса]/API/v1/inventory/assets/{asset_id}

ПОЛЕ	ТИП	ОПИСАНИЕ
		• `UNKNOWN`; • `WORKSTATION`.
`description`	`string`	Описание актива
`vendor`	`string`	Поставщик
`operating_system`	`object`	Информация об операционной системе актива
`asset_id`	`string`	Идентификатор актива
`created_at`	`string`	Дата и время создания ОС
`updated_at`	`string`	Дата и время обновления ОС
`product`	`string`	Описание продукта
`version`	`string`	Версия продукта
`vendor`	`string`	Поставщик
`status`	`string`	Статус. Доступны следующие значения: • `EMPTY`; • `OK`; • `WARNING`; • `CRITICAL`.
`created_at`	`string`	Дата и время создания актива
`updated_at`	`string`	Дата и время обновления актива
`ics_id`	`string`	Идентификатор идентификатор АСУ ТП, к которой принадлежит актив
`asset_group_id`	`string`	Идентификатор группы актива
`sensor_id`	`string`	Идентификатор сенсора
`ics`	`array`	Информация об АСУ ТП, к которой принадлежит актив

Табл. 60. Описание полей ответа на запрос GET [ip-адрес Комплекса]/API/v1/inventory/assets/{asset_id}

ПОЛЕ	ТИП	ОПИСАНИЕ
`name`	`string`	Наименование АСУ ТП, к которой принадлежит актив
`id`	`string`	Идентификатор АСУ ТП, к которой принадлежит актив
`description`	`string`	Описание АСУ ТП, к которой принадлежит актив
`parent_id`	`string`	Идентификатор родительского актива
`asset_group`	`object`	Группа актива
`id`	`string`	Идентификатор группы актива
`name`	`string`	Наименование группы актива
`description`	`string`	Описание группы актива
`parent_id`	`string`	Идентификатор родительской группы актива
`labels`	`array`	Метка актива
`name`	`string`	Наименование метки актива
`id`	`string`	Идентификатор метки актива
`parent_id`	`string`	Идентификатор метки родительского актива
`is_system`	`boolean`	Признак того, что актив является системой
`network_interfaces`	`array`	Сетевые интерфейсы
`name`	`string`	Наименование сетевого интерфейса
`id`	`string`	Идентификатор сетевого интерфейса
`description`	`string`	Описание сетевого интерфейса

Табл. 60. Описание полей ответа на запрос GET [ip-адрес Комплекса]/API/v1/inventory/assets/{asset_id}

ПОЛЕ	ТИП	ОПИСАНИЕ
`ip_v4_address`	`string`	Адрес IPv4
`mac_address`	`string`	MAC-адрес
`status`	`boolean`	Статус сетевого интерфейса
`last_network_activity`	`string`	Дата и время последней сетевой активности
`created_at`	`number`	Дата и время создания сетевого интерфейса
`updated_at`	`number`	Дата и время обновления сетевого интерфейса
`asset_id`	`string`	Идентификатор актива
`network_switch_interface_id`	`string`	Идентификатор интерфейса сетевого переключателя
`sensor_id`	`string`	Идентификатор сенсора
`default`	`boolean`	Сетевой интерфейс установлен по умолчанию
`default_interface`	`array`	Сетевой интерфейс, установленный по умолчанию
`name`	`string`	Наименование сетевого интерфейса, установленного по умолчанию
`id`	`string`	Идентификатор сетевого интерфейса, установленного по умолчанию
`description`	`string`	Описание сетевого интерфейса, установленного по умолчанию
`ip_v4_address`	`string`	Адрес IPv4 интерфейса, установленного по умолчанию
`mac_address`	`string`	MAC-адрес интерфейса, установленного по умолчанию

Табл. 60. Описание полей ответа на запрос GET [ip-адрес Комплекса]/API/v1/inventory/assets/{asset_id}

ПОЛЕ	ТИП	ОПИСАНИЕ
`status`	`boolean`	Статус сетевого интерфейса, установленного по умолчанию
`last_network_activity`	`string`	Дата и время последней сетевой активности сетевого интерфейса, установленного по умолчанию
`created_at`	`number`	Дата и время создания сетевого интерфейса сетевого интерфейса, установленного по умолчанию
`updated_at`	`number`	Дата и время обновления сетевого интерфейса сетевого интерфейса, установленного по умолчанию
`asset_id`	`string`	Идентификатор актива
`network_switch_interface_id`	`string`	Идентификатор интерфейса сетевого переключателя
`sensor_id`	`string`	Идентификатор сенсора
`default`	`boolean`	Признак того, что сетевой интерфейс установлен по умолчанию
`total_count`	`integer`	Общее количество активов
`filtered_count`	`integer`	Количество активов, соответствующих указанным параметрам

Заголовки ответа:

```
connection: keep-alive
content-encoding: gzip
content-type: application/json
strict-transport-security: max-age=31536000
x-content-type-options: nosniff
x-frame-options: DENY
x-xss-protection: 1; mode=block
```

19.2.2.2.2.3. Возможные ошибки

Информация о возможных ошибках представлена в таблице ниже.

Табл. 61. Возможные ошибки при выполнении запроса GET [ip-адрес Комплекса]/API/v1/inventory/assets/{asset_id}

HTTP-КОД	ЗНАЧЕНИЕ	ОПИСАНИЕ	ПРИМЕР ТЕЛА ОТВЕТА
`401`	`Unauthorized`	Ошибка авторизации	`{ "detail": "Could not validate credentials" }`
`403`	`Forbidden`	Ошибка доступа	`{ "detail": "Not authenticated" }`
`422`	`Validation Error`	Ошибка валидации	`{ "detail": [ { "loc": [ "string" ], "msg": "string", "type": "string" } ] }`

19.2.2.2.3. Получение списка доступных типов активов

19.2.2.2.3.1. Запрос

URL: `GET [ip-адрес Комплекса]/API/v1/inventory/asset_types`

Описание: С помощью этой конечной точки пользователь может получить информацию о типах активов, регистрируемых Комплексом.

Авторизация: Требуется передача заголовка X-API-Token с действительным токеном доступа.

Пример запроса:

```
curl -i -X GET \
'https://[IP-адрес Комплекса]/API/v1/inventory/asset_types' \
-H 'accept: application/json' \
-H 'X-API-Token: [токен доступа]'
```

19.2.2.2.3.2. Успешный ответ

Код ответа: `200 OK`

Тип содержимого: `application/json`

Пример тела ответа:

```
[
  "APPLIANCE",
  "IDS",
  "PERIFERY",
  "PLC",
  "ROUTER",
  "SENSOR",
  "SERVER",
  "SWITCH",
  "UNKNOWN",
  "WORKSTATION"
]
```

Табл. 62. Описание полей ответа на запрос GET [IP-адрес Комплекса]/API/v1/inventory/asset_types

ПОЛЕ	ТИП	ОПИСАНИЕ
`APPLIANCE`	`string`	Комплекс
`IDS`	`string`	Сетевое средство защиты
`PERIFERY`	`string`	Периферийное оборудование
`PLC`	`string`	ПЛК
`ROUTER`	`string`	Маршрутизатор
`SWITCH`	`string`	Коммутатор
`SERVER`	`string`	Сервер
`SENSOR`	`string`	Сенсор
`UNKNOWN`		Неизвестный тип
`WORKSTATION`	`string`	АРМ

Заголовки ответа:

```
connection: keep-alive
content-encoding: gzip
content-type: application/json
date: Thu,29 May 2025 07:59:37 GMT
public-key-pins: pin-sha256="base64+info1="; max-age=31536000
server: nginx
strict-transport-security: max-age=31536000
```

```
transfer-encoding: chunked
x-content-type-options: nosniff
x-frame-options: DENY
x-xss-protection: 1; mode=block
```

19.2.2.2.3.3. Возможные ошибки

Информация о возможных ошибках представлена в таблице ниже.

Табл. 63. Возможные ошибки при выполнении запроса GET [ip-адрес Комплекса]/API/v1/inventory/asset_types

HTTP-КОД	ЗНАЧЕНИЕ	ОПИСАНИЕ	ПРИМЕР ТЕЛА ОТВЕТА
`401`	`Unauthorized`	Ошибка авторизации	`{ "detail": "Could not validate credentials" }`
`403`	`Forbidden`	Ошибка доступа	`{ "detail": "Not authenticated" }`
`422`	`Validation Error`	Ошибка валидации	`{ "detail": [ { "loc": [ "string" ], "msg": "string", "type": "string" } ] }`

19.2.2.2.4. Получение информации о сетевых интерфейсах

19.2.2.2.4.1. Запрос

URL: `GET [ip-адрес Комплекса]/API/v1/inventory/assets/{asset_id}`

Описание: С помощью этой конечной точки пользователь может получить список сетевых атрибутов активов, соответствующих параметрам, установленным в запросе.

Авторизация: Требуется передача заголовка X-API-Token с действительным токеном доступа.

Пример запроса:

```
curl -i -X GET \
'https://[IP-адрес Комплекса]/API/v1/inventory/interfaces?default=true \
&host_interface_ids=497f6eca-6276-4993-bfeb-53cbbbba6f08 \
&host_types=APPLIANCE \
```

```
&host_ids=497f6eca-6276-4993-bfeb-53cbbbba6f08 \
&ip_v4_addresses=192.168.0.1 \
&limit=1000 \
&mac_addresses=string \
&nodes_ids=string \
&number_from=9223372036854776000 \
&only_with_addresses=true \
&search=string \
&status=true'' \
-H 'accept: application/json' \
-H 'X-API-Token: [токен доступа]'
-H 'Content-Type: application/json'
```

Табл. 64. Параметры запроса GET [IP-адрес Комплекса]/API/v1/inventory/interfaces

ПОЛЕ	ТИП	ОПИСАНИЕ
`host_interface_id`	`string`	Идентификатор сетевого интерфейса
`host_ids`	`array`	Идентификаторы хостов
`node_ids`	`array`	Идентификаторы сетевых узлов
`ip_v4_addresses`	`array`	Адреса IPv4
`mac_addresses`	`array`	MAC-адреса
`status`	`boolean`	Статус сетевого интерфейса
`default`	`boolean`	Признак того, что сетевой интерфейс установлен по умолчанию
`only_with_addresses`	`boolean`	Сетевые интерфейсы только с адресами
`host_types`	`string`	Типы активов. Доступны следующие значения: • `APPLIANCE`; • `IDS`; • `PERIFERY`; • `PLC`; • `ROUTER`; • `SENSOR`; • `SERVER`; • `SWITCH`;

Табл. 64. Параметры запроса GET [IP-адрес Комплекса]/API/v1/inventory/interfaces

ПОЛЕ	ТИП	ОПИСАНИЕ
		• `UNKNOWN`; • `WORKSTATION`.
`search`	`string`	Значение, по которому должен выполняться поиск
`limit`	`integer`	Предельное количество
`number_from`	`integer`	Начальное число сортировки

19.2.2.2.4.2. Успешный ответ

Код ответа: `200 OK`

Тип содержимого: `application/json`

Пример тела ответа:

```
[
  {
    "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
    "asset_id": "eb4e20fc-2b4a-4d0c-811f-48abcf12b89b",
    "name": "string",
    "description": "string",
    "default": true,
    "status": true,
    "ip_v4_address": "192.168.0.1",
    "mac_address": "string",
    "created_at": 0,
    "updated_at": 0,
    "last_network_activity": 0,
    "switch_interface_id": "dc0c08a3-1760-4e70-82db-9511d8a22f97",
    "number": 0,
    "sensor_id": "string"
  }
]
```

Табл. 65. Описание полей ответа на запрос GET [IP-адрес Комплекса]/API/v1/inventory/interfaces

ПОЛЕ	ТИП	ОПИСАНИЕ
`id`	`string`	Идентификатор сетевого интерфейса
`asset_id`	`string`	Идентификатор хоста, которому принадлежит сетевой интерфейс

Табл. 65. Описание полей ответа на запрос GET [IP-адрес Комплекса]/API/v1/inventory/interfaces

ПОЛЕ	ТИП	ОПИСАНИЕ
`name`	`string`	Наименование сетевого интерфейса
`description`	`string`	Описание сетевого интерфейса
`default`	`boolean`	Признак того, что сетевой интерфейс установлен по умолчанию
`status`	`boolean`	Статус сетевого интерфейса
`ip_v4_address`	`string`	Адрес IPv4
`mac_address`	`string`	MAC-адрес
`created_at`	`number`	Дата создания сетевого интерфейса
`updated_at`	`number`	Дата обновления сетевого интерфейса
`last_network_activity`	`number or null`	Время последней сетевой активности
`switch_interface_id`	`string`	Идентификатор интерфейса сетевого переключателя
`number`	`integer`	Номер сетевого интерфейса
`sensor_id`	`string`	Идентификатор сетевого узла

Заголовки ответа:

```
connection: keep-alive
content-encoding: gzip
content-type: application/json
strict-transport-security: max-age=31536000
x-content-type-options: nosniff
x-frame-options: DENY
x-xss-protection: 1; mode=block
```

19.2.2.2.4.3. Возможные ошибки

Информация о возможных ошибках представлена в таблице ниже.

Табл. 66. Возможные ошибки при выполнении запроса GET [ip-адрес Комплекса]/API/v1/inventory/interfaces

HTTP-КОД	ЗНАЧЕНИЕ	ОПИСАНИЕ	ПРИМЕР ТЕЛА ОТВЕТА
`401`	`Unauthorized`	Ошибка авторизации	`{ "detail": "Could not validate credentials" }`
`403`	`Forbidden`	Ошибка доступа	`{ "detail": "Not authenticated" }`
`422`	`Validation Error`	Ошибка валидации	`{ "detail": [ { "loc": [ "string" ], "msg": "string", "type": "string" } ] }`

19.2.2.3. Инциденты

Для выполнения операций с инцидентами доступны следующие конечные точки:

- `GET [ip-адрес Комплекса]/API/v1/incidents` — конечная точка для получения списка всех инцидентов;
- `GET [ip-адрес Комплекса]/API/v1/incidents/incident_statuses` — конечная точка для получения списка доступных статусов инцидентов;
- `GET [ip-адрес Комплекса]/API/v1/incidents/{incident_id}` — конечная точка для получения информации об инциденте по его идентификатору;
- `PATCH [ip-адрес Комплекса]/API/v1/incidents/incident_statuses/{incident_status_id}` — конечная точка для обновления статуса инцидента.

19.2.2.3.1. Получение списка всех инцидентов, зарегистрированных Комплексом

19.2.2.3.1.1. Запрос

URL: `GET [ip-адрес Комплекса]/API/v1/incidents`

Описание: С помощью этой конечной точки пользователь может просмотреть список инцидентов, зарегистрированных Комплексом и соответствующих параметрам, переданным в запросе.

Авторизация: Требуется передача заголовка X-API-Token с действительным токеном доступа.

Пример запроса:

```
curl -X 'GET' \
'https://[IP-адрес Комплекса]/API/v1/incidents' \
-H 'accept: application/json' \
-H 'X-API-Token: [токен доступа]' \
-H 'Content-Type: application/json' \
-d '{
  "pagination_last_number": 0,
    "pagination_sort_order": "asc",
    "pagination_sort_field": "created_at",
    "pagination_sort_field_value": 0,
    "search": "string",
    "created_at_from": 0,
    "created_at_to": 0,
    "updated_at_from": 0,
    "updated_at_to": 0,
    "is_confirmed": true,
    "user": "string",
    "incident_type": "current",
    "limit": 1000,
    "fields": [
      "host_ids"
    ],
    "source_appliances_ids": [
      "497f6eca-6276-4993-bfeb-53cbbbba6f08"
    ],
    "retro_entries_ids": [
      "497f6eca-6276-4993-bfeb-53cbbbba6f08"
    ],
    "priority": [
      "LOW"
    ],
    "status_ids": [
      "497f6eca-6276-4993-bfeb-53cbbbba6f08"
    ],
    "asset_ids": [
      "497f6eca-6276-4993-bfeb-53cbbbba6f08"
    ],
    "incidents_ids": [
      "497f6eca-6276-4993-bfeb-53cbbbba6f08"
    ]
}'
```

Табл. 67. Параметры запроса GET [IP-адрес Комплекса]/API/v1/incidents

ПОЛЕ	ТИП	ОПИСАНИЕ
`pagination_last_number`	`integer`	Номер записи, от которой следует начитать отсчет
`pagination_sort_order`	`string`	Направление сортировки инцидентов. Доступны следующие значения: • `asc` — по возрастанию; • `desc` — по убыванию. Данное значение установлено по умолчанию.
`pagination_sort_field`	`string`	Поле, по которому должна выполняться сортировка инцидентов. Доступны следующие значения: • `created_at` — дата создания; • `updated_at` — дата обновления.
`pagination_sort_field_value`	`number`	Значение поля, по которому должна выполняться сортировка инцидентов
`search`	`string`	Значение, по которому должен выполняться поиск
`created_at_from`	`number`	Начальное время создания инцидента
`created_at_to`	`number`	Конечное время создания инцидента
`updated_at_from`	`number`	Начальное время обновления инцидента
`updated_at_to`	`number`	Конечное время обновления инцидента
`is_confirmed`	`boolean`	Признак того, что инцидент подтвержден

Табл. 67. Параметры запроса GET [IP-адрес Комплекса]/API/v1/incidents

ПОЛЕ	ТИП	ОПИСАНИЕ
`user`	`string`	Пользователь, ответственный за работу с инцидентом
`incident_type`	`string`	Тип инцидента. Доступны следующие значения: • `current` — инцидент, выявленный в процессе работы Комплекса; • `retro` — инцидент, выявленный в ходе ретроспективной проверки.
`limit`	`integer`	Количество записей
`fields`	`array`	Поля значений инцидентов. Доступны следующие значения: • `host_ids` — идентификаторы хостов; • `status` — статус инцидента; • `history` — история инцидента.
`source_appliances_ids`	`array`	Идентификаторы источников
`retro_entries_ids`	`array`	Идентификаторы ретроспективных проверок
`priority`	`array`	Приоритет инцидента. Доступны следующие значения: • `LOW` — низкий приоритет; • `MEDIUM` — средний приоритет; • `HIGH` — высокий приоритет; • `CRITICAL` — критический приоритет.
`status_ids`	`array`	Идентификаторы статусов
`asset_ids`	`array`	Идентификаторы активов
`incidents_ids`	`array`	Идентификаторы инцидентов

19.2.2.3.1.2. Успешный ответ

Код ответа: `200 OK`

Тип содержимого: `application/json`

Пример тела ответа:


```
{
  "total_count": 0,
  "filtered_count": 0,
  "total_count_is_approximate": true,
  "data": [
    {
      "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
      "status_id": "4e949624-bc0f-439e-a9f2-25a23938812c",
      "name": "string",
      "description": "string",
      "comment": "string",
      "created_at": 0,
      "source_events": [
        "497f6eca-6276-4993-bfeb-53cbbbba6f08"
      ],
      "priority": "LOW",
      "updated_at": 0,
      "status": {
        "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
        "name": "string",
        "category": "NEW",
        "custom": true,
        "order": 0,
        "is_used": true
      },
      "is_confirmed": false,
      "additional_info": {},
      "number": 0,
      "asset_ids": [
        "497f6eca-6276-4993-bfeb-53cbbbba6f08"
      ],
      "user": "string",
      "history": [
        {
          "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
          "incident_id": "2f811c5b-b888-4fb3-aac5-3c6a4b05df32",
          "status": "string",
          "is_confirmed": true,
          "priority": "LOW",
          "created_at": 0,
          "user": "string",
```

```
          "comment": "string",
          "status_id": "4e949624-bc0f-439e-a9f2-25a23938812c"
        }
      ],
      "type": "current",
      "retro_entry_id": "f17716a7-60a9-44e0-ad4f-1bddec028d1d",
      "source_appliances_ids": [
        "string"
      ]
    }
  ]
}
```


Табл. 68. Описание полей ответа на запрос GET [IP-адрес Комплекса]/API/v1/incidents

ПОЛЕ	ТИП	ОПИСАНИЕ
`total_count`	`integer`	Общее количество инцидентов
`filtered_count`	`integer`	Количество инцидентов, соответствующих параметрам
`total_count_is_approximate`	`boolean`	Признак того, что общее количество является приблизительным
`data`	`array`	Информация об инцидентах
`id`	`string`	Идентификатор инцидента
`status_id`	`string`	Идентификатор статуса
`name`	`string`	Название инцидента
`description`	`string`	Описание инцидента
`comment`	`string`	Комментарий к инциденту
`created_at`	`number`	Дата и время создания инцидента
`source_events`	`array`	Источники событий
`priority`	`string`	Приоритет. Доступны следующие значения:

Табл. 68. Описание полей ответа на запрос GET [IP-адрес Комплекса]/API/v1/incidents

ПОЛЕ	ТИП	ОПИСАНИЕ
		• `LOW` — низкий приоритет; • `MEDIUM` — средний приоритет. Данное значение установлено значением по умолчанию; • `HIGH` — высокий приоритет; • `CRITICAL` — критический приоритет.
`updated_at`	`number`	Дата и время обновления инцидента
`status`	`object`	Статус инцидента
`id`	`string`	Идентификатор статуса
`name`	`string`	Название статуса
`category`	`string`	Категория инцидента. Доступны следующие значения: • `NEW` — новый инцидент; • `IN_PROGRESS` — инцидент, находящийся в работе; • `COMPLETED` — закрытый инцидент.
`custom`	`boolean`	Признак того, что инцидент имеет пользовательский статус
`order`	`integer`	Порядковый номер
`is_used`	`boolean`	Признак того, что статус используется
`is_confirmed`	`boolean`	Признак того, что инцидент подтвержден
`additional_info`	`object`	Дополнительная информация
`number`	`integer`	Номер инцидента
`asset_ids`	`array`	Идентификаторы активов

Табл. 68. Описание полей ответа на запрос GET [IP-адрес Комплекса]/API/v1/incidents

ПОЛЕ	ТИП	ОПИСАНИЕ
`user`	`string`	Пользователь, ответственный за работу с инцидентом
`history`	`array`	История инцидента
`id`	`string`	Идентификатор
`incident_id`	`string`	Идентификатор инцидента
`status`	`string`	Статус инцидента
`is_confirmed`	`boolean`	Признак того, что инцидент подтвержден
`priority`	`string`	Приоритет. Доступны следующие значения: • `LOW` — низкий приоритет; • `MEDIUM` — средний приоритет.; • `HIGH` — высокий приоритет; • `CRITICAL` — критический приоритет.
`created_at`	`integer`	Дата и время создания инцидента
`user`	`string`	Пользователь, ответственный за работу с инцидентом
`comment`	`string`	Комментарий
`status_id`	`string`	Идентификатор статуса
`type`	`string`	Тип инцидента. Доступны следующие значения: • `current` — инцидент, выявленный в процессе работы Комплекса; • `retro` — инцидент, выявленный в ходе ретроспективной проверки.

Табл. 68. Описание полей ответа на запрос GET [IP-адрес Комплекса]/API/v1/incidents

ПОЛЕ	ТИП	ОПИСАНИЕ
`retro_entry_id`	`string`	Идентификаторы ретроспективных проверок
`source_appliances_ids`	`array`	Идентификаторы источников

Заголовки ответа:

```
connection: keep-alive
content-encoding: gzip
content-type: application/json
strict-transport-security: max-age=31536000
x-content-type-options: nosniff
x-frame-options: DENY
x-xss-protection: 1; mode=block
```

19.2.2.3.1.3. Возможные ошибки

Информация о возможных ошибках представлена в таблице ниже.

Табл. 69. Возможные ошибки при выполнении запроса GET [ip-адрес Комплекса]/API/v1/incidents

HTTP-КОД	ЗНАЧЕНИЕ	ОПИСАНИЕ	ПРИМЕР ТЕЛА ОТВЕТА
`401`	`Unauthorized`	Ошибка авторизации	`{ "detail": "Could not validate credentials" }`
`403`	`Forbidden`	Ошибка доступа	`{ "detail": "Not authenticated" }`
`404`	`Not Found`	Запись не найдена	`{ "message": "Request failed", "errors": [ "{\"message\":\"Запись не найдена\", \"errors\":[\"No row was found when one was required\"]}" ] }`
`422`	`Validation Error`	Ошибка валидации	`{ "detail": [ { "loc": [`

Табл. 69. Возможные ошибки при выполнении запроса GET [ip-адрес Комплекса]/API/v1/incidents

HTTP-КОД	ЗНАЧЕНИЕ	ОПИСАНИЕ	ПРИМЕР ТЕЛА ОТВЕТА

			<pre>"string"
			],
			"msg": "string",
			"type": "string"
			}
			]
			}</pre>

19.2.2.3.2. Получение списка доступных статусов инцидентов

19.2.2.3.2.1. Запрос

URL: `GET [ip-адрес Комплекса]/API/v1/incidents/incident_statuses`

Описание: С помощью этой конечной точки пользователь может получить информацию о статусах инцидентов, зарегистрированных в Комплексе.

Пример запроса:

```
curl -i -X GET \
'https://[IP-адрес Комплекса]/API/v1/incidents/incident_statuses?limit=1&offset=0' \
-H 'accept: application/json' \
-H 'X-API-Token: [токен доступа]'
-H 'Content-Type: application/json'
```

Табл. 70. Параметры запроса GET [IP-адрес Комплекса]/API/v1/incidents/incident_statuses

ПОЛЕ	ТИП	ОПИСАНИЕ
`offset`	`integer`	Количество пропускаемых записей
`limit`	`integer`	Максимальное количество записей

19.2.2.3.2.2. Успешный ответ

Код ответа: `200 OK`

Тип содержимого: `application/json`

Пример тела ответа:

```
{
  "total_count": 0,
  "data": [
    {
      "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
      "name": "string",
```

```
      "category": "NEW",
      "custom": true,
      "order": 0,
      "is_used": true
    }
  ]
}
```

Табл. 71. Описание полей ответа на запрос GET [ip-адрес Комплекса]/API/v1/incidents/incident_statuses

ПОЛЕ	ТИП	ОПИСАНИЕ
`total_count`	`string`	Общее количество статусов инцидента
`data`	`array`	Информация о статусе инцидента
`id`	`string`	Идентификатор инцидента
`name`	`string`	Название инцидента
`category`	`string`	Категория инцидента. Доступны следующие значения: • `NEW` — новый инцидент; • `IN_PROGRESS` — инцидент, находящийся в работе; • `COMPLETED` — закрытый инцидент.
`custom`	`boolean`	Признак того, что инцидент имеет пользовательский статус
`order`	`integer`	Порядковый номер
`is_used`	`boolean`	Признак того, что статус используется

Заголовки ответа:

```
 connection: keep-alive
content-encoding: gzip
content-type: application/json
date: Mon,05 May 2025 11:08:01 GMT
public-key-pins: pin-sha256="base64+info1="; max-age=31536000
server: nginx
strict-transport-security: max-age=31536000
transfer-encoding: chunked
```

```
x-content-type-options: nosniff
x-frame-options: DENY
x-xss-protection: 1; mode=block
```

19.2.2.3.2.3. Возможные ошибки

Информация о возможных ошибках представлена в таблице ниже.

Табл. 72. Возможные ошибки при выполнении запроса GET [ip-адрес Комплекса]/API/v1/incidents/incident_statuses

HTTP-КОД	ЗНАЧЕНИЕ	ОПИСАНИЕ	ПРИМЕР ТЕЛА ОТВЕТА
`401`	`Unauthorized`	Ошибка авторизации	`{ "detail": "Could not validate credentials" }`
`403`	`Forbidden`	Ошибка доступа	`{ "detail": "Not authenticated" }`
`422`	`Validation Error`	Ошибка валидации	`{ "detail": [ { "loc": [ "string" ], "msg": "string", "type": "string" } ] }`

19.2.2.3.3. Получение информации об определенном инциденте

19.2.2.3.3.1. Запрос

URL: `GET [ip-адрес Комплекса]/API/v1/incidents/{incident_id}`

Описание: С помощью этой конечной точки пользователь может получить информацию о конкретном инциденте по его идентификатору.

Пример запроса:

```
curl -i -X GET \
'https://[IP-адрес Комплекса]/API/v1/incidents/{incident_id}' \
-H 'accept: application/json' \
-H 'X-API-Token: [токен доступа]'
-H 'Content-Type: application/json'
```

Табл. 73. Параметры запроса GET [IP-адрес Комплекса]/API/v1/incidents/{incident_id}

ПОЛЕ	ТИП	ОПИСАНИЕ
`incident_id`	`string`	Идентификатор инцидента

19.2.2.3.3.2. Успешный ответ

Код ответа: `200 OK`

Тип содержимого: `application/json`

Пример тела ответа:


```
{
  "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
  "status_id": "4e949624-bc0f-439e-a9f2-25a23938812c",
  "name": "string",
  "description": "string",
  "comment": "string",
  "created_at": 0,
  "source_events": [
    "497f6eca-6276-4993-bfeb-53cbbbba6f08"
  ],
  "priority": "LOW",
  "updated_at": 0,
  "status": {
    "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
    "name": "string",
    "category": "NEW",
    "custom": true,
    "order": 0,
    "is_used": true
  },
  "is_confirmed": false,
  "additional_info": {},
  "number": 0,
  "asset_ids": [
    "497f6eca-6276-4993-bfeb-53cbbbba6f08"
  ],
  "user": "string",
  "history": [
    {
      "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
      "incident_id": "2f811c5b-b888-4fb3-aac5-3c6a4b05df32",
      "status": "string",
      "is_confirmed": true,
      "priority": "LOW",
      "created_at": 0,
```

```
      "user": "string",
      "comment": "string",
      "status_id": "4e949624-bc0f-439e-a9f2-25a23938812c"
    }
  ],
  "type": "current",
  "retro_entry_id": "f17716a7-60a9-44e0-ad4f-1bddec028d1d",
  "source_appliances_ids": [
    "string"
  ]
}
```


Табл. 74. Описание полей ответа на запрос GET [IP-адрес Комплекса]/API/v1/incidents/{incident_id}

ПОЛЕ	ТИП	ОПИСАНИЕ
`id`	`string`	Идентификатор инцидента
`status_id`	`string`	Идентификатор статуса
`name`	`string`	Название инцидента
`description`	`string`	Описание инцидента
`comment`	`string`	Комментарий к инциденту
`created_at`	`number`	Дата и время создания инцидента
`source_events`	`array`	Источники событий
`priority`	`string`	Приоритет. Доступны следующие значения: • `LOW` — низкий приоритет; • `MEDIUM` — средний приоритет. Данное значение установлено значением по умолчанию; • `HIGH` — высокий приоритет; • `CRITICAL` — критический приоритет.
`updated_at`	`number`	Дата и время обновления инцидента
`status`	`object`	Статус инцидента

Табл. 74. Описание полей ответа на запрос GET [IP-адрес Комплекса]/API/v1/incidents/{incident_id}

ПОЛЕ	ТИП	ОПИСАНИЕ
`id`	`string`	Идентификатор статуса
`name`	`string`	Название статуса
`category`	`string`	Категория инцидента. Доступны следующие значения: • `NEW` — новый инцидент; • `IN_PROGRESS` — инцидент, находящийся в работе; • `COMPLETED` — закрытый инцидент.
`custom`	`boolean`	Признак того, что инцидент имеет пользовательский статус
`order`	`integer`	Порядковый номер
`is_used`	`boolean`	Признак того, что статус используется
`is_confirmed`	`boolean`	Признак того, что инцидент подтвержден
`additional_info`	`object`	Дополнительная информация
`number`	`integer`	Номер инцидента
`asset_ids`	`array`	Идентификаторы активов
`user`	`string`	Пользователь, ответственный за работу с инцидентом
`history`	`array`	История инцидента
`id`	`string`	Идентификатор
`incident_id`	`string`	Идентификатор инцидента
`status`	`string`	Статус инцидента
`is_confirmed`	`boolean`	Признак того, что инцидент подтвержден

Табл. 74. Описание полей ответа на запрос GET [IP-адрес Комплекса]/API/v1/incidents/{incident_id}

ПОЛЕ	ТИП	ОПИСАНИЕ
`priority`	`string`	Приоритет. Доступны следующие значения: • `LOW` — низкий приоритет; • `MEDIUM` — средний приоритет.; • `HIGH` — высокий приоритет; • `CRITICAL` — критический приоритет.
`created_at`	`integer`	Дата и время создания инцидента
`user`	`string`	Пользователь, ответственный за работу с инцидентом
`comment`	`string`	Комментарий
`status_id`	`string`	Идентификатор статуса
`type`	`string`	Тип инцидента. Доступны следующие значения: • `current` — инцидент, выявленный в процессе работы Комплекса; • `retro` — инцидент, выявленный в ходе ретроспективной проверки.
`retro_entry_id`	`string`	Идентификаторы ретроспективных проверок
`source_appliances_ids`	`array`	Идентификаторы источников

Заголовки ответа:

```
 connection: keep-alive
content-encoding: gzip
content-type: application/json
date: Mon,05 May 2025 11:08:01 GMT
public-key-pins: pin-sha256="base64+info1="; max-age=31536000
server: nginx
strict-transport-security: max-age=31536000
transfer-encoding: chunked
```

```
x-content-type-options: nosniff
x-frame-options: DENY
x-xss-protection: 1; mode=block
```

19.2.2.3.3.3. Возможные ошибки

Информация о возможных ошибках представлена в таблице ниже.

Табл. 75. Возможные ошибки при выполнении запроса GET [ip-адрес Комплекса]/API/v1/incidents/{incident_id}

HTTP-КОД	ЗНАЧЕНИЕ	ОПИСАНИЕ	ПРИМЕР ТЕЛА ОТВЕТА
`401`	`Unauthorized`	Ошибка авторизации	`{ "detail": "Could not validate credentials" }`
`403`	`Forbidden`	Ошибка доступа	`{ "detail": "Not authenticated" }`
`404`	`Not Found`	Запись не найдена	`{ "message": "Request failed", "errors": [ "{\"message\":\"Запись не найдена\",\"errors\":[\"No row was found when one was required\"]}" ] }`
`422`	`Validation Error`	Ошибка валидации	`{ "detail": [ { "loc": [ "string" ], "msg": "string", "type": "string" } ] }`

19.2.2.3.4. Обновление статуса инцидента

19.2.2.3.4.1. Запрос

URL: `PATCH [ip-адрес Комплекса]/API/v1/incidents/incident_statuses/{incident_status_id}`

Описание: С помощью этой конечной точки пользователь может обновить статус инцидента, зарегистрированного в Комплексе, по идентификатору этого инцидента.

Авторизация: Требуется передача заголовка X-API-Token с действительным токеном доступа.

Пример запроса:

```
curl -X 'PATCH' \
'https://[IP-адрес Комплекса]/API/v1/incidents/incident_statuses/{incident_status_id}' \
-H 'accept: application/json' \
-H 'X-API-Token: [токен доступа]' \
-H 'Content-Type: application/json' \
-d '{
  "justification": "string",
  "name": "string",
  "category": "NEW"
}'
```

Табл. 76. Параметры запроса PATCH [ip-адрес Комплекса]/API/v1/incidents/incident_statuses/{incident_status_id}

ПОЛЕ	ТИП	ОПИСАНИЕ
`justification`	`string`	Обоснование изменения статуса инцидента
`name`	`string`	Название инцидента
`category`	`string`	Категория инцидента. Доступны следующие значения: • `NEW` — новый инцидент; • `IN_PROGRESS` — инцидент, находящийся в работе; • `COMPLETED` — закрытый инцидент.

19.2.2.3.4.2. Успешный ответ

Код ответа: `200 OK`

Тип содержимого: `application/json`

Пример тела ответа:

```
{
  "id": "497f6eca-6276-4993-bfeb-53cbbbba6f08",
  "name": "string",
  "category": "NEW",
  "custom": true,
  "order": 0,
```

```
  "is_used": true
}
```

Табл. 77. Описание полей ответа на запрос PATCH [ip-адрес Комплекса]/API/v1/incidents/incident_statuses/{incident_status_id}

ПОЛЕ	ТИП	ОПИСАНИЕ
`id`	`string`	Идентификатор статуса
`name`	`string`	Название статуса
`category`	`string`	Категория инцидента. Доступны следующие значения: • `NEW` — новый инцидент; • `IN_PROGRESS` — инцидент, находящийся в работе; • `COMPLETED` — закрытый инцидент.
`custom`	`boolean`	Признак того, что инцидент имеет пользовательский статус
`order`	`integer`	Порядковый номер
`is_used`	`boolean`	Признак того, что статус используется

Заголовки ответа:

```
connection: keep-alive
content-encoding: gzip
content-type: application/json
strict-transport-security: max-age=31536000
x-content-type-options: nosniff
x-frame-options: DENY
x-xss-protection: 1; mode=block
```

19.2.2.3.4.3. Возможные ошибки

Информация о возможных ошибках представлена в таблице ниже.

Табл. 78. Возможные ошибки при выполнении запроса PATCH [ip-адрес Комплекса]/API/v1/incidents/incident_statuses/{incident_status_id}

HTTP-КОД	ЗНАЧЕНИЕ	ОПИСАНИЕ	ПРИМЕР ТЕЛА ОТВЕТА
`401`	`Unauthorized`	Ошибка авторизации	`{ "detail": "Could not validate credentials" }`
`403`	`Forbidden`	Ошибка доступа	`{ "detail": "Not authenticated" }`
`404`	`Not Found`	Запись не найдена	`{ "message": "Request failed", "errors": [ "{\"message\":\"Запись не найдена\", \"errors\":[\"No row was found when one was required\"]}" ] }`
`422`	`Validation Error`	Ошибка валидации	`{ "detail": [ { "loc": [ "string" ], "msg": "string", "type": "string" } ] }`

19.2.2.4. Информация о Комплексе

Для получения информации о Комплексе доступны следующие конечные точки:

- `GET [ip-адрес Комплекса]/API/v1/about` — конечная точка для получения информации о производителе и версии текущего Комплекса уровня Management;
- `GET [ip-адрес Комплекса]/API/v1/about/installation_info` — конечная точка для получения сетевой информации о Комплексе уровня Management.

19.2.2.4.1. Получение информации о Комплексе

19.2.2.4.1.1. Запрос

URL: `GET [IP-адрес Комплекса]/API/v1/about`

Описание: С помощью этой конечной точки пользователь может получить следующую информацию о Комплексе:

- поставщик Комплекса;
- название Комплекса;
- версия Комплекса.

Пример запроса:

```
curl -i -X GET \
'https://[IP-адрес Комплекса]/API/v1/about' \
-H 'accept: application/json' \
-H 'X-API-Token: [токен доступа]'
-H 'Content-Type: application/json'
```

19.2.2.4.1.2. Успешный ответ

Код ответа: `200 OK`

Тип содержимого: `application/json`

Пример тела ответа:

```
{
  "vendor": "string",
  "name": "CyberLympha DATAPK",
  "version": "string"
}
```

Табл. 79. Описание полей ответа на запрос GET [IP-адрес Комплекса]/API/v1/about

ПОЛЕ	ТИП	ОПИСАНИЕ
`vendor`	`string`	Поставщик продукта
`name`	`string`	Название Комплекса
`version`	`string`	Версия Комплекса

Заголовки ответа:

```
 connection: keep-alive
content-encoding: gzip
content-type: application/json
date: Mon,05 May 2025 11:08:01 GMT
public-key-pins: pin-sha256="base64+info1="; max-age=31536000
server: nginx
strict-transport-security: max-age=31536000
```

```
transfer-encoding: chunked
x-content-type-options: nosniff
x-frame-options: DENY
x-xss-protection: 1; mode=block
```

19.2.2.4.1.3. Возможные ошибки

Информация о возможных ошибках представлена в таблице ниже.

Табл. 80. Возможные ошибки при выполнении запроса GET [IP-адрес Комплекса]/API/v1/about

HTTP-КОД	ЗНАЧЕНИЕ	ОПИСАНИЕ	ПРИМЕР ТЕЛА ОТВЕТА
`401`	`Unauthorized`	Ошибка авторизации	`{ "detail": "Could not validate credentials" }`
`403`	`Forbidden`	Ошибка доступа	`{ "detail": "Not authenticated" }`
`404`	`Not Found`	Запись не найдена	`{ "message": "Request failed", "errors": [ "{\"message\":\"Запись не найдена\", \"errors\":[\"No row was found when one was required\"]}" ] }`
`422`	`Validation Error`	Ошибка валидации	`{ "detail": [ { "loc": [ "string" ], "msg": "string", "type": "string" } ] }`

19.2.2.4.2. Получение сетевой информации о Комплексе

19.2.2.4.2.1. Запрос

URL: `GET [ip-адрес Комплекса]/API/v1/about/installation_info`

Описание: С помощью этой конечной точки пользователь может получить основную сетевую информацию о Комплексе.

Пример запроса:

```
curl -i -X GET \
'https://[IP-адрес Комплекса]/API/v1/about/installation_info' \
-H 'accept: application/json' \
-H 'X-API-Token: [токен доступа]'
-H 'Content-Type: application/json'
```

19.2.2.4.2.2. Успешный ответ

Код ответа: `200 OK`

Тип содержимого: `application/json`

Пример тела ответа:

```
{
  "id": "string",
  "hostname": "string",
  "ip": "string",
  "mac": "string"
}
```

Табл. 81. Описание полей ответа на запрос GET [IP-адрес Комплекса]/API/v1/about/installation_info

ПОЛЕ	ТИП	ОПИСАНИЕ
`id`	`string`	Идентификатор виртуальной машины
`hostname`	`string`	Название хоста
`ip`	`string`	IP-адрес Комплекса
`mac`	`boolean`	MAC-адрес Комплекса

Заголовки ответа:

```
 connection: keep-alive
content-encoding: gzip
content-type: application/json
date: Mon,05 May 2025 11:08:01 GMT
public-key-pins: pin-sha256="base64+info1="; max-age=31536000
server: nginx
strict-transport-security: max-age=31536000
transfer-encoding: chunked
x-content-type-options: nosniff
x-frame-options: DENY
x-xss-protection: 1; mode=block
```

19.2.2.4.2.3. Возможные ошибки

Информация о возможных ошибках представлена в таблице ниже.

Табл. 82. Возможные ошибки при выполнении запроса GET [ip-адрес Комплекса]/API/v1/about/installation_info

HTTP-КОД	ЗНАЧЕНИЕ	ОПИСАНИЕ	ПРИМЕР ТЕЛА ОТВЕТА
`401`	`Unauthorized`	Ошибка авторизации	`{ "detail": "Could not validate credentials" }`
`403`	`Forbidden`	Ошибка доступа	`{ "detail": "Not authenticated" }`
`404`	`Not Found`	Запись не найдена	`{ "message": "Request failed", "errors": [ "{\"message\":\"Запись не найдена\", \"errors\":[\"No row was found when one was required\"]}" ] }`
`422`	`Validation Error`	Ошибка валидации	`{ "detail": [ { "loc": [ "string" ], "msg": "string", "type": "string" } ] }`

19.2.2.5. Конфигурации

Для выполнения операций с конфигурациями и получения списка установленного ПО доступны следующие конечные точки:

- `GET [ip-адрес Комплекса]/API/v1/configs` — конечная точка для получения информации обо всех полученных конфигурациях;
- `GET [ip-адрес Комплекса]/API/v1/configs/{config_id}` — конечная точка для получения информации о конфигурации по ее идентификатору;

- `POST [ip-адрес Комплекса]/API/v1/configs/{config_id}/reference` — конечная точка для установки конфигурации в качестве эталонной;
- `GET [ip-адрес Комплекса]/API/v1/configurations/software` — конечная точка для получения списка установленного ПО выбранных активов.

19.2.2.5.1. Получение информации обо всех конфигурациях

19.2.2.5.1.1. Запрос

URL: `GET [ip-адрес Комплекса]/API/v1/configs`

Описание: С помощью этой конечной точки пользователь может получить информацию обо всех конфигурациях, собранных Комплексом за определенное время.

Авторизация: Требуется передача заголовка X-API-Token с действительным токеном доступа.

Табл. 83. Параметры запроса GET [IP-адрес Комплекса]/API/v1/configs

ПОЛЕ	ТИП	ОПИСАНИЕ
`limit`	`integer`	Количество записей
`pagination_last_number`	`integer`	Номер записи, от которой следует начитать отсчет
`sort_field`	`string`	Поле для сортировки конфигурации
`sort_field_last_value`	`number`	Значение поля, по которому выполняется сортировка
`created_at_from`	`number`	Начальное время создания объекта
`created_at_to`	`number`	Конечное время создания объекта
`asset_ids`	`array`	Идентификаторы активов
`scanners_ids`	`array`	Идентификаторы сканеров
`search_text`	`string`	Текст для поиска по конфигурациям
`is_reference`	`boolean`	Конфигурация является эталонной
`last_only`	`boolean`	Только последние конфигурации

Табл. 83. Параметры запроса GET [IP-адрес Комплекса]/API/v1/configs

ПОЛЕ	ТИП	ОПИСАНИЕ
`exclude_fields`	`string`	Поля, которые необходимо исключить

Пример запроса:

```
curl -X 'GET' \
'https://[IP-адрес                                                    Комплекса]/API/v1/configs?
limit=10&pagination_last_number=2&sort_field=collected_at&asset_ids=3fa85f64-5717-4562-
b3fc-2c963f66afa6&is_reference=false&last_only=false \
-H 'accept: application/json' \
-H 'X-API-Token: [токен доступа]'
```

19.2.2.5.1.2. Успешный ответ

Код ответа: `200 OK`

Тип содержимого: `application/json`

Пример тела ответа:

```
{
  "data": [],
  "total_count": 20,
  "filtered_count": 3
}
```

Табл. 84. Описание полей ответа на запрос GET [IP-адрес Комплекса]/API/v1/configs

ПОЛЕ	ТИП	ОПИСАНИЕ
`data`	`array`	Информация о конфигурациях
`id`	`string`	Идентификатор конфигурации
`created_at`	`number`	Дата и время создания задачи сбора конфигурации
`collected_at`	`number`	Дата и время сбора конфигурации
`last_change_by`	`number`	Пользователь, внесший последние изменения
`justification`	`string`	Обоснование внесения изменений

Табл. 84. Описание полей ответа на запрос GET [IP-адрес Комплекса]/API/v1/configs

ПОЛЕ	ТИП	ОПИСАНИЕ
`is_reference`	`boolean`	Конфигурация является эталонной
`reference_last_change_at`	`number`	Дата и время последних изменений эталонной конфигурации
`compliant_with_reference`	`boolean`	Конфигурация совпадает с эталонной
`config_details`	`object`	Подробная информация о конфигурации
`columns`	`array`	Названия столбцов для строк из поля `data`
`column_names`	`object`	Сопоставление ключей из поля `keys` и названия их формата (`[ключ]: [отображаемое название]`)
`config_details`	`array`	Информация о конфигурации
`status`	`string`	Статус конфигурации. Доступные значения: • `EMPTY` — пустая конфигурация. Данное значение установлено по умолчанию; • `IS_REFERENCE` — конфигурация соответствует эталонной; • `NOT_COMPLIANT_WITH_REFERENCE` — конфигурация не соответствует эталонной; • `WAS_NOT_COMPLIANT_WITH_REFERENCE` — ранее конфигурация не соответствовала эталонной.
`asset_id`	`string`	Идентификатор актива
`scanner_id`	`string`	Идентификатор сканера

Табл. 84. Описание полей ответа на запрос GET [IP-адрес Комплекса]/API/v1/configs

ПОЛЕ	ТИП	ОПИСАНИЕ
`pagination_number`	`number`	Номер записи
`total_count`	`integer`	Общее количество конфигураций
`filtered_count`	`integer`	Количество конфигураций, соответствующих указанным параметрам

Заголовки ответа:

```
connection: keep-alive
content-encoding: gzip
content-type: application/json
date: Fri,25 Apr 2025 08:13:20 GMT
public-key-pins: pin-sha256="base64+info1="; max-age=31536000
server: nginx
strict-transport-security: max-age=31536000
transfer-encoding: chunked
x-content-type-options: nosniff
x-frame-options: DENY
x-xss-protection: 1; mode=block
```

19.2.2.5.1.3. Возможные ошибки

Информация о возможных ошибках представлена в таблице ниже.

Табл. 85. Возможные ошибки при выполнении запроса GET [IP-адрес Комплекса]/API/v1/configs

HTTP-КОД	ЗНАЧЕНИЕ	ОПИСАНИЕ	ПРИМЕР ТЕЛА ОТВЕТА
`401`	`Unauthorized`	Ошибка авторизации	`{ "detail": "Could not validate credentials" }`
`403`	`Forbidden`	Ошибка доступа	`{ "detail": "Not authenticated" }`
`422`	`Validation Error`	Ошибка валидации	`{ "detail": [ { "loc": [ "string" ],`

Табл. 85. Возможные ошибки при выполнении запроса GET [IP-адрес Комплекса]/API/v1/configs

HTTP-КОД	ЗНАЧЕНИЕ	ОПИСАНИЕ	ПРИМЕР ТЕЛА ОТВЕТА

			<pre>"msg": "string",
			"type": "string"
			}
			]
			}</pre>

19.2.2.5.2. Получение информации об определенной конфигурации

19.2.2.5.2.1. Запрос

URL: `GET [ip-адрес Комплекса]/API/v1/configs/{config_id}`

Описание: С помощью этой конечной точки пользователь может получить информацию об определенной конфигурации по ее идентификатору.

Авторизация: Требуется передача заголовка X-API-Token с действительным токеном доступа.

Пример запроса:

```
curl -X 'GET' \
  'https://[IP-адрес Комплекса]/API/v1/configs/303ed663-34b9-4df3-a241-0c60f4d8c43e' \
  -H 'accept: application/json' \
  -H 'X-API-Token: [токен доступа]'
```

19.2.2.5.2.2. Успешный ответ

Код ответа: `200 OK`

Тип содержимого: `application/json`

Пример тела ответа:

```
{
    "id": "303ed663-34b9-4df3-a241-0c60f4d8c43e",
    "created_at": 1745568723.995315,
    "collected_at": 1745568723.995326,
    "last_change_by": "string",
    "justification": "string",
    "is_reference": false,
    "reference_last_change_at": 1745568723.995323,
    "compliant_with_reference": false,
    "config_details": {
        "columns": [
            "caption",
            "description",
            "executable_path",
            "name",
            "ProcessID"
        ],
```

```
        "column_names": {
            "name": "Имя",
            "caption": "Заголовок",
            "ProcessID": "Идентификатор процесса",
            "description": "Описание",
            "executable_path": "Исполняемый путь"
        },
        "rows": [
            "System Idle Process",
            "System Idle Process",
            "None",
            "System Idle Process",
            "0"
        ]
    },
    "status": "NON_COMPIANT_WITH_REFERENCE",
    "asset_id": "a53bbac6-90f3-4d93-af42-8df7d328e414",
    "scanner_id": "1ff936a3-b4a1-4c3a-a970-fea876477210",
    "pagination_number": 3213
}
```


Табл. 86. Описание полей ответа на запрос GET [IP-адрес Комплекса]/API/v1/configs/{config_id}

ПОЛЕ	ТИП	ОПИСАНИЕ
`id`	`string`	Идентификатор конфигурации
`created_at`	`number`	Дата и время создания задачи сбора конфигурации
`collected_at`	`number`	Дата и время сбора конфигурации
`last_change_by`	`number`	Пользователь, внесший последние изменения
`justification`	`string`	Обоснование внесения изменений
`is_reference`	`boolean`	Конфигурация является эталонной
`reference_last_change_at`	`number`	Дата и время последних изменений эталонной конфигурации

Табл. 86. Описание полей ответа на запрос GET [IP-адрес Комплекса]/API/v1/configs/{config_id}

ПОЛЕ	ТИП	ОПИСАНИЕ
`compliant_with_reference`	`boolean`	Конфигурация совпадает с эталонной
`config_details`	`array`	Данные конфигурации
`columns`	`array`	Колонки таблицы
`column_names`	`array`	Названия колонок таблицы
`rows`	`array`	Значения в строках таблицы, соответствующие колонкам
`status`	`string`	Статус конфигурации. Доступные значения: • `EMPTY` — пустая конфигурация. Данное значение установлено по умолчанию; • `IS_REFERENCE` — конфигурация соответствует эталонной; • `NOT_COMPLIANT_WITH_REFERENCE` — конфигурация не соответствует эталонной; • `WAS_NOT_COMPLIANT_WITH_REFERENCE` — ранее конфигурация не соответствовала эталонной.
`asset_id`	`string`	Идентификатор актива
`scanner_id`	`string`	Идентификатор сканера
`pagination_number`	`number`	Номер записи

Заголовки ответа:

```
connection: keep-alive
content-encoding: gzip
content-type: application/json
strict-transport-security: max-age=31536000
x-content-type-options: nosniff
x-frame-options: DENY
x-xss-protection: 1; mode=block
```

19.2.2.5.2.3. Возможные ошибки

Информация о возможных ошибках представлена в таблице ниже.

Табл. 87. Возможные ошибки при выполнении запроса GET [ip-адрес Комплекса]/API/v1/configs/{config_id}

HTTP-КОД	ЗНАЧЕНИЕ	ОПИСАНИЕ	ПРИМЕР ТЕЛА ОТВЕТА
`401`	`Unauthorized`	Ошибка авторизации	`{ "detail": "Could not validate credentials" }`
`403`	`Forbidden`	Ошибка доступа	`{ "detail": "Not authenticated" }`
`404`	`Not Found`	Запись не найдена	`{ "message": "Request failed", "errors": [ "{\"message\":\"Запись не найдена\", \"errors\":[\"No row was found when one was required\"]}" ] }`
`422`	`Validation Error`	Ошибка валидации	`{ "detail": [ { "loc": [ "string" ], "msg": "string", "type": "string" } ] }`

19.2.2.5.3. Установка конфигурации в качестве эталонной

19.2.2.5.3.1. Запрос

URL: `POST [ip-адрес Комплекса]/API/v1/configs/{config_id}/reference`

Описание: С помощью этой конечной точки пользователь может установить выбранную конфигурацию в качестве эталонной.

Авторизация: Требуется передача заголовка X-API-Token с действительным токеном доступа.

Табл. 88. Параметры запроса

ПОЛЕ	ТИП	ОПИСАНИЕ
`config_id`	`string`	Идентификатор конфигурации

Пример запроса:

```
curl -X 'POST' \
'https://[IP-адрес Комплекса]/API/v1/configs/3fa85f64-5717-4562-b3fc-2c963f66afa6/reference' \
-H 'accept: application/json' \
-H 'X-API-Token: [токен доступа]' \
-H 'Content-Type: application/json' \
-d '{
  "justification": "string"
}'
```

Табл. 89. Параметры запроса POST [IP-адрес Комплекса]/API/v1/configs/{config_id}/reference

ПОЛЕ	ТИП	ОПИСАНИЕ
`justification`	`string`	Обоснование для установки конфигурации в качестве эталонной

19.2.2.5.3.2. Успешный ответ

Код ответа: `200 OK`

Тип содержимого: `application/json`

Пример тела ответа:

```
{
  "id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
  "created_at": 1745568723.995315,
  "collected_at": 1745568723.995326,
  "last_change_by": "string",
  "justification": "string",
  "is_reference": true,
  "reference_last_change_at": 1745568723.995323,
  "compliant_with_reference": true,
  "config_details": {
      "columns": [
          "caption",
          "description",
          "executable_path",
          "name",
          "ProcessID"
      ],
      "column_names": {
          "name": "Имя",
```

```
            "caption": "Заголовок",
            "ProcessID": "Идентификатор процесса",
            "description": "Описание",
            "executable_path": "Исполняемый путь"
        },
        "rows": [
            "System Idle Process",
            "System Idle Process",
            "None",
            "System Idle Process",
            "0"
        ]
      },
  "status": "NON_COMPIANT_WITH_REFERENCE",
  "asset_id": "a53bbac6-90f3-4d93-af42-8df7d328e414",
  "scanner_id": "1ff936a3-b4a1-4c3a-a970-fea876477210",
  "pagination_number": 3213
}
```


Табл. 90. Описание полей ответа на запрос POST [ip-адрес Комплекса]/API/v1/configs/{config_id}/reference

ПОЛЕ	ТИП	ОПИСАНИЕ
`id`	`string`	Идентификатор конфигурации
`created_at`	`number`	Дата и время создания задачи сбора конфигурации
`collected_at`	`number`	Дата и время сбора конфигурации
`last_change_by`	`number`	Пользователь, внесший последние изменения
`justification`	`string`	Обоснование внесения изменений
`is_reference`	`boolean`	Конфигурация является эталонной
`reference_last_change_at`	`number`	Дата и время последних изменений эталонной конфигурации
`compliant_with_reference`	`boolean`	Конфигурация совпадает с эталонной

Табл. 90. Описание полей ответа на запрос POST [ip-адрес Комплекса]/API/v1/configs/{config_id}/reference

ПОЛЕ	ТИП	ОПИСАНИЕ
`config_details`	`array`	Данные конфигурации
`columns`	`array`	Колонки таблицы
`column_names`	`array`	Названия колонок таблицы
`rows`	`array`	Значения в строках таблицы, соответствующие колонкам
`status`	`string`	Статус конфигурации. Доступные значения: • `EMPTY` — пустая конфигурация. Данное значение установлено по умолчанию; • `IS_REFERENCE` — конфигурация соответствует эталонной; • `NOT_COMPLIANT_WITH_REFERENCE` — конфигурация не соответствует эталонной; • `WAS_NOT_COMPLIANT_WITH_REFERENCE` — ранее конфигурация не соответствовала эталонной.
`asset_id`	`string`	Идентификатор актива
`scanner_id`	`string`	Идентификатор сканера
`pagination_number`	`number`	Номер записи

Заголовки ответа:

```
connection: keep-alive
content-encoding: gzip
content-type: application/json
strict-transport-security: max-age=31536000
x-content-type-options: nosniff
x-frame-options: DENY
x-xss-protection: 1; mode=block
```

19.2.2.5.3.3. Возможные ошибки

Информация о возможных ошибках представлена в таблице ниже.

Табл. 91. Возможные ошибки при выполнении запроса POST [ip-адрес Комплекса]/API/v1/configs/{config_id}/reference

HTTP-КОД	ЗНАЧЕНИЕ	ОПИСАНИЕ	ПРИМЕР ТЕЛА ОТВЕТА
`401`	`Unauthorized`	Ошибка авторизации	`{ "detail": "Could not validate credentials" }`
`403`	`Forbidden`	Ошибка доступа	`{ "detail": "Not authenticated" }`
`404`	`Not Found`	Запись не найдена	`{ "message": "Request failed", "errors": [ "{\"message\":\"Запись не найдена\", \"errors\":[\"No row was found when one was required\"]}" ] }`
`422`	`Validation Error`	Ошибка валидации	`{ "detail": [ { "loc": [ "string" ], "msg": "string", "type": "string" } ] }`

19.2.2.5.4. Получение списка установленного ПО указанных активов

19.2.2.5.4.1. Запрос

URL: `GET [ip-адрес Комплекса]/API/v1/configurations/software`

Описание: С помощью этой конечной точки пользователь может получить список ПО, установленного на определенных активах.

Авторизация: Требуется передача заголовка X-API-Token с действительным токеном доступа.

Пример запроса:

```
curl -X 'GET' \
'https://[IP-адрес Комплекса]/API/v1/configurations/software' \
```

```
-H 'accept: application/json' \
-H 'X-API-Token: [токен доступа]'
-d '{
  "number_for_pagination": 0,
  "updated_at_for_pagination": 0,
  "limit": 1000,
  "updated_at_from": 0,
  "updated_at_to": 0,
  "created_at_from": 0,
  "created_at_to": 0,
  "vendor_search": "string",
  "product_search": "string",
  "version_search": "string",
  "asset_ids": [
    "3fa85f64-5717-4562-b3fc-2c963f66afa6"
  ]
}'
```

Табл. 92. Параметры запроса GET [IP-адрес Комплекса]/API/v1/configurations/software

ПОЛЕ	ТИП	ОПИСАНИЕ
`number_for_pagination`	`number`	Номер последней записи на странице
`updated_at_for_pagination`	`number`	Время обновления последней записи на странице
`limit`	`integer`	Максимальное количество записей
`updated_at_from`	`number`	Начальное время обновления
`updated_at_to`	`number`	Конечное время обновления
`created_at_from`	`number`	Начальное время создания
`created_at_to`	`number`	Начальное время создания
`vendor_search`	`string`	Поиск по поставщику
`product_search`	`string`	Поиск по продукту
`version_search`	`string`	Поиск по версии
`asset_ids`	`array`	Идентификаторы активов

19.2.2.5.4.2. Успешный ответ

Код ответа: `200 OK`

Тип содержимого: `application/json`

Пример тела ответа:

```
{
  "data": [],
  "total_count": 20,
  "filtered_count": 3
}
```

Табл. 93. Описание полей ответа на запрос GET [IP-адрес Комплекса]/API/v1/configurations/software

ПОЛЕ	ТИП	ОПИСАНИЕ
`data`	`array`	Информация о собранном ПО
`id`	`string`	Идентификатор актива
`created_at`	`number`	Дата создания
`updated_at`	`number`	Дата обновления
`host_id`	`string`	Идентификатор сенсора
`number`	`integer`	Номер
`vendor`	`string`	Поставщик
`product`	`string`	Продукт
`version`	`string`	Версия
`update`	`string`	Обновление
`edition`	`string`	Версия продукта
`sw_edition`	`string`	Версия ПО
`target_sw`	`string`	Требуемое ПО
`total_count`	`integer`	Общее количество активов, на которых был собран список ПО
`filtered_count`	`integer`	Количество активов, соответствующих указанным параметрам

Заголовки ответа:

```
connection: keep-alive
content-encoding: gzip
content-type: application/json
strict-transport-security: max-age=31536000
x-content-type-options: nosniff
x-frame-options: DENY
x-xss-protection: 1; mode=block
```

19.2.2.5.4.3. Возможные ошибки

Информация о возможных ошибках представлена в таблице ниже.

Табл. 94. Возможные ошибки при выполнении запроса GET [ip-адрес Комплекса]/API/v1/configurations/software

HTTP-КОД	ЗНАЧЕНИЕ	ОПИСАНИЕ	ПРИМЕР ТЕЛА ОТВЕТА
`401`	`Unauthorized`	Ошибка авторизации	`{ "detail": "Could not validate credentials" }`
`403`	`Forbidden`	Ошибка доступа	`{ "detail": "Not authenticated" }`
`404`	`Not Found`	Запись не найдена	`{ "message": "Request failed", "errors": [ "{\"message\":\"Запись не найдена\",\"errors\":[\"No row was found when one was required\"]}" ] }`
`422`	`Validation Error`	Ошибка валидации	`{ "detail": [ { "loc": [ "string" ], "msg": "string", "type": "string" } ] }`

19.2.2.6. Сенсоры

Для выполнения операций с сенсорами доступны следующие конечные точки:

- `GET [ip-адрес Комплекса]/API/v1/sensors` — конечная точка для получения списка подключенных сенсоров и их базовых параметров;
- `GET [ip-адрес Комплекса]/API/v1/sensors/home_networks` — конечная точка для получения списка контролируемых сетей подключенных сенсоров;
- `PUT [ip-адрес Комплекса]/API/v1/sensors/home_networks/{sensor_id}` — конечная точка для обновления списка контролируемых сетей для определенного сенсора по его идентификатору.

19.2.2.6.1. Получение информации о сенсорах и их параметрах

19.2.2.6.1.1. Запрос

URL: `GET [ip-адрес Комплекса]/API/v1/sensors`

Описание: С помощью этой конечной точки пользователь может получить информацию о сенсорах, зарегистрированных на Комплексе.

Пример запроса:

```
curl -i -X GET \
'https://[IP-адрес Комплекса]/API/v1/sensors' \
-H 'accept: application/json' \
-H 'X-API-Token: [токен доступа]'
-H 'Content-Type: application/json'
```

19.2.2.6.1.2. Успешный ответ

Код ответа: `200 OK`

Тип содержимого: `application/json`

Пример тела ответа:

```
[
  {
    "comment": "string",
    "company": "string",
    "location": "string",
    "hostname": "string",
    "last_availability_time": 0,
    "sensor_id": "string"
  }
]
```

Табл. 95. Описание полей ответа на запрос GET [IP-адрес Комплекса]/API/v1/sensors

ПОЛЕ	ТИП	ОПИСАНИЕ
`comment`	`string`	Комментарий

Табл. 95. Описание полей ответа на запрос GET [IP-адрес Комплекса]/API/v1/sensors

ПОЛЕ	ТИП	ОПИСАНИЕ
`company`	`string`	Эксплуатирующая организация
`location`	`string`	Место установки сенсора
`hostname`	`string`	Название хоста
`last_availability_time`	`number`	Дата и время последней доступности сенсора
`sensor_id`	`string`	Идентификатор сенсора

Заголовки ответа:

```
 connection: keep-alive
content-encoding: gzip
content-type: application/json
date: Mon,05 May 2025 11:08:01 GMT
public-key-pins: pin-sha256="base64+info1="; max-age=31536000
server: nginx
strict-transport-security: max-age=31536000
transfer-encoding: chunked
x-content-type-options: nosniff
x-frame-options: DENY
x-xss-protection: 1; mode=block
```

19.2.2.6.1.3. Возможные ошибки

Информация о возможных ошибках представлена в таблице ниже.

Табл. 96. Возможные ошибки при выполнении запроса GET [IP-адрес Комплекса]/API/v1/sensors

HTTP-КОД	ЗНАЧЕНИЕ	ОПИСАНИЕ	ПРИМЕР ТЕЛА ОТВЕТА
`401`	`Unauthorized`	Ошибка авторизации	`{ "detail": "Could not validate credentials" }`
`403`	`Forbidden`	Ошибка доступа	`{ "detail": "Not authenticated" }`
`404`	`Not Found`	Запись не найдена	`{ "message": "Request failed", "errors": [`

Табл. 96. Возможные ошибки при выполнении запроса GET [IP-адрес Комплекса]/API/v1/sensors

HTTP-КОД	ЗНАЧЕНИЕ	ОПИСАНИЕ	ПРИМЕР ТЕЛА ОТВЕТА
			"{\"message\":\"Запись не найдена\", \"errors\":[\"No row was found when one was required\"]}"] }
422	Validation Error	Ошибка валидации	{ "detail": [{ "loc": ["string"], "msg": "string", "type": "string" }] }

19.2.2.6.2. Получение списка контролируемых сетей, связанных с сенсором

19.2.2.6.2.1. Запрос

URL: `GET [ip-адрес Комплекса]/API/v1/sensors/home_networks`

Описание: С помощью этой конечной точки пользователь может получить информацию о контролируемой сети сенсора.

Пример запроса:

```
curl -i -X GET \
'https://[IP-адрес Комплекса]/API/v1/sensors/home_networks' \
-H 'accept: application/json' \
-H 'X-API-Token: [токен доступа]'
-H 'Content-Type: application/json'
```

19.2.2.6.2.2. Успешный ответ

Код ответа: `200 OK`

Тип содержимого: `application/json`

Пример тела ответа:

```
[
  {
    "networks": [
      "string"
    ],
```

```
    "sensor_id": "string"
  }
]
```

Табл. 97. Описание полей ответа на запрос GET [IP-адрес Комплекса]/API/v1/sensors/home_networks

ПОЛЕ	ТИП	ОПИСАНИЕ
`networks`	`array`	Массив контролируемых подсетей сенсора
`sensor_id`	`string`	Идентификатор сенсора

Заголовки ответа:

```
connection: keep-alive
content-encoding: gzip
content-type: application/json
date: Mon,05 May 2025 11:08:01 GMT
public-key-pins: pin-sha256="base64+info1="; max-age=31536000
server: nginx
strict-transport-security: max-age=31536000
transfer-encoding: chunked
x-content-type-options: nosniff
x-frame-options: DENY
x-xss-protection: 1; mode=block
```

19.2.2.6.2.3. Возможные ошибки

Информация о возможных ошибках представлена в таблице ниже.

Табл. 98. Возможные ошибки при выполнении запроса GET [ip-адрес Комплекса]/API/v1/sensors/home_networks

HTTP-КОД	ЗНАЧЕНИЕ	ОПИСАНИЕ	ПРИМЕР ТЕЛА ОТВЕТА
`401`	`Unauthorized`	Ошибка авторизации	`{ "detail": "Could not validate credentials" }`
`403`	`Forbidden`	Ошибка доступа	`{ "detail": "Not authenticated" }`
`404`	`Not Found`	Запись не найдена	`{ "message": "Request failed", "errors": [`

Табл. 98. Возможные ошибки при выполнении запроса GET [ip-адрес Комплекса]/API/v1/sensors/home_networks

HTTP-КОД	ЗНАЧЕНИЕ	ОПИСАНИЕ	ПРИМЕР ТЕЛА ОТВЕТА

			`"{\"message\":\"Запись не найдена\",\"errors\":[\"No row was found when one was required\"]}"`
			`]`
			`}`

`422`	`Validation Error`	Ошибка валидации	`{`
			`"detail": [`
			`{`
			`"loc": [`
			`"string"`
			`],`
			`"msg": "string",`
			`"type": "string"`
			`}`
			`]`
			`}`

19.2.2.6.3. Обновление списка контролируемых сетей

19.2.2.6.3.1. Запрос

URL: `PUT [ip-адрес Комплекса]/API/v1/sensors/home_networks/{sensor_id}`

Описание: С помощью этой конечной точки пользователь может обновить контролируемую сеть сенсора по его идентификатору.

Авторизация: Требуется передача заголовка X-API-Token с действительным токеном доступа.

Пример запроса:

```
curl -X 'PUT' \
'https://[IP-адрес Комплекса]/API/v1/sensors/home_networks/{sensor_id}' \
-H 'accept: application/json' \
-H 'X-API-Token: [токен доступа]' \
-H 'Content-Type: application/json' \
-d '{
  "networks": [
    "string"
  ]
}'
```

Табл. 99. Параметры запроса PUT [ip-адрес Комплекса]/API/v1/sensors/home_networks/{sensor_id}

ПОЛЕ	ТИП	ОПИСАНИЕ
`networks`	`array`	Массив контролируемых подсетей сенсора

19.2.2.6.3.2. Успешный ответ

Код ответа: `200 OK`

Тип содержимого: `application/json`

Пример тела ответа:

```
{
  "networks": [
    "string"
  ],
  "sensor_id": "string"
}
```

Табл. 100. Описание полей ответа на запрос PUT [ip-адрес Комплекса]/API/v1/sensors/home_networks/{sensor_id}

ПОЛЕ	ТИП	ОПИСАНИЕ
`networks`	`array`	Массив контролируемых подсетей сенсора
`sensor_id`	`string`	Идентификатор сенсора

Заголовки ответа:

```
connection: keep-alive
content-encoding: gzip
content-type: application/json
strict-transport-security: max-age=31536000
x-content-type-options: nosniff
x-frame-options: DENY
x-xss-protection: 1; mode=block
```

19.2.2.6.3.3. Возможные ошибки

Информация о возможных ошибках представлена в таблице ниже.

Табл. 101. Возможные ошибки при выполнении запроса PUT [ip-адрес Комплекса]/API/v1/sensors/home_networks/{sensor_id}

HTTP-КОД	ЗНАЧЕНИЕ	ОПИСАНИЕ	ПРИМЕР ТЕЛА ОТВЕТА
`401`	`Unauthorized`	Ошибка авторизации	`{ "detail": "Could not validate credentials" }`
`403`	`Forbidden`	Ошибка доступа	`{ "detail": "Not authenticated" }`
`404`	`Not Found`	Запись не найдена	`{ "message": "Request failed", "errors": [ "{\"message\":\"Запись не найдена\", \"errors\":[\"No row was found when one was required\"]}" ] }`
`422`	`Validation Error`	Ошибка валидации	`{ "detail": [ { "loc": [ "string" ], "msg": "string", "type": "string" } ] }`

19.2.2.7. Сессии

Для выполнения операций с сессиями доступны следующие конечные точки:

- `GET [ip-адрес Комплекса]/API/v1/network_sessions` — конечная точка для получения информации о выбранных сессиях;
- `GET [ip-адрес Комплекса]/API/v1/dpi_protocols` — конечная точка для получения списка всех протоколов, обнаруженных в сетевом трафике;
- `GET [ip-адрес Комплекса]/API/v1/network_sessions/network_session_rules` — конечная точка для получения списка правил сессий;
- `GET [ip-адрес Комплекса]/API/v1/network_sessions/process_control_rules` — конечная точка для получения списка правил контроля тегов.

19.2.2.7.1. Получение информации о сетевых соединениях

19.2.2.7.1.1. Запрос

URL: `GET [ip-адрес Комплекса]/API/v1/network_sessions`

Описание: С помощью этой конечной точки пользователь может получить информацию о сетевых соединениях, регистрируемых Комплексом.

Пример запроса:

```
curl -i -X GET \
'https://[IP-адрес                                    Комплекса]/API/v1/network_sessions?
limit=1000&offset=0&sort=created_time&sort_type=asc&count_response_entities=false' \
-H 'accept: application/json' \
-H 'X-API-Token: [токен доступа]'
-d '{
  "created_time_from": number,
  "created_time_to": number,
  "ids": "string",
  "statuses": "string",
  "transport_protocols": "string",
  "protocols": array,
  "is_active": boolean,
  "source_hostnames": "string",
  "target_hostnames": "string",
  "source_ips": array,
  "target_ips": array,
  "source_macs": array,
  "target_macs": array,
  "source_ports": array,
  "target_ports": array,
  "sensor_names": "string",
  "sensor_ids": "string",
  "limit": integer,
  "offset": integer,
  "sort": "string",
  "sort_type": "string",
  "count_response_entities": boolean
}'
```

Табл. 102. Параметры запроса GET [IP-адрес Комплекса]/API/v1/network_sessions

ПОЛЕ	ТИП	ОПИСАНИЕ
`created_time_from`	`number`	Начальное время регистрации сетевого соединения
`created_time_to`	`number`	Конечное время регистрации сетевого соединения

Табл. 102. Параметры запроса GET [IP-адрес Комплекса]/API/v1/network_sessions

ПОЛЕ	ТИП	ОПИСАНИЕ
`ids`	`string`	Идентификаторы сетевых соединений
`statuses`	`string`	Статусы сетевых соединений. Доступны следующие значения: • `APPROVED` — сетевое соединение разрешено; • `NOT_APPROVED` — сетевое соединение не разрешено; • `NOT_DEFINED` — сетевое соединение не определено.
`transport_protocols`	`string`	Транспортный протокол. Доступны следующие значения: • `icmp`; • `tcp`; • `udp`.
`protocols`	`array`	Протоколы
`is_active`	`boolean`	Признак активности сетевого соединения
`source_hostnames`	`string`	Сеть отправителя
`target_hostnames`	`string`	Сеть получателя
`source_ips`	`array`	IP-адреса отправителя
`target_ips`	`array`	IP-адреса получателя
`source_macs`	`array`	MAC-адреса отправителя
`target_macs`	`array`	MAC-адреса получателя
`source_ports`	`array`	Порты отправителя
`target_ports`	`array`	Порты получателя
`sensor_names`	`string`	Названия сенсоров
`sensor_ids`	`string`	Идентификаторы сенсоров

Табл. 102. Параметры запроса GET [IP-адрес Комплекса]/API/v1/network_sessions

ПОЛЕ	ТИП	ОПИСАНИЕ
`limit`	`integer`	Максимальное количество записей
`offset`	`integer`	Количество пропускаемых записей
`sort`	`string`	Поле, по которому выполняется сортировка данных. Доступны следующие значения: • `created_time` — время создания. Данное значение установлено значением по умолчанию; • `detected_time` — время обнаружения; • `files_detected` — файлов обнаружено; • `packets_sent` — отправлено пакетов; • `packets_received` — получено пакетов.
`sort_type`	`string`	Направление сортировки. Доступны следующие значения: • `asc` — по возрастанию. Данное значение установлено значением по умолчанию; • `desc` — по убыванию.
`count_response_entities`	`boolean`	Параметр, отвечающий за отображение счетчиков количества записей

19.2.2.7.1.2. Успешный ответ

Код ответа: `200 OK`

Тип содержимого: `application/json`

Пример тела ответа:

```
{
  "data": [
```

```
    {
      "id": "string",
      "category": "string",
      "state": "OTH",
      "created_time": 0,
      "detected_time": 0,
      "status": "APPROVED",
      "transport_protocol": "icmp",
      "protocols": [
        "string"
      ],
      "duration": 0,
      "files_detected": 0,
      "vlan": 0,
      "is_active": true,
      "source_host_id": "string",
      "target_host_id": "string",
      "source_hostname": "string",
      "target_hostname": "string",
      "source_network_is_local": "string",
      "target_network_is_local": "string",
      "source_network_is_controlled": "string",
      "target_network_is_controlled": "string",
      "source_ip": "198.51.100.42",
      "target_ip": "198.51.100.42",
      "source_mac": "string",
      "target_mac": "string",
      "source_port": 0,
      "target_port": 0,
      "bytes_sent": 0,
      "bytes_received": 0,
      "packets_sent": 0,
      "packets_received": 0,
      "sensor_name": "string",
      "sensor_id": "string",
      "ids_session_id": "string"
    }
  ],
  "total_count": 0,
  "filtered_count": 0
}
```

Табл. 103. Описание полей ответа на запрос GET [IP-адрес Комплекса]/API/v1/network_sessions

ПОЛЕ	ТИП	ОПИСАНИЕ
`data`	`array`	Информация о сетевом соединении
`id`	`string`	Идентификатор сетевого соединения
`category`	`string`	Категория сетевого соединения
`state`	`string`	Состояние сетевого соединения
`created_time`	`number`	Время создания сетевого соединения
`detected_time`	`number`	Время обновления сетевого соединения
`status`	`string`	Статус сетевого соединения
`transport_protocol`	`string`	Транспортный протокол
`protocols`	`string`	Протоколы
`duration`	`number`	Длительность сетевого соединения
`files_detected`	`number`	Файлов обнаружено
`vlan`	`number`	Адрес сети VLAN
`is_active`	`boolean`	Признак активности сетевого соединения
`source_host_id`	`string`	Идентификатор хоста отправителя
`target_host_id`	`string`	Идентификатор хоста получателя
`source_hostname`	`string`	Название хоста отправителя
`target_hostname`	`string`	Название хоста получателя
`source_network_is_local`	`string`	Признак того, что сеть отправителя является локальной

Табл. 103. Описание полей ответа на запрос GET [IP-адрес Комплекса]/API/v1/network_sessions

ПОЛЕ	ТИП	ОПИСАНИЕ
`target_network_is_local`	`string`	Признак того, что сеть получателя является локальной
`source_network_is_controlled`	`string`	Признак того, что сеть отправителя является контролируемой
`target_network_is_controlled`	`string`	Признак того, что сеть получателя является контролируемой
`source_ip`	`string`	IP-адрес отправителя
`target_ip`	`string`	IP-адрес получателя
`source_mac`	`string`	MAC-адрес отправителя
`target_mac`	`string`	MAC-адрес получателя
`source_port`	`number`	Порт отправителя
`target_port`	`number`	Порт получателя
`bytes_sent`	`number`	Байт отправлено
`bytes_received`	`number`	Байт получено
`packets_sent`	`number`	Пакетов отправлено
`packets_received`	`number`	Пакетов получено
`sensor_name`	`string`	Название сенсора
`sensor_id`	`string`	Идентификатор сенсора
`ids_session_id`	`string`	Идентификатор сетевого соединения
`total_count`	`number`	Общее количество сетевых соединений
`filtered_count`	`number`	Количество сетевых соединений, соответствующих указанным параметрам

Заголовки ответа:

```
 connection: keep-alive
content-encoding: gzip
content-type: application/json
date: Mon,05 May 2025 11:08:01 GMT
public-key-pins: pin-sha256="base64+info1="; max-age=31536000
server: nginx
strict-transport-security: max-age=31536000
transfer-encoding: chunked
x-content-type-options: nosniff
x-frame-options: DENY
x-xss-protection: 1; mode=block
```

19.2.2.7.1.3. Возможные ошибки

Информация о возможных ошибках представлена в таблице ниже.

Табл. 104. Возможные ошибки при выполнении запроса GET [ip-адрес Комплекса]/API/v1/network_sessions

HTTP-КОД	ЗНАЧЕНИЕ	ОПИСАНИЕ	ПРИМЕР ТЕЛА ОТВЕТА
`401`	`Unauthorized`	Ошибка авторизации	`{ "detail": "Could not validate credentials" }`
`403`	`Forbidden`	Ошибка доступа	`{ "detail": "Not authenticated" }`
`404`	`Not Found`	Запись не найдена	`{ "message": "Request failed", "errors": [ "{\"message\":\"Запись не найдена\", \"errors\":[\"No row was found when one was required\"]}" ] }`
`422`	`Validation Error`	Ошибка валидации	`{ "detail": [ { "loc": [ "string" ], "msg": "string", "type": "string"`

Табл. 104. Возможные ошибки при выполнении запроса GET [ip-адрес Комплекса]/API/v1/network_sessions

HTTP-КОД	ЗНАЧЕНИЕ	ОПИСАНИЕ	ПРИМЕР ТЕЛА ОТВЕТА
			<pre> }] }</pre>

19.2.2.7.2. Получение списка протоколов, обнаруженных в сетевом трафике

19.2.2.7.2.1. Запрос

URL: `GET [ip-адрес Комплекса]/API/v1/dpi_protocols`

Описание: С помощью этой конечной точки пользователь может получить информацию о протоколах, зарегистрированных в Комплексе.

Пример запроса:

```
curl -i -X GET \
'https://[IP-адрес Комплекса]/API/v1/dpi_protocols' \
-H 'accept: application/json' \
-H 'X-API-Token: [токен доступа]'
-H 'Content-Type: application/json'
```

19.2.2.7.2.2. Успешный ответ

Код ответа: `200 OK`

Тип содержимого: `application/json`

Пример тела ответа:

```
[
  {
    "name": "string"
  }
]
```

Табл. 105. Описание полей ответа на запрос GET [IP-адрес Комплекса]/API/v1/dpi_protocols

ПОЛЕ	ТИП	ОПИСАНИЕ
`name`	`string`	Название протокола

Заголовки ответа:

```
 connection: keep-alive
content-encoding: gzip
content-type: application/json
date: Mon,05 May 2025 11:08:01 GMT
public-key-pins: pin-sha256="base64+info1="; max-age=31536000
server: nginx
strict-transport-security: max-age=31536000
```

```
transfer-encoding: chunked
x-content-type-options: nosniff
x-frame-options: DENY
x-xss-protection: 1; mode=block
```

19.2.2.7.2.3. Возможные ошибки

Информация о возможных ошибках представлена в таблице ниже.

Табл. 106. Возможные ошибки при выполнении запроса GET [ip-адрес Комплекса]/API/v1/dpi_protocols

HTTP-КОД	ЗНАЧЕНИЕ	ОПИСАНИЕ	ПРИМЕР ТЕЛА ОТВЕТА
`401`	`Unauthorized`	Ошибка авторизации	`{ "detail": "Could not validate credentials" }`
`403`	`Forbidden`	Ошибка доступа	`{ "detail": "Not authenticated" }`
`404`	`Not Found`	Запись не найдена	`{ "message": "Request failed", "errors": [ "{\"message\": \"Запись не найдена\",\"errors\":[\"No row was found when one was required\"]}" ] }`
`422`	`Validation Error`	Ошибка валидации	`{ "detail": [ { "loc": [ "string" ], "msg": "string", "type": "string" }`

Табл. 106. Возможные ошибки при выполнении запроса GET [ip-адрес Комплекса]/API/v1/dpi_protocols

HTTP-КОД	ЗНАЧЕНИЕ	ОПИСАНИЕ	ПРИМЕР ТЕЛА ОТВЕТА
			<pre>] }</pre>

19.2.2.7.3. Получение списка правил сессий

19.2.2.7.3.1. Запрос

URL: `GET [ip-адрес Комплекса]/API/v1/network_sessions/network_session_rules`

Описание: С помощью этой конечной точки пользователь может получить все правила сессий, зарегистрированных в рамках Комплекса.

Пример запроса:

```
curl -i -X GET \
'https://[IP-адрес                    Комплекса]/API/v1/network_sessions/network_session_rules?
names=string&sort_field=created_at&sort_order=desc&limit=1000&offset=0' \
-H 'accept: application/json' \
-H 'X-API-Token: [токен доступа]'
-d '{
  "created_at_from": number,
  "created_at_to": number,
  "updated_at_from": number,
  "updated_at_to": number,
  "src_ips": array,
  "dst_ips": array,
  "dst_ports": array,
  "protocols": array,
  "node_ids": array,
  "enabled": boolean,
  "rule_types": array,
  "authors": array,
  "sort_field": "string",
  "sort_order": "string",
  "limit": integer,
  "offset": integer
}'
```

Табл. 107. Параметры запроса GET [ip-адрес Комплекса]/API/v1/network_sessions/network_session_rules

ПОЛЕ	ТИП	ОПИСАНИЕ
`created_at_from`	`number`	Начальное время создания правила сессии

Табл. 107. Параметры запроса GET [ip-адрес Комплекса]/API/v1/network_sessions/network_session_rules

ПОЛЕ	ТИП	ОПИСАНИЕ
`created_at_to`	`number`	Конечное время правила создания сессии
`updated_at_from`	`number`	Начальное время обновления правила сессии
`updated_at_to`	`number`	Конечное время обновления создания сессии
`src_ips`	`array`	IP-адреса отправителя
`dst_ips`	`array`	IP-адреса получателя
`dst_ports`	`array`	Порты получателя
`protocols`	`array`	Протоколы. Доступны следующие значения: • `ICMP`; • `TCP`; • `UDP`.
`node_ids`	`array`	Идентификаторы сетевых узлов
`enabled`	`boolean`	Признак активности правила
`rule_types`	`string`	Тип правила. Доступны следующие значения: • `AUTO` — автоматически созданное правило; • `MANUAL` — созданное вручную правило; • `FROM_SESSION` — правило, созданное из сессии.
`authors`	`array`	Пользователь, создавший правило
`sort_field`	`string`	Поле, по которому выполняется сортировка данных. Доступны следующие значения:

Табл. 107. Параметры запроса GET [ip-адрес Комплекса]/API/v1/network_sessions/network_session_rules

ПОЛЕ	ТИП	ОПИСАНИЕ
		• `created_at` — время создания правила сессий.
`sort_order`	`string`	Направление сортировки данных. Доступны следующие значения: • `asc` — по возрастанию; • `desc` — по убыванию.
`limit`	`integer`	Количество записей
`offset`	`integer`	Количество пропускаемых записей

19.2.2.7.3.2. Успешный ответ

Код ответа: `200 OK`

Тип содержимого: `application/json`

Пример тела ответа:


```
{
  "data": [
    {
      "node_ids": [
        "string"
      ],
      "src_ips": [
        "198.51.100.42",
        "string"
      ],
      "dst_ips": [
        "198.51.100.42",
        "string"
      ],
      "dst_ports": [
        0
      ],
      "proto": "icmp",
      "id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
      "enabled": true,
      "rule_name": "string",
      "comment": "string",
      "created_at": 0,
```

```
      "updated_at": 0,
      "rule_type": "AUTO",
      "author": "string"
    }
  ],
  "total_count": 0,
  "filtered_count": 0
}
```


Табл. 108. Описание полей ответа на запрос GET [ip-адрес Комплекса]/API/v1/network_sessions/network_session_rules

ПОЛЕ	ТИП	ОПИСАНИЕ
`data`	`array`	Информация о сетевом соединении
`node_ids`	`string`	Идентификаторы сетевых узлов
`src_ips`	`array`	IP-адреса отправителя
`dst_ips`	`array`	IP-адреса получателя
`dst_ports`	`array`	Порты получателя
`proto`	`string`	Протокол
`id`	`string`	Идентификатор правила сессий
`enabled`	`boolean`	Признак активности правила
`rule_name`	`string`	Название правила сессий
`comment`	`string`	Комментарий
`created_at`	`number`	Дата создания правила сессий
`updated_at`	`number`	Дата обновления правила сессий
`rule_type`	`string`	Тип правила. Доступны следующие значения: • `AUTO` — автоматически созданное правило; • `MANUAL` — созданное вручную правило; • `FROM_SESSION` — правило, созданное из сессии.

Табл. 108. Описание полей ответа на запрос GET [ip-адрес Комплекса]/API/v1/network_sessions/network_session_rules

ПОЛЕ	ТИП	ОПИСАНИЕ
`author`	`array`	Пользователь, создавший правило
`total_count`	`number`	Общее количество сетевых соединений
`filtered_count`	`number`	Количество сетевых соединений, соответствующих указанным параметрам

Заголовки ответа:

```
 connection: keep-alive
content-encoding: gzip
content-type: application/json
date: Mon,05 May 2025 11:08:01 GMT
public-key-pins: pin-sha256="base64+info1="; max-age=31536000
server: nginx
strict-transport-security: max-age=31536000
transfer-encoding: chunked
x-content-type-options: nosniff
x-frame-options: DENY
x-xss-protection: 1; mode=block
```

19.2.2.7.3.3. Возможные ошибки

Информация о возможных ошибках представлена в таблице ниже.

Табл. 109. Возможные ошибки при выполнении запроса GET [ip-адрес Комплекса]/API/v1/network_sessions/network_session_rules

HTTP-КОД	ЗНАЧЕНИЕ	ОПИСАНИЕ	ПРИМЕР ТЕЛА ОТВЕТА
`401`	`Unauthorized`	Ошибка авторизации	`{ "detail": "Could not validate credentials" }`
`403`	`Forbidden`	Ошибка доступа	`{ "detail": "Not authenticated" }`
`404`	`Not Found`	Запись не найдена	`{ "message": "Request failed",`

Табл. 109. Возможные ошибки при выполнении запроса GET [ip-адрес Комплекса]/API/v1/network_sessions/network_session_rules

HTTP-КОД	ЗНАЧЕНИЕ	ОПИСАНИЕ	ПРИМЕР ТЕЛА ОТВЕТА
			`"errors": [ "{\"message\":\"Запись не найдена\",\"errors\":[\"No row was found when one was required\"]}" ] }`
`422`	`Validation Error`	Ошибка валидации	`{ "detail": [ { "loc": [ "string" ], "msg": "string", "type": "string" } ] }`

19.2.2.7.4. Получение информации о правилах контроля тегов

19.2.2.7.4.1. Запрос

URL: `GET [ip-адрес Комплекса]/API/v1/network_sessions/process_control_rules`

Описание: С помощью этой конечной точки пользователь может получить информацию о всех правилах контроля тегов, созданных в рамках Комплекса.

Пример запроса:

```
curl -i -X GET \
'https://[IP-адрес Комплекса]/API/v1/network_sessions/process_control_rules?sort_field=created_at&sort_order=desc&limit=1000&offset=0&protocol=MODBUS' \
-H 'accept: application/json' \
-H 'X-API-Token: [токен доступа]'
-d '{
  "name": "string",
  "created_at_from": number,
  "created_at_to": number,
  "updated_at_from": number,
  "updated_at_to": number,
  "sensor_ids": array,
  "dst_ip": string,
  "tag": "string",
  "sort_field": "string",
```

```
  "sort_order": "string",
  "limit": integer,
  "offset": integer,
  "protocol": "string"
}'
```

Табл. 110. Параметры запроса GET [ip-адрес Комплекса]/API/v1/network_sessions/process_control_rules

ПОЛЕ	ТИП	ОПИСАНИЕ
`name`	`string`	Название правила контроля тегов
`created_at_from`	`number`	Начальное время создания правила контроля тегов
`created_at_to`	`number`	Конечное время создания правила контроля тегов
`updated_at_from`	`number`	Начальное время обновления правила контроля тегов
`updated_at_to`	`number`	Конечное время обновления правила контроля тегов
`sensor_ids`	`array`	Идентификаторы сенсоров
`dst_ip`	`string`	IP-адреса получателя
`tag`	`string`	Метка
`sort_field`	`string`	Поле, по которому выполняется сортировка данных. Доступны следующие значения: • `created_at` — дата создания; • `updated_at` — дата обновления; • `name` — название правила.
`sort_order`	`string`	Направление сортировки данных. Доступны следующие значения: • `asc` — по возрастанию; • `desc` — по убыванию.
`limit`	`integer`	Количество записей

Табл. 110. Параметры запроса GET [ip-адрес Комплекса]/API/v1/network_sessions/process_control_rules

ПОЛЕ	ТИП	ОПИСАНИЕ
`offset`	`integer`	Количество пропускаемых записей
`protocol`	`string`	Протокол. Доступны следующие значения: • `MODBUS`; • `OPC UA`; • `DELTA V`,

19.2.2.7.4.2. Успешный ответ

Код ответа: `200 OK`

Тип содержимого: `application/json`

Пример тела ответа:


```
{
  "rules": [
    {
      "author": "string",
      "params_hash": "string",
      "created_at": 0,
      "updated_at": 0,
      "dst_ip": "198.51.100.42",
      "tag": "string",
      "protocol": "MODBUS",
      "name": "string",
      "enabled": true,
      "description": "string",
      "operator": "eq",
      "sensor_id": "string",
      "data_type": "bool",
      "value": true,
      "register_type": "coils",
      "mem_address": 0,
      "id": "3fa85f64-5717-4562-b3fc-2c963f66afa6"
    }
  ],
  "total_count": 0,
  "filtered_count": 0
}
```

Табл. 111. Описание полей ответа на запрос GET [ip-адрес Комплекса]/API/v1/network_sessions/process_control_rules

ПОЛЕ	ТИП	ОПИСАНИЕ
`rules`	`array`	Правила контроля тегов
`author`	`string`	Пользователь, создавший правило
`params_hash`	`string`	Хеш-сумма правила контроля тегов
`created_at`	`number`	Дата создания правила контроля тегов
`updated_at`	`number`	Дата обновления правила контроля тегов
`dst_ip`	`string`	IP-адреса получателя
`tag`	`string`	Тег
`protocol`	`string`	Протокол
`name`	`string`	Название правила контроля тегов
`enabled`	`boolean`	Признак активности правила контроля тегов
`description`	`string`	Описание
`operator`	`string`	Оператор
`sensor_id`	`string`	Идентификатор сенсора
`data_type`	`string`	Тип данных
`value`	`boolean`	Значение
`register_type`	`string`	Область памяти
`mem_address`	`number`	Адрес регистра
`id`	`string`	Идентификатор правила контроля тегов

Заголовки ответа:

```
 connection: keep-alive
content-encoding: gzip
content-type: application/json
date: Mon,05 May 2025 11:08:01 GMT
public-key-pins: pin-sha256="base64+info1="; max-age=31536000
server: nginx
strict-transport-security: max-age=31536000
transfer-encoding: chunked
x-content-type-options: nosniff
x-frame-options: DENY
x-xss-protection: 1; mode=block
```

19.2.2.7.4.3. Возможные ошибки

Информация о возможных ошибках представлена в таблице ниже.

Табл. 112. Возможные ошибки при выполнении запроса GET [ip-адрес Комплекса]/API/v1/network_sessions/process_control_rules

HTTP-КОД	ЗНАЧЕНИЕ	ОПИСАНИЕ	ПРИМЕР ТЕЛА ОТВЕТА
`401`	`Unauthorized`	Ошибка авторизации	`{ "detail": "Could not validate credentials" }`
`403`	`Forbidden`	Ошибка доступа	`{ "detail": "Not authenticated" }`
`404`	`Not Found`	Запись не найдена	`{ "message": "Request failed", "errors": [ "{\"message\":\"Запись не найдена\", \"errors\":[\"No row was found when one was required\"]}" ] }`
`422`	`Validation Error`	Ошибка валидации	`{ "detail": [ { "loc": [ "string" ], "msg": "string",`

Табл. 112. Возможные ошибки при выполнении запроса GET [ip-адрес Комплекса]/API/v1/network_sessions/process_control_rules

HTTP-КОД	ЗНАЧЕНИЕ	ОПИСАНИЕ	ПРИМЕР ТЕЛА ОТВЕТА

			<pre>"type": "string"
			}
			]
			}</pre>

19.2.2.8. Сканеры

Для выполнения операций со сканерами доступны следующие конечные точки:

- `GET [ip-адрес Комплекса]/API/v1/scanners/{scanner_id}` — конечная точка для получения данных о выбранном сканере сбора данных по его идентификатору;
- `GET [IP-адрес Комплекса]/API/v1/scanners` — конечная точка для получения списка всех сканеров сбора данных.

19.2.2.8.1. Получение информации о сканере

19.2.2.8.1.1. Запрос

URL: `GET [ip-адрес Комплекса]/API/v1/scanners/{scanner_id}`

Описание: С помощью этой конечной точки пользователь может получить созданный на Комплексе сканер по его идентификатору.

Пример запроса:

```
curl -i -X GET \
'https://[IP-адрес Комплекса]/API/v1/scanners/{scanner_id}' \
-H 'accept: application/json' \
-H 'Authorization: Basic ZGF0YXBrOmRhdGFwaw=='
-d '{
  "scanner_id": string,
}'
```

19.2.2.8.1.2. Успешный ответ

Код ответа: `200 OK`

Тип содержимого: `application/json`

Пример тела ответа:

```
{
  "id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
  "created_at": 0,
  "updated_at": 0,
  "name": "string",
  "description": "string",
  "text": "string",
  "signature": "string",
```

```
  "expiration": 0,
  "type": "CONFIG",
  "scanner_groups": [
    {
      "id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
      "created_at": 0,
      "updated_at": 0,
      "name": "string",
      "description": "string",
      "parent_id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
      "path": [
        "string"
      ],
      "depth": 0,
      "scanners_ids": [
        "3fa85f64-5717-4562-b3fc-2c963f66afa6"
      ]
    }
  ]
}
```


Табл. 113. Описание полей ответа на запрос GET [IP-адрес Комплекса]/API/v1/scanners/{scanner_id}

ПОЛЕ	ТИП	ОПИСАНИЕ
`id`	`string`	Идентификатор сканера
`created_at`	`string`	Дата и время создания сканера
`updated_at`	`string`	Дата и время обновления сканера
`name`	`string`	Название сканера
`description`	`string`	Описание сканера
`text`	`string`	Текст сканера
`signature`	`string`	Электронная подпись
`expiration`	`string`	Срок действия подписи
`type`	`string`	Тип сканера
`scanner_groups`	`array`	Группа сканеров, в которую входит сканер
`id`	`string`	Идентификатор группы сканеров

Табл. 113. Описание полей ответа на запрос GET [IP-адрес Комплекса]/API/v1/scanners/{scanner_id}

ПОЛЕ	ТИП	ОПИСАНИЕ
`created_at`	`string`	Дата и время создания группы сканеров
`updated_at`	`string`	Дата и время обновления группы сканеров
`name`	`string`	Название группы сканеров
`description`	`string`	Описание группы сканеров
`parent_id`	`string`	Идентификатор родительской группы сканеров
`path`	`string`	Путь к группе сканеров
`depth`	`string`	Глубина группы сканеров
`scanners_ids`	`string`	Идентификаторы сканеров, входящих в группу сканеров

Заголовки ответа:

```
 connection: keep-alive
content-encoding: gzip
content-type: application/json
date: Mon,05 May 2025 11:08:01 GMT
public-key-pins: pin-sha256="base64+info1="; max-age=31536000
server: nginx
strict-transport-security: max-age=31536000
transfer-encoding: chunked
x-content-type-options: nosniff
x-frame-options: DENY
x-xss-protection: 1; mode=block
```

19.2.2.8.1.3. Возможные ошибки

Информация о возможных ошибках представлена в таблице ниже.

Табл. 114. Возможные ошибки при выполнении запроса GET [ip-адрес Комплекса]/API/v1/scanners/{scanner_id}

HTTP-КОД	ЗНАЧЕНИЕ	ОПИСАНИЕ	ПРИМЕР ТЕЛА ОТВЕТА
`400`	`Bad request`	Некорректный запрос	`{ "message": "Ошибка валидации", "errors": [`

Табл. 114. Возможные ошибки при выполнении запроса GET [ip-адрес Комплекса]/API/v1/scanners/{scanner_id}

HTTP-КОД	ЗНАЧЕНИЕ	ОПИСАНИЕ	ПРИМЕР ТЕЛА ОТВЕТА
			"body -> offset: ensure this value is less than or equal to 9223372036854775807"] }
`403`	`Forbidden`	Ошибка доступа	{ "detail": "Not authenticated" }
`422`	`Validation Error`	Ошибка валидации	{ "detail": [{ "loc": ["string"], "msg": "string", "type": "string" }] }

19.2.2.8.2. Получение списка всех сканеров

19.2.2.8.2.1. Запрос

URL: `GET [IP-адрес Комплекса]/API/v1/scanners`

Описание: С помощью этой конечной точки пользователь может получить информацию о всех сканерах на Комплексе.

Авторизация: Требуется передача заголовка X-API-Token с действительным токеном доступа.

Пример запроса:

```
curl -X 'GET' \
'https://[IP-адрес Комплекса]/API/v1/scanners' \
-H 'accept: application/json' \
-H 'X-API-Token: [токен доступа]' \
-H 'Content-Type: application/json' \
-d '{
  "offset": 9223372036854776000,
  "limit": 1000,
  "scanner_groups_ids": [
    "3fa85f64-5717-4562-b3fc-2c963f66afa6"
  ],
```

```
  "subtree_root_ids": [
    "3fa85f64-5717-4562-b3fc-2c963f66afa6"
  ],
  "scanners_ids": [
    "3fa85f64-5717-4562-b3fc-2c963f66afa6"
  ],
  "scanner_type": "CONFIG",
  "created_at_from": 0,
  "created_at_to": 0,
  "updated_at_from": 0,
  "updated_at_to": 0,
  "name_search": "string",
  "description_search": "string"
}'
```

Табл. 115. Параметры запроса GET [IP-адрес Комплекса]/API/v1/scanners

ПОЛЕ	ТИП	ОПИСАНИЕ
`offset`	`integer`	Количество пропускаемых записей
`limit`	`integer`	Количество записей
`scanner_groups_ids`	`string`	Идентификаторы групп сканеров
`subtree_root_ids`	`string`	Параметр фильтрации по группам сканеров
`scanners_ids`	`string`	Идентификаторы сканеров
`scanner_type`	`string`	Тип сканера
`created_at_from`	`number`	Начальное время создания сканера
`created_at_to`	`number`	Конечное время создания сканера
`updated_at_from`	`number`	Начальное время обновления сканера
`updated_at_to`	`number`	Конечное время обновления сканера
`name_search`	`string`	Поиск сканера по названию
`description_search`	`string`	Поиск сканера по описанию

19.2.2.8.2.2. Успешный ответ

Код ответа: `200 OK`

Тип содержимого: `application/json`

Пример тела ответа:


```
{
  "data": [
    {
      "id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
      "created_at": 0,
      "updated_at": 0,
      "name": "string",
      "description": "string",
      "text": "string",
      "signature": "string",
      "expiration": 0,
      "type": "CONFIG",
      "scanner_groups": [
        {
          "id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
          "created_at": 0,
          "updated_at": 0,
          "name": "string",
          "description": "string",
          "parent_id": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
          "path": [
            "string"
          ],
          "depth": 0,
          "scanners_ids": [
            "3fa85f64-5717-4562-b3fc-2c963f66afa6"
          ]
        }
      ]
    }
  ],
  "total_count": 0,
  "filtered_count": 0
}
```


Табл. 116. Описание полей ответа на запрос GET [IP-адрес Комплекса]/API/v1/scanners

ПОЛЕ	ТИП	ОПИСАНИЕ
`data`	`array`	Информация о сканерах
`id`	`string`	Идентификатор сканера

Табл. 116. Описание полей ответа на запрос GET [IP-адрес Комплекса]/API/v1/scanners

ПОЛЕ	ТИП	ОПИСАНИЕ
`created_at`	`number`	Дата и время создания сканера
`updated_at`	`number`	Дата и время обновления сканера
`name`	`string`	Название сканера
`description`	`string`	Описание сканера
`text`	`string`	Текст сканера
`signature`	`string`	Электронная подпись
`expiration`	`string`	Срок действия подписи
`type`	`string`	Тип сканера
`scanner_groups`	`array`	Группа сканеров, в которую входит сканер
`id`	`string`	Идентификатор группы сканеров
`created_at`	`string`	Дата и время создания группы сканеров
`updated_at`	`string`	Дата и время обновления группы сканеров
`name`	`string`	Название группы сканеров
`description`	`string`	Описание группы сканеров
`parent_id`	`string`	Идентификатор родительской группы сканеров
`path`	`string`	Путь к группе сканеров
`depth`	`string`	Глубина группы сканеров
`scanners_ids`	`string`	Идентификаторы сканеров, входящих в группу сканеров
`total_count`	`integer`	Общее количество активов

Табл. 116. Описание полей ответа на запрос GET [IP-адрес Комплекса]/API/v1/scanners

ПОЛЕ	ТИП	ОПИСАНИЕ
`filtered_count`	`integer`	Количество активов, соответствующих указанным параметрам

Заголовки ответа:

```
connection: keep-alive
content-encoding: gzip
content-type: application/json
strict-transport-security: max-age=31536000
x-content-type-options: nosniff
x-frame-options: DENY
x-xss-protection: 1; mode=block
```

19.2.2.8.2.3. Возможные ошибки

Информация о возможных ошибках представлена в таблице ниже.

Табл. 117. Возможные ошибки при выполнении запроса GET [IP-адрес Комплекса]/API/v1/scanners

HTTP-КОД	ЗНАЧЕНИЕ	ОПИСАНИЕ	ПРИМЕР ТЕЛА ОТВЕТА
`400`	`Bad request`	Некорректный запрос	`{ "message": "Ошибка валидации", "errors": [ "body -> offset: ensure this value is less than or equal to 9223372036854775807" ] }`
`401`	`Unauthorized`	Ошибка авторизации	`{ "detail": "Could not validate credentials" }`
`403`	`Forbidden`	Ошибка доступа	`{ "detail": "Not authenticated" }`
`404`	`Not Found`	Запись не найдена	`{ "message": "Request failed", "errors": [`

Табл. 117. Возможные ошибки при выполнении запроса GET [IP-адрес Комплекса]/API/v1/scanners

HTTP-КОД	ЗНАЧЕНИЕ	ОПИСАНИЕ	ПРИМЕР ТЕЛА ОТВЕТА
			`"{\"message\":\"Запись не найдена\", \"errors\":[\"No row was found when one was required\"]}" ] }`
`422`	`Validation Error`	Ошибка валидации	`{ "detail": [ { "loc": [ "string" ], "msg": "string", "type": "string" } ] }`

19.2.2.9. Уязвимости

Для выполнения операций с уязвимостями доступны следующие конечные точки:

- `GET [ip-адрес Комплекса]/API/v1/vulnerabilities/oval_assessments` — конечная точка для получения списка всех проверок OVAL;
- `GET [ip-адрес Комплекса]/API/v1/vulnerabilities/oval_assessments/{oval_assessment_id}` — конечная точка для получения информации о выбранной проверке OVAL по ее идентификатору.

19.2.2.9.1. Получение списка OVAL-проверок

19.2.2.9.1.1. Запрос

URL: `GET [ip-адрес Комплекса]/API/v1/vulnerabilities/oval_assessments`

Описание: С помощью этой конечной точки пользователь может получить информацию о всех OVAL-проверках, выполняемых Комплексом.

Пример запроса:

```
curl -i -X GET \
'https://[IP-адрес Комплекса]/API/v1/vulnerabilities/oval_assessments?offset=0&limit=1000&statuses=string&asset_ids=3fa85f64-5717-4562-b3fc-2c963f66afa6&oval_groups_ids=3fa85f64-5717-4562-b3fc-2c963f66afa6&with_oval_group=false' \
-H 'accept: application/json' \
-H 'X-API-Token: [токен доступа]'
-d '{
  "offset": integer,
  "limit": integer,
```

```
  "statuses": array,
  "asset_ids": array,
  "oval_groups_ids": array,
  "created_by": "string",
  "updated_at_from": number,
  "updated_at_to": number,
  "search": "string",
  "with_oval_group": boolean
}'
```

Табл. 118. Параметры запроса GET [ip-адрес Комплекса]/API/v1/vulnerabilities/oval_assessments

ПОЛЕ	ТИП	ОПИСАНИЕ
`offset`	`integer`	Количество пропускаемых записей
`limit`	`integer`	Количество записей
`statuses`	`array`	Статусы OVAL-проверок
`asset_ids`	`array`	Идентификаторы активов
`oval_groups_ids`	`array`	Идентификаторы OVAL-групп
`created_by`	`string`	Пользователь, создавший OVAL-проверку
`updated_at_from`	`number`	Начальная дата обновления OVAL-проверки
`updated_at_to`	`number`	Конечная дата обновления OVAL-проверки
`search`	`string`	Поисковое значение
`with_oval_group`	`boolean`	Признак принадлежности к OVAL-группе

19.2.2.9.1.2. Успешный ответ

Код ответа: `200 OK`

Тип содержимого: `application/json`

Пример тела ответа:

```
{
  "data": [],
  "total_count": 0,
```

```
  "filtered_count": 0
}
```

Табл. 119. Описание полей ответа на запрос GET [ip-адрес Комплекса]/API/v1/vulnerabilities/oval_assessments

ПОЛЕ	ТИП	ОПИСАНИЕ
`data`	`array`	Информация об OVAL-проверке
`total_count`	`number`	Общее количество OVAL-проверок
`filtered_count`	`number`	Количество OVAL-проверок, соответствующих указанным параметрам

Заголовки ответа:

```
 connection: keep-alive
content-encoding: gzip
content-type: application/json
date: Mon,05 May 2025 11:08:01 GMT
public-key-pins: pin-sha256="base64+info1="; max-age=31536000
server: nginx
strict-transport-security: max-age=31536000
transfer-encoding: chunked
x-content-type-options: nosniff
x-frame-options: DENY
x-xss-protection: 1; mode=block
```

19.2.2.9.1.3. Возможные ошибки

Информация о возможных ошибках представлена в таблице ниже.

Табл. 120. Возможные ошибки при выполнении запроса GET [ip-адрес Комплекса]/API/v1/vulnerabilities/oval_assessments

HTTP-КОД	ЗНАЧЕНИЕ	ОПИСАНИЕ	ПРИМЕР ТЕЛА ОТВЕТА
`401`	`Unauthorized`	Ошибка авторизации	`{ "detail": "Could not validate credentials" }`
`403`	`Forbidden`	Ошибка доступа	`{ "detail": "Not authenticated" }`

Табл. 120. Возможные ошибки при выполнении запроса GET [ip-адрес Комплекса]/API/v1/vulnerabilities/oval_assessments

HTTP-КОД	ЗНАЧЕНИЕ	ОПИСАНИЕ	ПРИМЕР ТЕЛА ОТВЕТА
`404`	`Not Found`	Запись не найдена	`{ "message": "Request failed", "errors": [ "{\"message\":\"Запись не найдена\",\"errors\":[\"No row was found when one was required\"]}" ] }`
`422`	`Validation Error`	Ошибка валидации	`{ "detail": [ { "loc": [ "string" ], "msg": "string", "type": "string" } ] }`

19.2.2.9.2. Получение информации об определенной OVAL-проверке

19.2.2.9.2.1. Запрос

URL: `GET [ip-адрес Комплекса]/API/v1/vulnerabilities/oval_assessments/{oval_assessment_id}`

Описание: С помощью этой конечной точки пользователь может получить информацию об определенной OVAL-проверке по ее идентификатору.

Авторизация: Требуется передача заголовка X-API-Token с действительным токеном доступа.

Пример запроса:

```
curl -i -X GET \
'https://[IP-адрес Комплекса]/API/v1/vulnerabilities/oval_assessments/oval_assessment_id=3fa85f64-5717-4562-b3fc-2c963f66afa6' \
-H 'accept: application/json' \
-H 'X-API-Token: [токен доступа]'
-d '{
  "oval_assessment_id": "string"
}'
```

Табл. 121. Параметры запроса GET [ip-адрес Комплекса]/API/v1/vulnerabilities/oval_assessments/{oval_assessment_id}

ПОЛЕ	ТИП	ОПИСАНИЕ
`oval_assessment_id`	`string`	Идентификатор OVAL-проверки

19.2.2.9.2.2. Успешный ответ

Код ответа: `200 OK`

Тип содержимого: `application/json`

Пример тела ответа:

Пример тела ответа:

```
{
  "data": [],
  "total_count": 0,
  "filtered_count": 0
}
```

Табл. 122. Описание полей ответа на запрос GET [ip-адрес Комплекса]/API/v1/vulnerabilities/oval_assessments/{oval_assessment_id}

ПОЛЕ	ТИП	ОПИСАНИЕ
`data`	`array`	Информация об OVAL-проверке
`total_count`	`number`	Общее количество OVAL-проверок
`filtered_count`	`number`	Количество OVAL-проверок, соответствующих указанным параметрам

Заголовки ответа:

```
connection: keep-alive
content-encoding: gzip
content-type: application/json
strict-transport-security: max-age=31536000
x-content-type-options: nosniff
x-frame-options: DENY
x-xss-protection: 1; mode=block
```

19.2.2.9.2.3. Возможные ошибки

Информация о возможных ошибках представлена в таблице ниже.

Табл. 123. Возможные ошибки при выполнении запроса GET [ip-адрес Комплекса]/API/v1/vulnerabilities/oval_assessments/{oval_assessment_id}

HTTP-КОД	ЗНАЧЕНИЕ	ОПИСАНИЕ	ПРИМЕР ТЕЛА ОТВЕТА
`401`	`Unauthorized`	Ошибка авторизации	`{ "detail": "Could not validate credentials" }`
`403`	`Forbidden`	Ошибка доступа	`{ "detail": "Not authenticated" }`
`422`	`Validation Error`	Ошибка валидации	`{ "detail": [ { "loc": [ "string" ], "msg": "string", "type": "string" } ] }`

20. Регламентные работы

В этом разделе:

1. **Резервное копирование данных**
2. **Смена паролей**
3. **Удаление данных Комплекса**
4. **Очистка дискового пространства от внутренних событий**

Регламентные работы – комплекс профилактических работ и проверок, выполняемых на объектах систем автоматики в определенные (регламентированные) моменты времени периода эксплуатации и направленных на поддержание их надежности в течение межрегламентного срока.

Для своевременного исполнения регламентных работ администратор системы в интерфейсе Комплекса может создавать резервные копии ключевых данных и изменять пароли пользователей.

20.1. Резервное копирование данных

В этом разделе:

- Резервное копирование рабочей директории и данных Комплекса уровня Management
- Выгрузка внешних событий Комплекса в архив
- Экспорт отдельных справочников
- Экспорт нескольких справочников

Периодическому архивированию и резервному копированию на резервные машинные носители подлежат следующие объекты Комплекса:

1. Базы данных Комплекса.
2. Рабочая директория Комплекса.
3. Индексы событий.
4. Информация о подключенных сенсорах и контролируемых сетях, которые прослушивают сенсоры.
5. Информация из подраздела О системе.
6. Активность службы обнаружения вторжений по отдельным сенсорам.
7. Оперативные данные:
    - список активов;
    - список сессий;
    - события активов (в том числе инциденты);
    - связи сессий, активов и инцидентов с сенсорами.
8. Справочные данные (пакеты экспертизы):
    - иерархия АСУ ТП;
    - иерархия меток активов;
    - группы сканеров;
    - источники событий;
    - задачи сбора данных;
    - правила разбора событий;
    - правила обогащения событий;
    - схема событий;

- правила службы обнаружения вторжений;
- исключения для правил службы обнаружения вторжений;
- политика корреляции (схема и правила корреляции);
- OVAL-определения и группы OVAL-определений.
- скрипты OVAL;
- настройки OVAL;
- справочники ПО и уязвимостей (CPE и CVE);
- сопоставление собранного сканерами ПО со справочником CPE.

Периодичность резервного копирования определяется внутренними регламентами эксплуатирующей организации.

20.1.1. Резервное копирование рабочей директории и данных Комплекса уровня Management

В этом разделе:

- Запуск резервного копирования рабочей директории и баз данных Комплекса уровня Management
- Содержание архива резервной копии рабочей директории и баз данных Комплекса

Модуль резервного копирования `backup_manager` локального Комплекса уровня Management сохраняет следующие данные в резервной копии:

- пользовательские конфигурационные файлы сервисов Комплекса;
- справочники уязвимостей (CPE, CVE и БДУ ФСТЭК России) для поиска уязвимостей с помощью установленного модуля «Управление уязвимостями»;
- репозитории ПЛК, которые хранятся в модуле «Управление проектами ПЛК»;
- базы данных локального Комплекса, содержащие все накопленные данные.

Подробное содержание резервной копии приведено в разделе «Содержание архива резервной копии рабочей директории и баз данных Комплекса».

> Внимание:
>
> Сервис резервного копирования не сохраняет внешние события Комплекса (индексы). Для архивирования индексов событий воспользуйтесь инструкцией в разделе «Выгрузка внешних событий Комплекса в архив».

> Внимание:
>
> Сервис резервного копирования не сохраняет проверки OVAL.

20.1.1.1. Содержание архива резервной копии рабочей директории и баз данных Комплекса

Архив резервной копии `dtpk-backup-[version]-[YYYYmmddhhmmss].tar` содержит:

- `data.tar.bz2` — архив, включающий в себя следующие файлы:
  - директория `/usr/share/udv/vulnerability-backend`, содержащая справочники уязвимостей (CPE, CVE и БДУ ФСТЭК России) для работы модуля «Управление уязвимостями»;
  - директория `/etc/logstash/pipeline` с файлом `09-custom-filter.conf`, содержащим пользовательские фильтры для нормализации внешних событий модулем «Управление внешними событиями»;
  - директория `/var/backup/` с файлом `nta-backup-[версия_Комплекса]-[дата]` резервной копии базы данных `clickhouse` модуля «Анализ промышленного сетевого трафика» (если в команде создания резервной копии был задан параметр `--include-nta` для создания копии этой БД и модуль был установлен при выполнении резервного копирования);
  - директория `/usr/share/udv/datapk` с конфигурационным файлом `manager.env` сервисов Комплекса.
- `repos_data.tar.bz2`— архив, содержащий репозитории ПЛК, которые хранятся в модуле «Управление проектами ПЛК»;
- `maria_db_dump.aes`, `redis_db_dump.aes` и `postgres_db_dump.aes` — резервные копии баз данных, зашифрованные паролем, который задается при запуске резервного копирования (в ключе `--password`);
- `info.json` — метаданные, включающие контрольные суммы файлов резервной копии.

Внимание:

Директория `/etc/logstash/pipeline` и файл `09-custom-filter.conf` создаются из сервиса `udv-logstash` только при установке модуля «Управление внешними событиями». Изменения в других конфигурационных файлах сервиса `udv-logstash` могут быть перезаписаны при обновлении сервиса и не сохраняются автоматически.

20.1.1.2. Запуск резервного копирования рабочей директории и баз данных Комплекса уровня Management

Для выполнения резервного копирования рабочей директории и баз данных локального Комплекса уровня Management в режиме командной строки:

1. Подключитесь к Комплексу уровня Management по протоколу SSH с учетной записью `user` и повысьте привилегии до администратора с помощью команды `su -`
2. Убедитесь, что директория `/usr/share/udv/datapk` занимает менее 500 Мбайт:

   ```
   du -h -d 1 /usr/share/udv/datapk | sort -h
   ```

3. Из любой директории выполните следующую команду для запуска резервного копирования:

   ```
   python3 -m backup_manager create --include-nta [quick|full] --justification 'Регламентные
    работы' --username 'datapk' --password '1234567890' --db-username DB_USER --db-password
    DB_PASS
   ```

   где:
   - `--include-nta` — параметр для создания в директории `/var/backups` отдельного архива с резервной копией базы данных `clickhouse` установленного модуля «Анализ промышленного сетевого трафика». Вместо `[quick|full]` укажите глубину создания резервной копии БД:
     - `quick` — создание резервной копии оперативных данных БД;
     - `full` — создание полной резервной копии БД.

Если модуль «Анализ промышленного сетевого трафика» не установлен, удалите параметр и его значение из команды.

- `--justification` — комментарий к создаваемой резервной копии;
- `--username` — имя пользователя, который создает резервную копию;
- `--password` — пример пароля для архива резервной копии;
- `--db-username` — логин пользователя базы данных, значение которого необходимо скопировать из переменной `DB_USER` конфигурационного файла `/usr/share/udv/datapk/manager.env`;
- `--db-password` — пароль доступа к базе данных, значение которого необходимо скопировать из переменной `DB_PASS` конфигурационного файла `/usr/share/udv/datapk/manager.env`.

Прим.:

В команду создания резервной копии можно добавить команды для автоматического копирования значений переменных `DB_USER` и `DB_PASS` из файла `manager.env`:

```
python3 -m backup_manager create --include-nta [quick|full] --justification
 'Регламентные работы' --username 'datapk' --password '1234567890' --db-username
 $(cat /usr/share/udv/datapk/manager.env | grep DB_USER | sed s/DB_USER=//g)
 --db-password $(cat /usr/share/udv/datapk/manager.env | grep DB_PASS | sed
 s/DB_PASS=//g)
```

Внимание:

Значения переменных `DB_USER` и `DB_PASS` из файла `manager.env`, а также пароль от архива (значение параметра `--password`) рекомендуется скопировать и сохранить отдельно — эти значения необходимо будет вводить вручную при восстановлении Комплекса из резервной копии.

Результат шага:

- В процессе резервного копирования будут отображаться следующие строки:

```
INFO:backup_manager.operations.create:Backup creation started
DEBUG:httpx._client:HTTP Request: POST http://127.0.0.1:10006/datapk_event_by_code
 "HTTP/1.1 204 "
INFO:backup_manager.operations.create:Creating a postgres database dump
...
INFO:backup_manager.operations.check:dump.rdb Ok
INFO:backup_manager.main:Backup
 created: /
var/backups/dtpk-backup-v3.0.[минорная_версия].[патч_версия]-{ГГГГММДДччммсс}.tar
```

- В директории по умолчанию `/var/backups` будет создан архив резервной копии `dtpk-backup-v3.0.[минорная_версия].[патч_версия]-{ГГГГММДДччммсс}.tar`.
- Если был задан параметр `--include-nta` и был установлен модуль «Анализ промышленного сетевого трафика», в директории по умолчанию `/var/backups` будет создан архив `nta-backup-[версия_Комплекса]-[дата]` резервной копии БД `clickhouse`.

4. Проверьте корректность созданного архива резервной копии. Для этого выполните следующую команду:

```
python3 -m backup_manager check --file=dtpk-backup-[version]-[YYYYmmddhhmmss].tar
 --password='1234567890'
```

где:

- `--file` — название созданного ранее архива резервной копии, который нужно проверить на корректность;
- `--password` — пример пароля от архива, заданного в одноименном ключе при запуске резервного копирования в шаге 3.

5. Скопируйте созданный архив резервной копии из директории `/var/backups` на отдельный физический носитель.
6. Вручную сохраните на отдельный физический носитель следующие файлы:
   - конфигурационный файл `manager.env` из директории `/usr/share/udv/datapk`;
   - конфигурационный файл `sensor.env` из директории `/usr/share/udv/datapk/` (если на текущем Комплексе установлен сенсор).

20.1.2. Резервное копирование Комплекса уровня Sensor

Комплексы уровня Sensor не хранят данные, поэтому их резервное копирование заключается только в ручном сохранении следующих локальных файлов сенсора:

- `/etc/machine-id` — идентификатор текущего сенсора;
- `/usr/share/udv/datapk/sensor.env` — конфигурационный файл сенсора.
- `/usr/share/udv/zeek-wrapper/configs/general.dat` и `/usr/share/udv/zeek-wrapper/configs/ics-function.dat` — конфигурационные файлы модуля «Анализ промышленного сетевого трафика» (если он установлен на сенсоре).

Восстановление сенсоров из резервной копии заключается в их развертывании с нуля согласно инструкциям для сенсоров в разделе «Установка и настройка Комплекса на базе ОС Альт Сервер» Руководства по внедрению и поддержке.

20.1.3. Выгрузка внешних событий Комплекса в архив

Комплекс сохраняет архивы индексов событий в операционную систему в директорию `/var/backups/elasticsearch/indices`.

20.1.3.1. Выгрузка индекса событий в архив

Чтобы сохранить отдельный индекс с событиями в архив в операционную систему Комплекса:

1. Перейдите на страницу **Администрирование → События и инциденты → Индексы**.

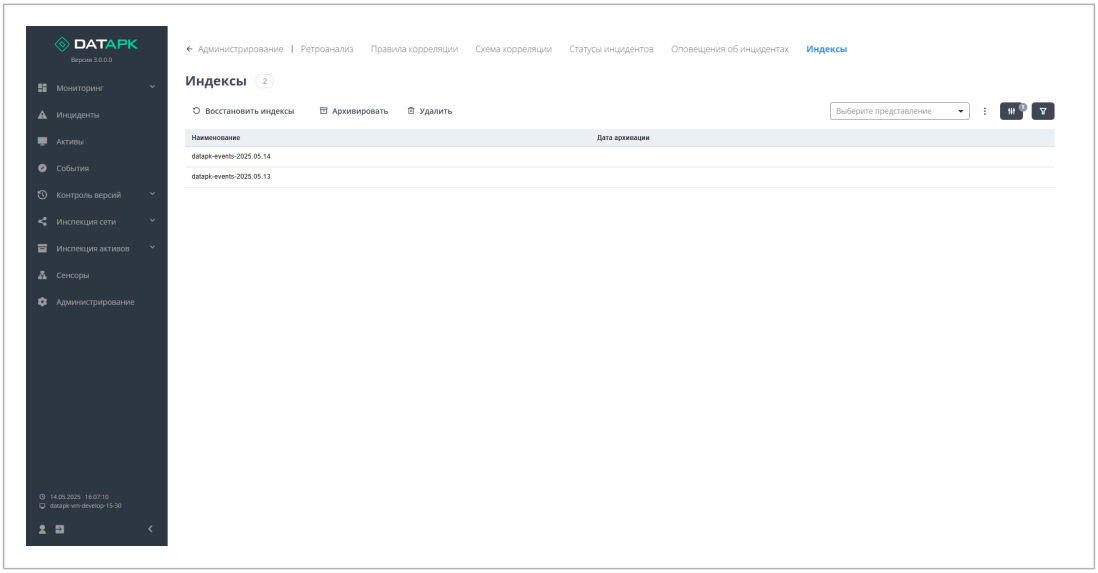


Рис. 458. Страница «Индексы»

2. Нажмите кнопку (**Архивировать**) справа от выбранного индекса.
   - **Результат шага:** архив с событиями `datapk_events_[тип_индекса]_[дата_индекса]` будет загружен в директорию `/var/backups/elasticsearch/indices` в операционной системе Комплекса.

20.1.3.2. Выгрузка нескольких индексов событий в архив

Чтобы сохранить отфильтрованные индексы с событиями в архивы в операционную систему Комплекса:

1. Перейдите на страницу **Администрирование → События и инциденты → Индексы**.
2. Воспользуйтесь фильтрами для получения списка индексов, подлежащих архивированию.
3. Нажмите кнопку (**Архивировать**) в верхней части страницы.
   - **Результат шага:** для каждого отфильтрованного индекса отдельный архив `datapk_events_[тип_индекса]_[дата_индекса]` будет загружен в директорию `/var/backups/elasticsearch/indices` в операционной системе Комплекса.

20.1.4. Экспорт отдельных справочников

В качестве дополнительного способа создания резервных копий в веб-интерфейсе можно выгружать справочники объектов в файлы и сохранять их. В таблице ниже (Таблица 124. Ссылки на разделы документа с описанием экспорта объектов Комплекса) приведены ссылки на разделы с описанием выполнения резервных копий объектов Комплекса путем экспорта.

Табл. 124. Ссылки на разделы документа с описанием экспорта объектов Комплекса

НАИМЕНОВАНИЕ	ССЫЛКА	ФОРМАТ
Правила разбора событий	Экспорт правил разбора событий	`zip`
Правила обогащения событий	Экспорт правил обогащения событий	`zip`
Схема событий	Экспорт схемы событий	`zip`
Иерархия АСУ ТП	Экспорт справочника с классификаторами АСУ ТП	`json`
Иерархия меток активов	Экспорт меток	`json`
Группы активов (без активов)	Экспорт групп активов	`json`
Политика корреляции	Экспорт политики корреляции	`json`
Сканеры в составе групп сканеров	Экспорт сканеров и их групп	`json`
Задачи сбора данных	Экспорт задач сбора данных	`json`
Статусы инцидентов	Экспорт статусов инцидентов	`json`
Правила службы обнаружения вторжений	Экспорт правил службы обнаружения вторжений	`json`
Группы OVAL-определений	Экспорт групп OVAL-определений	`json`
Скрипты OVAL	Экспорт скриптов OVAL	`json`
Настройки OVAL	Экспорт настроек OVAL	`json`
Источники событий	Экспорт источников событий	`json`
Сохраненные запросы, визуализации, панели мониторинга	Экспорт сохраненных объектов в экспертном режиме просмотра событий	`json`
Активы	Экспорт активов	`json`

Внимание:

Экспорт следующих справочников недоступен в веб-интерфейсе:

- справочники ПО и уязвимостей (CPE и CVE) и база сопоставления собранного сканерами ПО со справочником CPE. Экспорт этих справочников доступен только в операционной системе Комплекса путем копирования директории `/cve` вместе с содержимым (по умолчанию расположена в директории `/usr/share/udv/vulnerability-backend`);
- правила корреляции и схема корреляции — экспорт доступен только в составе политики корреляции;
- наборы сигнатур правил обнаружения вторжений в формате Suricata — экспорт доступен только в составе правил обнаружения вторжений;
- OVAL-определения — экспорт доступен только в составе групп OVAL-определений;
- учетные данные активов.

20.1.5. Экспорт нескольких справочников

В Комплексе возможен экспорт справочных данных в единый архив формата `.tar`. Список доступных для экспорта справочников приведен в разделе «Экспорт отдельных справочников». Для экспорта:

1. Перейдите на страницу **Администрирование → Основные настройки → Импорт и экспорт**.
2. Нажмите кнопку (**Экспортировать...**) в верхней части страницы.
   - **Результат шага:** справа откроется карточка **Экспорт справочных данных**.
3. В открывшейся справа карточке измените при необходимости набор справочников для выгрузки.

> Внимание:
>
> По умолчанию выбраны все справочники, кроме справочников **Правила разбора событий**, **Правила обогащения событий** и **Схема событий**. Такой выбор рекомендован, если планируется дальнейший импорт файла на другие **Комплекс**ы, так как при импорте настроек событий могут проявляться проблемы с формированием инцидентов.

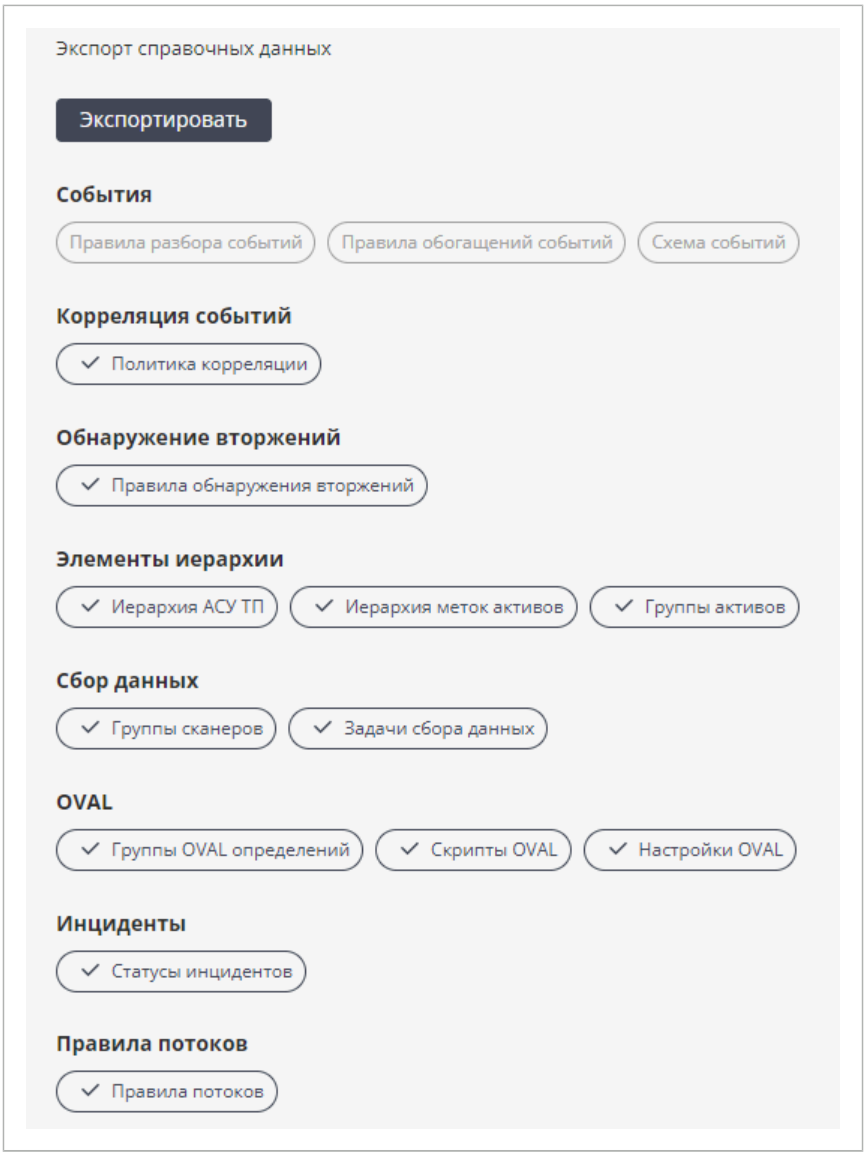


Рис. 459. Окно «Экспорт справочных данных»

4. Нажмите **Экспортировать**.
   - **Результат шага:** появится уведомление `Запущен экспорт справочников`.
5. Дождитесь подготовки архива формата `export_[дата_и_время].tar` в поле **Результат последнего экспорта** в правом верхнем углу страницы.
6. Нажмите на подготовленный архив для его скачивания.
   - **Результат шага:** файл с архивом справочников формата `export_[дата_и_время].tar` будет загружен.

20.2. Смена паролей

В этом разделе:

- Смена пароля системной учетной записи администратора
- Смена пароля учетной записи в веб-интерфейсе Комплекса

20.2.1. Смена пароля системной учетной записи администратора

Для смены пароля системной учетной записи администратора Комплекса:

1. Подключитесь к операционной системе Комплекса.
2. Войдите в систему под системной учетной записью администратора.
3. Смените пароль администратора. Для этого введите команду:

   ```
   passwd [имя_пользователя]
   ```

4. Введите новый пароль администратора и нажмите клавишу **Enter**. После соответствующего запроса повторите ввод нового пароля администратора и нажмите клавишу **Enter**.

20.2.2. Смена пароля учетной записи в веб-интерфейсе Комплекса

Смена паролей учетных записей Комплекса может быть выполнена только пользователем с назначенной ролью `Администратор`.

Для смены пароля учетной записи другого пользователя:

1. Перейдите на страницу **Администрирование** → **Пользователи**.
2. Выберите учетную запись, для которой необходимо сменить пароль, и нажмите кнопку (**Редактировать**).
3. В открывшемся окне введите в поле **Пароль** новый пароль пользователя, повторите ввод нового пароля в поле **Подтверждение пароля**.
4. Нажмите кнопку **Сохранить**.
5. Выполните шаги 1-3 для других учетных записей Комплекса.

> Подсказка:
>
> Порядок смены пароля текущего пользователя приведен в подразделе «Управление учетными записями пользователей».

20.3. Удаление данных Комплекса

Для удаления данных Комплекса:

1. Остановите работу сервисов, выполнив команду:

   ```
   systemctl stop udv-* --all
   ```

2. Выполните удаление данных командой:

   ```
   /usr/bin/udv-remove-data
   ```

3. Запустите работу сервисов командой:

   ```
   systemctl start udv-* --all
   ```

4. Дождитесь запуска работы всех сервисов.
5. Войдите в веб-интерфейс Комплекса и убедитесь, что все данные удалены.

20.4. Очистка дискового пространства от внутренних событий

Перед выполнением:

Если внутренние события занимают весь объем дискового пространства, указанный в переменной `EVENTS_RETENTION_DISK_CAPACITY_SIZE_MB`, регистрация внутренних событий останавливается. Для возобновления регистрации событий требуется очистить дисковое пространство.

> Прим.:
>
> Подробнее о рекомендациях по использованию переменной см. в разделе «Рекомендации по использованию переменных файлов manager.env и sensor.env» Руководства по эксплуатации.

Очистка дискового пространства от внутренних событий Комплекса выполняется с помощью скрипта `udv-internal-events-cleanup.py`. Этот скрипт поставляется в комплекте дистрибутива Комплекса.

По умолчанию скрипт `udv-internal-events-cleanup` располагается в директории `/usr/bin`, запуск скрипта возможен от любого привилегированного пользователя из любой директории Комплекса.

Для очистки дискового пространства от внутренних событий:

1. Подключитесь к операционной системе Комплекса.
2. Остановите сервис регистрации внутренних событий:

   ```
   service udv-event-manager stop
   ```

3. > Прим.:
   >
   > Этот шаг необходимо выполнить, если вы хотите оставить часть событий определенного объема. Если эта информация не требуется, перейдите к следующему шагу.

   Уточните объем дискового пространства, занимаемого внутренними событиями:

   ```
   udv-internal-events-cleanup
   ```

   ▸ **Результат шага:** В терминале отобразится объем, занимаемый базой данных, и объем, занимаемый внутренними событиями.
4. Запустите скрипт `internal_events_cleanup.py`:

   ```
   udv-internal-events-cleanup --[параметры]
   ```

   Укажите один из двух параметров в блоке `[параметры]`:
   - `--date-before-cleanup "YYYY-MM-DDThh:mm:ss"` — дата и время, события старше которых будут удалены;
   - `--mb-before-cleanup "МБ"` — объем событий, которые должны остаться после очистки. Задается в мегабайтах.

   > Прим.:
   >
   > Если необходимо удалить все события, укажите дату и время в будущем или укажите объем в 0 МБ.

   > **Пример**
   > Примеры команды:

```
udv-internal-events-cleanup --date-before-cleanup "2025-02-11T14:15:16"
udv-internal-events-cleanup --mb-before-cleanup "200"
```

5. После выполнения скрипта `internal_events_cleanup.py` запустите сервис регистрации внутренних событий:

```
service udv-event-manager start
```

- **Результат шага:** В Комплексе будет зарегистрировано событие `1070011 «Запущен сервис регистрации внутренних событий»`.

21. Нештатные ситуации и действия по их устранению

В этом разделе:

1. **Диагностика сервисов и иерархии**
2. **Действия по восстановлению комплекса при сбойных ситуациях и ошибках в данных**
3. **Восстановление данных из резервных копий**
4. **Действия в случаях несанкционированного доступа к данным**
5. **Действия в других аварийных ситуациях**
6. **Анкета при обращении в сервисный центр**
7. **Диагностика сервиса сбора данных по протоколам SSH, Telnet, WinRM, winexe**

Комплекс функционирует круглосуточно. В процессе использования Комплекса возможно появление неполадок, ограничивающих возможности управления защитными механизмами или открывающих возможности для атаки на активы.

Если вам не удается самостоятельно устранить нештатную ситуацию, заполните анкету (см. раздел Анкета при обращении в сервисный центр) и отправьте на адрес сервисного центра UDV Group: support@udv.group.

21.1. Диагностика сервисов и иерархии

Скрипт `dtpk_get_logs-3_0.bash` однократно собирает состояние системы и журналы сервисов Комплекса уровней Management и Sensor на текущем сервере за заданный период времени в часах.

Для диагностики работоспособности сервисов и иерархии в операционной системе Комплекса:

1. Примонтируйте диск с дистрибутивом Комплекса, либо с помощью приложения для обмена файлами по протоколу SFTP (или аналогичным способом по сети) скопируйте скрипт `dtpk_get_logs-3_0.bash` в директорию `/opt` операционной системы Комплекса.
2. Подключитесь к выбранному Комплексу по протоколу SSH с учетной записью обычного пользователя и повысьте привилегии до администратора с помощью команды `su -`
3. Перейдите в директорию `/opt` по команде:

   ```
   cd /opt
   ```

4. Запустите скрипт `dtpk_get_logs-3_0.bash` командой:

   ```
   bash dtpk_get_logs-3_0.bash N
   ```

   где `N` — период, за который будут собраны журналы (в часах).

   > **Пример**
   > Чтобы собрать журналы за последние 6 часов, выполните команду:
   >
   > ```
   > bash dtpk_get_logs-3_0.bash 6
   > ```

   ▸ **Результат шага:** в текущей директории `/opt` будет создан архив `logs-[hostname]-[текущая_дата].tar.gz` с журналами сервисов текущего Комплекса за выбранный период времени.
5. Заполните анкету и отправьте с ней архив на адрес сервисного центра UDV Group : support@udv.group. Шаблон анкеты доступен в разделе «Анкета при обращении в сервисный центр».

21.2. Действия по восстановлению комплекса при сбойных ситуациях и ошибках в данных

При эксплуатации Комплекса пользователь может столкнуться с различными видами затруднений, которые также возможно самостоятельно устранить. Основные типы затруднений:

- Веб-интерфейс не загружается
- Время на Комплексе отличается от времени получения события
- После запуска Комплекса при попытке загрузки веб-интерфейса открывается пустая страница
- 502-я ошибка при загрузке страницы авторизации, 500-е ошибки сразу после авторизации
- Не обнаруживаются новые сессии
- Комплекс не обнаруживает активы в автоматическом режиме
- Два актива с одинаковым IP-адресом
- Не осуществляется сбор необходимых событий или конфигураций с активов
- При попытке сбора данных в результатах выводится предупреждение «Превышено время ожидания выполнения задачи сбора событий»
- Сбор конфигураций осуществляется, но результаты сбора не отображаются
- Отсутствуют внутренние события на странице «События»
- Отсутствуют внешние события на странице «События»
- Не принимаются Syslog-сообщения от активов
- Не принимаются сообщения от службы обнаружения вторжений
- Не принимаются сообщения от службы корреляции
- Не инициализируются сервисы udv-opensearch, udv-opensearch-dashboards, udv-logstash модуля «Управление внешними событиями»
- Не создается индекс в экспертном режиме страницы «События»
- Не удается отфильтровать записи в экспертном режиме страницы «События» по новым значениям полей после нормализации
- Объекты мониторинга и визуализации импортируются с ошибкой
- Не удается импортировать сканер сбора данных в веб-интерфейсе
- Не выполняется архивация внешних событий при превышении размера или времени хранения индекса
- Ошибки вида «<...>Cannot start service <...>. Bind for <ip_address>:<TCP/UDP_port> is ready allocated» при попытке запуска сервисов
- При бездействии в веб-интерфейсе сеанс завершается раньше, чем через 10 минут
- Ошибки поиска уязвимостей в базах CVE, CPE и БДУ ФСТЭК России
- Не устанавливается соединение с сенсором
- Не работает сложное исключение для правила службы обнаружения вторжений
- Обнаружен конфликт версий проектов ПЛК
- Каталог проекта ПЛК содержит информацию других файлов
- Путь к файлу превышает допустимую длину

21.2.1. Веб-интерфейс не загружается

В качестве причины недоступности веб-интерфейса рассмотрены следующие:

- Некорректная инициализация сервисов Комплекса
- Некорректная генерация серверного сертификата и ключа Комплекса уровня Management
- Запрет на доступ к веб-интерфейсу Комплекса с текущей рабочей станции
- Отсутствие свободного места на диске

Некорректная инициализация сервисов Комплекса

Способ устранения

Для устранения затруднения:

1. Подключитесь к операционной системе Комплекса.
2. Просмотрите состояние сервисов, выполнив команду:

   ```
   systemctl list-units udv-* --all
   ```

   > Внимание:
   >
   > `Все сервисы в полученном списке должны быть в состоянии active (поле Active).` Сервисы `udv-event-correlator.service` (при наличии модуля «Управление внешними событиями» в комплекте поставки) и `udv-sensor-registrar.service` могут штатно находиться в состоянии `inactive (dead)`, так как их запуск выполняется по необходимости в процессе работы Комплекса.

3. Если какие-либо сервисы не запущены или имеют статус, отличный от `active`, остановите работу сервисов, выполнив команду:

   ```
   systemctl stop udv-* --all
   ```

4. Дождитесь остановки работы всех сервисов.
5. В рабочей директории Комплекса уровня Management проверьте и, в случае необходимости, откорректируйте файл `manager.env`.
6. В рабочей директории Комплекса уровня Sensor проверьте и, в случае необходимости, откорректируйте файл `sensor.env`.
7. В случае необходимости восстановите данные из резервной копии.

   > Подсказка:
   >
   > Порядок восстановления данных приведен в разделе «Восстановление данных из резервных копий».

8. Запустить работу сервисов командой:

   ```
   systemctl start udv-* --all
   ```

9. Дождитесь запуска работы всех сервисов.

   > Внимание:
   >
   > При запуске не должно быть ошибок или предупреждений.

Некорректная генерация серверного сертификата и ключа Комплекса уровня Management

Способ устранения

Для устранения затруднения:

1. Убедитесь, что серверный сертификат и ключ в директории `/var/cache/udv/nginx/certs` корректно инициализированы, срок действия сертификата не истек. При необходимости сгенерируйте или замените сертификат и ключ.
2. Убедитесь, что файл серверного сертификата имеет расширение `.cert`.
3. Убедитесь, что значение переменной `HOST_IP` в файле `manager.env` соответствует значению IP-адреса сетевого интерфейса. Для этого выполните команду:

   ```
   cat /usr/share/udv/datapk/manager.env | grep HOST_IP
   ```

4. Если значение переменной не соответствует значению IP-адреса сетевого интерфейса, выполните следующие действия:

   а. Остановите работу сервисов, выполнив команду:

   ```
   systemctl stop udv-* --all
   ```

   б. Откройте файл `manager.env` на редактирование, выполнив команду:

   ```
   mcedit /usr/share/udv/datapk/manager.env
   ```

   в. Измените значение переменной `HOST_IP`.

   г. Сохраните изменения в файле, нажав клавишу **F10**, и подтвердите сохранение изменений, выбрав **Yes**.

   д. Запустите работу сервисов, выполнив команду:

   ```
   systemctl start udv-* --all
   ```

Запрет на доступ к веб-интерфейсу Комплекса с текущей рабочей станции

Способ устранения

Для устранения затруднения:

1. Убедитесь, что в правилах межсетевого экрана `iptables` в файле `/etc/sysconfig/iptables` не указаны правила, разрешающие доступ к веб-интерфейсу Комплекса только с рабочих станций определенной подсети и запрещающий доступ со всех остальных. Для этого проверьте наличие следующего правила:

   ```
   -A INPUT -p tcp -s [IP-адрес_подсети/маска_подсети] -m state --state NEW -m tcp
   --dport 443 -j ACCEPT
   ```

2. Если правила присутствуют в файле `/etc/sysconfig/iptables`, выполните вход в веб-интерфейс Комплекса из подсети, разрешенной правилами.

Отсутствие свободного места на диске

Способ устранения

Для устранения затруднения:

1. Проверьте свободное место на диске, выполнив команду:

   ```
   df -h /
   ```

2. При отсутствии свободного места:

а. Остановите сервисы Комплекса.

б. Удалите ненужные данные с диска.

в. Запустите сервисы Комплекса.

21.2.2. Время на Комплексе отличается от времени получения события

В качестве причин некорректного отображения времени в Комплексе рассмотрены следующие:

- Время на активе отличается от времени на операционной системе Комплекса
- Время на рабочей станции отличается от времени на операционной системе Комплекса
- Некорректная настройка часового пояса в операционной системе Комплекса
- Часовой пояс в базе данных PostgreSQL отличается от часового пояса на сервере Комплекса

Время на активе отличается от времени на операционной системе Комплекса

Способ устранения

Для устранения затруднения:

1. Авторизуйтесь на операционной системе актива.
2. Измените часовой пояс операционной системы.
3. При необходимости перезагрузите актив.

Время на рабочей станции отличается от времени на операционной системе Комплекса

Способ устранения

Для устранения затруднения:

1. Авторизуйтесь на рабочей станции, с которой ведется работа с веб-интерфейсом Комплекса уровня Management.
2. Измените часовой пояс рабочей станции так, чтобы он совпадал с часовым поясом Комплекса.

Некорректная настройка часового пояса в операционной системе Комплекса

Способ устранения

Для устранения затруднения:

1. Авторизуйтесь на операционной системе Комплекса уровня Management.
2. Настройте синхронизацию времени Комплекса с NTP-сервером.

> Подсказка:
>
> Подробнее о настройке NTP-сервера см. в инструкции Руководства по внедрению и поддержке «Настройка сертифицированной ОС Альт Сервер 10.2 SP».

Часовой пояс в базе данных PostgreSQL отличается от часового пояса на сервере Комплекса

Способ устранения

Для устранения затруднения:

1. Убедитесь, что часовые пояса на сервере и в базе данных `PostgreSQL` не совпадают:
    a. Команда покажет часовой пояс сервера:

    ```
    timedatectl show
    ```

    б. Команда покажет часовой пояс базы данных:

    ```
    cat /var/lib/pgsql/data/postgresql.conf | grep "^timezone ="
    ```

2. Если часовые пояса не совпадают, при необходимости измените часовой пояс сервера.

> Подсказка:
>
> Подробнее об изменении часового пояса Комплекса см. в инструкции Руководства по внедрению и поддержке «Изменение часового пояса»

3. Измените часовой пояс базы данных так, чтобы он совпадал с часовым поясом сервера. Для этого:
    a. Откройте для редактирования конфигурационный файл сервиса базы данных:

    ```
    mcedit /usr/share/udv/postgresql/postgresql.conf
    ```

    б. В строке `timezone` укажите тот же часовой пояс, что на сервере.

> Важное замечание:
>
> При изменении часового пояса на более ранний, чем предыдущий (сдвиг в минус), старые события могут оказаться новее по времени, чем новые события. Учитывайте это при работе с данными.

    в. Сохраните внесенные изменения, нажав клавишу **F10**, и подтвердите сохранение изменений, выбрав **Да** или **Yes**.
4. Перезагрузите сервис `udv-postgresql` командой:

```
sudo systemctl restart udv-postgresql.service
```

См. также

Отображение времени в Комплексе

21.2.3. После запуска Комплекса при попытке загрузки веб-интерфейса открывается пустая страница

Причина: некорректный файл environment.json, либо его отсутствие

Способ устранения

Для устранения затруднения:

1. Проверьте наличие и корректность файла `environment.json` в директории `/usr/share/udv/frontend`, расположенной в рабочей директории Комплекса уровня Management.
2. При необходимости переустановите сервис `udv-frontend`, выполнив команду:

```
apt-get install --reinstall udv-frontend -y
```

- **Результат шага:** Если файл `environment.json` был изменен или удален, при переустановке сервиса `udv-frontend` он будет восстановлен до состояния по умолчанию.

21.2.4. 502-я ошибка при загрузке страницы авторизации, 500-е ошибки сразу после авторизации

В качестве причин ошибок в веб-интерфейсе Комплекса рассмотрены следующие:

- Комплекс не до конца инициализировался после запуска работы сервисов
- Некорректно настроены правила межсетевого экрана для доступа к сервисам Комплекса
- Отсутствие свободного места на диске

Комплекс не до конца инициализировался после запуска работы сервисов

Способ устранения

Для устранения затруднения:

1. Подождите 3-5 минут после запуска сервисов.
2. При повторяющихся ошибках выполните команду:

   ```
   systemctl list-units udv-* --all
   ```

3. Все сервисы должны быть в состоянии `active`. При ошибках в журналах сервисов см. п. «Некорректная инициализация сервисов Комплекса» в разделе «Веб-интерфейс не загружается».

Некорректно настроены правила межсетевого экрана для доступа к сервисам Комплекса

Способ устранения

Для устранения затруднения:

1. Убедитесь, что на Комплексе уровня установлены корректные правила межсетевого экранирования `iptables` в файле `/etc/sysconfig/iptables`.

   > Прим.:
   >
   > Подробнее о настройках правил межсетевого экранирования см. в разделах:
   > - для Комплекса уровня Management — шаг 7 раздела «Установка базового модуля (Core) Комплекса уровня Management»;
   > - для Комплекса уровня Sensor — шаг 7 раздела «Установка базового модуля (Core) Комплекса уровня Sensor».

2. При необходимости настройте правила `iptables`:

   a. Остановите работу сервисов, выполнив команду:

   ```
   systemctl stop udv-* --all
   ```

   б. Откройте для редактирования конфигурационный файл `iptables` с правилами межсетевого экранирования:

```
mcedit /etc/sysconfig/iptables
```

в. Добавьте правила в конфигурационный файл `iptables` в зависимости от конфигурации Комплекса согласно шагу 1.

г. Перезапустите сервис `iptables`:

```
systemctl restart iptables
```

д. Запустите работу сервисов, выполнив команду:

```
systemctl start udv-* --all
```

Отсутствие свободного места на диске

Способ устранения

Для устранения затруднения:

1. Проверьте свободное место на диске, выполнив команду:

   ```
   df -h /
   ```

2. При отсутствии свободного места:

   а. Остановите сервисы Комплекса.

   б. Удалите ненужные данные с диска.

   в. Запустите сервисы Комплекса.

21.2.5. Не обнаруживаются новые сессии

В качестве причин отсутствия обнаружения новых сессий рассмотрены следующие:

- Некорректные настройки контролируемой сети на странице Сенсоры
- Комплекс получает информацию о новых сессиях с задержкой
- Некорректные настройки интерфейса сенсора, выполняющего прослушивание всего трафика контролируемой сети (listening interface)
- Некорректные настройки зеркалирования трафика на активном сетевом оборудовании (АСО) или отсутствие сетевого трафика
- Некорректное значение переменной сенсора LISTENING_INTERFACES
- Ошибки сервиса udv-zeek-wrapper

Некорректные настройки контролируемой сети на странице Сенсоры

Способ устранения

Для устранения проблемы:

1. На странице **Сенсоры** веб-интерфейса Комплекса убедитесь, что добавлены все контролируемые сети, которые прослушивают подключенные сенсоры.
2. Убедитесь, что IP-адрес актива принадлежит хотя бы одному из диапазонов адресов контролируемой сети сенсоров.
3. Выполните сканирование контролируемой сети (см. раздел «Сканирование сети и определение интерфейсов активного сетевого оборудования»).

Комплекс получает информацию о новых сессиях с задержкой

Способ устранения

Для устранения проблемы:

1. Выполните настройку контролируемой сети сенсоров согласно инструкции «Некорректные настройки контролируемой сети на странице Сенсоры».
2. Дождитесь обновления информации о сессиях на вкладке **Сессии** на странице **Инспекция сети → Сетевые соединения** (до 5 минут) — такая задержка допустима из-за особенностей передачи данных с сенсоров на Комплекс.

Некорректные настройки интерфейса сенсора, выполняющего прослушивание всего трафика контролируемой сети (listening interface)

Способ устранения

Для устранения проблемы:

1. Выведите информацию о прослушивающем интерфейсе, выполнив команду в операционной системе сенсора:

   ```
   ifconfig [наименование прослушивающего интерфейса сенсора]
   ```

   или:

   ```
   ip -a link show [наименование прослушивающего интерфейса сенсора]
   ```

   > Подсказка:
   >
   > Интерфейсы пишутся через запятую без пробелов.

2. Убедитесь, что интерфейс — в состоянии `UP` и режиме `PROMISC`.
3. При необходимости откорректируйте сетевые настройки.

Некорректные настройки зеркалирования трафика на активном сетевом оборудовании (АСО) или отсутствие сетевого трафика

Способ устранения

Для устранения проблемы:

1. Несколько раз выполните команду в операционной системе сенсора:

   ```
   ifconfig [наименование прослушивающего интерфейса сенсора]
   или:
   ip -s -s link show [наименование прослушивающего интерфейса сенсора]
   ```

2. Убедитесь, что параметр `RX packets` постепенно увеличивается.
3. Проверьте настройки зеркалирования на АСО. При необходимости откорректируйте их.
4. Убедитесь в наличии связи между интерфейсами АСО и сенсором.
5. Сгенерируйте сетевую активность. Для этого отправьте ICMP-пакеты с интерфейса сенсора на интерфейс любого актива.

Некорректное значение переменной сенсора LISTENING_INTERFACES

Способ устранения

Для устранения затруднения:

1. Остановите работу сервисов, выполнив команду:

   ```
   systemctl stop udv-* --all
   ```

2. Укажите значения слушающих интерфейсов в переменной `LISTENING_INTERFACES` файла `sensor.env`.

   > Подсказка:
   >
   > Переменная может быть представлена в виде списка интерфейсов через запятую, и одно из значений должно быть равно названию интерфейса сенсора, выполняющего прослушивание всего трафика.

3. Запустите сервисы, выполнив команду:

   ```
   systemctl start udv-* --all
   ```

Ошибки сервиса udv-zeek-wrapper

Способ устранения

Для устранения проблемы:

1. Просмотрите состояние сервисов, выполнив команду:

   ```
   systemctl list-units udv-*
   ```

   > Внимание:
   >
   > Все сервисы в полученном списке должны быть в состоянии `active` (поле **Active**).

2. Просмотрите журнал `udv-zeek-wrapper` на наличие критичных ошибок:

   ```
   journalctl -feu udv-zeek-wrapper
   ```

3. Убедитесь, что в начале инициализации `udv-zeek-wrapper` корректно подключился к базе, загрузил правила, и публикация событий о сессиях начата. При ошибках см. п. «Некорректная инициализация сервисов Комплекса» в разделе «Веб-интерфейс не загружается».

См. также

Правила сессий

21.2.6. Комплекс не обнаруживает активы в автоматическом режиме

В качестве причин отсутствия автоматического обнаружения активов рассмотрены следующие:

- Некорректные настройки контролируемой сети на странице «Сенсоры»
- Отсутствие трафика с актива

- Комплекс получает информацию о новых активах с задержкой
- Частичное зеркалирование сетевого трафика

Некорректные настройки контролируемой сети на странице «Сенсоры»

Способ устранения

Для устранения затруднения:

1. На странице **Сенсоры** веб-интерфейса Комплекса убедитесь, что добавлены все контролируемые сети, которые прослушивают подключенные сенсоры.
2. Убедитесь, что IP-адрес актива принадлежит хотя бы одному из диапазонов адресов контролируемой сети сенсоров.
3. Выполните сканирование контролируемой сети (см. раздел «Сканирование сети и определение интерфейсов активного сетевого оборудования»).

Отсутствие трафика с актива

Способ устранения

Для устранения затруднения:

Сгенерируйте сетевую активность требуемого актива. Для этого отправьте ICMP-трафик между интерфейсами сенсора и актива.

▸ **Результат шага:** при отсутствии проблем с обнаружением сессий требуемый актив должен появиться в списке активов на странице **Активы** веб-интерфейса Комплекса.

Комплекс получает информацию о новых активах с задержкой

Способ устранения

Для устранения затруднения:

1. Выполните настройку контролируемой сети сенсоров согласно п. выше «Некорректные настройки контролируемой сети на странице «Сенсоры»».
2. Сгенерируйте сетевую активность на активе согласно п. выше «Отсутствие трафика с актива».
3. Дождитесь обновления информации о сессиях на странице **Сессии** (до 5 минут) — такая задержка допустима из-за особенностей передачи данных с сенсоров на Комплекс.
4. Дождитесь обновления информации об активах на странице **Активы** (до 5 минут) — такая задержка допустима из-за особенностей передачи данных с сенсоров на Комплекс.

Частичное зеркалирование сетевого трафика

Способ устранения

Для устранения затруднения:

1. Создайте актив вручную на странице **Активы** веб-интерфейса Комплекса.
2. Отредактируйте сетевые настройки в реквизитах созданного актива.

> Подсказка:
>
> Подробнее см. раздел «Работа с активами».

21.2.7. Два актива с одинаковым IP-адресом

В списке на странице **Активы** отображается новый актив с IP-адресом актива, который уже был в списке. Возможные причины:

- При снятии трафика с нескольких точек актив был обнаружен с MAC-адресом маршрутизатора
- Один актив был обнаружен несколькими сенсорами

> Подсказка:
>
> Похожие ошибки см. в разделе «Рекомендуемые действия в случае обнаружения событий на странице «Контроль активов»».

При снятии трафика с нескольких точек актив был обнаружен с MAC-адресом маршрутизатора

> Подсказка:
>
> Если актив был обнаружен сперва со своим IP-адресом и MAC-адресом маршрутизатора, а уже после был распознан MAC-адрес самого актива, то на странице **Активы** будут отображаться оба актива (с одинаковым IP и разными MAC-адресами). Такое поведение необходимо для отслеживания попыток подмены MAC-адреса.

Способ устранения

Для устранения затруднения:

В карточке более раннего актива присвойте ему интерфейс с MAC-адресом маршрутизатора:

а. Перейдите в **карточку актива**.

б. Нажмите кнопку напротив блока **Сетевые атрибуты**.

- **Результат шага:** появится окно **Редактирование сетевых атрибутов актива**.

в. Отметьте параметр **Выбрать сетевой атрибут неизвестного актива**.

г. В выпадающем списке выберите интерфейс неизвестного актива с тем же IP-адресом.

д. Нажмите (**Создать сетевой атрибут**) для подтверждения изменений.

е. Установите чекбокс **Интерфейс для сбора данных** напротив интерфейса с собственным MAC-адресом.

ж. Нажмите (**Сохранить изменения**) для подтверждения изменений.

> Подсказка:
>
> Подробнее о присвоении активам интерфейсов других активов см. раздел «Редактирование актива».

- **Результат шага:** Актив, чей единственный интерфейс был привязан к другому активу, будет удален из списка на странице **Активы**.

Один актив был обнаружен несколькими сенсорами

Способ устранения

Для устранения затруднения:

В карточке одного актива присвойте ему интерфейс другого актива согласно инструкции в п. выше «При снятии трафика с нескольких точек актив был обнаружен с MAC-адресом маршрутизатора».

21.2.8. Не осуществляется сбор необходимых событий или конфигураций с активов

Для проблем со сбором событий или конфигураций могут быть следующие причины:

- Некорректные настройки актива
- Ошибки в Python-скрипте сбора данных, неверные настройки учетных данных актива или расписания задачи сбора данных

> Подсказка:
>
> Список возможных проблем сбора данных см. в разделе «Рекомендуемые действия в случае обнаружения событий на панели мониторинга «Сбор данных».

Некорректные настройки актива

Способ устранения

Для устранения затруднения:

1. Убедитесь в корректности настроек служб и разрешений для сбора данных с выбранного актива.
2. Убедитесь, что активу присвоены учетные данные с правами, которые:
   - позволяют получать информацию удаленно;
   - позволяют получать критичную информацию, запрашиваемую скриптом сбора данных.

Ошибки в Python-скрипте сбора данных, неверные настройки учетных данных актива или расписания задачи сбора данных

Способ устранения

Для устранения затруднения:

1. Проанализируйте сообщения об ошибках на страницах **Статус сбора**, **Задачи сбора**, **События**, на панели мониторинга Сбор данных и на диаграммах в карточке актива.
2. Просмотрите содержание Python-скриптов сбора данных из сканеров, работа которых завершается ошибками, и найдите в них названия сервисов, участвующих в сборе данных (коннекторов). Название расположено в скобках после команды `execute`.

```
table = execute('sql',protocol_args, expiration)
return {
    'visible_keys': {
        'ID': 'Идентификатор группы',
        'name': 'Имя группы',
        'EXPTIME': 'Параметры отключения пользователей',
    },
    'keys': ['ID','name','EXPTIME'],
    'data': [[str(row[col]) for col in ['ID','name','EXPTIME']] for row in table]
}
```

Рис. 460. Расположение названия коннектора в Python-скрипте сбора данных

3. На странице **Сенсоры** найдите сенсор, прослушивающий контролируемую сеть актива.
4. Подключитесь к операционной системе сенсора, который собирает данные из контролируемой сети актива.
5. Просмотрите список имеющихся сервисов-коннекторов:

```
systemctl list-units *-connector.service --all
```

- **Результат шага:** будет выведен список сервисов-коннекторов.

```
[root@DATAPKTESTTK22 ~]# systemctl list-units *-connector.service --all
  UNIT                                LOAD   ACTIVE SUB     DESCRIPTION
  udv-modbus-connector.service        loaded active running Modbus connector
  udv-opc-connector.service           loaded active running Opc connector service
  udv-plc-config-connector.service    loaded active running Config acquisition from PLC
  udv-plc-connector.service           loaded active running Data acquisition from PLC by oven and s7comm protocol.
  udv-snmp-connector.service          loaded active running SNMP connector
  udv-sql-connector.service           loaded active running Service for connecting to a database
  udv-terminal-connector.service      loaded active running Terminal connector

LOAD   = Reflects whether the unit definition was properly loaded.
ACTIVE = The high-level unit activation state, i.e. generalization of SUB.
SUB    = The low-level unit activation state, values depend on unit type.
7 loaded units listed.
To show all installed unit files use 'systemctl list-unit-files'.
```

Рис. 461. Список коннекторов Комплекса

6. Найдите подходящий коннектор.

> Подсказка:
>
> Название коннектора в выводе команды не полностью совпадает с названием в Python-скрипте сбора данных. За исключением `msrpc` название коннектора в выводе команды содержит `_connector`.

7. Просмотрите журналы коннекторов, на которых обнаружены проблемы. Например `udv-host-data-collector`:

```
journalctl -fu udv-host-data-collector.service
```

8. Посмотрите журналы сервиса `udv-command-processor`, который отвечает за все запущенные процессы сбора данных:

```
journalctl -fu udv-command-processor.service
```

9. При необходимости отредактируйте сканеры сбора данных, расписание задачи, учетные данные актива.

Альтернативный способ устранения

Для устранения затруднения:

1. Остановите работу сервисов Комплекса:

   ```
   systemctl stop udv-* --all
   ```

2. Откройте на редактирование конфигурационный файл `manager.env`.
3. Установите значение `DEBUG` для переменной `LOG_LEVEL`.
4. Сохраните и закройте файл.
5. Запустите сервисы Комплекса:

   ```
   systemctl start udv-* --all
   ```

6. Повторно выполните сбор данных.
7. Просмотрите журнал сообщений командой:

   ```
   journalctl -u название_сканера_сбора_событий -f -n 100
   ```

21.2.9. При попытке сбора данных в результатах выводится предупреждение «Превышено время ожидания выполнения задачи сбора событий»

Для получения предупреждения `Превышено время ожидания выполнения задачи сбора событий` возможны следующие причины:

- Актив не может принять несколько одновременных подключений к нему по одному или нескольким протоколам
- Переполнена очередь задач сбора данных в сервисе udv-rabbitmq Комплекса
- Заканчивается максимальное время ожидания выполнения задачи сбора данных

> Подсказка:
>
> Список возможных проблем сбора данных см. в разделе «Рекомендуемые действия в случае обнаружения событий на панели мониторинга «Сбор данных».

Актив не может принять несколько одновременных подключений к нему по одному или нескольким протоколам

Рекомендации по настройке запуска задач сбора данных с одного актива

Для устранения затруднения:

1. Настраивайте сбор событий с промежутком между запусками задач (для каждой задачи установите отдельное от остальных задач время выполнения).
2. Используйте сканеры сбора событий с ОС Windows, которые собирают только критичные события.
3. В одну задачу добавляйте не более одного сканера сбора данных.

Переполнена очередь задач сбора данных в сервисе udv-rabbitmq Комплекса

Способ устранения

Для устранения затруднения:

1. Перейдите в карточку актива (или нескольких активов), для которого настроено расписание задачи сбора данных.
2. Отмените выполнение одной или нескольких задач сбора данных по расписанию (отмените выбор чекбокса ☑ в строке с названием задачи).
3. Подключитесь к операционной системе Комплекса уровня Management.
4. Остановите работу сервисов, выполнив команду:

```
systemctl stop udv-* --all
```

5. Очистите очередь сервиса `udv-rabbitmq`. Для этого выполните команду:

```
rm -rf /var/lib/rabbitmq/mnesia/*
rm -rf /var/lib/rabbitmq-sensor/mnesia*
```

6. Если установлен модуль «Управление внешними событиями», очистите его очередь:

```
rm -rf /var/lib/rabbitmq/*
rm -rf /var/lib/rabbitmq-sensor/*
```

7. Перезагрузите Комплекс командой:

```
shutdown -r now
```

8. Запустите работу сервисов командой:

```
systemctl start udv-* --all
```

9. Дождитесь запуска работы всех сервисов.
10. Выполните повторный запуск сбора данных.

Заканчивается максимальное время ожидания выполнения задачи сбора данных

Способ устранения

Увеличьте максимальное время ожидания выполнения задачи сбора данных для одного сканера.

1. Перейдите на страницу **Администрирование → Инспекция активов → Сканеры**.
2. Откройте необходимый сканер сбора данных на редактирование.
3. Увеличьте значение в поле **Максимальное время ожидания выполнения задачи**.
4. Нажмите кнопку **Сохранить** для подтверждения изменений.
5. Дождитесь сбора задачи сбора данных, создайте новую или запустите сканер.

21.2.10. Сбор конфигураций осуществляется, но результаты сбора не отображаются

> Подсказка:
>
> Список возможных проблем сбора данных см. в разделе «Рекомендуемые действия в случае обнаружения событий на панели мониторинга «Сбор данных».

Причина: некорректный Python-скрипт сбора данных, неверное регулярное выражение

Способ устранения

Для устранения затруднения:

Проверьте на корректность Python-скрипт из сканера, работа которого завершается с ошибкой.

> Внимание:
>
> Для первого запуска рекомендуется отказаться от синтаксического разбора данных в скрипте посредством регулярных выражений.

21.2.11. Отсутствуют внутренние события на странице «События»

На странице **События** частично или полностью отсутствуют события. В качестве причин рассмотрены следующие:

- Генерация внутренних событий отключена в настройках переменных

Генерация внутренних событий отключена в настройках переменных

В конфигурационном файле `manager.env` Комплекса уровня Management переменным, отвечающим за отключение и включение генерации внутренних событий от служебных источников, присвоены значения `true` (генерация событий отключена).

Способ устранения

Для устранения затруднения:

Присвойте необходимым переменным значение `false` или удалите переменные из файла `manager.env`.

> Подсказка:
>
> Порядок работы с указанными переменными приведен в подразделе «Включение и отключение служебных источников» Руководства по эксплуатации.«Включение и отключение служебных источников».

21.2.12. Отсутствуют внешние события на странице «События»

На странице **События** частично или полностью отсутствуют события. В качестве причин рассмотрены следующие:

- Диск операционной системы Комплекса заполнен более, чем на 90%, и внешние события больше не принимаются

Диск операционной системы Комплекса заполнен более, чем на 90%, и внешние события больше не принимаются

Сервис хранения и поиска внешних событий недоступен в результате заполнения раздела диска, выделенного для хранения внешних событий, более, чем на 90%.

Способ устранения

Для устранения затруднения:

1. Авторизуйтесь на операционной системе Комплекса уровня Management.
2. Убедитесь, что сервис хранения и поиска событий недоступен:

```
journalctl -fu udv-logstash.service
```

- **Результат шага:** в журнале будут отображаться события вида `Opensearch в режиме read-only`.

3. Остановите работу сервисов Комплекса:

```
systemctl stop udv-* --all
```

4. Удалите ненужные файлы с дискового раздела.
5. При необходимости измените значения переменных `EVENT_INDICES_MAX_SIZE_GB` и `EVENT_ARCHIVES_MAX_SIZE_GB`:
   a. Откройте на редактирование файл `manager.env`.
   б. Найдите и измените значения переменных:

```
EVENT_INDICES_MAX_SIZE_GB=[значение]
EVENT_ARCHIVES_MAX_SIZE_GB=[значение]
```

> Внимание:
>
> Суммарный объем с `EVENT_ARCHIVES_MAX_SIZE_GB` не должен составлять более 50-60% объема дискового пространства
>
> На Комплексах базового уровня и (или) с HDD — не более 100 ГБ. На Комплексах среднего и верхнего уровней с SSD — не более 300 ГБ

6. Очистите репозиторий с пакетами.
7. Если предыдущие способы не дали результата, очистите метаданные сервиса.

> ОСТОРОЖНО:
>
> При очистке будут утеряны все индексы событий и элементы раздела **Мониторинг**: шаблон индекса, панели мониторинга, сохраненные поиски, фильтры.

Для очистки выполните команду:

```
rm -rf /var/lib/opensearch/nodes/*
```

8. Восстановите утерянные данные.

> Подсказка:
>
> Подробнее о настройке см. разделы «Создание шаблона индекса», «Импорт сохраненных объектов в экспертном режиме просмотра событий».

9. Запустите сервисы Комплекса:

```
systemctl start udv-* --all
```

10. Убедитесь в работоспособности сервиса хранения и поиска событий:
    a. Выполните следующий запрос:

```
curl -XPUT "http://127.0.0.1:9200/_settings" -H 'Content-Type: application/json' -d
 '{"index":{"blocks":{"read_only_allow_delete":"false"}}}'
```

▸ **Результат шага:** запись вида `"acknowledged":true` свидетельствует об успешном выполнении запроса.

б. Выполните действия, в результате которых должны появиться события.

> Подсказка:
>
> Например, создайте и удалите новые элементы справочников (правил, классификаторов), выполните сбор событий или конфигураций с актива.

в. Перейдите на страницу **События**.

г. Найдите события по результатам выполненных действий.

11. Если события отсутствуют, ознакомьтесь с инструкциями ниже по устранению нештатных ситуаций.

См. также

Не инициализируются сервисы udv-opensearch, udv-opensearch-dashboards, udv-logstash модуля «Управление внешними событиями»

21.2.13. Не принимаются Syslog-сообщения от активов

Для отсутствия сообщений Syslog от активов могут быть следующие причины:

- Наименование актива не совпадает с сетевым именем (hostname) узла или в списке активов присутствуют активы с такими же IP-адресами
- Не создан или некорректно создан источник для приема Syslog-сообщений
- Некорректная настройка отправки Syslog-сообщений на активе

Наименование актива не совпадает с сетевым именем (hostname) узла или в списке активов присутствуют активы с такими же IP-адресами

Способ устранения

Для устранения затруднения:

1. Убедитесь, что наименование актива совпадает с его hostname.
2. Убедитесь в отсутствии известных активов с такими же IP-адресами.

Не создан или некорректно создан источник для приема Syslog-сообщений

Способ устранения

Для устранения затруднения:

Убедитесь, что источник для приема Syslog-сообщений выбранного актива корректно инициализирован на странице **Администрирование → Настройка активов → Источники**.

Некорректная настройка отправки Syslog-сообщений на активе

Способ устранения

Для устранения затруднения:

Проверьте настройки отправки Syslog-сообщений на активе, убедитесь, что актив отправляет события на требуемый IP-адрес и порт.

21.2.14. Не принимаются сообщения от службы обнаружения вторжений

Причина: наименование служебного актива не совпадает с сетевым именем (hostname) Комплекса

Способ устранения

Для устранения затруднения:

1. Убедитесь, что наименование Комплекса уровня Management совпадает с его сетевым именем на странице **Администрирование → О системе**.
2. Подключитесь к операционной системе Комплекса уровня Management.
3. Выполните команду `export`. Убедитесь, что переменная `HOSTNAME` присутствует в выводе команды и содержит сетевое имя Комплекса.
4. Если переменная `HOSTNAME` отсутствует в выводе команды `export`:
    а. Остановите работу сервисов Комплекса без удаления накопленных данных.
    б. Откройте файл `/etc/profile` в режиме редактирования с помощью редактора `mcedit`:

    ```
    mcedit /etc/profile
    ```

    в. Добавьте в конец файла строку:

    ```
    export HOSTNAME
    ```

    г. Сохраните изменения и закройте файл `/etc/profile`.
    д. Перезагрузите сеанс пользователя или перезагрузите ОС.
    е. Запустите работу сервисов Комплекса.
    ж. Убедитесь, что наименование Комплекса совпадает с его сетевым именем на странице **Администрирование → О системе**.

21.2.15. Не принимаются сообщения от службы корреляции

В качестве причин рассмотрены следующие:

- Наименование служебного актива не совпадает с сетевым именем (hostname) Комплекса
- Некорректная или устаревшая директория logstash

Наименование служебного актива не совпадает с сетевым именем (hostname) Комплекса

Способ устранения

Для устранения затруднения:

1. Убедитесь, что наименование Комплекса уровня Management совпадает с его сетевым именем на странице **Администрирование → О системе**.
2. Подключитесь к операционной системе Комплекса уровня Management.
3. Выполните команду `export`. Убедитесь, что переменная `HOSTNAME` присутствует в выводе команды и содержит сетевое имя Комплекса.

4. Если переменная `HOSTNAME` отсутствует в выводе команды `export`:
    а. Остановите работу сервисов Комплекса без удаления накопленных данных.
    б. Откройте файл `/etc/profile` в режиме редактирования с помощью редактора `mcedit`:

    ```
    mcedit /etc/profile
    ```

    в. Добавьте в конец файла строку:

    ```
    export HOSTNAME
    ```

    г. Сохраните изменения и закройте файл `/etc/profile`.
    д. Перезагрузите сеанс пользователя или перезагрузите ОС.
    е. Запустите работу сервисов Комплекса.
    ж. Убедитесь, что наименование Комплекса совпадает с его сетевым именем на странице **Администрирование → О системе**.

Некорректная или устаревшая директория logstash

Способ устранения

Для устранения затруднения:

1. Остановите работу сервисов, выполнив команду:

    ```
    systemctl stop udv-* --all
    ```

2. Дождитесь остановки работы всех сервисов.
3. Переустановите сервис `udv-logstash`, выполнив команду:

    ```
    apt-get install --reinstall udv-logstash -y
    ```

4. Запустите работу сервисов командой:

    ```
    systemctl start udv-* --all
    ```

5. Дождитесь запуска работы всех сервисов.

21.2.16. Не инициализируются сервисы udv-opensearch, udv-opensearch-dashboards, udv-logstash модуля «Управление внешними событиями»

Возможны следующие причины:

- Некорректное значение системной переменной vm.max_map_count
- Ошибки в настройках нормализациии

Некорректное значение системной переменной vm.max_map_count

Способ устранения

Для устранения затруднения:

1. Проверьте значение переменной в операционной системе Комплекса уровня Management. Для этого выполните команду:

    ```
    sysctl vm.max_map_count
    ```

2. Убедитесь, что данная переменная имеет значение `262144`.
3. При необходимости откорректируйте значение переменной. Для этого:
    a. Откройте файл `/etc/sysctl.conf`.
    б. Добавьте строку `vm.max_map_count=262144`.
    в. Либо, если строка с переменной уже была добавлена, измените значение переменной.
4. Выполните команду для немедленной установки переменной `vm.max_map_count` (без перезагрузки):

```
sysctl -w vm.max_map_count=262144
```

Ошибки в настройках нормализациии

Способ устранения

Для устранения затруднения:

1. Посмотрите журнал сервиса `udv-logstash`. Для этого введите команду:

```
journalctl -fu udv-logstash.service
```

2. Остановите работу сервисов, выполнив команду:

```
systemctl stop udv-* --all
```

3. Дождитесь остановки работы всех сервисов.
4. Переустановите сервис `udv-logstash`, выполнив команду:

```
apt-get install --reinstall udv-logstash -y
```

5. Запустите работу сервисов командой:

```
systemctl start udv-* --all
```

6. Дождитесь запуска работы всех сервисов.

См. также

Отсутствуют внешние события на странице «События»

21.2.17. Не создается индекс в экспертном режиме страницы «События»

Причина: отсутствуют события в Комплексе

Способ устранения

Для устранения затруднения:

1. Сгенерируйте события действий в веб-интерфейсе.

Подсказка:

Например, создайте и удалите новые элементы справочников (правил, классификаторов), выполните сбор событий или конфигураций с актива.

2. Создайте или включите источники активов и сгенерируйте на них события.

21.2.18. Не удается отфильтровать записи в экспертном режиме страницы «События» по новым значениям полей после нормализации

Причина: отсутствуют события с новыми полями, не обновлен шаблон индекса

Способ устранения

Для устранения затруднения:

1. Обновите шаблон индекса на странице **Администрирование → Настройки мониторинга**, вкладка **Шаблоны Индексов**.
2. Убедитесь, что после нормализации было принято событие с новыми полями (помеченными желтым восклицательным знаком на странице **События → Экспертный режим**).

21.2.19. Объекты мониторинга и визуализации импортируются с ошибкой

Причина: отсутствуют нужные поля в шаблоне индекса

Способ устранения

Для устранения затруднения:

1. Убедитесь в целостности директории `/etc/logstash`, расположенном в рабочей директории Комплекса уровня Management.
2. Убедитесь, что все нужные поля присутствуют в шаблоне индекса.
3. При отсутствии необходимых полей:
    а. Обновите шаблон индекса.
    б. Убедитесь, что было принято событие с новыми полями.
    в. Удалите сохраненные объекты (страница **Мониторинг → Настройки мониторинга**, вкладка **Сохраненные Объекты**).
    г. Повторите импорт.

См. также

Импорт сохраненных объектов в экспертном режиме просмотра событий

21.2.20. Не удается импортировать сканер сбора данных в веб-интерфейсе

Для проблем с импортом сканера сбора данных могут быть следующие причины:

- Неверная цепочка сертификатов для проверки цифровой подписи Python-скрипта в сканере
- Неверная кодировка Python-скрипта сбора данных
- Сканер сбора данных был изменен с момента создания его последней цифровой подписи

Неверная цепочка сертификатов для проверки цифровой подписи Python-скрипта в сканере

Способ устранения

Для устранения затруднения:

1. Убедитесь, что конечный сертификат `datapk_script.crt`, используемый для проверки подлинности Python-скриптов сбора данных, является клиентским для корневого сертификата `ca.crt`. Для этого выполните следующую команду:

   ```
   openssl verify
    -CAfile /usr/share/udv/certs/ca.crt /usr/share/udv/scripts-certs/datapk_script.crt
   ```

   ▸ **Результат шага:** если верификация пройдет успешно, в командную строку будет выведена следующая информация:

   ```
   /usr/share/udv/scripts-certs/datapk_script.crt: OK
   ```

2. При необходимости замените конечный сертификат `datapk_script.crt` и повторно выполните верификацию.
3. Повторно выполните цифровую подпись Python-скрипта. Подробнее см. раздел «Цифровая подпись Python-скрипта».
4. Создайте новый сканер или измените существующий, импортировав в него новый Python-скрипт и его цифровую подпись. Либо импортируйте набор сканеров с новыми цифровыми подписями в веб-интерфейсе Комплекса.

Неверная кодировка Python-скрипта сбора данных

Способ устранения

Для устранения затруднения:

1. Откройте Python-скрипт сбора данных с помощью текстового редактора.
2. Убедитесь, что Python-скрипт имеет кодировку UTF-8 без BOM. При необходимости измените кодировку и сохраните изменения.
3. Повторно выполните цифровую подпись Python-скрипта. Подробнее см. раздел «Цифровая подпись Python-скрипта».
4. Создайте новый сканер или измените существующий, импортировав в него новый Python-скрипт и его цифровую подпись. Либо импортируйте набор сканеров с новыми цифровыми подписями в веб-интерфейсе Комплекса.

Сканер сбора данных был изменен с момента создания его последней цифровой подписи

Python-скрипт, размещенный и подписываемый в операционной системе Комплекса, не совпадает со скриптом, размещенным на локальной ОС и загружаемым в веб-интерфейсе Комплекса) при создании сканера.

Способ устранения

Для устранения затруднения:

1. Убедитесь в целостности Python-скрипта сбора данных.
2. Повторно выполните цифровую подпись Python-скрипта. Подробнее см. раздел «Цифровая подпись Python-скрипта».
3. Создайте новый сканер или измените существующий, импортировав в него новый Python-скрипт и его цифровую подпись. Либо импортируйте набор сканеров с новыми цифровыми подписями в веб-интерфейсе Комплекса.

См. также

Создание сканера сбора данных

Управление сканерами сбора данных

Импорт сканеров и их групп

21.2.21. Не выполняется архивация внешних событий при превышении размера или времени хранения индекса

Возможны следующие причины:

- Директориям, в которые выполняется загрузка архивов, не присвоены права для загрузки в них файлов
- В переменной файла manager.env настроено удаление индексов вместо сохранения в архив

Директориям, в которые выполняется загрузка архивов, не присвоены права для загрузки в них файлов

Способ устранения

Для устранения затруднения:

1. Подключитесь к операционной системе Комплекса уровня Management.
2. Убедитесь, что следующим директориям, расположенным в рабочей директории Комплекса уровня Management, присвоены права доступа `drwxrwxrwx`:
    - `/var/backups/elasticsearch`:
        - `/var/backups/elasticsearch/indices`
        - `/var/backups/elasticsearch/uploads`

    Для этого введите команду:

    ```
    ls -la [путь к директории]
    ```
3. При необходимости измените права на указанные директории с помощью следующих команд:

    ```
    chmod -R 777 /var/backups/elasticsearch
    ```

    где ключ `-R` — рекурсивное изменение прав (они будут применены и к вложенным директориям).
4. Повторно выполните архивацию событий (индексов) через веб-интерфейс Комплекса (подробнее см. раздел «Выгрузка внешних событий Комплекса в архив»).

В переменной файла manager.env настроено удаление индексов вместо сохранения в архив

Способ устранения

Для устранения затруднения:

1. Остановите работу сервисов, выполнив команду:

    ```
    systemctl stop udv-* --all
    ```
2. В конфигурационном файле `manager.env` присвойте переменной `EVENT_INDICES_ACTION_SIZE_EXCEEDED` значение `rotate`.
3. Запустите работу сервисов командой:

```
systemctl start udv-* --all
```

4. Дождитесь запуска работы всех сервисов.

21.2.22. Ошибки вида «<...>Cannot start service <...>. Bind for <ip_address>:<TCP/UDP_port> is ready allocated» при попытке запуска сервисов

Причина: указанный в тексте ошибки TCP или UDP-порт требуется для запуска сервиса, но он занят сторонним сервисом или утилитой

Способ устранения

Для устранения затруднения:

1. Измените номер используемого порта для стороннего сервиса в настройках сервиса.
2. При невозможности изменения номера порта отключите сторонний сервис, которым занят порт:
    a. Узнайте наименование сервиса, которым занят порт, с помощью команды:

```
ss -tulpn | grep [номер_порта]
```

▸ **Результат шага:** в выводе команды в последнем столбце отображаются наименование сервиса, занятый им порт и идентификатор процесса.

```
[root@datapk-vm-develop-244-3 ~]# ss -tulpn | grep 9300
tcp   LISTEN 0      4096               [::1]:9300          [::]:*    users:(("java",pid=13494,fd=149))

tcp   LISTEN 0      4096   [::ffff:127.0.0.1]:9300            *:*    users:(("java",pid=13494,fd=150))
```

Рис. 462. Наименование сервиса, занятый им порт и идентификатор процесса в последнем столбце вывода команды

    б. Остановите процесс с полученным номером:

```
kill -9 [идентификатор_процесса]
```

    в. При необходимости остановки процесса и его дочерних процессов:

```
killall [идентификатор_процесса]
```

    г. Повторите запуск работы сервисов Комплекса.

21.2.23. При бездействии в веб-интерфейсе сеанс завершается раньше, чем через 10 минут

В качестве причин раннего завершения сеанса рассмотрены следующие:

- Время завершения сеанса пользователя при бездействии задано меньше 10 минут
- Под уже используемой учетной записью совершил вход другой пользователь

Время завершения сеанса пользователя при бездействии задано меньше 10 минут

Время бездействия в веб-интерфейсе, после которого текущая сессия пользователя автоматически завершается и происходит переход на страницу авторизации, настраивается в переменной `USER_SESSION_INACTIVITY_TIMEOUT` файла `manager.env` Комплекса уровня Management.

Значение по умолчанию — 600 секунд, однако вы можете указать любое значение, включая интервалы менее 600 секунд.

Способ устранения

Для устранения затруднения:

1. Перейдите в командную строку операционной системы Комплекса уровня Management.
2. Остановите работу сервисов, выполнив команду:

```
systemctl stop udv-* --all
```

3. Дождитесь остановки работы всех сервисов.
4. В конфигурационном файле `manager.env` присвойте переменной `USER_SESSION_INACTIVITY_TIMEOUT` необходимый лимит времени бездействия в секундах.
5. Запустить работу сервисов командой:

```
systemctl start udv-* --all
```

6. Дождитесь запуска работы всех сервисов.

Результат шага: сессия пользователей будет завершаться после времени бездействия, указанного в переменной `USER_SESSION_INACTIVITY_TIMEOUT`.

Под уже используемой учетной записью совершил вход другой пользователь

Ограничение на количество сессий под одной учетной записью настраивается в переменной `LIMIT_USER_SESSIONS` файла `manager.env` Комплекса уровня Management. По умолчанию разрешается вход с неограниченного количества устройств под одной учетной записью (переменная имеет значение `false`) — при создании новой сессии предыдущая завершается.

Способ устранения

Для устранения затруднения:

1. При необходимости создайте в веб-интерфейсе новые учетные записи для других пользователей.
2. При необходимости отключите ограничение на вход под одной учетной записью:
    a. Остановите работу сервисов, выполнив команду:

```
systemctl stop udv-* --all
```

    б. В конфигурационном файле `manager.env` добавьте переменную `LIMIT_USER_SESSIONS` и установите ей значение `false`.
    в. Запустите работу сервисов командой:

```
systemctl start udv-* --all
```

    г. Дождитесь запуска работы всех сервисов.

Результат шага: станет возможным вход в веб-интерфейс под любой учетной записью с любого количества устройств.

21.2.24. Ошибки поиска уязвимостей в базах CVE, CPE и БДУ ФСТЭК России

Результаты поиска уязвимостей в базах CVE и CPE отображаются через 5 минут после завершения поиска. Однако возможны следующие ошибки:

- Ошибка вида «Не удалось получить список ПО. Убедитесь, что данные об установленном ПО были собраны корректно»
- Ошибка вида «Не удалось сохранить отчет. Убедитесь в работоспособности Комплекса или обратитесь к администратору»
- Ошибка вида «Непредвиденная ошибка. Убедитесь в работоспособности Комплекса или обратитесь к администратору»
- Ошибка вида «ПО для сканирования уязвимостей в реестре CPE не обнаружено»

21.2.24.1. Ошибка вида «Не удалось получить список ПО. Убедитесь, что данные об установленном ПО были собраны корректно»

Возможны следующие причины:

- Не удается запустить сканер сбора списка ПО, либо запуск завершается с ошибками
- Сканер запустился, но не отображает результаты на странице «Список ПО»

Не удается запустить сканер сбора списка ПО, либо запуск завершается с ошибками

Способ устранения

Для устранения затруднения перейдите в раздел «Не осуществляется сбор необходимых событий или конфигураций с активов» или «При попытке сбора данных в результатах выводится предупреждение «Превышено время ожидания выполнения задачи сбора событий»».

Сканер запустился, но не отображает результаты на странице «Список ПО»

Способ устранения

Для устранения затруднения перейдите в раздел «Сбор конфигураций осуществляется, но результаты сбора не отображаются».

21.2.24.2. Ошибка вида «Не удалось сохранить отчет. Убедитесь в работоспособности Комплекса или обратитесь к администратору»

Возможны следующие причины:

- Отсутствие свободного места на диске
- Ошибки в сервисе udv-vulnerability-backend

Отсутствие свободного места на диске

Способ устранения

Для устранения затруднения:

1. Проверьте свободное место на диске, выполнив команду:

   ```
   df -h /
   ```

2. При отсутствии свободного места:

а. Остановите сервисы Комплекса.

б. Удалите ненужные данные с диска.

в. Запустите сервисы Комплекса.

Ошибки в сервисе udv-vulnerability-backend

Способ устранения

Для устранения затруднения:

1. Убедитесь, что в журнале системных сообщений сервиса `udv-vulnerability-backend` нет ошибок, по команде:

   ```
   journalctl -fu udv-vulnerability-backend.service
   ```

2. При ошибках в журналах сервисов см. п. «Некорректная инициализация сервисов Комплекса» в разделе «Веб-интерфейс не загружается».

21.2.24.3. Ошибка вида «Непредвиденная ошибка. Убедитесь в работоспособности Комплекса или обратитесь к администратору»

Причина: ошибки в сервисе поиска уязвимостей

Способ устранения

Для устранения затруднения:

1. Убедитесь, что в журналах системных сообщений сервиса `udv-vulnerability-backend` нет ошибок, по команде:

   ```
   journalctl -fu udv-vulnerability-backend.service
   ```

2. При ошибках в журналах сервисов см. п. «Некорректная инициализация сервисов Комплекса» в разделе «Веб-интерфейс не загружается».

21.2.24.4. Ошибка вида «ПО для сканирования уязвимостей в реестре CPE не обнаружено»

Причина: для ПО, по которому выполнялся поиск уязвимостей, элементы CPE подобраны с недостаточной точностью, либо их не удалось подобрать

Способ устранения

Для устранения затруднения перейдите в раздел «Выгрузка отчета по результатам сопоставления собранного ПО со справочником CPE».

21.2.25. Не устанавливается соединение с сенсором

В качестве причины недоступности сенсора при первом подключении рассмотрены следующие:

- Отключен межсетевой экран iptables на сенсоре или Комплексе уровня Management
- Некорректные настройки подключения сенсора

Если сенсор стал недоступен в процессе корректной работы, см. причину «Ошибки в работе сервисов в период корректной работы иерархии».

Отключен межсетевой экран iptables на сенсоре или Комплексе уровня Management

> Внимание:
>
> Если сенсор или Комплекс установлены на ОС Альт Сервер, необходимо использовать `iptables` в качестве межсетевого экрана.

Способ устранения

Для устранения затруднения:

1. В командной строке операционной системы сенсора:
    a. Убедитесь, что межсетевой экран `efw` не запущен и не будет конфликтовать с `iptables`:

    ```
    grep CONFIG_FW /etc/net/ifaces/default/options
    ```

    > Внимание:
    >
    > Значение параметра `CONFIG_FW` должно быть `no`.

    б. Убедитесь, что межсетевой экран `iptables` запущен:

    ```
    systemctl status iptables
    ```

    > Подсказка:
    >
    > Сервис должен быть в состоянии `active`.

    в. При необходимости выполните настройки `iptables` сенсора и запустите `iptables` согласно инструкциям в следующих разделах Руководства по внедрению и поддержке:
    - «Установка Комплекса уровня Sensor» и «Установка Комплекса уровня Management» (при установке сенсора и Комплекса уровня Management на разных серверах);
    - «Установка Комплекса уровня Management+Sensor на одном аппаратном средстве» (при установке сенсора и Комплекса уровня Management на одном сервере).
2. Выполните шаг 1 в командной строке операционной системы Комплекса уровня Management.

Некорректные настройки подключения сенсора

Способ устранения

Для устранения затруднения убедитесь в корректности настроек подключения сенсора к Комплексу уровня Management — для этого вы можете воспользоваться инструкцией «Подключение сенсора к другому Комплексу уровня Management».

Ошибки в работе сервисов в период корректной работы иерархии

Способ устранения

Если сенсор стал недоступен в процессе корректной работы, ошибки будут отображаться на странице **Сенсоры** веб-интерфейса Комплекса. В таблице ниже приведен список возможных ошибок, причины их возникновения и сервисы, работоспособность которых необходимо проверить.

Табл. 125. Возможные ошибки в процессе работы иерархии

НАИМЕНОВАНИЕ ОШИБКИ	ВОЗМОЖНАЯ ПРИЧИНА	СЕРВИС, ОТВЕЧАЮЩИЙ ЗА РАБОТУ ИЕРАРХИИ
Не удается получить статус	Не поступает информация о состоянии сервисов `udv-rabbitmq`, `udv-rabbitmq-sensor`, `udv-redis` или `udv-redis-sensor`	Уровень Sensor: • `udv-node-exporter-sensor` • `udv-pushgateway` Уровень Management: • `udv-node_exporter` • `udv-prometheus`
Получение данных недоступно	Затруднения в работе сервиса отправки оперативных данных с сенсора	`udv-rabbitmq-sensor` (уровень Sensor)
	Затруднения в работе сервиса получения оперативных данных с сенсора на Комплексе	`udv-rabbitmq` (уровень Management)
Синхронизация настроек недоступна	Затруднения в работе сервиса отправки справочников с Комплекса на сенсор	`udv-redis` (уровень Management)
	Затруднения в работе сервиса получения справочников на сенсоре	`udv-redis-sensor` (уровень Sensor)
Не удается установить соединение с сенсором	Совокупность причин, приведенных выше	Все сервисы, приведенные выше

Для устранения затруднения:

1. Просмотрите ошибку на странице **Сенсоры** веб-интерфейса Комплекса.
2. По таблице выше определите список сервисов, для которых необходимо просмотреть журнал.
3. Просмотрите журнал выбранного сервиса при помощи команды:

   ```
   journalctl -fu [наименование_сервиса] -n [количество последних строк журнала, которое нужно показать]
   ```

4. При ошибках в журналах сервисов см. п. «Некорректная инициализация сервисов Комплекса» в разделе «Веб-интерфейс не загружается».

21.2.26. Не работает сложное исключение для правила службы обнаружения вторжений

Причина: при создании исключения в виде pass-правила использовалась конструкция вида threshold: type both и/или threshold: type limit

Способ устранения

Для устранения затруднения:

1. Деактивируйте нерабочее правило службы обнаружения вторжений.
2. Создайте новое правило, добавив исключения для IP-адресов и портов.

> **Пример**
> в Комплексе создано правило службы обнаружения вторжений с конструкцией `threshold: type both`:
>
> ```
> alert tcp any any -> any any (msg:"ET SCAN NMAP -sS window 1024"; fragbits:!D;
> dsize:0; flags:S,12; ack:0; window:1024; threshold: type both, track by_dst, count 1,
> seconds 60; reference:url,doc.emergingthreats.net/2009582; classtype:attempted-recon;
> sid:2009582; rev:3; metadata:created_at 2010_07_30, updated_at 2010_07_30;)
> ```
>
> Измененное правило будет выглядеть следующим образом:
>
> ```
> pass tcp 192.168.0.1 any -> 192.168.0.2 any (msg:"ET SCAN NMAP -sS
> window 1024"; fragbits:!D; dsize:0; flags:S,12; ack:0; window:1024;
> reference:url,doc.emergingthreats.net/2009582; classtype:attempted-recon; sid:
> 94000000-94999999;)
> ```

21.2.27. Обнаружен конфликт версий проектов ПЛК

При одновременной работе разных пользователей с одним проектом возникает ошибка Обнаружен конфликт версий.

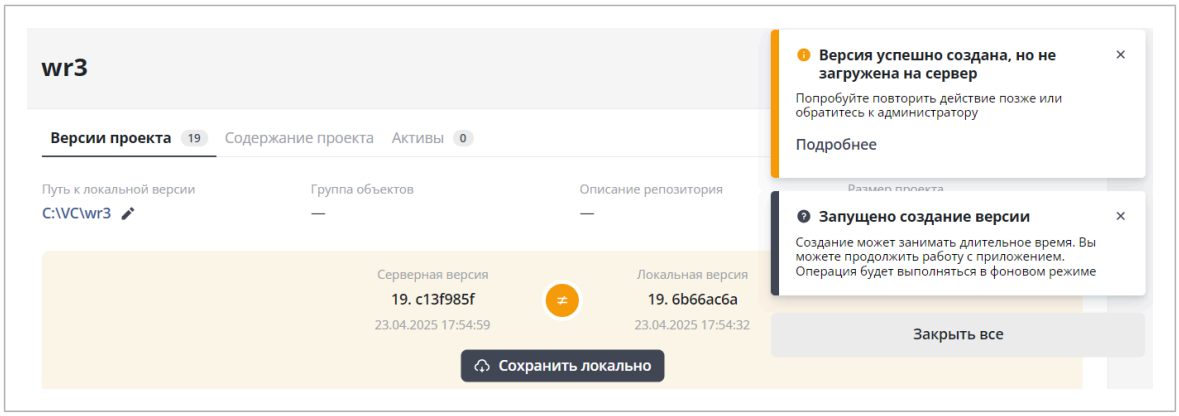


Рис. 463. Обнаружен конфликт версий

Причина

При одновременной работе разных пользователей с одним проектом возможна ситуация, когда пользователь 1 загрузил изменения на сервер, и проект получил новую версию. В таком случае при попытке пользователя 2 загрузить изменения предыдущей версии проекта возникнет ошибка Обнаружен конфликт версий.

Способ устранения

1. Нажмите кнопку **Сохранить локально**.
   - **Результат шага:** откроется окно **Обнаружен конфликт версий**.

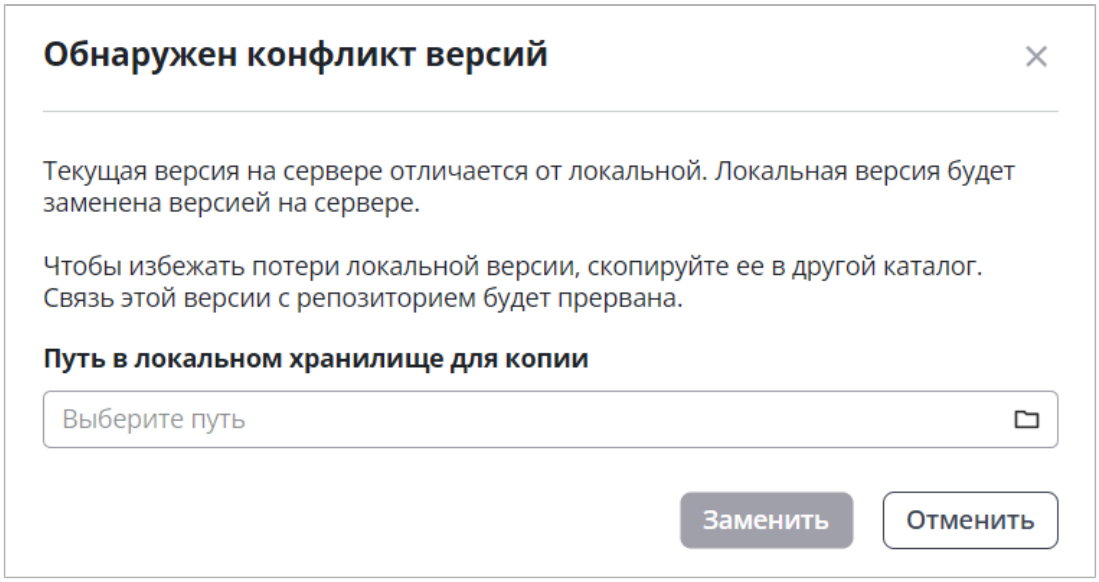


Рис. 464. Обнаружен конфликт версий

2. Укажите новый путь к файлам репозитория или выберите новое локальное хранилище с помощью кнопки 🗀
3. Нажмите кнопку **Заменить**.
   - **Результат шага:** система переместит файлы проекта в указанный каталог. После этого в исходный каталог будет загружена актуальная версия проекта с сервера Version Control Management.

21.2.28. Каталог проекта ПЛК содержит информацию других файлов

При добавлении файлов в каталог проекта возникает ошибка `Каталог содержит информацию других файлов`.

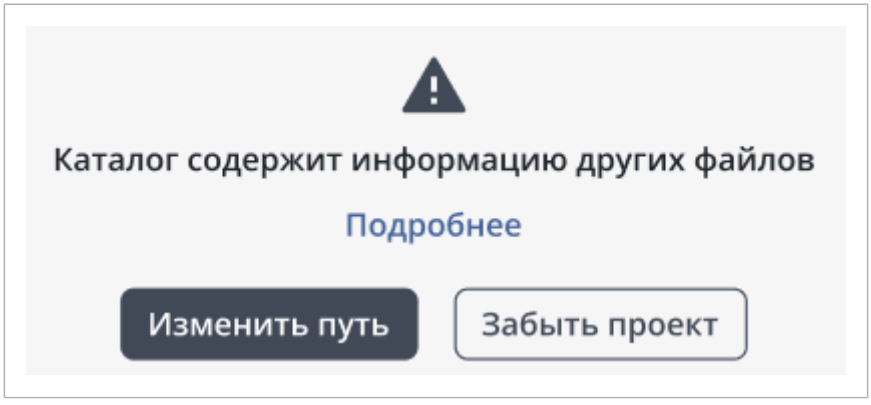


Рис. 465. Сообщение об ошибке

Причина

В каталог проекта были добавлены файлы других Git-платформ или серверов Version Control Management.

Способ устранения

Выберите способ устранения ошибки:

- Изменить каталог проекта с помощью кнопки **Изменить путь**.
- Удалить связь между локальным и серверным репозиторием с помощью кнопки **Забыть проект**.

21.2.29. Путь к файлу превышает допустимую длину

В процессе работы с Version Control Desktop App могут возникнуть следующие ошибки:

Рис. 466. Ошибка создания версии

Рис. 467. Ошибка подключения репозитория

Рис. 468. Ошибка редактирования пути

Рис. 469. Ошибка отмены изменений

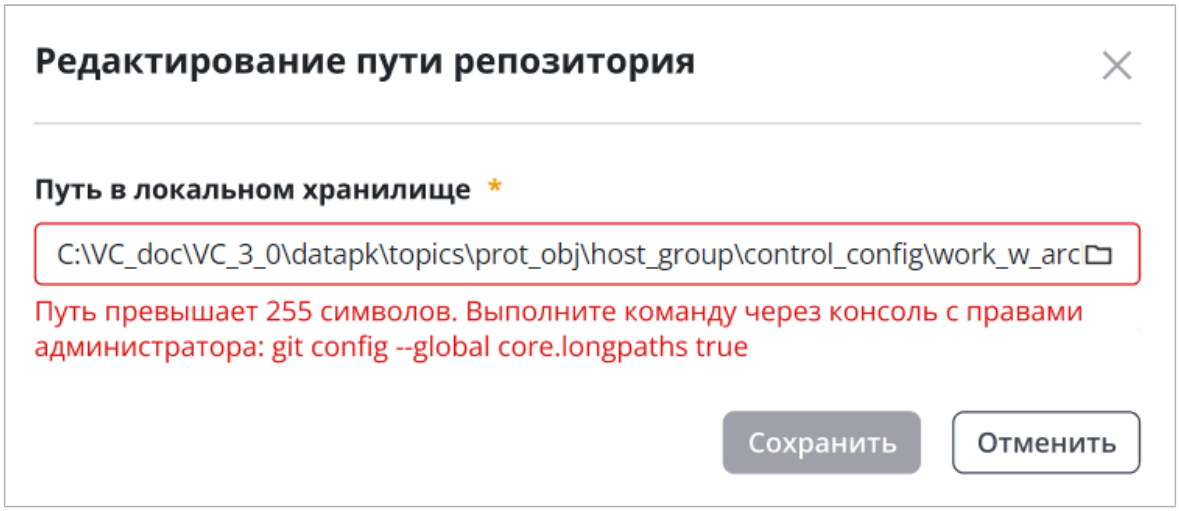


Рис. 470. Ошибка длины пути

Причина

При снятии ограничений на длину пути к файлу может произойти ситуация, когда путь к файлу репозитория превышает допустимые 255 символов.

Способ устранения

1. Откройте консоль с правами администратора.
2. Введите следующую команду:

```
git config --global core.longpaths true
```

21.3. Восстановление данных из резервных копий

Восстановление данных на текущей версии Комплекса уровня Management возможно только из резервной копии, выполненной для той же версии Комплекса уровня Management.

Восстановление данных рекомендуется выполнять в следующем порядке Комплекса уровня Management:

1. Резервное копирование данных.
2. Проверка наличия резервной копии.
3. Восстановление данных из резервной копии.

Комплексы уровня Sensor не хранят данные, поэтому их восстановление из резервной копии заключается в их развертывании с нуля — необходимо только скопировать сохраненные файлы `machine-id`, `sensor.env`, .

> Внимание:
>
> Не рекомендуется использовать резервную копию данных с целью развернуть еще одну копию Комплекса — идентификатор в файле `machine-id` должен быть уникальным на каждом Комплексе, и не допускается наличие двух Комплексов с одинаковыми идентификаторами в одной сети.

21.3.1. Восстановление данных из резервных копий Комплекса уровня Management и Комплекса уровня Management+Sensor

Для восстановления данных из резервных копий Комплекса уровня Management или Комплекса уровня Management+Sensor необходимо выполнить следующие действия:

- Проверка наличия резервной копии Комплекса уровня Management и Комплекса уровня Management +Sensor;
- Восстановление данных из резервной копии Комплекса уровня Management и Комплекса уровня Management+Sensor.

Для подготовки к восстановлению данных Комплекса уровня Management из резервной копии необходимо подготовить следующие файлы, заранее сохраненные на отдельном носителе на этапе создания резервной копии:

- архив `dtpk-backup-v3.0.[минорная_версия].[патч_версия]-{ГГГГММДДччммсс}.tar` с резервной копией;
- архив `nta-backup-[версия_Комплекса]-[дата]` с резервной копией БД `clickhouse`, если на восстанавливаемом Комплексе установлен модуль «Анализ промышленного сетевого трафика» и необходимо восстановить его базу данных;
- конфигурационный файл `manager.env`;
- конфигурационный файл `sensor.env`, если на Комплексе также будет восстанавливаться уровень Sensor (сенсор);
- индексы внешних событий, если на восстанавливаемом Комплексе установлен модуль «Управление внешними событиями».

21.3.1.1. Проверка наличия резервной копии Комплекса уровня Management и Комплекса уровня Management+Sensor

Для проверки наличия резервной копии:

1. Подключитесь к Комплексу уровня Management по протоколу SSH с учетной записью `user` и повысьте привилегии до администратора с помощью команды `su -`
2. Убедитесь, что архив резервной копии `dtpk-backup-v3.0.[минорная_версия].[патч_версия]-{ГГГГММДДччммсс}.tar` расположен в директории `/var/backups`
3. Если на восстанавливаемом Комплексе установлен модуль «Анализ промышленного сетевого трафика» и необходимо восстановить его данные, убедитесь, что архив `nta-backup-[версия_Комплекса]-[дата]` резервной копии БД `clickhouse` расположен в директории `/var/backups`
4. Проверьте целостность архива резервной копии. Для этого выполните команду из любой директории:

```
python3 -m backup_manager check
 --file=dtpk-backup-v3.0.[минорная_версия].[патч_версия]-{ГГГГММДДччммсс}.tar
 --password='1234567890'
```

где `--password` — пример пароля, заданного для архива при создании резервной копии.

- **Результат шага:** пример вывода в терминале при успешной проверке целостности архива:

```
INFO:backup_manager.operations.check:Start
 checking /var/backups/dtpk-backup-v3.0.1.0-rc1-20250827104814.tar backup file
INFO:backup_manager.operations.check:Version 3.0.1.0-rc1
INFO:backup_manager.operations.check:data.tar.bz2 Ok
INFO:backup_manager.operations.check:repos_data.tar.bz2 Ok
INFO:backup_manager.operations.check:maria_db_dump.sql Ok
INFO:backup_manager.operations.check:postgres_db_dump.sql Ok
INFO:backup_manager.operations.check:dump.rdb Ok
INFO:backup_manager.main:Backup checked
```

5. Убедитесь в отсутствии ошибок после окончания проверки резервной копии.

21.3.1.2. Восстановление данных из резервной копии Комплекса уровня Management и Комплекса уровня Management+Sensor

ОСТОРОЖНО:

При восстановлении Комплекса уровня Management уникальный идентификатор `/etc/machine-id` и `/var/lib/dbus/machine-id` будет заменен на идентификатор из резервной копии. Во избежание проблем убедитесь в следующем:

- если восстановление Комплекса выполняется на другом устройстве, то на предыдущем устройстве в ОС необходимо изменить `machine-id` во избежание наличия в сети двух устройств с одинаковым `machine-id`;
- на ОС отсутствуют приложения, работа которых может быть нарушена в связи с изменением `machine-id`.

Для восстановления данных из резервной копии:

1. Остановите работу всех сервисов Комплекса, кроме `udv-postgresql.service`. Для этого выполните команду:

```
/usr/bin/stop_services.sh
```

2. Если на восстанавливаемом Комплексе установлен модуль «Анализ промышленного сетевого трафика» и необходимо восстановить его базу данных, запустите СУБД `clickhouse`:

```
systemctl restart udv-clickhouse-service.service
```

3. После остановки работы сервисов выполните из любой директории команду для восстановления Комплекса из резервной копии:

```
python3 -m backup_manager restore --include-nta [путь_к_резервной_копии_NTA]
 --file=dtpk-backup-v3.0.[минорная_версия].[патч_версия]-{ГГГГММДДччммсс}.tar
 --password='1234567890' --db-username DB_USER --db-password DB_PASS
```

где:

- `--include-nta` — путь к файлу `nta-backup-[версия_Комплекса]-[дата]` резервной копии базы данных `clickhouse`, если на восстанавливаемом Комплексе установлен модуль «Анализ промышленного сетевого трафика». Если модуль не установлен, удалите параметр и его значение из команды.
- `--password` — пример пароля от архива резервной копии, который был задан при создании резервной копии;
- `--db-username` — логин пользователя базы данных, значение которого необходимо было скопировать из переменной `DB_USER` конфигурационного файла `/usr/share/udv/datapk/manager.env` при создании архива резервной копии (либо можно скопировать из файла `manager.env` в архиве резервной копии);
- `--db-password` — пароль доступа к базе данных, значение которого необходимо было скопировать из переменной `DB_PASS` конфигурационного файла `/usr/share/udv/datapk/manager.env` при создании архива резервной копии (либо можно скопировать из файла `manager.env` в архиве резервной копии).

4. Выполните восстановление внешних событий. Для этого поместите сохраненные ранее индексы событий в директорию `/var/backups/elasticsearch/uploads`.
   а. Поместите с заменой файлы `manager.env` и `sensor.env` (если на восстанавливаемом Комплексе будет развернут сенсор), сохраненные ранее отдельно, в директорию `/usr/share/udv/datapk`.
   б. После успешного восстановления перезагрузите Комплекс, выполнив команду:

   ```
   shutdown -r now
   ```

   ▸ **Результат шага:** перезагрузка Комплекс успешно выполнена.

   в. Войдите в веб-интерфейс Комплекса под учетной записью администратора.
   г. Перейдите в раздел **События → Экспертный режим**.
   д. Нажмите **Create index pattern**.
   е. В поле **Index pattern name** введите `datapk-events-*` и нажмите **Next step**.
   ж. В поле **Time field** выберите **create_time** и нажмите **Create index pattern**.
   з. Перейдите в раздел **Администрирование → События и инциденты → Индексы**.
   и. Нажмите **Восстановить индексы**.

21.3.2. Восстановление данных из резервных копий Комплекса уровня Sensor

Для восстановления данных из резервных копий Комплекса уровня Sensor необходимо выполнить следующие действия:

- Резервное копирование данных Комплекса уровня Sensor;
- Восстановление данных из резервной копии Комплекса уровня Sensor.

21.3.2.1. Резервное копирование данных Комплекса уровня Sensor

Для выполнения резервного копирования данных:

1. Войдите в терминал Комплекса под учетной записью `root`.
2. Сохраните файл `machine-id` из директории `/etc`.
3. Сохраните файл `machine-id` из директории `/var/lib/dbus`.
4. Сохраните файл `sensor.env` из директории `/usr/share/udv/datapk`.
5. Если на сенсоре был установлен модуль «Анализ промышленного сетевого трафика», сохраните конфигурационные файлы `/usr/share/udv/zeek-wrapper/configs/general.dat` и `/usr/share/udv/zeek-wrapper/configs/ics-function.dat`.

21.3.2.2. Восстановление данных из резервной копии Комплекса уровня Sensor

Для восстановления данных из резервной копии:

1. Выполните развертывание Комплекса уровня Sensor в соответствии с разделом «Установка Комплекса уровня Sensor».
2. Замените файл `/etc/machine-id` на файл, сохраненный при резервном копировании.
3. Сохраните файл `machine-id` в директории `/var/lib/dbus`.
4. Замените файл `/usr/share/udv/datapk/sensor.env` на файл, сохраненный при резервном копировании.
5. Если на сенсоре был установлен модуль «Анализ промышленного сетевого трафика», замените конфигурационные файлы `/usr/share/udv/zeek-wrapper/configs/general.dat` и `/usr/share/udv/zeek-wrapper/configs/ics-function.dat` на файлы, сохраненные при резервном копировании.
6. Перезагрузите Комплекс, выполнив команду:

   ```
   shutdown -r now
   ```

7. Войдите в веб-интерфейс Комплекса уровня Management, к которому подключен данный Комплекс уровня Sensor.
8. Перейдите в раздел **Сенсоры** и убедитесь, что Комплекс уровня Sensor успешно подключился к Комплексу уровня Management.

21.4. Действия в случаях несанкционированного доступа к данным

После обнаружения нелегитимных действий со стороны пользователя администратор может воспользоваться следующими возможностями по блокировке пользователей:

- Просмотр журнала действий пользователей Комплекса
- Изменение статуса активности учетной записи пользователя Комплекса

21.4.1. Просмотр журнала действий пользователей Комплекса

Все действия пользователей Комплекса журналируются. При установлении фактов попыток несанкционированных действий пользователей их работа в веб-интерфейсе Комплекса блокируется. Дальнейшая работа пользователя с Комплексом возможна только после расследования администратора комплекса по выявлению причин возникновения аварийной ситуации.

Для самостоятельного установления или подтверждения фактов несанкционированного доступа администратор может обратиться к журналу действий пользователей. Для просмотра журнала действий пользователей Комплекса:

1. Перейдите на страницу **События**.
2. Настройте фильтрацию событий по значениям `user_action_control` или `appliance_authentication` поля **Тип**.
3. Нажмите кнопку **Сохранить** для применения фильтра.
4. В «быстром» фильтре **Дата создания** выберите временной интервал, за который необходимо получить события действий пользователей.
5. Проанализируйте полученные события на предмет несанкционированного доступа.

21.4.2. Изменение статуса активности учетной записи пользователя Комплекса

Чтобы изменить статус активности учетной записи пользователя Комплекса:

1. Перейдите на страницу **Администрирование → Пользователи**.
2. Выберите учетную запись в списке и нажмите (**Редактировать учетную запись**).
3. В зависимости от желаемого действия:
   - установите чекбокс Учетная запись **пользователя активна**, чтобы активировать (разблокировать) доступ пользователя к веб-интерфейсу Комплекса;
   - отмените установку чекбокса Учетная запись **пользователя активна** для учетной записи, чтобы заблокировать пользователю доступ к веб-интерфейсу Комплекса.
4. Сохраните изменения.
   - **Результат шага:** после подтверждения активность учетной записи пользователя будет изменена.

21.5. Действия в других аварийных ситуациях

Действия в экстремальных условиях осуществляются по правилам, принятым в эксплуатирующей организации.

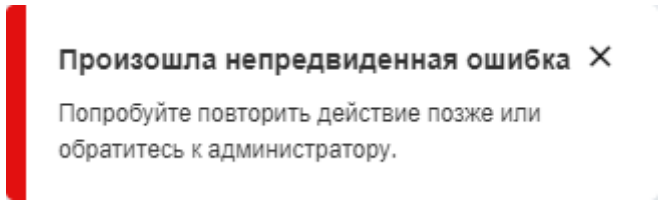
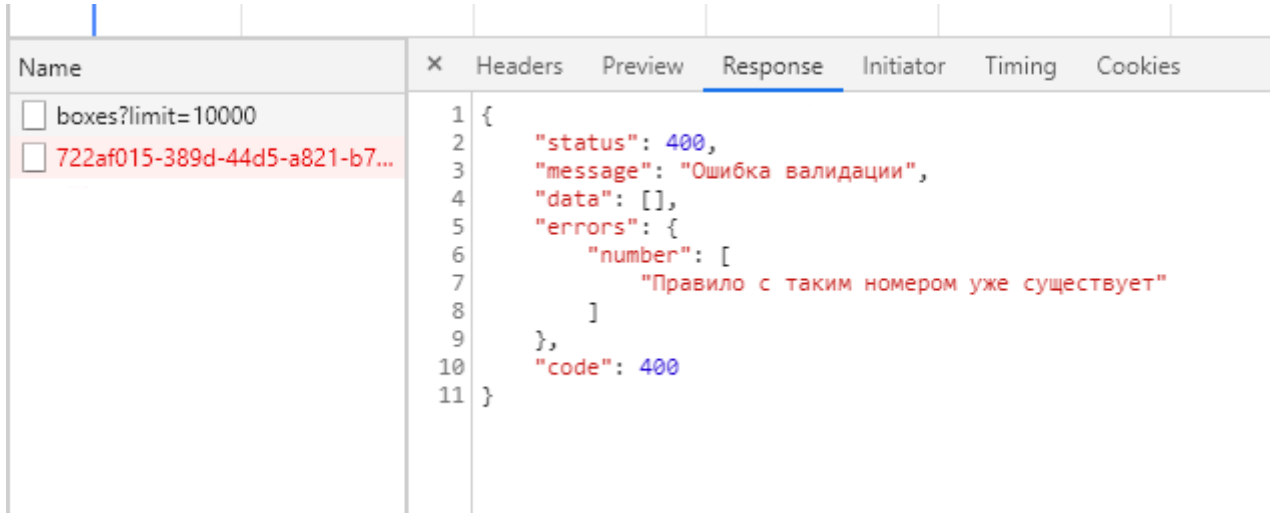
Аварийные ситуации, связанные с некорректным функционированием Комплекса в сетевой инфраструктуре АСУ ТП, устраняются путем проверки и исправлений настроек сети управляющего контура комплекса и локальных настроек Комплекса.

21.6. Анкета при обращении в сервисный центр

Внимание:

Поля, отмеченные знаком «*», обязательны для заполнения

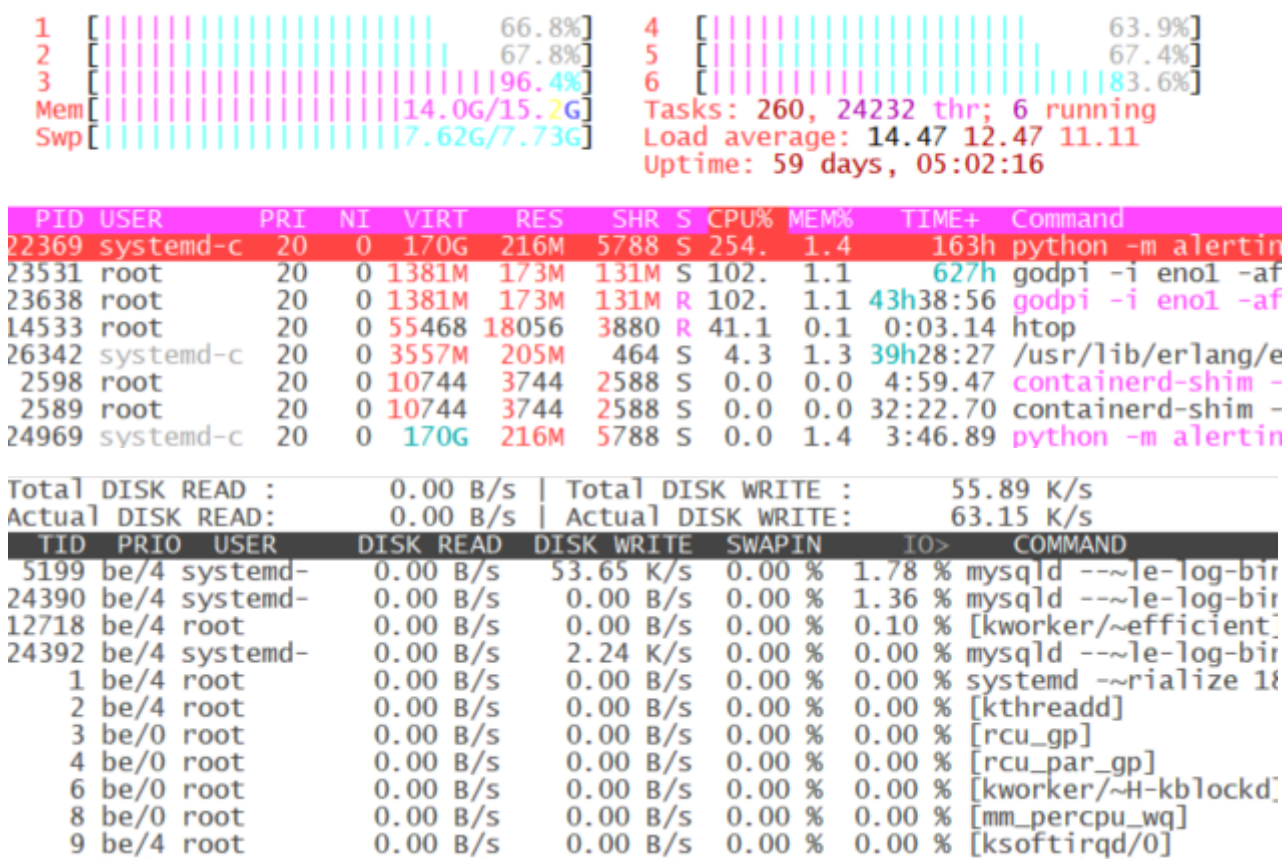
ПАРАМЕТР	ЗНАЧЕНИЕ	ПРИМЕР ЗАПОЛНЕНИЯ
ФИО, должность обратившегося, контактные данные *		Иванов Иван Иванович, системный инженер, ООО «Партнер», partner@partner.ru, +7(900)-012-34-56
Проект/место установки, уровень в иерархии *		ООО «Заказчик», КС-1, уровень Management
Сертификат технической поддержки *		CI-12345678
Версия Комплекса *		3.0.0.0.0.0
Общее количество активов, сетевых сессий, событий в сутки на проблемном (включая полученные с сенсора)		150 активов, 300 тыс. сессий, 250 тыс. событий в сутки
Количество подчиненных уровня Sensor		2 уровня Sensor
Краткое описание ошибки (словесное) *		Не создается правило сессий
Действия, которые привели к ошибке (подробное описание шагов, приведших к ошибке) *		Перешел на страницу правил сессий, создал новое правило, задал диапазон IP-адресов и последний распознанный протокол, при сохранении ошибка валидации.

ПАРАМЕТР	ЗНАЧЕНИЕ	ПРИМЕР ЗАПОЛНЕНИЯ
Скриншот ошибки в веб-интерфейсе		
Результаты ошибочных запросов (панель разработчика в браузере, вкладка response у проблемного запроса)		
Логи сопутствующих сервисов *		Во вложении логи udv-zeek-backend, udv-rules-backend
Архив всех логов сервисов (см. раздел «Диагностика сервисов и иерархии»)		Архив во вложении
Данные по аппаратной платформе (сервер, процессор, объем оперативной памяти, объем дискового пространства, тип дисков)*		Сервер Huawei X6000, Xeon Bronze 3104, 1.7 GHz. 16 ГБ RAM, 4 ТБ HDD (SATA 7200 rpm)

ПАРАМЕТР	ЗНАЧЕНИЕ	ПРИМЕР ЗАПОЛНЕНИЯ
Версия ОС *		ОС Альт Сервер 10.2 SP

Вывод таблицы маршрутизации (`route -n` или `ip route show`)		`[root@datapk-srv-apollo-253-37 datapk]# ip route show`
		`default via 192.168.253.1 dev eno1 proto static metric 100`
		`172.8.0.0/24 dev br-48bed0f17439 proto kernel scope link src 172.8.0.1`
		`172.8.0.0/24 dev br-48bed0f17439 proto kernel scope link src 172.8.0.1 metric 428`
		`172.10.0.0/16 dev br-842698bddad2 proto kernel scope link src 172.10.0.1`
		`172.11.0.0/16 dev br-3221910b41eb proto kernel scope link src 172.11.0.1`
		`172.17.2.0/24 via 172.17.100.1 dev eno1 proto static metric 100`
		`172.17.100.1 dev eno1 proto static scope link metric 100`
		`172.18.0.0/16 dev docker0 proto kernel scope link src 172.18.0.1 linkdown`
		`172.18.0.0/16 dev docker0 proto kernel scope link src 172.18.0.1 metric 430 linkdown`
		`172.19.0.0/16 dev br-40ac11103665 proto kernel scope link src 172.19.0.1`
		`172.19.0.0/16 dev br-40ac11103665 proto kernel scope link src 172.19.0.1 metric 427`
		`172.20.0.0/16 dev br-3ed25b69f5c4 proto kernel scope link src 172.20.0.1`
		`172.20.0.0/16 dev br-3ed25b69f5c4 proto kernel scope link src 172.20.0.1 metric 426`
		`192.168.253.0/24 dev eno1 proto kernel scope link src 192.168.253.37 metric 100`
		`[root@datapk-srv-apollo-253-37 datapk]#`

Свободное место на корневом разделе диска (`df -Th /`) Свободная оперативная память, текущий список процессов (`top`) Значение Load Average Загрузка диска (`iotop`)		Свободное место на корневом разделе: 2.5 ТБ Свободная оперативная память: 1 МБ Load Average: 14

ПАРАМЕТР	ЗНАЧЕНИЕ	ПРИМЕР ЗАПОЛНЕНИЯ
		
Наличие сетевых доступов до проблемного актива/ (`curl [ip_-addr]:[port_number]`)		curl: (56) Recv failure: Connection reset by peer [root@datapk-srv-apollo-253-37 datapk]# curl 192.168.243.16:5985 <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd"> <HTML><HEAD><TITLE>Not Found</TITLE> <META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD> <BODY> Not Found <hr> HTTP Error 404. The requested resource is not found. </BODY></HTML>

ПАРАМЕТР	ЗНАЧЕНИЕ	ПРИМЕР ЗАПОЛНЕНИЯ
Запись трафика (PCAP-файл) с прослушивающего интерфейса сенсора для заявок с проблемами, связанными с обнаружением сессий или вторжений		Во вложении
Сведения о проблемном активе (тип, версия ОС, настроенные протоколы сбора данных) для заявок с проблемами в запуске сканеров сбора данных		АРМ оператора, Windows 7, сбор данных по WinRM HTTPS
Проблемные сканеры сбора данных для заявок с проблемами в запуске сканеров		Во вложении

21.7. Диагностика сервиса сбора данных по протоколам SSH, Telnet, WinRM, winexe

Перед выполнением:

> Внимание:
>
> Данная инструкция актуальна для следующих сервисов и портов:
>
> - `udv-msrpc`, порт `10008`;
> - `udv-plc-connector`, порт `10206`;
> - `udv-opc-connector`, порт `10205`;
> - `udv-terminal-connector`, порт `10208`;
> - `udv-modbus-connector`, порт `10203`;
> - `udv-sql-connector`, порт `10202`;
> - `udv-snmp-connector`, порт `10204`;

Для расследования причин появления ошибок сбора данных по протоколам SSH, Telnet, WinRM, winexe:

1. Подключитесь к операционной системе Комплекса.
2. Просмотрите текущее состояние журналирования сервиса, выполнив команду:

   ```
   curl http://[IP_адрес_сервиса]:[порт_сервиса]/log/level
   ```

   Пример

   Сервис имеет состояние `NOTSET`. Это значит, что уровень журналирования для этого сервиса не задан.

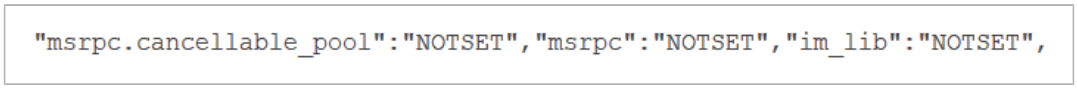
   

   Рис. 471. Состояние «NOTSET» журналирования сервиса «msrpc»

3. Измените уровень журналирования сервиса, выполнив команду:

   ```
   curl -X POST
    "http://[IP_адрес_сервиса]:[порт_сервиса]/log/level?logger_name=[название_сервиса/назван
   ие_пакета_в_сервисе]&log_level=[уровень_журналирования]"
   ```

   где:

   - `[IP_адрес_сервиса]` — IP-адрес необходимого сервиса;
   - `[порт_сервиса]` — порт необходимого сервиса;
   - `[название_сервиса/название_пакета_в_сервисе]` — имя необходимого сервиса или пакета в сервисе;
   - `[уровень_журналирования]` — требуемый уровень журналирования сервиса (`INFO` или `DEBUG`).

   > Внимание:
   >
   > На данном шаге название сервиса вводится через нижнее подчеркивание, без добавления приставки `udv-` (например, `udv-terminal-connector.service` → `terminal_connector`)

4. В веб-интерфейсе Комплекса однократно повторите сбор данных с активов, на которых ранее были ошибки сбора.
5. Проверьте установленный уровень журналирования сервиса, выполнив команду:

```
curl http://[IP_адрес_сервиса]:[порт_сервиса]/log/level
```

Пример

Сервис имеет состояние `DEBUG`

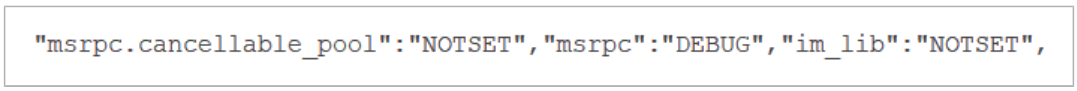


Рис. 472. Состояние «DEBUG» журналирования сервиса «msrpc»

6. Посмотрите журнал сервиса при помощи команды:

```
journalctl -fu [полное_название_сервиса].service -n [количество последних строк журнала,
 которое нужно показать]
```

- **Результат шага:** Отображается указанное количество последних строк журнала сервиса.

Рис. 473. Отображение последних пять строк журнала сервиса «udv-msrpc»

22. Справочная информация

В этом разделе:

1. **Архитектура UDV DATAPK Industrial Kit**
2. **Условия эксплуатации Комплекса**
3. **Описание источников событий**
4. **Описание полей событий в экспертном режиме страницы «События»**
5. **Переменные Комплекса**
6. **События Комплекса**
7. **Механизмы хранения событий**
8. **Отправка внутренних событий по протоколу Syslog**
9. **Перечень данных, собираемых Комплексом с помощью сканеров**
10. **Работа с импортируемыми панелями мониторинга**
11. **Рекомендации по настройке сбора данных**
12. **Определение максимально допустимого количества активов сбора данных**
13. **Содержание Python-скриптов**
14. **Перечень SCADA, с которых поддерживается сбор данных**
15. **Реестр сканеров Комплекса**
16. **Сетевые взаимодействия Комплексов**
17. **Поддерживаемые типы событий**
18. **Синтаксис правил корреляции событий**
19. **Список внутренних правил корреляции событий**
20. **Отображение времени в Комплексе**
21. **Структура директорий Комплекса**
22. **Работа с контрольными суммами исполняемых файлов сертифицированного Комплекса**
23. **Справочная информация о модуле «Анализ промышленного сетевого трафика»**
24. **Справочная информация о модуле «Управление проектами ПЛК»**
25. **Справочная информация о модуле «EDR for PLC»**
26. **Справочная информация о компоненте Supervision**

22.1. Архитектура UDV DATAPK Industrial Kit

В этом разделе:

- Интерфейс Комплекса
- Дополнительные функции Комплекса

В UDV DATAPK реализован механизм, предоставляющий возможности по выстраиванию трех уровней иерархии. Каждый уровень иерархии представлен отдельным вариантом исполнения.

- UDV DATAPK уровня Sensor (Сенсор) обладает следующим набором функций:
  - Получение данных от компонентов АСУ ТП, их обработка и передача в Комплекс уровня Management;
  - Пассивный анализ копии сетевого трафика;
  - Активный сбор данных о конфигурациях, уязвимостях и т.д.;
  - Пассивное получение событий из внешних источников по протоколу Syslog.

> Внимание:
>
> Сенсор не имеет веб-интерфейса. Управление сенсорами выполняет Комплекс уровня Management.

- UDV DATAPK уровня Management (UDV DATAPK среднего уровня) обладает следующим набором функций:
  - Детализированное представление данных;
  - Базовые панели мониторинга и отчетность;
  - Настройка анализа защищенности, парольной политики, правил сессий;
  - Анализ и корреляция событий безопасности;
  - Управление сенсорами;
  - Управление конфигурациями системы;
  - Интеграция со сторонними сервисами и автоматизация процессов ИБ с помощью REST API.
- UDV DATAPK уровня Supervision (UDV DATAPK верхнего уровня) обладает следующим набором функций:
  - Централизованный мониторинг состояния защищенности АСУ ТП и контроль деятельности распределенных отделов по ИБ АСУ ТП;
  - Получение аналитических данных для принятия обоснованных управленческих решений;
  - Централизованное управление учетными записями пользователей Комплексов уровня Management

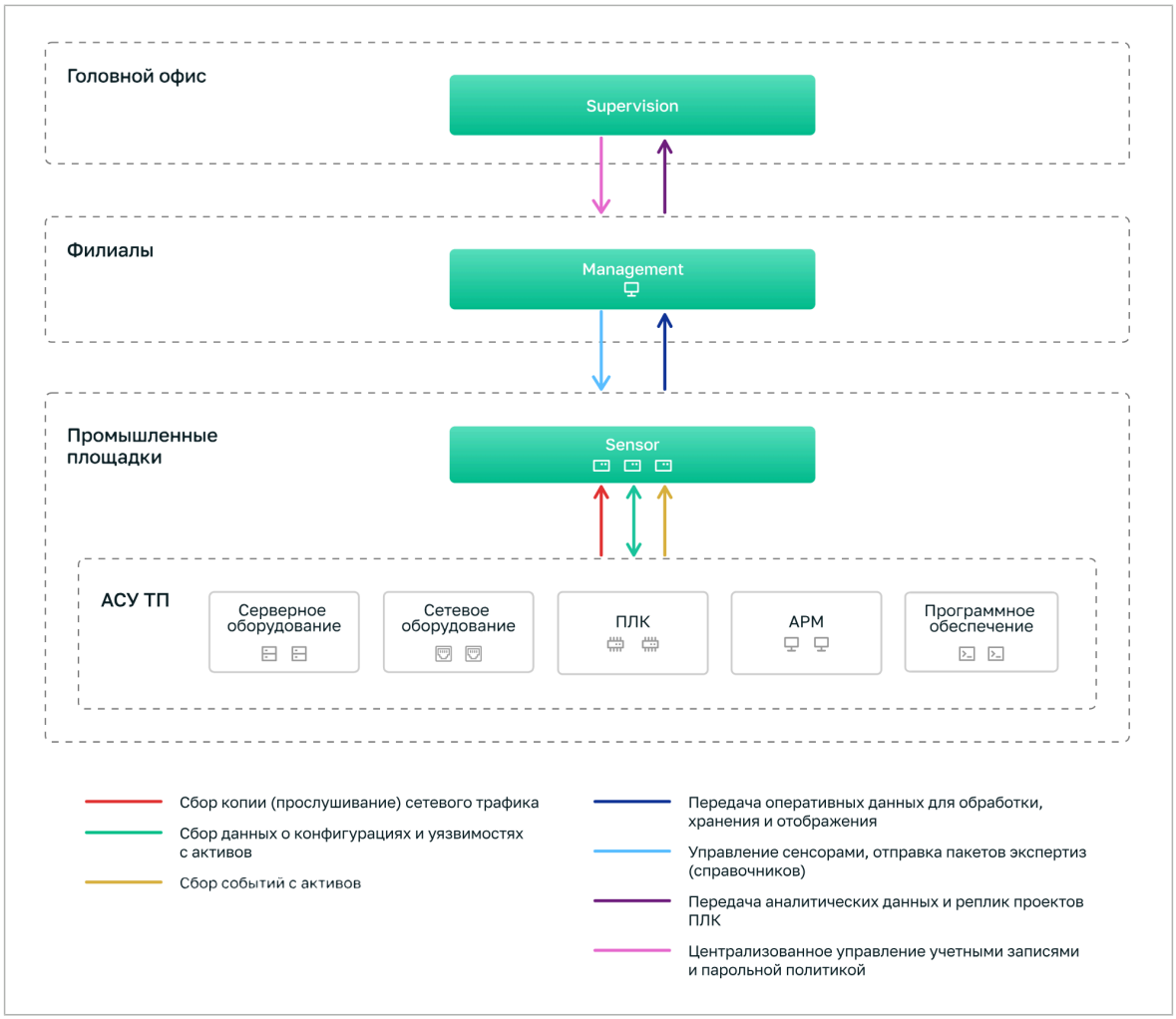


Рис. 474. Структурная схема иерархии

Порядок передачи информации по иерархии Комплексов

Предусмотрен следующий порядок взаимодействия между уровнями иерархии:

- Сенсор (Sensor) → Комплекс среднего уровня (Management) → Комплекс верхнего уровня (Supervision) – передача оперативных данных (результатов анализа сетевого трафика, событий и конфигураций, проверок на уязвимости и соответствие требованиям ИБ).
- Комплекс верхнего уровня (Supervision) → Комплекс среднего уровня (Management) – передача (репликация) учетных записей пользователей и парольной политики.
- Комплекс среднего уровня (Management) → Комплекс верхнего уровня (Supervision) – передача статистической информации об оперативных данных, о состоянии сенсоров и самих Комплексов уровня Management.

Перечень данных, передаваемых по иерархии «снизу вверх» (от сенсоров до Комплексов уровня Management), приведен в таблице ниже (Таблица 126. Перечень данных, передаваемых по иерархии «снизу вверх»).

Табл. 126. Перечень данных, передаваемых по иерархии «снизу вверх»

ДАННЫЕ	СЕНСОР → КОМПЛЕКС УРОВНЯ MANAGEMENT
События	✔

Табл. 126. Перечень данных, передаваемых по иерархии «снизу вверх»

ДАННЫЕ	СЕНСОР → КОМПЛЕКС УРОВНЯ MANAGEMENT
Активы	✔
Сетевые соединения	✔
Конфигурации	✔
Результаты проверок на уязвимости	✔
Результаты проверок на соответствие требованиям ИБ	✔
Инциденты ИБ	-

22.1.1. Список модулей UDV DATAPK Industrial Kit

Модульная архитектура UDV DATAPK включает в себя 7 модулей:

- **Core** — базовый модуль UDV DATAPK. Установлен по умолчанию на всех UDV DATAPK и требуется для работы всех остальных модулей. Содержит функции для внутреннего администрирования и мониторинга UDV DATAPK (управление пользователями, регистрация внутренних событий аудита, корреляция событий аудита, диагностика UDV DATAPK), а также позволяет проводить инвентаризацию активов в контролируемой сети.
- **Контроль версий (Version Control)** — предоставляет программистам и инженерам АСУ ТП инструменты для централизованного отказоустойчивого хранения проектов ПЛК, аудита изменений в проектах ПЛК, их резервирования и восстановления, а также отслеживания неизменности программ на ПЛК. Подробнее о работе с модулем см. раздел «Управление проектами ПЛК».
- **Анализ промышленного сетевого трафика (Industrial NTA)** — позволяет организациям находить устройства внутри сети и сетевые взаимодействия между ними, быстро выявлять атаки и проводить расследования, а также контролировать параметры технологических процессов, опираясь на данные из копии промышленного сетевого трафика. Подробнее о работе с модулем см. раздел «Анализ промышленного сетевого трафика».
- **Управление конфигурациями (Configuration Management)** — позволяет инженерам АСУ ТП и специалистам по ИБ контролировать соответствие любых конфигурационных параметров IT-устройств и устройств АСУ ТП на соответствие необходимым значениям, отслеживать изменения в значениях, проводить аудит и оперативно реагировать на изменения. Подробнее о работе с модулем см. раздел «Активный сбор данных с активов».
- **Управление уязвимостями (Vulnerability Management)** — позволяет специалистам по ИБ возможность проводить неинвазивный аудит защищенности компонентов АСУ ТП методом белого ящика (White Box), выявлять угрозы информационной безопасности, устранять их, а также провести проверку соответствия требованиям ИБ. Подробнее о работе с модулем см. раздел «Поиск уязвимостей и проверка соответствия требованиям информационной безопасности».

> Внимание:
>
> Для работы модуля «Управление уязвимостями» необходимо установить модуль «Управление конфигурациями».

- **Управление внешними событиями (External Events Management)** — предоставляет организациям набор инструментов для обработки и анализа событий ИБ, собранных с внешних источников. В составе модуля механизмы сбора, нормализации и корреляции событий ИБ, поиска по событиям ИБ, визуализации данных на основе событий ИБ с возможностью дальнейшей отправки данных в сторонние системы класса SIEM. Подробнее о работе с модулем см. разделы:
  - Просмотр событий и создание запросов в экспертном режиме
  - Импортируемые панели мониторинга
  - Настройка и управление мониторингом
  - Работа с инцидентами
- **Обнаружение и реагирование для ПЛК (EDR for PLC)** — позволяет организациям оперативно начать выявлять аномалии в поведении ПЛК посредством безагентного поведенческого анализа на основе запатентованных методов машинного обучения, а также реагировать на них. Подробнее о работе с модулем см. раздел «Управление модулем обнаружения и реагирования для ПЛК («EDR for PLC»)».

> Внимание:
>
> Для работы модуля EDR for PLC необходимо установить модули «Анализ промышленного сетевого трафика» и «Управление внешними событиями».

22.1.2. Интерфейс Комплекса

В разделе описаны детали работы с веб-интерфейсом Комплекса.

- Управляющие элементы
- Элементы управления таблицами
- Цветовая индикация и виды уведомлений
- Страницы интерфейса

22.1.2.1. Страницы интерфейса

В подразделе описаны все содержащиеся в интерфейсе страницы.

- Мониторинг
  - Статус защищенности
  - Панели мониторинга
  - Виджеты
- Инциденты
- Активы
  - Карточка актива
- События
  - Экспертный режим
- Контроль версий

    - Репозитории
- Инспекция сети
    - Карта сети
    - Сетевые соединения
        - Сессии
        - Пакеты
        - Файлы
    - Правила сессий
    - Правила контроля тегов
- Инспекция активов
    - Задачи сбора
    - Перечень ПО
    - Статус сбора
    - Конфигурации
        - Конфигурации актива
    - Результаты проверок
- Сенсоры
- Администрирование
    - О системе
        - О системе
        - Импорт и экспорт
        - Диагностика
        - Настройки мониторинга
    - Инспекция активов
        - Сканеры
        - Группы OVAL
        - Определения OVAL
        - Скрипты OVAL
        - Настройки OVAL
    - События и инциденты
        - Ретроанализ
        - Правила корреляции
        - Схема корреляции
        - Статусы инцидентов
        - Оповещения об инцидентах
        - Индексы
    - Пользователи
        - Пользователи
        - Парольная политика
    - Сигнатурный анализ
        - Правила обнаружения
    - Настройка активов
        - Учетные данные
        - Классификаторы
        - Источники
- Страница «Страница не найдена»

22.1.2.1.1. Мониторинг

Пункт главного меню, содержащий страницу **Статус защищенности**, а также страницы **Панели мониторинга** и **Виджеты**.

См. также

Статус защищенности

Панели мониторинга

Виджеты

22.1.2.1.1.1. Статус защищенности

Подраздел мониторинга, в котором отображаются статистика и изменения в реальном времени по ключевым оперативным данным Комплекса.

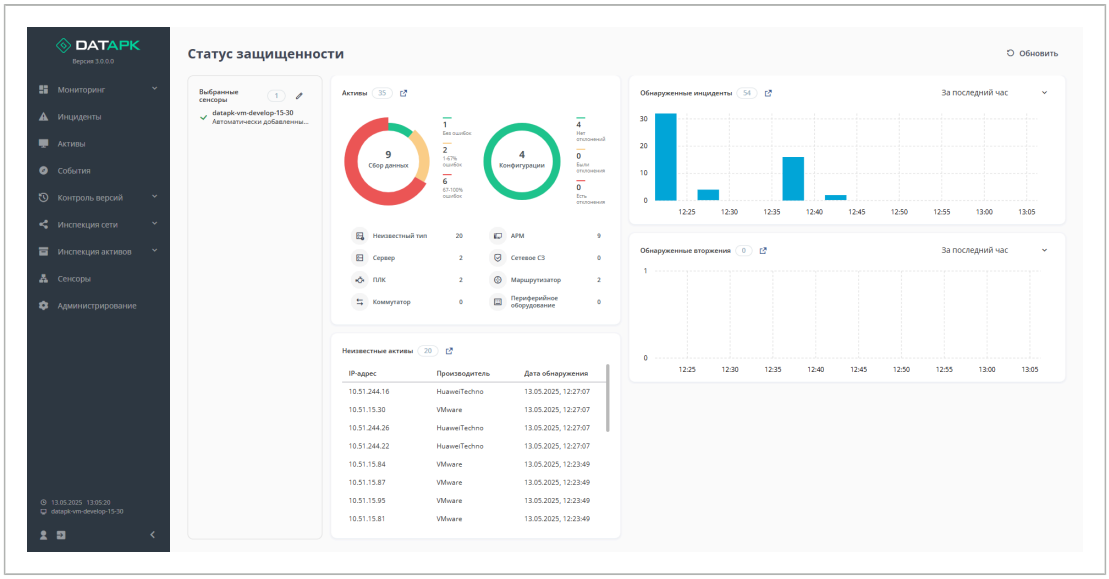


Рис. 475. Страница «Статус защищенности»

См. также

Просмотр главной панели мониторинга «Статус защищенности»

22.1.2.1.1.2. Панели мониторинга

Подраздел мониторинга, в котором располагаются созданные пользователем или предоставленные производителем Комплекса панели мониторинга. Расположенные в подразделе объекты доступны для редактирования.

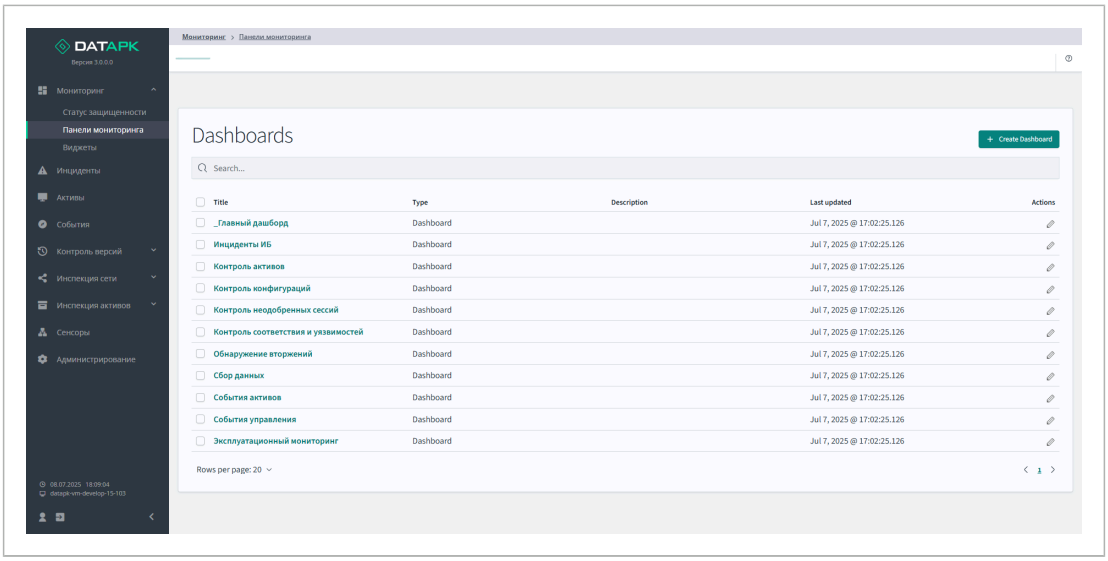


Рис. 476. Страница «Панели мониторинга»

См. также

Создание и настройка панели мониторинга

Импортируемые панели мониторинга

Виджеты

22.1.2.1.1.3. Виджеты

Подраздел мониторинга, в котором можно создавать и редактировать визуализации. Из визуализаций состоят панели мониторинга.

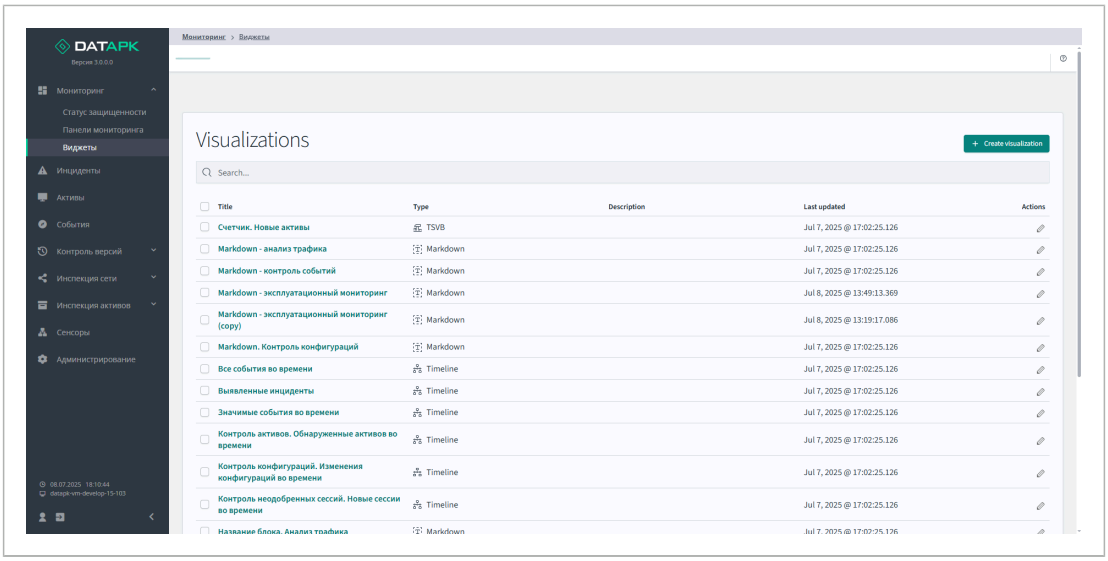


Рис. 477. Страница «Виджеты»

См. также

Панели мониторинга

Создание и настройка виджета

22.1.2.1.2. Инциденты

Подраздел меню **События и инциденты**, содержащий информацию обо всех выявленных инцидентах. На странице можно ознакомиться с подробностями инцидента: его текущим статусом, сформировавшими инцидент событиями, историей изменения инцидента, детализацией. В процессе расследования можно обновить статус и приоритет инцидента, подтвердить его или удалить. В результате будет сформировано событие с указанием выполненного действия, ответственного и его комментария.

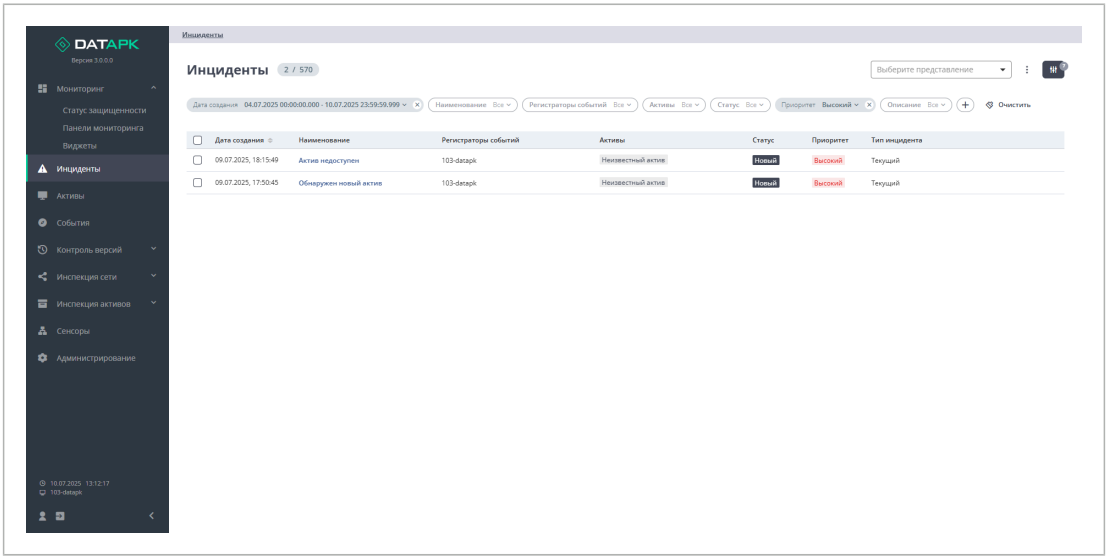


Рис. 478. Страница «Инциденты»

См. также

Управление статусами инцидентов

Изменение параметров инцидентов

Удаление инцидентов

Групповые операции над инцидентами

22.1.2.1.3. Активы

Страница главного меню, содержащая список всех найденных автоматически и добавленных пользователем активов. На странице присутствуют широкие возможности фильтрации и перехода к отдельным страницам различных аспектов активов (карточка актива, события, инциденты, учетные данные актива, конфигурации), кнопки экспорта, импорта, поиска уязвимостей, создания отчетов и удаления активов, столбцы статусов и статистики по сбору данных, отклонениям конфигураций, инцидентам, уязвимостям.

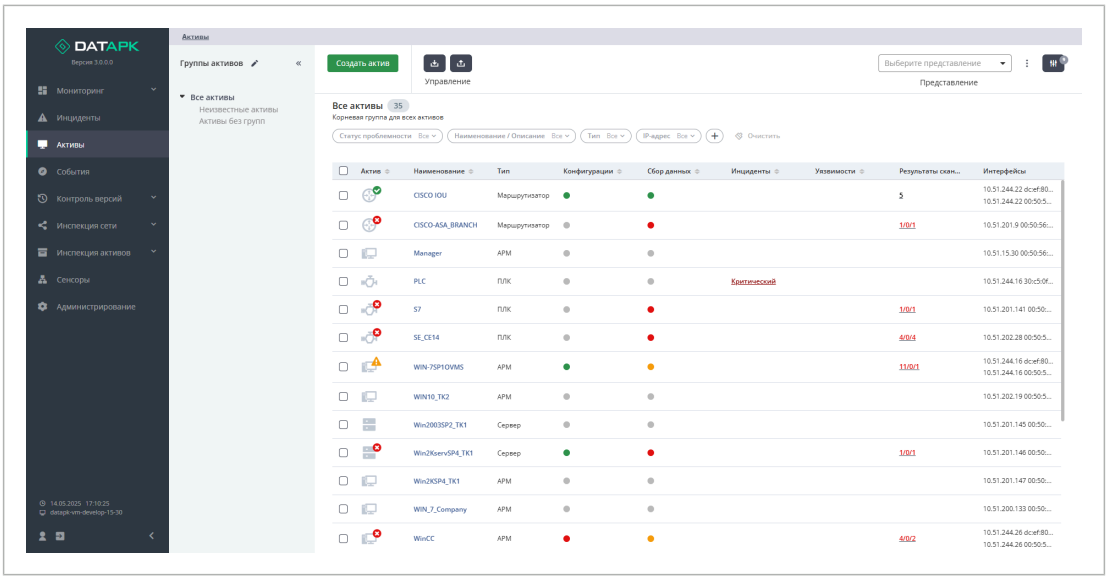


Рис. 479. Страница «Активы»

См. также

Работа с активами

22.1.2.1.3.1. Карточка актива

Не является разделом основного интерфейса. Перейти в карточку можно со страницы **Активы**, **Сессии**, **Карта сети** при нажатии на иконку или название актива. Доступен просмотр в отдельной вкладке. Содержание страницы различается в зависимости от актива, для которого открыта карточка.

В верхней части карточки расположен заголовок, совпадающий с наименованием просматриваемого актива. В правой части заголовка расположена кнопка удаления актива.

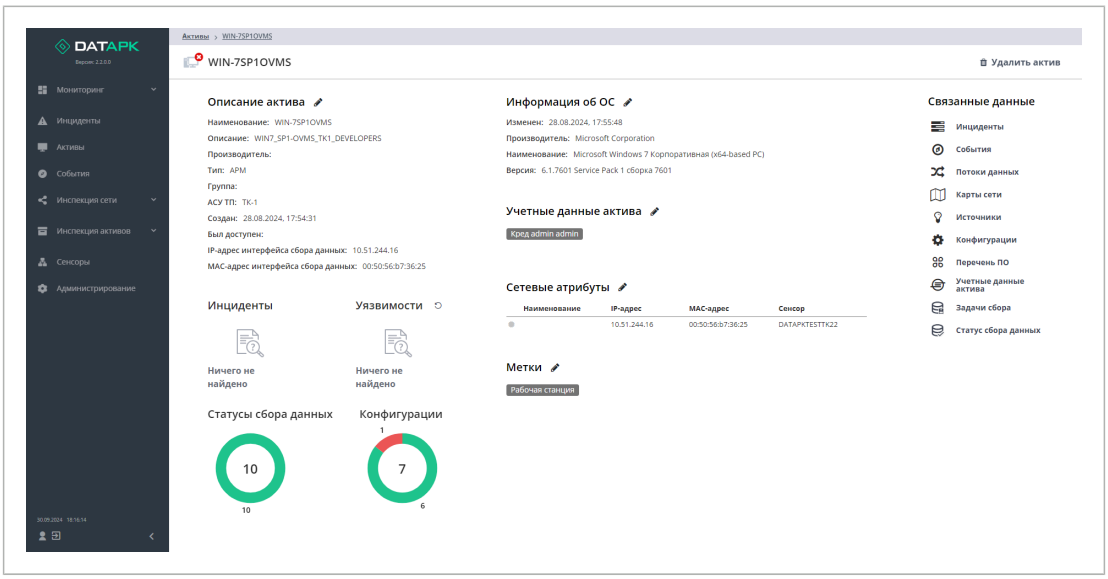


Рис. 480. Карточка актива

После заголовка расположены следующие блоки с информацией о примененных к активу параметрах и сборе данных:

1. Описание актива. Содержит информацию о Комплексе, к которому относится Актив, наименовании, описании, производителе, типе, группе Актив, АСУ ТП, датах создания и появления, IP и MAC-адресах.
2. Виджеты для отображения состояния компонентов ИБ на активе:
    a. Инциденты.
    b. Уязвимости.
    c. Статусы сбора данных.
    d. Конфигурации.
3. Информация об ОС. Содержит дату и время последнего изменения указанных данных, производителя, наименование и версию ОС. Для актива с типом `ПЛК` содержит информацию о прошивке.
4. Учетные данные. Содержит список учетных данных, присвоенных активу.
5. Сетевые атрибуты. Содержит используемые IP и MAC-адреса, с которых происходит прослушивание трафика и сбора данных с Актив (при наличии соответствующих модулей в составе Комплекса), а также содержит информацию о сенсорах, чьим контролируемым сетям принадлежат IP-адреса сетевых атрибутов.
6. Метки. Содержит список присвоенных Актив меток и кнопку (**Редактировать**) для присвоения активу ранее созданных меток.
7. Связанные данные. Содержит ссылки на разделы, относящиеся к Активу.

22.1.2.1.4. События

Раздел главного меню, содержащий список всех событий Комплекса и набор фильтров для упрощенного поиска событий.

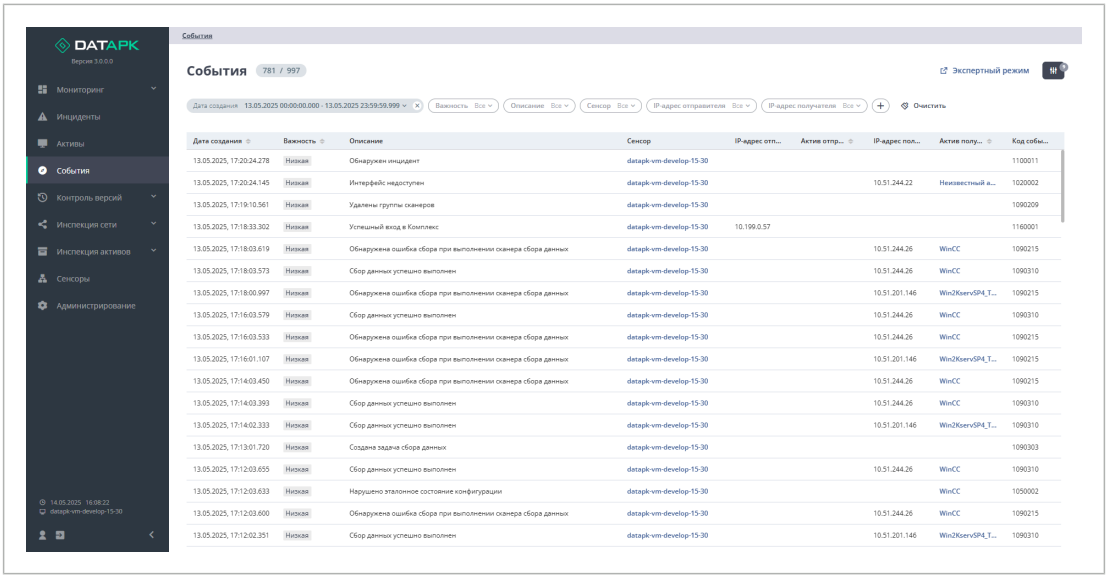


Рис. 481. Страница «События»

См. также

Поиск и просмотр событий в упрощенном режиме

22.1.2.1.4.1. Экспертный режим

Страница для работы с событиями Комплекса в расширенном режиме.

Не является разделом основного интерфейса. Перейти в экспертный режим можно со страницы **События** по кнопке Экспертный режим.

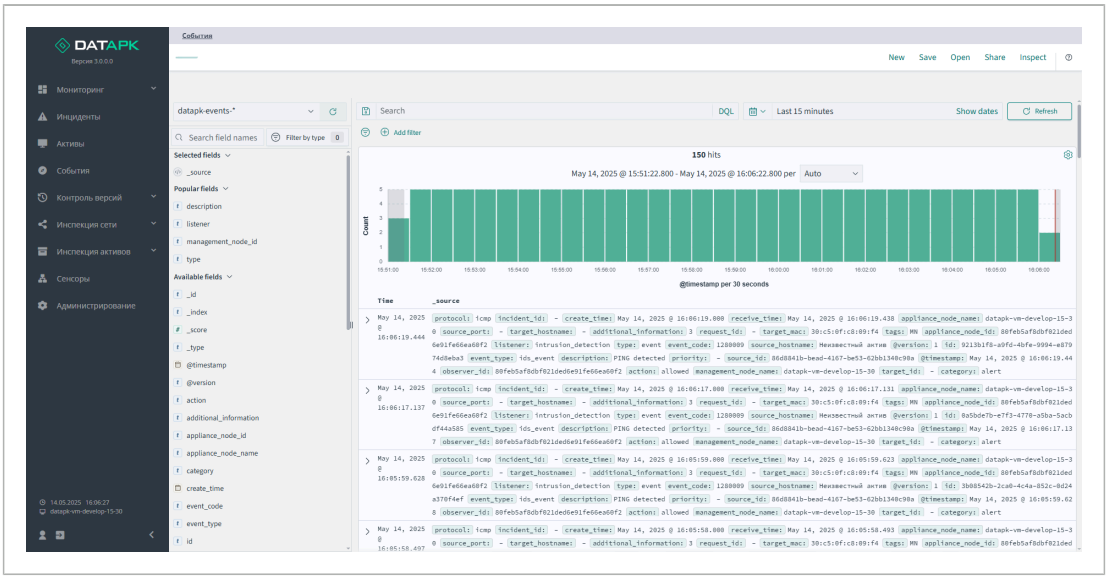


Рис. 482. Страница «Экспертный режим»

См. также

Просмотр событий и создание запросов в экспертном режиме

22.1.2.1.5. Контроль версий

Раздел главного меню, который содержит страницу для управления репозиториями.

22.1.2.1.5.1. Репозитории

Страница для управления репозиториями.

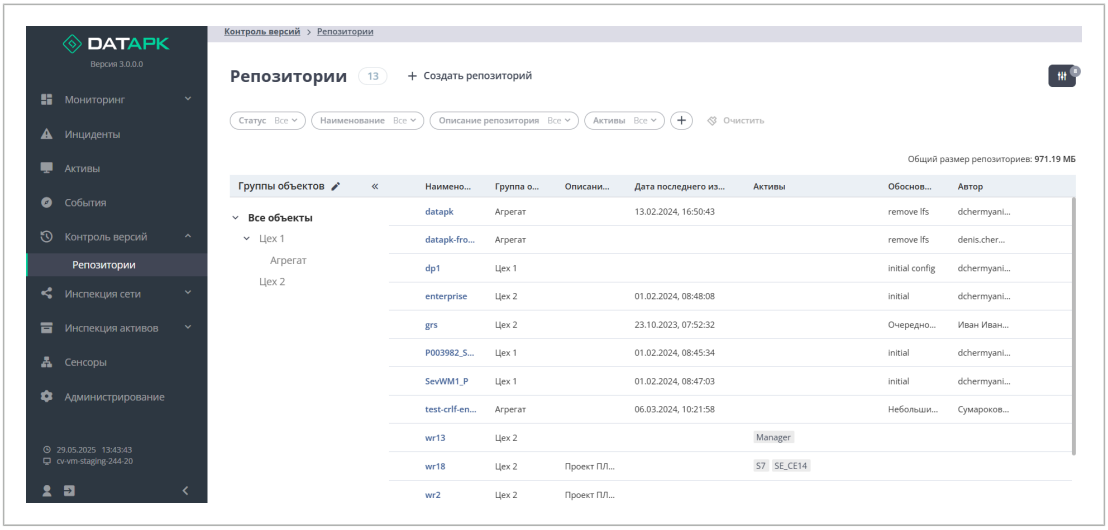


Рис. 483. Страница «Репозитории»

22.1.2.1.6. Инспекция сети

Пункт главного меню, содержащий страницы **Карта сети**, **Сетевые соединения**, **Правила сессий** и **Правила контроля тегов**.

См. также

Карта сети

Сетевые соединения

Правила сессий

Правила контроля тегов

22.1.2.1.6.1. Карта сети

Подраздел инспекции сети, предназначенный для просмотра карты сети и сохраненных фильтров.

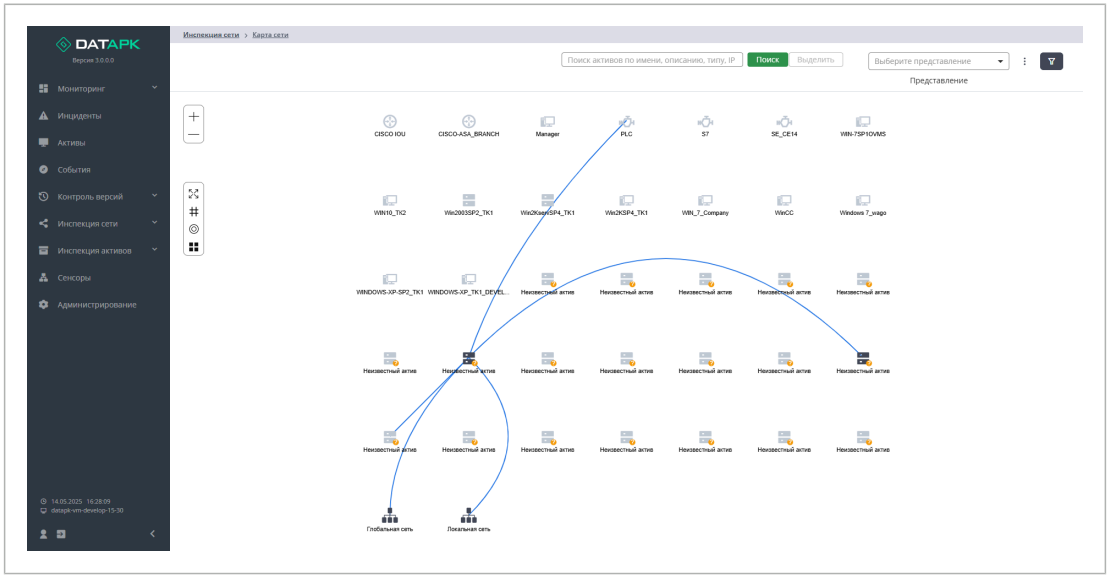


Рис. 484. Страница «Карта сети»

См. также

Просмотр карты сети

Настройка представлений на карте

22.1.2.1.6.2. Сетевые соединения

Подраздел инспекции сети для просмотра журналов взаимодействия активов в прослушиваемых сетях. В разделе можно просматривать следующую информацию:

- список сессий, которые обнаруживает Комплекс, — вкладка **Сессии**;
- записи о сетевых пакетах, которые обнаружены в рамках сессий, — вкладка **Пакеты**;
- записи о распознанных файлах, которые передавались в рамках сессий, — вкладка **Файлы**;
- записи о сетевых пакетах с вкладки **Пакеты**, дополнительно отфильтрованных по протоколам:
  - **HTTP**
  - **DNS**
  - **SMB_CMD**
  - **DCE_RPC**
  - **NTLM**
  - **SSH**
  - **SSL**
  - **Kerberos**

- **Modbus**
- **RDP**
- **SMTP**
- **OPC UA**
- **DELTAV**

22.1.2.1.6.2.1. Сессии

Вкладка на странице **Сетевые соединения** — для просмотра журнала сетевых сессий, которые обнаруживает Комплекс.

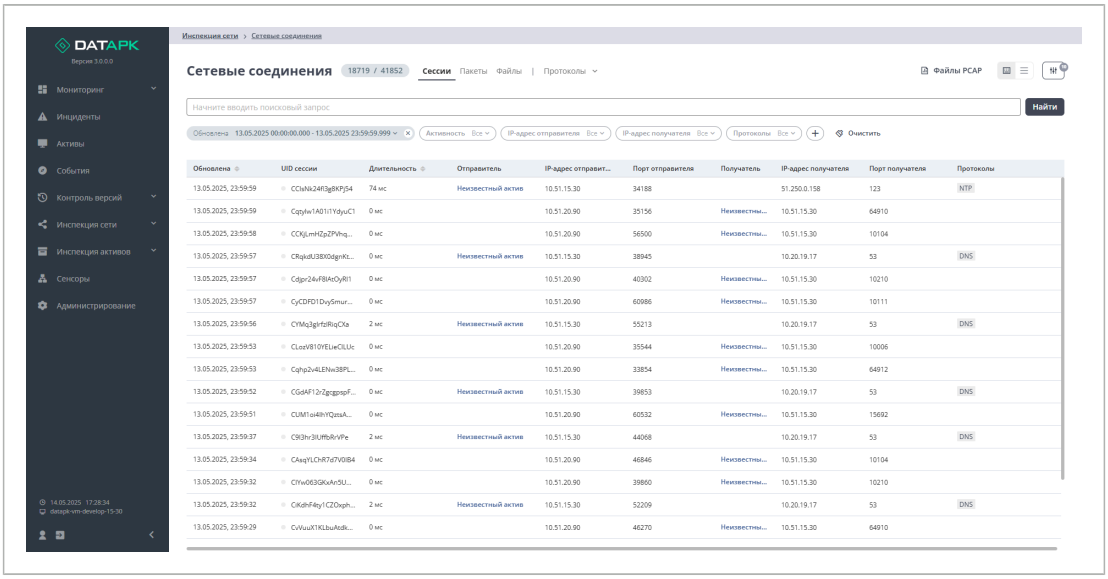


Рис. 485. Вкладка «Сессии» на странице «Сетевые соединения»

См. также

Сессия

22.1.2.1.6.2.2. Пакеты

Вкладка на странице **Сетевые соединения** — для просмотра записей о сетевых пакетах, обнаруживаемых Комплексом в рамках сессий. Одна запись о пакетах содержит информацию о наборе пакетов, сгруппированных по протоколу и идентификатору сессии (UID).

На вкладке также можно экспортировать трафик из записей о пакетах в формат `.pcap`.

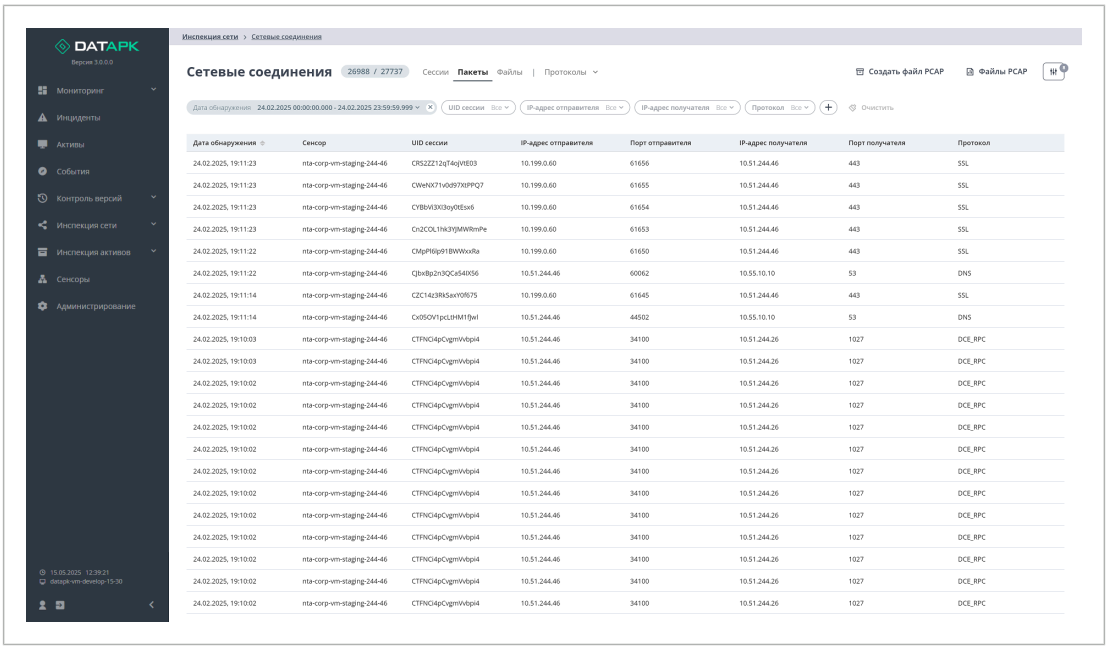


Рис. 486. Вкладка «Пакеты» на странице «Сетевые соединения»

22.1.2.1.6.2.2.1. HTTP

Вкладка из группы вкладок **Протоколы** на странице **Сетевые соединения** — для мониторинга HTTP-пакетов, обнаруживаемых Комплексом в рамках сессий.

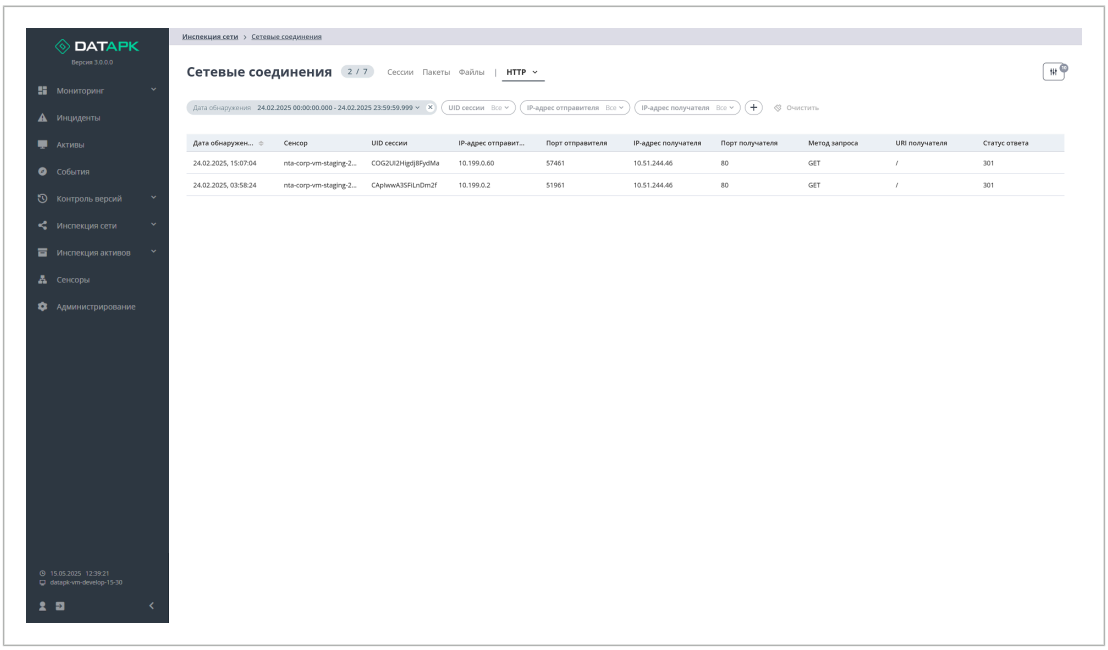


Рис. 487. Вкладка «HTTP» на странице «Сетевые соединения»

22.1.2.1.6.2.2.2. DNS

Вкладка из группы вкладок **Протоколы** на странице **Сетевые соединения** — для мониторинга DNS-пакетов, обнаруживаемых Комплексом в рамках сессий.

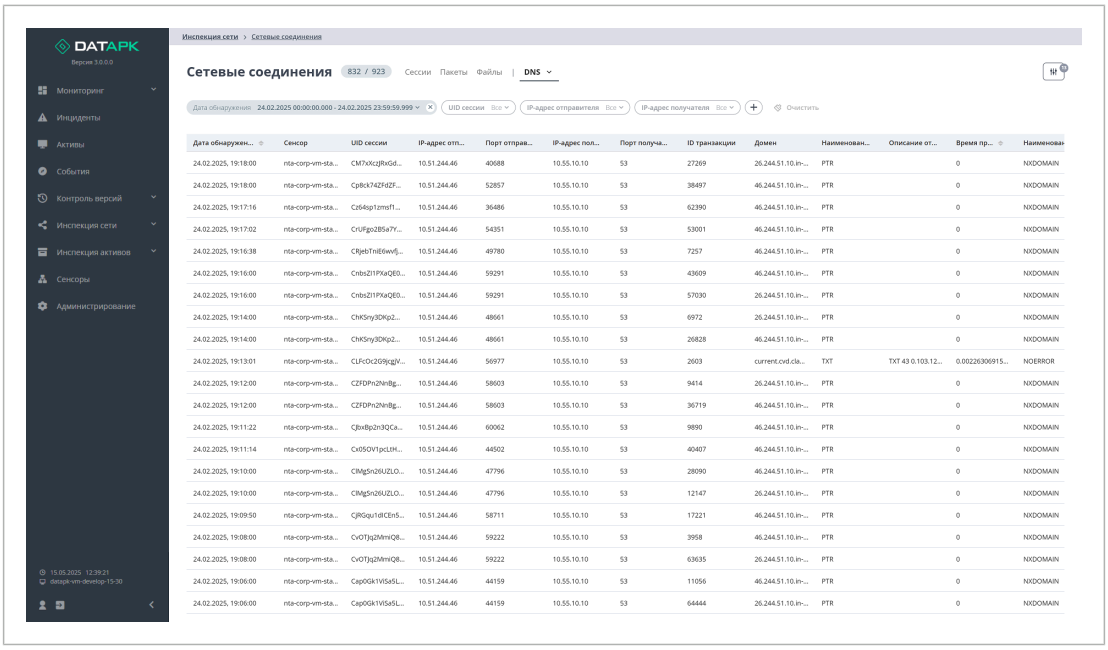


Рис. 488. Вкладка «DNS» на странице «Сетевые соединения»

См. также

Туннелирование DNS

22.1.2.1.6.2.2.3. SMB_CMD

Вкладка из группы вкладок **Протоколы** на странице **Сетевые соединения** — для мониторинга пакетов SMB_CMD, обнаруживаемых Комплексом в рамках сессий.

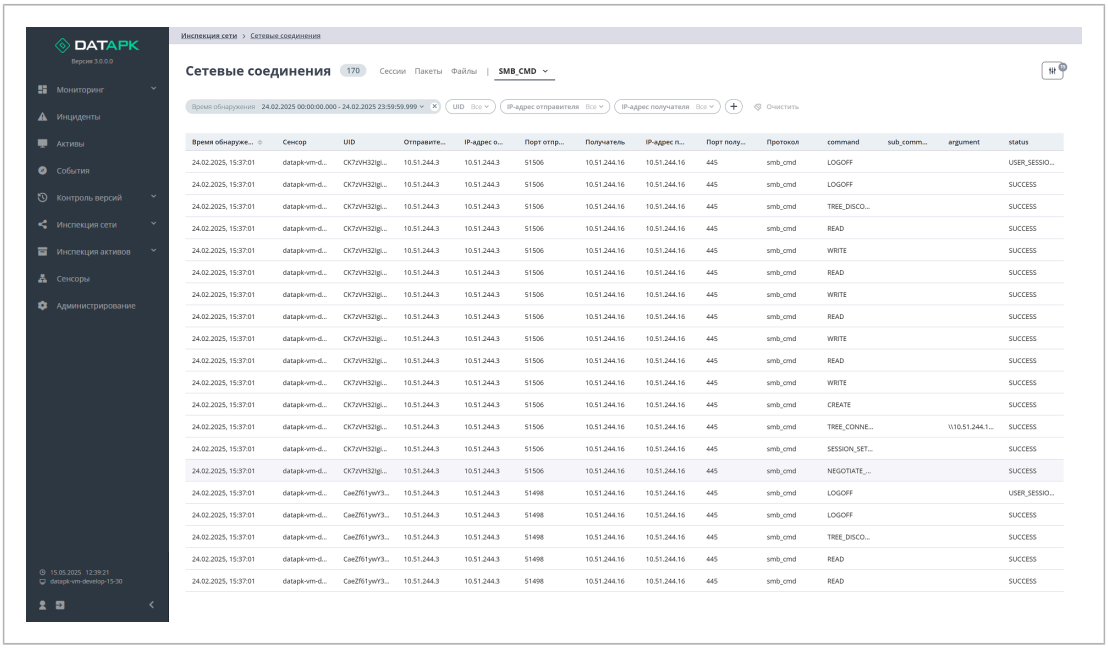


Рис. 489. Вкладка «SMB_CMD» на странице «Сетевые соединения»

22.1.2.1.6.2.2.4. DCE_RPC

Вкладка из группы вкладок **Протоколы** на странице **Сетевые соединения** — для мониторинга пакетов DCE/RPC, обнаруживаемых Комплексом в рамках сессий.

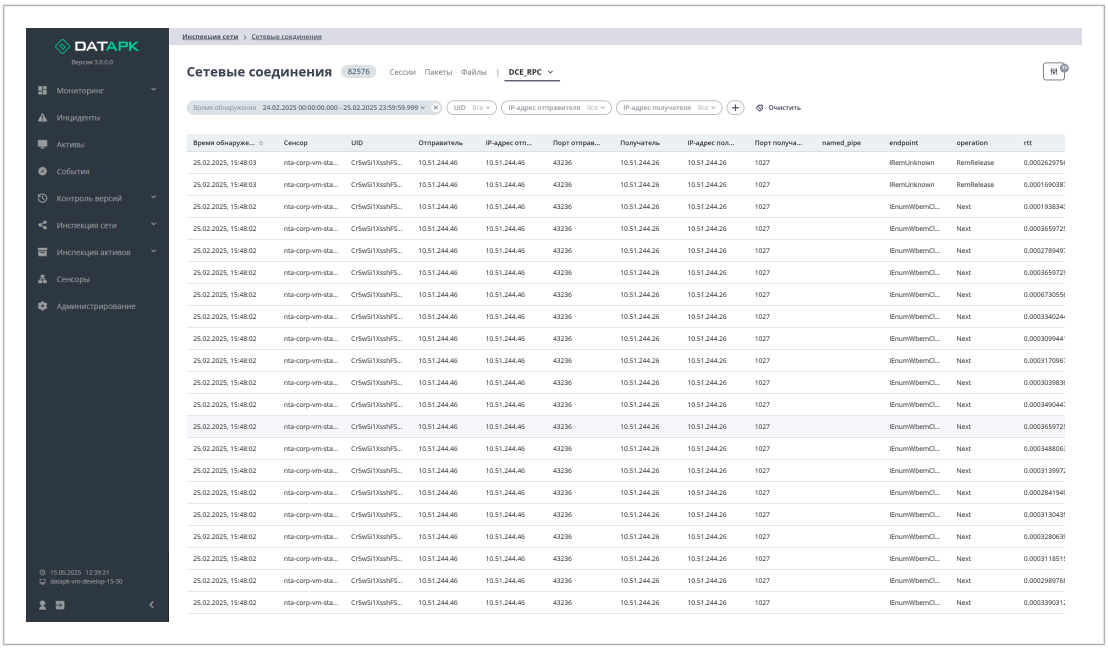


Рис. 490. Вкладка «DCE_RPC» на странице «Сетевые соединения»

22.1.2.1.6.2.2.5. NTLM

Вкладка из группы вкладок **Протоколы** на странице **Сетевые соединения** — для мониторинга NTLM-пакетов, обнаруживаемых Комплексом в рамках сессий.

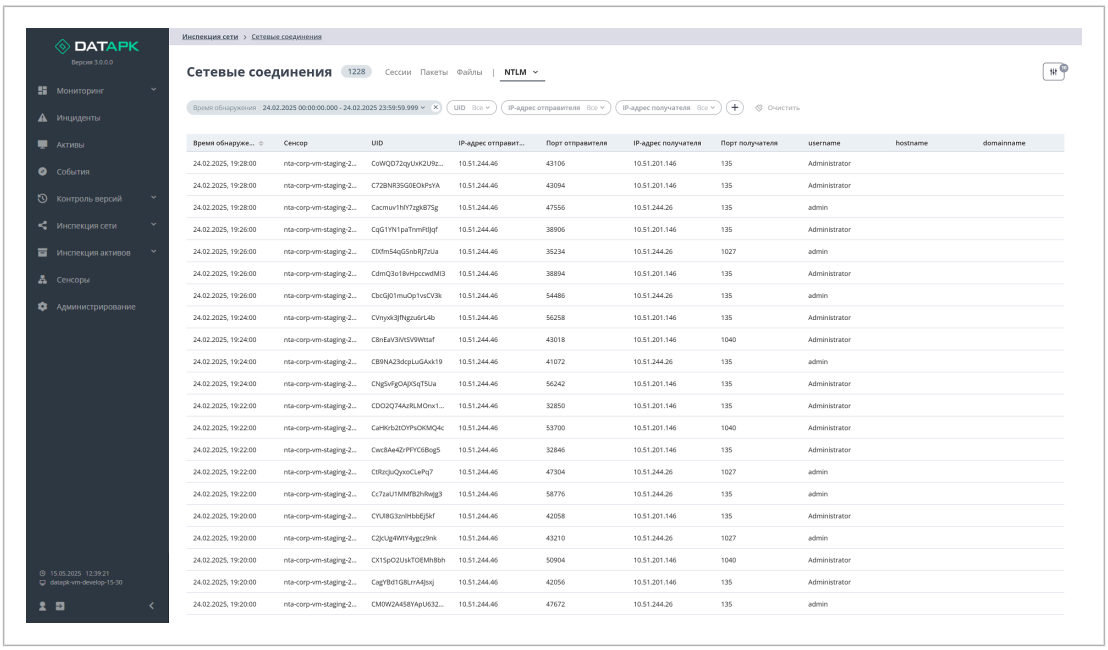


Рис. 491. Вкладка «NTLM» на странице «Сетевые соединения»

22.1.2.1.6.2.2.6. SSH

Вкладка из группы вкладок **Протоколы** на странице **Сетевые соединения** — для мониторинга SSH-пакетов, обнаруживаемых Комплексом в рамках сессий.

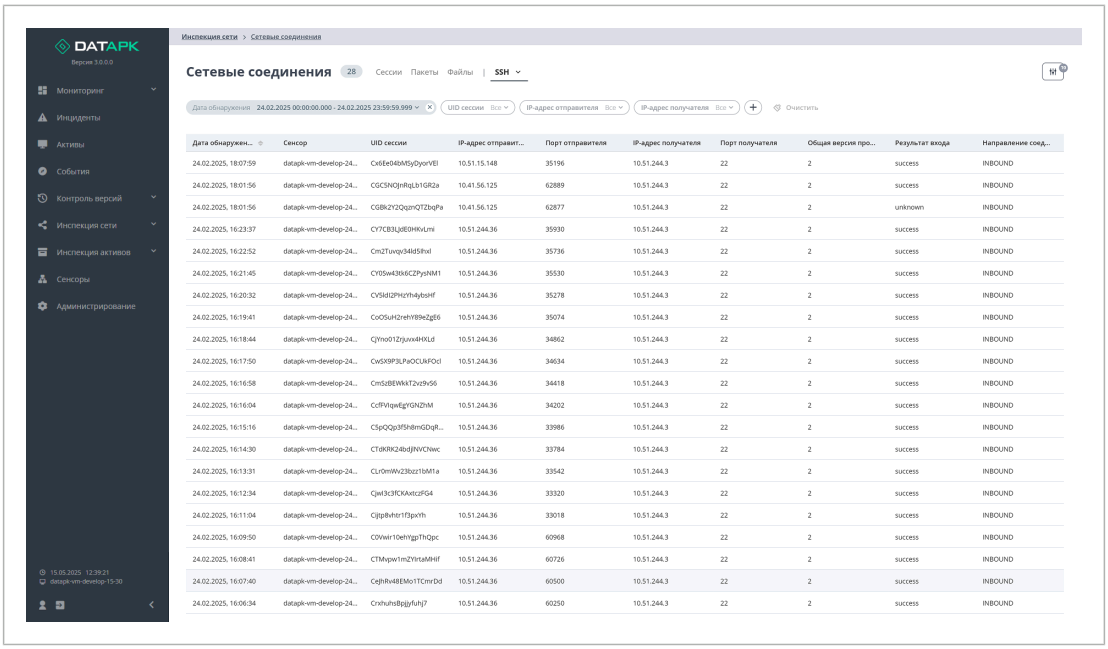


Рис. 492. Вкладка «SSH» на странице «Сетевые соединения»

22.1.2.1.6.2.2.7. SSL

Вкладка из группы вкладок **Протоколы** на странице **Сетевые соединения** — для мониторинга SSL-пакетов, обнаруживаемых Комплексом в рамках сессий.

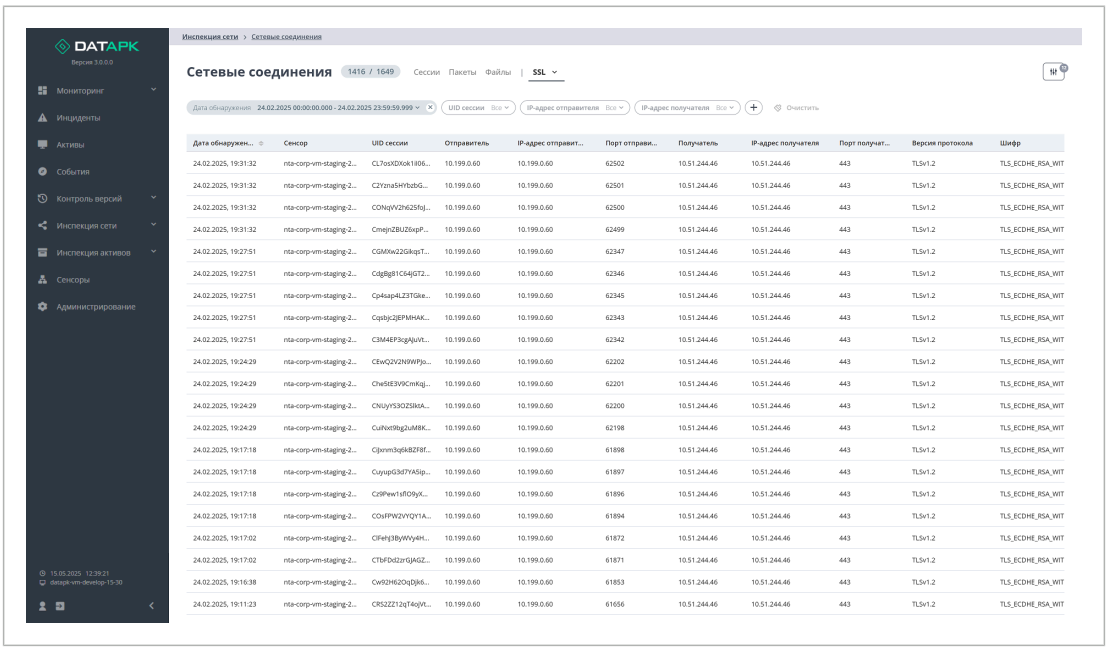


Рис. 493. Вкладка «SSL» на странице «Сетевые соединения»

22.1.2.1.6.2.2.8. Kerberos

Вкладка из группы вкладок **Протоколы** на странице **Сетевые соединения** — для мониторинга Kerberos-пакетов, обнаруживаемых Комплексом в рамках сессий.

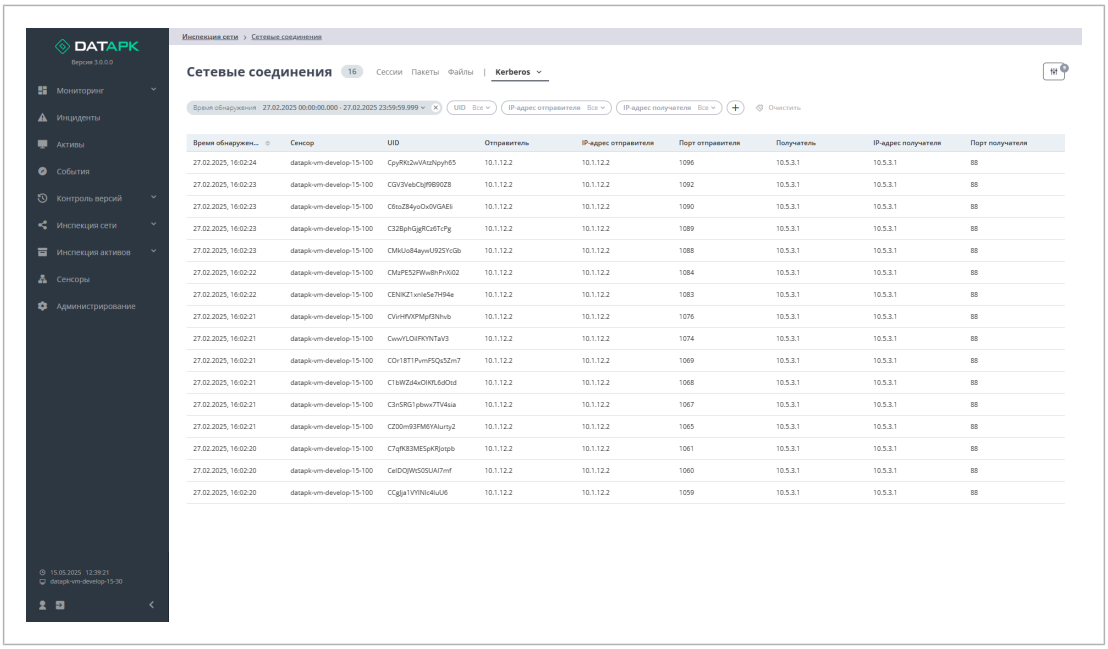


Рис. 494. Вкладка «Kerberos» на странице «Сетевые соединения»

22.1.2.1.6.2.2.9. Modbus

Вкладка из группы вкладок **Протоколы** на странице **Сетевые соединения** — для мониторинга Modbus-пакетов, обнаруживаемых Комплексом в рамках сессий.

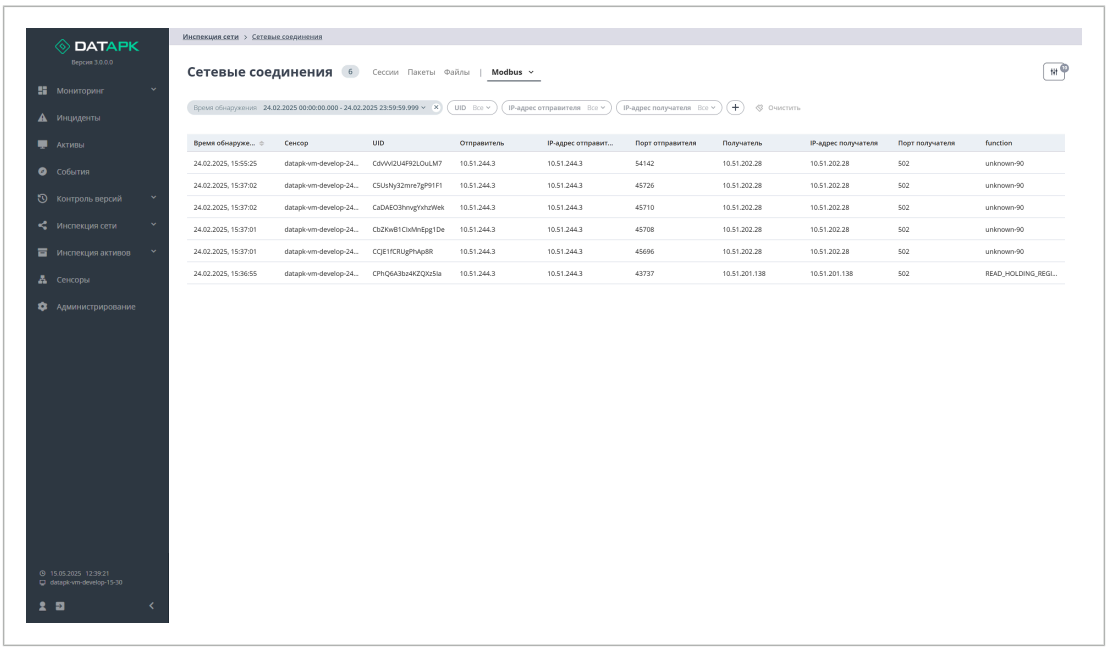


Рис. 495. Вкладка «Modbus» на странице «Сетевые соединения»

22.1.2.1.6.2.2.10. RDP

Вкладка из группы вкладок **Протоколы** на странице **Сетевые соединения** — для мониторинга RDP-пакетов, обнаруживаемых Комплексом в рамках сессий.

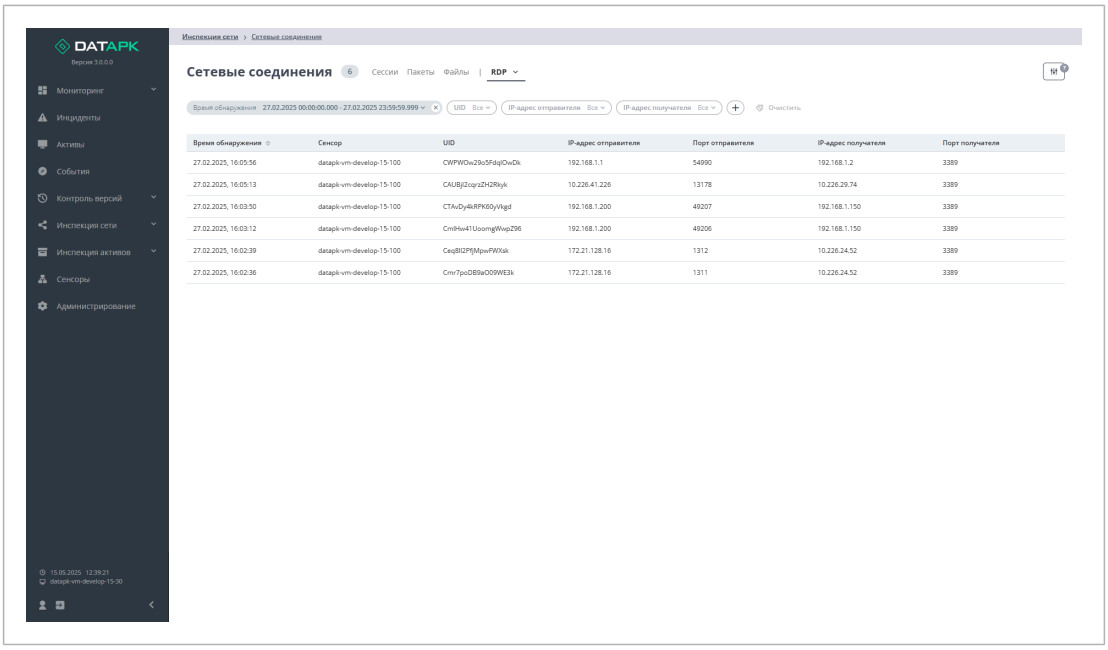


Рис. 496. Вкладка «RDP» на странице «Сетевые соединения»

22.1.2.1.6.2.2.11. SMTP

Вкладка из группы вкладок **Протоколы** на странице **Сетевые соединения** — для мониторинга SMTP-пакетов, обнаруживаемых Комплексом в рамках сессий.

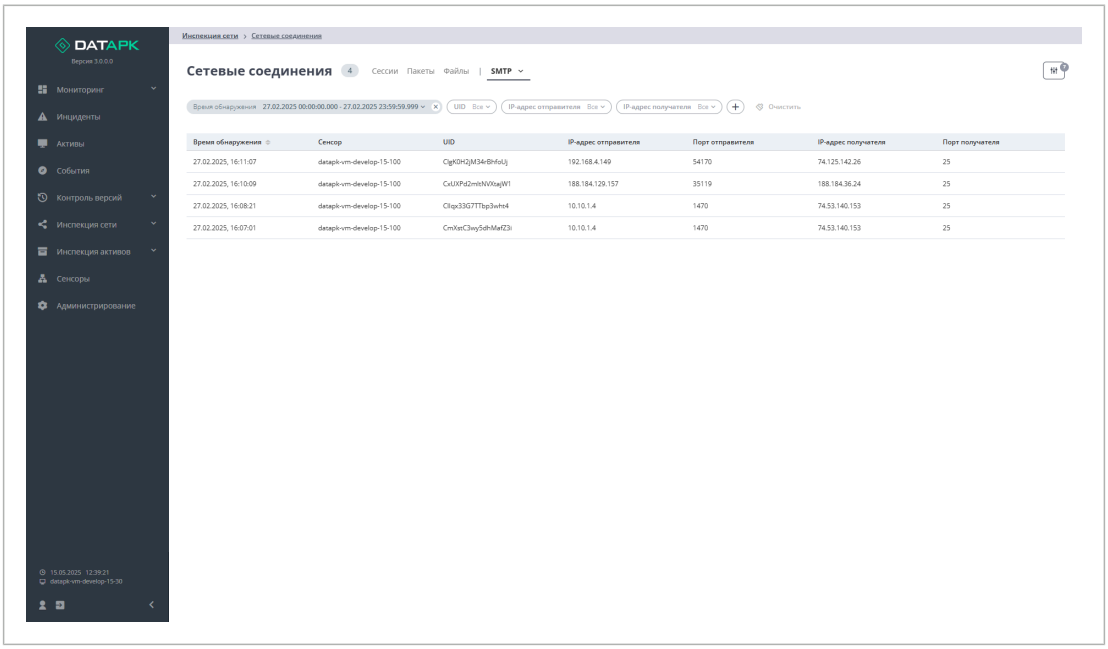


Рис. 497. Вкладка «SMTP» на странице «Сетевые соединения»

22.1.2.1.6.2.2.12. OPC UA

Вкладка из группы вкладок **Протоколы** на странице **Сетевые соединения** — для мониторинга пакетов OPC UA, обнаруживаемых Комплексом в рамках сессий.

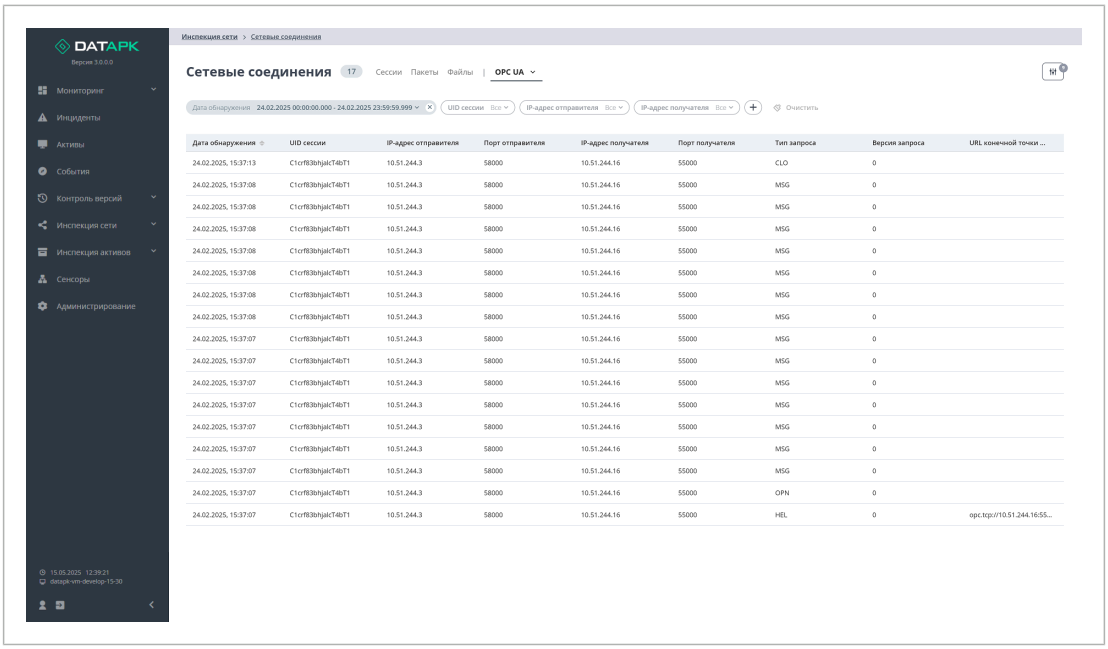


Рис. 498. Вкладка «OPC UA» на странице «Сетевые соединения»

22.1.2.1.6.2.2.13. DELTAV

Вкладка из группы вкладок **Протоколы** на странице **Сетевые соединения** — для мониторинга DeltaV-пакетов, обнаруживаемых Комплексом в рамках сессий.

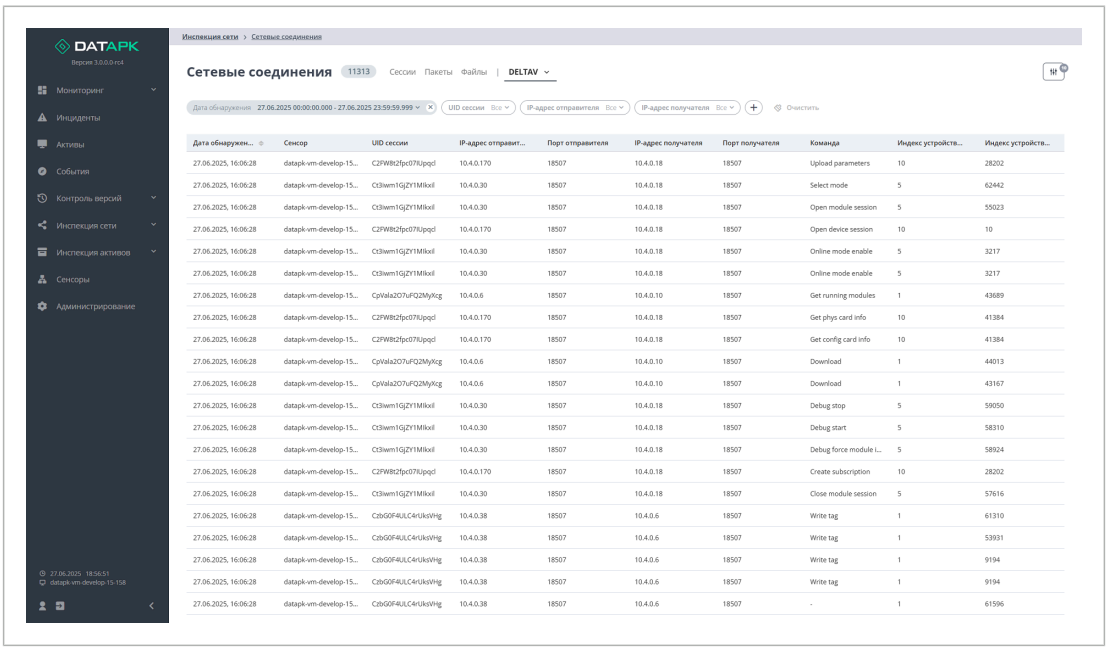


Рис. 499. Вкладка «DELTAV» на странице «Сетевые соединения»

22.1.2.1.6.2.3. Файлы

Вкладка на странице **Сетевые соединения** — для просмотра информации о распознанных файлах, переданных в рамках сессий, и скачивания этих файлов.

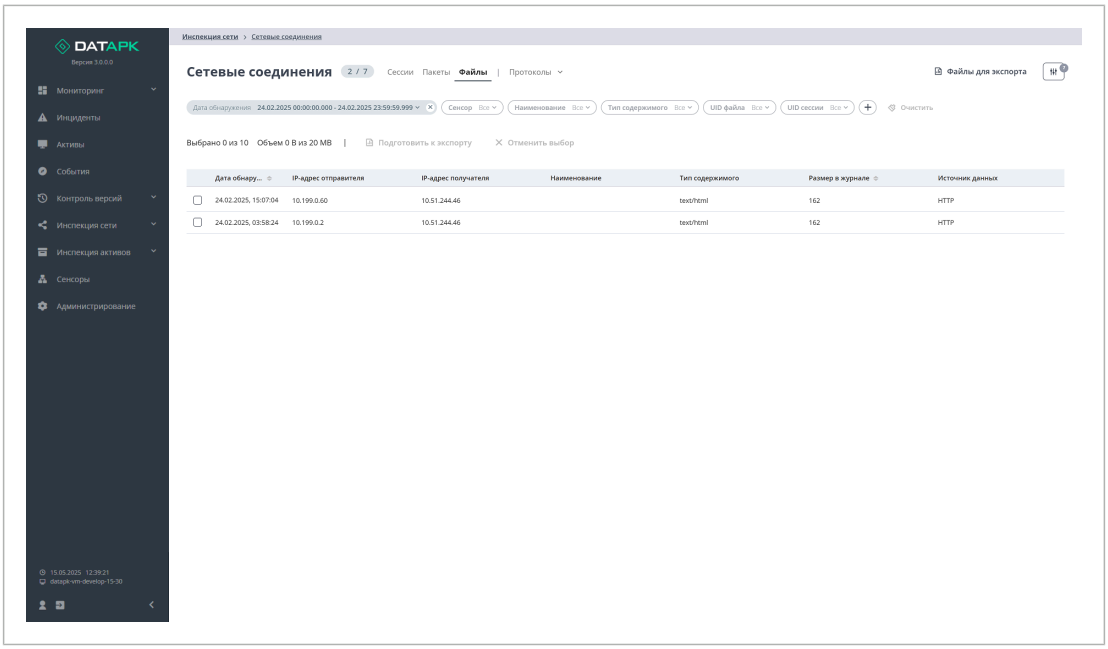


Рис. 500. Страница «Файлы»

См. также

Экспорт файлов, обнаруженных в сетевом трафике

22.1.2.1.6.3. Правила сессий

Подраздел инспекции сети, где можно просматривать, создавать, редактировать и удалять правила автоматической обработки сессий, а также можно переходить к сессиям, которые попали под правило.

Просмотр подробной информации о правиле сессий доступен по нажатию на строку с интересующим правилом.

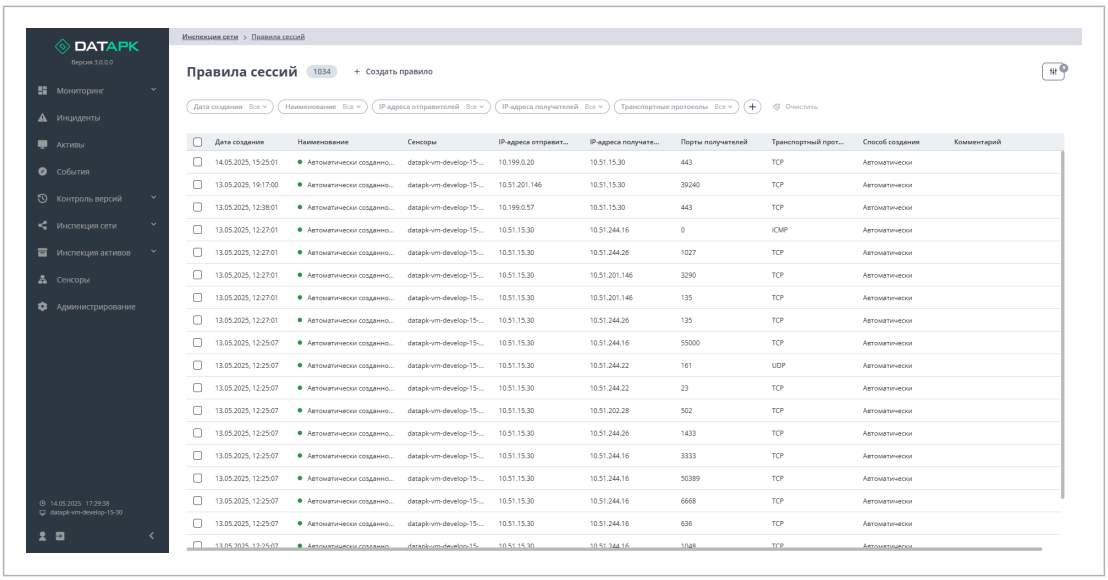


Рис. 501. Страница «Правила сессий»

См. также

Просмотр правил сессий

Фильтрация списка правил сессий

Автоматическое создание правил сессий

Деактивация автоматического создания правил сессий

Редактирование правил сессий

Активация и деактивация правил сессий

Удаление правил сессий

22.1.2.1.6.4. Правила контроля тегов

Подраздел инспекции сети, где можно просматривать, создавать, редактировать и удалять правила контроля тегов.

Просмотр подробной информации о правиле контроля тегов доступен по нажатию на строку с интересующим правилом.

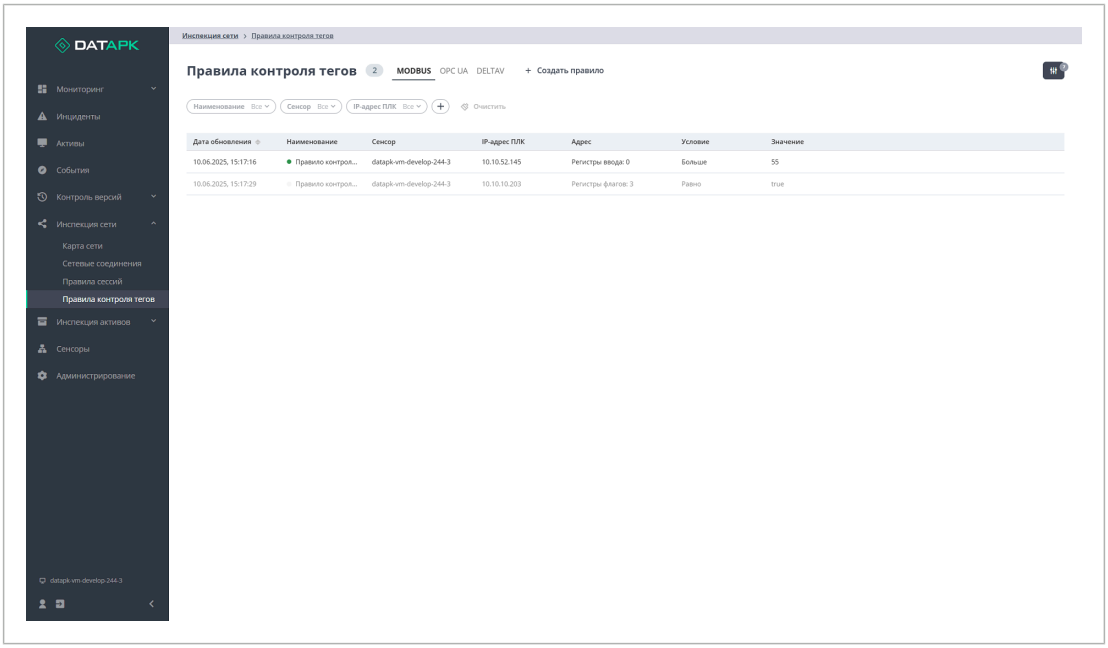


Рис. 502. Страница «Правила контроля тегов»

22.1.2.1.7. Инспекция активов

Пункт главного меню, содержащий страницы **Задачи сбора**, **Статус сбора**, **Перечень ПО**, **Конфигурации**, **Результаты проверок**.

См. также

Задачи сбора

Статус сбора

Перечень ПО

Конфигурации

Результаты проверок

22.1.2.1.7.1. Задачи сбора

Подраздел инспекции активов, в котором можно создавать, редактировать, запускать и удалять задачи сбора данных.

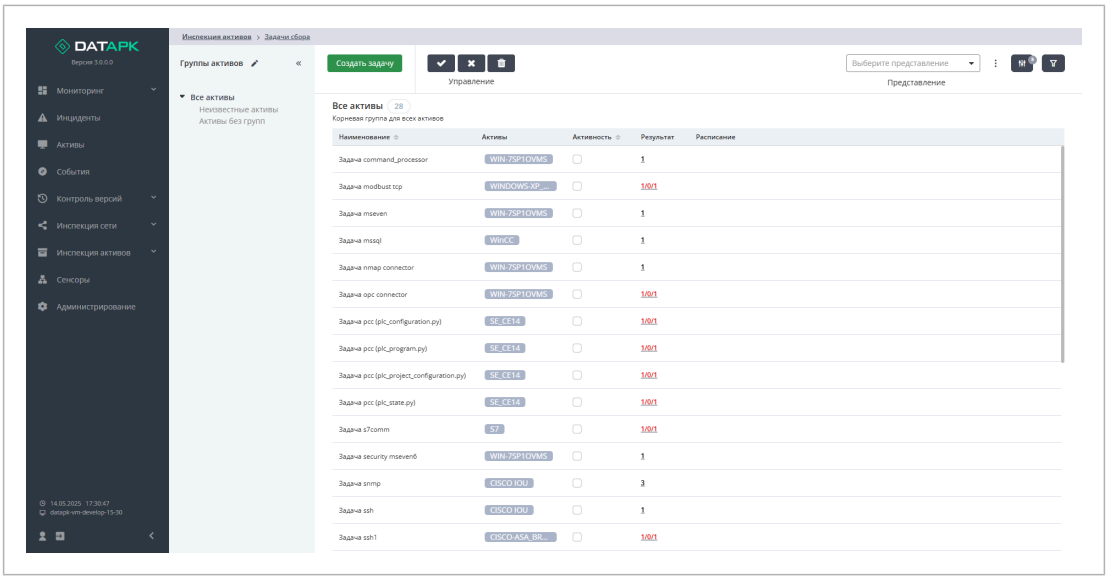


Рис. 503. Страница «Задачи сбора»

См. также

Создание задачи сбора данных

Управление задачами сбора данных

22.1.2.1.7.2. Статус сбора

Подраздел инспекции активов, в котором можно просматривать и удалять результаты, полученные при выполнении задач и сканеров.

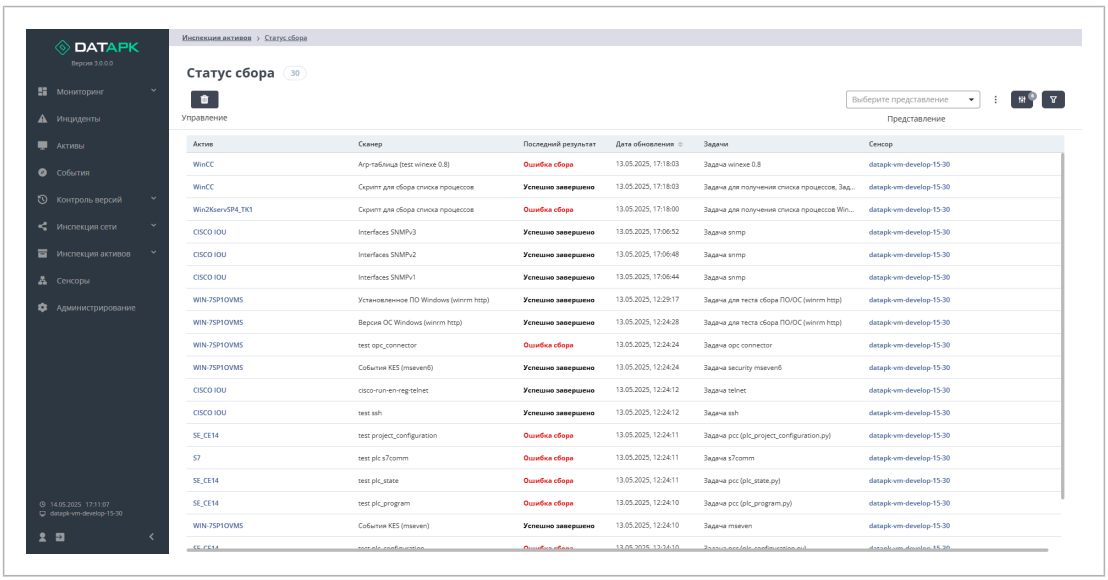


Рис. 504. Страница «Статус сбора»

См. также

Просмотр статуса сбора данных

22.1.2.1.7.3. Перечень ПО

Подраздел инспекции активов, в котором можно просматривать и фильтровать список ПО, собранный сканерами, а также экспортировать отчет по результатам сопоставления ПО со справочником CPE.

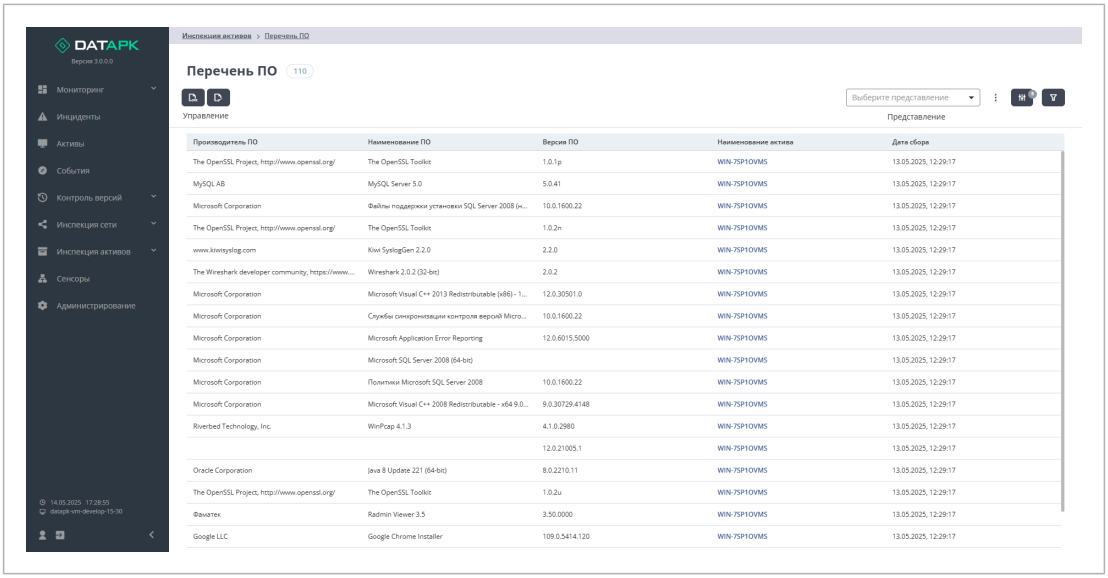


Рис. 505. Страница «Перечень ПО»

См. также

Запуск сбора данных об операционной системе и установленном ПО

Выгрузка отчета по результатам сопоставления собранного ПО со справочником CPE

22.1.2.1.7.4. Конфигурации

Подраздел инспекции активов, в котором можно просматривать последние собранные конфигурации со всех активов. Страница предоставляет широкие возможности по фильтрации собранных данных. При необходимости можно сформировать отчет.

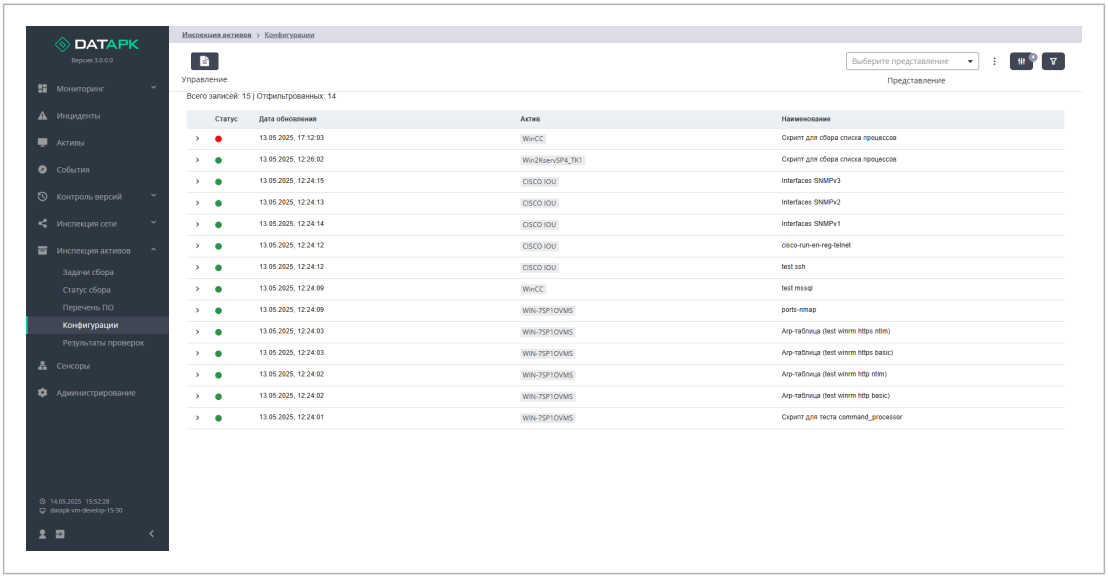


Рис. 506. Страница «Конфигурации»

См. также

Выгрузка отчетов

Просмотр сводки конфигураций

22.1.2.1.7.4.1. Конфигурации актива

Не является разделом основного интерфейса. Перейти к конфигурациям актива можно двумя способами:

- со страницы **Конфигурации** по кнопке (**Просмотреть конфигурацию актива**) напротив выбранной конфигурации;
- из **карточки актива** по ссылке **Конфигурации** в разделе **Связанные данные**.

Содержание страницы различается в зависимости от актива, для которого открыта карточка. Основные блоки страницы конфигураций:

1. Меню со списком всех собранных когда-либо типов конфигураций в левой части страницы.
2. Управление конфигурациями в верхней части страницы:
    - выпадающий список со всеми собранными конфигурациями;
    - кнопка **Принять за эталонную**;
    - кнопка удаления конфигурации;
    - кнопка **Создать интерфейсы**. Отображается для коммутаторов при сборе по протоколу SNMP.
3. Список собранных данных, доступных для просмотра и сравнению в виде:
    - таблицы;
    - строки под строкой;
    - двух экранов.

Если текущая конфигурация соответствует эталону, но в промежутке между эталонной и текущей обнаружены конфигурации, не соответствующие эталону, на страницу выводится предупреждение о том, что необходимо оценить легитимность таких изменений.

Конфигурация, не соответствующая эталону, отмечена значком

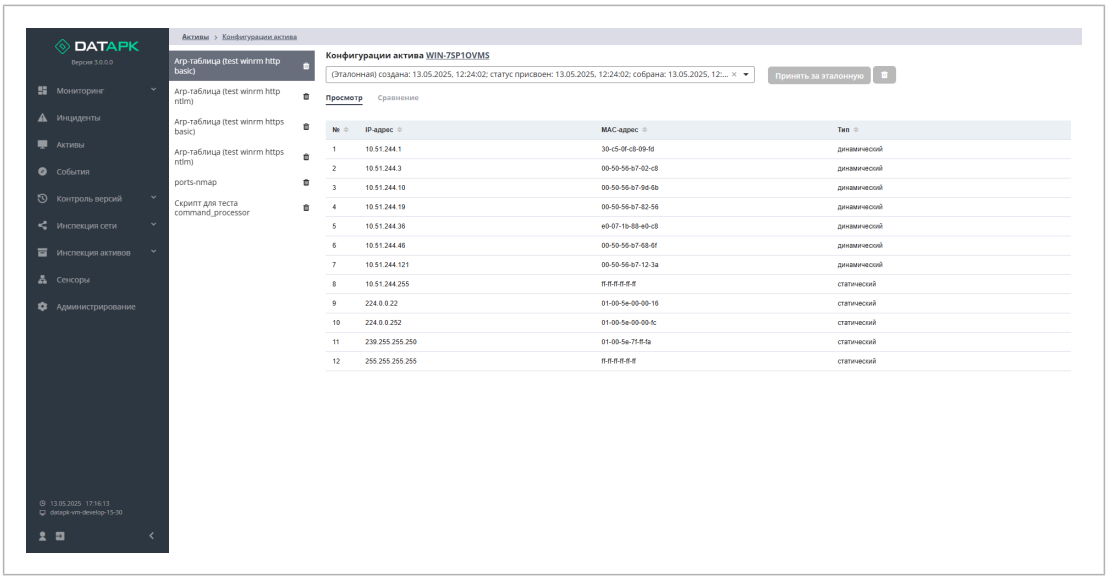


Рис. 507. Страница «Конфигурации актива»

22.1.2.1.7.5. Результаты проверок

Подраздел инспекции активов, где можно создавать, редактировать и удалять проверки на соответствие требованиям ИБ. После получения результата имеются возможности просмотреть и сохранить результат отдельной проверки, перезапустить проверку, сохранить отчет по результатам проверок на странице.

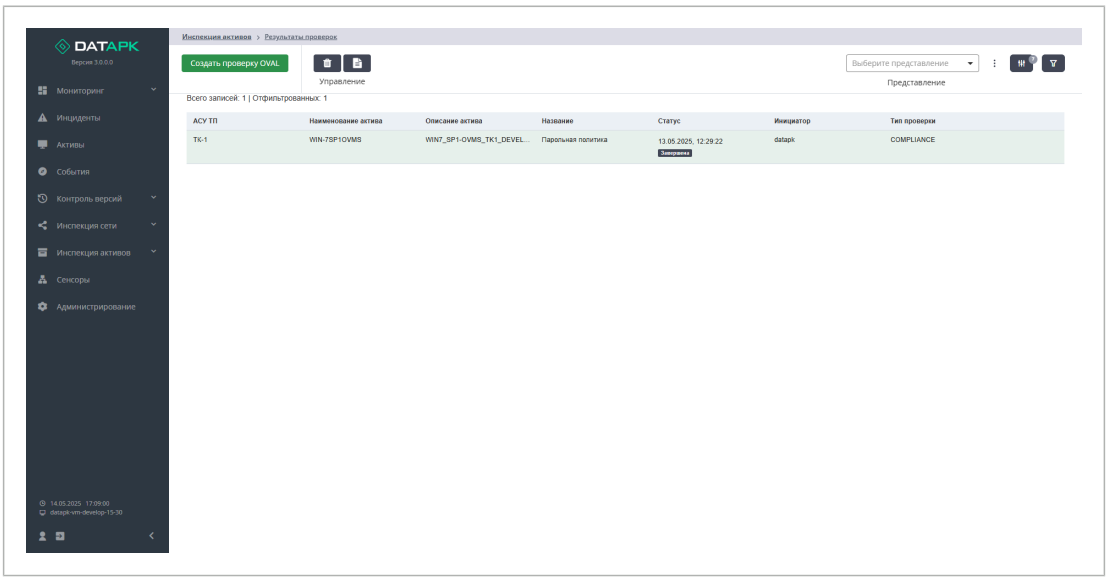


Рис. 508. Страница «Результаты проверок»

См. также

Запуск OVAL-проверки актива на соответствие требованиям информационной безопасности

Просмотр и выгрузка результатов проверки актива на соответствие требованиям информационной безопасности

Повторный запуск OVAL-проверки на соответствие требованиям ИБ

Удаление OVAL-проверок актива на соответствие требованиям информационной безопасности

22.1.2.1.7.5.1. Результаты проверки

Не является разделом основного интерфейса. Перейти к подробным результатам проверки актива на соответствие требованиям ИБ можно со страницы по кнопке ☰ (**Просмотреть результаты**) напротив успешно выполненной проверки.

Страница содержит таблицу с подробной информацией об отдельных критериях проверки соответствия, которые сформировали итоговый результат проверки. Содержание страницы различается в зависимости от актива и набора критериев проверки.

Для критериев наличия уязвимости (с классом `VULNERABILITY`) в колонке **Меры по исправлению уязвимостей** приводятся рекомендации по устранению как для обнаруженных, так и не обнаруженных уязвимостей.

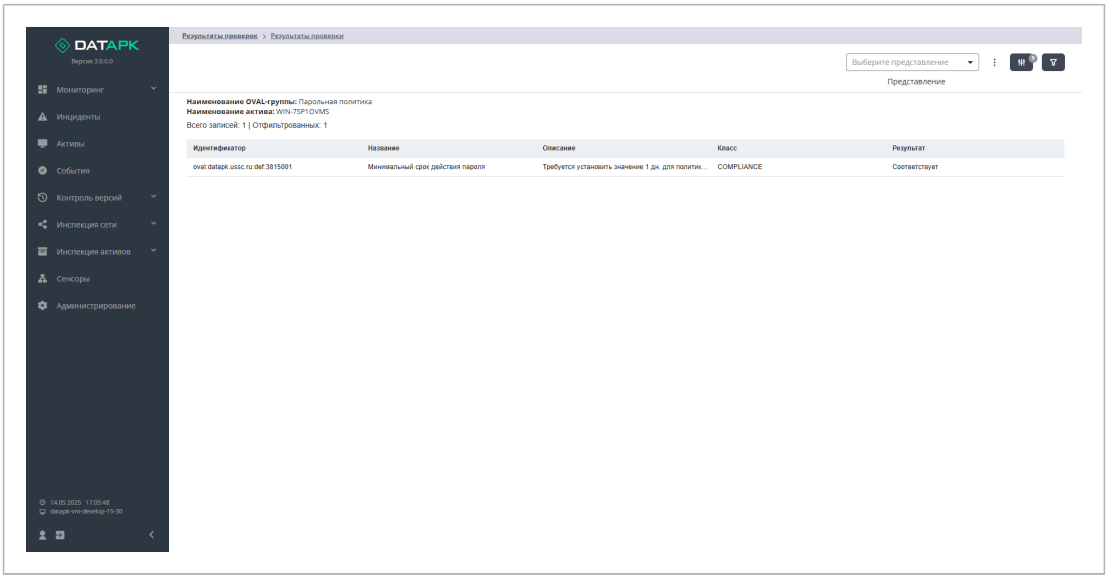


Рис. 509. Страница «Результаты проверки»

См. также

Просмотр и выгрузка результатов проверки актива на соответствие требованиям информационной безопасности

22.1.2.1.8. Сенсоры

Пункт главного меню Комплекса, содержащий список всех сенсоров, подключенных к Комплексу.

На странице для каждого сенсора можно задавать основные сведения, просматривать статусы и графики активности, запускать сканирование сети, выбирать контролируемые сети, включать службу обнаружения вторжений, удалять сенсор и его данные из Комплекса.

На данной странице отображается следующая информация о сенсоре:

- **Статус**
- **Наименование сенсора**
- **Описание сенсора**
- **Контролируемая сеть**
- **Эксплуатирующая организация**
- **Место установки**
- **Последнее появление** — время последней успешной проверки доступности сенсора.

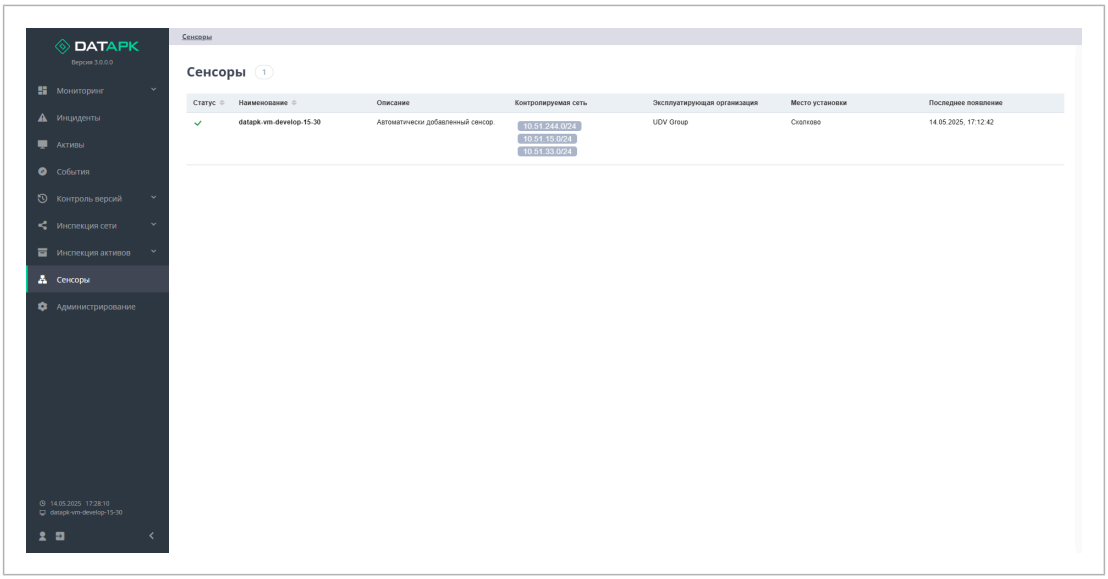


Рис. 510. Страница «Сенсоры»

22.1.2.1.9. Администрирование

Раздел главного меню, который содержит страницы, связанные с настройкой различных аспектов работы Комплекса:

- **Основные настройки**
- **Инспекция активов**
- **События и инциденты**
- **Пользователи**
- **Сигнатурный анализ**
- **Настройка активов**

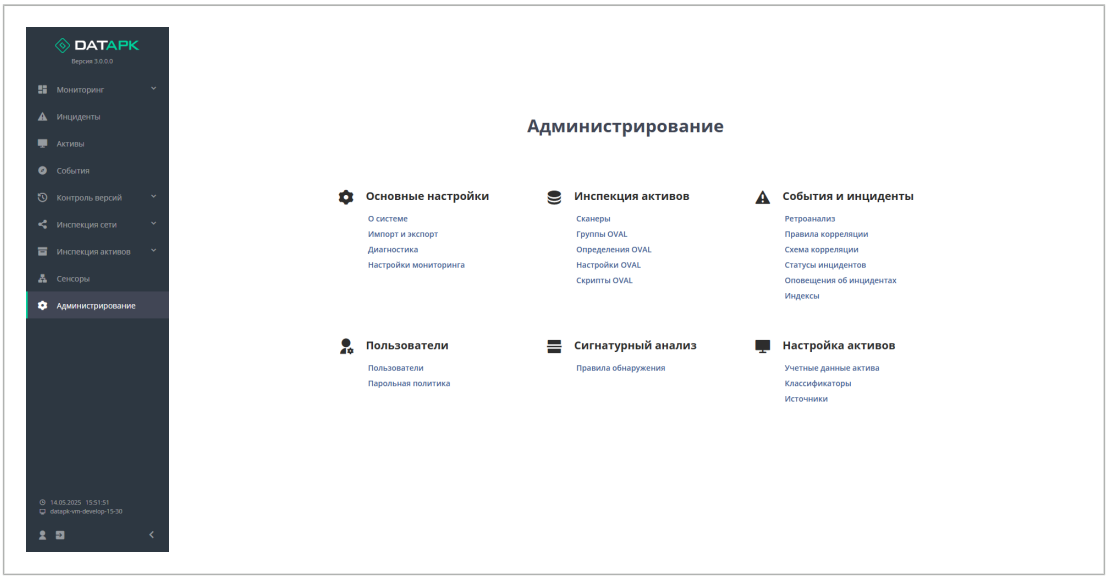


Рис. 512. Страница «Администрирование»

22.1.2.1.9.1. Основные настройки

22.1.2.1.9.1.1. О системе

Подраздел управления Комплексом, где можно задавать основные сведения о расположении Комплекса, эксплуатирующей организации, а также его описание. В правой части страницы указан производитель Комплекса и его версия.

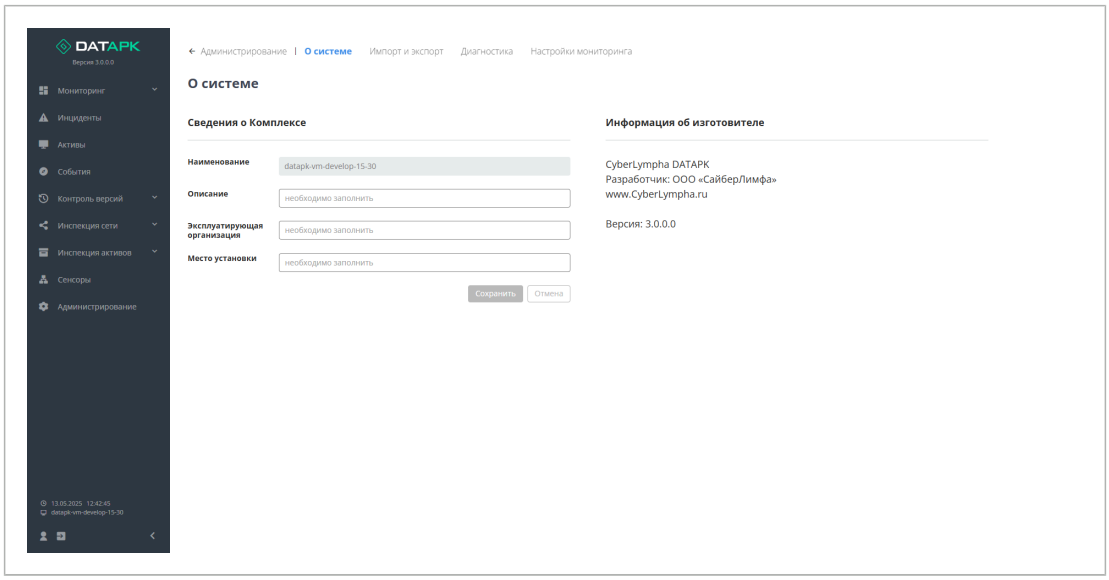


Рис. 513. Страница «О системе»

См. также

Изменение сведений о Комплексе и сенсорах

22.1.2.1.9.1.2. Импорт и экспорт

Страница, где можно экспортировать и импортировать справочники.

> Подсказка:
>
> Доступен импорт справочников размером до 145 МБ.

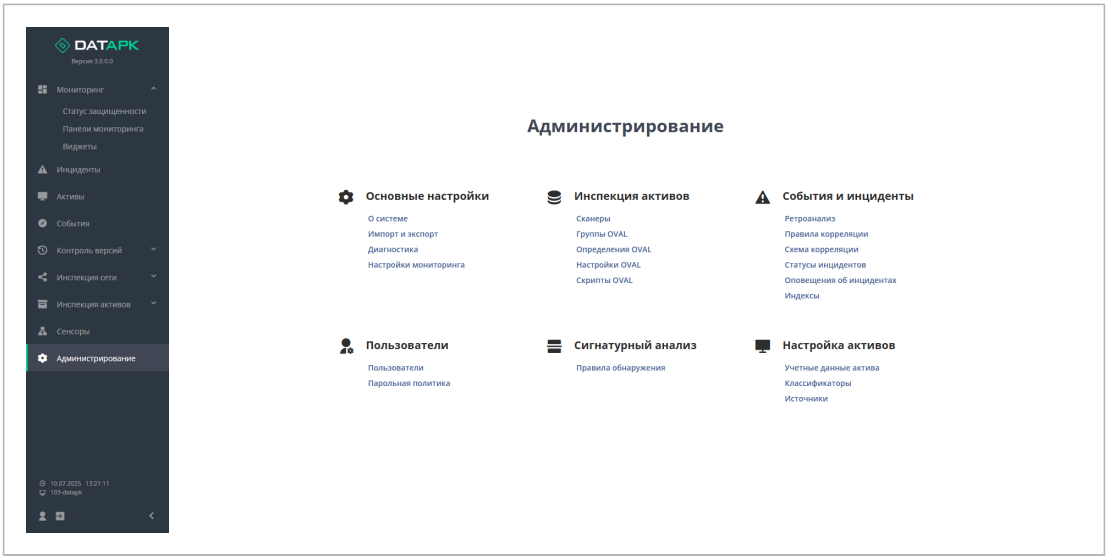


Рис. 514. Страница «Импорт и экспорт»

См. также

Экспорт и импорт правил нормализации событий

Экспорт и импорт политики корреляции

Экспорт и импорт классификаторов

Импорт и экспорт скриптов, настроек, групп определений OVAL

Импорт учетных данных активов

Экспорт и импорт источников событий

Экспорт и импорт правил службы обнаружения вторжения

Экспорт и импорт задач сбора данных, сканеров и их групп

22.1.2.1.9.1.3. Диагностика

Подраздел управления Комплексом, где можно просматривать графики нагрузки на различные компоненты системы, на которой установлен текущий Комплекс. Для выбора доступны периоды 1 час, 24 часа и 7 дней.

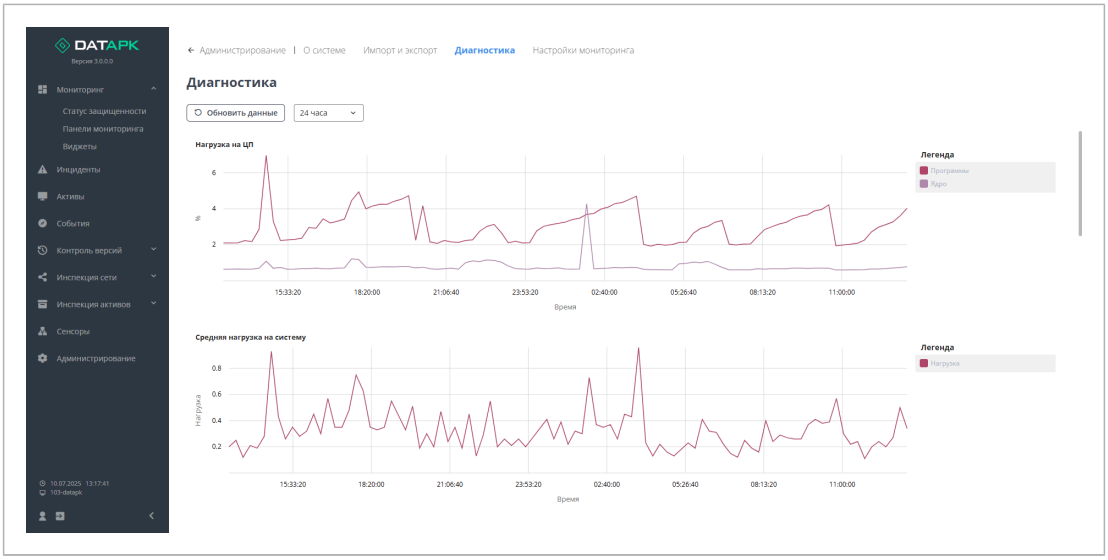


Рис. 515. Страница «Диагностика»

См. также

Диагностика состояния системы Комплекса

22.1.2.1.9.1.4. Настройки мониторинга

Подраздел мониторинга, в котором можно настраивать шаблоны индекса, осуществлять экспорт и импорт, настраивать отображение в подразделах мониторинга.

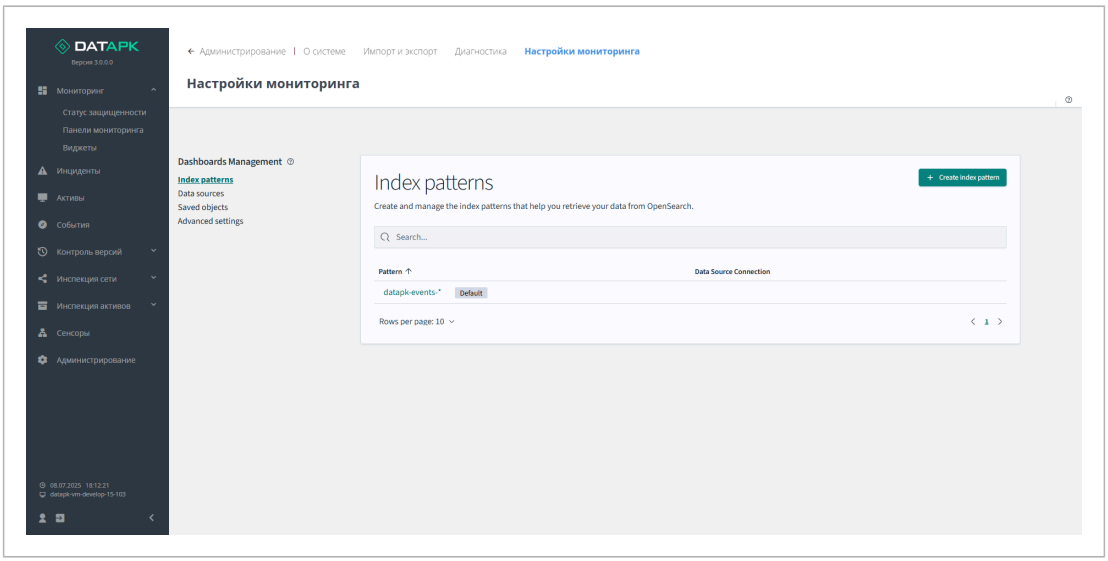


Рис. 517. Страница «Настройки мониторинга»

См. также

Настройка пользовательских правил нормализации событий

Настройка форматирования чисел и дат в разделе «Мониторинг»

Экспорт и импорт объектов раздела «Мониторинг»

22.1.2.1.9.2. Инспекция активов

Пункт меню страницы **Администрирование**.

См. также

Сканеры

Группы OVAL

Определения OVAL

Настройки OVAL

Скрипты OVAL

22.1.2.1.9.2.1. Сканеры

Подраздел настроек конфигураций, где можно создавать, редактировать, запускать и удалять сканеры сбора данных.

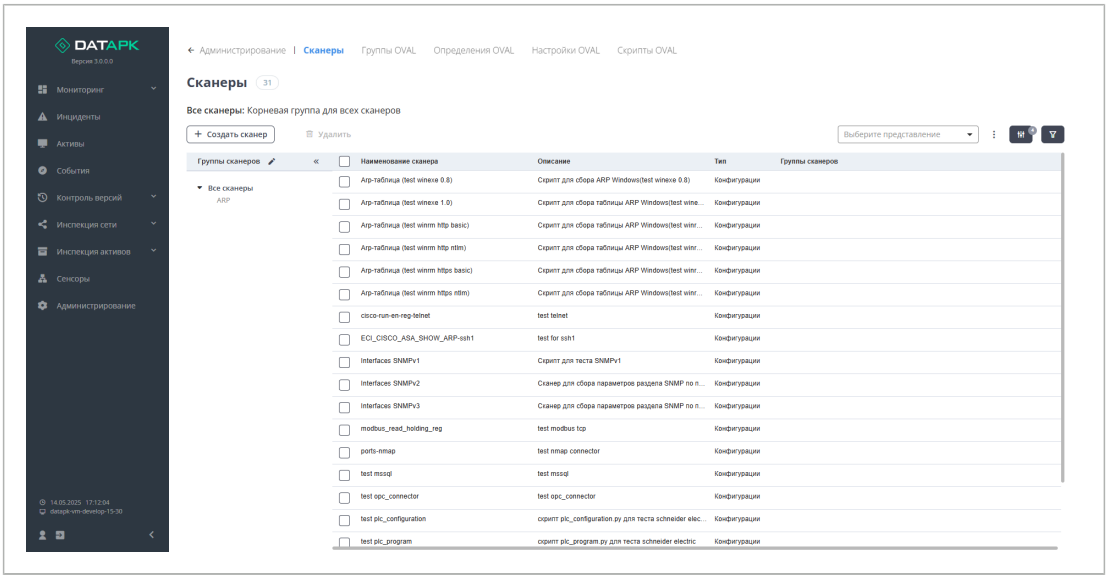


Рис. 518. Страница «Сканеры»

См. также

Создание сканера сбора данных

Настройка сканеров сбора данных

Управление сканерами сбора данных

Группировка сканеров сбора данных

22.1.2.1.9.2.2. Группы OVAL

Подраздел настроек проверок и отчетов, где можно создавать, редактировать и удалять группы OVAL-определений.

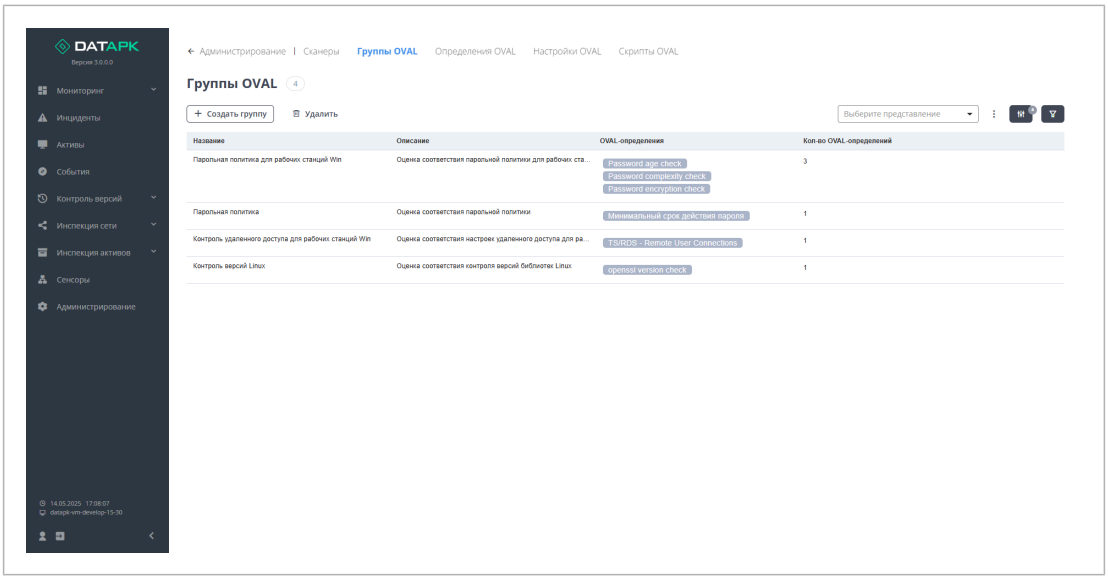


Рис. 519. Страница «Группы OVAL определений»

См. также

Создание группы определений OVAL

Добавление и исключение OVAL-определений из групп

Импорт групп OVAL-определений

22.1.2.1.9.2.3. Определения OVAL

Страница, где можно добавлять в группы, исключать из групп и удалять OVAL-определения.

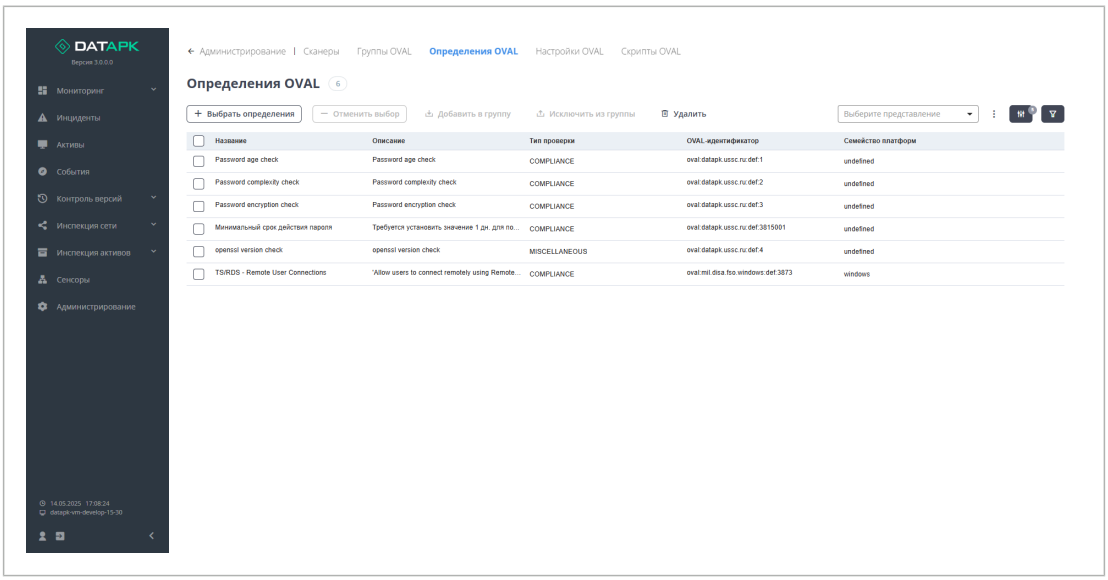


Рис. 520. Страница «Определения OVAL»

См. также

Добавление и исключение OVAL-определений из групп

Импорт OVAL-определений

22.1.2.1.9.2.4. Настройки OVAL

Подраздел настроек проверок и отчетов, в котором можно создавать, редактировать и удалять настройки скриптов OVAL по отношению к активам и меткам.

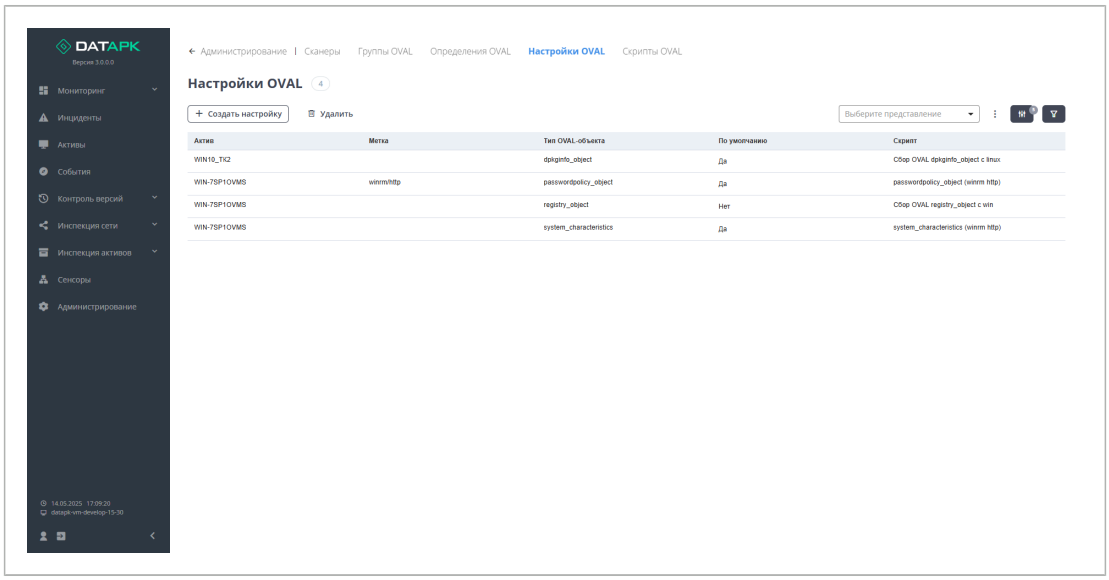


Рис. 521. Страница «Настройки OVAL»

См. также

Настройка доступа к активу для сбора OVAL-объектов

22.1.2.1.9.2.5. Скрипты OVAL

Подраздел настроек проверок и отчетов, где можно создавать, редактировать и удалять скрипты сбора проверок на соответствие требованиям ИБ.

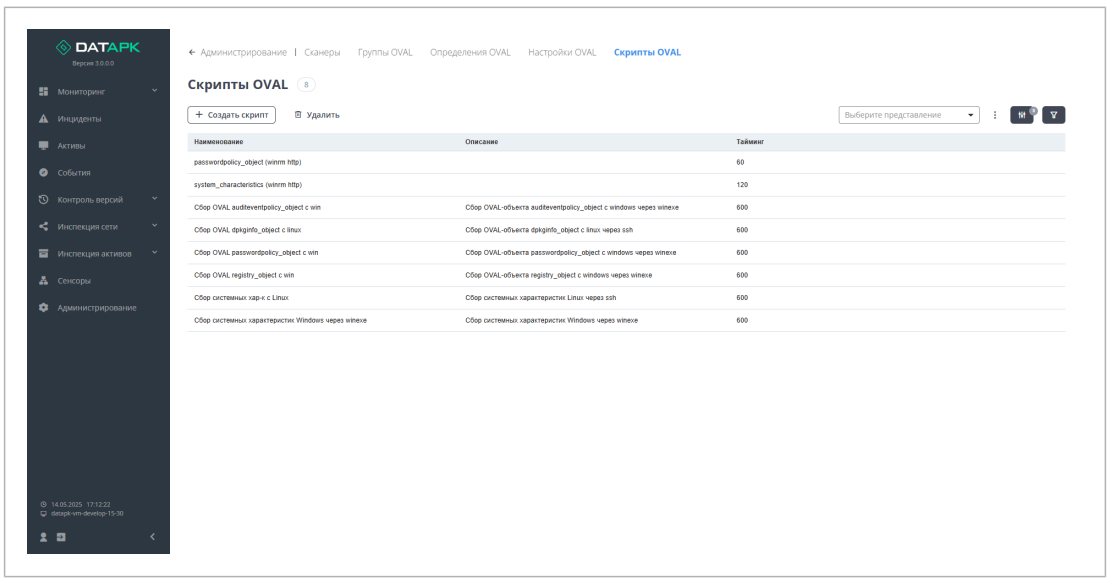


Рис. 522. Страница «Скрипты»

См. также

Содержание Python-скриптов

22.1.2.1.9.3. События и инциденты

Пункт главного меню, содержащий подразделы **События и инциденты** и **Ретроанализ**.

См. также

Инциденты

Статусы инцидентов

Правила корреляции

Оповещения об инцидентах

Схема корреляции

Ретроанализ

22.1.2.1.9.3.1. Ретроанализ

Страница, где можно запускать, перезапускать и удалять ретроспективные проверки.

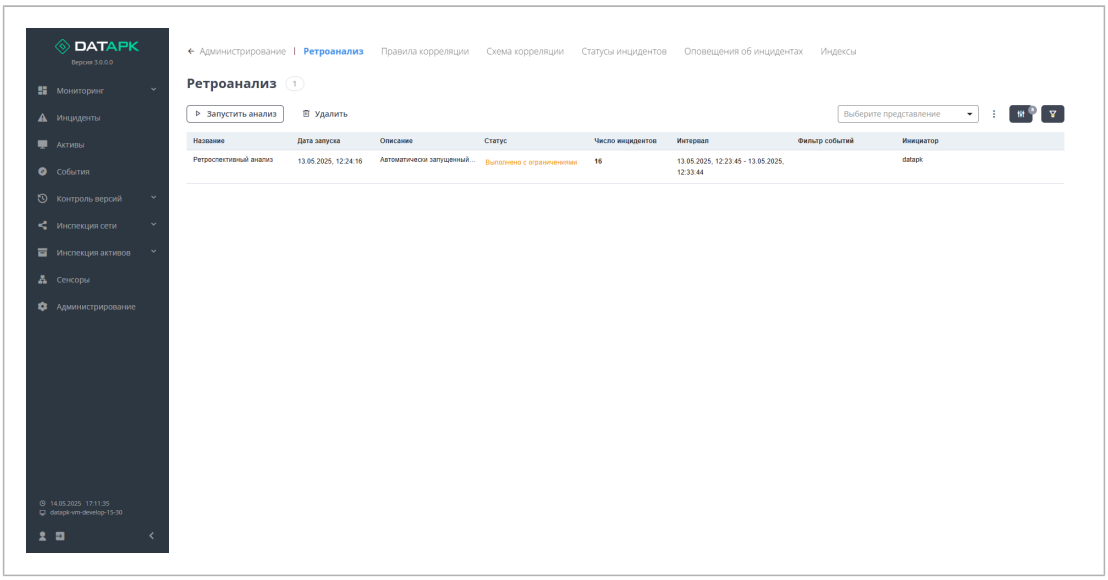


Рис. 523. Страница «Ретроанализ»

См. также

Ретроспективный анализ событий

22.1.2.1.9.3.2. Правила корреляции

Подраздел настроек инцидентов, в котором можно управлять службой корреляции событий, создавать, редактировать, применять, удалять, активировать и деактивировать правила корреляции.

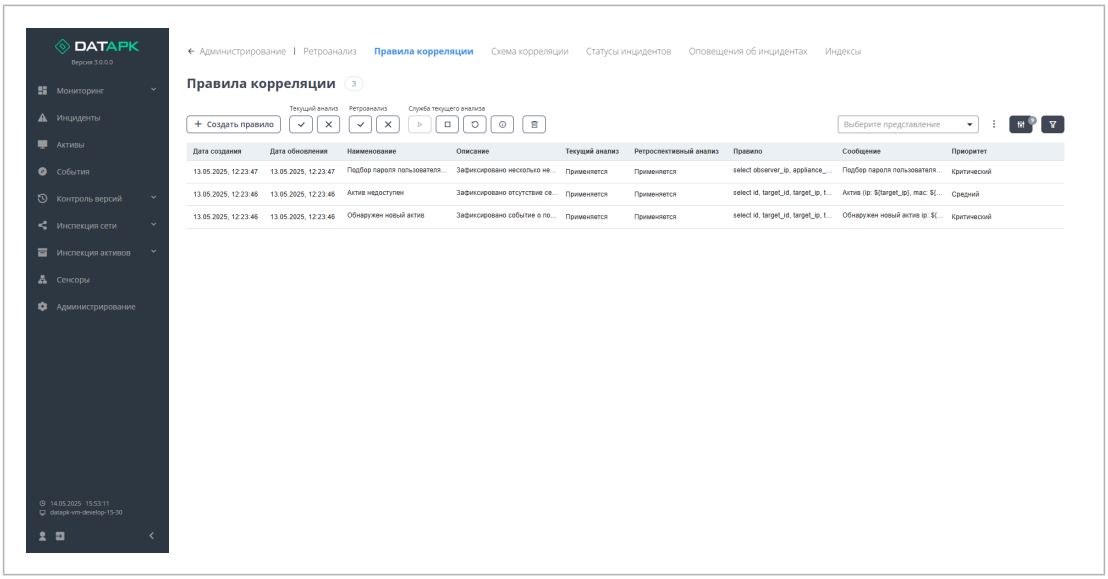


Рис. 524. Страница «Правила корреляции»

См. также

Управление правилами корреляции событий

Управление службой корреляции событий

22.1.2.1.9.3.3. Схема корреляции

Подраздел настроек инцидентов, в котором можно создавать, редактировать, проверять, ассоциировать с тем или иным видом анализа, удалять элементы схемы корреляции.

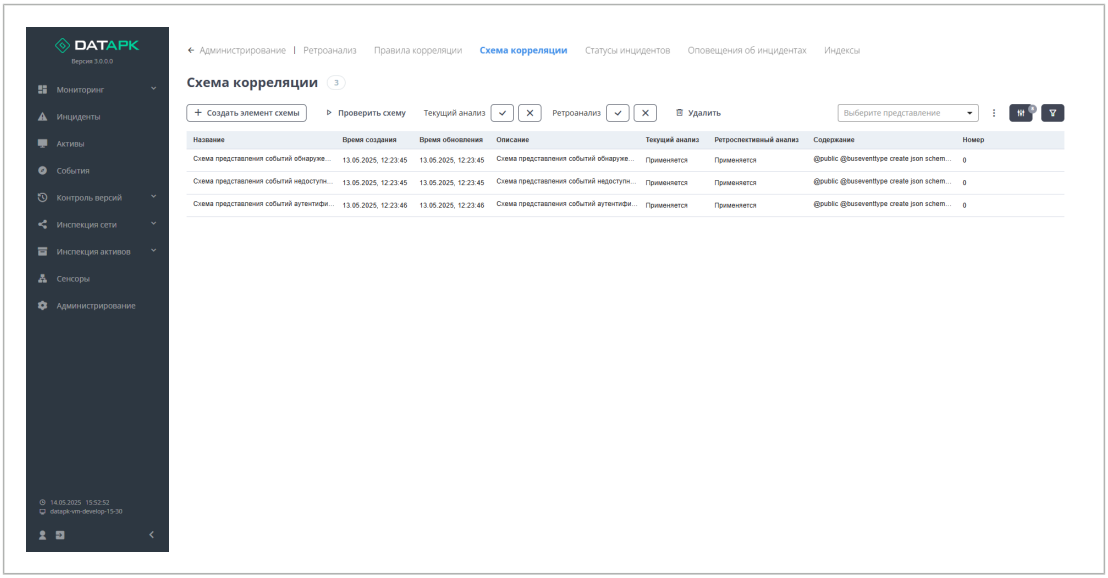


Рис. 525. Страница «Схема корреляции»

См. также

Анализ событий для генерации инцидентов

Управление схемой корреляции

22.1.2.1.9.3.4. Статусы инцидентов

Подраздел настроек инцидентов, содержащий доступные для редактирования статусы, которые оператор может присвоить инцидентам. Доступна сортировка, редактирование и удаление (в т. ч. групповое).

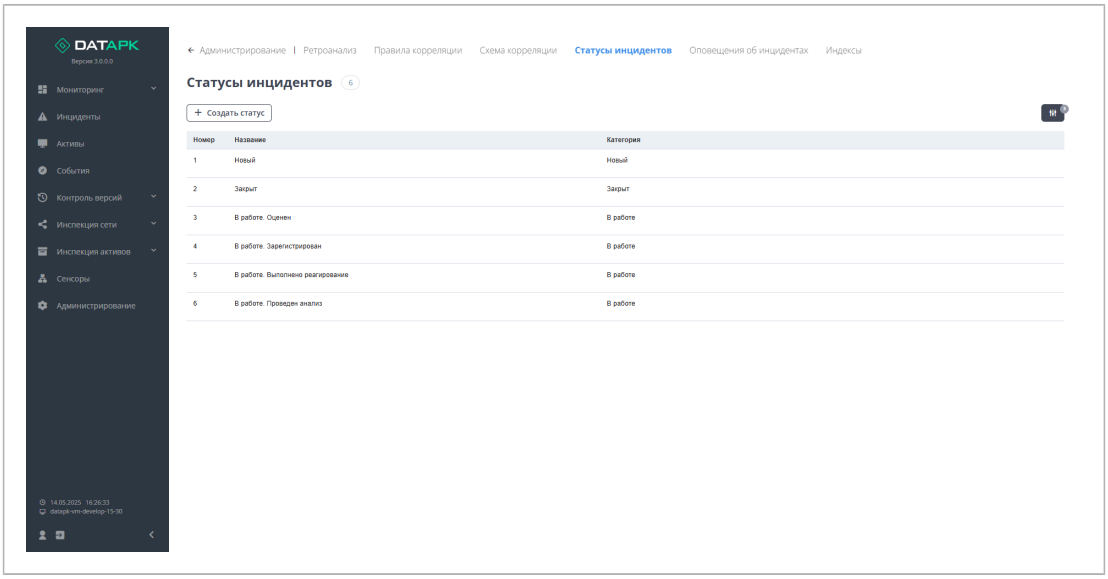


Рис. 526. Страница «Статусы инцидентов»

См. также

Управление статусами инцидентов

22.1.2.1.9.3.5. Оповещения об инцидентах

Подраздел настроек инцидентов, в котором можно создавать, редактировать, удалять оповещения об инцидентах.

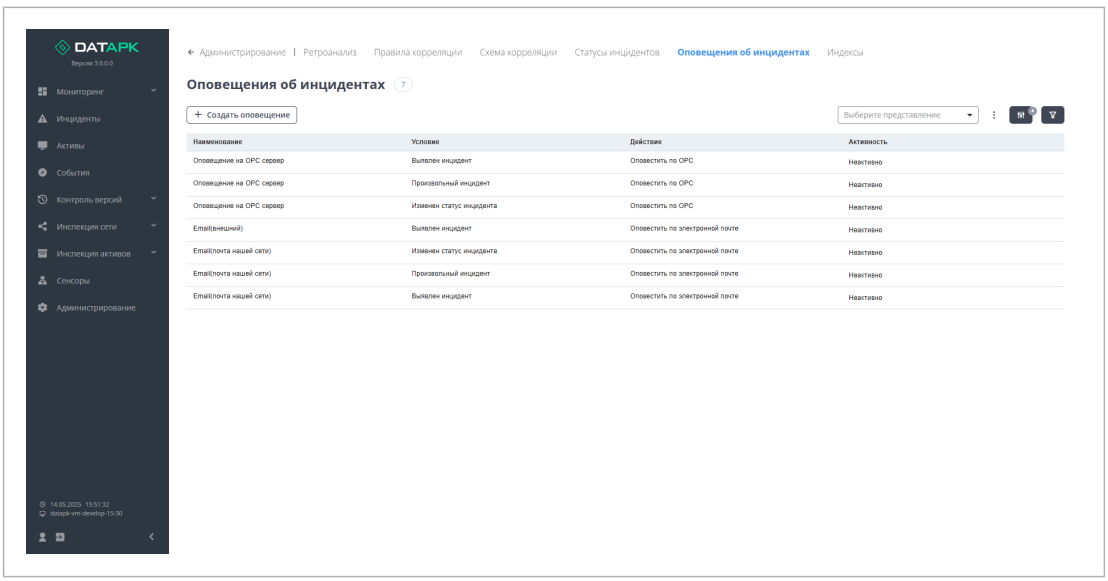


Рис. 527. Страница «Оповещения об инцидентах»

См. также

Настройка оповещений при появлении инцидентов

22.1.2.1.9.3.6. Индексы

Подраздел настроек мониторинга, в котором можно восстанавливать, архивировать и удалять индексы событий.

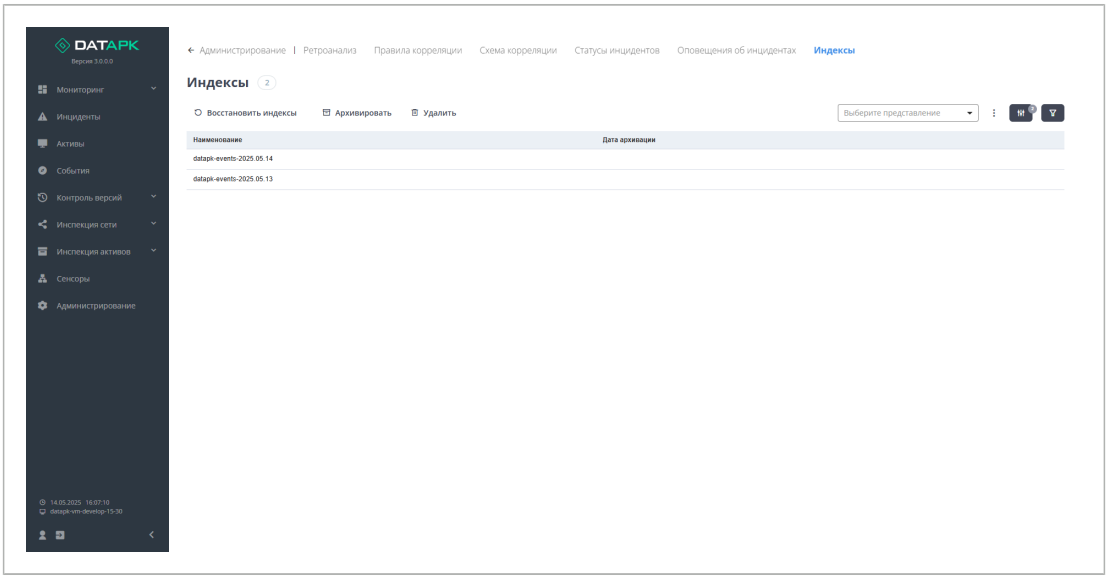


Рис. 528. Страница «Индексы»

См. также

Выгрузка внешних событий Комплекса в архив

22.1.2.1.9.4. Пользователи

Пункт меню подраздела Пользователи, содержащий страницу Парольная политика.

См. также

Парольная политика

22.1.2.1.9.4.1. Пользователи

Подраздел управления Комплексом, где можно создавать, редактировать, блокировать и разблокировать, удалять пользователей.

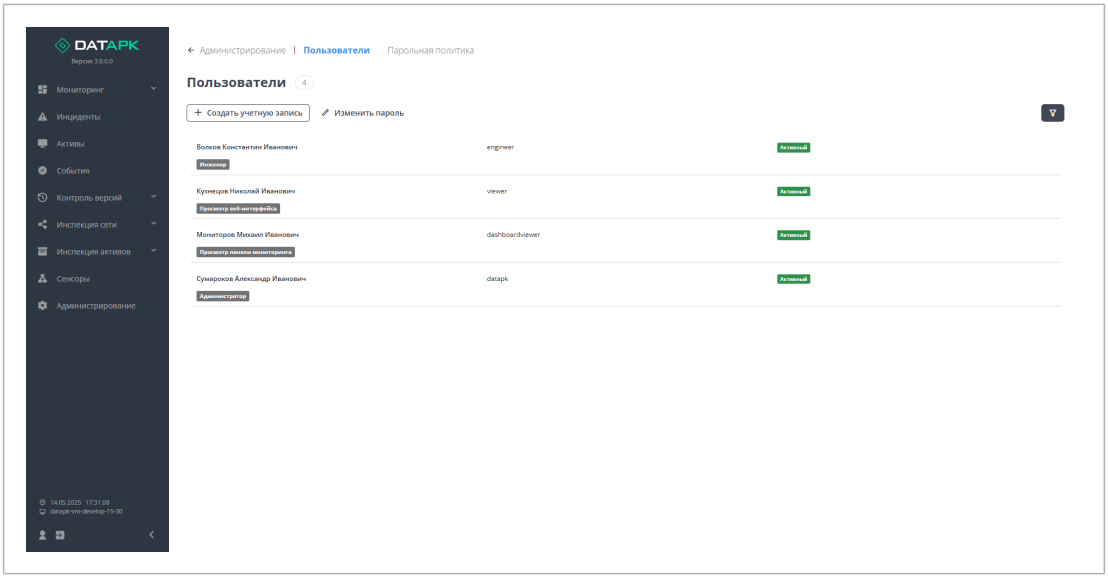


Рис. 529. Страница «Пользователи»

См. также

Создание локальной учетной записи

Редактирование учетных записей пользователей

22.1.2.1.9.4.2. Парольная политика

Подраздел настроек пользователей, где можно настраивать требования к паролям в Комплексе.

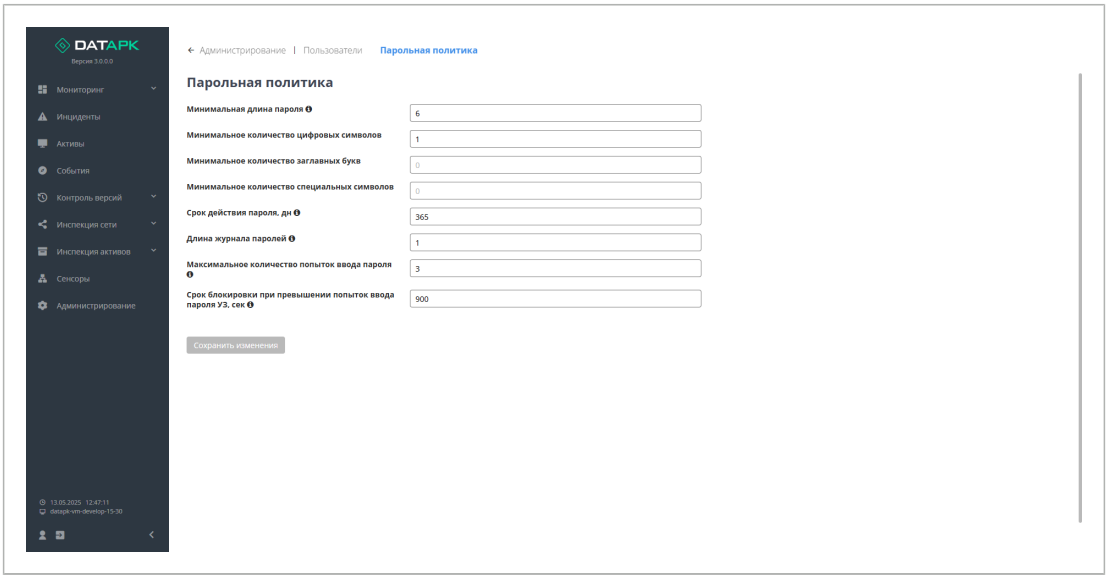


Рис. 530. Страница «Парольная политика»

См. также

Настройка парольной политики

22.1.2.1.9.5. Сигнатурный анализ

22.1.2.1.9.5.1. Правила обнаружения

Страница для работы с правилами обнаружения вторжений, содержащая следующие вкладки:

- Правила;
- Исключения.

См. также

Служба обнаружения вторжений

22.1.2.1.9.5.1.1. Правила

Подраздел инспекции сети, в котором можно управлять службой обнаружения вторжений, создавать, редактировать, активировать и деактивировать правила обнаружения вторжений.

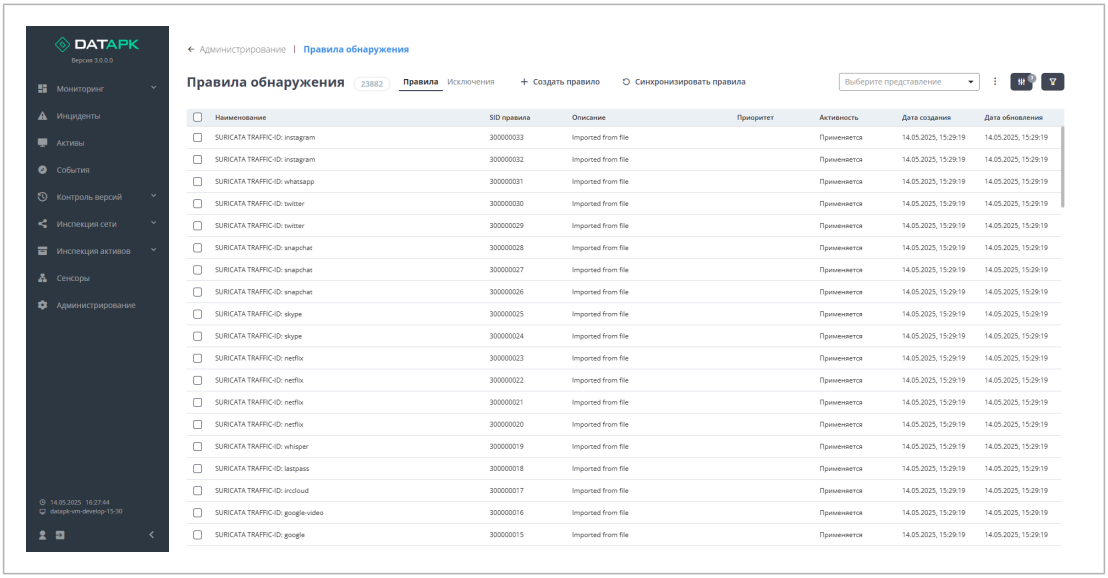


Рис. 531. Вкладка «Правила» на странице «Правила обнаружения»

См. также

Служба обнаружения вторжений

22.1.2.1.9.5.1.2. Исключения

Подраздел инспекции сети, в котором можно создавать, редактировать и удалять исключения для правил обнаружения вторжений.

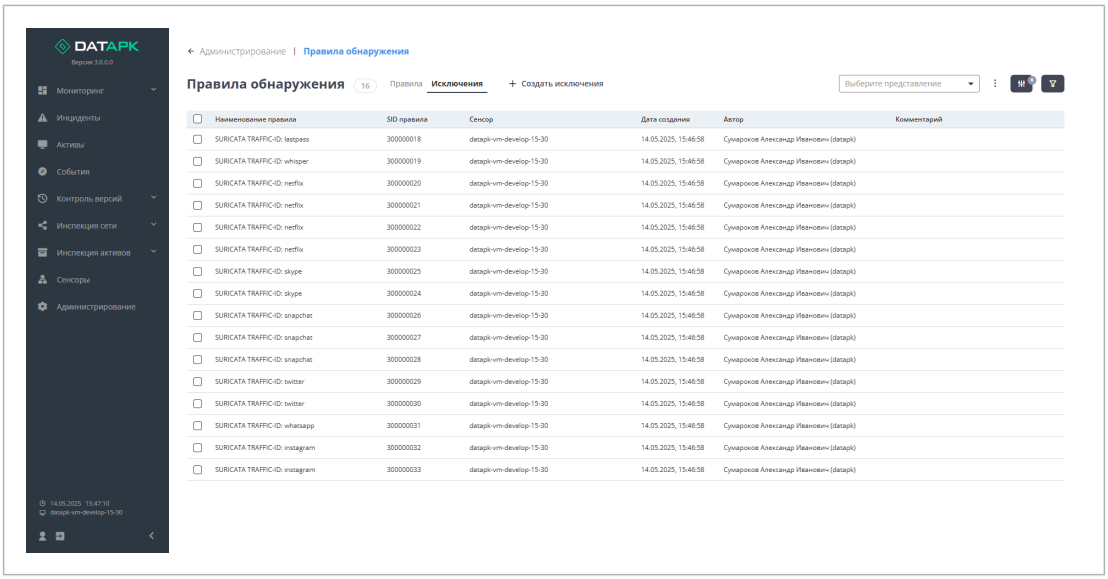


Рис. 532. Вкладка «Исключения» на странице «Правила обнаружения»

См. также

Служба обнаружения вторжений

22.1.2.1.9.6. Настройка активов

Пункт меню раздела Администрирование, содержащий страницы Классификаторы, Учетные данные и Источники.

См. также

Классификаторы

Учетные данные

Источники

22.1.2.1.9.6.1. Учетные данные

Подраздел настроек активов, где можно просмотреть, добавить, отредактировать учетные данные для сбора событий и конфигураций с активов. Пароль просмотреть нельзя.

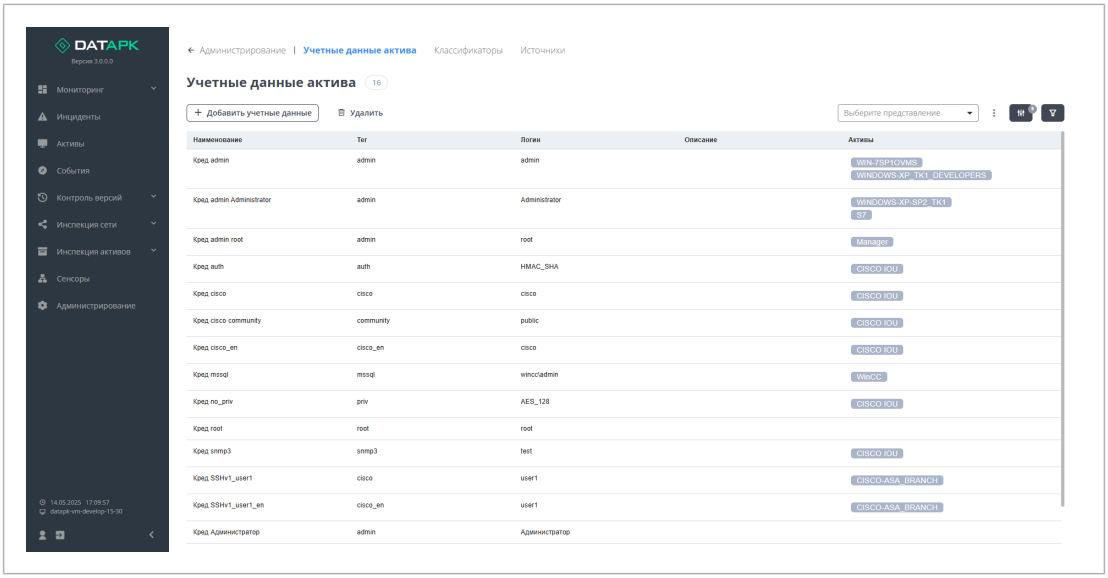


Рис. 533. Страница «Учетные данные актива»

См. также

Настройка учетных данных активов

22.1.2.1.9.6.2. Классификаторы

Подраздел настроек активов, где можно создавать, редактировать и удалять классификаторы типов **Метки** и **АСУ ТП**.

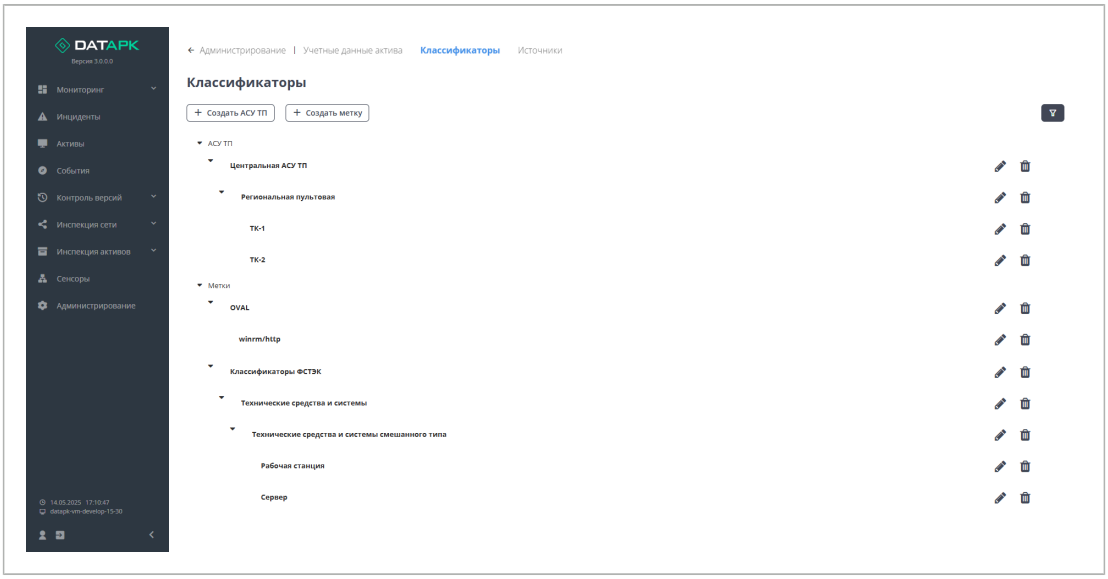


Рис. 534. Страница «Классификаторы»

См. также

Создание классификатора АСУ ТП

Создание метки

Редактирование и удаление классификаторов

22.1.2.1.9.6.3. Источники

Подраздел настроек активов, в котором можно создавать и редактировать источники событий, а также запускать и останавливать прием данных от них.

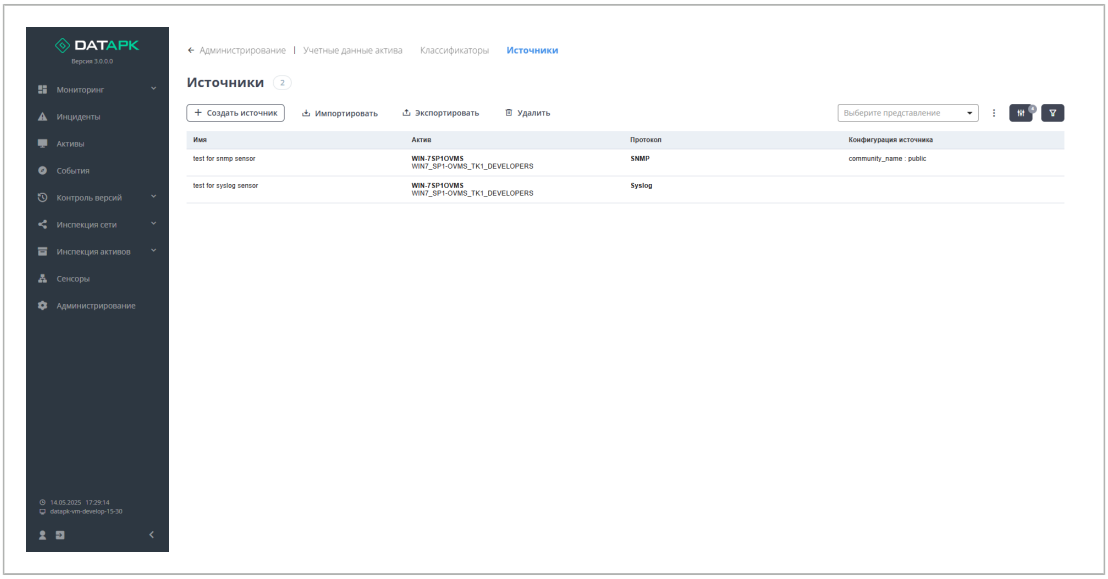


Рис. 535. Страница «Источники»

См. также

Создание источника событий

Управление источниками событий

22.1.2.1.10. Страница «Страница не найдена»

Страница, которая автоматически открывается при переходе по ссылке на несуществующую страницу веб-интерфейса Комплекса. Страница также содержит ссылку для перехода на страницу **Статус защищенности**.

Рис. 536. Страница «Страница не найдена»

См. также

Статус защищенности

22.1.2.1.11. Разделы интерфейса Supervision

Интерфейс Супервижна состоит из следующих разделов:

- Мониторинг:
  - Обзор;
  - Контроль версий;
- Контроль версий:
  - Репозитории;
- Администрирование:
  - Пользователи:
    - Пользователи;
    - Парольная политика;
  - Менеджменты:
    - Менеджменты;
- Страница «Страница не найдена»;
- Страница «Изменение пароля».

22.1.2.1.11.1. Мониторинг

Пункт главного меню, содержащий страницы **Обзор** и **Контроль версий** для мониторинга состояния Менеджментов и их активов.

22.1.2.1.11.1.1. Обзор

Подраздел раздела **Мониторинг**, в котором представлены виджеты с основной статистикой по работе системы.

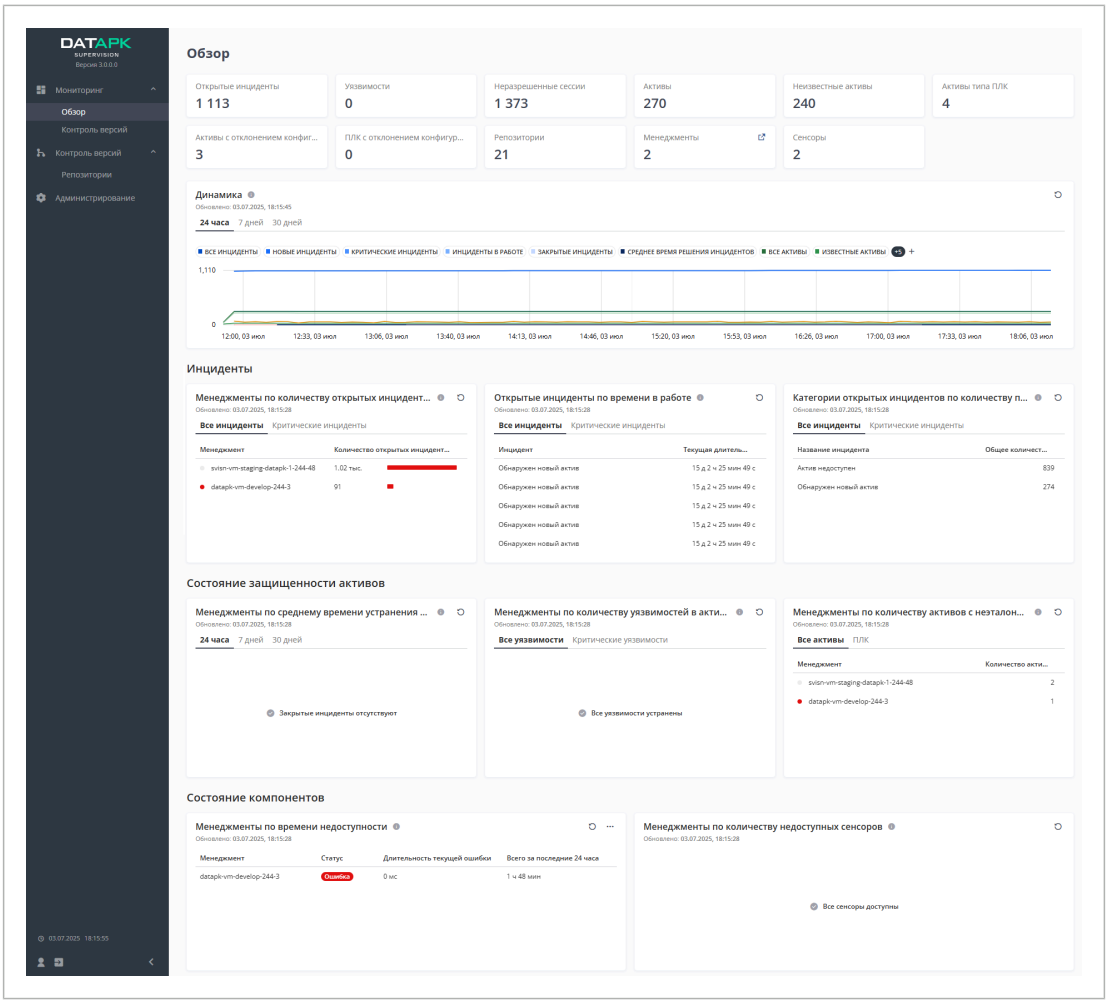


Рис. 537. Страница «Обзор»

См. также

Просмотр панели виджетов «Обзор»

22.1.2.1.11.1.2. Контроль версий

Подраздел раздела **Мониторинг**, в котором представлены виджеты для отслеживания следующих показателей состояния активов с типом `ПЛК`:

- статус подключения ПЛК к репозиториям;
- актуальность конфигураций ПЛК;
- соответствие конфигураций ПЛК эталону;
- количество и причины изменений, вносимых в репозитории проектов ПЛК.

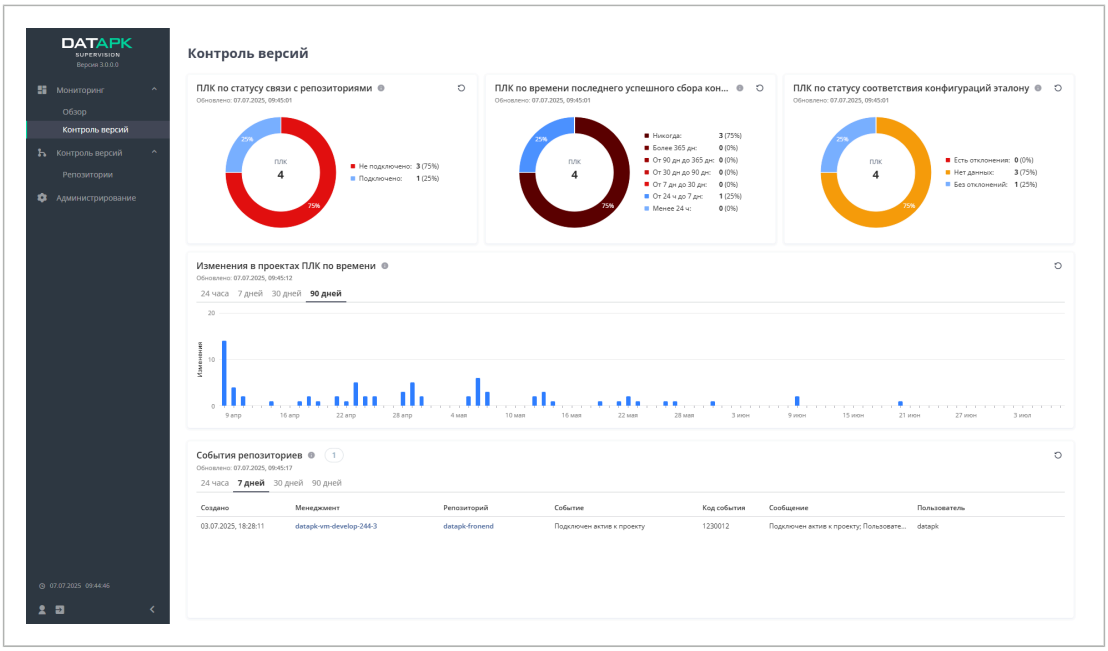


Рис. 538. Страница «Контроль версий»

См. также

Контроль версий

22.1.2.1.11.2. Контроль версий

Раздел главного меню, который содержит страницу **Репозитории** для просмотра подключенных репозиториев.

22.1.2.1.11.2.1. Репозитории

Подраздел раздела **Контроль версий**, где можно просматривать подключенные репозитории, хранимые в репозиториях файлы и их версии.

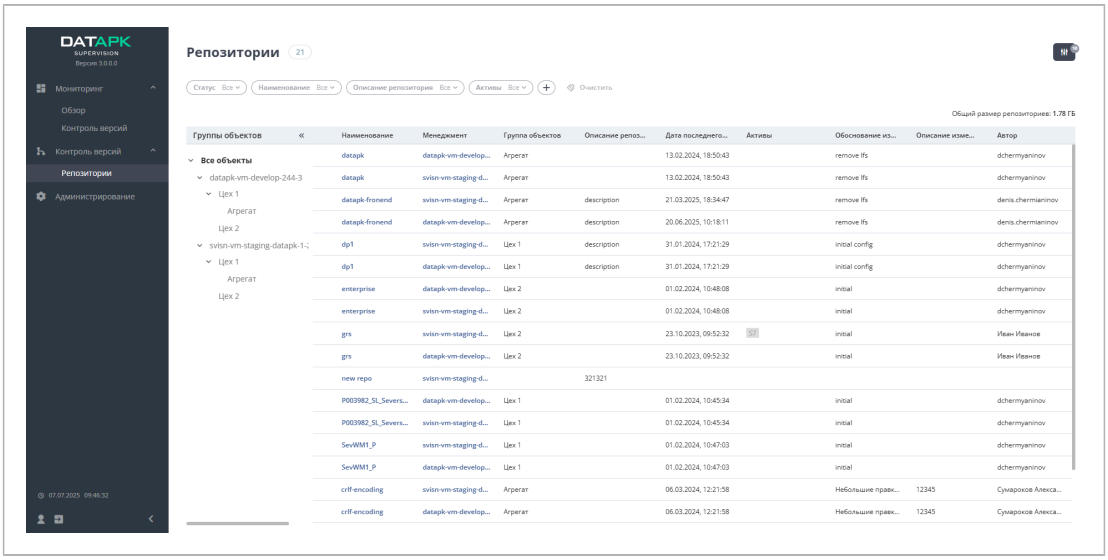


Рис. 539. Страница «Репозитории»

См. также

Управление проектами ПЛК

22.1.2.1.11.3. Администрирование

Раздел главного меню, который содержит группы настроек различных аспектов работы Supervision:

- **Пользователи**
- **Менеджменты**

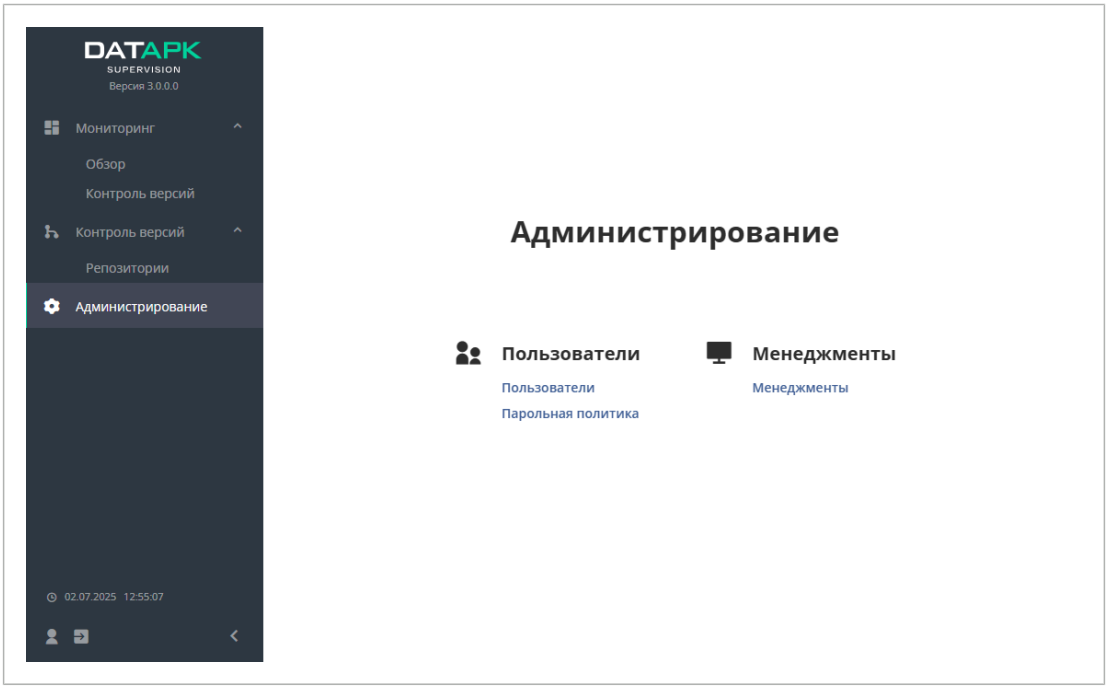


Рис. 540. Страница «Администрирование»

22.1.2.1.11.3.1. Пользователи

Пункт меню раздела **Администрирование**, содержащий страницы:

- **Пользователи**
- **Парольная политика**

См. также

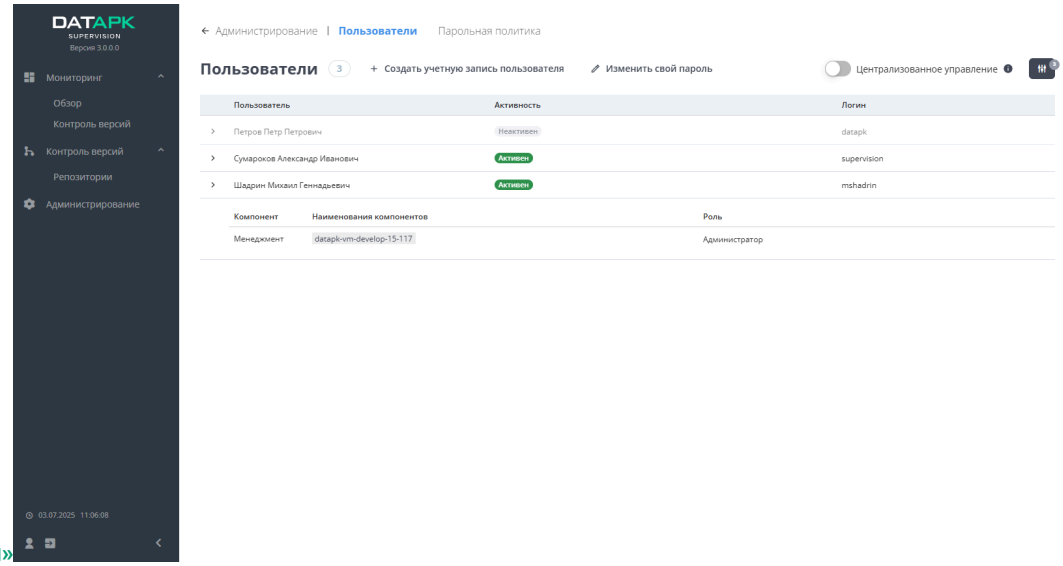
Пользователи

Парольная политика

22.1.2.1.11.3.1.1. Пользователи

Подраздел раздела **Администрирование**, где можно создавать, редактировать, блокировать и разблокировать, удалять пользователей.

Рис. 541.Страница «Пользователи»



См. также

Управление учетными записями пользователей

22.1.2.1.11.3.1.2. Парольная политика

Подраздел раздела **Администрирование**, где можно настраивать требования к паролям в Супервижн.

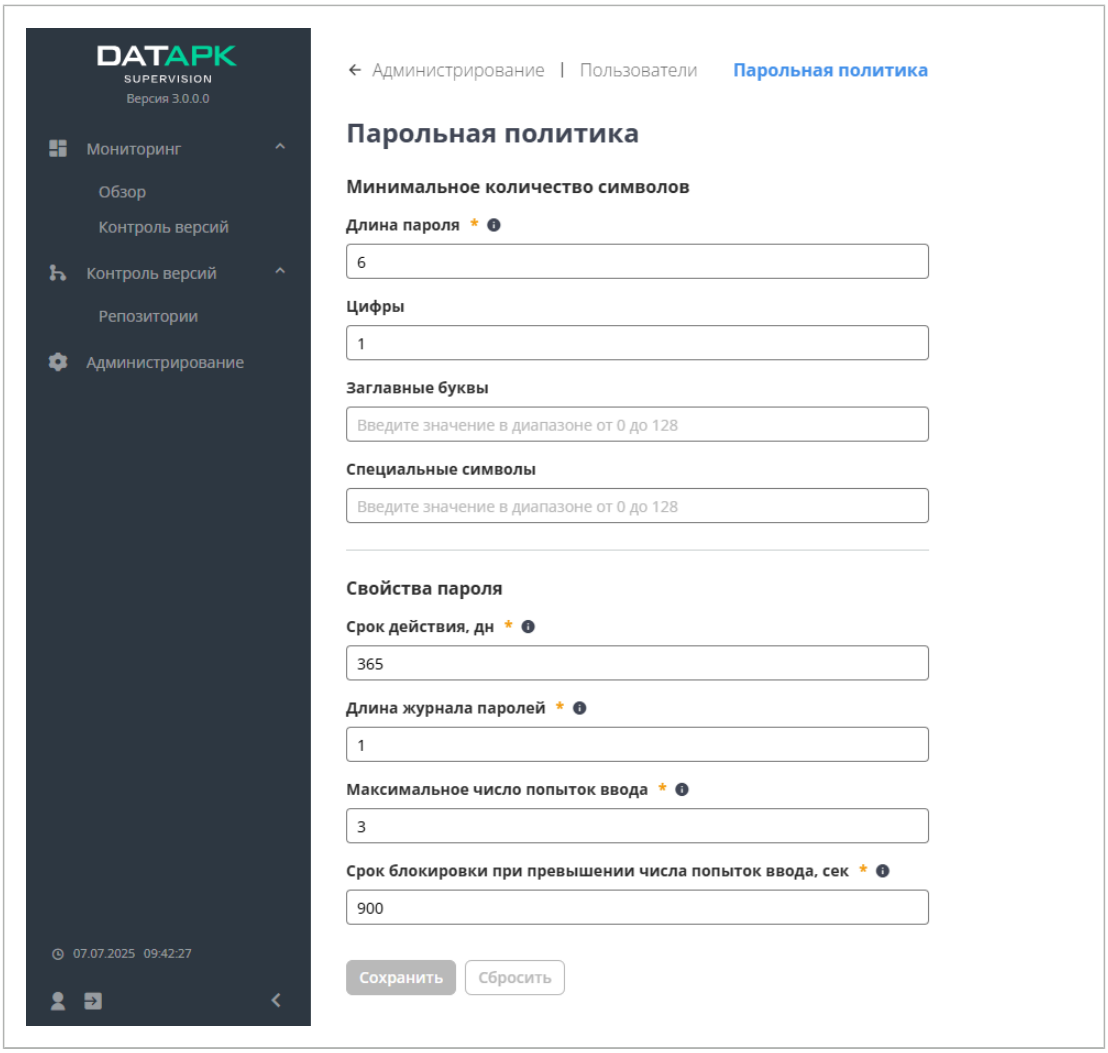


Рис. 542. Страница «Парольная политика»

См. также

Управление парольной политикой

22.1.2.1.11.3.2. Менеджменты

Пункт меню раздела **Администрирование**, содержащий страницу **Менеджменты**.

22.1.2.1.11.3.2.1. Менеджменты

Подраздел раздела **Администрирование**, где можно управлять и отслеживать подключение Менеджментов.

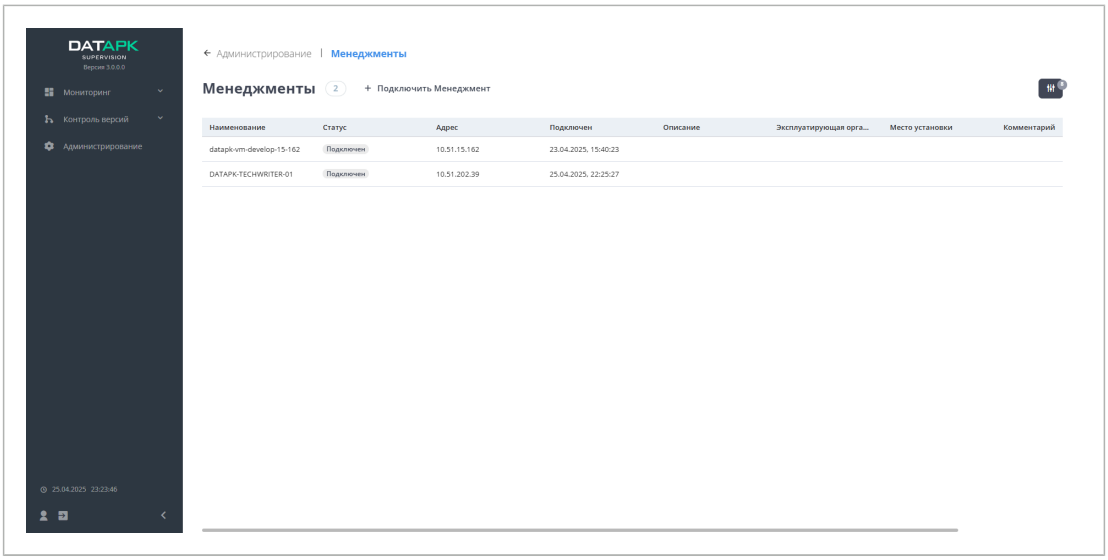


Рис. 543. Страница «Менеджменты»

См. также

Управление компонентами Management

22.1.2.1.11.4. Страница «Страница не найдена»

Страница, которая открывается, если срок действия пароля пользователя истек или если при создании или редактировании пользователя был активирован чекбокс **Изменить пароль при следующем входе**.

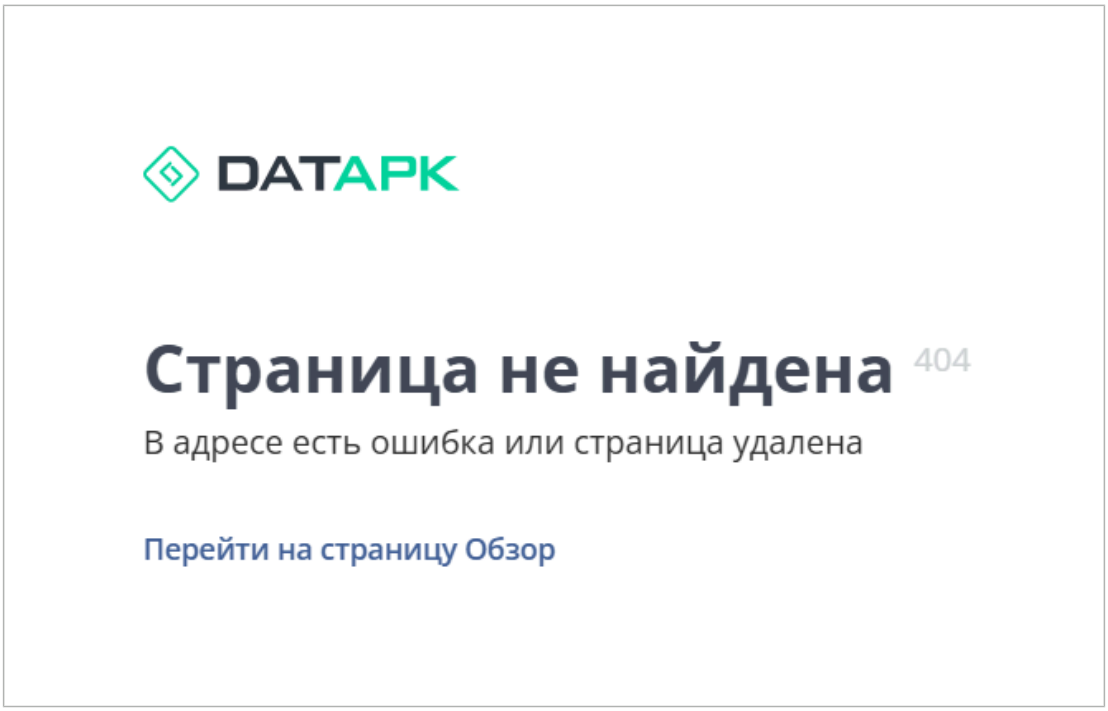


Рис. 544. Страница «Изменение пароля»

22.1.2.1.11.5. Страница «Изменение пароля»

Страница, которая открывается, если срок действия пароля пользователя истек или если при создании либо редактировании пользователя был активирован чекбокс **Изменить пароль при следующем входе**.

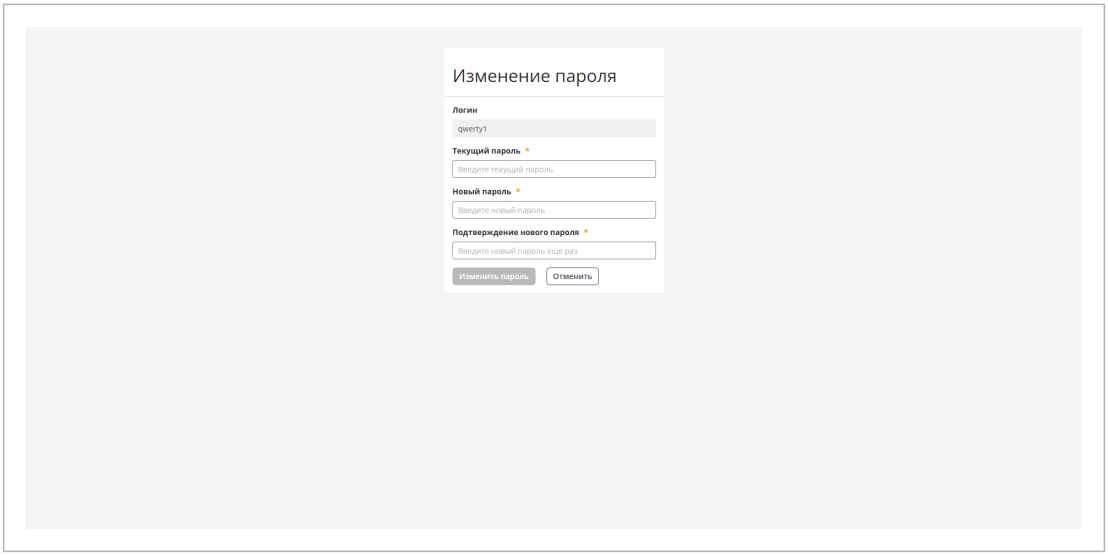


Рис. 545. Страница «Изменение пароля»

22.1.2.2. Управляющие элементы

В таблице ниже (Таблица 127. Управляющие элементы Комплекса) описаны управляющие элементы — кнопки и иконки, доступные в основном интерфейсе Комплекса.

Табл. 127. Управляющие элементы Комплекса

УПР. ЭЛ-Т	ОПИСАНИЕ	
	Отфильтровать содержимое страницы	Базовый модуль (Core)
	Развернуть	Управление конфигурациями
	Свернуть. Отображается, когда элемент развернут	
	Управление масштабом карт: **+** Увеличить масштаб **–** Уменьшить масштаб	Анализ промышленного сетевого трафика
	Установить масштаб 100%	
	Расположить узлы на карте на сетке	

Табл. 127. Управляющие элементы Комплекса

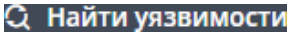
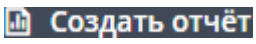
УПР. ЭЛ-Т	ОПИСАНИЕ	
	Расположить узлы на карте по кругу	
	Выполнить визуальную сортировку узлов по количеству соединений	
	Запустить сканер	Управление конфигурациями
	Запустить сбор событий от источника	Управление внешними событиями
	Приостановить сбор событий от источника	
	Запустить службу	Управление внешними событиями
	Остановить службу	
	Перезапустить службу	
	Перейти к событиям службы	
	Экспортировать справочники	Базовый модуль (Core)
	Экспортировать источники	Управление внешними событиями
	Исключить из группы OVAL-определений	Управление уязвимостями
	Импортировать справочники	Базовый модуль (Core)
	Импортировать источники	Управление внешними событиями
	Добавить в группу OVAL-определений	Управление уязвимостями
	Запустить поиск уязвимостей на выбранных активах	Управление уязвимостями
	Сформировать отчет по выбранным активам	Базовый модуль (Core)

Табл. 127. Управляющие элементы Комплекса

УПР. ЭЛ-Т	ОПИСАНИЕ	
	Импортировать активы	
	Экспортировать активы	
	Перейти к конфигурациям актива	Управление конфигурациями
	Перейти к конфигурациям выбранных активов	Управление конфигурациями
События	Перейти к событиям актива	Базовый модуль (Core)
	Перейти к событиям выбранных активов	Базовый модуль (Core)
Инциденты	Перейти к инцидентам актива	Базовый модуль (Core)
Инциденты	Перейти к инцидентам выбранных активов	Базовый модуль (Core)
Источники	Перейти к источникам актива	Управление внешними событиями
	Перейти к источникам выбранных активов	Управление внешними событиями
Учетные данные актива	Перейти к учетным данным актива	Управление конфигурациями
	Перейти к учетным данным выбранных активов	Управление конфигурациями
Перечень ПО	Перейти к перечню ПО актива	Управление конфигурациями
	Перейти к перечню ПО выбранных активов	Управление конфигурациями
Карта сети	Показать сессии актива на карте сети	Анализ промышленного сетевого трафика
Карта сети	Показать сессии выбранных активов на карте сети	Анализ промышленного сетевого трафика
	Показать задачи сбора данных актива	Управление конфигурациями

Табл. 127. Управляющие элементы Комплекса

УПР. ЭЛ-Т	ОПИСАНИЕ		
Задачи сбора данных	Показать задачи сбора данных выбранных активов		Управление конфигурациями
Статус сбора данных	Показать статус сбора данных актива		Управление конфигурациями
	Показать статус сбора данных выбранных активов		Управление конфигурациями
	Отвязать сетевые атрибуты от актива		Базовый модуль (Core)
	Сохранить изменения сетевых атрибутов актива		Базовый модуль (Core)
	Автоматизированное рабочее место (АРМ)	Внимание: Активы могут иметь также цветовую индикацию и специальные символы — подробнее см. раздел «Цветовая индикация и виды уведомлений».	Базовый модуль (Core), Анализ промышлен
	Коммутатор		
	Маршрутизатор		
	Неизвестный тип		
	Сервер		
	Периферийное оборудование		

Табл. 127. Управляющие элементы Комплекса

УПР. ЭЛ-Т	ОПИСАНИЕ	
	Программируемый логический контроллер (ПЛК)	
	Средство защиты	
	Сенсор	
	Комплекс	
	Глобальная или локальная сеть	Анализ промышленного сетевого трафика
	Удалить элемент	Базовый модуль (Core)
	Удалить группу элементов	Базовый модуль (Core)
	Недоступная для использования кнопка группового удаления. Можно увидеть, когда нет элементов для удаления, либо они недоступны	Базовый модуль (Core)
	Редактировать элемент	Базовый модуль (Core)
	Редактировать группу элементов	Базовый модуль (Core)
	Настроить список столбцов таблицы	Базовый модуль (Core)
	Сформировать отчет по содержимому страницы	Базовый модуль (Core)

Табл. 127. Управляющие элементы Комплекса

УПР. ЭЛ-Т	ОПИСАНИЕ	
	Отменить изменения сетевых атрибутов актива	Базовый модуль (Core)
	Добавить email-адрес получателя	Базовый модуль (Core)
	Удалить email-дрес получателя	Базовый модуль (Core)
	Архивировать группу индексов событий	Управление внешними событиями
	Архивировать индекс событий	
	Восстановить индексы из архива	
	Добавить все определения для добавления в группу	Управление уязвимостями
	Исключить все определения из выбора для добавления в группу	Управление уязвимостями
	Показать еще 5 строк	Управление конфгурациями
	Выбрать определение для добавления в группу	Управление уязвимостями
	Скрыть 5 строк	Управление конфигурациями
	Исключить определение из выбора	Управление уязвимостями
	Посмотреть результаты	Управление уязвимостями
	Перезапустить проверку	
	Отменить проверку	
	Сохранить результаты в файл	

Табл. 127. Управляющие элементы Комплекса

УПР. ЭЛ-Т	ОПИСАНИЕ	
	Удалить сеть	Базовый модуль (Core)
	Служба обнаружения вторжений включена (выключить службу)	Анализ промышленного сетевого трафика
	Служба обнаружения вторжений выключена (включить службу)	Анализ промышленного сетевого трафика
	Не применять все выбранные в фильтре элементы	Управление внешними событиями
	Применить все выбранные в фильтре элементы	Управление внешними событиями
	Повысить порядок статуса инцидентов	Базовый модуль (Core)
	Понизить порядок статуса инцидентов	Базовый модуль (Core)
	Просмотреть информацию об элементе (при наведении)	Базовый модуль (Core)
	Просмотреть информацию об элементе (кнопка)	Базовый модуль (Core)
	Копировать задачу	Управление конфигурациями

22.1.2.3. Элементы управления таблицами

В интерфейсе Комплекса большинство страниц имеют табличное представление. Возможности управления отображением содержимого таблиц:

- регулирование ширины столбцов таблицы;
- выбор списка столбцов для отображения;
- изменение порядка столбцов для отображения;
- просмотр текста, который не помещается в ячейку;
- просмотр списка элементов, который не помещается в ячейку;
- сортировка по столбцам таблицы;
- множественный выбор элементов.

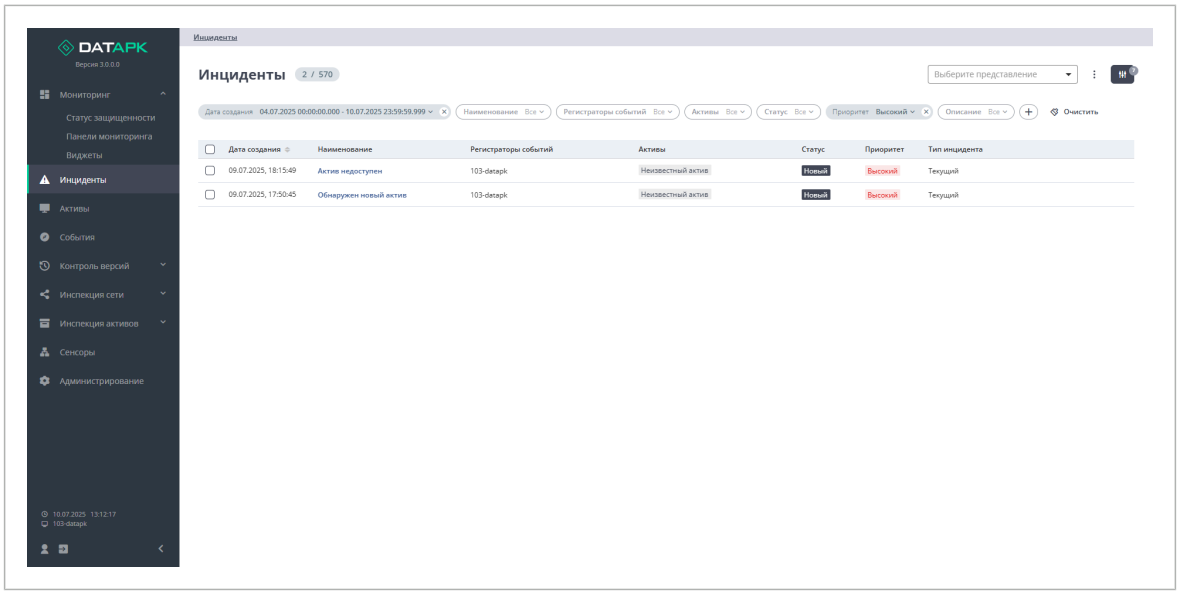


Рис. 546. Табличное представление данных на странице «Инциденты»

Регулирование ширины столбцов таблицы

Для регулирования ширины столбцов:

1. Наведите курсор мыши на правую границу заголовка столбца, ширину которого нужно изменить. Курсор изменит свой вид.
2. Зажмите левую клавишу мыши и потяните:
    - вправо — для расширения столбца;
    - влево — для сужения столбца.
3. Отпустите левую клавишу мыши. Столбец таблицы изменит свою ширину.

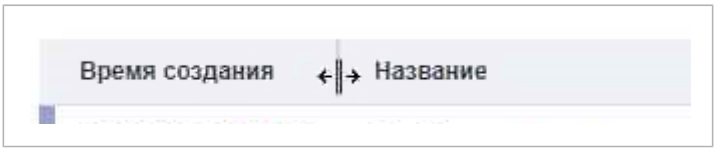


Рис. 547. Вид курсора при изменении ширины столбца

Выбор списка столбцов для отображения

Для выбора списка отображаемых столбцов:

1. В правой верхней части страницы нажмите кнопку .
2. При помощи чекбоксов выберите интересующие столбцы.

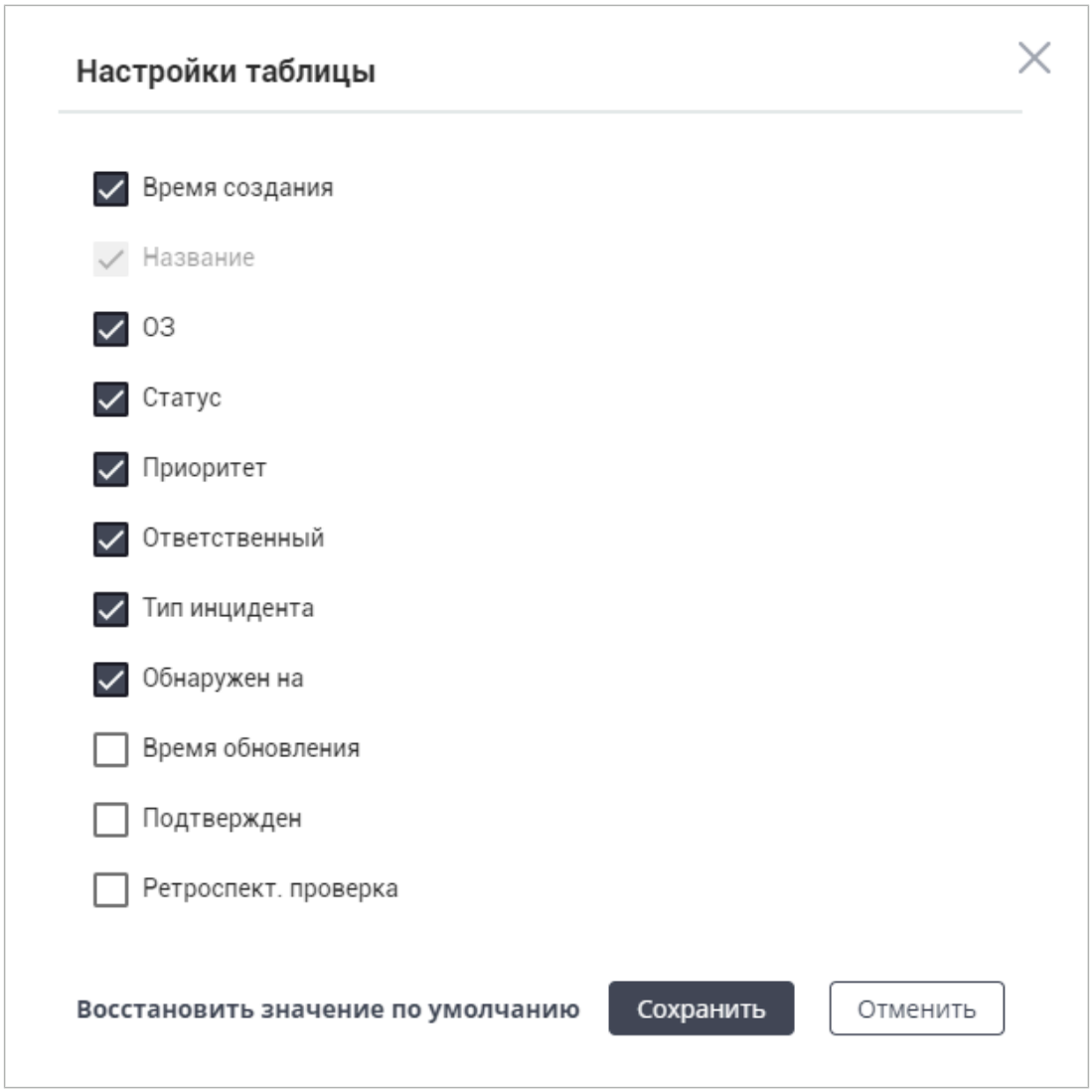


Рис. 548. Окно для выбора столбцов таблицы

> Подсказка:
>
> Серым цветом отмечены столбцы, которые всегда отображаются в таблице.

3. Для возврата к стандартному набору столбцов таблицы нажмите **Восстановить значение по умолчанию**.
4. Для сохранения изменений нажмите кнопку **Сохранить**.

Для скрытия окна кликните любой клавишей мыши в любом месте страницы.

Изменение порядка столбцов для отображения

Для изменения порядка отображаемых столбцов:

1. В правой верхней части страницы нажмите кнопку .
2. Наведите курсор на интересующий столбец и зажмите левую кнопку мыши.
3. Не отпуская левую кнопку мыши, перетащите столбец на новое место в списке.
4. Для возврата к стандартному набору столбцов таблицы нажмите **Восстановить значение по умолчанию**.
5. Для сохранения изменений нажмите кнопку **Сохранить**.

Просмотр текста, который не помещается в ячейку

Для просмотра длинного текста, который не помещается в ячейку целиком, наведите курсор на эту ячейку таблицы. Появится всплывающая подсказка с полным текстом.

Просмотр списка элементов, который не помещается в ячейку

Для просмотра длинного списка элементов, который не помещается в ячейку, нажмите на кнопку **Просмотреть все** внизу ячейки. Появится всплывающее окно с полным списком элементов.

Сортировка по столбцам таблицы

Сортировка по столбцам таблицы

Для сортировки по нарастанию или убыванию нажмите рядом с интересующим столбцом таблицы. При выборе сортировки по нарастанию кнопка имеет вид , а по убыванию —

Множественный выбор элементов

Множественный выбор элементов доступен для таблиц на страницах **Активы**, **Сканеры**, **Определения OVAL**.

- **Выбор нескольких строк**

  Способ 1:

  Установите чекбоксы в выбранных строках.

  Способ 2:

  1. Зажмите клавишу **Ctrl**.
  2. Отметьте выбранные строки, кликнув в любом месте строки.

- **Выбор нескольких строк подряд**

  Для выбора нескольких строк подряд:

  1. Установите чекбокс в первой строке нужного диапазона.
  2. Зажмите клавишу **Shift**.
  3. Установите чекбокс в последней строке нужного диапазона.

  В результате будут выбраны все строки между первой и последней.

- **Выбор всех строк на странице**

  Установите чекбокс в заголовке таблицы — в результате будут установлены чекбоксы во всех строках таблицы.

  Выбор всех строк доступен также на странице **Виджеты**.

- **Отмена выбора всех строк**

  При выборе всех строк на страницах **Сканеры** и **Определения OVAL** появляется кнопка **Отменить выделение**. Нажмите на кнопку, чтобы отменить выбор чекбоксов во всех строках.

  Для отмены выбора всех строк на страницах **Активы**, **Правила сессий** и **Правила обнаружения** отмените выбор чекбокса в заголовке таблицы.

22.1.2.4. Цветовая индикация и виды уведомлений

В этом разделе вы можете ознакомиться со всеми видами цветовых индикаций и уведомлений, которые могут встретиться в веб-интерфейсе Комплекса:

- Цветовая индикация активов
- Статусы активов
- Индикация статусов операций
- Виды уведомлений
- Индикация результатов OVAL-проверок
- Статусы поиска уязвимостей
- Статусы подготовки файлов к экспорту

22.1.2.4.1. Цветовая индикация активов

В интерфейсе Комплекса на страницах **Инспекция сети** → **Карта сети** и **Активы** присутствует специфическая цветовая индикация активов. Ознакомиться с ней вы можете в таблице ниже.

Табл. 128. Индикация активов

ИНДИКАТОР	ОБОЗНАЧЕНИЕ	ОПИСАНИЕ
	Актив отмечен темно-синим	Трафик между устройством и прослушивающими интерфейсами Комплекса присутствует
	Актив отмечен серым	Отсутствует трафик между устройством и прослушивающими интерфейсами Комплекса
	Желтый знак вопроса в нижнем правом углу	Актив неизвестен
	Зеленая галочка в верхнем правом углу	На активе не обнаружено ошибок сбора данных и конфигураций, не соответствующих эталону
	Желтый восклицательный знак в верхнем правом углу	На активе обнаружена одна или несколько следующих ошибок:

Табл. 128. Индикация активов

ИНДИКАТОР	ОБОЗНАЧЕНИЕ	ОПИСАНИЕ
		• неподтвержденное изменение конфигурации (последняя собранная конфигурация не равна эталонной); • обнаружены затруднения при сборе данных некоторыми сканерами — выполнены успешно от 33 до 99% процессов сбора данных
	Красный крестик в верхнем правом углу	Обнаружены затруднения при сборе данных некоторыми сканерами — выполнены успешно от 0 до 33% процессов сбора данных
Индикация активов цветом и спецсимволами не зависят друг от друга		

22.1.2.4.2. Статусы активов

В таблице на странице **Активы** можно просматривать статусы выполненных операций активного сбора данных с активов и статистику по обнаруженным инцидентам и уязвимостям.

Столбцы таблицы можно выбрать и отобразить по кнопке в правом верхнем углу страницы.

Описание статусов приведено в таблице ниже.

Табл. 129. Статусы активов на странице «Активы»

ОБОЗНАЧЕНИЕ	ОПИСАНИЕ	ИНДИКАТОРЫ
Конфигурации	Статус отклонения последней собранной с актива конфигурации от эталона. При наведении на статус отображается количество собранных конфигураций, сгруппированных по статусу их отклонения: • нет отклонений — количество конфигураций актива, соответствующих эталону в данный момент; • есть отклонения — количество конфигураций, не соответствующих эталону в данный момент; • были отклонения — количество конфигураций, которые соответствуют эталону в данный момент, но в их предыдущих версиях были отклонения	• Красный — последняя конфигурация не соответствует эталону. • Оранжевый — последняя конфигурация соответствует эталону, но в ее предыдущих версиях были отклонения. • Зеленый — последняя конфигурация соответствует эталону. • Серый — сбор конфигураций не выполнялся
Сбор данных	Процент успешно выполненных процессов сбора данных на активе. При наведении на статус отображается количество выполненных попыток сбора данных с активов по категориям: • количество процессов, выполненных успешно; • количество процессов, которые не удалось выполнить из-за ошибок соединения; • количество процессов, которые не удалось выполнить из-за ошибок сбора. Подробнее см. раздел «Просмотр статуса сбора данных»	• (красный) — 0-33% процессов сбора данных выполнены успешно. • (оранжевый) — 33-99% процессов сбора данных выполнены успешно. • (зеленый) — 100% процессов сбора данных выполнены успешно. • (серый) — сбор данных не выполнялся.

Табл. 129. Статусы активов на странице «Активы»

ОБОЗНАЧЕНИЕ	ОПИСАНИЕ	ИНДИКАТОРЫ
Инциденты	Наивысший приоритет среди обнаруженных инцидентов с категорией Новый на активе. При наведении на статус отображается количество обнаруженных инцидентов, сгруппированных по приоритету	• Критический • Высокий • Средний • Низкий • пусто — инциденты с категорией Новый не обнаружены, либо поиск не выполнялся
Уязвимости	Наивысший приоритет среди уязвимостей из базы CVE, обнаруженных на активе. При наведении на статус отображается количество обнаруженных уязвимостей, сгруппированных по приоритету. По нажатию на статус откроется окно просмотра уязвимостей выбранного актива	• Критический • Высокий • Средний • Низкий • пусто — уязвимости не обнаружены, либо поиск не выполнялся
Результаты сканирования	Статус процессов всех задач сбора данных актива. При наведении на статус отображается количество выполненных процессов сбора данных с активов по трем категориям: • назначено — общее количество процессов сбора данных, выполненных на активе; • количество процессов, которые не удалось выполнить из-за ошибок соединения; • количество процессов, которые не удалось выполнить из-за ошибок сбора.	• 167/1/156 (красный) — присутствуют ошибки сбора. Отображается количество всех результатов по категориям. • 97/43/0 (оранжевый) — присутствуют ошибки соединения, ошибок сбора нет. Отображается количество всех результатов по категориям. • 79 (черный) — успешный сбор всех конфигураций или событий. Отображается только количество назначенных процессов. • Пусто — сбор конфигураций или событий не выполнялся. Подробнее см. раздел «Просмотр статуса сбора данных»

Табл. 129. Статусы активов на странице «Активы»

ОБОЗНАЧЕНИЕ	ОПИСАНИЕ	ИНДИКАТОРЫ
	При нажатии на статус открывается страница **Задачи сбора** с результатами сбора для выбранного актива	

Статусы можно сортировать в порядке критичности. Порядок критичности по убыванию: темно-красный, красный, оранжевый, зеленый, серый/нет данных.

Внимание:

Статусы **Сбор данных** и **Конфигурации** формируют единый показатель актива **Статус проблемности**, по которому можно фильтровать список активов. Проблемность для каждого актива принимает одно из следующих значений:

- **Критический**: хотя бы один из статусов актива — **Сбор данных** или **Конфигурации** — имеет красный индикатор.
- **Важный**: хотя бы один из статусов актива — **Сбор данных** или **Конфигурации** — имеет оранжевый индикатор, но красные индикаторы отсутствуют.
- **ОК**: оба статуса имеют зеленый индикатор.
- **Нет данных**: сбор данных не выполнялся.

Подробнее см. раздел «Фильтрация списка активов».

22.1.2.4.3. Индикация статусов операций

В веб-интерфейсе присутствует индикация статусов выполнения длительных операций (например, группового удаления или изменения объектов). Ознакомиться с видами индикации статусов вы можете в таблице ниже.

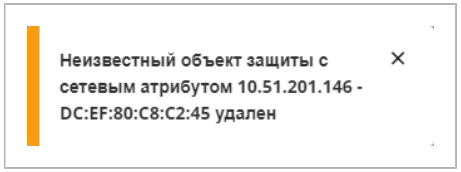
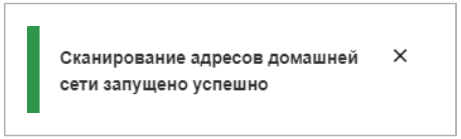
Табл. 130. Индикаторы статусов операций в интерфейсе Комплекса

ИН-ДИКАТОР	ЦВЕТ	ОПИСАНИЕ	СТРАНИЦА ИНТЕРФЕЙСА
Ошибка обработки	Красный	Операция не была завершена вследствие ошибки. При нажатии на «▼» можно посмотреть детали	**Карточка актива**
Ошибка соединения	Оранжевый	Операция была инициирована пользователем, ожидает в очереди на выполнение	**Карточка актива**
Успешно завершено		Операция была запущена и выполняется в данный момент	**Карточка актива**
Предупреждение	Оранжевый	Операция не была завершена вследствие превышения времени ожидания	**Карточка актива**

22.1.2.4.4. Виды уведомлений

В результате действий в интерфейсе Комплекса пользователь может увидеть также всплывающие уведомления в правом верхнем углу. С их основными видами вы можете ознакомиться в таблице ниже.

Табл. 131. Виды уведомлений в интерфейсе Комплекса

ПРИМЕР УВЕДОМЛЕНИЯ	ЦВЕТ	ОПИСАНИЕ
	Оранжевый	Предупреждения. Уведомляет пользователя о специфике работы выбранной операции и ее последствиях.
	Зеленый	Уведомляет пользователя об успешном начале потенциально длительной операции.
	Красный	Ошибки. Уведомляет пользователя о проблемах при выполнении операции.

22.1.2.4.5. Индикация результатов OVAL-проверок

Результаты OVAL-проверок актива на уязвимости или соответствие требованиям информационной безопасности имеют цветовую индикацию на странице **Инспекция активов** → **Результаты проверок** веб-интерфейса.

Если проверка выполнена успешно и для актива не было обнаружено несоответствие по любому из критериев оценки соответствия (тип проверки: `COMPLIANCE`) либо ни одна из уязвимостей не была обнаружена (тип проверки: `VULNERABILITY`), в таблице результатов в строке **Статус** появится надпись `Завершена`, и строка таблицы будет выделена зеленым цветом.

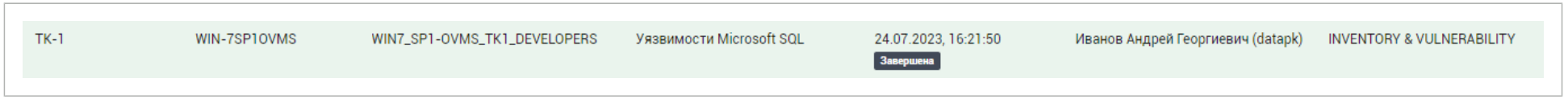


Рис. 549. Результат успешной проверки на соответствие требованиям ИБ **в случае выполнения всех критериев оценки**

Если проверка выполнена, но для актива обнаружено несоответствие хотя бы по одному из критериев оценки (тип проверки: `COMPLIANCE`) либо была обнаружена хотя бы одна из уязвимостей (тип проверки: `VULNERABILITY`), в таблице результатов в строке **Статус** появится статус: `Завершена`, а строка таблицы будет выделена красным цветом.

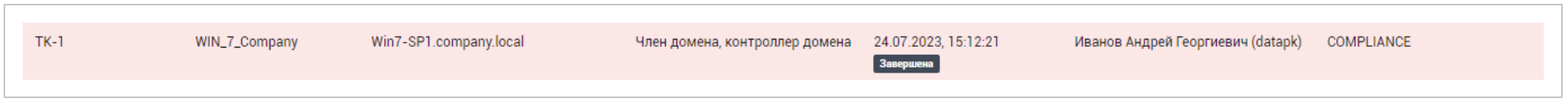


Рис. 550. Результат успешной проверки на соответствие требованиям ИБ **в случае невыполнения критериев оценки**

Если проверка не выполнена, в таблице результатов в столбце **Статус** появится статус: `Ошибка` с описанием ошибки.

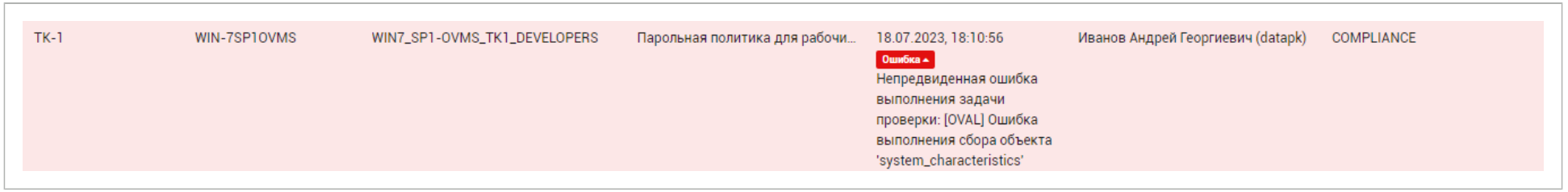


Рис. 551. Результат неуспешной проверки на соответствие требованиям ИБ

Результаты проверок будут выделены желтым цветом, если в случае проверок типа `COMPLIANCE` и `VULNERABILITY` хотя бы один критерий имеет результат, отличный от `true` и `false` (например, в случае ошибки или невозможности получить данные с актива).

Результаты проверок типа `INVENTORY` (проверка наличия установленного ПО и версий ПО) и `MISCELLANEOUS` (иные виды проверок) не выделяются цветом.

См. также

Запуск OVAL-проверки актива на соответствие требованиям информационной безопасности

Просмотр и выгрузка результатов проверки актива на соответствие требованиям информационной безопасности

22.1.2.4.6. Статусы поиска уязвимостей

В окне **Запустить поиск уязвимостей** на странице **Активы** можно просматривать статус поиска уязвимостей.

Описание статусов приведено в таблице ниже.

Табл. 132. Описание статусов поиска уязвимостей

ИНДИКАТОР	ОПИСАНИЕ
Не запущено	Поиск уязвимостей не был запущен пользователем
Выполняется	Поиск уязвимостей запущен и выполняется
Завершено	Поиск уязвимостей успешно завершился
Отменено	Поиск уязвимостей был отменен пользователем
Ошибка	Поиск уязвимостей завершен с ошибкой

Подробнее см. раздел «Запуск поиска уязвимостей в базах CVE, CPE и БДУ ФСТЭК России».

22.1.2.4.7. Статусы подготовки файлов к экспорту

На следующих страницах модуля «Анализ промышленного сетевого трафика» можно экспортировать данные из прослушиваемого трафика:

- на вкладке **Пакеты** страницы **Сетевые соединения** доступен экспорт копии трафика в файл формата `.pcap`;
- на странице **Файлы** доступен экспорт файлов, которые передавались в прослушиваемом трафике.

Для возможности экспорта файл необходимо подготовить. Ознакомиться со статусами подготовки файлов вы можете в таблице ниже.

Табл. 133. Статусы подготовки файлов с копией трафика

ТЕКСТ СТАТУСА	ЦВЕТ	ОПИСАНИЕ
Готов к экспорту	Зеленый	Файл подготовлен и доступен для скачивания
Получение	Желтый	Выполняется подготовка файла

Табл. 133. Статусы подготовки файлов с копией трафика

ТЕКСТ СТАТУСА	ЦВЕТ	ОПИСАНИЕ
Ошибка	Красный	Не удалось подготовить файл из-за недоступности сенсора
Превышен лимит	Красный	Не удалось подготовить файл: размер файла превысил 1 ГБ
Удален	Красный	Файл подготовлен ранее, но больше не доступен для скачивания: в процессе ротации файл был перезаписан более новым

22.1.2.5. Сведения о версиях Комплекса

Версия Комплекса указывается в поставляемой документации на комплекс и отображается в веб-интерфейсе возле логотипа в верхней левой части страницы. Информация о версии также отображается на странице **Администрирование → О системе**.

22.1.3. Дополнительные функции Комплекса

В разделе описаны следующие дополнительные функциональные возможности Комплекса.

- Выгрузка отчетов
- Групповые операции
- Нормализация событий

22.1.3.1. Выгрузка отчетов

Комплекс позволяет пользователям выгружать отчеты в форматы `pdf`, `xlsx` и `csv` по содержимому следующих страниц:

СТРАНИЦА	СОДЕРЖАНИЕ ОТЧЕТА	ФОРМАТ ОТЧЕТА
Активы	Активы, выбранные чекбоксами	html , xlsx
	Уязвимости актива, для которого в последний раз выполнялся поиск	csv
Инциденты	Инциденты, выбранные чек-боксами	html, xlsx
Конфигурации	Все или отфильтрованные конфигурации	html, xlsx
Перечень ПО	Результаты сопоставления собранного сканерами ПО и ОС со справочником CPE для актива, для которого в последний раз выполнялся поиск уязвимостей	csv
Результаты проверок	Все или отфильтрованные результаты проверок	html, xlsx

Помимо таблицы, отчеты формата `*.html` и `*.xlsx` содержат название, фильтры, использованные при создании отчета, дату выгрузки, автора запроса и заголовок.

Внимание:

Максимальное количество строк, выгружаемых при формировании отчета — 1000 строк. Если значение переменной `MAX_ROWS_PER_REPORT` более 1000, в отчет выгрузится только 1000 строк.

Для задачи создания отчета возможны следующие состояния:

- `Не запущена` — задача создания отчета не начата.
- `Ожидание` — обычно кратковременный статус: происходит подготовка к созданию отчета. Может отображаться долго, если выбранных элементов много или есть другие задачи.
- `Выполняется` — отчет формируется в данный момент.
- `Ошибка` — во время формирования отчета произошла ошибка. При наведении на статус можно увидеть, какая именно ошибка вызвала статус.
- `Завершена` — отчет был успешно сформирован и его можно скачать.

См. также

Выгрузка отчета по активам

Выгрузка отчета по инцидентам

Просмотр сводки конфигураций

Выгрузка отчета по результатам сопоставления собранного ПО со справочником CPE

Просмотр и выгрузка результатов проверки актива на соответствие требованиям информационной безопасности

22.1.3.2. Групповые операции

Для страниц оперативных данных и управления в интерфейсе Комплекса предусмотрен ряд групповых операций, которые имеют идентичный механизм работы.

Основные групповые операции

Основные групповые операции, общие для нескольких страниц интерфейса, вы можете увидеть в таблице ниже (Таблица 134. Основные групповые операции).

Табл. 134. Основные групповые операции

НАЗВАНИЕ	СТРАНИЦЫ ИНТЕРФЕЙСА
Удаление	**Активы** **Инциденты** **Индексы** **Настройки OVAL** **Определения OVAL** **Группы OVAL** **Результаты проверок** **Скрипты OVAL** **Сканеры** **Источники** **Учетные данные** **Правила корреляции**

Табл. 134. Основные групповые операции

НАЗВАНИЕ	СТРАНИЦЫ ИНТЕРФЕЙСА
	Оповещения об инцидентах **Правила обнаружения** **Статус сбора** **Ретроанализ** **Схема корреляции**
Включение и отключение правил корреляции	**Правила корреляции**
Включение и отключение правил обнаружения вторжений	**Правила обнаружения**

ОСТОРОЖНО:

Действие групповой операции применяется ко всем выбранным элементам страницы. Для страниц **Активы**, **Виджеты**, **Сканеры**, **Определения OVAL** выбор осуществляется при помощи установки чекбоксов. Выбор на остальных страницах осуществляется при помощи фильтров. Если фильтры и чекбоксы не установлены, операция будет применена ко всем элементам страницы.

Операции, доступные только при выборе одного или нескольких элементов

Если на странице, где элементы выбираются с помощью чекбоксов, ни одна строка не выбрана, часть операций будет недоступна. Подробности указаны в таблице ниже (Таблица 135. Операции, доступные только при выборе одного или нескольких элементов.).

Табл. 135. Операции, доступные только при выборе одного или нескольких элементов.

СТРАНИЦА	КНОПКИ ОПЕРАЦИЙ, ДОСТУПНЫЕ ПРИ ВЫБОРЕ ХОТЯ БЫ ОДНОГО ЭЛЕМЕНТА
Виджеты	**Удалить визуализации**
Активы	Удалить Найти уязвимости Создать отчёт
Сканеры	Удалить
Определения OVAL	Отменить выбор, (**Добавить в группу**), (**Исключить из группы**)

Дополнительные групповые операции

Ознакомиться с дополнительными групповыми операциями, которые используются только на одной странице интерфейса, вы можете в таблице ниже.

Табл. 136. Дополнительные групповые операции

НАЗВАНИЕ	СТРАНИЦЫ ИНТЕРФЕЙСА
Изменить параметры инцидентов	**Инциденты**
Архивировать	**Индексы**
Добавление в группу OVAL-определений	**Определения OVAL**
Активировать	**Задачи сбора**
Деактивировать	**Задачи сбора**
Применить элементы схемы для текущего анализа	**Схема корреляции**
Не применять элементы схемы для текущего анализа	**Схема корреляции**
Применить элементы схемы для ретроспективного анализа	**Схема корреляции**
Не применять элементы схемы для ретроспективного анализа	**Схема корреляции**

Использование групповых операций

При использовании групповых операций необходимо ввести обоснование групповой операции, чтобы администратор системы мог найти причину серьезных изменений.

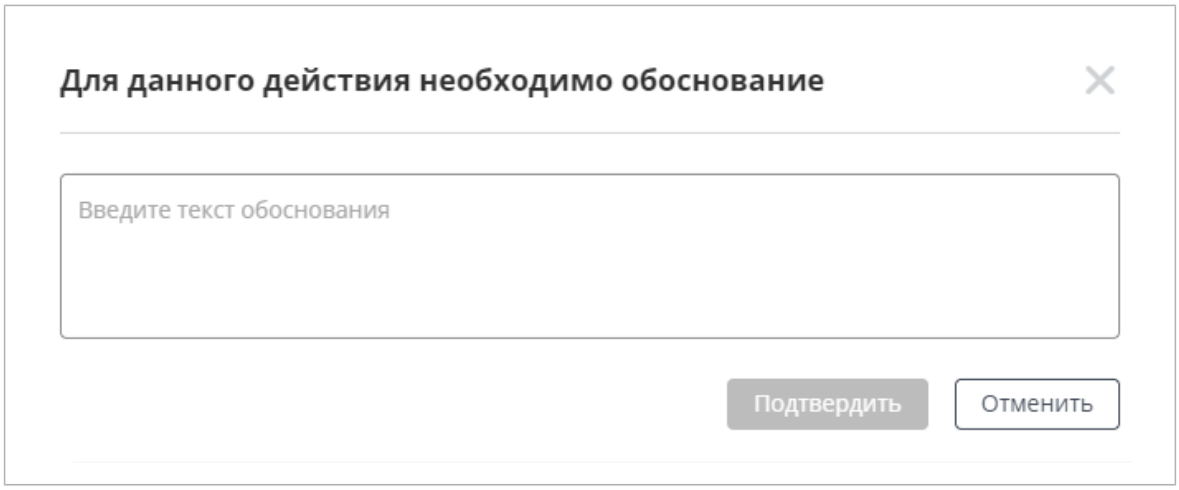


Рис. 552. Обоснование групповой операции

22.1.3.3. Нормализация событий

Выходным форматом сообщений Комплекса — внутренних или поступающих от источников событий — являются нормализованные события, которые отображаются на странице **События**.

Поля нормализованных событий и их значения используются в правилах корреляции событий, на основе которых Комплекс обнаруживает инциденты.

События приводятся к нормализованному виду по встроенным в Комплекс правилам нормализации с использованием следующих полей (часть полей может отсутствовать в зависимости от типа получаемых сообщений): `@timestamp`, `@version`, `action`, `appliance_node_id`, `category`, `config_diff`, `config_type`, `create_time`, `description`, `event_code`, `event_type`, `observer_id`, `observer_name`, `id`, `justification`, `login`, `message`, `protocol`, `protocol_specific_data`, `receive_time`, `shell`, `source_ip`, `source_mac`, `status`, `target_ip`, `target_mac`, `type`, `user`. Данные поля определены во встроенном шаблоне формата `*.json`, который хранится в директории `/logstash/config/plugins/templates` рабочей директории Комплекса.

Нормализация событий также осуществляется с помощью встроенных и пользовательских конфигурационных файлов Logstash. Файлы хранятся с расширением `*.conf` в директории `/logstash/config/plugins/pipeline` рабочей директории Комплекса.

Конфигурационные файлы нормализации делятся на три типа:

- `input` — генерируют события на основании сообщений из различных сервисов и определяют, к какому типу событий оно относится. Могут также содержать фильтры для начальной нормализации;
- `filter` — в зависимости от типа события выполняют основную нормализацию с помощью фильтров формата grok;
- `output` — в зависимости от типа нормализованных событий отправляют их в соответствующий сервис или в дополнительный `output`.

Рекомендуемый формат именования конфигурационных файлов нормализации: `${N}-${NAME}-{TYPE}.conf`.

Grok-фильтры имеют следующий формат: `%{ТИП_ДАННЫХ:значение_поля_события}`.

> **Пример**
>
> Пример grok-фильтра:
>
> ```
> %{TIMESTAMP_ISO8601:date} %{WORD:method} %{IPV4:client} %{NUMBER:size} %{WORD:def} (?<VerOs>.*)
> ```

Grok-фильтры могут применяться для разделения информации из встроенного поля по дополнительным пользовательским полям.

Пример

Пример конфигурационного файла с фильтром grok для сообщений из журнала SCADA:

```
filter {
 if [type] == "event" and [message] =~ "EventLog" {
 grok {
 # События SCADA
 #
 # Пример:
 # type="Info" message="TrainView session is ended" result="" source="User: admin"
 match => {"[message]" => "type=\"%{WORD:SCADA_type}\" message=\"%{GREEDYDATA:SCADA_message}\"
 result=\"%{GREEDYDATA:SCADA_result}\" source=\"%{GREEDYDATA:SCADA_sourse}\"" }
 add_field => {"event_type" => "eventlog" }
 tag_on_failure => []
 }
 }
}
```

Сообщение из журнала SCADA, отправленное в Комплекс, сначала целиком записывается во встроенное поле `message`. Затем при помощи grok-фильтра содержимое этого поля нормализуется по следующим пользовательским полям: `SCADA_type`, `SCADA_message`, `SCADA_result`, `SCADA_source`.

22.1.3.3.1. Работа с файлами с расширением .conf

Тип события в Комплексе (`event_type`) определяется на основе источника данных (IP-адреса), а не только по содержимому события.

Все события анализируются по правилам, заданным в файле `04-event_type-translate-filter.conf`, после чего получают тип событий (`event_type = undefined`). Далее событие анализируется по правилам из других файлов с разрешением `.conf`.

22.1.3.3.1.1. Назначение файла 09-custom-filter.conf

Файл `09-custom-filter.conf` является точкой расширения Комплекса для обработки новых, нестандартных или пользовательских источников данных, которые не входят в стандартную поставку продукта. Изначально файл пустой, что позволяет пользователю добавлять свои фильтры, не опасаясь конфликтов с обновлениями основного продукта.

Для корректной работы фильтр должен быть обернут в условие, которое явно указывает, на какие типы событий должен срабатывать этот фильтр.

Пример

Ниже представлен пример заполнения файла `09-custom-filter.conf`:

```
filter{
  if [event_type] == "undefined" or [event_type] == "my_custom_app" {

    # Здесь располагаются Grok-паттерны и другие фильтры.
    # Пример:
```

```
    grok {
      match => { "message" => "{TIMESTAMP_ISO8601}%{WORD}\[%{INT}\]" }
      add_field => { "some_test_name" => "Some_test_value" }
    }

    # После успешного поиска можно переназначить event_type на пользовательский,
    # чтобы следующие фильтры знали, что событие было обработано
    mutate {
      replace => { "[event_type]" => "my_custom_app" }
      # Также можно добавить пользовательские для нормализации
      add_field => { "same_test_name" => "same_test_value" }
    }
  }
}
```

Внимание:

При работе с файлом `09-custom-filter.conf` важно не использовать «жадные» фильтры, т.к. это может привести к следующим последствиям:

- некорректная обработка данных — события от межсетевого экрана могут обрабатываться правилами для VPN, что приведет к ошибкам в извлеченных полях;
- потеря данных — событие может быть обработано «жадным» фильтром и не дойти до целевого правила;
- снижение производительности — Комплекс будет тратить ресурсы на многократную обработку одного события разными фильтрами.

22.1.3.4. Представления

Представление — элемент веб-интерфейса, предназначенный для сохранения текущего вида страницы. В большинстве случаев в представлении сохраняются примененные фильтры и выбранные для отображения колонки таблиц.

Например, на странице **Карта сети** сохраняются примененные фильтры, расположение узлов на карте, их вид (на сетке, по кругу), наличие сортировки по количеству сессий.

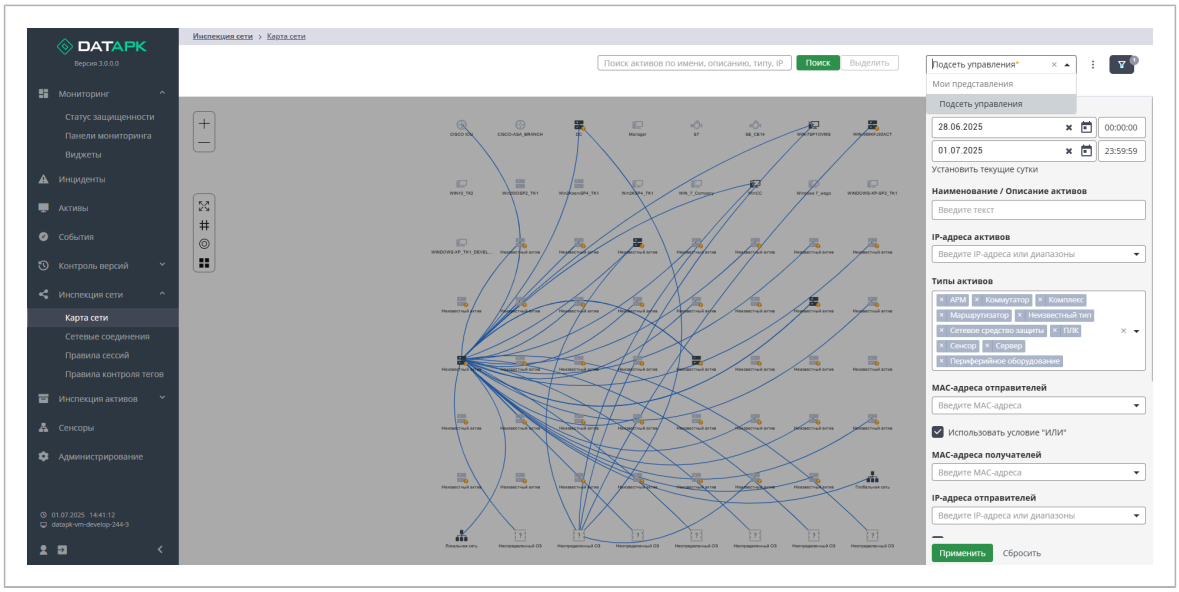


Рис. 553. Представления на странице «Карта сети»

После настройки фильтров, отображаемых колонок или узлов на карте представление можно сохранить. Для сохраненных представлений доступно редактирование и удаление.

22.1.3.4.1. Управление представлениями

Для управления представлениями доступны следующие возможности:

1. Сохранение представления. Для сохранения:
    а. Заполните все необходимые параметры фильтрации, выберите столбцы для отображения в представлении, либо отображение узлов на карте.
    б. В верхней правой части страницы нажмите ⋮.
    в. В выпадающем меню выберите опцию **Сохранить как**.
    ▸ **Результат шага:** появится окно сохранения представления.
    г. В окне сохранения представления:
        - введите подходящее наименование;

        > ⚠ Внимание:
        >
        > Имя не должно совпадать с уже существующим.

        - выберите, будет ли представление доступно для использования другими пользователями.

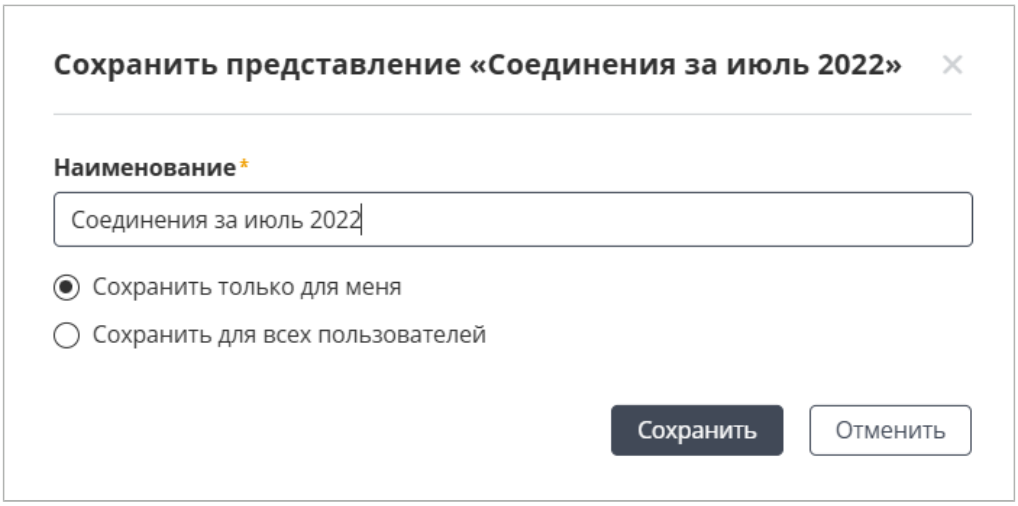


Рис. 554. Окно сохранения представления

д. Нажмите **Сохранить**.

▸ **Результат шага:** на странице, где было сохранено представление, будет доступно для выбора новое представление.

2. Изменение представления. Для изменения:

а. В верхней части панели фильтров выберите из выпадающего списка представление, которое будет изменено.

б. Измените параметры фильтрации, отображение столбцов или отображение узлов на карте.

> Внимание:
>
> Возле названия представления в верхней части панели фильтров появится оранжевый символ *. Это означает, что есть несохраненные изменения представления.

в. Нажмите ⋮ в верхней правой части страницы.

г. В появившемся меню выберите одну из следующих опций:

- **Сохранить** для сохранения изменений в выбранном представлении;
- **Сохранить как** для сохранения изменений в новом представлении;
- **Редактировать** для изменения названия и сохранения выбранного фильтра.

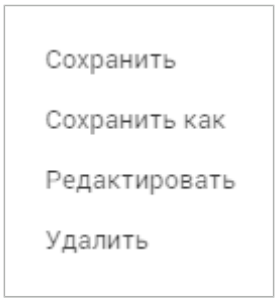


Рис. 555. Меню управления представлением

д. В окне сохранения представления введите имя представления.

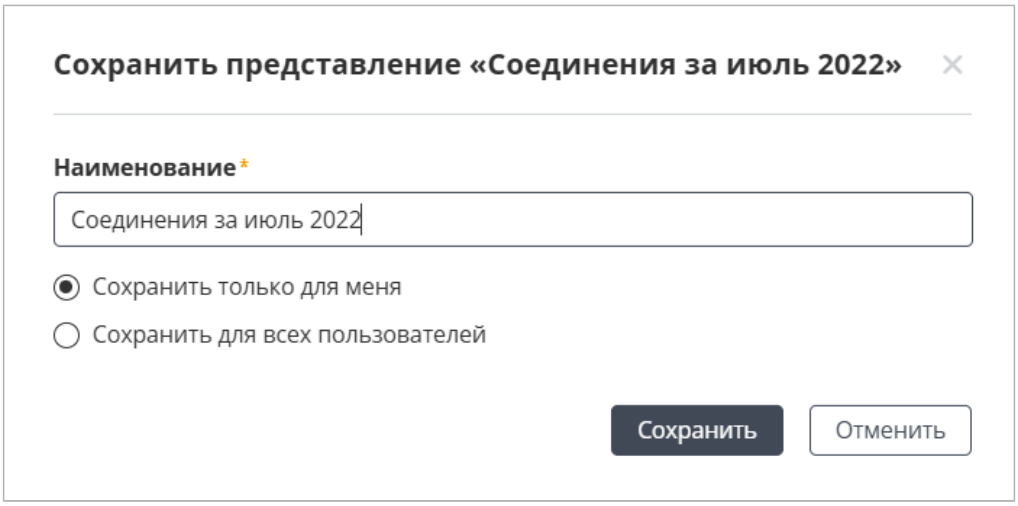


Рис. 556. Предупреждение в окне сохранения представления

e. Нажмите **Сохранить**.

3. Удаление представления. Для удаления представления:

   a. Нажмите ⋮ в верхней правой части страницы.

   б. В появившемся меню нажмите **Удалить**.

   ▸ **Результат шага:** появится окно удаления представления.

   в. В окне **Удалить представление** нажмите **Удалить**.

> ⚠ Внимание:
>
> Удаление представления является невозвратной операцией.

▸ **Результат шага:** появится всплывающее уведомление: Представление удалено.

22.2. Условия эксплуатации Комплекса

По условиям эксплуатации аппаратная часть для Комплекса предназначена для установки в стационарных, специальных и временных отапливаемых помещениях и укрытиях в условиях круглосуточной работы с перерывами на техническое обслуживание.

Нормальными климатическими условиями эксплуатации аппаратной части для Комплекса являются:

- температура окружающего воздуха – от –10 до +60 °С;
- относительная влажность воздуха – от 5 до 95%;
- атмосферное давление – от 630 до 800 мм рт.ст.

Способ подключения аппаратной части для Комплекса к оборудованию объекта информатизации определяется на этапе предпроектного обследования.

22.3. Описание источников событий

В этом разделе:

- Описание служебных источников событий
- Описание безагентного сбора событий Eventlog

22.3.1. Описание служебных источников событий

Служебные источники событий описаны в таблице ниже (Таблица 137. Служебные источники событий Комплекса).

Табл. 137. Служебные источники событий Комплекса

НАЗВАНИЕ ИСТОЧНИКА (LISTENER)	ОПИСАНИЕ
Availability control	Изменение доступности активов, невозможность установки соединения с активом
Backup control	Статус процедуры резервного копирования
Configuration control	Изменение состояния эталонной конфигурации актива
Session control	Появление новых сессий, подтверждение сессий
Event control	Запуск или остановка системы регистрации событий
Host control	Создание, удаление и изменение активов, обнаружение неизвестных активов
Host data collecting	Статус выполнения задачи сбора данных с актива, состояние работы ее расписания
Incident control	Создание, удаление, изменение инцидентов
OVAL assessment control	Состояние выполнения проверок на соответствие требованиям ИБ
OVAL definitions control	Состояние задачи удаления проверок на соответствие требованиям ИБ
OVAL groups control	Состояние задачи на удаление группы или нескольких групп OVAL-определений
Script verification	Статус верификации Python-скриптов, используемых в сканерах сбора данных
User action control	Выполнение действий пользователями
System control	Статус компонентов Комплекса: оперативной памяти, дискового пространства, нагрузки на ЦП, средней нагрузки (Load average), целостность контрольных сумм исполняемых файлов
IDS control	Статус службы обнаружения вторжений
Esper control	Статус службы корреляции

Сбор событий с использованием служебных источников запускается автоматически после включения Комплекса.

Переменные для управления служебными источниками событий

Администратор Комплекса, имеющий доступ к консольному управлению, может настроить включение и отключение, а также критичность служебных событий. Для этого в файл `manager.env` добавляются соответствующие переменные, ознакомиться с которыми вы можете в таблице ниже (Таблица 138. Переменные для управления событиями Комплекса).

> Подсказка:
>
> Переменные, наименование которых оканчивается на `_EVENTS`, могут иметь одно из следующих значений:
>
> - `true` — для остановки работы служебного источника событий;
> - `false` — для запуска работы служебного источника событий, если ранее он был отключен.
>
> Переменные, наименование которых оканчивается на `_EVENTS_SEVERITY`, могут иметь одно из следующих значений:
>
> - `critical` — для установки критичного приоритета событиям, сгенерированным сенсорами;
> - `low` — для установки низкого приоритета событиям, сгенерированных сенсорами.

Табл. 138. Переменные для управления событиями Комплекса

ПЕРЕМЕННАЯ	ОПИСАНИЕ	ЗНАЧЕНИЕ ПЕРЕМЕННОЙ ПО УМОЛЧАНИЮ
`DISABLE_CONFIGURATION_CONTROL_EVENTS`	При значении переменной `true` события об изменении конфигурации не создаются	`false`
`DISABLE_HOST_DATA_COLLECTING_EVENTS`	При значении переменной `true` события сбора данных не создаются	`false`
`DISABLE_USER_ACTION_CONTROL_EVENTS`	При значении переменной `true` события о действиях пользователей не создаются	`false`
`DISABLE_HOST_CONTROL_EVENTS`	При значении переменной `true` события о появлении новых, изменении и удалении узлов не создаются	`false`
`DISABLE_AVAILABILITY_CONTROL_EVENTS`	При значении переменной `true` события о доступности узлов не создаются	`false`
`DISABLE_OVAL_ASSESSMENT_CONTROL_EVENTS`	При значении переменной `true` события о проверках на соответствие требованиям ИБ не создаются	`false`

Табл. 138. Переменные для управления событиями Комплекса

ПЕРЕМЕННАЯ	ОПИСАНИЕ	ЗНАЧЕНИЕ ПЕРЕ-МЕННОЙ ПО УМОЛЧАНИЮ
`DISABLE_INCIDENT_CONTROL_EVENTS`	При значении переменной `true` события об инцидентах не создаются	`false`
`DISABLE_OVAL_DEFINITIONS_CONTROL_EVENTS`	При значении переменной `true` события об удалении проверок на соответствие требованиям ИБ не создаются	`false`
`DISABLE_OVAL_GROUPS_CONTROL_EVENTS`	При значении переменной `true` события об удалении групп OVAL-определений не создаются	`false`
`DISABLE_BACKUP_CONTROL_EVENTS`	При значении переменной `true` события о резервном копировании не создаются	`false`
`DISABLE_SURICATA_CONTROL_EVENTS`	При значении переменной `true` события службы обнаружения вторжений не собираются	`false`
`CONFIGURATION_CONTROL_EVENTS_SEVERITY`	Важность событий изменения конфигурации	`low`
`HOST_DATA_COLLECTING_EVENTS_SEVERITY`	Важность событий сбора и ошибок сбора данных	`low`
`USER_ACTION_CONTROL_EVENTS_SEVERITY`	Важность событий по действиям пользователей	`low`
`HOST_CONTROL_EVENTS_SEVERITY`	Важность событий появления новых узлов	`low`
`AVAILABILITY_CONTROL_EVENTS_SEVERITY`	Важность событий доступности узлов	`low`
`OVAL_ASSESSMENT_CONTROL_EVENTS_SEVERITY`	Важность событий об объектах OVAL	`low`
`INCIDENT_CONTROL_EVENTS_SEVERITY`	Важность событий о создании, удалении, изменении инцидентов	`low`
`OVAL_DEFINITIONS_CONTROL_EVENTS_SEVERITY`	Важность событий удаления проверок на соответствие требованиям ИБ	`low`

Табл. 138. Переменные для управления событиями Комплекса

ПЕРЕМЕННАЯ	ОПИСАНИЕ	ЗНАЧЕНИЕ ПЕРЕ-МЕННОЙ ПО УМОЛЧАНИЮ
`OVAL_GROUPS_CONTROL_EVENTS_SEVERITY`	Важность событий удаления групп OVAL-определений	`low`
`BACKUP_CONTROL_EVENTS_SEVERITY`	Важность событий резервного копирования	`low`
`EVENT_CONTROL_EVENTS_SEVERITY`	Важность событий, полученных от сервиса регистрации событий	`critical`
`HOME_NET_SCAN_CONTROL_EVENTS_SEVERITY`	Важность событий, полученных при сканировании контро-лируемой сети	`low`
`SCRIPT_VERIFICATION_EVENTS_SEVERITY`	Важность событий верификации скриптов	`low`
`SYSTEM_CONTROL_EVENTS_SEVERITY`	Важность системных событий	`low`
`IDS_CONTROL_EVENTS_SEVERITY`	Важность событий службы обнаружения вторжений	`critical`
`DPI_CONTROL_EVENTS_SEVERITY`	Важность событий `dpi_notice`	`critical`
`ML_CONTROL_EVENTS_SEVERITY`	Важность событий `ml_notice`	`critical`
`SESSION_CONTROL_EVENTS_SEVERITY`	Важность событий, связанных с сетевыми соединениями	`critical`

См. также

Переменные Комплекса

Включение и отключение служебных источников

22.3.2. Описание безагентного сбора событий Eventlog

Задачи сбора событий могут быть описаны в исполняемом файле, которые выполняются в среде, поддерживающей подмножество синтаксиса языка Python (RestrictedPython) — скрипте.

Пример Python-скрипта, используемого в сканере для сбора событий из журнала **security** Microsoft Windows с помощью учетной записи с тегом `admin`:

```
journal_name = 'Security'
offset = store.get('offset') if store else None
fetch_old_events = False # Нужно ли получать события с активов , созданные до первого запуска
 скрипта
try:
 credential = credentials['admin']
except KeyError as e:
 raise KeyError('Учетные данные для пользователя admin не найдены') # Получаем смещение, если
 необходимо
if not fetch_old_events and offset is None:
 protocol_args = {
 'interface': 'mseven',
 'host': host,
 'user': credential['user'],
 'password': credential['password'],
 'query': {
 'object': 'offset',
 'path': journal_name,
 'offset': 0
 },
 'timeout': 300,
 'ttl': 300,
 }
 offset = execute('msrpc', protocol_args, expiration)['newest_record_number'] # Получаем события
protocol_args = {
 'interface': 'mseven',
 'host': host,
 'user': credential['user'],
 'password': credential['password'],
 'query': {
 'object': 'events',
 'path': journal_name,
 'offset': offset
 },
 'timeout': 300,
 'ttl': 300,
}events = execute('msrpc', protocol_args, expiration)result = []
for event in events:
                        if                          event['EventId']                          in
 [4720, 4722, 4726, 4738, 4740, 4767, 4781, 4724, 4725, 4727, 4728, 4729, 4730, 4731, 4732,
4733, 4734, 4735, 4737, 4754, 4755, 4756, 4757, 4758, 4764, 4616, 1102, 4625, 4624]:
 result.append({
 'receive_time': datetime.datetime.utcfromtimestamp(event['TimeGenerated']).isoformat(),
 'message': event['Message'],
 'host_id': host_id,
 'observer_id': observer_id,
 'protocol_specific_data': {
```

```
 'journal_name': journal_name,
 'computer_name': event['ComputerName'],
 'event_id': event['EventId'],
 'event_type': event['EventType'],
 'event_category': event['EventCategory'],
 'source_name': event['SourceName']
 }
 }) offset = event['RecordNumber'] + 1return {
 'data': result,
 'store': {'offset': offset}
}
```

Общий состав задачи сбора событий определяется в тексте Python-скрипта. В качестве настраиваемых параметров для описания задачи сбора событий могут быть выбраны:

- `computer_name` – идентификатор хоста;
- `event_category` – категория события;
- `event_id` – идентификатор события;
- `event_type` – тип события;
- `journal_name` – наименование журнала;
- `source_name` – название источника, создавшего событие.

Для возможности сбора событий с активов необходимо создать и настроить учетные записи на активах с правами, достаточными для удаленного доступа к необходимой информации. Учетную запись, настроенную в операционной системе актива, необходимо добавить в список учетных данных в веб-интерфейсе Комплекса. Порядок настройки учетных данных в Комплексе приведен в разделе «Добавление учетных данных актива».

22.4. Описание полей событий в экспертном режиме страницы «События»

Для каждого события на странице **События** → **Экспертный режим** предусмотрен набор полей, в которых отображается уникальная для события информация.

Табл. 139. Основные поля событий

ПОЛЕ	ОПИСАНИЕ	ПРИМЕРЫ ЗНАЧЕНИЯ ПОЛЯ
action	Краткое описание действия	detect, block, permit, audit_success, connection success, connection failure, auth success
additional_-information	Дополнительная информация о действии или его результате	rpc_s_access_denied
appliance_-node_id	ID Комплекса уровня Sensor, на котором было зафиксировано событие	b08deaf7edc5def382d2580870de5fbe
appliance_-node_name	Наименование Комплекса уровня Sensor, на котором было зафиксировано событие	datapk-vm-tk2-test-244-36

Табл. 139. Основные поля событий

ПОЛЕ	ОПИСАНИЕ	ПРИМЕРЫ ЗНАЧЕНИЯ ПОЛЯ
category	Классификация события по результату или источнику	OK
create_time	Время регистрации события на источнике. Может не совпадать с часовым поясом Комплекса	11.05.2022 @ 18:42:33.789
description	Краткое описание события	Create incoming message
event_code	Идентификатор или классификатор типа события	1170004
event_type	Тип события	info_exchange
id	Уникальный идентификатор события	019b35f6-2b98-47de-a3d0-c37c554029a6
justification	Обоснование или комментарий к выполняемому действию	
link	Поле для внешних интеграторов	
listener	Наименование служебного источника событий	event_log_sensor
management_node_id	ID Комплекса уровня Management, на котором было зафиксировано событие	b08deaf7edc5def382d2580870de5fbe
management_node_name	Наименование Комплекса уровня Management, на котором было зафиксировано событие	datapk-vm-tk2-test-244-36
message	Исходное (оригинальное) событие	Выявлена ошибка подключения к активу 192.168.243.80 по MSRPC: rpc_s_access_denied
observer_id	ID регистратора события: актива, сенсора или Комплекса	9429058a-835a-4f9e-a666-ee5799b33db0
observer_ip	IP-адрес регистратора события: актива, сенсора или Комплекса	10.51.203.99
observer_name	Сетевое имя регистратора события: актива, сенсора или Комплекса	datapk-vm-tk2-test-244-36

Табл. 139. Основные поля событий

ПОЛЕ	ОПИСАНИЕ	ПРИМЕРЫ ЗНАЧЕНИЯ ПОЛЯ
priority	Приоритет инцидента	low
protocol	Протокол взаимодействия/API/ID канала инфообмена	ssh
receive_time	Время регистрации события на Комплексе	11.05.2022 @ 18:30:11.960
request_id	Идентификатор HTTP-запроса	GET /index.html HTTP/1.1
severity	Важность события	critical
source_-hostname	Наименование отправителя (актива)	datapk-vm-tk2-test-244-36
source_id	Идентификатор отправителя (актива)	f37b0f20-c1f5-4401-9240-0cfccd9daa58
source_ip	IP-адрес отправителя (актива)	10.51.203.19
source_mac	datapk-vm-tk2-test-244-36	00:50:56:B7:2C:3C
source_port	Порт отправителя (актива)	5353
target_ip	IP-адрес получателя (актива)	10.51.203.9
target_mac	MAC-адрес получателя (актива)	00:50:56:B7:2C:3C
target_id	Идентификатор получателя (актива)	2098ebf1-7e32-4d8f-8b0e-3cfc92e9e921
target_-hostname	Наименование получателя (актива)	WIN-7
target_port	Порт получателя (актива)	80
user	Логин пользователя, инициировавшего событие	aivanov

22.5. Переменные Комплекса

В этом разделе:

- Переменные Комплекса уровня Management
    - Установка переменных модуля «Анализ промышленного сетевого трафика» через запрос в Redis
- Переменные Комплекса уровня Sensor
- Переменные службы обнаружения вторжений
- Конфигурационные файлы модуля «EDR for PLC»
- Рекомендации по использованию переменных файлов manager.env и sensor.env

Для Комплексов уровня Management и Sensor, а также их сервисов устанавливаются разные конфигурационные файлы с различным набором переменных.

Конфигурационные файлы с переменными и их расположение представлены в таблице ниже.

Табл. 140. Конфигурационные файлы с переменными и их расположение

ТИП КОМПЛЕКСА	МОДУЛЬ
Комплекс уровня Management	Базовый модуль (Core)
	Управление внешними событиями
	Анализ промышленного сетевого трафика
Комплекс уровня Sensor	Базовый модуль (Core)

Табл. 140. Конфигурационные файлы с переменными и их расположение

ТИП КОМПЛЕКСА	МОДУЛЬ
	Анализ промышленного сетевого трафика
	EDR for PLC

22.5.1. Переменные Комплекса уровня Management

Обязательные переменные файла manager.env

Переменные файла `manager.env` устанавливаются в директории `/usr/share/udv/datapk`

Список обязательных переменных, содержащийся в файле `manager.env` Комплекса уровня Management, представлен в таблице ниже.

Табл. 141. Обязательные переменные файла `manager.env`

ПЕРЕМЕННАЯ	ОПИСАНИЕ	ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ (ЖИРНЫМ), ЛИБО ПРИМЕР
`DB_USER`	Пользователь базы данных. ОСТОРОЖНО: Изменение значения переменной может привести к отсутствию доступа к базе данных.	`postgres`
`DB_PASS`	Пароль доступа к базе данных.	`P@ssw0rd`

Табл. 141. Обязательные переменные файла `manager.env`

ПЕРЕМЕННАЯ	ОПИСАНИЕ	ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ (ЖИРНЫМ), ЛИБО ПРИМЕР
	ОСТОРОЖНО: Изменение значения переменной может привести к отсутствию доступа к базе данных.	
`HOST_IP`	Интерфейс управления Комплекса. В качестве значения переменной задается IP-адрес одного из активных интерфейсов Комплекса	`10.51.15.104`
`DB_ENCRYPTION_KEY`	Ключ шифрования базы данных в сборщике данных (`udv-host-data-collector`). Ключ должен иметь длину 24 символа. ОСТОРОЖНО: Изменение значения переменной может привести к отсутствию доступа к базе данных.	`dJ2ZOZeU0nJhHwjfhqlOwF1x`
`EVENT_INDICES_MAX_SIZE_GB`	Максимально допустимый объем оперативного архива внешних событий. Суммарный объем с `EVENT_ARCHIVES_MAX_SIZE_GB` не должен составлять более 50-60% объема дискового пространства Внимание: На Комплексах базового уровня и (или) с HDD — не более 100 ГБ. На Комплексах среднего и верхнего уровней с SSD — не более 300 ГБ	`10`
`EVENT_INDICES_ACTION_SIZE_EXCEEDED`	Действие в случае переполнения оперативного архива внешних событий. Возможные варианты значений переменной:	`rotate`

Табл. 141. Обязательные переменные файла `manager.env`

ПЕРЕМЕННАЯ	ОПИСАНИЕ	ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ (ЖИРНЫМ), ЛИБО ПРИМЕР
	• `nothing`; • `break`; • `rotate`.	
`EVENT_INDICES_LIFETIME_DAYS`	Время хранения внешних событий в оперативном архиве, задается в днях	`30`
`EVENT_ARCHIVES_LIFETIME_DAYS`	Время хранения внешних событий в глубоком архиве, события старше указанного значения удаляются. Значение задается в днях	`60`
`EVENT_ARCHIVES_MAX_SIZE_GB`	Максимально допустимый объем глубокого архива внешних событий. Суммарный объем с `EVENT_INDICES_MAX_SIZE_GB` должен составлять не более 50-60% объема дискового пространства. Значение задается в гигабайтах	`5`
`EVENT_ARCHIVES_ACTION_SIZE_EXCEEDED`	Действие, выполняемое при превышении лимита на размер глубокого архива внешних событий. Возможные значения переменной: • `nothing` • `break` • `rotate`	`rotate`
`EVENTS_RETENTION_DISK_CAPACITY_SIZE_MB`	Максимально допустимый объем архива событий, хранящегося в модуле внутренних событий. При достижении предельного значения, заданного в этой переменной, регистрация внутренних событий останавливается. Значение задается в мегабайтах. При значении `0` лимит на хранение архива внутренних событий отключен	`0`
`EVENTS_RETENTION_MONTHS`	Временной период, по истечении которого удаляются внутренние события старше срока, указанного в этой переменной. Значение задается в месяцах	`3`

Дополнительные переменные файла manager.env

Переменные, которые не включены в автоматически генерируемый файл `manager.env` Комплекса уровня Management и добавляются при необходимости, указаны в таблице ниже.

Табл. 142. Дополнительные переменные файла `manager.env`

ПЕРЕМЕННАЯ	ОПИСАНИЕ	ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ (ЖИРНЫМ), ЛИБО ПРИМЕР
`API_SKIP_FIRST_INITIALIZATION`	Отключение первичной инициализации при первом запуске Комплекса при значении переменной `true`	`false`
`AUTOMATIC_HOST_CREATION_BY_MAC`	При значении переменной `true` Комплекс фиксирует активы только по MAC-адресу независимо от наличия у них IP-адреса. В списке активов отображаются все найденные активы (до настройки контролируемой сети активы отображаются только с MAC-адресами). При значении переменной `false`, Комплекс фиксирует активы по MAC-адресу (если IP-адрес не обнаружен) и по связке MAC-адреса и IP-адреса. В списке активов будут отображаться только активы, IP-адреса которых входят в контролируемую сеть, а также активы, IP-адреса которых не обнаружены	`false`
`ASSETS_INACTIVITY_TIMEOUT`	Время, по истечении которого при отсутствии трафика от актива на активных интерфейсах формируется событие о его недоступности и индикатор на странице **Активы** становится серым. Значение задается в секундах. Внимание: Значение переменной не может быть меньше `600` секунд.	`600`
`LIMIT_USER_SESSIONS`	При значении переменной `true` ограничивает до одной количество одновременных активных сессий в веб-интерфейсе Комплекса для каждой учетной записи. При значении переменной `false` ограничений на количество сессий нет	`false`
`NGINX_HTTPS_PORT`	Порт для подключения к Комплексу по протоколу HTTPS	`443`

Табл. 142. Дополнительные переменные файла `manager.env`

ПЕРЕМЕННАЯ	ОПИСАНИЕ	ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ (ЖИРНЫМ), ЛИБО ПРИМЕР
`USER_SESSION_INACTIVITY_TIMEOUT`	Ограничение сессии при отсутствии активности пользователя. Значение задается в секундах	`600`
`LDAP_CONNECTION_STRING`	IP-адрес LDAP-сервера Active Directory для создания пользователей из службы каталогов	`ldaps://192.168.243.121`
`LDAP_TLS`	Использовать TLS-шифрование для Active Directory	`false`
`LOG_LEVEL`	Минимальная критичность системных событий, которые генерирует Комплекс уровня Management. Возможные значения: • `CRITICAL` • `FATAL` • `ERROR` • `WARNING` • `INFO` • `DEBUG` • `NOTSET`	`INFO`
`MAX_ROWS_PER_REPORT`	Максимальное количество строк, выгружаемых при формировании отчета. Если значение переменной более 1000, в отчет выгрузится только 1000 строк	`1000`
`DISABLE_CONFIGURATION_CONTROL_EVENTS`	При значении переменной `true` события об изменении конфигурации не создаются	`false`
`DISABLE_HOST_DATA_COLLECTING_EVENTS`	При значении переменной `true` события сбора данных не создаются	`false`
`DISABLE_USER_ACTION_CONTROL_EVENTS`	При значении переменной `true` события о действиях пользователей не создаются	`false`

Табл. 142. Дополнительные переменные файла `manager.env`

ПЕРЕМЕННАЯ	ОПИСАНИЕ	ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ (ЖИРНЫМ), ЛИБО ПРИМЕР
`DISABLE_HOST_CONTROL_EVENTS`	При значении переменной `true` события о появлении новых, изменении и удалении узлов не создаются	`false`
`DISABLE_AVAILABILITY_CONTROL_EVENTS`	При значении переменной `true` события о доступности узлов не создаются	`false`
`DISABLE_OVAL_ASSESSMENT_CONTROL_EVENTS`	При значении переменной `true` события о проверках на соответствие требованиям ИБ не создаются	`false`
`DISABLE_INCIDENT_CONTROL_EVENTS`	При значении переменной `true` события об инцидентах не создаются	`false`
`DISABLE_OVAL_DEFINITIONS_CONTROL_EVENTS`	При значении переменной `true` события об удалении проверок на соответствие требованиям ИБ не создаются	`false`
`DISABLE_OVAL_GROUPS_CONTROL_EVENTS`	При значении переменной `true` события об удалении групп OVAL-определений не создаются	`false`
`DISABLE_BACKUP_CONTROL_EVENTS`	При значении переменной `true` события о резервном копировании не создаются	`false`
`DISABLE_SURICATA_CONTROL_EVENTS`	При значении переменной `true` события службы обнаружения вторжений не собираются	`false`
`DISABLE_HOME_NET_SCAN_CONTROL_EVENTS`	При значении переменной `true` события при сканировании контролируемой сети не собираются	`false`
`DISABLE_SCRIPT_VERIFICATION_EVENTS`	При значении переменной `true` события регистрации скриптов не собираются	`false`
`DISABLE_SYSTEM_CONTROL_EVENTS`	При значении переменной `true` системные события не собираются	`false`
`CONFIGURATION_CONTROL_EVENTS_SEVERITY`	Важность событий изменения конфигурации	`low`

Табл. 142. Дополнительные переменные файла `manager.env`

ПЕРЕМЕННАЯ	ОПИСАНИЕ	ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ (ЖИРНЫМ), ЛИБО ПРИМЕР
`HOST_DATA_COLLECTING_EVENTS_SEVERITY`	Важность событий сбора и ошибок сбора данных	`low`
`USER_ACTION_CONTROL_EVENTS_SEVERITY`	Важность событий по действиям пользователей	`low`
`HOST_CONTROL_EVENTS_SEVERITY`	Важность событий появления новых узлов	`low`
`AVAILABILITY_CONTROL_EVENTS_SEVERITY`	Важность событий доступности узлов	`low`
`OVAL_ASSESSMENT_CONTROL_EVENTS_SEVERITY`	Важность событий об объектах OVAL	`low`
`INCIDENT_CONTROL_EVENTS_SEVERITY`	Важность событий о создании, удалении, изменении инцидентов	`low`
`OVAL_DEFINITIONS_CONTROL_EVENTS_SEVERITY`	Важность событий удаления проверок на соответствие требованиям ИБ	`low`
`OVAL_GROUPS_CONTROL_EVENTS_SEVERITY`	Важность событий удаления групп OVAL-определений	`low`
`BACKUP_CONTROL_EVENTS_SEVERITY`	Важность событий резервного копирования	`low`
`EVENT_CONTROL_EVENTS_SEVERITY`	Важность событий, полученных от сервиса регистрации событий	`critical`
`HOME_NET_SCAN_CONTROL_EVENTS_SEVERITY`	Важность событий, полученных при сканировании контролируемой сети	`low`
`SCRIPT_VERIFICATION_EVENTS_SEVERITY`	Важность событий верификации скриптов	`low`
`SYSTEM_CONTROL_EVENTS_SEVERITY`	Важность системных событий	`low`
`IDS_CONTROL_EVENTS_SEVERITY`	Важность событий службы обнаружения вторжений	`critical`
`DPI_CONTROL_EVENTS_SEVERITY`	Важность событий `dpi_notice`	`critical`

Табл. 142. Дополнительные переменные файла `manager.env`

ПЕРЕМЕННАЯ	ОПИСАНИЕ	ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ (ЖИРНЫМ), ЛИБО ПРИМЕР
`ML_CONTROL_EVENTS_SEVERITY`	Важность событий `ml_notice`	`critical`
`SESSION_CONTROL_EVENTS_SEVERITY`	Важность событий, связанных с сетевыми соединениями	`critical`
`FSTEC_MAPPINGS_ENABLED`	При значении переменной `false`: • скрывает на странице **Импорт и экспорт** импорт справочника БДУ ФСТЭК России; • скрывает в окне **Просмотр уязвимостей** столбец **БДУ ФСТЭК** с дополнительной информацией об уязвимостях из БДУ ФСТЭК России; • скрывает в CSV-отчете результатов поиска уязвимостей столбцы с дополнительной информацией об уязвимостях из БДУ ФСТЭК России	`true`
`OVAL_IMPORT_TIMEOUT_MINUTES`	Время, по истечении которого импорт OVAL-групп завершается с ошибкой. Значение задается в минутах	`10`
`ENABLE_DNS_PINNING_PROTECTION`	Включение защиты от атаки Anti DNS Pinning. При значении переменной `true` веб-сервер будет отправлять 404 ошибку, если запрос пришел на адрес, не равный CN серверного сертификата	`false`
`API_TOKEN_SECRET`	Ключ, необходимый для подписи токена доступа по REST API	`dJ2ZOZeU0nJhHwjfhqlOwF1x`
`CPE_PRODUCT_THRESHOLD`	Пороговое значение для сопоставления наименования ПО актива при поиске уязвимостей	`0.6`
`CPE_VENDOR_THRESHOLD`	Пороговое значение для сопоставления поставщика ПО актива при поиске уязвимостей	`0.6`
`CPE_VERSION_THRESHOLD`	Пороговое значение для сопоставления версии ПО актива при поиске уязвимостей	`0.95`

Табл. 142. Дополнительные переменные файла `manager.env`

ПЕРЕМЕННАЯ	ОПИСАНИЕ	ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ (ЖИРНЫМ), ЛИБО ПРИМЕР
`REPOS_DIR`	Директория, в которой располагаются репозитории для модуля «Управление проектами ПЛК»	`/var/lib/udv/cv-repos-backend/repositories`
`EVENT_SYSLOG_SEND`	При значении переменной `true` выполняется отправка внутренних событий во внешние системы по протоколу Syslog	`false`
`EVENT_SYSLOG_HOST`	IP-адрес внешнего сервера, используемого для передачи событий по протоколу Syslog	`127.0.0.1`
`EVENT_SYSLOG_PORT`	Порт, используемый для отправки внутренних событий по протоколу Syslog	`514`
`EVENT_SYSLOG_PROTOCOL`	Протокол передачи внутренних событий по Syslog. Возможные варианты значения переменной: • TCP; • UDP.	`UDP`
`EVENT_SYSLOG_FACILITY`	Категория источника внутренних событий при их передаче во внешние системы по Syslog	`LOC0`
`EVENT_SYSLOG_SEVERITY`	Уровень критичности сообщений о передаче внутренних событий во внешние системы по Syslog. Доступны следующие значения переменной: • `INFORMATIONAL` • `CRITICAL` При значении переменной `INFORMATIONAL` будут отображаться информационные сообщения. При значении переменной `CRITICAL` будут отображаться информационные сообщения, а также сообщения о состоянии системы, сообщения об ошибках, предупреждения о возможных проблемах	`INFORMATIONAL`

Табл. 142. Дополнительные переменные файла `manager.env`

ПЕРЕМЕННАЯ	ОПИСАНИЕ	ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ (ЖИРНЫМ), ЛИБО ПРИМЕР
`SV_EVENTS_QUEUE_MAX_LENGTH`	Максимальная длина очереди для отправки событий репозиториев на UDV Supervision. Минимальное значение — `100`	`200000`

Переменные сервиса udv-prometheus

Переменные сервиса `udv-prometheus` устанавливаются в директории `/etc/sysconfig/udv-prometheus`

Список переменных сервиса `udv-prometheus` Комплекса уровня Management, представлен в таблице ниже.

Табл. 143. Список переменных сервиса udv-prometheus

ПЕРЕМЕННАЯ	ОПИСАНИЕ	ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ (ЖИРНЫМ), ЛИБО ПРИМЕР
`MAX_DISK_SPACE_CONSUMED_PERCENTAGE`	Лимит заполнения ПЗУ (HDD, SSD) операционной системы Комплекса. Значение задается в процентах	`80`
`MAX_CPU_LOAD_CONSUMED_PERCENTAGE`	Лимит нагрузки на центральный процессор (CPU) операционной системы Комплекса. Значение задается в процентах	`80`
`MAX_LA`	Лимит средней нагрузки (Load average) операционной системы Комплекса. Значение задается в количестве ядер	`8`
`MAX_RAM_CONSUMED_PERCENTAGE`	Максимальный допустимый объем используемой оперативной памяти. Значение задается в процентах	`90`
`RMQ_LOW_AVAILABLE_DISK_SPACE_WATERMARK_BYTES`	Минимальный уровень свободного дискового пространства для брокера сообщений `rabbitmq`, при достижении которого в веб-интерфейсе появляется соответствующее событие 1180013, а при его нормализации появляется событие 1180014. Значение задается в байтах	`500000000`

Табл. 143. Список переменных сервиса udv-prometheus

ПЕРЕМЕННАЯ	ОПИСАНИЕ	ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ (ЖИРНЫМ), ЛИБО ПРИМЕР
`RMQ_LOW_AVAILABLE_MEMORY_WATERMARK_BYTES`	Минимальный уровень свободной оперативной памяти для брокера сообщений `rabbitmq`, при достижении которого в веб-интерфейсе появляется соответствующее событие 1180011, а при его нормализации появляется событие 1180012. Значение задается в байтах	`500000000`
`PUSHGATEWAY_MAX_DELAY_METRICS`	Максимальный интервал задержки между отправкой значений в систему мониторинга. Значение задается в секундах	`600`

Переменные сервиса udv-logstash

Переменные сервиса `udv-logstash` устанавливаются в директории `/etc/sysconfig/udv-logstash`

Список переменных сервиса `udv-logstash` Комплекса уровня Management, представлен в таблице ниже.

Табл. 144. Список переменных сервиса udv-logstash

ПЕРЕМЕННАЯ	ОПИСАНИЕ	ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ (ЖИРНЫМ), ЛИБО ПРИМЕР
`LOG_LEVEL`	Минимальная критичность системных событий, которые генерирует Комплекс уровня Management. Возможные значения: • `CRITICAL` • `FATAL` • `ERROR` • `WARNING` • `INFO` • `DEBUG` • `NOTSET`	`INFO`

Табл. 144. Список переменных сервиса udv-logstash

ПЕРЕМЕННАЯ	ОПИСАНИЕ	ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ (ЖИРНЫМ), ЛИБО ПРИМЕР
`ESPER_PORT`	Порт сервиса корреляции событий	`517`
`LS_JAVA_OPTS`	Объем оперативной памяти, выделяемой под сервис `udv-logstash`. Значение задается в мегабайтах	`-Dlog4j2.formatMsgNoLookups=true-Xmx1024m-Xms1024m`
`INDEX_NAME`	Наименование индексов событий Комплекса	`"datapk-events-%{+YYYY.MM.dd}"`
`TEMPLATE_NAME`	Наименование шаблона событий Комплекса	`"datapk-event.json"`

Переменные сервиса udv-opensearch

Переменные сервиса `udv-opensearch` устанавливаются в директории `/etc/sysconfig/udv-opensearch`

Список переменных сервиса `udv-opensearch` Комплекса уровня Management представлен в таблице ниже.

Табл. 145. Список переменных сервиса udv-opensearch

ПЕРЕМЕННАЯ	ОПИСАНИЕ	ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ (ЖИРНЫМ), ЛИБО ПРИМЕР
`ES_JAVA_OPTS`	Объем оперативной памяти, выделяемой под сервис `opensearch`. Задается в мегабайтах	`-Dlog4j2.formatMsgNoLookups=true-Xmx1024m-Xms1024m`
`OPENSEARCH_PATH_CONF`	Директория, в которой расположен конфигурационный файл сервиса `opensearch`	`/etc/opensearch`

Табл. 145. Список переменных сервиса udv-opensearch

ПЕРЕМЕННАЯ	ОПИСАНИЕ	ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ (ЖИРНЫМ), ЛИБО ПРИМЕР
`OPENSEARCH_STARTUP_SLEEP_TIME`	Время ожидания перед началом проверки успешного запуска сервиса `opensearch`	`5`
`OPENSEARCH_SD_NOTIFY`	При значении переменной `true` в систему будут отправляться уведомления `systemd`	`true`

Переменные сервиса udv-esper

Переменные сервиса `udv-esper` устанавливаются в директории `/etc/sysconfig/udv-esper`

Список переменных сервиса `udv-esper` Комплекса уровня Management, представлен в таблице ниже.

Табл. 146. Список переменных сервиса udv-esper

ПЕРЕМЕННАЯ	ОПИСАНИЕ	ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ (ЖИРНЫМ), ЛИБО ПРИМЕР
`ESPER_RMQ_MAX_QUEUE_SIZE`	Максимальный размер очереди сервиса `udv-rabbitmq` для отправки событий на корреляцию. Задается в количестве сообщений	`100000`
`ESPER_JAVA_OPTS`	Объем оперативной памяти, выделяемой под сервис корреляции событий. Задается в мегабайтах	`-Djava.net.prefer-IPv4Stack=true-Dlog4j2.format-MsgNoLookups=true-Xmx1024m`
`JETTY_PORT`	Порт сервера `Jetty`, по которому доступен API модуля «Управление внешними событиями»	`10007`
`ESPER_STARTUP_TIMEOUT`	Задержка при запуске модуля «Управление внешними событиями». Значение переменной задается в секундах	`180`
`HOST_MANAGER_API_PORT`	Порт API, по которому доступен модуль управления узлами	`10012`

Табл. 146. Список переменных сервиса udv-esper

ПЕРЕМЕННАЯ	ОПИСАНИЕ	ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ (ЖИРНЫМ), ЛИБО ПРИМЕР
`ESPER_ELASTICSEARCH_HOST`	IP-адрес узла, используемого модулем «Управление внешними событиями»	`127.0.0.1`
`ESPER_ELASTICSEARCH_PORT`	Порт, по которому доступен модуль «Управление внешними событиями»	`9200`
`ESPER_INCIDENT_ANALYSIS`	При значении переменной `disabled` функция повторной обработки инцидентов будет недоступна	`disabled`
`ESPER_ELASTICSEARCH_BATCH_COUNT`	Количество записей из модуля «Управление внешними событиями», читаемых за одну минуту	`2000`
`ESPER_RETRO_TIME_FIELD`	Название поля, по которому сортируются события при запросе	`create_time`
`ESPER_RETRO_SCROLL_TIMEOUT_MIN`	Задержка при выполнении запроса к модулю «Управление внешними событиями». Значение переменной задается в минутах	`3`
`ESPER_MAX_SERVICE_INFO_SIZE`	Максимальное количество сообщений о состоянии службы, хранимое в оперативной памяти	`50`
`ESPER_EVENT_COUNTER_INTERVAL`	Интервал между выводом счетчика внешних событий, полученных при текущем анализе. Значение переменной задается в миллисекундах	`300000`
`ESPER_INCIDENT_SENDER_CONNECT_TIMEOUT_MS`	Задержка установления соединения с модулем управления инцидентами. Значение переменной задается в миллисекундах	`1000`
`ESPER_INCIDENT_SENDER_READ_TIMEOUT_MS`	Задержка времени ответа о создании инцидента от модуля управления инцидентами. Значение переменной задается в миллисекундах	`5000`
`ESPER_INCIDENT_SENDER_THREADPOOL_SIZE`	Объем потоков, используемого для связи с модулем управления инцидентов	`40`

Табл. 146. Список переменных сервиса udv-esper

ПЕРЕМЕННАЯ	ОПИСАНИЕ	ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ (ЖИРНЫМ), ЛИБО ПРИМЕР
`INCIDENT_MANAGER_API_PORT`	Порт API, по которому доступен модуль управления инцидентами	`10011`
`API_CONNECTION_RETRY_COUNT`	Количество повторных попыток подключения к API Комплекса	`3`

Переменные сервиса udv-vector-manager

Переменные сервиса `udv-vector-manager` устанавливаются в директории `/lib/systemd/system/udv-vector.service`

Список переменных сервиса `udv-vector-manager` Комплекса уровня Management представлен в таблице ниже.

Табл. 147. Список переменных сервиса udv-vector-manager

ПЕРЕМЕННАЯ	ОПИСАНИЕ	ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ (ЖИРНЫМ), ЛИБО ПРИМЕР
`BUFFER_SIZE`	Размер буфера одного обработчика в сервисе `udv-vector-manager` (один обработчик — один протокол). Задается в байтах	`268435488`
`MANAGER_NETWORK_GATEWAY`	Адрес для отправки данных в сервис `udv-clickhouse`	`127.0.0.1`

Переменные сервиса udv-zeek-backend

Если Комплекс еще не запускался, переменные сервиса `udv-zeek-backend` устанавливаются в файле `manager.env` в директории `/usr/share/udv/datapk/manager.env`.

Если Комплекс уже запускался, переменные сервиса `udv-zeek-backend` устанавливаются с помощью запроса в базу данных `Redis` (см. инструкцию «Установка переменных модуля «Анализ промышленного сетевого трафика» через запрос в Redis»).

Список переменных сервиса `udv-zeek-backend` Комплекса уровня Management представлен в таблице ниже.

Табл. 148. Список переменных сервиса udv-zeek-backend

ПЕРЕМЕННАЯ	ОПИСАНИЕ	ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ (ЖИРНЫМ), ЛИБО ПРИМЕР
`DPI_PASSWORD_CAPTURE`	При значении переменной `true` обрабатываются пароли в трафике HTTP	`false`

Переменные сервиса udv-rules-backend

Если Комплекс еще не запускался, переменные сервиса `udv-rules-backend` устанавливаются в файле `manager.env` в директории `/usr/share/udv/datapk/manager.env`.

Если Комплекс уже запускался, переменные сервиса `udv-rules-backend` устанавливаются через запрос в базу данных `Redis` (см. инструкцию «Установка переменных модуля «Анализ промышленного сетевого трафика» через запрос в Redis»).

Список переменных сервиса `udv-rules-backend` Комплекса уровня Management представлен в таблице ниже.

Табл. 149. Список переменных сервиса udv-rules-backend

ПЕРЕМЕННАЯ	ОПИСАНИЕ	ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ (ЖИРНЫМ), ЛИБО ПРИМЕР
`SESSION_RULES_ENABLED`	При значении переменной `true` будет включен сервис правил сессий	`true`

См. также

Переменные службы обнаружения вторжений

Конфигурационные файлы модуля «EDR for PLC»

Рекомендации по использованию переменных файлов manager.env и sensor.env

22.5.1.1. Установка переменных модуля «Анализ промышленного сетевого трафика» через запрос в Redis

Инструкция применима для установки переменных сервисов udv-zeek-backend и udv-rules-backend на Комплексе, который уже запускался.

Для установки переменных через запрос в базу данных `Redis` в терминале сервера, на котором установлен Комплекс уровня Management:

1. Подключитесь к базе данных `Redis` командой:

```
redis-cli
```

2. Выполните запрос текущих настроек сервиса:

    a. Для сервиса `udv-zeek-backend` введите команду:

    ```
    get /v1/nodes/[node_id]/v1/zeek/service/settings/items/
    ```

    б. Для сервиса `udv-rules-backend` введите команду:

    ```
    get /v1/nodes/[node_id]/v1/rules/settings/items/
    ```

    Где `[node_id]` — идентификатор сенсора, на котором требуется установить переменные. Например, `fc30d73435387abbfbb61c10676106ae`.

    > Подсказка:
    >
    > Узнать `node_id` можно командой:
    >
    > ```
    > curl -X GET http://127.0.0.1:32456/sensors_nodes
    > ```

3. Скопируйте в любой текстовый редактор вывод команды, полученный в шаге 2, и измените в нем значения переменных (подробнее о переменных см. пункты «Переменные сервиса udv-zeek-backend» и «Переменные сервиса udv-rules-backend» раздела «Переменные Комплекса уровня Management»).
4. Выполните команду, подставив в нее значение `node_id` и строку из шага 3 с новыми настройками:

    ```
    set /v1/nodes/[node_id]/v1/zeek/service/settings/items/ [новые_настройки]
    ```

22.5.2. Переменные Комплекса уровня Sensor

Обязательные переменные файла sensor.env

Переменные файла `sensor.env` устанавливаются в директории `/usr/share/udv/datapk`

Список обязательных переменных, содержащийся в файле `sensor.env` Комплекса уровня Sensor, представлен в таблице ниже.

Табл. 150. Обязательные переменные файла `sensor.env`

ПЕРЕМЕННАЯ	ОПИСАНИЕ	ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ (ЖИРНЫМ), ЛИБО ПРИМЕР
`MANAGER_NODE_ADDRESS`	IP-адрес для подключения сенсора к Комплексу уровня Management. Значение `127.0.0.1` задается в случае, если сенсор и Management установлены на одном сервере.	`127.0.0.1`
`LISTENING_INTERFACES`	Наименования всех интерфейсов, с которых сенсор анализирует трафик. Можно указывать интерфейсы в любом режиме (не только прослушивания трафика). Интерфейсы перечисляются через запятую без пробелов. Все интерфейсы должны быть в состоянии up, иначе сенсор не сможет корректно инициализироваться. ⚠ Внимание: Запись трафика в файлы `.pcap` модулем «Управление сетевым трафиком» будет доступна только для первого интерфейса из перечисленных в переменной. Если необходимо записывать трафик с нескольких интерфейсов, создайте для них единый виртуальный интерфейс (bond) — подробнее см. в разделе «Создание единого виртуального интерфейса (bond) для прослушивания и записи трафика с нескольких физических интерфейсов» Руководства по внедрению и поддержке.	`ens32,ens33,ens35,dummy0`
`LOG_LEVEL`	Минимальная критичность системных событий, которые генерирует Комплекс уровня Management. Возможные значения: • `CRITICAL` • `FATAL` • `ERROR` • `WARNING` • `INFO`	`INFO`

Табл. 150. Обязательные переменные файла `sensor.env`

ПЕРЕМЕННАЯ	ОПИСАНИЕ	ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ (ЖИРНЫМ), ЛИБО ПРИМЕР
	• `DEBUG` • `NOTSET`	

Дополнительные переменные файла sensor.env

Переменные, которые не включены в автоматически генерируемый файл `sensor.env` Комплекса уровня Sensor и добавляются при необходимости, указаны в таблице ниже.

Табл. 151. Дополнительные переменные файла `sensor.env`

ПЕРЕМЕННАЯ	ОПИСАНИЕ	ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ (ЖИРНЫМ), ЛИБО ПРИМЕР
`TERMINAL_CONNECTOR_SSH_TIMEOUT`	Максимальное время ожидания выполнения задачи сбора данных по протоколу SSH. Задается в секундах	`30`
`COMMAND_PROCESSOR_WORKER_MAX_MEMORY_LIMIT_MB`	Лимит памяти для обработки одного процесса сбора данных. При превышении лимита в результаты сбора выводится ошибка `Сбор данных был прерван в результате обнаружения большего объема данных, чем ожидалось.` Задается в мегабайтах	`256`
`MIBS_TO_COMPILE`	Список MIB-словарей для интерпретации данных, получаемых с сетевых устройств помощью сканеров сбора данных по протоколу SNMP	`<mib1>`, `<mib2>`
`COMMAND_PROCESSOR_USER_SCRIPT_MODULES`	Список Python-модулей, доступных для сканеров сбора данных	`re, string, unicodedata, hashlib,datetime, _strptime, textwrap, struct,dbfread, dateutil, dateutil.tz, parsel, random`

Переменные модуля «EDR for PLC»

Переменные модуля UDV DATAPK EDR for PLC устанавливаются в директории `/opt/sensor/.env`

Список переменных сервиса модуля UDV DATAPK EDR for PLC Комплекса уровня Sensor представлен в таблице ниже.

Табл. 152. Список переменных модуля «EDR for PLC»

ПЕРЕМЕННАЯ	ОПИСАНИЕ	ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ (ЖИРНЫМ), ЛИБО ПРИМЕР
`LOG_LEVEL`	Минимальная критичность системных событий, которые генерирует модуль	`INFO`
`CONTROLLER_API_PORT`	Порт для доступа к API модуля	`8081`
`SOCKET_HOST`	Адреса, с которых доступно API управления модулем	`0.0.0.0`
`DB_PATH`	Путь до базы данных внутри контейнера модуля «EDR for PLC»	`/db/store.db`
`TZ`	Часовой пояс	`Asia/Yekaterinburg`

Переменные сервиса udv-zeek-wrapper

Переменные сервиса `udv-zeek-wrapper` устанавливаются в директории `/lib/systemd/system/udv-zeek-wrapper.service`

Список переменных сервиса `udv-zeek-wrapper` Комплекса уровня Sensor представлен в таблице ниже.

Табл. 153. Список переменных сервиса udv-zeek-wrapper

ПЕРЕМЕННАЯ	ОПИСАНИЕ	ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ (ЖИРНЫМ), ЛИБО ПРИМЕР
`ZEEK_ROTATION_INTERVAL`	Период ротации системных журналов сервиса `udv-zeek-wrapper`. Задается в минутах	1
`ARCHIVE_COMPRESS_LOG`	Перевод создаваемых копий журналов событий сервиса `udv-zeek-wrapper` в сжатый формат хранения при значении `true`.	`true`

Табл. 153. Список переменных сервиса udv-zeek-wrapper

ПЕРЕМЕННАЯ	ОПИСАНИЕ	ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ (ЖИРНЫМ), ЛИБО ПРИМЕР
	ОСТОРОЖНО: Изменение значения переменной может привести к отказу в работе a.	
`ARCHIVE_COPY_LOG`	Создание копии журналов событий сервиса `udv-zeek` при значении `true`. ОСТОРОЖНО: Изменение значения переменной может привести к отказу в работе a.	`false`

Переменные сервиса udv-dns-classifier

Переменные сервиса `udv-dns-classifier` устанавливаются в директории `/etc/sysconfig/udv-dns-classifier`

Список переменных сервиса `udv-dns-classifier` Комплекса уровня Sensor представлен в таблице ниже.

Табл. 154. Список переменных сервиса udv-dns-classifier

ПЕРЕМЕННАЯ	ОПИСАНИЕ	ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ (ЖИРНЫМ), ЛИБО ПРИМЕР
`REQUEST_LOG_THRESHOLD`	Граница вероятности, с которой события считаются туннелями для dns_request-модели	`0.8`
`RESPONSE_LOG_THRESHOLD`	Граница вероятности, с которой события считаются туннелями для dns_-response-модели	`0.8`
`REQUEST_ANOMALY_THRESHOLD`	Граница вероятности, с которой события dns_request отправляются в сервис `udv-event-manager`	`0.5`

Табл. 154. Список переменных сервиса udv-dns-classifier

ПЕРЕМЕННАЯ	ОПИСАНИЕ	ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ (ЖИРНЫМ), ЛИБО ПРИМЕР
`RESPONSE_ANOMALY_THRESHOLD`	Граница вероятности, с которой события dns_response отправляются в сервис `udv-event-manager`	`0.75`
`DGA_ANOMALY_THRESHOLD`	Граница вероятности, с которой DGA-события отправляются в сервис `udv-event-manager`	**0.75**
`DGA_LOG_THRESHOLD`	Граница вероятности, с которой события считаются DGA	`0.75`
`DEBUG_MODE`	Перевод сервиса `udv-dns-classifier` в debug-режим при значении `true`. При этом модели сервиса сохраняют на диск датафреймы с результатами работы. ОСТОРОЖНО: Изменение значения переменной может привести к отказу в работе а.	`false`

См. также

Переменные службы обнаружения вторжений

Конфигурационные файлы модуля «EDR for PLC»

Рекомендации по использованию переменных файлов manager.env и sensor.env

22.5.3. Переменные Комплекса уровня Supervision

Конфигурационный файл .env с переменными устанавливается в директории `/usr/share/udv/supervision`

Список обязательных переменных представлен в таблице ниже.

Табл. 155. Обязательные переменные файла env

ПЕРЕМЕННАЯ	ОПИСАНИЕ	ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ (ЖИРНЫМ) ИЛИ ПРИМЕР
`NGINX_HTTPS_PORT`	Порт для подключения по протоколу HTTPS. Возможные значения: от 1 до 65534.	`443`
`HOST_IP`	IP-адрес для перехода в интерфейс Супервижн в браузере.	`172.16.100.200`
`LOG_LEVEL`	Минимальная критичность системных событий, которые генерирует Супервижн. Возможные значения: • `DEBUG` • `INFO` • `WARNING` • `ERROR` • `CRITICAL`	`INFO`
`DB_PASS`	Пароль доступа к базе данных. ⚠ Внимание: Изменение значения переменной может привести к отсутствию доступа к базе данных	`P@ssw0rd`
`VPN_NETWORK`	Подсеть VPN для связи с Менеджментами	`172.16.0.0/24`
`PROMETHEUS_RETENTION_TIME_DAYS`	Предельный срок хранения метрик Prometheus (в днях). Требуется для отображения исторических данных в виджете «Динамика» на странице «Обзор». Возможные значения: от 30 до 1095 (три года)	`30`

Табл. 155. Обязательные переменные файла env

ПЕРЕМЕННАЯ	ОПИСАНИЕ	ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ (ЖИРНЫМ) ИЛИ ПРИМЕР
`MAX_CHANGE_EVENTS_AGE_DAYS`	Предельный срок хранения записей об изменениях в репозиториях (в днях). Требуется для отображения исторических данных в виджете «Просмотр панели виджетов «Контроль версий»» на странице «Контроль версий». Возможные значения: от 90 до 1095 (три года)	`90`
`DATAPK_EVENTS_RETENTION_DAYS`	Предельный срок хранения событий из DATAPK (в днях). Требуется для отображения исторических данных в виджете «События репозиториев» на странице «Контроль версий». Возможные значения: от 90 до 1095 (три года)	`90`
`USER_SESSION_INACTIVITY_TIMEOUT`	Ограничение сессии при отсутствии активности пользователя (в секундах). Возможные значения: от 300	`600`

22.5.4. Переменные службы обнаружения вторжений

Для службы обнаружения вторжений Комплекса уровня Sensor устанавливается конфигурационный файл с набором переменных, расположенный в директории `/etc/sysconfig/suricata-wrapper`.

Значения переменных указываются следующим образом:

- одиночный IP-адрес или порт указываются в следующем формате: `20` или `192.168.0.0`;
- несколько IP-адресов указываются в следующем формате: `[192.168.0.0/16,10.0.0.0/8,172.16.0.0/12]`;
- несколько портов указываются в следующем формате: `[20,21]`.

Список переменных, содержащихся в данного конфигурационном файле, представлен в таблице ниже.

Табл. 156. Переменные службы обнаружения вторжений

ПЕРЕМЕННАЯ	ОПИСАНИЕ	ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ (ЖИРНЫМ), ЛИБО ПРИМЕР
ADDRESS_VARIABLEA	Переменные для добавления пользовательского IP-адреса или диапазона IP-адресов	$HOME_NET
ADDRESS_VARIABLEB		
ADDRESS_VARIABLEC		
ADDRESS_VARIABLED		
AIM_SERVERS	Домашняя (контролируемая) сеть серверов AIM (AOL Instant Messenger)	$EXTERNAL_NET
DC_SERVERS	Домашняя (контролируемая) сеть серверов DC (Domain Controllers)	$HOME_NET
DNP3_CLIENT	Домашняя (контролируемая) сеть клиентов DNP3-протокола	$HOME_NET
DNP3_PORT	Порты DNP3-протокола	20000
DNP3_SERVER	Домашняя (контролируемая) сеть серверов DNP3	$HOME_NET
DNS_SERVERS	Домашняя (контролируемая) сеть серверов DNS	$HOME_NET
ENIP_CLIENT	Домашняя (контролируемая) сеть клиентов ENIP-протокола	$HOME_NET
ENIP_SERVER	Домашняя (контролируемая) сеть серверов ENIP	$HOME_NET
EXTERNAL_NET	IP-адреса, не входящих в домашнюю (контролируемую) сеть	!$HOME_NET
FILE_DATA_PORTS	Порты, через которые выполняется передача файлов	[$HTTP_PORTS,110,143]
FTP_PORTS	Порты, используемые для соединения по протоколу FTP	21

Табл. 156. Переменные службы обнаружения вторжений

ПЕРЕМЕННАЯ	ОПИСАНИЕ	ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ (ЖИРНЫМ), ЛИБО ПРИМЕР
HOME_NET	IP-адреса домашней (контролируемой) сети	[192.168.0.0/16,10.0.0.0/8,172.16.0.0/12]
HTTP_PORTS	Порты, используемые для HTTP-трафика	80
HTTP_SERVERS	Домашняя (контролируемая) сеть HTTP-серверов	$HOME_NET
MODBUS_CLIENT	Домашняя (контролируемая) сеть клиентов протокола Modbus	$HOME_NET
MODBUS_PORTS	Порты протокола Modbus	502
MODBUS_SERVER	Домашняя (контролируемая) сеть серверов Modbus	$HOME_NET
ORACLE_PORTS	Порты для подключения к серверам Oracle	1521
PORT_VARIABLEA	Переменные для добавления пользовательского порта, предназначенного для определенных протоколов	!80
PORT_VARIABLEB		
PORT_VARIABLEC		
PORT_VARIABLED		
SHELLCODE_PORTS	Порты, на которых выполняется мониторинг попыток выполнения shell-кодов	!80
SMTP_SERVERS	Домашняя (контролируемая) сеть SMTP-серверов	$HOME_NET
SQL_SERVERS	Домашняя (контролируемая) сеть серверов баз данных SQL	$HOME_NET

Табл. 156. Переменные службы обнаружения вторжений

ПЕРЕМЕННАЯ	ОПИСАНИЕ	ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ (ЖИРНЫМ), ЛИБО ПРИМЕР
`SSH_PORTS`	Домашняя (контролируемая) сеть SSH-серверов	`22`
`TELNET_SERVERS`	Домашняя (контролируемая) сеть Telnet-серверов	`$HOME_NET`

22.5.5. Конфигурационные файлы модуля «EDR for PLC»

Для настройки модуля UDV DATAPK EDR for PLC используются файлы, описанные в таблице ниже. Конфигурационные файлы UDV DATAPK EDR for PLC хранятся и настраиваются в Комплексе уровня Sensor.

Табл. 157. Конфигурационные файлы модуля «EDR for PLC»

ФАЙЛ	ДИРЕКТОРИЯ, В КОТОРОЙ РАСПОЛОЖЕН ФАЙЛ	НАЗНАЧЕНИЕ ФАЙЛА
`protocol-fields.yaml`	`/opt/sensor/protocol-fields.yaml`	Используется для классификации полей сетевых протоколов
`.env`	`/opt/sensor/.env`	Используется для настройки переменных окружения модуля UDV DATAPK EDR for PLC
`configuration.yaml`	`/opt/sensor/configuration.yaml`	Основной файл конфигурации, которые определяет набор и параметры моделей

22.5.5.1. Файл protocol-fields.yaml

Файл `protocol-fields.yaml` предназначен для классификации полей сетевых протоколов с целью их последующей обработки в аналитической системе.

Описание классов полей представлено в таблице ниже.

Табл. 158. Описание классов полей в файле protocol-fields.yaml

КЛАСС	ОПИСАНИЕ	ХАРАКТЕРИСТИКИ
`address`	Используется для определения полей, содержащих адресную информацию для маршрутизации данных	• Эти поля содержат идентификаторы узлов или сервисов (например: IP-адрес, TCP-порт); • Используются только для маршрутизации данных до целевой модели; • Не передаются в модель для анализа.
`payload`	Используется для определения полей, содержащих полезную нагрузку для анализа моделями	• Эти поля передаются на анализ в модели; • Обычно содержат данные о состоянии или управлении технологическим процессом; • Для моделей на основе гибридного автомата набор анализируемых полей задается в `configuration.yaml`.
`other`	Используется для определения полей, исключаемых из анализа	• Такие поля игнорируются при анализе; • Обычно содержат случайно генерируемые или нерелевантные данные; • Включение таких полей в анализ снижает точность моделей.

22.5.5.2. Файл .env

В данном файле настраиваются следующие переменные:

- `LOG_LEVEL`;
- `CONTROLLER_API_PORT`;
- `SOCKET_HOST`;
- `DB_PATH`;
- `TZ`.

Подробное описание переменных приведено в разделе «Переменные модуля «EDR for PLC»».

22.5.5.3. Файл configuration.yaml

Файл `configuration.yaml` состоит из следующих блоков:

1. Блок входных данных модуля — определяет параметры приема проанализированного трафика от механизма DPI.
2. Блок выходных данных модуля — определяет способ отправки событий модуля в вышестоящие системы. Существует два способа отправки событий:
   - с помощью сервиса `udv-rabbitmq` — основной способ отправки событий, настраиваемый при установке Комплекса;
   - по протоколу Syslog — альтернативный способ отправки событий с поддержкой стандарта RFC 5424/UDP.

> ⚠ Внимание:
>
> При отправке в сторонние системы необходимо проверить настройки межсетевого экранирования.

3. Блок контроллера моделей — определяет перечень моделей анализа и их параметры. Для конфигурации модели необходимо указать следующие данные:
   - способ представления модели;
   - адресная информация конечных точек для анализа;
   - специфичные параметры модели.

> ℹ Прим.:
>
> Для каждого типа модели и набора конечных точек определяются специфичные параметры. Если определенный тип модели не указан для набора конечных точек, соответствующий блок параметров не включается в конфигурацию.

При определении конечных точек доступны два режима сопоставления адресов:

- `starts_with` — адресная информация сетевого взаимодействия должна начинаться с адресов, указанных в поле `layers`;
- `equal` — адресная информация сетевого взаимодействия должна точно соответствовать адресам конечных точек из поля `layers`. Данный режим обеспечивает более строгую фильтрацию по сравнению с режимом `starts_with`.

Пример

Пример режима сопоставления `starts_with`:

Для узла с настройкой IP `192.168.1.1` будут обрабатываться все соединения с данного IP-адреса, для узла `192.168.1.2:102` — соединения с указанного IP и TCP-порта `102`.

Результирующий анализ: `192.168.1.1:* ↔ 192.168.1.2:102`

Подробное содержание файла `configuration.yaml`, формируемое по умолчанию, представлено ниже.

```
# Блок входных данных модуля

# Получение проанализированного трафика от механизма DPI
socket_config:
  enabled: true

# Блок входных данных модуля

# Конфигурация отправки событий по syslog (rfc5424/udp)
syslog:
  - enabled: false # активность отправки по syslog
    ip_or_domain: logstash # ip-адрес или DNS имя хоста для отправки событий
    port: 5514 # порт для отправки событий
    models_metrics:
      enabled: true # активность отправки событий о текущих метриках моделей
      send_interval: 30 # интервал отправки событий о текущих метриках моделей

# Конфигурация отправки событий в RabbitMQ
rabbitmq_config:
    enabled: true  # активность отправки в RabbitMQ
    host: '127.0.0.2' # ip-адрес или DNS имя хоста для отправки событий
    port: 5672 # порт для отправки событий
    models_metrics:
      enabled: true # активность отправки событий о текущих метриках моделей
      send_interval: 30 # интервал отправки событий о текущих метриках моделей

# Конфигурация контроллера моделей
models_controller_config:
  nodes_configurations: # далее идет задание моделей
    - models: [otala, qdict, hybrid_automaton] # указывается тип моделей для следующих далее конечных точек взаимодействия, доступны три варианта: otala
 и/или qdict и/или hybrid_automaton
      first_node: # описание первой конечной точки
```

```
      mode: 'starts_with' # режим сопоставления адресной информации
      layers: # уровни представления адресной информации (их может быть несколько, важно соблюдать порядок согласно модели OSI)
        - value: '192.168.1.1' # значение, которое учитывается в адресной информации
          protocol: 'ip' # сетевой протокол, для которого учитывается указанное выше значение
          format: 'ip' # формат, в котором задается значение в поле value
    second_node: # описание второй конечной точки
      mode: 'starts_with' # режим сопоставления адресной информации
      layers: # уровни представления адресной информации (их может быть несколько)
        - value: '192.168.1.2' # значение, которое учитывается в адресной информации
          protocol: 'ip' # сетевой протокол, для которого учитывается указанное выше значение
          format: 'ip' # формат, в котором задается значение в поле value
          - value: '1f6' # значение, которое учитывается в адресной информации (для hex формата указывается без лидирующих нулей, например, в данном
случае это 502 порт)
          protocol: 'tcp' # сетевой протокол, для которого учитывается указанное выше значение
          format: 'hex' # формат, в котором задается значение в поле value
    qdict_configuration: # конфигурация модели на основе иерархического словаря (для взаимодействия, описанного выше)
      separation: # управление режимом формирования маски данных
        enabled: false # активность режима формирования маски данных (поддерживается только для протокола CIP)
      max_stagnation_number: 10 # условие сходимости модели
      max_buffer_len: 10000 # предельный размер буфера данных при формировании иерархического словаря (фактически определяет "глубину" иерархии)
      max_qdict_len: 100000 # предельное количество записей в иерархическом словаре
      validation: # блок настроек режима валидации для модели
        min_checks_count_before_validation: 1000 # минимальный размер данных (запрос-ответ) необходимых для выполнения валидации модели
       min_probability_of_correct_prediction: 50.0 # минимальная предсказательная способность модели (в %), необходимая для успешного прохождения валидации
    otala_configuration: # конфигурация модели на основе временного автомата (для взаимодействия, описанного выше)
      separation: # управление режимом формирования маски данных (поддерживается только для протокола CIP)
        enabled: true # активность режима формирования маски данных
        max_group_commands_count: 100 # количество команд одной группы CIP, которое необходимо накопить для начала расчета энтропии
        entropy_threshold: 0.5 # пороговое значение энтропии, определяющее попадание в маску данных
      convergence_number_max: null # условие сходимости модели
    hybrid_automaton_configuration: # конфигурация модели на основе гибридного автомата (для взаимодействия, описанного выше)
      controlled_data: # определение областей памяти протокола Modbus, которые будут переданы в модель
        discrete_inputs: [0,1,2] # перечень анализируемых дискретных входов
```

```
        coils: [8,9,10,17,21] # перечень анализируемых регистров флагов
        input_registers: [] # перечень анализируемых входных регистров
        holding_registers: [45,32] # перечень анализируемых регистров хранения
      controlled_func: [1,2,3,4] # перечень номеров анализируемых функций протокола Modbus
      modbus_detectors: # описание активности и параметров modbus детекторов в рамках модели на основе гибридного автомата
        detector_new_tags: # детектор для контроля используемых областей памяти в рамках обмена по протоколу modbus
          enabled: true # состояние активности данного детектора
        detector_exception: # детектор для сигнализации о возникновении исключений на уровне протокола modbus
          enabled: true # состояние активности данного детектора
        detector_event_type: # детектор для выявления modbus-запросов без ответов и/или modbus-ответов без запросов
          enabled: true # состояние активности данного детектора
        detector_empty_request_address: # детектор для выявления неправильно сформированных запросов
          enabled: true # состояние активности данного детектора
        detector_stacked_coils_request: # детектор для выявления неверного формата данных (например, передача строки в бинарном регистре)
          enabled: true # состояние активности данного детектора
        detector_unknown_func: # детектор для выявления отсутствующих в режиме обучения функций протокола modbus
          enabled: true # состояние активности данного детектора
        detector_long_delay_in_requests: # детектор для выявления задержек между запросами, превосходящих предельные значения режима обучения
          enabled: true # состояние активности данного детектора
          skip_max_ejection: 2 # количество отсортированных выбросов в режиме обучения, которые игнорируются при формировании предельных значений
        detector_large_number_of_requests_over_time: # детектор для выявления слишком частых запросов (относительно режима обучения)
          enabled: true # состояние активности данного детектора
          skip_max_ejection: 2 # количество отсортированных выбросов в режиме обучения, которые игнорируются при формировании предельных значений
      train_connections_num: 100000 # количество сформированных входных векторов, необходимых для прохождения обучения
          part_of_data_training_the_model: 0.7 # определяет какая часть от сформированных входных векторов, необходимых для прохождения обучения
(train_connections_num) будет использована для формирования автомата, оставшиеся данные используются для формирования граничных значений
      min_checks_count_before_validation: 50000 # количество сформированных входных векторов для прохождения этапа валидации автомата
    min_probability_of_correct_prediction: 80 # минимальное значение метрики "предсказательная способность" (в %) для успешного прохождения этапа валидации
      sync_connections_num: 5000 # количество сформированных входных векторов, необходимых для синхронизации гибридного автомата
      validation: true # активность этапа валидации после этапа обучения
    states_ode_model_type: 'RidgeCV' # тип модели, используемой для предсказания следующего значения регистра (допустимы LinearRegression, Ridge, RidgeCV)
      max_ape_coef: 2.0 # допустимая величина ошибки предсказания по сравнению с аналогичной на валидационных данных
      turn_on_forbidden_transitions: true # активность формирования события при детектировании несуществующего перехода в рамках гибридного автомата
```

```
       filter_anomalies_after_transitions: false # игнорирование ошибок предсказания значений регистров в области перехода между состояниями гибридного автомата
      area_after_transition_to_filter_anomalies: 0 # количество входных векторов, для которых выполняется игнорирование ошибок предсказания после перехода между состояниями гибридного автомата (только при filter_anomalies_after_transitions: true)
         unknown_function_ignore_notification: false # отображение информации о детектировании функций Modbus, которые не входят в анализируемые (не указаны в controlled_func)
      input_vector_creation_time_limit_sec: 180 # лимит времени (в секундах), отведенный на формирование входного вектора. При его превышении формируется предупреждение в логах
       input_vector_waiting_sleep_delay_sec: 5 # пауза (в секундах) при формировании входного вектора
       log_input_vector_description_delay_commands: 4 # пауза (в секундах) для логирования входного вектора в логах
       separation: # управление режимом формирования маски данных
         enabled: false # активность режима формирования маски данных (для гибридного автомата всегда False)
       segmentation_threshold: 0 # порог принятия решения о границе сегмента для переменной
       ignore_segments_shorter_then: 0 # указание минимальной длины сегмента, допустимой для анализа в рамках гибридного автомата
        number_of_folds: 5 # количество фолдов для кросс-валидации при подборе коэффициентов уравнений состояния гибридного автомата (применимо только для states_ode_model_type: 'RidgeCV')
```

См. также

Модель на основе гибридного автомата

Модель на основе временного автомата

Модель на основе иерархического словаря

22.5.6. Рекомендации по использованию переменных файлов manager.env и sensor.env

Не все доступные для использования переменные, которые могут быть в файле `manager.env` или `sensor.env`, сразу находятся в нем. Некоторые из них необходимо вводить самостоятельно или раскомментировать.

При использовании переменных объема и времени рекомендуется использовать форматы, предложенные производителем Комплекса. Значительные отклонения от значений по умолчанию могут повлечь некорректную работу, недоступность системы или ее частей.

Список рекомендаций приведен в таблице ниже.

Табл. 159. Рекомендации по использованию переменных файлов manager.env и sensor.env

ПЕРЕМЕННАЯ	РЕКОМЕНДАЦИИ ПО ИСПОЛЬЗОВАНИЮ	ПРИМЕНИМО ДЛЯ УРОВНЯ КОМПЛЕКСА
`EVENT_INDICES_MAX_SIZE_GB`	Если присутствует дисковый раздел под оперативный архив, установите значение переменной не более 90% от общего объема раздела (например, 90 ГБ для 100 ГБ). Если отдельного раздела нет, то установите значение не более 300 ГБ	Management
`EVENT_ARCHIVES_MAX_SIZE_GB`	Рекомендуется установить значение переменной около 30% от общего объема раздела `backups`, который был выделен при установке Комплекса — подробнее см. раздел «Разметка диска для хранения резервных копий Комплекса»	Management
`EVENT_INDICES_LIFETIME_DAYS`	Установите значение около 30 дней	Management
`EVENT_ARCHIVES_LIFETIME_DAYS`	Установите адекватную системе длительность хранения глубокого архива. Она должна быть больше длительности хранения оперативного архива — например, укажите на несколько дней больше, чем указано в `EVENT_INDICES_LIFETIME_DAYS`	Management
`EVENTS_RETENTION_DISK_CAPACITY_SIZE_MB`	Установите значение не более 20-30 ГБ	Management
`EVENTS_RETENTION_MONTHS`	Установите значение от 1 до 3 месяцев	Management

См. также

Переменные Комплекса уровня Management

22.6. События Комплекса

Большинство событий, которые попадают в разделы мониторинга, приведены в таблице (Таблица 160. Основные события Комплекса).

Виды служебных источников событий (поле `listener`) см. в разделе «Описание служебных источников событий».

Помимо событий от сервисов Комплекса могут быть получены события от службы обнаружения вторжений. Поле `event_type` в таких событиях имеет значение `ids_event`, а идентификаторы событий отличаются от стандартных.

Табл. 160. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИСТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВАТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫПОЛНЕНИЕ ФУНКЦИИ
1020001	Комплекс в фоновом режиме помечает доступные интерфейсы	Доступность интерфейса восстановлена	[`{ip}` – `{mac}`]: Доступность интерфейса восстановлена (Актив: `{netbios_name}`)	Availability Control	нет (внутренняя пассивная функция Комплекса)	нет
1020002	Комплекс в фоновом режиме помечает недоступные интерфейсы	Интерфейс недоступен	[`{ip}` – `{mac}`]: Интерфейс недоступен (Актив: `{netbios_name}`)	Availability Control	нет (внутренняя пассивная функция Комплекса)	нет
1030001	Запущенную операцию резервного копирования завершить не удалось	Не удалось завершить создание резервной копии в результате ошибки	Обоснование: `{justification}`; Пользователь: `{username}`; Ошибка: `{exception}`	Backup Control	`/backup/create` `POST`	Администратор
1030002	Запущенная операция создания резервной копии завершена успешно	Резервная копия создана успешно	Обоснование: `{justification}`; Пользователь: `{username}`	Backup Control	`/backup/create` `POST`	Администратор

Табл. 160. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИСТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВАТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫПОЛНЕНИЕ ФУНКЦИИ
1030003	Пользователь запустил создание резервной копии	Запущено создание резервной копии	Обоснование: `{justification}`; Пользователь: `{username}`	Backup Control	`/backup/create` `POST`	Администратор
1050001	Конфигурация собрана впервые и принята за эталон	Изменено эталонное состояние конфигурации	Актив: `{host_netbios_name}`; Наименование сканера: `{scanner_name}`	Configuration Control	нет (внутренняя пассивная функция Комплекса)	нет
1050002	Состояние конфигурации не соответствует эталонному	Нарушено эталонное состояние конфигурации	Актив: `{host_netbios_name}`; Наименование сканера: `{scanner_name}`; Изменения: `{changes}`	Configuration Control	Внутренняя проверка очередного (не первого) результата сбора конфигурации после выполнения запроса: `/config_collection_tasks` `POST`	нет
1050004	Пользователь удалил конфигурацию	Удалена конфигурация	Актив: `{host_netbios_name}`; Наименование сканера: `{scanner_name}`; Пользователь: `{user_login}`; Обоснование: `{justification}`; Собрана: `{collected_at}`	Configuration Control	`/collected_configs/[config_id]/delete` `POST`	Администратор

Табл. 160. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИСТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВАТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫПОЛНЕНИЕ ФУНКЦИИ
1050005	Пользователь изменил эталонную конфигурацию	Изменено эталонное состояние конфигурации	Актив: `{host_netbios_name}`; Наименование сканера: `{scanner_name}`; Пользователь: `{user_login}`; Обоснование: `{justification}`	Configuration Control	`/collected_configs/[config_id]/standard` `POST`	Администратор Инженер
1050006	Пользователь удалил все конфигурации сканера	Удалены конфигурации	Актив: `{host_netbios_name}`; Наименование сканера: `{scanner_name}`; Пользователь: `{user_login}`; Обоснование: `{justification}`	Configuration Control	`/collected_configs/delete` `POST`	Администратор
1070001	Сообщение о запуске регистрации событий	Запущен сервис регистрации событий		System Event	нет (внутренняя пассивная функция Комплекса)	нет
1070002	Сообщение об остановке регистрации событий	Остановлен сервис регистрации событий		System Event	нет (внутренняя пассивная функция Комплекса)	нет
1070003	После остановки получения событий журнал был очищен	Сервис регистрации событий запущен после очистки заре-		System Event	нет (внутренняя пассивная функция Комплекса)	нет

Табл. 160. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИСТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВАТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫПОЛНЕНИЕ ФУНКЦИИ
		зервированного дискового пространства				
1070004	Достигнуто предельное значение размера журнала событий	Сервис регистрации событий остановлен в результате переполнения зарезервированного дискового пространства		System Event	нет (внутренняя пассивная функция Комплекса)	нет
1070005	Выявлено отклонение от указанного минимального количества событий от источника	С источника получено меньше событий, чем указано в его параметрах	Источник: `{source_name}`; Актив: `{host_name}` (`{host_id}`); За `{delay}` секунд было получено `{received}` событий, ожидалось `{threshold}` событий.	System Event	нет (внутренняя пассивная функция Комплекса)	нет
1070006	Новых событий не обнаружилось в результате выполнения задачи	Задача сбора событий успешно выполнена, новых событий не обнаружено	Актив: `{host_name}` (`{host_id}`); Наименование сканера: `{scanner_name}`	System Event	нет (внутренняя пассивная функция Комплекса)	нет

Табл. 160. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИСТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВАТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫПОЛНЕНИЕ ФУНКЦИИ
1070007	Импорт событий не завершен из-за проблем с подключением к базе данных	Не удалось импортировать события с актива: обнаружены проблемы с подключением к базе данных	Не удалось импортировать события с актива: обнаружены проблемы с подключением к базе данных; Актив: `{host_netbios_name} ({host_id})`; Сканер: `{scanner_name}`	System Event		нет
1070008	Импорт событий не завершен из-за затруднений в работе сервиса обработки событий	Импорт события завершить не удалось: обнаружены затруднения в работе сервиса обработки событий	Импорт события завершить не удалось: обнаружены затруднения в работе сервиса обработки событий; Актив: `{host_netbios_name} ({host_id})`; Сканер: `{scanner_name}`	System Event		нет
1070009	Объем дискового пространства, зарезервированного для внутренних событий, превышает значение, установленное пользователем	Сервис регистрации внутренних событий остановлен в результате переполнения дискового пространства, заре-		System Event		

Табл. 160. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИСТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВАТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫПОЛНЕНИЕ ФУНКЦИИ
		зервированного для событий				
1070010	Объем дискового пространства, зарезервированного для внутренних событий, занят на 85%	События сервиса регистрации внутренних событий заняли 85% дискового пространства, зарезервированного для событий		System Event		
1070011	Сервис регистрации внутренних событий возобновил работу после очистки дискового пространства, зарезервированного для событий	Запущен сервис регистрации внутренних событий		System Event		
1080001	Пользователь создает актив	Создан новый актив	id: `{id}`; Имя: `{netbios_name}`; Описание: `{description}`;	Host Control	`/hosts` `POST`	Администратор Инженер

Табл. 160. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИСТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВАТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫПОЛНЕНИЕ ФУНКЦИИ
			Тип: `{host_type}`; ipv4-ipv6-mac: `{interfaces_list}`			
1080002	Пользователь удаляет актив	Удален актив	Обоснование: `{justification}`; Пользователь: `{user}` id: `{id}`; Имя: `{netbios_name}`; Описание: `{description}`; Тип: `{host_type}`; ipv4-mac: `{interfaces_list}`	Host Control	`/hosts/[host_id]/delete` `POST`	Администратор
1080003	Пользователь редактирует актив	Изменен актив	ID актива: `{old_id}`; Старые значения: [id: `{old_id}`; Имя: `{old_netbios_name}`; Описание: `{old_description}`; Тип: `{old_host_type}`; ipv4-ipv6-mac: `{old_interfaces_list}`]; Новые значения: [id: `{new_id}`; Имя: `{new_netbios_name}`; Описание: `{new_description}`; Тип: `{new_host_type}`; ipv4-ipv6-mac:	Host Control	`/hosts/[host_id]` `PATCH`	Администратор Инженер

Табл. 160. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИСТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВАТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫПОЛНЕНИЕ ФУНКЦИИ
			{new_interfaces_list}]; Пользователь: {user}			
1080004	Пользователь изменил контролируемую сеть	Актив был удален в результате изменения адресов контролируемой сети	id: {id}; Имя: {netbios_name}; Описание: {description}; Тип: {host_type}; ipv4-ipv6-mac: {interfaces_list}	Host Control	/sensors-backend/home_nets PUT	Администратор
1080005	Пользователь изменил контролируемую сеть	Интерфейс был удален в результате изменения адресов контролируемой сети	ID: {id}; ID актива: {host_-id}; Имя: {name}; Интерфейс сбора данных: {default}; ipv4: {ip_v4_address}; mac: {mac_address}	Host Control	/sensors-backend/home_nets PUT	Администратор
1080006	Пользователь удалил несколько активов	Удалены активы	Количество активов: {filtered_count}; Примененный фильтр: [АСУ ТП: {asu_tp}; Типы активов: {host_types}; Метки: {host_-labels}; IP-адреса: {ip_-filters}; Активы: {hosts}; Производители: {vendors};	Host Control	/hosts/bulk/delete POST	Администратор

Табл. 160. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИСТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВАТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫПОЛНЕНИЕ ФУНКЦИИ
			Группы активов: `{host_groups}`; Активы без групп: `{outside_tree}`]; Пользователь: `{user}`; Обоснование: `{justification}`			
1080007	Пользователь удалил сетевые атрибуты актива	Отвязан интерфейс	[ID: `{id}`; ID актива: `{host_id}`; Имя: `{name}`; Интерфейс сбора данных: `{default}`; ipv4: `{ip_v4_address}`; mac: `{mac_address}`] Пользователь: `{user}`	Host Control	`/host_interfaces/[host_interface_id]` `PATCH`	Администратор Инженер
1080008	Пользователь присвоил сетевые атрибуты активу	Привязан интерфейс	[ID: `{id}`; ID актива: `{host_id}`; Имя: `{name}`; Интерфейс сбора данных: `{default}`; ipv4: `{ip_v4_address}`; mac: `{mac_address}`] Пользователь: `{user}`	Host Control	`/host_interfaces/[host_interface_id]` `PATCH`	Администратор Инженер
1080009	Пользователь не изменил данные в	Вместе с сенсором удалены сетевые атрибуты актива	Сенсор: `{sensor_name}` (`{sensor_id}`); Актив: `{host_name}` (`{host_id}`); Сетевые	Host Control	`/hosts/[host_id]` `PATCH`	Администратор Инженер

Табл. 160. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИСТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВАТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫПОЛНЕНИЕ ФУНКЦИИ
	карточке актива, но нажал **Сохранить**		атрибуты: `{ip_v4_address}`, `{mac_address}`			
1080010	Сетевые атрибуты присвоены активу	Интерфейс привязан к активу	Интерфейс `<{ip}, {mac}>` был привязан к активу `<{netbios_name}, {host_id}>`	Host Control	нет (внутренняя пассивная функция Комплекса)	нет
1080011	Комплекс просканировал контролируемую сеть и обнаружил неизвестный актив	Обнаружен неизвестный актив	id: `{host_id}`; ip-mac: [`{ip}` - `{mac}`]	Host Control	нет (внутренняя пассивная функция Комплекса)	нет
1080013	Пользователь удаляет сенсор. Вместе с сенсором удаляется актив с единственным сетевым атрибутом, IP-адрес которого входил в контролируемую сеть сенсора	Вместе с сенсором удален актив	Сенсор: `{sensor_name}` (`{sensor_id}`); Актив: `{netbios_name}` (`{id}`); Сетевые атрибуты: `{ip}`, `{mac}`	Host Control	нет (внутренняя пассивная функция Комплекса)	нет

Табл. 160. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИСТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВАТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫПОЛНЕНИЕ ФУНКЦИИ
1080015	Пользователь удалил несколько групп активов	Изменены группы активов	Пользователь: `{user}`; Число удаленных групп активов: `{removed_host_groups_quantity}`; Число созданных групп активов: `{created_host_groups_quantity}`; Число измененных групп активов: `{changed_host_groups_quantity}`; Число неизмененных групп активов: `{unchanged_host_groups_quantity}`	Host Control	`/host_groups/replace` `PUT`	Администратор
1080016	Один и тот же IP-адрес присвоен более, чем одному активу	Обнаружено дублирование IP-адреса	IP-адрес: `{duplicated_ip}`; Актив 1: `{target_name}` (`{target_id}`, `{target_ip}`, `{target_mac}`); Актив 2: `{source_name}` (`{source_id}`, `{source_ip}`, `{source_mac}`); Сенсор: `{observer_id}` (`{observer_name}`).	Host Control	нет (внутренняя пассивная функция Комплекса)	нет

Табл. 160. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИСТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВАТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫПОЛНЕНИЕ ФУНКЦИИ
1080017	Одно и то же наименование присвоено нескольким активам	Обнаружены активы с совпадающим сетевым именем	Обнаружены активы с совпадающим сетевым именем: `{target_name}` (`{target_id}`, `{target_ip}`, `{target_mac}`, сенсор: `{target_sensor_name}`) и `{source_name}` (`{source_id}`, `{source_ip}`, `{source_mac}`, сенсор: `{source_sensor_name}`).	Host Control	нет (внутренняя пассивная функция Комплекса)	нет
1080018	Пользователь создал сетевые атрибуты актива	Созданы сетевые атрибуты актива	ID актива: `{host_id}`; `{interface_str}`	Host Control	`/host_interfaces` `POST`	Администратор Инженер
1080019	Пользователь удалил сетевые атрибуты актива	Удалены сетевые атрибуты актива	ID актива: `{host_id}`; `{interface_str}`	Host Control	`/host_interfaces/[interface_id]` `DELETE`	
1080020	Пользователь изменил сетевые атрибуты актива	Изменены сетевые атрибуты актива	ID актива: `{host_interface_id}`; Старые значения: [`{old_values}`]; Новые значения: [`{new_values}`]	Host Control	`/host_interfaces/[interface_id]` `PATCH`	

Табл. 160. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИСТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВАТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫПОЛНЕНИЕ ФУНКЦИИ
1080022	Пользователь присвоил учетные данные активу	Присвоены учетные данные активу	Актив: `{host_netbios_name}`; Учетные данные: `{cred_name}`; Пользователь: `{user_login}`	Host Control	`/host_data_collector/host_credential_relations/bulk/replace` `POST`	Администратор Инженер
1080023	Пользователь отменил присвоение учетных данных активу	Отменено присвоение учетных данных активу	Актив: `{host_netbios_name}`; Учетные данные: `{cred_name}`; Пользователь: `{user_login}`	Host Control	`/host_data_collector/host_credential_relations/bulk/replace` `POST`	
1080024	Пользователь удалил учетные данные актива	Удалены учетные данные активов	Наименование УД: `{cred_name}`; активы, которым были присвоены УД: `{host_netbios_names}`; Пользователь: `{user}`; Обоснование: `{justification}`	Host Control	`host_data_collector/credentials/[credentials_id]/delete` `POST`	
1080025	Пользователь удалил несколько учетных данных активов	Удалено `{count}` учетных данных активов	Наименование УД: `{cred_names}`; Пользователь: `{user}`; Обоснование: `{justification}`	Host Control	`host_data_collector/credentials` `POST`	

Табл. 160. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИСТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВАТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫПОЛНЕНИЕ ФУНКЦИИ
1080026	Пользователь добавил учетные данные активов	Добавлены учетные данные активов	Наименование УД: `{cred_name}`; Пользователь: `{user}`	Host Control	`host_data_collector/credentials/bulk/delete?name=[cred_name]` `POST`	
1080027	Пользователь изменил учетные данные активов	Изменены учетные данные активов	Наименование УД: `{cred_name}`; Пользователь: `{user}`	Host Control	`host_data_collector/credentials/[cred_id]` `PATCH`	
1080028	Пользователь изменил IP-адрес актива	Изменен IP-адрес актива	Изменен IP-адрес актива; Актив: `{host_name}` (`{host_id}`); Старое значение: [`{old_IP-address}`]; Новое значение: [`{new_IP-address}`]	Host Control		
1090023	Пользователь удаляет скрипт OVAL	Удален скрипт OVAL	Пользователь: `{user}`; Обоснование: `{justification}`; Название: `{script_name}`; Описание: `{script_description}`	Host Data Collecting	`/host_data_collector/oval/scripts/[script_id]/delete` `POST`	Администратор

Табл. 160. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИСТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВАТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫПОЛНЕНИЕ ФУНКЦИИ
1090024	Пользователь удаляет несколько скриптов OVAL	Удалены скрипты OVAL	Пользователь: `{user}`; Обоснование: `{justification}`; Удалено: `{deleted_count}`	Host Data Collecting	`/host_data_collector/oval/scripts/bulk/delete` `POST`	
1090201	Пользователь импортирует группы сканеров	Импортированы группы сканеров	Пользователь: `{user}`; Импортировано `{count}` из `{file_count}` групп; Выбранное действие для добавленных ранее элементов: `{action_for_missing_elements}`	Host Data Collecting	`/exporter/import/catalogs/file?catalog=scanner_groups` `PUT`	Администратор
1090202	Пользователь экспортирует группы сканеров	Экспортированы группы сканеров	Пользователь: `{user}`	Host Data Collecting	`/exporter/export/catalogs/file?catalog=scanner_groups` `POST`	Администратор Инженер
1090203	Пользователь создает сканер	Создан сканер	Пользователь: `{user}`; Тип: `{scanner_type}`; Наименование: `{scanner_name}`; Группы сканеров: `{scanner_group_name}`	Host Data Collecting	`/host_data_collector/scanners` `POST`	Администратор

Табл. 160. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИСТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВАТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫПОЛНЕНИЕ ФУНКЦИИ
1090206	Пользователь запускает сканер	Запущен сканер на активе	Пользователь: `{user}`; Тип: `{scanner_type}`; Наименование: `{scanner_name}`; Актив: `{host_name}` (`{host_id}`);	Host Data Collecting	`/host_data_collector/scanners/execute` `POST`	Администратор Инженер
1090208	Пользователь редактирует сканер	Изменен сканер	Пользователь: `{user}`; Предыдущее состояние: [Наименование: `{old_scanner_name}`; Описание: `{old_scanner_description}`; Тип `{old_scanner_type}`; Группа `{old_scanner_group_name}`]; Новое состояние: [Наименование: `{new_scanner_name}`; Описание: `{new_scanner_description}`; Тип `{new_scanner_type}`; Группа `{new_scanner_group_name}`];	Host Data Collecting	`/host_data_collector/scanners/[scanner_id]` `PATCH`	Администратор
1090209	Пользователь удаляет несколько групп сканеров	Удалены группы сканеров	Пользователь: `{user}`; Количество: `{deleted_count}`	Host Data Collecting	`/host_data_collector/scanner_groups/bulk/delete`	

Табл. 160. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИСТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВАТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫПОЛНЕНИЕ ФУНКЦИИ
					`POST`	
1090210	Пользователь удаляет группу сканеров	Удалена группа сканеров	Пользователь: `{user}`; Наименование: `{scanner_group_name}`	Host Data Collecting	`/host_data_collector/scanner_groups/[id]/deletee` `POST`	
1090211	Пользователь удаляет несколько сканеров сбора данных	Удалены сканеры	Пользователь: `{user}`; Обоснование: `{justification}`; Количество: `{deleted_count}`	Host Data Collecting	`/scanners/bulk/delete` `POST`	
1090212	Пользователь удаляет сканер сбора данных	Удален сканер	Пользователь: `{user}`; Обоснование: `{justification}`; Наименование: `{scanner_name}`; Описание: `{scanner_description}`; Тип: `{scanner_type}`	Host Data Collecting	`/scanners/[scanner_id]/delete` `POST`	
1090213	Пользователь удаляет сканер, который используется при сборе данных	Удален сканер во время выполнения сбора данных	Пользователь: `{user}`; Обоснование: `{justification}`; Результаты сбора не будут сохранены; Задачи, где использовался сканер:	Host Data Collecting	`/scanners/[scanner_id]/delete` `POST`	

Табл. 160. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИСТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВАТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫПОЛНЕНИЕ ФУНКЦИИ
			{task_name}; Наименование: {scanner_name}; Описание: {scanner_description}; Тип: {scanner_type}			
1090214	В результате выполнения сканера получен некорректный ответ	Обнаружена ошибка соединения при выполнении сканера сбора данных	Актив: {host_netbios_name} ({host_id}); Сканер: {scanner_name}; Задачи: {task_names}; Ошибка: {error}	Host Data Collecting	/config_collection_tasks POST или /commands/create_event_task POST	Администратор Инженер
1090215	Сбор данных завершился ошибкой	Обнаружена ошибка сбора при выполнении сканера сбора данных	Актив: {host_netbios_name} ({host_id}); Сканер: {scanner_name}; Задачи: {task_names}; Ошибка: {error}	Host Data Collecting	нет (внутренняя пассивная функция Комплекса)	нет
1090301	Пользователь импортирует задачи сбора данных	Импортированы задачи сбора данных	Пользователь: {user}; Импортировано {count} из {file_count} групп; Выбранное действие для добавленных	Host Data Collecting	/exporter/import/catalogs/file?catalog=collection_tasks PUT	Администратор Инженер

Табл. 160. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИСТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВАТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫПОЛНЕНИЕ ФУНКЦИИ
			ранее элементов: `{action_for_missing_elements}`			
1090302	Пользователь экспортирует задачи сбора данных	Экспортированы задачи сбора данных	Пользователь: `{user}`	Host Data Collecting	`/exporter/export/catalogs/file?catalog=collection_tasks` `POST`	
1090303	Пользователь создает задачу сбора данных	Создана задача сбора данных	Пользователь: `{user}`; Наименование: `{task_name}`; Активность: `{activity}`; Время запуска расписания: `{start_date}`; Тип запуска: `{type}`	Host Data Collecting	`/host_data_collector/collection/tasks` `POST`	
1090304	Пользователь меняет активность нескольких задач сбора данных	Изменена активность задач сбора данных	Пользователь: `{user}`; Обоснование: `{justification}`; Статус активности: `{activity}`; Наименование: `{tasks_name}`; Количество: `{updated_count}`	Host Data Collecting	`/host_data_collector/collection/tasks/bulk/activity` `POST`	

Табл. 160. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИСТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВАТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫПОЛНЕНИЕ ФУНКЦИИ
1090305	Пользователь редактирует задачу сбора данных	Изменена задача сбора данных	Пользователь: `{user}`; Предыдущее состояние: [Наименование: `{old_name}`; Описание: `{old_description}`; Период запуска `{old_cron}`; Время старта `{old_start_date}`; Время завершения `{old_end_date}`; Активность `{old_active}`; Список групп сканеров `{old_scanner_groups_ids}`; Список групп активов `{old_host_groups_ids}`; Список активов `{old_host_ids}`]; Новое состояние: [Наименование: `{new_name}`; Описание: `{new_description}`; Период запуска `{new_cron}`; Время старта `{new_start_date}`; Время завершения `{new_end_date}`; Активность	Host Data Collecting	`/host_data_collector/collection/tasks/[task_id]` `PATCH`	

Табл. 160. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИСТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВАТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫПОЛНЕНИЕ ФУНКЦИИ
			{new_active}; Список групп сканеров {new_scanner_groups_ids}; Список групп активов {new_host_groups_ids}; Список активов {new_host_ids}]			
1090308	Пользователь удаляет несколько задач сбора данных	Удалены задачи сбора данных	Пользователь: {user}; Обоснование: {justification}; Количество: {count} задач	Host Data Collecting	/host_data_collector/collection/tasks/bulk/delete DELETE	
1090309	Пользователь удаляет задачу сбора данных	Удалена задача сбора данных	Пользователь: {user}; Обоснование: {justification}; Наименование: {task_name}; Группы сканеров: {scanner_groups}; Активы: {host_names}; Группы активов: {host_group_names}	Host Data Collecting	/host_data_collector/collection/tasks/[task_id] DELETE	
1090310	Получен результат сбора данных	Сбор данных успешно выполнен	Тип: {scanner_type}; Актив: {host_netbios_name}; Сканер: {scanner_name}	Host Data Collecting	/config_collection_tasks POST	

Табл. 160. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИСТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВАТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫПОЛНЕНИЕ ФУНКЦИИ

					или
					`/commands/create_event_task`
					`POST`	

1090313	Пользователь удаляет несколько результатов сбора данных	Удалены статусы сбора данных	Пользователь: `{user}`; Обоснование: `{justification}`; Количество удаленных результатов: `{deleted_count}`	Host Data Collecting	`/host_data_collector/collection/logs/bulk/delete` `DELETE`	Администратор
1090314	Пользователь удаляет статус сбора данных	Удален статус сбора данных	Пользователь: `{user}`; Обоснование: `{justification}`; Сканер: `{scanner_name}`; Актив: `{host_name}`; Задачи: `{task_names}`; Результат: `{result_type}`; Дата получения: `{updated_at}`	Host Data Collecting	`/host_data_collector/collection/logs/delete` `POST`	
1100001	Пользователь удаляет статус инцидентов	Удален пользовательский статус инцидента	Обоснование: `{justification}`; Пользователь: `{user}`; Название: `{name}`; Категория: `{category}`	Incident Control	`/incident_statuses/[status_id]/delete` `DELETE`	Администратор

Табл. 160. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИСТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВАТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫПОЛНЕНИЕ ФУНКЦИИ
1100003	Пользователь создает статус инцидента	Создан пользовательский статус инцидента	Обоснование: `{justification}`; Пользователь: `{user}`; Новый статус: [Название: `{name}`; Категория: `{category}`]	Incident Control	`/incident_manager/statuses` `POST`	
1100004	Пользователь редактирует статус инцидента	Изменен пользовательский статус инцидента	Обоснование: `{justification}`; Пользователь: `{user}`; Предыдущий статус: [Название: `{name}`; Категория: `{category}`]; Новый статус: [Название: `{new_name}`; Категория: `{new_category}`)	Incident Control	`/incident_manager/statuses/[status_id]` `PATCH`	
1100005	Пользователь редактирует параметры инцидента	Изменен инцидент	Комментарий: `{action_comment}`; Пользователь: `{user}`; Предыдущий статус: `{status}`; Название: `{name}`; Описание: Изменен инцидент; Приоритет: `{priority}`; Комментарий: `{comment}`; Подтвержден: `{is_confirmed}`;	Incident Control	`/incident/[incident_id]` `PATCH`	Администратор Инженер

Табл. 160. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИСТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВАТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫПОЛНЕНИЕ ФУНКЦИИ
			Новый статус: `{new_status}`; Название: `{new_name}`; Описание: `{new_description}`; Приоритет: `{new_priority}`; Комментарий: `{new_comment}`; Подтвержден: `{new_is_confirmed}`			
1100006	Пользователь удаляет инцидент	Удален инцидент	Обоснование: `{justification}`; Пользователь: `{user}`; Название: `{name}`; Описание: Удален инцидент; Приоритет: `{priority}`; Статус: `{status}`; Комментарий: `{comment}`; Подтвержден: `{is_confirmed}`	Incident Control	`/incident/[incident_id]` `DELETE`	
1100007	Пользователь удаляет несколько инцидентов	Удалена группа инцидентов	Обоснование: `{justification}`; Пользователь: `{user}`; Количество удаленных инци-	Incident Control	`/incidents/bulk/delete` `DELETE`	

Табл. 160. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИСТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВАТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫПОЛНЕНИЕ ФУНКЦИИ
			дентов: `{deleted_incident_count}`; Примененный фильтр: `{filter_info}`			
1100008	Пользователь отменяет групповое удаление инцидентов	Удаление инцидентов прервано пользователем	Обоснование: `{justification}`; Пользователь: `{user}`; Количество удаленных инцидентов: `{deleted_incident_count}`; Примененный фильтр: `{filter_info}`	Incident Control	`/incidents/bulk/stop_deletion` `POST`	Администратор Инженер
1100009	Пользователь меняет параметры нескольких инцидентов	Изменена группа инцидентов	Комментарий: `{action_comment}`; Пользователь: `{user}`; Количество измененных инцидентов: `{incident_count}`; Примененный фильтр: `{filter_info}`	Incident Control	`/incidents/bulk/update` `POST`	Администратор Инженер
1100010	Пользователь отменяет групповое из-	Задача обновления инцидентов была	Комментарий: `{action_comment}`; Пользователь: `{user}`; Количество изме-	Incident Control	`/incidents/bulk/stop_update` `POST`	Администратор Инженер

Табл. 160. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИСТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВАТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫПОЛНЕНИЕ ФУНКЦИИ
	менение параметров инцидентов	отменена пользователем	ненных инцидентов: `{incident_count}`; Примененный фильтр: `{filter_info}`			
1100011	Срабатывает правило корреляции	Обнаружен инцидент	Описание: `{incident_description}`; Правило: `{rule_name}`; Активы: `{host_ids}`; Приоритет: `{priority}`; Тип инцидента: `{incident_type}`; Идентификатор проверки: `{retro_entry_id}`	Incident Control	нет (внутренняя пассивная функция Комплекса)	нет
1110001	Пользователь прерывает выполнение проверки на соответствие требованиям ИБ	Выполнение проверки прервано	Название проверки: `{assessment_title}`; Название актива: `{host_netbios_name}`; ID актива: `{assessment_host_id}`; Пользователь: `{assessment_created_by}`; Результат: `{assessment_status_value}`; Описание: Выполнение проверки прервано; Время	OVAL Event	`/oval_scanner/oval/assessments/[assestment_id]/cancel` `POST`	Администратор

Табл. 160. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИСТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВАТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫПОЛНЕНИЕ ФУНКЦИИ
			запуска проверки: `{assessment_created_at}`; Время окончания проверки: `{assessment_updated_at}`; IP актива: `{host_interface_ip_v4_address}`; MAC актива: `{host_interface_mac_address}`			
1110002	Проверка на соответствие требованиям ИБ не завершена в результате превышения времени ожидания	Превышено время ожидания выполнения задачи проверки	Название проверки: `{assessment_title}`; Название актива: `{host_netbios_name}`; ID актива: `{assessment_host_id}`; Пользователь: `{assessment_created_by}`; Результат: `{assessment_status_value}`; Описание: Превышено время ожидания выполнения задачи проверки; Время запуска проверки: `{assessment_created_at}`; Время окончания проверки:	OVAL Event	`/oval_scanner/oval/assessments` `POST`	Администратор Инженер

Табл. 160. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИСТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВАТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫПОЛНЕНИЕ ФУНКЦИИ
			{assessment_updated_at}; IP актива: {host_interface_ip_v4_address}; MAC актива: {host_interface_mac_address}; Ошибка: {timeout_error}			
1110003	Проверка на соответствие требованиям ИБ удалена до ее завершения	Задача проверки была удалена в процессе выполнения	Название проверки: {assessment_title}; Название актива: {host_netbios_name}; ID актива: {assessment_host_id}; Пользователь: {assessment_created_by}; Результат: {assessment_status_value}; Описание: Задача проверки была удалена в процессе выполнения; Время запуска проверки: {assessment_created_at}; Время окончания проверки: {assessment_updated_at}; IP актива: {host_interface_	OVAL Event	/oval_scanner/oval/assessments/[assestment_id]/delete POST	Администратор

Табл. 160. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИСТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВАТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫПОЛНЕНИЕ ФУНКЦИИ
			`ip_v4_address}`; MAC актива: `{host_interface_mac_address}`			
1110004	При выполнении проверки на соответствие требованиям ИБ получена ошибка	Ошибка выполнения задачи проверки	Название проверки: `{assessment_title}`; Название актива: `{host_netbios_name}`; ID актива: `{assessment_host_id}`; Пользователь: `{assessment_created_by}`; Результат: `{assessment_status_value}`; Описание: Ошибка выполнения задачи проверки; Время запуска проверки: `{assessment_created_at}`; Время окончания проверки: `{assessment_updated_at}`; IP актива: `{host_interface_ip_v4_address}`; MAC актива: `{host_interface_mac_address}`; Ошибка: `{error}`	OVAL Event	`/oval_scanner/oval/assessments` `POST`	Администратор Инженер

Табл. 160. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИСТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВАТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫПОЛНЕНИЕ ФУНКЦИИ
1110005	При выполнении проверки на соответствие требованиям ИБ произошла ошибка	Непредвиденная ошибка выполнения задачи проверки	Название проверки: `{assessment_title}`; Название актива: `{host_netbios_name}`; ID актива: `{assessment_host_id}`; Пользователь: `{assessment_created_by}`; Результат: `{assessment_status_value}`; Описание: Непредвиденная ошибка выполнения задачи проверки; Время запуска проверки: `{assessment_created_at}`; Время окончания проверки: `{assessment_updated_at}`; IP актива: `{host_interface_ip_v4_address}`; MAC актива: `{host_interface_mac_address}`; Ошибка: `{error}`	OVAL Event		
1110006	В результате проверки на соответствие требованиям ИБ об-	Выполнение проверки завершено успешно	Название проверки: `{assessment_title}`; Название актива: `{host_-`	OVAL Event		

Табл. 160. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИСТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВАТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫПОЛНЕНИЕ ФУНКЦИИ
	наружены несоответствия и уязвимости		`netbios_name}`; ID актива: `{assessment_host_id}`; Пользователь: `{assessment_created_by}`; Результат: `{assessment_status_value}`; Описание: Выполнение проверки завершено успешно; Время запуска проверки: `{assessment_created_at}`; Время окончания проверки: `{assessment_updated_at}`; IP актива: `{host_interface_ip_v4_address}`; MAC актива: `{host_interface_mac_address}`; `{self.assessment_status_value}`; Количество OVAL-определений: `{oval_definitions_count}`; Количество выполненных проверок: `{performed_checks_count}`; Состояние со-			

Табл. 160. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИСТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВАТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫПОЛНЕНИЕ ФУНКЦИИ
			ответствия: есть несоответствия/есть уязвимости; Количество выявленных несоответствий: `{compliance_false_count}`; Количество выявленных уязвимостей: `{vulnerabilities_true_count}`			
1110007	В результате проверки на соответствие требованиям ИБ обнаружены несоответствия	Выполнение проверки завершено успешно	Название проверки: `{assessment_title}`; Название актива: `{host_netbios_name}`; ID актива: `{assessment_host_id}`; Пользователь: `{assessment_created_by}`; Результат: `{assessment_status_value}`; Описание: Выполнение проверки завершено успешно; Время запуска проверки: `{assessment_created_at}`; Время	OVAL Event		

Табл. 160. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИСТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВАТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫПОЛНЕНИЕ ФУНКЦИИ
			окончания проверки: `{assessment_updated_at}`; IP актива: `{host_interface_ip_v4_address}`; MAC актива: `{host_interface_mac_address}`; `{self.assessment_status_value}`;Количество OVAL-определений: `{oval_definitions_count}`; Количество выполненных проверок: `{performed_checks_count}`; Состояние соответствия: есть несоответствия/уязвимостей нет; Количество выявленных несоответствий: `{compliance_false_count}`; Количество выявленных уязвимостей: `{vulnerabilities_true_count}`			

Табл. 160. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИСТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВАТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫПОЛНЕНИЕ ФУНКЦИИ
1110008	В результате проверки на соответствие требованиям ИБ обнаружены уязвимости	Выполнение проверки завершено успешно	Название проверки: {assessment_title}; Название актива: {host_netbios_name}; ID актива: {assessment_host_id}; Пользователь: {assessment_created_by}; Результат: {assessment_status_value}; Описание: Выполнение проверки завершено успешно; Время запуска проверки: {assessment_created_at}; Время окончания проверки: {assessment_updated_at}; IP актива: {host_interface_ip_v4_address}; MAC актива: {host_interface_mac_address}; {self.assessment_status_value};Количество OVAL-определений: {oval_	OVAL Event		

Табл. 160. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИСТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВАТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫПОЛНЕНИЕ ФУНКЦИИ
			`definitions_count}`; Количество выполненных проверок: `{performed_checks_count}`; Состояние соответствия: соответствуют/есть уязвимости; Количество выявленных несоответствий: `{compliance_false_count}`; Количество выявленных уязвимостей: `{vulnerabilities_true_count}`			
1110009	В результате проверки на соответствие требованиям ИБ уязвимости и несоответствия не обнаружены	Выполнение проверки завершено успешно	Название проверки: `{assessment_title}`; Название актива: `{host_netbios_name}`; ID актива: `{assessment_host_id}`; Пользователь: `{assessment_created_by}`; Результат: `{assessment_status_value}`; Описание: Выполнение проверки завершено	OVAL Event		

Табл. 160. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИСТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВАТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫПОЛНЕНИЕ ФУНКЦИИ
			успешно; Время запуска проверки: {assessment_created_at}; Время окончания проверки: {assessment_updated_at}; IP актива: {host_interface_ip_v4_address}; MAC актива: {host_interface_mac_address}; {self.assessment_status_value};Количество OVAL-определений: {oval_definitions_count}; Количество выполненных проверок: {performed_checks_count}; Состояние соответствия: соответствуют/уязвимостей нет; Количество выявленных несоответствий: {compliance_false_count}; Количество выявленных уязвимостей:			

Табл. 160. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИСТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВАТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫПОЛНЕНИЕ ФУНКЦИИ
			`{vulnerabilities_true_count}`			
1110010	В результате проверки на соответствие требованиям ИБ получена ошибка	Ошибка получения результатов задачи проверки	Название проверки: `{assessment_title}`; Название актива: `{host_netbios_name}`; ID актива: `{assessment_host_id}`; Пользователь: `{assessment_created_by}`; Результат: `{assessment_status_value}`; Описание: Ошибка получения результатов задачи проверки; Время запуска проверки: `{assessment_created_at}`; Время окончания проверки: `{assessment_updated_at}`; IP актива: `{host_interface_ip_v4_address}`; MAC актива: `{host_interface_mac_address}`; Ошибка: `{error}`	OVAL Event		

Табл. 160. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИСТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВАТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫПОЛНЕНИЕ ФУНКЦИИ
1110011	Пользователь удаляет несколько проверок на соответствие требованиям ИБ	Удалены проверки OVAL	Обоснование: `{justification}`; Пользователь: `{user_login}`; Фильтр: [Активы: `{filter_hosts}`; Инициатор: `{filter_created_by}`; Статус: `{filter_status}`; Дата обновления от: `{filter_updated_at_from}`; Дата обновления до: `{filter_updated_at_to}`; Название: `{filter_title}`]; Количество удаленных проверок: `{deleted_count}`	OVAL Event	`/host_data_collector/oval/assessments/bulk/delete` `DELETE`	Администратор Инженер
1110012	Пользователь удаляет проверку на соответствие требованиям ИБ	Удалена проверка	Пользователь: `{user_login}`; Обоснование: `{justification}`; Проверка: [Название: `{assessment_title}`; Наименование актива: `{host_netbios_name}`; Инициатор:	OVAL Event	`/host_data_collector/oval/assessments/[assestment_id]/delete` `DELETE`	

Табл. 160. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИСТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВАТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫПОЛНЕНИЕ ФУНКЦИИ
			{assessment_created_by}; Статус: {assessment_status}]			
1120001	Пользователь удаляет OVAL-определение	Удалено OVAL-определение	Пользователь: {user_login}; Обоснование: {justification}; OVAL-определение: [Название: {definition_title}; Описание: {definition_description}; Тип: {definition_type}; OVAL-идентификатор: {definition_oval_id}]	OVAL Event	oval_scanner/oval/definitions/delete POST	
1120002	Пользователь удаляет несколько OVAL-определений	Удалены OVAL-определения	Пользователь: {user_login}; Обоснование: {justification}; Фильтр: [Название: {definition_title}; Описание: {definition_description}; Тип проверки: {definition_type}; OVAL-идентификатор: {definition_oval_id}; Се-	OVAL Event	/oval_scanner/definitions/bulk/delete POST	

Табл. 160. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИСТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВАТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫПОЛНЕНИЕ ФУНКЦИИ
			мейство платформ: `{definition_affected_families}`; Платформы: `{definition_affected_platforms}`; Продукты: `{definition_affected_products}`]; Количество удаленных определений: `{deleted_count}`]			
1120003	Пользователь предпринимает неудачную попытку удалить несколько OVAL-определений	Не удалось выполнить групповое удаление OVAL определений	Ошибка `{error_message}`; Пользователь: `{user_login}`; Обоснование: `{justification}`; Фильтр: [Название: `{definition_title}`; Описание: `{definition_description}`; Тип проверки: `{definition_type}`; OVAL-идентификатор: `{definition_oval_id}`; Семейство платформ: `{definition_affected_families}`; Платформы:	OVAL Event	`/oval_scanner/definitions/bulk/delete` `POST`	Администратор Инженер Просмотрщик

Табл. 160. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИСТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВАТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫПОЛНЕНИЕ ФУНКЦИИ
			`{definition_affected_platforms}`; Продукты: `{definition_affected_products}`]			
1130001	Пользователь удаляет несколько групп OVAL-определений	Удалены группы OVAL-определений	Пользователь: `{user_login}`; Обоснование: `{justification}`; Фильтр: [Название или описание содержит: `{filter_search}`]; Количество удаленных групп: `{deleted_count}`	OVAL Event	`/oval_scanner/oval/groups/bulk/delete` `POST`	Администратор
1130002	Пользователь удаляет группу OVAL-определений	Удалена группа OVAL-определений	Пользователь: `{user_login}`; Обоснование: `{justification}`; Группа OVAL определений: [Название: `{oval_group_title}`; Описание: `{oval_group_description}`;]	OVAL Event	`/oval_scanner/oval/groups/[group_id]/delete` `POST`	Администратор
1150001	При попытке сохранения сканера об-	Ошибка верификации сканера	Ошибка: `{error}`	Script Verification	`/host_data_collector/scanners`	Администратор

Табл. 160. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИСТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВАТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫПОЛНЕНИЕ ФУНКЦИИ
	наружена ошибка в синтаксисе скрипта				`POST`	
1150002	Пользователь, которому не назначена соответствующая роль, предпринимает неудачную попытку импорта сканеров сбора данных	Попытка импорта сканеров пользователем без соответствующих ролей	Ошибка: `{error}`; Пользователь: `{user}`	Script Verification	`/host_data_collector/scanner_groups` `POST`	Администратор
1150003	Пользователь, которому не назначена соответствующая роль, предпринимает неудачную попытку создания сканера сбора данных	Попытка создания сканера пользователем без соответствующих ролей	Ошибка: `{error}`; Пользователь: `{user}`	Script Verification	`/host_data_collector/scanners` `POST`	Администратор
1150004	Пользователь, которому не назначена соответствующая роль, предпринимает	Попытка внесения изменений в сканер пользователем без	Ошибка: `{error}`; Пользователь: `{user}`	Script Verification		

Табл. 160. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИСТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВАТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫПОЛНЕНИЕ ФУНКЦИИ
	неудачную попытку изменения сканера сбора данных	соответствующих ролей				
1150005	Пользователь, которому не назначена соответствующая роль, предпринимает неудачную попытку создания скрипта OVAL	Попытка создания скрипта OVAL пользователем без соответствующих ролей	Ошибка: `{error}`; Пользователь: `{user}`	Script Verification	`/oval_scanner/oval/scripts` `POST`	Администратор
1150006	Пользователь, которому не назначена соответствующая роль, предпринимает неудачную попытку изменения скрипта OVAL	Попытка внесения изменений в скрипт OVAL пользователем без соответствующих ролей	Ошибка: `{error}`; Пользователь: `{user}`	Script Verification	`/oval_scanner/oval/scripts/[script_id]` `PATCH`	Администратор
1150007	Пользователь, которому не назначена соответствующая	Попытка импорта скриптов OVAL поль-	Ошибка: `{error}`; Пользователь: `{user}`	Script Verification	`/host_data_collector/oval/scripts/import` `POST`	

Табл. 160. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИСТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВАТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫПОЛНЕНИЕ ФУНКЦИИ
	роль, предпринимает неудачную попытку импорта скриптов OVAL	зователем без соответствующих ролей				
1160001	Пользователь авторизовался	Успешный вход в Комплекс	Пользователь: `{user}`; IP-адрес: `{user_ip}`	User Action Control	`/users/auth_token` `GET`	Все роли
1160002	Авторизоваться не удалось	Неудачная попытка входа в Комплекс	Пользователь: `{user_name}`; IP-адрес: `{client_ip}`	User Action Control	`/users/auth_token` `GET`	Генерируется при выполнении действия неавторизованным пользователем
1160003	Пользователь выполняет какие-либо действия без соответствующих ролей	Ошибка аутентификации	Ошибка: `{error}`; IP-адрес: `{user_ip}`	User Action Control	`/users/auth_token` `GET`	Все роли

Табл. 160. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИСТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВАТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫПОЛНЕНИЕ ФУНКЦИИ
1160006	Пользователь нажал кнопку «Выход»	Успешный выход из Комплекса	Пользователь: `{user}` IP-адрес: `{user_ip}`	User Action Control	`/users/auth_token` `GET`	Все роли
1160007	Пользователь изменил пароль и другие данные учетной записи (своей или чужой)	Изменены данные и пароль учетной записи пользователя	Ответственный: `{login_initiator}`; Пользователь, чьи данные были изменены: `{login_edited}`; Старые значения: [Состояние: `{old_state}`, Роль: `{old_role}`, Логин: `{old_login}`, Имя: `{old_name}`, Отчество: `{old_patronymic_name}`, Фамилия: `{old_surname}`], Новые значения: [Состояние: `{new_state}`, Роль: `{new_role}`, Логин: `{new_login}`, Имя: `{new_name}`, Отчество: `{new_patronymic_name}`, Фамилия: `{new_surname}`]	User Action Control	`/users/[uuid:user_id]` `PATCH`	Администратор

Табл. 160. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИСТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВАТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫПОЛНЕНИЕ ФУНКЦИИ
1160011	Попытка сохранения учетной записи с логином, уже существующим в Комплексе	Не удалось изменить данные учетной записи пользователя: пользователь с таким логином уже существует	Пользователь: `{login}`	User Action Control	`/users/[uuid:user_id]` `PATCH`	Администратор
1160012	Попытка изменения статуса активности собственной учетной записи	Не удалось изменить данные учетной записи пользователя: деактивация текущего пользователя невозможна	Пользователь: `{login}`	User Action Control	`/users/[uuid:user_id]` `PATCH`	Администратор
1160016	Пользователь меняет пароль своей учетной записи	Изменен пароль учетной записи	Учетная запись: `{target_user_login}`; Пользователь: `{source_user_login}`	User Action Control	`/users/current_user/password` `PATCH`	Все роли
1160018	Пользователь редактирует данные учетной записи,	Изменены данные учетной записи пользователя. Пароль не изменен	Ответственный: `{login_initiator}`; Пользователь, чьи данные были изменены: `{login_edited}`;	User Action Control	`/users/[uuid:user_id]` `PATCH`	Администратор

Табл. 160. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИСТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВАТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫПОЛНЕНИЕ ФУНКЦИИ
	оставляя пароль прежним		Старые значения: [Состояние: `{old_state}`, Роль: `{old_role}`, Логин: `{old_login}`, Имя: `{old_name}`, Отчество: `{old_patronymic_name}`, Фамилия: `{old_surname}`], Новые значения: [Состояние: `{new_state}`, Роль: `{new_role}`, Логин: `{new_login}`, Имя: `{new_name}`, Отчество: `{new_patronymic_name}`, Фамилия: `{new_surname}`]			
1160026	Пользователь отредактировал парольную политику	Изменена парольная политика	Старые значения: [`{old_policy_fields}`]; Новые значения [`{new_policy_fields}`]	User Action Control	`/`	Администратор
1160027	Пользователь создал учетную запись пользователя Комплекса	Пользователь создан	Состояние: `{new_state}`, Роль: `{new_role}`, Логин: `{new_login}`, Имя: `{new_name}`, Отчество: `{new_`	User Action Control	`/users` `POST`	

Табл. 160. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИСТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВАТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫПОЛНЕНИЕ ФУНКЦИИ
			`patronymic_name}`, Фамилия: `{new_surname}`			
1160028	Пользователь удалил учетную запись пользователя Комплекса	Пользователь удален	Состояние: `{new_state}`, Роль: `{new_role}`, Логин: `{new_login}`, Имя: `{new_name}`, Отчество: `{new_patronymic_name}`, Фамилия: `{new_surname}`	User Action Control	`/users/[user_id]` `DELETE`	
1160029	Пользователь выполнил вход в веб-интерфейс Комплекса с нового устройства, не выполнив выход с предыдущего, при условии, что переменная `LIMIT_USER_SESSIONS` имеет значение `true`	Обнаружено одновременное использование веб-интерфейса Комплекса более, чем на одном устройстве пользователем `{user_login}`	Пользователь: `{user}`; IP-адрес первого устройства: `{old_ip}`; IP-адрес второго устройства: `{new_ip}`	User Action Control		

Табл. 160. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИСТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВАТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫПОЛНЕНИЕ ФУНКЦИИ
1180001	Оперативная память на ОС Комплекса заполнена на значение, превышающее заданное в переменной `DATAPK_MAX_RAM_PERCENTAGE_CONSUMED`	Обнаружено превышение потребления оперативной памяти (RAM)	Комплекс: `{hostname_label}`; Превышен порог в `{max_ram_consumed_percentage}`%	System Control	нет (внутренняя пассивная функция Комплекса)	нет
1180002	Потребление оперативной памяти снижено до значений, не превышающих заданных в переменной `DATAPK_MAX_RAM_PERCENTAGE_CONSUMED`	Потребление оперативной памяти (RAM) нормализовано	Комплекс: `{hostname_label}`	System Control	нет (внутренняя пассивная функция Комплекса)	нет
1180003	Заполненность диска на ОС Комплекса превысило значение, заданное в переменной `MAX_DISK_`	Обнаружено переполнение дискового пространства (HDD/SSD) на Комплексе	Комплекс: `{hostname_label}`; Превышен порог в `{max_disk_space_consumed_percentage}`%	System Control	нет (внутренняя пассивная функция Комплекса)	нет

Табл. 160. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИСТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВАТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫПОЛНЕНИЕ ФУНКЦИИ
	`SPACE_CONSUMED_PERCENTAGE`					
1180004	Дисковое пространство освобождено до значений, не превышающих заданных в переменной `MAX_DISK_SPACE_CONSUMED_PERCENTAGE`	Переполнение дискового пространства (HDD, SSD) на Комплексе устранено	Комплекс: `{hostname_label}`	System Control	нет (внутренняя пассивная функция Комплекса)	нет
1180005	Нагрузка на центральный процессор ОС Комплекса превысила значение, заданное в переменной `MAX_CPU_LOAD_CONSUMED_PERCENTAGE`	Обнаружено превышение нагрузки на центральный процессор (CPU)	Комплекс: `{hostname_label}`; Превышен порог в `{max_cpu_load_consumed_percentage}`%	System Control	нет (внутренняя пассивная функция Комплекса)	нет
1180006	Нагрузка на центральный процессор	Нагрузка на центральный процессор	Комплекс: `{hostname_label}`	System Control	нет (внутренняя пассивная функция Комплекса)	нет

Табл. 160. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИСТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВАТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫПОЛНЕНИЕ ФУНКЦИИ
	снижена до значений, не превышающих заданных в переменной `MAX_CPU_LOAD_CONSUMED_PERCENTAGE`	(CPU) нормализована				
1180007	Средняя нагрузка на ОС Комплекса превысила значение, заданное в переменной `DATAPK_MAX_LA`	Обнаружено превышение средней нагрузки (Load average)	Комплекс: `{hostname_label}`; Значение превышает `{max_la}`	System Control	нет (внутренняя пассивная функция Комплекса)	нет
1180008	Средняя нагрузка снижена до значений, не превышающих заданных в переменной `DATAPK_MAX_LA`	Средняя нагрузка (Load average) нормализована	Комплекс: `{hostname_label}`	System Control	нет (внутренняя пассивная функция Комплекса)	нет
1180009	Пользователь меняет NTP-серверы	NTP-серверы изменены	Старое значение: `{old_value}`; Новое значение: `{new_value}`	datapk sensor	нет (внутренняя пассивная функция Комплекса)	учетная запись администратора ОС

Табл. 160. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИСТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВАТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫПОЛНЕНИЕ ФУНКЦИИ
1180010	Пользователь меняет временную зону Комплекса	Временная зона (TZ) Комплекса была изменена	Старое значение: `{old_value}`; Новое значение: `{new_value}`	datapk sensor	нет (внутренняя пассивная функция Комплекса)	учетная запись администратора ОС
1180011	Брокер сообщений потребляет больше оперативной памяти, чем указано в переменной `RMQ_LOW_AVAILABLE_MEMORY_WATERMARK_BYTES`	Обнаружено превышение потребления выделенной для брокера сообщений оперативной памяти (RAM)	Комплекс: `{hostname_label}`; Лимит RAM: `{low_available_memory_watermark_mb}` Мбайт	System Control	нет (внутренняя пассивная функция Комплекса)	нет
1180012	Потребление оперативной памяти брокером нормализовано до значений, не превышающих указанных в переменной `RMQ_LOW_AVAILABLE_MEMORY_WATERMARK_BYTES`	Потребление выделенной для брокера сообщений оперативной памяти (RAM) нормализовано	Комплекс: `{hostname_label}`; Лимит RAM: `{low_available_memory_watermark_mb}` Мбайт	System Control	нет (внутренняя пассивная функция Комплекса)	нет

Табл. 160. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИСТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВАТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫПОЛНЕНИЕ ФУНКЦИИ
1180013	Брокер сообщений потребляет больше дискового пространства, чем указано в переменной `RMQ_LOW_AVAILABLE_DISK_SPACE_WATERMARK_BYTES`	Обнаружено переполнение выделенного для брокера сообщений дискового пространства (HDD/SSD) на Комплексе	Комплекс: `{hostname_label}`; Лимит HDD/SSD: `{low_available_disk_space_watermark_mb}` Мбайт	System Control	нет (внутренняя пассивная функция Комплекса)	нет
1180014	Дисковое пространство освобождено до значений, не превышающих заданных в переменной `RMQ_LOW_AVAILABLE_DISK_SPACE_WATERMARK_BYTES`	Переполнение выделенного для брокера сообщений дискового пространства (HDD, SSD) устранено	Комплекс: `{hostname_label}`; Лимит HDD/SSD: `{low_available_disk_space_watermark_mb}` Мбайт	System Control	нет (внутренняя пассивная функция Комплекса)	нет
1180015	Запрос к сенсору остался без ответа	Не удается установить соединение с сенсором	Сенсор: `{node_name}({node_id}`; Источник данных: `{exporter_name}`; Был до-	System Control	нет (внутренняя пассивная функция Комплекса)	нет

Табл. 160. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИСТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВАТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫПОЛНЕНИЕ ФУНКЦИИ
			ступен `{max_delay:.3f}` минут назад;			
1180016	Соединение с сенсором восстановлено	Соединение с сенсором восстановлено	Сенсор: `{node_name}({node_id}`;	System Control	нет (внутренняя пассивная функция Комплекса)	нет
1180017	Комплексу не удается установить соединение с сервисом получения данных на сенсоре	Не удается установить соединение с сенсором. Получение данных недоступно	Сенсор: `{node_name}({node_id}`; Был доступен `{max_delay.3f}` минут назад;	System Control	нет (внутренняя пассивная функция Комплекса)	нет
1180018	Комплекс установил соединение с сервисом получения данных на сенсоре	Соединение и возможность получения данных с сенсора восстановлены	Сенсор: `{node_name}({node_id}`;	System Control	нет (внутренняя пассивная функция Комплекса)	нет
1180019	Комплексу не удается установить соединение с сервисом отправки данных на сенсоре	Недоступен сервис отправки данных с сенсора	Сенсор: `{node_name}({node_id}`; Был доступен `{max_delay:.3f}` минут назад;	System Control	нет (внутренняя пассивная функция Комплекса)	нет

Табл. 160. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИСТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВАТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫПОЛНЕНИЕ ФУНКЦИИ
1180020	Комплекс установил соединение с сервисом отправки данных на сенсоре	Доступность сервиса отправки данных восстановлена	Сенсор: `{node_name}({node_id}`;	System Control	нет (внутренняя пассивная функция Комплекса)	нет
1180021	Комплексу не удается установить соединение с сервисом синхронизации настроек на сенсоре	Не удается установить соединение с сенсором. Синхронизация настроек недоступна	Сенсор: `{node_name}({node_id}`; Был доступен `{max_delay:.3f}` минут назад;	System Control	нет (внутренняя пассивная функция Комплекса)	нет
1180022	Комплексу установил соединение с сервисом синхронизации настроек на сенсоре	Соединение и возможность синхронизации настроек сенсора восстановлены	Сенсор: `{node_name}({node_id}`;	System Control	нет (внутренняя пассивная функция Комплекса)	нет
1180023	Сервис синхронизации настроек на сенсоре не отвечает	Недоступен сервис синхронизации настроек	Сенсор: `{node_name}({node_id}`; Был доступен `{max_delay:.3f}` минут назад;	System Control	нет (внутренняя пассивная функция Комплекса)	нет
1180024	Работоспособность сервиса синхро-	Доступность сервиса синхро-	Сенсор: `{node_name}({node_id}`;	System Control	нет	нет

Табл. 160. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИСТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВАТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫПОЛНЕНИЕ ФУНКЦИИ
	низации настроек на сенсоре восстановлена	низации настроек восстановлена			(внутренняя пассивная функция Комплекса)	
1180025	Соединение между Комплексом и сенсором было прервано некоторое время. Часть накопленных за этот период данных для отправки будет удалена	Достигнут установленный лимит для отправки данных. Старейшие данные будут удалены	Сенсор: `{node_name}({node_id}`;	System Control	нет (внутренняя пассивная функция Комплекса)	нет
1180026	Соединение между Комплексом и сенсором было восстановлено. Данные отправляются в обычном режиме	Отправка данных нормализована	Сенсор: `{node_name}({node_id}`;	System Control	нет (внутренняя пассивная функция Комплекса)	нет
1180027	Пользователь удаляет сенсор	Удален сенсор	Наименование сенсора: `{node_name}`; Идентификатор сенсора: `{node_id}`; Пользо-	System Control	нет (внутренняя пассивная функция Комплекса)	нет

Табл. 160. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИСТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВАТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫПОЛНЕНИЕ ФУНКЦИИ
			ватель: `{user}`; Обоснование: `{justification}`			
1180028	Сенсор отклоняет сообщения от источника	Сенсор отклонил входящее сообщение от источника: не удалось обработать текст сообщения	Сенсор: `{node_name}({node_id})`;	System Control		
1180029	На сенсоре восстановлен прием сообщений от источника	Прием сенсором входящих сообщений от источника восстановлен	Сенсор: `{node_name}({node_id})`;	System Control		
1180030	Пользователь изменил NTP-серверы на сенсоре	NTP-серверы изменены на сенсоре	Сенсор: `{node_id}`; Старое значение: `{old_value}`; Новое значение: `{new_value}`	System Control		
1180031	Пользователь изменил временную зону сенсора	Временная зона (TZ) сенсора была изменена	Сенсор: `{node_id}`; Старое значение: `{old_value}`; Новое значение: `{new_value}`	System Control		

Табл. 160. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИСТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВАТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫПОЛНЕНИЕ ФУНКЦИИ
1180032	Комплекс автоматически выполнил проверку контрольных сумм исполняемых файлов. По результатам не обнаружено нарушение целостности файлов	Успешная проверка контрольных сумм исполняемых файлов: целостность файлов не нарушена	Проверяемый компонент: `{node_name}`; Дата проверки: `{created}`	System Control		Администратор
1180033	Комплекс автоматически выполнил проверку контрольных сумм исполняемых файлов. По результатам было обнаружено нарушение целостности файлов	Обнаружено нарушение целостности исполняемых файлов в результате проверки их контрольных сумм	Проверяемый компонент: `{node_name}`; Отчет: `{report_path}`; Дата проверки: `{created}`	System Control		Администратор
1180034	Комплекс остановил обработку внешних событий, поступаемых от сенсоров, по	Остановлена обработка внешних событий от сенсоров из-за нехватки системных ресурсов.	Остановлена обработка внешних событий от сенсоров из-за нехватки системных ресурсов. Запущено удаление	System Control		

Табл. 160. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИСТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВАТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫПОЛНЕНИЕ ФУНКЦИИ
	причине нехватки системных ресурсов	Запущено удаление внешних событий старше 1ч. Обратитесь в техподдержку	внешних событий старше 1ч. Обратитесь в техподдержку			
1180035	Комплекс возобновил обработку внешних событий, поступаемых от сенсоров	Восстановлена обработка внешних событий от сенсоров после освобождения системных ресурсов	Восстановлена обработка внешних событий от сенсоров после освобождения системных ресурсов	System Control		
1220001	Пользователь запускает сканирование сети	Запущено сканирование сети	Диапазон сканирования: `{first_ip}` - `{last_ip}`; Пользователь: `{user}`	home_net	`/scan` `POST`	Администратор
1220002	Сеть была успешно просканирована	Сканирование сети успешно завершено	Диапазон сканирования: `{first_ip}` - `{last_ip}`	home_net	нет (внутренняя пассивная функция Комплекса)	нет
1220003	Не удалось завершить сканирование сети	Обнаружена ошибка при попытке сканирования сети	Ошибка: `{error}`	home_net	нет (внутренняя пассивная функция Комплекса)	нет

Табл. 160. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИСТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВАТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫПОЛНЕНИЕ ФУНКЦИИ
1250001	Обнаружено туннелирование протокола	T1572: Туннелирование протокола	Вероятность: {prob}%	ML Control		
1250002	Обнаружено туннелирование протокола	T1572: Туннелирование протокола	Вероятность: {prob}%	ML Control		
1250003	Обнаружена генерация доменных имен с помощью алгоритма	T1568.002: Алгоритмы генерирования доменных имен	Вероятность: {prob}%; Семейство: {family}	ML Control		
1260001	Значение тега нарушает правило контроля тега, установленного пользователем	Значение тега "`{tag_name}`" не соответствует критериям правила	Значение тега "{tag_name}" = {tag_value}	Tag Control		
1260002	Пользователь изменил значение тега и оно больше не нарушает правило контроля тега, уста-	Значение тега "`{tag_name}`" нормализовалось	Значение тега "{tag_name}" = {tag_value}	Tag Control		

Табл. 160. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИСТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВАТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫПОЛНЕНИЕ ФУНКЦИИ
	новленного пользователем					
1260003	Пользователь удалил правило контроля тегов	Удалено правило контроля тегов "`{rule_name}`"	Обоснование: {justification}; Пользователь: {user_login}	Tag Control		
1260004	Пользователь активировал правило контроля тегов	Активировано правило контроля тегов "`{rule_name}`"		Tag Control		
1260005	Пользователь деактивировал правило контроля тегов	Деактивировано правило контроля тегов "`{rule_name}`"		Tag Control		
1270001	Комплекс обнаружил сессию, не соответствующую активным правилам сессий	Обнаружена сессия, не разрешенная правилами сессий		Session Control		
1270002	Режим работы контроля сессий был изменен	Изменен режим работы контроля сессий	Режим изменен на: service_mode={Режим обучения, Режим обнаружения}	Session Control		

Табл. 160. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИСТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВАТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫПОЛНЕНИЕ ФУНКЦИИ
1270003	Пользователь удалил правило сессий	Удалено правило сессий	Пользователь: {user}; Правило: {rule_id}	Session Control		
1270004	Пользователь удалил несколько правил сессий	Удалены правила сессий	Пользователь: {user}; Правила: {rule_ids}; Количество правил: {count}	Session Control		
1270005	Пользователь активировал правило сессий	Активировано правило сессий	Пользователь: {user}; Правило: {rule_id}	Session Control		
1270006	Пользователь активировал несколько правил сессий	Активированы правила сессий	Пользователь: {user}; Правила: {rule_ids}; Количество правил: {count}	Session Control		
1270007	Пользователь деактивировал несколько правил сессий	Деактивированы правила сессий	Пользователь: {user}; Правила: {rule_ids}; Количество правил: {count}	Session Control		
1280001	Пользователь удалил правило обнаружения вторжений	Удалено правило обнаружения вторжений	Пользователь: `{user_login}`; Обоснование:	IDS Control		

Табл. 160. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИСТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВАТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫПОЛНЕНИЕ ФУНКЦИИ
			`{justification}`; ID правила: `{rule_id}`			
1280002	Пользователь удалил несколько правил обнаружения вторжений	Удалены правила обнаружения вторжений	Пользователь: {user_login}; Обоснование: {justification}; ID правил: {rule_ids}; Всего удалено правил: {len_rule_ids}	IDS Control		
1280006	Пользователь деактивировал несколько правил обнаружения вторжений	Деактивированы правила обнаружения вторжений	Правила (ID правила - Сенсор): {rule_sid_ids}; Обоснование: {justification}; Всего деактивировано правил: {len_rule_ids}	IDS Control		
1280007	Пользователь активировал правило обнаружения вторжений	Активировано правило обнаружения вторжений	ID правила: `{rule_id}`; Сенсор: `{node_hostname}`	IDS Control		
1280008	Пользователь активировал несколько правил обнаружения вторжений	Активированы правила обнаружения вторжений	Правил (ID правила - Сенсор): `{rule_sid_ids}`; Обоснование: `{justification}`; Всего ак-	IDS Control		

Табл. 160. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИСТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВАТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫПОЛНЕНИЕ ФУНКЦИИ
			тивировано правил: `{len_rule_ids}`			
1300001	Зафиксирована попытка недопустимого перехода между состояниями модели на основе временного автомата	Уведомления OTALA-агента: недопустимый переход		EDR for PLC		
1300002	Обнаружено отклонение временных параметров выполнения операции от ожидаемых значений в рамках модели на основе временного автомата	Уведомления OTALA-агента: временная аномалия		EDR for PLC		
1300003	Обнаружены потенциально опасные шаблоны в данных, обрабатываемых	Алерты QDICT-агента		EDR for PLC		

Табл. 160. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИСТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВАТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫПОЛНЕНИЕ ФУНКЦИИ
	моделью на основе иерархического словаря					
1300004	Зафиксирован сетевой трафик с характеристиками, не соответствующими эталонным	Уведомления о ранее неизвестных сетевых сигналах		EDR for PLC		
1300005	Модуль «EDR for PLC» собрал и предоставил актуальные данные о функционировании моделей	Показатели функционирования (или метрики агентов)		EDR for PLC		
1300006	Обнаружено расхождение между прогнозируемыми и фактическими данными модели на основе гибридного автомата	Уведомления гибридного автомата: ошибка предсказания внутри состояния		EDR for PLC		

Табл. 160. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИСТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВАТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫПОЛНЕНИЕ ФУНКЦИИ
1300007	Зафиксирована попытка несуществующего перехода между состояниями модели на основе гибридного автомата	Уведомления гибридного автомата: выполнен запрещенный (несуществующий) переход		EDR for PLC		
1300008	Зафиксировано уведомление от modbus-детектора модели на основе гибридного автомата	Алерты modbus-детекторов в рамках гибридного автомата: сработал детектор		EDR for PLC		
230001	Пользователь создал репозиторий для хранения версий проекта ПЛК	Создан репозиторий	Путь: `{group_path}`; Наименование проекта: `{project_name}`; Описание: `{description}`; ID проекта: `{project_id}`	Version Control		
230002	Пользователь изменил репозиторий для хранения версий проекта ПЛК	Изменен репозиторий	Старые значения: [ID проекта: `{project_id}`; Наименование проекта: `{old_project_name}`; Описание:	Version Control		

Табл. 160. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИСТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВАТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫПОЛНЕНИЕ ФУНКЦИИ
			{old_description}; Путь: {old_group_path}]; Новые значения: [ID проекта: {project_id}; Наименование проекта: {new_project_name}; Описание: {new_description}; Путь: {new_group_path}]			
230003	Пользователь удалил репозиторий для хранения версий проекта ПЛК	Удален репозиторий	Путь: {group_path}; Наименование проекта: {project_name}; Описание: {description}; ID проекта: {project_id}	Version Control		
230004	Пользователь изменил древовидную структуру групп репозиториев для хранения версий проектов ПЛК	Изменены группы репозиториев	Измененные группы: {changed_paths}; Число удаленных: {removed_quantity}; Число созданных: {created_quantity}; Число измененных: {changed_quantity}	Version Control		

Табл. 160. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИСТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВАТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫПОЛНЕНИЕ ФУНКЦИИ
230005	Пользователь создал новую версию проекта ПЛК и отправил ее на сервер	Добавлена новая версия проекта Обоснование изменений: `{justification}`; Описание изменений: `{details}`; Пользователь: `{user}`	Путь: `{tree_path}`; Название: `{project_name}`; Описание: `{project_description}`; ID:`{project_id}`	Version Control		
230006	Пользователь заблокировал проект для запрета его изменения	Проект заблокирован	Наименование проекта: `{project_name}`; Причина блокировки: `{justification}`; ID проекта: `{project_id}`; Инициатор блокировки: `{user}`	Version Control		
230007	Пользователь разблокировал проект для возможности его изменения	Проект разблокирован	Наименование проекта: `{project_name}`; ID проекта: `{project_id}`; Инициатор разблокировки: `{user}`	Version Control		

Табл. 160. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИСТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВАТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫПОЛНЕНИЕ ФУНКЦИИ
230009	Пользователь скачал из репозитория файлы проекта ПЛК выбранной версии	Скачивание проекта из репозитория	Пользователь: `{user}`; Проект: `{project_name}` (`{project_id}`); Путь: `{tree_path}`; Версия: `{commit_short_id}`	Version Control		
230012	Пользователь подключил актив к проекту	Подключен актив к проекту	Пользователь: `{user}`; Актив: `{target_hostname}` (ID: `{target_id}`); Проект: `{project_name}` (`{project_id}`)	Version Control		
230013	Пользователь отключил актив от проекта	Отключен актив от проекта	Пользователь: `{user}`; Актив: `{target_hostname}` (ID: `{target_id}`); Проект: `{project_name}` (`{project_id}`)	Version Control		
230014	Пользователь удалил актив, подключенный к проекту	Удалена связь проекта с активом в результате удаления актива	Актив: `{target_hostname}` (ID: `{target_id}`); Проект: `{project_name}` (`{project_id}`)	Version Control		

См. также

Описание служебных источников событий

22.7. Механизмы хранения событий

Механизм хранения внешних событий

Комплекс по умолчанию выполняет ротацию (поэтапное хранение, архивирование и удаление) событий. Администратор ОС, в которой функционирует Комплекс, может добавлять и изменять в конфигурационном файле `manager.env` следующие параметры политики хранения событий:

- `EVENT_INDICES_MAX_SIZE_GB` — максимальный объем оперативного архива событий;
- `EVENT_INDICES_LIFETIME_DAYS` — максимальное время хранения событий в оперативном архиве;
- `EVENT_ARCHIVES_LIFETIME_DAYS` — время хранения внешних событий в глубоком архиве,;
- `EVENT_INDICES_LIFETIME_DAYS` — время хранения внешних событий в оперативном архиве;
- `EVENT_ARCHIVES_MAX_SIZE_GB` — максимально допустимый объем глубокого архива внешних событий.

> Прим.:
>
> Подробнее о рекомендациях по использованию переменных см. в разделе «Рекомендации по использованию переменных файлов manager.env и sensor.env» Руководства по эксплуатации.

По умолчанию ротация событий Комплекса выполняется в соответствии со следующими правилами:

1. Один раз в сутки Комплекс проверяет количество доступного места для хранения оперативных и архивных событий, а также время их хранения.
2. Оперативные события, время хранения которых превышено, архивируются в директорию `/var/backups/elasticsearch/indicies` в файл с названием `datapk-events-yyyy-mm-dd` .
3. При превышении максимального объема памяти для хранения оперативных событий или при превышении времени хранения оперативных событий самые ранние хранимые события архивируются (выполняется архивация событий (индекса) за те сутки, которые ближе всего к максимальному времени хранения).
4. Архивирование событий выполняется по тому условию (по превышению объема памяти или по превышению времени хранения), которое возникло раньше.
5. Максимальное время хранения архива событий включает в себя максимальное время хранения оперативных событий.
6. Архивные события, время хранения которых превышено, удаляются.
7. При превышении максимального объема памяти для хранения архивных событий самые ранние архивные события удаляются (выполняется удаление событий в архиве за те сутки, которые ближе всего к максимальному времени хранения в архиве).
8. В случае генерации аномально большого количества событий за сутки сервис Комплекса отключает генерацию событий при превышении 90% общего объема дискового пространства.
9. При превышении максимального объема памяти для хранения оперативных событий до момента суточной проверки количества доступного объема памяти Комплекс продолжает генерировать и сохранять новые события (с превышением ограничения на объем памяти для хранения оперативных событий) до момента очередной суточной проверки.

Механизм хранения внутренних событий

С помощью сервиса регистрации внутренних событий Комплекса выполняется ротация (поэтапное хранение, архивирование и удаление) внутренних событий.

Администратор ОС, в которой функционирует Комплекс, может добавлять и изменять в конфигурационном файле `manager.env` следующие параметры политики хранения внутренних событий:

- `EVENTS_RETENTION_MONTHS` — максимальное время хранения внутренних событий;
- `EVENTS_RETENTION_DISK_CAPACITY_SIZE_MB` — максимальный объем архива внутренних событий.

> Прим.:
>
> В случае превышения объема архива, указанного в этой переменной, необходимо очистить дисковое пространство от внутренних событий с помощью скрипта очистки. Подробнее см. в разделе «Очистка дискового пространства от внутренних событий».

Прим.:

Подробнее о рекомендациях по использованию переменных см. в разделе «Рекомендации по использованию переменных файлов manager.env и sensor.env» Руководства по эксплуатации.

По умолчанию ротация внутренних событий Комплекса выполняется в соответствии со следующими правилами:

1. Комплекс создает архив событий раз в месяц на основе поля `create_time` в событиях: при создании архива учитываются первая и последняя даты текущего месяца.
2. Отключение архивных событий происходит автоматически.
3. Архивные события, время хранения которых превышено, удаляются.
4. При достижении максимального объема архива внутренних событий останавливается дальнейшая регистрация внутренних событий.
5. Возобновление работы сервиса регистрации внутренних событий возможно после запуска скрипта очистки дискового пространства.

См. также

Переменные Комплекса уровня Management

Рекомендации по использованию переменных файлов manager.env и sensor.env

Очистка дискового пространства от внутренних событий

22.8. Отправка внутренних событий по протоколу Syslog

Для передачи внутренних событий Комплекса во внешние системы (например, SIEM) используется сервис `udv-rabbitmq` с отдельной очередью `dtpk_event_syslog`. Поддерживаются следующие транспортные протоколы:

- UDP;
- TCP.

Передача внутренних событий настраивается через переменные в файле `manager.env`:

- `EVENT_SYSLOG_SEND` — включение/выключение передачи событий;
- `EVENT_SYSLOG_HOST` — IP-адрес внешнего сервера;
- `EVENT_SYSLOG_PORT` — порт для отправки событий;

- `EVENT_SYSLOG_PROTOCOL` — протокол отправки событий;
- `EVENT_SYSLOG_FACILITY` — категория источника событий;
- `EVENT_SYSLOG_SEVERITY` — уровень критичности событий;

Управление очередью внутренних событий настраивается с помощью следующих параметров сервиса `udv-rabbitmq`:

- `x-max-length-bytes` - максимальный размер очереди. Значение по умолчанию — 20 ГБ на все очереди сервиса `udv-rabbitmq`;
- `x-overflow` - поведение при переполнении;

> Прим.:
>
> По умолчанию установлено поведение `drop-head`, при котором при переполнении очереди событий самые старые события будут удаляться. Также можно установить поведение `reject-publish`, при котором в случае переполнения очереди прием новых событий будет приостановлен.

- `x-message-ttl` — время жизни события. Значение по умолчанию — 1 час.

При разрыве соединения Комплекс выполняет попытки доставки каждые 100 секунд. При этом события накапливаются в очереди `dtpk_event_syslog` сервиса `udv-rabbitmq`. Одно событие отправляется в течение 5 минут прогрессивно, т.е. через 10 секунд, далее через 30 секунд, через 1 минуту. Если за час сообщение о событии не было передано по Syslog, сообщение удаляется из очереди. При восстановлении соединения накопленные события выгружаются.

Гарантированная пропускная способность отправки внутренних событий по протоколу TCP/IP — 315 событий в секунду. Для протокола UDP требования по пропускной способности не регламентированы.

Основную инструкцию по отправке внутренних событий через Syslog см. в разделе «Настройка отправки внутренних событий во внешнюю систему по протоколу Syslog».

22.9. Перечень данных, собираемых Комплексом с помощью сканеров

Подробный список сканеров сбора данных Комплекса см. в разделе «Реестр сканеров Комплекса» Руководства по эксплуатации.

Табл. 161. Перечень данных, собираемых Комплексом

ТИП АКТИВА	ДАННЫЕ	ПРОТОКОЛ
Windows	События Security	RPC (WMI/MSEVEN)
Windows	События System	RPC (WMI/MSEVEN)
Windows	События Application	RPC (WMI/MSEVEN)
Windows	События Kaspersky Event Log	RPC (WMI/MSEVEN)
Windows	Список процессов	RPC (WMI/MSEVEN)

Табл. 161. Перечень данных, собираемых Комплексом

ТИП АКТИВА	ДАННЫЕ	ПРОТОКОЛ
Windows	Список установленных обновлений	RPC (WMI/MSEVEN)
Windows	Список пользователей (локальные)	RPC (WMI/MSEVEN)
Windows	Список пользователей (все)	RPC (WMI/MSEVEN)
Windows	Список устройств	RPC (WMI/MSEVEN)
Windows	Список групп пользователей	RPC (WMI/MSEVEN)
Windows	Автозагрузка	RPC (WMI/MSEVEN)
Windows	Список служб (автозапуск)	RPC (WMI/MSEVEN)
Windows	Список служб	RPC (WMI/MSEVEN)
Windows	Список установленных обновлений	WinRM
Windows	Содержимое файла Hosts	WinRM
Windows	Содержимое файла Hosts	WinRM over HTTPS
Windows	Содержимое файла Hosts	WinEXE
Windows	Общие папки	WinRM
Windows	Сетевые порты в режиме «LISTENING»	WinRM
Windows	Сетевые порты в режиме «LISTENING»	WinRM over HTTPS
Windows	Сетевые порты в режиме «LISTENING»	WinEXE
Windows	Список процессов с указанием пользователя	WinRM
Windows	Список процессов с указанием пользователя	WinRM over HTTPS
Windows	Список процессов с указанием пользователя	WinEXE
Windows	Параметры сетевых интерфейсов	WinRM
Windows	Параметры сетевых интерфейсов	WinRM over HTTPS
Windows	Параметры сетевых интерфейсов	WinEXE

Табл. 161. Перечень данных, собираемых Комплексом

ТИП АКТИВА	ДАННЫЕ	ПРОТОКОЛ
Windows	ARP-таблица	WinRM
Windows	ARP-таблица	WinRM over HTTPS
Windows	ARP-таблица	WinEXE
Windows	Таблица маршрутизации	WinRM
Windows	Таблица маршрутизации	WinRM over HTTPS
Windows	Таблица маршрутизации	WinEXE
Windows	Установленное ПО (по ключам реестра)	WinRM
Windows	Версия Windows (ver)	WinRM
Windows	Версия Windows (ver)	WinRM over HTTPS
Windows	Версия Windows (ver)	WinEXE
Windows	Версия Windows (winver)	WinRM
Windows	Версия Windows (winver)	WinRM over HTTPS
Windows	Версия Windows (winver)	WinEXE
Windows	Имя актива	WinRM
Windows	Имя актива	WinRM over HTTPS
Windows	Имя актива	WinEXE
Windows	Политика безопасности	WinRM
Windows	Настройки парольной политики	WinRM
Windows	Правила МЭ	WinRM
Windows	Правила МЭ	WinRM over HTTPS
Windows	Правила МЭ	WinEXE
Windows	Состояние МЭ	WinRM

Табл. 161. Перечень данных, собираемых Комплексом

ТИП АКТИВА	ДАННЫЕ	ПРОТОКОЛ
Windows	Состояние МЭ	WinRM over HTTPS
Windows	Состояние МЭ	WinEXE
Windows	Настройки аудита	WinRM
UNIX	ARP-таблица	SSH
UNIX	Таблица маршрутизации	SSH
UNIX	Имя сетевого узла	SSH
UNIX	Подключенные носители информации	SSH
UNIX	Список пользователей	SSH
UNIX	Список групп пользователей и их членов	SSH
UNIX	Список процессов	SSH
UNIX	Список установленного ПО	SSH
UNIX	Содержимое файла /etc/sudoers	SSH
UNIX	Используемые DNS-серверы	SSH
UNIX	Содержимое файла /etc/hosts	SSH
UNIX	Сетевые порты в режиме LISTENINIG	SSH
UNIX	Правила межсетевого экрана iptables	SSH
UNIX	Объекты автозапуска	SSH
UNIX	Контроль целостности критичных файлов (/etc/network/interfaces и др.)	SSH
Debian	Список включенных служб	SSH
Debian	Список сервисов	SSH
Debian	Установленное ПО	SSH
Debian	Список устройств	SSH

Табл. 161. Перечень данных, собираемых Комплексом

ТИП АКТИВА	ДАННЫЕ	ПРОТОКОЛ
Debian	Контрольные суммы файлов конфигурации	SSH
QNX	Параметры DNS	SSH
QNX	Список групп	SSH
QNX	Сетевые порты в режиме прослушивания	SSH
QNX	Список пользователей	SSH
QNX	Файл hosts	SSH
RHEL	ARP-таблица	SSH
RHEL	Список служб	SSH
RHEL	Планировщик задач	SSH
RHEL	Параметры DNS	SSH
RHEL	Файл hosts	SSH
RHEL	Правила iptables	SSH
RHEL	Список sudoers	SSH
RHEL	Список групп	SSH
RHEL	Имя актива	SSH
RHEL	Подключенные носители информации	SSH
RHEL	Список пользователей	SSH
RHEL	Сетевые порты в режиме прослушивания	SSH
RHEL	Список процессов	SSH
RHEL	Таблица маршрутизации	SSH
RHEL	Установленное ПО	SSH
RHEL	Список устройств	SSH

Табл. 161. Перечень данных, собираемых Комплексом

ТИП АКТИВА	ДАННЫЕ	ПРОТОКОЛ
АСО Cisco IOS	Текущая конфигурация	SSH
АСО Cisco IOS	Начальная конфигурация	SSH
АСО Cisco IOS	ARP-таблица	SSH
АСО Cisco IOS	Таблица MAC-адресов	SSH
АСО Cisco IOS	Версия ОС	SSH
АСО HP	Текущая конфигурация	SSH
АСО HP	Начальная конфигурация	SSH
АСО HP	Версия ОС	SSH
АСО Cisco ASA	ARP-таблица	SSH
АСО Cisco ASA	Таблица маршрутизации	SSH
АСО Cisco ASA	Текущая конфигурация	SSH
АСО Cisco ASA	Стартовая конфигурация	SSH
АСО Cisco ASA	Версия ОС	SSH
АСО Hirschmann	ARP-таблица	SSH
АСО Hirschmann	Таблица MAC-адресов	SSH
АСО Hirschmann	Текущая конфигурация	SSH
АСО Hirschmann	Версия ОС	SSH
АСО Comware	ARP-таблица	SSH
АСО Comware	Текущая конфигурация	SSH
АСО Comware	Таблица маршрутизации	SSH
АСО Comware	Таблица MAC-адресов	SSH
АСО Comware	Стартовая конфигурация	SSH

Табл. 161. Перечень данных, собираемых Комплексом

ТИП АКТИВА	ДАННЫЕ	ПРОТОКОЛ
АСО Comware	Версия ОС	SSH
АСО Huawei	ARP-таблица	SSH
АСО Huawei	Таблица маршрутизации	SSH
АСО Huawei	Таблица MAC-адресов	SSH
АСО Huawei	Текущая конфигурация	SSH
АСО Huawei	Серийный номер	SSH
АСО Huawei	Стартовая конфигурация	SSH
АСО Huawei	Версия ОС	SSH
АСО Huawei	Параметры интерфейсов	SNMP
АСО/шлюзы/конвертеры MOXA	Таблица MAC-адресов	SSH
АСО/шлюзы/конвертеры MOXA	Текущая конфигурация	SSH
АСО/шлюзы/конвертеры MOXA	Стартовая конфигурация	SSH
АСО/шлюзы/конвертеры MOXA	Версия ОС	SSH
АСО/шлюзы/конвертеры MOXA	Параметры интерфейсов	SSH
MSSQL	Список логинов	MSSQL
MSSQL	Список пользователей	MSSQL
MSSQL	Права пользователей	MSSQL
MySQL	Список пользователей	MySQL
MySQL	Права пользователей	MySQL

Табл. 161. Перечень данных, собираемых Комплексом

ТИП АКТИВА	ДАННЫЕ	ПРОТОКОЛ
ПЛК ALLEN BRADLEY Control Logix	Сбор конфигураций ПЛК. • Сведения о ПЛК: вендор, тип ПЛК, код продукта, версия, серийный номер, наименование или модель ПЛК и его версия, режим работы ПЛК; • Программа(проект) ПЛК: контрольная сумма проекта, чтение проекта ПЛК; • Значения тегов, список тегов.	Ethernet/IP
ПЛК Siemens	Сбор конфигураций ПЛК (код заказа, версия ОС, тип модуля, наименование модуля, серийный номер, состояние ПЛК, контрольные суммы, размер, дата последней модификации программных блоков)	S7comm
ПЛК SCHNEIDER ELECTRIC	Сбор конфигураций ПЛК. • Сведения о проекте: дата компиляции проекта, время компиляции проекта, версия проекта, имя проекта; • Сведения о ПЛК: наименование, идентификатор, семейство ПЛК, тип ПЛК, версия firmware, идентификатор hardware; • Состояние ПЛК: контрольная сумма проекта ПЛК, статус ПЛК; • Программа(проект) ПЛК.	Modbus
Прочие активы с поддержкой SNMP	Параметры из раздела System – обобщенные данные о системе (имя, время работы с момента последней перезагрузки);	SNMP
Прочие активы с поддержкой SNMP	Параметры из раздела Interfaces – данные о сетевых интерфейсах (статус, количество, типы, размер пакетов);	SNMP
Прочие активы с поддержкой SNMP	Параметры из раздела TCP – данные протокола TCP (количество соединений, получено и отправлено пакетов, количество ошибок);	SNMP
Прочие активы с поддержкой SNMP	Параметры из раздела ICMP – данные протокола обмена управляющими сообщениями	SNMP

Табл. 161. Перечень данных, собираемых Комплексом

ТИП АКТИВА	ДАННЫЕ	ПРОТОКОЛ
	ICMP (количество сообщений получено и отправлено, количество ошибок и их виды);	
Прочие активы с поддержкой SNMP	Параметры из раздела EGP – протокол обмена информацией о состоянии маршрутизации (получено и отправлено пакетов, количество ошибок);	SNMP
Прочие активы с поддержкой SNMP	Параметры из раздела UDP – данные протокола UDP (получено и отправлено датаграмм, количество ошибок);	SNMP
Прочие активы с поддержкой SNMP	Параметры из раздела SNMP – статистика работы одноименного протокола (количество входящих и исходящих пакетов, обработано запросов, ошибки);	SNMP
Прочие активы с поддержкой SNMP	Параметры из раздела IP – данные о функционировании этого протокола (количество пакетов получено и отправлено, количество ошибок и их разновидности)	SNMP
ПЛК ОВЕН	Сбор конфигураций ПЛК ОВЕН: • сведения о проекте; • сведения о ПЛК: тип ПЛК, его текущее состояние, настройки, наличие парольной защиты	PLC-Browser

22.10. Работа с импортируемыми панелями мониторинга

В этом разделе:

- Навигация в разделах мониторинга
- Средства управления панелями мониторинга
  - Поиск в панелях мониторинга
  - Фильтры в панелях мониторинга
- Элементы управления интерфейсом визуализации
  - Диаграммы и таблицы на панелях мониторинга
  - Графики
  - Круговые диаграммы
  - Столбчатые диаграммы
  - Таблицы

22.10.1. Навигация в разделах мониторинга

Для удобства перемещения по разделам мониторинга предусмотрена навигация, которая содержит только те ссылки, которые необходимы в конкретный момент анализа событий ИБ.

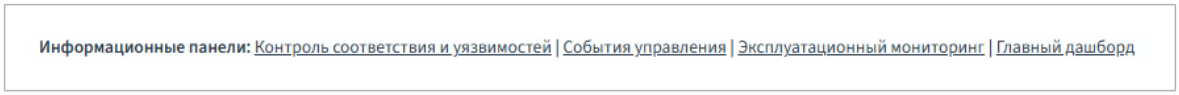


Рис. 557. Информационная панель

Панель состоит из следующих ссылок на визуализированные разделы мониторинга:

- Контроль соответствия и уязвимостей
- События управления Комплексами
- Эксплуатационный мониторинг
- Главный дашборд

22.10.2. Средства управления панелями мониторинга

На всех страницах раздела **Мониторинг** используются одни и те же инструменты управления событиями. Инструменты расположены в верхней части страниц (кроме экспорта).

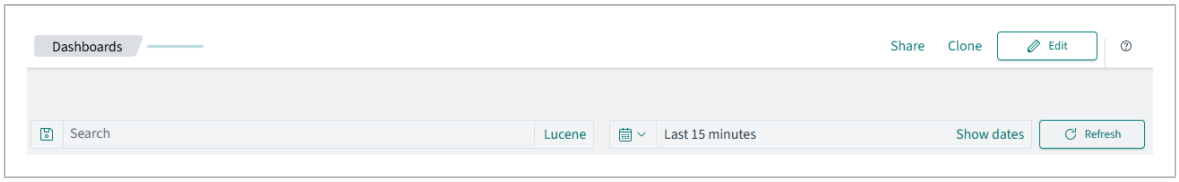


Рис. 558. Инструменты для управления страницами мониторинга

Представлены следующие возможности:

- Поиск. Расположен в верхней части страницы по всей длине;
- Фильтр. Расположен в верхней левой части страницы под разделом **Поиск**;
- Выбор периода отображения событий. Расположен в верхней правой части страницы.
    - Автообновление. Расположено в окне выбора отображения событий.
- Элементы управления интерфейса визуализации. Расположены в верхней правой части страницы, слева от автообновления.
- Экспорт списков событий. Расположен под разделом мониторинга с таблицей.

22.10.2.1. Поиск в панелях мониторинга

Поиск использует синтаксис запроса Lucene и позволяет искать события по наличию полей или их содержанию. Например, запрос target_ip: "192.168.243.31" AND target_mac: "F4:1D:6B:87:5C:7F" будет означать поиск событий по IP и MAC-адресам, находящимся в кавычках. Синтаксис позволяет найти события по наличию любого поля или его содержимого, а также поддерживает логические операторы OR (OR или ||), AND (AND, && или +) и NOT (NOT, ! или -).

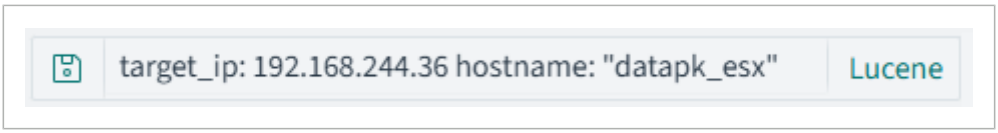


Рис. 559. Пример поискового запроса

22.10.2.2. Фильтры в панелях мониторинга

Фильтры используются для отображения событий по запросу. Возможно добавление нескольких фильтров, отключение или удаление ненужных в данный момент, а также закрепление. Среди данных фильтра можно задать любое поле событий.

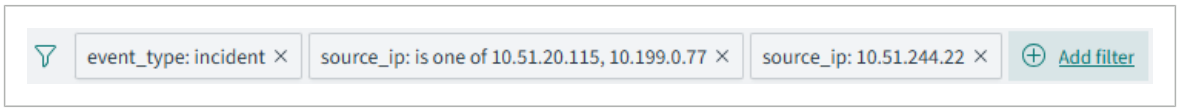


Рис. 560. Панель фильтров

Существует два способа создания фильтра:

1. При помощи кнопки «+Добавить фильтр» (**+Add filter**);
2. При помощи выбора значений из таблицы.

Оба способа позволяют создавать фильтры по одному из полей (один фильтр — одно поле).

Фильтры имеют следующие возможности:

1. Фильтр по наличию или отсутствию: по умолчанию используется фильтр по наличию, но после фильтрации есть возможность инвертировать выбор («все, кроме»);
2. Фильтрация с использованием синтаксиса запроса Query DSL;

> Подсказка:
>
> При использовании данного синтаксиса есть возможность задать несколько полей в рамках одного фильтра.

3. Использование нескольких фильтров одновременно;

> Внимание:
>
> При использовании нескольких фильтров существует ограничение, которое обуславливается предельной длиной URL. В среднем, ограничение составляет до 35 фильтров среднего размера.

4. Цветовая индикация фильтров;
5. Закрепление фильтра;
    - Использование фильтров на всех страницах мониторинга: при переходе на смежные страницы мониторинга фильтры сохранятся.

> Внимание:
>
> Функция работает только в рамках одной страницы. Если открыть новую вкладку, фильтры будут сброшены.

6. Редактирование фильтра;
7. Выбор использования фильтра;
8. Удаление фильтра;
9. Применение доступных операций на группу фильтров.

22.10.3. Элементы управления интерфейсом визуализации

Для управления панелями мониторинга можно также использовать специфические элементы управления раздела **Мониторинг**. Использование элементов управления интерфейсом визуализации рекомендуется только для опытных пользователей.

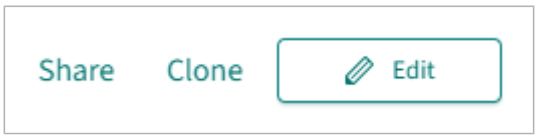


Рис. 561. Кнопки управления интерфейсом визуализации

Их можно увидеть на всех страницах раздела мониторинга:

- Поделиться (**Share**) — позволяет поделиться страницей мониторинга в виде элемента iframe или ссылки. Содержимое может быть как интерактивным, так и в виде статичного снимка.

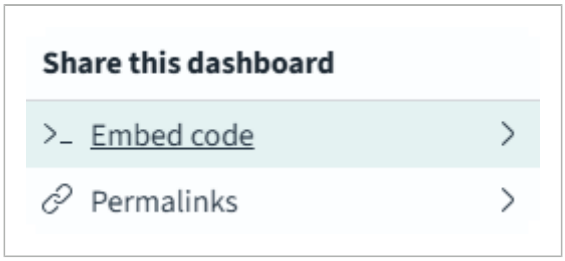


Рис. 562. Меню, позволяющее поделиться содержимым страницы

- Клонировать (**Clone**) — позволяет создать копию страницы панели мониторинга. В настройках можно задать имя скопированной страницы.

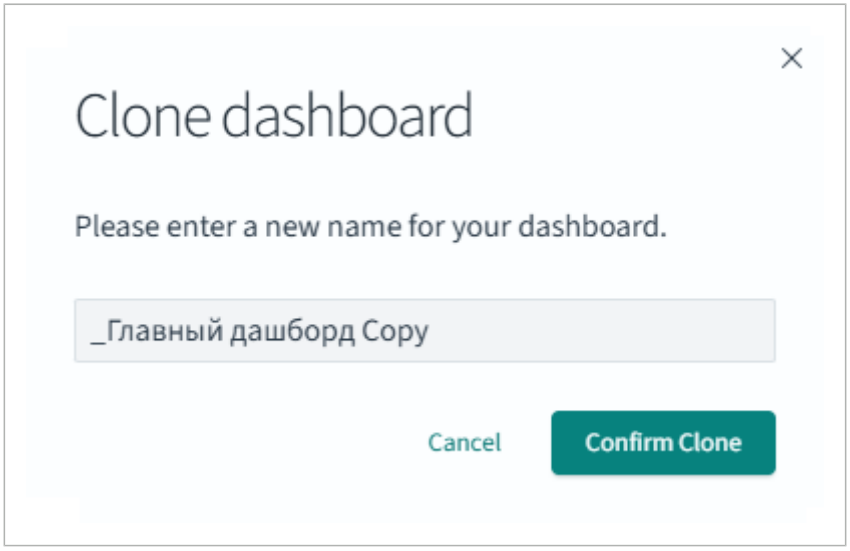


Рис. 563. Окно «Клонировать панель мониторинга»

- Редактировать (**Edit**) — позволяет редактировать расположение, размер, содержание элементов (визуализаций) панели мониторинга. В частности, можно настроить фильтры визуализации, заголовок, выбрать полноэкранный режим отображения визуализации или удалить элемент страницы. Также можно использовать поле между панелями и скрыть все заголовки в разделе «Параметры» (**Options**).

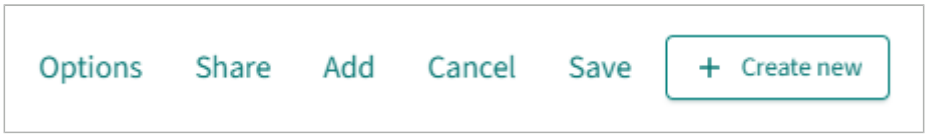


Рис. 564. Редактирование панели мониторинга

22.10.4. Диаграммы и таблицы на панелях мониторинга

Основными инструментами мониторинга событий в Комплексе являются визуализации, которые могут быть в виде диаграмм и таблиц. Диаграммы предназначены для быстрого просмотра количества событий, а таблицы — для более тщательного анализа. Диаграммы, в свою очередь, могут быть трех видов:

- Графики (диаграммы-линии)
- Круговые диаграммы
- Столбчатые диаграммы

Все визуализации можно развернуть — для этого нажмите кнопку ▫▫▫ в правом верхнем углу визуализации и выберите ⤢ (**Maximize panel**) из выпадающего списка.

См. также

Таблицы

22.10.4.1. Графики

На страницах мониторинга графики помогают отследить появление аномалий по количеству событий во времени.

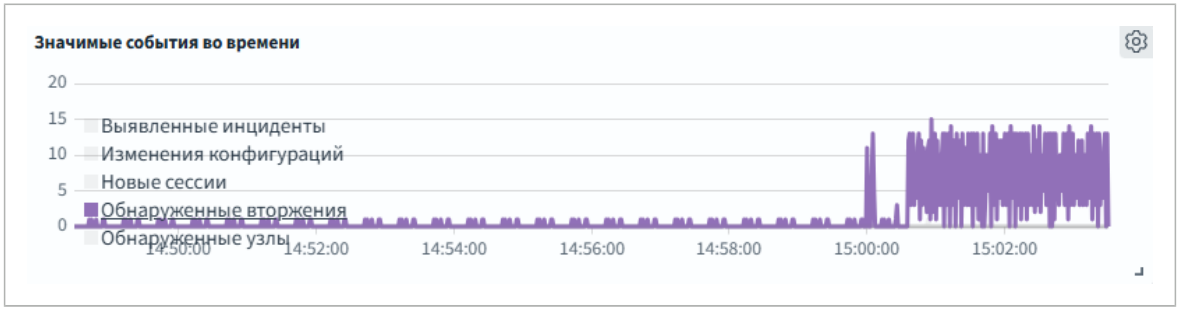


Рис. 565. Пример графика

Графики поддерживают следующие возможности:

- скрытие одного или нескольких видов событий;
- выбор периода отображения прямо на временной шкале;
- просмотр точной даты и времени на шкале.

Для отображения событий только одной категории наведите курсор на ее название.

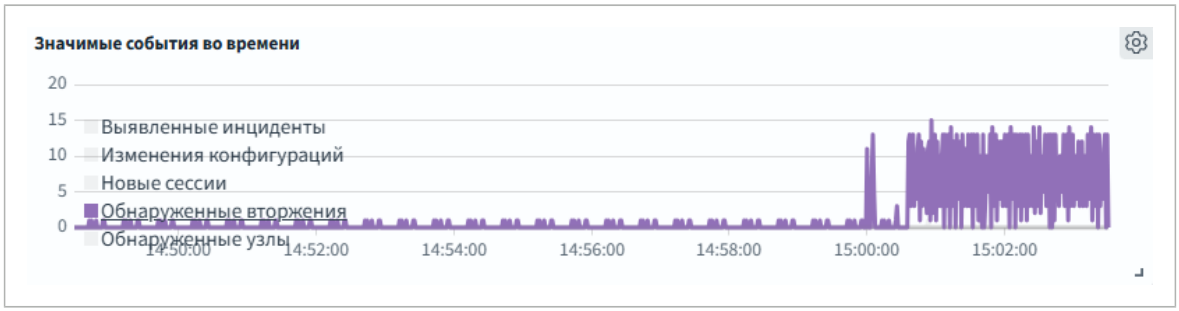


Рис. 566. Выбор одного типа событий для его отображения на графике

Для скрытия событий одной или нескольких категорий нажмите на название линии; после этого линия исчезнет с графика, а рядом с ее названием в скобках появится надпись `hidden`. Ограничений на количество скрытых графиков нет. Чтобы включить отображение категории событий, нажмите на название снова.

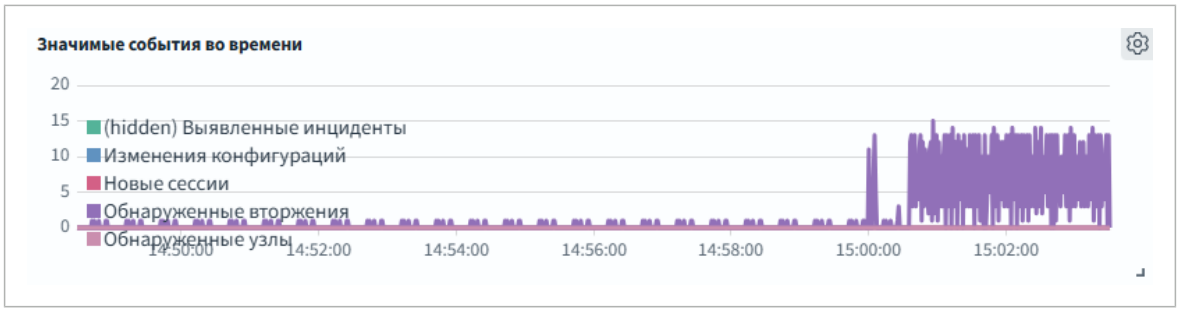


Рис. 567. Вид графика после того, как «Выявленные инциденты» были скрыты

Для выбора периода отображения событий на временной шкале: нажмите в начале периода на шкале, проведите, не отпуская, до окончания интересующего периода и отпустите. Подробнее см. раздел «Выбор периода отображения событий на панели мониторинга».

Для просмотра даты и времени интересующего момента на шкале наведите на него курсор мыши. Рядом с курсором появится красная вертикальная линия, а в правом верхнем углу — дата и время момента на шкале.

22.10.4.2. Круговые диаграммы

Круговые диаграммы используются для быстрого просмотра изменений в следующих разделах: контроль сетевых соединений, обнаружение вторжений, контроль конфигураций, инциденты ИБ.

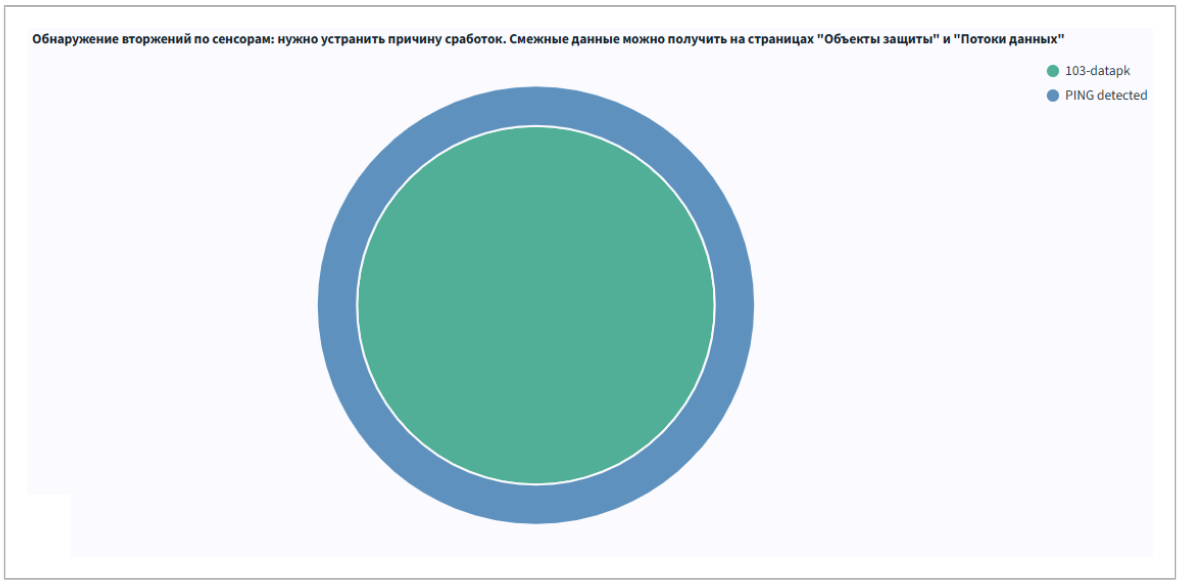


Рис. 568. Пример круговой диаграммы

Эти диаграммы имеют единую структуру:

- Центральный круг. В центральном внутреннем круге находится исследуемый Комплекс.
- Внешний круг. Во внешнем круге находятся конфигурации, инциденты, сигнатуры, протоколы.
- Второй внешний круг. Отображается только в разделе **Контроль конфигураций**. Содержит наименование актива, на котором были обнаружены изменения конфигураций.

Чтобы просмотреть информацию об элементе диаграммы, наведите на нее курсор мыши. Появится всплывающее окно с указанием количества и соотношения с другими элементами в процентах.

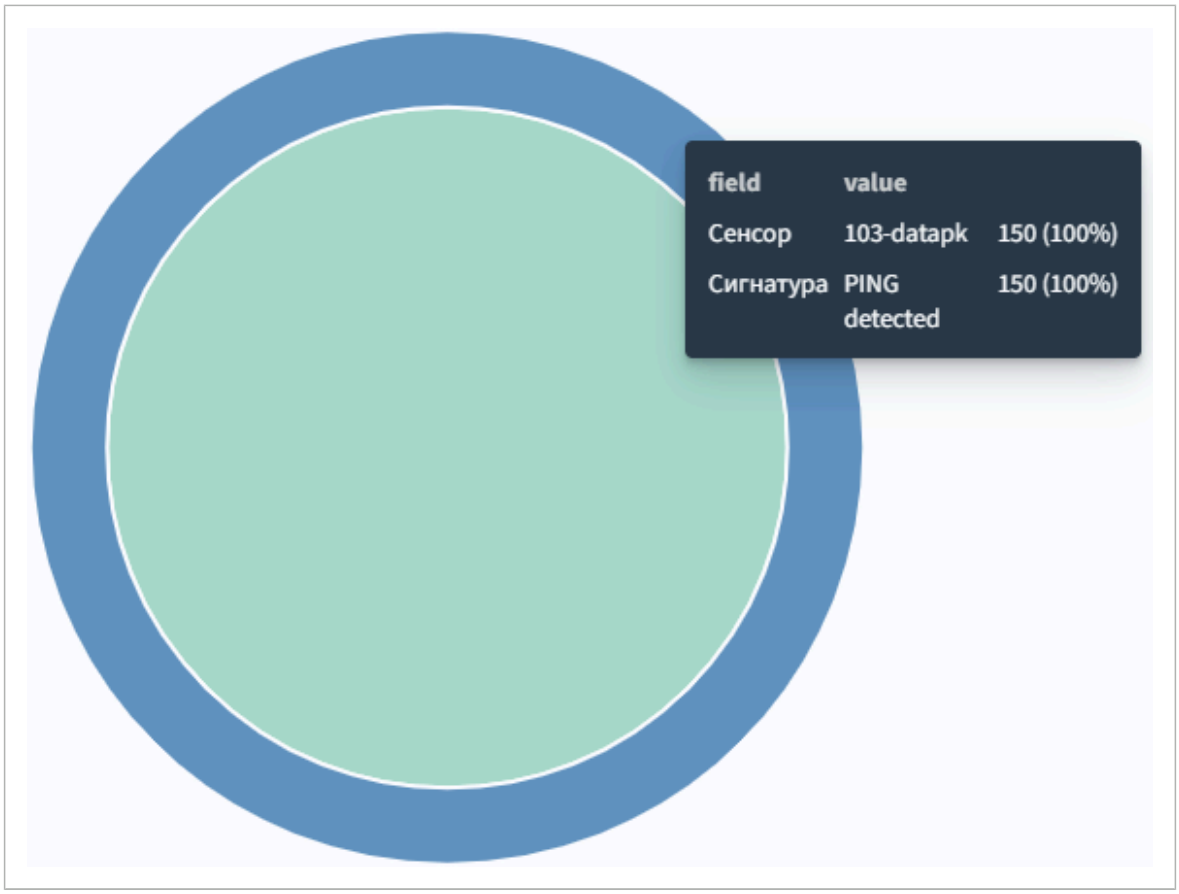


Рис. 569. Просмотр информации об элементе круговой диаграммы

22.10.4.3. Столбчатые диаграммы

Столбчатые диаграммы используются на следующих страницах: обнаружение вторжений, контроль сетевых соединений, контроль конфигураций. Представляют собой столбики данных, позволяющие сравнить количество, например, вторжений по их источнику. Таким образом можно быстро увидеть, на какие активы была нацелена атака.

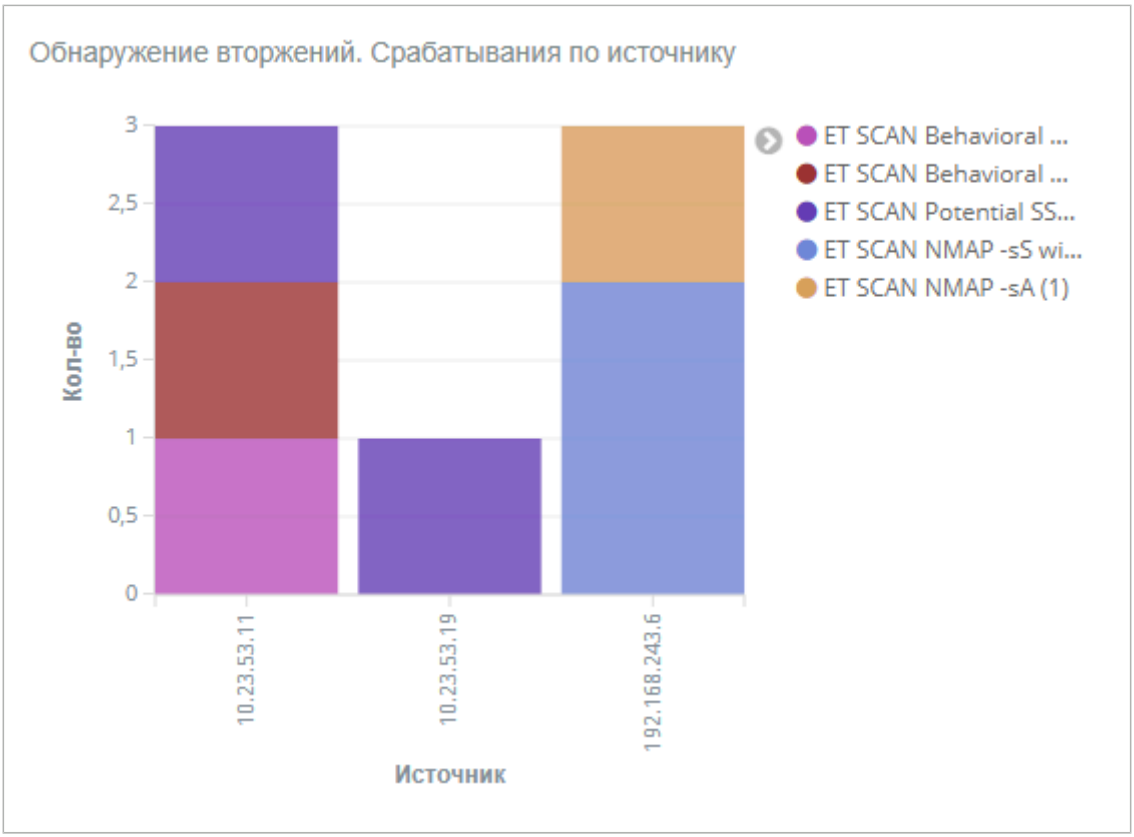


Рис. 570. Пример столбчатой диаграммы

22.10.4.4. Таблицы

В разделе мониторинга событий визуализации в виде таблиц используются для первичного анализа событий по различным критериям. Вид таблиц отличается от основного интерфейса Комплекса.

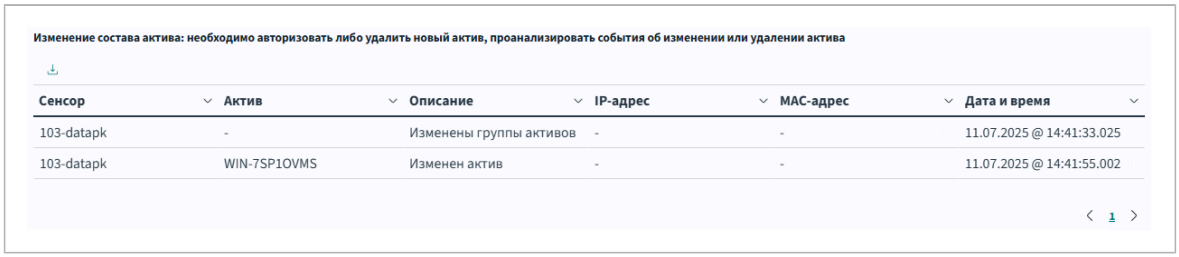


Рис. 571. Пример таблицы из интерфейса панелей мониторинга

Основные возможности:

- Сортировка по любым столбцам таблицы. Для сортировки по нарастанию или убыванию нажмите рядом с интересующим столбцом таблицы и выберите способ сортировки из выпадающего списка: для сортировки по возрастанию выберите (**Sort asc**), а по убыванию — (**Sort desc**).

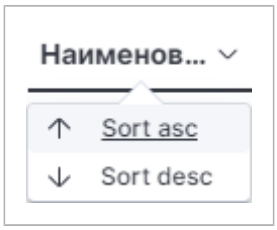


Рис. 572. Выбор в таблице способа сортировки значений столбца

- Создание фильтров по значениям из таблицы. Подробнее см. в разделе «Фильтр по значениям из таблицы».

22.11. Рекомендации по настройке сбора данных

Для корректного сбора данных на Комплексе необходимо придерживаться следующих общих принципов:

- Настройка сбора данных — только в режиме технического обслуживания.
- Расписания в задачах сбора данных различных компонентов не должны пересекаться. Во избежание ошибок, в один момент времени следует собирать данные только одной задачей.
- Устанавливать количество запросов сбора данных с активов не более четырех раз в сутки.
- Устанавливать интервал между задачами сбора данных не менее, чем в 10-20 минут.
- Формировать задачи согласно операционной системе активов.
- Использовать один протокол сбора данных в одной задаче.
- Не рекомендуется использовать группы, количество сканеров в которых превышает 30. Подробнее о группах сканеров см. в разделе «Группировка сканеров сбора данных».
- Сбор данных по протоколу ms-even4 возможен только для Windows XP, Windows Server 2003 и Windows Server 2000.

См. также

Сбор данных с активов

22.12. Определение максимально допустимого количества активов сбора данных

Для того, чтобы не создавать избыточную нагрузку на сеть, необходимо определить максимально допустимое количество активов, на которых выполняется сбор данных.

Максимально допустимое количество активов, на которых выполняется сбор данных, рассчитывается по следующей формуле:

```
maxHosts =  4 × tmax  × 60 ÷ (scannersCount ×  p95(executionTime) × 1,25)
```

где:

- `maxHosts` — максимально допустимое количество активов сбора данных;
- `4` — максимальное количество выполняющихся пар «актив-сканер»;
- `tmax` — время реагирования на инцидент на предприятии в минутах;
- `60` — количество секунд в минуте;

- `scannersCount` — количество сканеров в задаче сбора данных;
- `p95(executionTime)` — среднее время выполнения сканера. Представляет собой постоянное значение, равное `22`;
- `1,25` — постоянное значение производительности.

22.13. Содержание Python-скриптов

Скрипты для сбора данных выполняются в среде, поддерживающей подмножество синтаксиса языка Python (RestrictedPython).

> Внимание:
>
> Скрипт необходимо сохранять в файле формата `*.py` (кодировка – UTF-8 без BOM).

В скриптах запрещен импорт произвольных пакетов, по умолчанию в среду выполнения импортированы следующие пакеты из стандартной библиотеки Python: `re, string, unicodedata, hashlib, datetime, textwrap, struct, dbfread, dateutil, dateutil.tz`.

В скриптах доступны следующие переменные:

- `host` – IP-адрес актива, на котором выполняется сбор данных;
- `domain` – имя домена (используется в том случае, если с помощью скрипта осуществляется доступ к активам, находящимся в домене);
- `host_id` – идентификатор актива, на котором выполняется сбор данных;
- `credentials` – словарь (`dict`) с реквизитами доступа к активу; значение данной переменной – словарь с двумя ключами (`user`, `password`). Сканер получает данные о ключах из учетной записи актива Комплекса, тег которой совпадает с названием словаря;
- `store` – (`any`, `dict`) сохраненные данные с предыдущего запуска скрипта. Если скрипт запускается первый раз, то `store = None`;
- `expiration` – максимальное время выполнения скрипта;
- `execute` – метод, выполняющий запрос к коннектору.

Результат выполнения скрипта возвращается с помощью оператора `return`.

Ниже приведен пример скрипта для сбора ARP-таблицы в ОС семейства Unix по протоколу SSH с помощью учетной записи с тегом `admin`:

```
try:
    credential = credentials['admin']
except KeyError as e:
    raise KeyError('Учетные данные для %s не найдены' % e)
protocol_args = {
    'host': host,
    'username': credential.get('user'),
    'password': credential.get('password'),
    'interface': 'ssh',
    'port': 22,
    'query': [{
        'command': 'arp -an\r\n',
        'expects': [],
```

```
        'timeout': 10
    }]
}
def escape_ansi(line):
    ansi_escape = re.compile(r'(\x9B|\x1B\[)[0-?]*[ -\/]*[@-~]')
    return ansi_escape.sub('', line)
data = execute('terminal', protocol_args, expiration)
lines = bytes.fromhex(data).decode()
lines = escape_ansi(lines)
regex          =          r'\((?P<ip>((\d{1,3}\.?){4}))\)\sat\s(?P<mac>((\w{2}:?){6})).*\son\s(?
P<interface>(.*))\r\n'
matches = re.finditer(regex, lines)
interfaces = [[match.group(g) for g in ['ip', 'mac', 'interface']]
              for match in matches]
return {
    'visible_keys': {
        'ip': 'IP-адрес',
        'mac': 'MAC-адрес',
        'interface': 'Интерфейс',
    },
    'keys': ['ip', 'mac', 'interface'],
    'data': interfaces,
    'ignore_delete': True,
}
```

22.14. Перечень SCADA, с которых поддерживается сбор данных

- КРУГ-2000
- Программный комплекс Redkit SCADA
- Alpha
- Honeywell
- Phocus
- Unimod PRO от «ТРЭИ»
- Wonderware InTouch

22.15. Реестр сканеров Комплекса

В таблицах ниже представлен список предоставляемых разработчиком Комплекса Python-скриптов, входящих в состав сканеров сбора данных, и их описание. Доступен сбор данных следующих категорий:

- Таблица 162. Python-скрипты для сбора данных об ОС и ПО
- Таблица 163. Python-скрипты для сбора данных ПО Acronis
- Таблица 164. Python-скрипты для сбора данных ПЛК Allen Bradley
- Таблица 165. Python-скрипты для сбора данных сетевого оборудования Checkpoint
- Таблица 166. Python-скрипты для сбора данных межсетевых экранов Cisco ASA
- Таблица 167. Python-скрипты для сбора данных с сетевого оборудования Cisco
- Таблица 168. Python-скрипты для сбора данных сетевого оборудования Eltex
- Таблица 169. Python-скрипты для сбора данных SCADA Honeywell

- Таблица 170. Python-скрипты для сбора данных с сетевого оборудования Huawei VRP
- Таблица 171. Python-скрипты для сбора данных сетевого оборудования HP
- Таблица 172. Python-скрипты для сбора данных SCADA InTouch
- Таблица 173. Python-скрипты для сбора данных сетевого оборудования Mgate
- Таблица 174. Python-скрипты для сбора трафика баз данных MSSQL и MySQL
- Таблица 175. Python-скрипты для сбора данных сетевого оборудования NIS
- Таблица 176. Python-скрипты для сбора данных утилиты nmap
- Таблица 177. Python-скрипты для сбора данных с ОС QNX
- Таблица 178. Python-скрипты для сбора данных Redkit
- Таблица 179. Python-скрипты для сбора данных ПЛК Siemens
- Таблица 180. Python-скрипты для сбора данных ПЛК Schneider Electric
- Таблица 181. Python-скрипты для сбора данных по протоколу SNMP
- Таблица 182. Python-скрипты для сбора данных ОС Solaris
- Таблица 183. Python-скрипты для сбора данных ОС Unix
- Таблица 184. Python-скрипты для сбора данных ОС Windows
- Таблица 185. Python-скрипты для сбора данных ОС Windows CC
- Таблица 186. Python-скрипты для инвентаризации объектов Windows
- Таблица 187. Python-скрипты для сбора данных о ПЛК Regul

Внимание:

Сбор данных по протоколу ms-even4 возможен только для Windows XP, Windows Server 2003 и Windows Server 2000.

Внимание:

Сбор событий с помощью утилит winexe и ssh1 возможен при наличии установленного модуля «Управление внешними событиями». Подробнее об установке этого модуля см. в разделе «Установка модуля «Управление внешними событиями»» руководства по внедрению и поддержке.

Табл. 162. Python-скрипты для сбора данных об ОС и ПО

НАИМЕНОВАНИЕ	ОПИСАНИЕ	
Версия ОС Unix (ssh)	Сканер для сбора информации о версии ОС Unix по протоколу SSH	Версия ОС
Версия ОС Windows (winexe 0.8)	Сканер для сбора информации о версии ОС по протоколу winexe 0.8	Версия ОС
Версия ОС Windows (winexe 1.0)	Сканер для сбора информации о версии ОС по протоколу winexe 1.0	Версия ОС
Версия ОС Windows (winrm http)	Сканер для сбора информации о версии ОС Windows по протоколу winrm http	Версия ОС

Табл. 162. Python-скрипты для сбора данных об ОС и ПО

НАИМЕНОВАНИЕ	ОПИСАНИЕ	
Версия ОС Windows (winrm https)	Сканер для сбора информации о версии ОС Windows по протоколу winrm https	Версия ОС
Версия ОС Cisco (enable) (ssh)	Сканер для сбора информации о версии ОС Cisco (enable) по протоколу SSH	Версия ОС
Версия ОС Cisco (ssh)	Сканер для сбора информации о версии ОС Cisco по протоколу SSH	Версия ОС
Версия ОС DevLink	Сканер для сбора информации о версии ОС DevLink	Версия ОС
Версия ОС Eltex	Сканер для сбора информации о версии ОС Eltex	Версия ОС
Версия ОС ПЛК Allen Bradley	Сканер для сбора информации о версии ОС ПЛК Allen Bradley	Версия ОС
Версия ОС ПЛК Schneider	Сканер для сбора информации о версии ОС ПЛК Schneider Electric	Версия ОС
Версия ОС ПЛК Siemens	Сканер для сбора информации о версии ОС ПЛК Siemens	Версия ОС
Версия ОС ПЛК Regul	Сканер для сбора информации о версии ОС ПЛК Regul	Версия ОС
Версия ОС D-Link	Сканер для сбора информации о версии ОС D-Link	Версия ОС
Версия ОС Moxa	Сканер для сбора информации о версии ОС Moxa	Версия ОС
Версия ОС Huawei	Сканер для сбора информации о версии ОС Huawei	Версия ОС
Установленное ПО Centos (ssh) (os soft)	Сканер для сбора информации об установленном ПО Centos по протоколу SSH	Установленное ПО
Установленное ПО Debian (ssh) (os soft)	Сканер для сбора информации об установленном ПО Debian по протоколу SSH	Установленное ПО
Установленное ПО Windows (winexe 0.8)	Сканер для сбора информации об установленном ПО Windows по протоколу winexe 0.8	Установленное ПО
Установленное ПО Windows (winexe 1.0)	Сканер для сбора информации об установленном ПО Windows по протоколу winexe 1.0	Установленное ПО
Установленное ПО Windows (winrm http)	Сканер для сбора информации об установленном ПО Windows по протоколу winrm http	Установленное ПО
Установленное ПО Windows (winrm https)	Сканер для сбора информации об установленном ПО Windows по протоколу winrm https	Установленное ПО

Табл. 162. Python-скрипты для сбора данных об ОС и ПО

НАИМЕНОВАНИЕ	ОПИСАНИЕ	
Установленное ПО Windows (wmi)	Сканер для сбора информации об установленном ПО Windows по протоколу wmi	Установленное ПО

Табл. 163. Python-скрипты для сбора данных ПО Acronis

НАИМЕНОВАНИЕ	ОПИСАНИЕ	
Acronis список активных задач	Сканер для сбора списка активных задач Acronis по протоколу winexe	Список задач
Acronis список задач	Сканер для сбора списка задач Acronis по протоколу winexe	Список задач
Acronis список планов	Сканер для сбора списка планов Acronis по протоколу winexe	Список планов

Табл. 164. Python-скрипты для сбора данных ПЛК Allen Bradley

НАИМЕНОВАНИЕ	ОПИСАНИЕ	
Значения тегов ПЛК Allen Bradley	Сканер для сбора значений тегов ПЛК Allen Bradley	Значения те
Конфигурации ПЛК Allen Bradley (Ethernet_IP)	Сканер для сбора конфигурации ПЛК Allen Bradley по протоколу Ethernet IP	Конфигурац
Конфигурация ПЛК Allen Bradley	Сканер для сбора конфигурации ПЛК Allen Bradley	Конфигурац
Модули ПЛК Allen Bradley	Сканер для сбора модулей ПЛК Allen Bradley	Модули ПЛК
Наименование ПЛК Allen Bradley	Сканер для сбора наименования ПЛК Allen Bradley	Наименован
Программа ПЛК Allen Bradley	Сканер для сбора программы ПЛК Allen Bradley	Программы
Состояние ПЛК Allen Bradley	Сканер для сбора состояния ПЛК Allen Bradley	Состояния П
Список тегов ПЛК Allen Bradley	Сканер для сбора списка тегов ПЛК Allen Bradley	Теги ПЛК

Табл. 165. Python-скрипты для сбора данных сетевого оборудования Checkpoint

НАИМЕНОВАНИЕ	ОПИСАНИЕ	
Checkpoint изменение правил	Сканер для сбора изменений правил Checkpoint	Правила
Checkpoint изменить объекты	Сканер для сбора измененных объектов Checkpoint	Объекты

Табл. 165. Python-скрипты для сбора данных сетевого оборудования Checkpoint

НАИМЕНОВАНИЕ	ОПИСАНИЕ	
Checkpoint получить ARP-таблицу	Сканер для сбора ARP-таблицы Checkpoint	ARP-таблица
Checkpoint получить конфигурацию	Сканер для сбора конфигурации Checkpoint	Конфигурации
Checkpoint получить установленную политику	Сканер для получения установленной политики Checkpoint	Политика

Табл. 166. Python-скрипты для сбора данных межсетевых экранов Cisco ASA

НАИМЕНОВАНИЕ	ОПИСАНИЕ	
ECI_CISCO_ASA_SHOW_ARP (ssh1-en)	Сканер для сбора ARP-таблицы Cisco Asa по протоколу SSH (enable)	ARP-таблица
ECI_CISCO_ASA_SHOW_ARP (ssh2-en)	Сканер для сбора ARP-таблицы Cisco Asa по протоколу SSH (enable)	ARP-таблица
ECI_CISCO_ASA_SHOW_IPROUTE (ssh1-en)	Сканер для сбора таблицы маршрутизации Cisco Asa по протоколу SSH (enable)	Таблица маршрутизаци
ECI_CISCO_ASA_SHOW_IPROUTE (ssh2-en)	Сканер для сбора таблицы маршрутизации Cisco Asa по протоколу SSH (enable)	Таблица маршрутизаци
ECI_CISCO_ASA_SHOW_RUNNING_CONFIG (ssh1-en)	Сканер для сбора текущей конфигурации Cisco Asa по протоколу SSH (enable)	Конфигурации
ECI_CISCO_ASA_SHOW_RUNNING_CONFIG (ssh2-en)	Сканер для сбора текущей конфигурации Cisco Asa по протоколу SSH (enable)	Конфигурации
ECI_CISCO_ASA_SHOW_STARTUP_CONFIG (ssh1-en)	Сканер для сбора начальной конфигурации Cisco Asa по протоколу SSH (enable)	Конфигурации
ECI_CISCO_ASA_SHOW_STARTUP_CONFIG (ssh2-en)	Сканер для сбора начальной конфигурации Cisco Asa по протоколу SSH (enable)	Конфигурации

Табл. 166. Python-скрипты для сбора данных межсетевых экранов Cisco ASA

НАИМЕНОВАНИЕ	ОПИСАНИЕ	
ECI_CISCO_ASA_-SHOW_VERSION (ssh1)	Сканер для сбора версии Cisco Asa по протоколу SSH	Версия ПО
ECI_CISCO_ASA_-SHOW_VERSION (ssh2)	Сканер для сбора версии Cisco Asa по протоколу SSH	Версия ПО

Табл. 167. Python-скрипты для сбора данных с сетевого оборудования Cisco

НАИМЕНОВАНИЕ	ОПИСАНИЕ	
ECI_CISCO_IOS_-SHOW_ARP (ssh)	Сканер для сбора ARP-таблицы CIsco по протоколу SSH	ARP-таблица
ECI_CISCO_IOS_-SHOW_ARP (telnet)	Сканер для сбора ARP-таблицы CIsco по протоколу telnet	ARP-таблица
ECI_CISCO_IOS_SHOW_-ARP-telnet-nologin	Сканер для сбора ARP-таблицы Cisco по протоколу telnet (nologin)	ARP-таблица
ECI_CISCO_IOS_-SHOW_IPROUTE (ssh)	Сканер для сбора таблицы маршрутизации Cisco по протоколу SSH	Таблица маршрутизаци
ECI_CISCO_IOS_SHOW_-IPROUTE (ssh-en)	Сканер для сбора таблицы маршрутизации Cisco по протоколу SSH (enable)	Таблица маршрутизаци
ECI_CISCO_IOS_-SHOW_IPROUTE (telnet)	Сканер для сбора таблицы маршрутизации Cisco по протоколу telnet	Таблица маршрутизаци
ECI_CISCO_IOS_SHOW_-IPROUTE (telnet_en)	Сканер для сбора таблицы маршрутизации Cisco по протоколу telnet (enable)	Таблица маршрутизаци
ECI_CISCO_IOS_SHOW_-IPROUTE-telnet-nologin	Сканер для сбора таблицы маршрутизации Cisco по протоколу telnet (nologin)	Таблица маршрутизаци
ECI_CISCO_IOS_SHOW_-MAC_ADDRESS_TABLE (ssh)	Сканер для сбора таблицы mac-адресов Cisco по протоколу SSH	MAC-адреса
ECI_CISCO_IOS_SHOW_-MAC_ADDRESS_-TABLE (ssh) alternative	Сканер для сбора таблицы mac-адресов Cisco по протоколу SSH	MAC-адреса

Табл. 167. Python-скрипты для сбора данных с сетевого оборудования Cisco

НАИМЕНОВАНИЕ	ОПИСАНИЕ	
ECI_CISCO_IOS_SHOW_MAC_-ADDRESS_TABLE (ssh-en)	Сканер для сбора таблицы mac-адресов Cisco по протоколу SSH (enable)	MAC-адреса
ECI_CISCO_IOS_SHOW_MAC_-ADDRESS_TABLE (telnet)	Сканер для сбора таблицы mac-адресов Cisco по протоколу telnet	MAC-адреса
ECI_CISCO_IOS_SHOW_MAC_-ADDRESS_TABLE (telnet-en)	Сканер для сбора таблицы mac-адресов Cisco по протоколу telnet (enable)	MAC-адреса
ECI_CISCO_IOS_SHOW_MAC_-ADDRESS_TABLE-telnet-nologin	Сканер для сбора таблицы mac-адресов Cisco по протоколу telnet (nologin)	MAC-адреса
ECI_CISCO_IOS_SHOW_-RUNNING_CONFIG (ssh)	Сканер для сбора текущей конфигурации Cisco по протоколу SSH	Конфигурации
ECI_CISCO_IOS_SHOW_-RUNNING_CONFIG (ssh-en)	Сканер для сбора текущей конфигурации Cisco по протоколу SSH (enable)	Конфигурации
ECI_CISCO_IOS_SHOW_-RUNNING_CONFIG (telnet)	Сканер для сбора текущей конфигурации Cisco по протоколу telnet	Конфигурации
ECI_CISCO_IOS_SHOW_-RUNNING_CONFIG (telnet-en)	Сканер для сбора текущей конфигурации Cisco по протоколу telnet (enable)	Конфигурации
ECI_CISCO_IOS_-SHOW_RUNNING_-CONFIG-telnet-en-nologin	Сканер для сбора текущей конфигурации Cisco по протоколу telnet (nologin)	Конфигурации
ECI_CISCO_IOS_SHOW_-STARTUP_CONFIG (ssh)	Сканер для сбора начальной конфигурации Cisco по протоколу SSH	Конфигурации
ECI_CISCO_IOS_SHOW_-STARTUP_CONFIG (ssh-en)	Сканер для сбора начальной конфигурации Cisco по протоколу SSH (enable)	Конфигурации
ECI_CISCO_IOS_SHOW_-STARTUP_CONFIG (telnet)	Сканер для сбора начальной конфигурации Cisco по протоколу telnet	Конфигурации

Табл. 167. Python-скрипты для сбора данных с сетевого оборудования Cisco

НАИМЕНОВАНИЕ	ОПИСАНИЕ	
ECI_CISCO_IOS_SHOW_-STARTUP_CONFIG (telnet-en)	Сканер для сбора начальной конфигурации Cisco по протоколу telnet (enable)	Конфигурации
ECI_CISCO_IOS_-SHOW_STARTUP_-CONFIG-telnet-en-nologin	Сканер для сбора начальной конфигурации Cisco по протоколу telnet (nologin)	Конфигурации
ECI_CISCO_IOS_-SHOW_VERSION (ssh)	Сканер для сбора версии Cisco по протоколу SSH	Версия ПО
ECI_CISCO_IOS_SHOW_-VERSION (ssh-en)	Сканер для сбора версии Cisco по протоколу SSH (enable)	Версия ПО
ECI_CISCO_IOS_SHOW_-VERSION (telnet)	Сканер для сбора версии Cisco по протоколу telnet	Версия ПО
ECI_CISCO_IOS_SHOW_-VERSION (telnet-en)	Сканер для сбора версии Cisco по протоколу telnet (enable)	Версия ПО
ECI_CISCO_IOS_SHOW_-VERSION-telnet-nologin	Сканер для сбора версии Cisco по протоколу telnet (nologin)	Версия ПО
ECI_CISCO_IOS_-SH_INV (ssh-en)	Сканер для инвентаризации Cisco по протоколу SSH (enable)	Инвентаризационные д
ECI_CISCO_IOS_-SH_INV (telnet-en)	Сканер для инвентаризации Cisco по протоколу telnet (enable)	Инвентаризационные д

Табл. 168. Python-скрипты для сбора данных сетевого оборудования Eltex

НАИМЕНОВАНИЕ	ОПИСАНИЕ	
ECI_ELTEX_ESR_SHOW_ARP	Сканер для сбора ARP-таблицы Eltex по протоколу SSH	ARP-таблица
ECI_ELTEX_ESR_-SHOW_IP_ROUTE	Сканер для сбора таблицы маршрутизации Eltex по протоколу SSH	Таблица маршрутизаци
ECI_ELTEX_ESR_SHOW_-RUNNING_CONFIG	Сканер для сбора текущей конфигурации Eltex по протоколу SSH	Конфигурации

Табл. 168. Python-скрипты для сбора данных сетевого оборудования Eltex

НАИМЕНОВАНИЕ	ОПИСАНИЕ	
ECI_ELTEX_ESR_-SHOW_VERSION	Сканер для сбора версии Eltex по протоколу SSH	Версия ПО
ECI_ELTEX_MES_SHOW_ARP	Сканер для сбора ARP-таблицы Eltex по протоколу SSH	ARP-таблица
ECI_ELTEX_MES_-SHOW_IPROUTE	Сканер для сбора таблицы маршрутизации Eltex по протоколу SSH	Таблица маршрутизаци
ECI_ELTEX_MES_SHOW_-MAC_ADDRESS_TABLE	Сканер для сбора таблицы mac-адресов Eltex по протоколу SSH	MAC-адреса
ECI_ELTEX_MES_SHOW_-RUNNING_CONFIG	Сканер для сбора текущей конфигурации Eltex по протоколу SSH	Конфигурации
ECI_ELTEX_MES_SHOW_-STARTUP_CONFIG	Сканер для сбора начальной конфигурации Eltex по протоколу SSH	Конфигурации
ECI_ELTEX_MES_-SHOW_VERSION	Сканер для сбора версии Eltex по протоколу SSH	Версия ПО

Табл. 169. Python-скрипты для сбора данных SCADA Honeywell

НАИМЕНОВАНИЕ	ОПИСАНИЕ	
Шаблон безопасности Win Server 2008 для SCADA Honeywell (winrm http)	Сканер для сбора списка шаблонов безопасности Win Server 2008 для SCADA Honeywell по протоколу winrm http	Шаблоны безопасности
Шаблон безопасности Win Server 2008 для SCADA Honeywell (winrm https)	Сканер для сбора списка шаблонов безопасности Win Server 2008 для SCADA Honeywell по протоколу winrm https	Шаблоны безопасности
Шаблон безопасности Win10 для SCADA Honeywell (winrm http)	Сканер для сбора списка шаблонов безопасности Win10 для SCADA Honeywell по протоколу winrm http	Шаблоны безопасности
Шаблон безопасности Win10 для SCADA Honeywell (winrm https)	Сканер для сбора списка шаблонов безопасности Win10 для SCADA Honeywell по протоколу winrm https	Шаблоны безопасности
Шаблон безопасности Win7 для SCADA Honeywell (winrm http)	Сканер для сбора списка шаблонов безопасности Win7 для SCADA Honeywell по протоколу winrm http	Шаблоны безопасности

Табл. 169. Python-скрипты для сбора данных SCADA Honeywell

НАИМЕНОВАНИЕ	ОПИСАНИЕ	
Шаблон безопасности Win7 для SCADA Honeywell (winrm https)	Сканер для сбора списка шаблонов безопасности Win7 для SCADA Honeywell по протоколу winrm https	Шаблоны безопасности

Табл. 170. Python-скрипты для сбора данных с сетевого оборудования Huawei VRP

НАИМЕНОВАНИЕ	ОПИСАНИЕ	
ECI_HUAWEI_VRP_SHOW_-STARTUP_CONFIG (ssh, noen)	Начальная конфигурация (ssh, без enable)	Конфигурации
ECI_HUAWEI_VRP_-SHOW_MAC_ADDRESS_-TABLE (ssh,noen)	Таблица mac-адресов Huawei VRP (ssh, без enable)	MAC-адреса
ECI_HUAWEI_VRP_-SHOW_ARP (ssh, noen)	ARP таблица Huawei VRP (ssh, без enable)	ARP-таблица
ECI_HUAWEI_VRP_SHOW_-RUNNING_CONFIG (ssh, noen)	Текущая конфигурация Huawei VRP (ssh, без enable)	Конфигурации
ECI_HUAWEI_VRP_SHOW_-VERSION (ssh, noen)	Версия ОС Huawei VRP (ssh, без enable)	Версия ОС

Табл. 171. Python-скрипты для сбора данных сетевого оборудования HP

НАИМЕНОВАНИЕ	ОПИСАНИЕ	
HP2424 IP (telnet)	Сканер для сбора таблицы IP-адресов HP2424 по протоколу telnet	IP-адреса
HP2424 IP (telnet, nologin)	Сканер для сбора таблицы IP-адресов HP2424 по протоколу telnet (no login)	IP-адреса
HP2424 конфигурация (telnet)	Сканер для сбора конфигурации HP2424 по протоколу telnet	Конфигурации
HP2424 конфи-гурация (telnet, nologin)	Сканер для сбора конфигурации HP2424 по протоколу telnet (no login)	Конфигурации
HP2424 модули (telnet)	Сканер для сбора модулей HP2424 по протоколу telnet	Модули
HP2424 модули (telnet, nologin)	Сканер для сбора модулей HP2424 по протоколу telnet (no login)	Модули

Табл. 171. Python-скрипты для сбора данных сетевого оборудования HP

НАИМЕНОВАНИЕ	ОПИСАНИЕ	
HP2424 сведения о системе (telnet)	Сканер для сбора сведения о системе HP2424 по протоколу telnet	Информация о системе
HP2424 сведения о системе (telnet, nologin)	Сканер для сбора сведения о системе HP2424 по протоколу telnet (no login)	Информация о системе
Начальная конфигурация HP (ssh)	Сканер для сбора начальной конфигурации HP по протоколу SSH	Конфигурации
Конфигурация HP A5500 (ssh)	Сканер для сбора конфигурации HP A5500 по протоколу SSH	Конфигурации
Начальная конфигурация HP (telnet)	Сканер для сбора начальной конфигурации HP по протоколу telnet	Конфигурации
Текущая конфигурация HP (ssh)	Сканер для сбора текущей конфигурации HP по протоколу SSH	Конфигурации
Текущая конфигурация HP (telnet)	Сканер для сбора текущей конфигурации HP по протоколу telnet	Конфигурации

Табл. 172. Python-скрипты для сбора данных SCADA InTouch

НАИМЕНОВАНИЕ	ОПИСАНИЕ	
Проверка параметров операционной системы (winrm http)	Сканер для проверки параметров операционной системы по протоколу winrm http	Параметры ОС
Проверка параметров операционной системы (winrm https)	Сканер для проверки параметров операционной системы по протоколу winrm https	Параметры ОС
Проверка прав пользователя (winrm http)	Сканер для проверки прав пользователя по протоколу winrm http	Права пользователей
Проверка прав пользователя (winrm https)	Сканер для проверки прав пользователя по протоколу winrm https	Права пользователей

Табл. 173. Python-скрипты для сбора данных сетевого оборудования Mgate

НАИМЕНОВАНИЕ	ОПИСАНИЕ	
ECI_MOXA_MGATE_SHOW_-RUNNING_CONFIG (telnet)	Сканер для сбора списка запущенных конфигураций по протоколу telnet	Конфигурации

Табл. 173. Python-скрипты для сбора данных сетевого оборудования Mgate

НАИМЕНОВАНИЕ	ОПИСАНИЕ	
ECI_MOXA_MGATE_-SHOW_RUNNING_-CONFIG (telnet-noauth)	Сканер для сбора списка запущенных конфигураций по протоколу telnet (noauth)	Конфигурации
ECI_MOXA_MGATE_-SHOW_RUNNING_-CONFIG-telnet-noauth-full	Сканер для сбора списка запущенных конфигураций по протоколу telnet (noauth-full)	Конфигурации

Табл. 174. Python-скрипты для сбора трафика баз данных MSSQL и MySQL

НАИМЕНОВАНИЕ	ОПИСАНИЕ	
MSSQL_Логины и права	Сканер для сбора списка логинов и их прав на MSSQL по протоколу sql	Логины и права
MSSQL_Логины и права (noport)	Сканер для сбора списка логинов и их прав на MSSQL по протоколу sql (no port)	Логины и права
MSSQL_Логины и права (без паролей)	Сканер для сбора списка логинов и их прав на MSSQL по протоколу sql (no pass)	Логины и права
MSSQL_Права пользователей на БД	Сканер для сбора списка прав пользователей на БД MSSQL по протоколу sql	Права пользователей
MSSQL_Права пользователей на БД (noport)	Сканер для сбора списка прав пользователей на БД MSSQL по протоколу sql (no port)	Права пользователей
MySQL пользователи	Сканер для сбора списка пользователей на БД MySQL	Пользователи
MySQL права пользователей	Сканер для сбора списка прав пользователей на БД MySQL	Права пользователей
MySQL сбор событий входа и выхода пользователя	Сканер для сбора списка событий входа и выхода пользователей на БД MySQL	События
MySQL сбор событий запуска и остановки	Сканер для сбора списка событий запуска и останова на БД MySQL	События
MySQL_Права пользователей	Сканер для сбора списка прав пользователей на MySQL по протоколу sql	Права пользователей
MySQL_Права пользователей_Columns	Сканер для сбора списка прав пользователей на столбцы MySQL по протоколу sql	Права пользователей

Табл. 174. Python-скрипты для сбора трафика баз данных MSSQL и MySQL

НАИМЕНОВАНИЕ	ОПИСАНИЕ	
MySQL_Права пользователей_DB	Сканер для сбора списка прав пользователей на БД MySQL по протоколу sql	Права пользователей
MySQL_Права пользователей_Tables	Сканер для сбора списка прав пользователей на таблицы MySQL по протоколу sql	Права пользователей
MySQL_События входа-выхода	Сканер для сбора событий входа-выхода MySQL по протоколу sql	События

Табл. 175. Python-скрипты для сбора данных сетевого оборудования NIS

НАИМЕНОВАНИЕ	ОПИСАНИЕ	
ECI_NIS_SHOW_ARP-ssh	Сканер для сбора ARP-таблицы NIS по протоколу SSH	ARP-таблица
ECI_NIS_SHOW_IPROUTE-ssh	Сканер для сбора таблицы маршрутизации NIS по протоколу SSH	Таблица маршрутизаци
ECI_NIS_SHOW_MAC_-ADDRESS_TABLE-ssh	Сканер для сбора таблицы mac-адресов NIS по протоколу SSH	MAC-адреса
ECI_NIS_SHOW_RUNNING_-CONFIG-ssh-noen	Сканер для сбора текущей конфигурации NIS по протоколу SSH	Конфигурации
ECI_NIS_SHOW_VERSION-ssh	Сканер для сбора версии Nis по протоколу SSH	Версия ПО
NIS 3500-2216 интерфейсы (telnet)	Сканер для сбора интерфейсов NIS 3500-2216 по протоколу Telnet	Интерфейсы
NIS 3500-2216 информация об IP (telnet)	Сканер для сбора информации об IP NIS 3500-2216 по протоколу Telnet	Информация об IP
NIS 3500-2216 общая информация (telnet)	Сканер для сбора общей информации NIS 3500-2216 по протоколу Telnet	Общая информация
NIS_SHOW_ARP(telnet)	Сканер для сбора ARP-таблицы Nis по протоколу telnet	ARP-таблица
NIS_SHOW_IPROUTE(telnet)	Сканер для сбора таблицы маршрутизации Nis по протоколу telnet	Таблица маршрутизаци
NIS_SHOW_MAC_-ADDRESS_TABLE(telnet)	Сканер для сбора таблицы mac-адресов Nis по протоколу telnet	MAC-адреса
NIS_SHOW_RUNNING_-CONFIG(telnet)	Сканер для сбора текущей конфигурации NIS по протоколу telnet	Конфигурации

Табл. 176. Python-скрипты для сбора данных утилиты nmap

НАИМЕНОВАНИЕ	ОПИСАНИЕ	
Открытые порты (nmap)	Сканер для сбора списка открытых портов nmap	Порты
Расширенное сканирование (nmap)	Сканер для расширенного сканирования nmap	Конфигурац

Табл. 177. Python-скрипты для сбора данных с ОС QNX

НАИМЕНОВАНИЕ	ОПИСАНИЕ	
ARP таблица QNX 6.5 (ssh)	Сканер для сбора ARP-таблицы с QNX 6.5	ARP-таблица
ARP-таблица QNX (telnet)	Сканер для сбора ARP-таблицы QNX по протоколу telnet	ARP-таблица
Зарегистрированные пользователи QNX (lastlog)	Сканер для сбора зарегистрированных пользователей QNX по протоколу telnet (lastlog)	ARP-таблица
Зарегистрированные пользователи QNX (telnet)	Сканер для сбора зарегистрированных пользователей QNX по протоколу telnet	ARP-таблица
Зарегистрированные пользователи QNX 6.5 (ssh)	Сканер для сбора списка вошедших в систему пользователей по протоколу SSH	ARP-таблица
Имя сетевого узла QNX (telnet)	Сканер для сбора имени сетевого узла QNX по протоколу telnet	Имя сетевого узла
Имя сетевого узла QNX 6.5 (ssh)	Сканер для сбора имени сетевого узла по протоколу SSH	Имя сетевого узла
Информация об ОС QNX 6.5 (ssh)	Сканер для сбора информации об ОС по протоколу SSH	Информация об ОС
Используемые DNS-сервера QNX (telnet)	Сканер для сбора используемых DNS-серверов QNX по протоколу telnet	DNS-сервера
Используемые DNS-сервера QNX 6.5 (ssh)	Сканер для сбора содержимого файла resolv.conf по протоколу SSH	DNS-сервера
Конфигурационные строки QNX 6.5 (getconf -a) (ssh)	Сканер для сбора настроек безопасности QNX по протоколу SSH	Настройки безопаснос
Объекты cron QNX 6.5 (ssh)	Сканер для сбора объектов crontab по протоколу SSH	Объекты
Объекты cron QNX4 (telnet)	Сканер для сбора объектов cron QNX4 по протоколу telnet	Объекты

Табл. 177. Python-скрипты для сбора данных с ОС QNX

НАИМЕНОВАНИЕ	ОПИСАНИЕ	
Сетевая статистика QNX (telnet)	Сканер для сбора сетевой статистики QNX по протоколу telnet	Сетевая информация
Сетевая статистика QNX 6.5 (ssh)	Сканер для сбора сетевой статистики по протоколу SSH	Сетевая информация
Сетевые интерфейсы QNX (telnet)	Сканер для сбора сетевых интерфейсов QNX по протоколу telnet	Сетевые интерфейсы
Сетевые интерфейсы QNX 6.5 (ssh)	Сканер для сбора списка сетевых интерфейсов QNX по протоколу SSH	Сетевые интерфейсы
Сетевые порты в режиме Listening QNX (telnet)	Сканер для сбора сетевых портов в режиме Listening QNX по протоколу telnet	Порты
Сетевые порты в режиме listening QNX 6.5 (ssh)	Сканер для сбора списка портов в режиме LISTEN по протоколу SSH	Порты
Список групп QNX (telnet)	Сканер для сбора списка групп QNX по протоколу telnet	
Список групп QNX 6.5 (ssh)	Сканер для сбора списка групп QNX	Группы
Список подключенных устройств QNX4 (telnet)	Сканер для сбора списка подключенных устройств QNX4 по протоколу telnet	Устройства
Список пользователей QNX (telnet)	Сканер для сбора списка пользователей QNX по протоколу telnet	Пользователи
Список пользователей QNX 6.5 (ssh)	Сканер для сбора списка пользователей по протоколу SSH	Пользователи
Список процессов QNX 6.5 (ssh)	Сканер для сбора списка процессов по протоколу SSH с QNX	Процессы
Список процессов QNX4 (telnet)	Сканер для сбора списка процессов QNX4 по протоколу telnet	Процессы
Таблица маршрутизации QNX (telnet)	Сканер для сбора таблицы маршрутизации QNX4 по протоколу telnet	Таблица маршрутизаци
Таблица маршрутизации QNX 6.5 (ssh)	Сканер для сбора таблицы маршрутизации по протоколу SSH	Таблица маршрутизаци

Табл. 177. Python-скрипты для сбора данных с ОС QNX

НАИМЕНОВАНИЕ	ОПИСАНИЕ	
Установленные утилиты QNX 6.5 (ssh)	Сканер для сбора списка установленных утилит по протоколу SSH	Установленное ПО
Установленные утилиты QNX4 (telnet)	Сканер для сбора списка установленных утилит QNX4 по протоколу telnet	Установленное ПО
Файл hosts QNX (telnet)	Сканер для сбора файла hosts QNX по протоколу telnet	Сетевые узлы
Файл hosts QNX 6.5 (ssh)	Сканер для сбора содержимого файла hosts QNX	Сетевые узлы

Табл. 178. Python-скрипты для сбора данных Redkit

НАИМЕНОВАНИЕ	ОПИСАНИЕ	
Время изменения таблиц сигналов Redkit	Сканер для сбора времени изменения таблиц сигналов Redkit	Изменения таблиц сиг
Контроль неизменности проекта Redkit	Сканер для контроля неизменности проекта Redkit	Изменения проекта
Контрольная сумма каталогов Redkit (winrm https)	Сканер для сбора списка контрольных сумм каталогов Redkit по протоколу winrm https	Контрольные суммы
Контрольная сумма каталогов Redkit конфигурации (winrm https)	Сканер для сбора списка контрольных сумм каталогов конфигурации Redkit по протоколу winrm https	Контрольные суммы
Контрольная сумма каталогов Redkit кэши (winrm https)	Сканер для сбора списка кэша контрольных сумм каталогов Redkit по протоколу winrm https	Контрольные суммы
Контрольная сумма проекта Redkit	Сканер для сбора списка контрольных сумм проекта Redkit	Контрольные суммы
Перечень пользователей Redkit	Сканер для сбора списка пользователей проекта Redkit	Пользователи
Права пользователей в Redkit	Сканер для сбора списка прав пользователей Redkit	Права пользователей

Табл. 179. Python-скрипты для сбора данных ПЛК Siemens

НАИМЕНОВАНИЕ	ОПИСАНИЕ	
Конфигурация ПЛК (snap 7)	Сканер для сбора конфигурации ПЛК Siemens по протоколу SNAP 7	Конфигурац
Конфигурация ПЛК (snap 7) (1.18+)	Сканер для сбора конфигурации ПЛК Siemens по протоколу SNAP 7	Конфигурац
Конфигурация ПЛК (snap 7) (1.18+) (extended)	Сканер для сбора конфигурации ПЛК Siemens по протоколу SNAP 7 (extended)	Конфигурац
Конфигурация ПЛК (snap 7) (No CPU)	Сканер для сбора конфигурации ПЛК Siemens по протоколу SNAP 7	Конфигурац
Конфигурация ПЛК Slemens S7-300_400	Сканер для сбора конфигурации ПЛК Siemens по протоколу S7-300_400	Конфигурац
Просмотр слотов ПЛК (snap7)	Сканер для просмотра слотов ПЛК Siemens по протоколу SNAP7	Конфигурац
Расширенная конфигурация ПЛК Siemens S7-300_400	Сканер для сбора расширенной конфигурации ПЛК Siemens по протоколу S7-300_400	Конфигурац

Табл. 180. Python-скрипты для сбора данных ПЛК Schneider Electric

НАИМЕНОВАНИЕ	ОПИСАНИЕ	
Schenieder M340 Ethernet settings	Сканер для сбора настроек сети Ethernet ПЛК Schneider Electric M340	Настройки с
Schenieder M580 Ethernet settings NOR0200_NGD0100	Сканер для сбора настроек сети Ethernet ПЛК Schneider Electric M580 с сетевых интерфейсов NOR0200 и NGD0100	Настройки с
Schenieder M580 Ethernet settings встроенный модуль	Сканер для сбора настроек сети Ethernet ПЛК Schneider Electric M580 со встроенного модуля	Настройки с
Schenieder Momentum Ethernet settings	Сканер для сбора настроек сети Momentum Ethernet ПЛК Schneider Electric	Настройки с
Schenieder password_control	Сканер для сбора изменений пароля ПЛК Schneider Electric	Настройки с
Schenieder Premium Ethernet settings	Сканер для сбора настроек сети Premium Ethernet ПЛК Schneider Electric	Настройки с
Schenieder Quantum Ethernet settings	Сканер для сбора настроек сети Quantum Ethernet ПЛК Schneider Electric	Настройки с

Табл. 180. Python-скрипты для сбора данных ПЛК Schneider Electric

НАИМЕНОВАНИЕ	ОПИСАНИЕ	
Schenieder Quantum io_head settings	Сканер для сбора настроек сети Quantum с использованием головного модуля Remote IO ПЛК Schneider Electric	Настройки с
Конфигурация ПЛК Schneider	Сканер для сбора конфигурации ПЛК Schneider Electric	Конфигурац
Конфигурация проекта ПЛК Schneider	Сканер для сбора конфигурации проекта ПЛК Schneider Electric	Конфигурац
Программа ПЛК Schneider	Сканер для сбора программы ПЛК Schneider Electric	Программа
Состояние ПЛК Schneider	Сканер для сбора состояния ПЛК Schneider Electric	Состояние П

Табл. 181. Python-скрипты для сбора данных по протоколу SNMP

НАИМЕНОВАНИЕ	ОПИСАНИЕ	
SNMP 2c. Раздел IP	Сканер для сбора параметров IP по протоколу SNMP2c	Параметры
SNMP 2c. Раздел egp	Сканер для сбора параметров EGP по протоколу SNMP2c	Параметры
SNMP 2c. Раздел icmp	Сканер для сбора параметров ICMP по протоколу SNMP2c	Параметры
SNMP 2c. Раздел interfaces	Сканер для сбора списка интерфейсов по протоколу SNMP2c	Интерфейсы
SNMP 2c. Раздел snmp	Сканер для сбора параметров SNMP по протоколу SNMP2c	Параметры
SNMP 2c. Раздел system	Сканер для сбора параметров System по протоколу SNMP2c	Параметры
SNMP 2c. Раздел system (noformat)	Сканер для сбора параметров System по протоколу SNMP2c (noformat)	Параметры
SNMP 2c. Раздел tcp	Сканер для сбора параметров TCP по протоколу SNMP2c	Параметры
SNMP 2c. Раздел udp	Сканер для сбора параметров UDP по протоколу SNMP2c	Параметры
SNMP 3. Раздел IP	Сканер для сбора параметров IP по протоколу SNMP3	Параметры
SNMP 3. Раздел egp	Сканер для сбора параметров EGP по протоколу SNMP3	Параметры

Табл. 181. Python-скрипты для сбора данных по протоколу SNMP

НАИМЕНОВАНИЕ	ОПИСАНИЕ	
SNMP 3. Раздел icmp	Сканер для сбора параметров ICMP по протоколу SNMP3	Параметры
SNMP 3. Раздел interfaces	Сканер для сбора списка интерфейсов по протоколу SNMP3	Интерфейсы
SNMP 3. Раздел snmp	Сканер для сбора параметров SNMP по протоколу SNMP3	Параметры
SNMP 3. Раздел system	Сканер для сбора параметров System по протоколу SNMP3	Параметры
SNMP 3. Раздел system (noformat)	Сканер для сбора параметров System по протоколу SNMP3 (noformat)	Параметры
SNMP 3. Раздел tcp	Сканер для сбора параметров TCP по протоколу SNMP3	Параметры
SNMP 3. Раздел udp	Сканер для сбора параметров UDP по протоколу SNMP3	Параметры

Табл. 182. Python-скрипты для сбора данных ОС Solaris

НАИМЕНОВАНИЕ	ОПИСАНИЕ	
ARP-таблица Solaris (ssh)	Сканер для сбора ARP-таблицы Solaris по протоколу SSH	ARP-таблица
Группы пользо-вателей Solaris (ssh)	Сканер для сбора групп пользователей Solaris по протоколу SSH	Группы пользователей
Запланированные задачи cron Solaris (ssh, su)	Сканер для сбора запланированных задач cron Solaris по протоколу SSH (sudo)	Задачи
Имя сетевого узла Solaris (ssh)	Сканер для сбора имени сетевого узла Solaris по протоколу SSH	Сетевые узлы

Табл. 182. Python-скрипты для сбора данных ОС Solaris

НАИМЕНОВАНИЕ	ОПИСАНИЕ	
Объекты автозапуска Solaris (ssh)	Сканер для сбора объектов автозапуска Solaris по протоколу SSH	Объекты автозапуска
Пользователи Solaris (ssh)	Сканер для сбора списка пользователей Solaris по протоколу SSH	Пользователи
Сетевые порты в режиме LISTENING Solaris (ssh)	Сканер для сбора сетевых портов в режиме LISTENING Solaris по протоколу SSH	Сетевые порты
Список процессов Solaris (ssh)	Сканер для сбора списка процессов Solaris по протоколу SSH	Процессы
Таблица маршрутизации Solaris (ssh)	Сканер для сбора таблицы маршрутизации Solaris по протоколу SSH	Таблица маршрутизаци
Установленное ПО Solars (ssh)	Сканер для сбора списка установленного ПО Solaris по протоколу SSH	Установленное ПО

Табл. 183. Python-скрипты для сбора данных ОС Unix

НАИМЕНОВАНИЕ	ОПИСАНИЕ	
ARP-таблица (ssh, sudo)	Скрипт для сбора ARP-таблицы Unix по протоколу SSH (sudo)	ARP-таблица
ARP-таблица SuSE (ssh)	Сканер для сбора ARP-таблицы SuSE по протоколу SSH	ARP-таблица
ARP-таблица Unix (ssh)	Сканер для сбора ARP-таблицы Unix по протоколу SSH	ARP-таблица
DNS-сервера Unix (ssh)	Сканер для сбора DNS-серверов Unix по протоколу SSH	DNS-сервера
Запланированные задачи cron Unix (ssh)	Сканер для сбора запланированных задач cron Unix по протоколу SSH	Задачи
Запланированные задачи cron Unix (ssh, sudo)	Сканер для сбора запланированных задач cron Unix по протоколу SSH (sudo)	Задачи
Имя сетевого узла Unix (ssh)	Сканер для сбора имени сетевого узла Unix по протоколу SSH	Контрольные суммы
Контрольные суммы DATAPK (ssh)	Сканер для сбора контрольных сумм DATAPK по протоколу SSH	Контрольные суммы
Объекты автозапуска SuSE (ssh)	Сканер для сбора объектов автозапуска SuSE по протоколу SSH	Объекты автозапуска

Табл. 183. Python-скрипты для сбора данных ОС Unix

НАИМЕНОВАНИЕ	ОПИСАНИЕ	
Объекты авто-запуска Unix (ssh)	Сканер для сбора объектов автозапуска Unix по протоколу SSH	Объекты автозапуска
Подключенные носители информации SuSE (ssh)	Сканер для сбора подключенных носителей информации SuSE по протоколу SSH	Носители информации
Подключенные носители информации Unix (ssh)	Сканер для сбора подключенных носителей информации Unix по протоколу SSH	Носители информации
Подключенные устройства Unix (ssh)	Сканер для сбора подключенных устройств Unix по протоколу SSH	Устройства
Правила Iptables SuSE (ssh, sudo)	Сканер для сбора правил Iptables SuSE по протоколу SSH (sudo)	Правила iptables
Правила Iptables Unix (ssh)	Сканер для сбора правил Iptables Unix по протоколу SSH	Правила iptables
Правила Iptables Unix (ssh, sudo)	Сканер для сбора правил Iptables Unix по протоколу SSH (sudo)	Правила iptables
Правила SuSEfirewall2 (ssh)	Сканер для сбора правил SuSEfirewall2 по протоколу SSH	Правила SuSEfirewall2
Сетевые порты в режиме LISTENING Unix (ssh)	Сканер для сбора сетевых портов в режиме LISTENING Unix по протоколу SSH	Порты
Содержимое файла sudoers Unix (ssh)	Сканер для сбора содержимого файла sudoers Unix по протоколу SSH	Содержимое файла
Содержимое файла sudoers Unix (ssh, sudo)	Сканер для сбора содержимого файла sudoers Unix по протоколу SSH (sudo)	Содержимое файла
Состояние сервисов DATAPK (ssh)	Сканер для сбора состояния сервисов DATAPK по протоколу SSH	Состояние сервисов
Список групп Unix (ssh)	Сканер для сбора списка групп Unix по протоколу SSH	Группы
Список пользо-вателей Unix (ssh)	Сканер для сбора списка пользователей Unix по протоколу SSH	Пользователи
Список процессов Unix (ssh)	Сканер для сбора списка процессов Unix по протоколу SSH	Процессы
Список процессов Unix (ssh) nodiff	Сканер для сбора списка процессов Unix по протоколу SSH	Процессы

Табл. 183. Python-скрипты для сбора данных ОС Unix

НАИМЕНОВАНИЕ	ОПИСАНИЕ	
Список процессов Unix (ssh) без PID	Сканер для сбора списка процессов Unix без PID по протоколу SSH	Процессы
Таблица маршрутизации SuSE (ssh)	Сканер для сбора таблицы маршрутизации SuSE по протоколу SSH	Таблица маршрутизаци
Таблица маршрутизации Unix (ssh)	Сканер для сбора таблицы маршрутизации Unix по протоколу SSH	Таблица маршрутизаци
Файл Shadow Unix (ssh)	Сканер для сбора файла shadow Unix по протоколу SSH	Файл shadow Unix
Файл Shadow Unix (ssh, sudo)	Сканер для сбора файла shadow Unix по протоколу SSH (sudo)	Файл shadow Unix
Файл hosts Unix (ssh)	Сканер для сбора файла hosts Unix по протоколу SSH	Файл hosts Unix

Табл. 184. Python-скрипты для сбора данных ОС Windows

НАИМЕНОВАНИЕ	ОПИСАНИЕ	
ARP-таблица (basic) (winrm http)	Сканер для сбора таблицы ARP Windows по протоколу winrm http	ARP-таблица
ARP-таблица (basic) (winrm https)	Сканер для сбора таблицы ARP Windows по протоколу winrm https	ARP-таблица
ARP-таблица (winexe 0.8)	Сканер для сбора таблицы ARP Windows по протоколу winexe 0.8	ARP-таблица
ARP-таблица (winexe 1.0)	Сканер для сбора таблицы ARP Windows по протоколу winexe 1.0	ARP-таблица
ARP-таблица (winrm http)	Сканер для сбора таблицы ARP Windows по протоколу winrm http	ARP-таблица
ARP-таблица (winrm https)	Сканер для сбора таблицы ARP Windows по протоколу winrm https	ARP-таблица
Версия KES (basic) (winrm http)	Сбор версии Kaspersky Endpoint Security по протоколу winrm http	Версия ПО
Версия KES (basic) (winrm https)	Сбор версии Kaspersky Endpoint Security по протоколу winrm https	Версия ПО
Версия KES (winexe 0.8)	Сбор версии Kaspersky Endpoint Security по протоколу winexe 0.8	Версия ПО
Версия KES (winexe 1.0)	Сбор версии Kaspersky Endpoint Security по протоколу winexe 1.0	Версия ПО
Версия KES (winrm http)	Сбор версии Kaspersky Endpoint Security по протоколу winrm http	Версия ПО

Табл. 184. Python-скрипты для сбора данных ОС Windows

НАИМЕНОВАНИЕ	ОПИСАНИЕ	
Версия KES (winrm https)	Сбор версии Kaspersky Endpoint Security по протоколу winrm https	Версия ПО
Версия WinNT (basic) (winrm http)	Сканер для сбора версии Windows NT по протоколу winrm http	Версия ПО
Версия WinNT (basic) (winrm https)	Сканер для сбора версии Windows NT по протоколу winrm https	Версия ПО
Версия WinNT (winexe 0.8)	Сканер для сбора версии Windows NT по протоколу winexe 0.8	Версия ПО
Версия WinNT (winexe 1.0)	Сканер для сбора версии Windows NT по протоколу winexe 1.0	Версия ПО
Версия WinNT (winrm http)	Сканер для сбора версии Windows NT по протоколу winrm http	Версия ПО
Версия WinNT (winrm https)	Сканер для сбора версии Windows NT по протоколу winrm https	Версия ПО
Версия Windows (basic) (winrm http)	Сканер для сбора версии Windows по протоколу winrm http	Версия ПО
Версия Windows (basic) (winrm https)	Сканер для сбора версии Windows по протоколу winrm https	Версия ПО
Версия Windows (winexe 0.8)	Сканер для сбора версии Windows по протоколу winexe 0.8	Версия ПО
Версия Windows (winexe 1.0)	Сканер для сбора версии Windows по протоколу winexe 1.0	Версия ПО
Версия Windows (winrm http)	Сканер для сбора версии Windows по протоколу winrm http	Версия ПО
Версия Windows (winrm https)	Сканер для сбора версии Windows по протоколу winrm https	Версия ПО
Группы и их члены (wmi)	Сбор списка групп и членов групп Windows по протоколу wmi	Группы
Группы и их члены powershell (basic) (winrm http)	Сбор списка групп и членов групп Windows по протоколу winrm http	Группы
Группы и их члены powershell (basic) (winrm https)	Сбор списка групп и членов групп Windows по протоколу winrm https	Группы
Группы и их члены powershell (winrm http)	Сбор списка групп и членов групп Windows по протоколу winrm http	Группы
Группы и их члены powershell (winrm https)	Сбор списка групп и членов групп Windows по протоколу winrm https	Группы

Табл. 184. Python-скрипты для сбора данных ОС Windows

НАИМЕНОВАНИЕ	ОПИСАНИЕ	
Доверенные сертификаты (basic) (winrm http)	Сканер для сбора списка доверенных сертификатов на машине по протоколу winrm http	Сертификаты
Доверенные сертификаты (basic) (winrm https)	Сканер для сбора списка доверенных сертификатов на машине по протоколу winrm https	Сертификаты
Доверенные сертификаты (winexe 0.8)	Сканер для сбора списка доверенных сертификатов на машине по протоколу winexe 0.8	Сертификаты
Доверенные сертификаты (winexe 1.0)	Сканер для сбора списка доверенных сертификатов на машине по протоколу winexe 1.0	Сертификаты
Доверенные сертификаты (winrm http)	Сканер для сбора списка доверенных сертификатов на машине по протоколу winrm http	Сертификаты
Доверенные сертификаты (winrm https)	Сканер для сбора списка доверенных сертификатов на машине по протоколу winrm https	Сертификаты
Долгие/бесконечные пароли (basic) (winrm http)	Сканер для сбора паролей, до смены которых осталось больше 120 дней по протоколу winrm http	Журнал паролей
Долгие/бесконечные пароли (basic) (winrm https)	Сканер для сбора паролей, до смены которых осталось больше 120 дней по протоколу winrm https	Журнал паролей
Долгие/бесконечные пароли (winexe 0.8)	Сканер для сбора паролей, до смены которых осталось больше 120 дней по протоколу winexe 0.8	Журнал паролей
Долгие/бесконечные пароли (winexe 1.0)	Сканер для сбора паролей, до смены которых осталось больше 120 дней по протоколу winexe 1.0	Журнал паролей
Долгие/бесконечные пароли (winrm http)	Сканер для сбора паролей, до смены которых осталось больше 120 дней по протоколу winrm http	Журнал паролей
Долгие/бесконечные пароли (winrm https)	Сканер для сбора паролей, до смены которых осталось больше 120 дней по протоколу winrm https	Журнал паролей
Значимые события Security (mseven) cp866	Сбор значимых событий журнала Security по протоколу mseven	События
Значимые события System (mseven) cp866	Сбор значимых событий журнала System по протоколу mseven	События
Контрольные суммы файлов (basic) (winrm http)	Сканер для вычисления контрольных сумм файлов (ОС после XP) по протоколу winrm http	Контрольные суммы

Табл. 184. Python-скрипты для сбора данных ОС Windows

НАИМЕНОВАНИЕ	ОПИСАНИЕ	
Контрольные суммы файлов (basic) (winrm https)	Сканер для вычисления контрольных сумм файлов (ОС после XP) по протоколу winrm https	Контрольные суммы
Контрольные суммы файлов (winexe 0.8)	Сканер для вычисления контрольных сумм файлов (ОС после XP) по протоколу winexe 0.8	Контрольные суммы
Контрольные суммы файлов (winexe 1.0)	Сканер для вычисления контрольных сумм файлов (ОС после XP) по протоколу winexe 1.0	Контрольные суммы
Контрольные суммы файлов (winrm http)	Сканер для вычисления контрольных сумм файлов (ОС после XP) по протоколу winrm http	Контрольные суммы
Контрольные суммы файлов (winrm https)	Сканер для вычисления контрольных сумм файлов (ОС после XP) по протоколу winrm https	Контрольные суммы
Конфигурация KES (basic) (winrm http)	Сбор конфигурации Kaspersky Endpoint Security по протоколу winrm http	Конфигурации
Конфигурация KES (basic) (winrm https)	Сбор конфигурации Kaspersky Endpoint Security по протоколу winrm https	Конфигурации
Конфигурация KES (winexe 0.8)	Сбор конфигурации Kaspersky Endpoint Security по протоколу winexe 0.8	Конфигурации
Конфигурация KES (winexe 1.0)	Сбор конфигурации Kaspersky Endpoint Security по протоколу winexe 1.0	Конфигурации
Конфигурация KES (winrm http)	Сбор конфигурации Kaspersky Endpoint Security по протоколу winrm http	Конфигурации
Конфигурация KES (winrm https)	Сбор конфигурации Kaspersky Endpoint Security по протоколу winrm https	Конфигурации
Локальная политика безопасности (basic) (winrm http)	Сканер для сбора локальной политики безопасности по протоколу winrm http	Политика безопасности
Локальная политика безопасности (basic) (winrm https)	Сканер для сбора локальной политики безопасности по протоколу winrm https	Политика безопасности
Локальная политика безопасности (winexe 0.8)	Сканер для сбора локальной политики безопасности по протоколу winexe 0.8	Политика безопасности

Табл. 184. Python-скрипты для сбора данных ОС Windows

НАИМЕНОВАНИЕ	ОПИСАНИЕ	
Локальная политика безопасности (winexe 1.0)	Сканер для сбора локальной политики безопасности по протоколу winexe 1.0	Политика безопасности
Локальная политика безопасности (winrm http)	Сканер для сбора локальной политики безопасности по протоколу winrm http	Политика безопасности
Локальная политика безопасности (winrm https)	Сканер для сбора локальной политики безопасности по протоколу winrm https	Политика безопасности
Наименование актива (basic) (winrm http)	Сканер для сбора имени хоста по протоколу winrm http	Имя сетевого узла
Наименование актива (basic) (winrm https)	Сканер для сбора имени хоста по протоколу winrm https	Имя сетевого узла
Наименование актива (winexe 0.8)	Сканер для сбора имени хоста по протоколу winexe 0.8	Имя сетевого узла
Наименование актива (winexe 1.0)	Сканер для сбора имени хоста по протоколу winexe 1.0	Имя сетевого узла
Наименование актива (winrm http)	Сканер для сбора имени хоста по протоколу winrm http	Имя сетевого узла
Наименование актива (winrm https)	Сканер для сбора имени хоста по протоколу winrm https	Имя сетевого узла
Неактивные аккаунты (basic) (winrm http)	Сканер для сбора списка пользователей, неактивных 30 и более дней по протоколу winrm http	Пользователи
Неактивные аккаунты (basic) (winrm https)	Сканер для сбора списка пользователей, неактивных 30 и более дней по протоколу winrm https	Пользователи
Неактивные аккаунты (winexe 0.8)	Сканер для сбора списка пользователей, неактивных 30 и более дней по протоколу winexe 0.8	Пользователи
Неактивные аккаунты (winexe 1.0)	Сканер для сбора списка пользователей, неактивных 30 и более дней по протоколу winexe 1.0	Пользователи
Неактивные аккаунты (winrm http)	Сканер для сбора списка пользователей, неактивных 30 и более дней по протоколу winrm http	Пользователи
Неактивные аккаунты (winrm https)	Сканер для сбора списка пользователей, неактивных 30 и более дней по протоколу winrm https	Пользователи

Табл. 184. Python-скрипты для сбора данных ОС Windows

НАИМЕНОВАНИЕ	ОПИСАНИЕ	
Общие файловые ресурсы (basic) (winrm http)	Сканер для сбора общих файловых ресурсов через net share по протоколу winrm http	Общие файловые ресур
Общие файловые ресурсы (basic) (winrm https)	Сканер для сбора общих файловых ресурсов через net share по протоколу winrm https	Общие файловые ресур
Общие файловые ресурсы без системных (basic) (winrm http)	Сканер для сбора общих файловых ресурсов через net share по протоколу winrm http	Общие файловые ресур
Общие файловые ресурсы без системных (basic) (winrm https)	Сканер для сбора общих файловых ресурсов через net share по протоколу winrm https	Общие файловые ресур
Общие файловые ресурсы (winexe 0.8)	Сканер для сбора общих файловых ресурсов через net share по протоколу winexe 0.8	Общие файловые ресур
Общие файловые ресурсы (winexe 1.0)	Сканер для сбора общих файловых ресурсов через net share по протоколу winexe 1.0	Общие файловые ресур
Общие файловые ресурсы (winrm http)	Сканер для сбора общих файловых ресурсов через net share по протоколу winrm http	Общие файловые ресур
Общие файловые ресурсы (winrm https)	Сканер для сбора общих файловых ресурсов через net share по протоколу winrm https	Общие файловые ресур
Общие файловые ресурсы без системных (winrm https)	Сканер для сбора общих файловых ресурсов через net share по протоколу winrm https	Общие файловые ресур
Общие файловые ресурсы без системных (winexe 0.8)	Сканер для сбора общих файловых ресурсов через net share по протоколу winexe 0.8	Общие файловые ресур
Общие файловые ресурсы без системных (winexe 1.0)	Сканер для сбора общих файловых ресурсов через net share по протоколу winexe 1.0	Общие файловые ресур
Общие файловые ресурсы без системных (winrm http)	Сканер для сбора общих файловых ресурсов через net share по протоколу winrm http	Общие файловые ресур
Объекты автозапуска (basic) (winrm http)	Сканер для сбора объектов автозапуска по протоколу winrm http	Объекты автозапуска
Объекты автозапуска (basic) (winrm https)	Сканер для сбора объектов автозапуска по протоколу winrm https	Объекты автозапуска

Табл. 184. Python-скрипты для сбора данных ОС Windows

НАИМЕНОВАНИЕ	ОПИСАНИЕ	
Объекты автозапуска (winexe 0.8)	Сканер для сбора объектов автозапуска по протоколу winexe 0.8	Объекты автозапуска
Объекты автозапуска (winexe 1.0)	Сканер для сбора объектов автозапуска по протоколу winexe 1.0	Объекты автозапуска
Объекты автозапуска (winrm http)	Сканер для сбора объектов автозапуска по протоколу winrm http	Объекты автозапуска
Объекты автозапуска (winrm https)	Сканер для сбора объектов автозапуска по протоколу winrm https	Объекты автозапуска
Объекты автозапуска (wmi)	Сканер для сбора объектов автозапуска по wmi	Объекты автозапуска
Объекты автозапуска powershell (basic) (winrm http)	Сканер для сбора объектов автозапуска по протоколу winrm http	Объекты автозапуска
Объекты автозапуска powershell (basic) (winrm https)	Сканер для сбора объектов автозапуска по протоколу winrm https	Объекты автозапуска
Объекты автозапуска powershell (winrm http)	Сканер для сбора объектов автозапуска по протоколу winrm http	Объекты автозапуска
Объекты автозапуска powershell (winrm https)	Сканер для сбора объектов автозапуска по протоколу winrm https	Объекты автозапуска
Параметры сетевых интерфейсов (basic) (winrm http)	Сканер для сбора параметров ipconfig /all (кодировка 866) по протоколу winrm http	Сетевые интерфейсы
Параметры сетевых интерфейсов (basic) (winrm https)	Сканер для сбора параметров ipconfig /all (кодировка 866) по протоколу winrm https	Сетевые интерфейсы
Параметры сетевых интерфейсов (winexe 0.8)	Сканер для сбора параметров ipconfig /all (кодировка 866) по протоколу winexe 0.8	Сетевые интерфейсы
Параметры сетевых интерфейсов (winexe 1.0)	Сканер для сбора параметров ipconfig /all (кодировка 866) по протоколу winexe 1.0	Сетевые интерфейсы
Параметры сетевых интерфейсов (winrm http)	Сканер для сбора параметров ipconfig /all (кодировка 866) по протоколу winrm http	Сетевые интерфейсы
Параметры сетевых интерфейсов (winrm https)	Сканер для сбора параметров ipconfig /all (кодировка 866) по протоколу winrm https	Сетевые интерфейсы

Табл. 184. Python-скрипты для сбора данных ОС Windows

НАИМЕНОВАНИЕ	ОПИСАНИЕ	
Параметры сетевых интерфейсов XP (basic) (winrm http)	Сканер для сбора параметров Windows XP ipconfig /all (кодировка 1251) по протоколу winrm http	Сетевые интерфейсы
Параметры сетевых интерфейсов XP (basic) (winrm https)	Сканер для сбора параметров Windows XP ipconfig /all (кодировка 1251) по протоколу winrm https	Сетевые интерфейсы
Параметры сетевых интерфейсов XP (winexe 0.8)	Сканер для сбора параметров Windows XP ipconfig /all (кодировка 1251) по протоколу winexe 0.8	Сетевые интерфейсы
Параметры сетевых интерфейсов XP (winexe 1.0)	Сканер для сбора параметров Windows XP ipconfig /all (кодировка 1251) по протоколу winexe 1.0	Сетевые интерфейсы
Параметры сетевых интерфейсов XP (winrm http)	Сканер для сбора параметров Windows XP ipconfig /all (кодировка 1251) по протоколу winrm http	Сетевые интерфейсы
Параметры сетевых интерфейсов XP (winrm https)	Сканер для сбора параметров Windows XP ipconfig /all (кодировка 1251) по протоколу winrm https	Сетевые интерфейсы
Планировщик задач (basic) (winrm http)	Сканер для сбора планировщика задач Windows по протоколу winrm http	Задачи
Планировщик задач (basic) (winrm https)	Сканер для сбора планировщика задач Windows по протоколу winrm https	Задачи
Планировщик задач (winexe 0.8)	Сканер для сбора планировщика задач Windows по протоколу winexe 0.8	Задачи
Планировщик задач (winexe 1.0)	Сканер для сбора планировщика задач Windows по протоколу winexe 1.0	Задачи
Планировщик задач (winrm http)	Сканер для сбора планировщика задач Windows по протоколу winrm http	Задачи
Планировщик задач (winrm https)	Сканер для сбора планировщика задач Windows по протоколу winrm https	Задачи
Права на файлы и папки до XP (basic) (winrm http)	Сканер для сбора прав на файлы и папки cacls (ОС до XP включительно) по протоколу winrm http	Права на объекты
Права на файлы и папки до XP (basic) (winrm https)	Сканер для сбора прав на файлы и папки cacls (ОС до XP включительно) по протоколу winrm https	Права на объекты

Табл. 184. Python-скрипты для сбора данных ОС Windows

НАИМЕНОВАНИЕ	ОПИСАНИЕ	
Права на файлы и папки после XP (basic) (winrm http)	Сканер для сбора прав на файлы и папки icacls (ОС после XP) по протоколу winrm http	Права на объекты
Права на файлы и папки после XP (basic) (winrm https)	Сканер для сбора прав на файлы и папки icacls (ОС после XP) по протоколу winrm https	Права на объекты
Права на файлы и папки до XP (winexe 0.8)	Сканер для сбора прав на файлы и папки cacls (ОС до XP включительно) по протоколу winexe 0.8	Права на объекты
Права на файлы и папки до XP (winexe 1.0)	Сканер для сбора прав на файлы и папки cacls (ОС до XP включительно) по протоколу winexe 1.0	Права на объекты
Права на файлы и папки до XP (winrm http)	Сканер для сбора прав на файлы и папки cacls (ОС до XP включительно) по протоколу winrm http	Права на объекты
Права на файлы и папки до XP (winrm https)	Сканер для сбора прав на файлы и папки cacls (ОС до XP включительно) по протоколу winrm https	Права на объекты
Права на файлы и папки после XP (winexe 0.8)	Сканер для сбора прав на файлы и папки icacls (ОС после XP) по протоколу winexe 0.8	Права на объекты
Права на файлы и папки после XP (winexe 1.0)	Сканер для сбора прав на файлы и папки icacls (ОС после XP) по протоколу winexe 1.0	Права на объекты
Права на файлы и папки после XP (winrm http)	Сканер для сбора прав на файлы и папки icacls (ОС после XP) по протоколу winrm http	Права на объекты
Права на файлы и папки после XP (winrm https)	Сканер для сбора прав на файлы и папки icacls (ОС после XP) по протоколу winrm https	Права на объекты
Правила МЭ (basic) (winrm http)	Сканер для сбора правил межсетевого экрана для ОС после Windows XP по протоколу winrm http	Правила межсетевого э
Правила МЭ (basic) (winrm https)	Сканер для сбора правил межсетевого экрана для ОС после Windows XP по протоколу winrm https	Правила межсетевого э
Правила МЭ (winexe 0.8)	Сканер для сбора правил межсетевого экрана для ОС после Windows XP по протоколу winexe 0.8	Правила межсетевого э
Правила МЭ (winexe 1.0)	Сканер для сбора правил межсетевого экрана для ОС после Windows XP по протоколу winexe 1.0	Правила межсетевого э
Правила МЭ (winrm http)	Сканер для сбора правил межсетевого экрана для ОС после Windows XP по протоколу winrm http	Правила межсетевого э

Табл. 184. Python-скрипты для сбора данных ОС Windows

НАИМЕНОВАНИЕ	ОПИСАНИЕ	
Правила МЭ (winrm https)	Сканер для сбора правил межсетевого экрана для ОС после Windows XP по протоколу winrm https	Правила межсетевого э
Правила МЭ PS (winrm http)	Сканер для сбора правил межсетевого экрана для ОС после Windows XP по протоколу winrm http	Правила межсетевого э
Правила МЭ PS (winrm https)	Сканер для сбора правил межсетевого экрана для ОС после Windows XP по протоколу winrm https	Правила межсетевого э
Правила МЭ XP (basic) (winrm http)	Сканер для сбора правил межсетевого экрана для ОС Windows XP по протоколу winrm http	Правила межсетевого э
Правила МЭ XP (basic) (winrm https)	Сканер для сбора правил межсетевого экрана для ОС Windows XP по протоколу winrm https	Правила межсетевого э
Правила МЭ XP (winexe 0.8)	Сканер для сбора правил межсетевого экрана для ОС Windows XP по протоколу winexe 0.8	Правила межсетевого э
Правила МЭ XP (winexe 1.0)	Сканер для сбора правил межсетевого экрана для ОС Windows XP по протоколу winexe 1.0	Правила межсетевого э
Правила МЭ XP (winrm http)	Сканер для сбора правил межсетевого экрана для ОС Windows XP по протоколу winrm http	Правила межсетевого э
Правила МЭ XP (winrm https)	Сканер для сбора правил межсетевого экрана для ОС Windows XP по протоколу winrm https	Правила межсетевого э
Проверка обновлений KES (basic) (winrm http)	Сканер для сбора времени запуска обновлений KES по протоколу winrm http	Обновления ПО
Проверка обновлений KES (basic) (winrm https)	Сканер для сбора времени запуска обновлений KES по протоколу winrm https	Обновления ПО
Проверка обновлений KES (winexe 0.8)	Сканер для сбора времени запуска обновлений KES по протоколу winexe 0.8	Обновления ПО
Проверка обновлений KES (winexe 1.0)	Сканер для сбора времени запуска обновлений KES по протоколу winexe 1.0	Обновления ПО
Проверка обновлений KES (winrm http)	Сканер для сбора времени запуска обновлений KES по протоколу winrm http	Обновления ПО
Проверка обновлений KES (winrm https)	Сканер для сбора времени запуска обновлений KES по протоколу winrm https	Обновления ПО

Табл. 184. Python-скрипты для сбора данных ОС Windows

НАИМЕНОВАНИЕ	ОПИСАНИЕ	
Расширенная политика аудита (basic) (winrm http)	Сканер для сбора расширенной политики аудита по протоколу winrm http	Политика аудита
Расширенная политика аудита (basic) (winrm https)	Сканер для сбора расширенной политики аудита по протоколу winrm https	Политика аудита
Расширенная политика аудита (winexe 0.8)	Сканер для сбора расширенной политики аудита по протоколу winexe 0.8	Политика аудита
Расширенная политика аудита (winexe 1.0)	Сканер для сбора расширенной политики аудита по протоколу winexe 1.0	Политика аудита
Расширенная политика аудита (winrm http)	Сканер для сбора расширенной политики аудита по протоколу winrm http	Политика аудита
Расширенная политика аудита (winrm https)	Сканер для сбора расширенной политики аудита по протоколу winrm https	Политика аудита
Сетевые порты в режиме Listening (basic) (winrm http)	Сканер для сбора открытых портов Windows по протоколу winrm http	Порты
Сетевые порты в режиме Listening (basic) (winrm https)	Сканер для сбора открытых портов Windows по протоколу winrm https	Порты
Сетевые порты в режиме Listening (winexe 0.8)	Сканер для сбора открытых портов Windows по протоколу winexe 0.8	Порты
Сетевые порты в режиме Listening (winexe 1.0)	Сканер для сбора открытых портов Windows по протоколу winexe 1.0	Порты
Сетевые порты в режиме Listening (winrm http)	Сканер для сбора открытых портов Windows по протоколу winrm http	Порты
Сетевые порты в режиме Listening (winrm https)	Сканер для сбора открытых портов Windows по протоколу winrm https	Порты
Сканер для сбора компонентов Windows (winrm http)	Сбор компонентов Windows по протоколу winrm http	Компоненты ОС
Сканер для сбора компонентов Windows (winrm https)	Сбор компонентов Windows по протоколу winrm https	Компоненты ОС

Табл. 184. Python-скрипты для сбора данных ОС Windows

НАИМЕНОВАНИЕ	ОПИСАНИЕ	
Службы с автоматическим типом запуска (basic) (winrm https)	Сканер для сбора списка служб с автоматическим типом запуска по протоколу winrm https	Службы
Службы с автоматическим типом запуска (winrm https)	Сканер для сбора списка служб с автоматическим типом запуска по протоколу winrm https	Службы
Службы с автоматическим типом запуска (basic) (winrm http)	Сканер для сбора списка служб с автоматическим типом запуска по протоколу winrm http	Службы
Службы с автоматическим типом запуска (winexe 0.8)	Сканер для сбора списка служб с автоматическим типом запуска по протоколу winexe 0.8	Службы
Службы с автоматическим типом запуска (winexe 1.0)	Сканер для сбора списка служб с автоматическим типом запуска по протоколу winexe 1.0	Службы
Службы с автоматическим типом запуска (winrm http)	Сканер для сбора списка служб с автоматическим типом запуска по протоколу winrm http	Службы
Службы с автоматическим типом запуска (wmi)	Сканер для сбора списка служб с автоматическим типом запуска по протоколу wmi	Службы
Службы с автоматическим типом запуска Powershell (basic) (winrm http)	Сканер для сбора списка служб с автоматическим типом запуска по протоколу winrm http	Службы
Службы с автоматическим типом запуска Powershell (basic) (winrm https)	Сканер для сбора списка служб с автоматическим типом запуска по протоколу winrm https	Службы
Службы с автоматическим типом запуска Powershell (winrm http)	Сканер для сбора списка служб с автоматическим типом запуска по протоколу winrm http	Службы
Службы с автоматическим типом запуска Powershell (winrm https)	Сканер для сбора списка служб с автоматическим типом запуска по протоколу winrm https	Службы
События Windows (Application)	Сбор журнала событий Application по протоколу mseven	События
События Windows (Application) - XP и старше	Сбор журнала событий Application по протоколу mseven	События

Табл. 184. Python-скрипты для сбора данных ОС Windows

НАИМЕНОВАНИЕ	ОПИСАНИЕ	
События Windows (KES) winrm http	Сбор журнала событий KES по протоколу winrm http	События
События Windows (KES) winrm https	Сбор журнала событий KES по протоколу winrm https	События
События Windows (KSC) winrm http	Сбор журнала событий KSC по протоколу winrm http	События
События Windows (KSC) winrm https	Сбор журнала событий KSC по протоколу winrm https	События
События Windows (Kaspersky)	Сбор журнала событий Kaspersky по протоколу mseven	События
События Windows (Kaspersky) - XP и старше	Сбор журнала событий KES по протоколу mseven	События
События Windows (Security)	Сбор журнала событий Security по протоколу mseven	События
События Windows (Security) - XP и старше	Сбор журнала событий Security по протоколу mseven	События
События Windows (System)	Сбор журнала событий System по протоколу mseven	События
События Windows (System) - XP и старше	Сбор журнала событий System по протоколу mseven	События
События Windows (application) winrm http	Сбор журнала событий Application по протоколу winrm http	События
События Windows (application) winrm https	Сбор журнала событий Application по протоколу winrm https	События
События Windows (basic) (KES) winrm http	Сбор журнала событий KES по протоколу winrm http	События
События Windows (basic) (KES) winrm https	Сбор журнала событий KES по протоколу winrm https	События
События Windows (basic) (KSC) winrm http	Сбор журнала событий KSC по протоколу winrm http	События
События Windows (basic) (KSC) winrm https	Сбор журнала событий KSC по протоколу winrm https	События

Табл. 184. Python-скрипты для сбора данных ОС Windows

НАИМЕНОВАНИЕ	ОПИСАНИЕ	
События Windows (basic) (application) winrm http	Сбор журнала событий Application по протоколу winrm http	События
События Windows (basic) (application) winrm https	Сбор журнала событий Application по протоколу winrm https	События
События Windows (basic) (printservice/admin) winrm http	Сбор журнала событий Printservice/Admin по протоколу winrm http	События
События Windows (basic) (printservice/ admin) winrm https	Сбор журнала событий Printservice/Admin по протоколу winrm https	События
События Windows (basic) (printsrv/ operational) winrm http	Сбор журнала событий Printservice/Operational по протоколу winrm http	События
События Windows (basic) (printsrv/ operational) winrm https	Сбор журнала событий Printservice/Operational по протоколу winrm https	События
События Windows (basic) (security) winrm http	Сбор журнала событий Security по протоколу winrm http	События
События Windows (basic) (security) winrm https	Сбор журнала событий Security по протоколу winrm https	События
События Windows (basic) (system) winrm http	Сбор журнала событий System по протоколу winrm http	События
События Windows (basic) (system) winrm https	Сбор журнала событий System по протоколу winrm https	События
События Windows (printservice/admin) winrm http	Сбор журнала событий Printservice/Admin по протоколу winrm http	События
События Windows (printservice/ admin) winrm https	Сбор журнала событий Printservice/Admin по протоколу winrm https	События
События Windows (printsrv/ operational) winrm http	Сбор журнала событий Printservice/Operational по протоколу winrm http	События

Табл. 184. Python-скрипты для сбора данных ОС Windows

НАИМЕНОВАНИЕ	ОПИСАНИЕ	
События Windows (printsrv/operational) winrm https	Сбор журнала событий Printservice/Operational по протоколу winrm https	События
События Windows (security) winrm http	Сбор журнала событий Security по протоколу winrm http	События
События Windows (security) winrm https	Сбор журнала событий Security по протоколу winrm https	События
События Windows (system) winrm http	Сбор журнала событий System по протоколу winrm http	События
События Windows (system) winrm https	Сбор журнала событий System по протоколу winrm https	События
События Windows Application (mseven6)	Сбор журнала событий Application по протоколу mseven6	События
События Windows KES (mseven6)	Сбор журнала событий KES по протоколу mseven6	События
События Windows KSC (mseven6)	Сбор журнала событий KSC по протоколу mseven6	События
События Windows Print-Service_Admin (mseven6)	Сбор журнала событий PrintService_Admin по протоколу mseven6	События
События Windows Print-Service_Operational (mseven6)	Сбор журнала событий PrintService_Operational по протоколу mseven6	События
События Windows Security (mseven6)	Сбор журнала событий Security по протоколу mseven6	События
События Windows System (mseven6)	Сбор журнала событий System по протоколу mseven6	События
Состояние МЭ (basic) (winrm http)	Сканер для сбора статуса межсетевого экрана по протоколу winrm http	Состояние межсетевог
Состояние МЭ (basic) (winrm https)	Сканер для сбора статуса межсетевого экрана по протоколу winrm https	Состояние межсетевог
Состояние МЭ (winexe 0.8)	Сканер для сбора статуса межсетевого экрана по протоколу winexe 0.8	Состояние межсетевог

Табл. 184. Python-скрипты для сбора данных ОС Windows

НАИМЕНОВАНИЕ	ОПИСАНИЕ	
Состояние МЭ (winexe 1.0)	Сканер для сбора статуса межсетевого экрана по протоколу winexe 1.0	Состояние межсетевог
Состояние МЭ (winrm http)	Сканер для сбора статуса межсетевого экрана по протоколу winrm http	Состояние межсетевог
Состояние МЭ (winrm https)	Сканер для сбора статуса межсетевого экрана по протоколу winrm https	Состояние межсетевог
Состояние МЭ XP (basic) (winrm http)	Сканер для сбора статуса межсетевого экрана по протоколу winrm http	Состояние межсетевог
Состояние МЭ XP (basic) (winrm https)	Сканер для сбора статуса межсетевого экрана по протоколу winrm https	Состояние межсетевог
Состояние МЭ XP (winexe 0.8)	Сканер для сбора статуса межсетевого экрана по протоколу winexe 0.8	Состояние межсетевог
Состояние МЭ XP (winexe 1.0)	Сканер для сбора статуса межсетевого экрана по протоколу winexe 1.0	Состояние межсетевог
Состояние МЭ XP (winrm http)	Сканер для сбора статуса межсетевого экрана по протоколу winrm http	Состояние межсетевог
Состояние МЭ XP (winrm https)	Сканер для сбора статуса межсетевого экрана по протоколу winrm https	Состояние межсетевог
Список групп (basic) (winrm http)	Сбор списка групп Windows по протоколу winrm http	Группы
Список групп (basic) (winrm https)	Сбор списка групп Windows по протоколу winrm https	Группы
Список групп (winexe 0.8)	Сбор списка групп Windows по протоколу winexe 0.8	Группы
Список групп (winexe 1.0)	Сбор списка групп Windows по протоколу winexe 1.0	Группы
Список групп (winrm http)	Сбор списка групп Windows по протоколу winrm http	Группы
Список групп (winrm https)	Сбор списка групп Windows по протоколу winrm https	Группы
Список групп (wmi)	Сбор списка групп Windows по протоколу wmi	Группы
Список групп win2000 (wmi)	Сканер для сбора списка групп Windows 2000 по протоколу wmi	Группы

Табл. 184. Python-скрипты для сбора данных ОС Windows

НАИМЕНОВАНИЕ	ОПИСАНИЕ	
Список групп powershell (basic) (winrm http)	Сбор списка групп Windows по протоколу winrm https	Группы
Список групп powershell (basic) (winrm https)	Сбор списка групп Windows по протоколу winrm https	Группы
Список групп powershell (winrm http)	Сбор списка групп Windows по протоколу winrm http	Группы
Список групп powershell (winrm https)	Сбор списка групп Windows по протоколу winrm https	Группы
Список локальных групп (basic) (winrm http)	Сбор списка локальных групп Windows по протоколу winrm http	Группы
Список локальных групп (basic) (winrm https)	Сбор списка локальных групп Windows по протоколу winrm https	Группы
Список локальных групп (winexe 0.8)	Сбор списка локальных групп Windows по протоколу winexe 0.8	Группы
Список локальных групп (winexe 1.0)	Сбор списка локальных групп Windows по протоколу winexe 1.0	Группы
Список локальных групп (winrm http)	Сбор списка локальных групп Windows по протоколу winrm http	Группы
Список локальных групп (winrm https)	Сбор списка локальных групп Windows по протоколу winrm https	Группы
Список локальных групп (wmi)	Сбор списка локальных групп Windows по протоколу wmi	Группы
Список локальных групп powershell (basic) (winrm http)	Сбор списка локальных групп Windows по протоколу winrm http	Группы
Список локальных групп powershell (basic) (winrm https)	Сбор списка локальных групп Windows по протоколу winrm https	Группы
Список локальных групп powershell (winrm http)	Сбор списка локальных групп Windows по протоколу winrm http	Группы
Список локальных групп powershell (winrm https)	Сбор списка локальных групп Windows по протоколу winrm https	Группы

Табл. 184. Python-скрипты для сбора данных ОС Windows

НАИМЕНОВАНИЕ	ОПИСАНИЕ	
Список локальных пользователей (basic) (winrm http)	Сбор списка локальных пользователей Windows по протоколу winrm http	Пользователи
Список локальных пользователей (basic) (winrm https)	Сбор списка локальных пользователей Windows по протоколу winrm https	Пользователи
Список локальных пользователей (winexe 0.8)	Сбор списка локальных пользователей Windows по протоколу winexe 0.8	Пользователи
Список локальных пользователей (winexe 1.0)	Сбор списка локальных пользователей Windows по протоколу winexe 1.0	Пользователи
Список локальных пользователей (winrm http)	Сбор списка локальных пользователей Windows по протоколу winrm http	Пользователи
Список локальных пользователей Win10 (winrm http)	Сбор списка локальных пользователей Windows (Win10 only) по протоколу winrm http	Пользователи
Список локальных пользователей (winrm https)	Сбор списка локальных пользователей Windows по протоколу winrm https	Пользователи
Список локальных пользователей Win10 (winrm https)	Сбор списка локальных пользователей Windows (Win10 only) по протоколу winrm https	Пользователи
Список локальных пользователей (wmi)	Сбор списка локальных пользователей Windows по протоколу wmi	Пользователи
Список локальных пользователей powershell (basic) (winrm http)	Сбор списка локальных пользователей Windows по протоколу winrm http	Пользователи
Список локальных пользователей powershell (basic) (winrm https)	Сбор списка локальных пользователей Windows по протоколу winrm https	Пользователи
Список локальных пользователей powershell (winrm http)	Сбор списка локальных пользователей Windows по протоколу winrm http	Пользователи
Список локальных пользователей powershell (winrm https)	Сбор списка локальных пользователей Windows по протоколу winrm https	Пользователи

Табл. 184. Python-скрипты для сбора данных ОС Windows

НАИМЕНОВАНИЕ	ОПИСАНИЕ	
Список пользователей (basic) (winrm http)	Сбор списка пользователей Windows по протоколу winrm http	Пользователи
Список пользователей (basic) (winrm https)	Сбор списка пользователей Windows по протоколу winrm https	Пользователи
Список пользователей (winexe 0.8)	Сбор списка пользователей Windows по протоколу winexe 0.8	Пользователи
Список пользователей (winexe 1.0)	Сбор списка пользователей Windows по протоколу winexe 1.0	Пользователи
Список пользователей (winrm http)	Сбор списка пользователей Windows по протоколу winrm http	Пользователи
Список пользователей (winrm https)	Сбор списка пользователей Windows по протоколу winrm https	Пользователи
Список пользователей (wmi)	Сбор списка пользователей Windows по протоколу wmi	Пользователи
Список пользователей win2000 (wmi)	Сканер для сбора списка пользователей Windows 2000 по протоколу wmi	Пользователи
Список пользователей powershell (basic) (winrm http)	Сбор списка пользователей Windows по протоколу winrm http	Пользователи
Список пользователей powershell (basic) (winrm https)	Сбор списка пользователей Windows по протоколу winrm https	Пользователи
Список пользователей powershell (winrm http)	Сканер для сбора списка пользователей Windows по протоколу winrm http	Пользователи
Список пользователей powershell (winrm https)	Сбор списка пользователей Windows по протоколу winrm https	Пользователи
Список пользователей и их группы (basic) (winrm http)	Сбор списка пользователей и их групп по протоколу winrm http	Пользователи
Список пользователей и их группы (basic) (winrm https)	Сбор списка пользователей и их групп по протоколу winrm https	Пользователи
Список пользователей и их группы (winrm http)	Сбор списка пользователей и их групп по протоколу winrm http	Пользователи

Табл. 184. Python-скрипты для сбора данных ОС Windows

НАИМЕНОВАНИЕ	ОПИСАНИЕ	
Список пользователей и их группы (winrm https)	Сбор списка пользователей и их групп по протоколу winrm https	Пользователи
Список пользователей и их группы (wmi)	Сбор списка пользователей и их групп по протоколу wmi	Пользователи
Список пользователей и их группы win2000 (wmi)	Сканер для сбора списка пользователей и их групп Windows 2000 по протоколу wmi	Пользователи
Список пользователей и их группы PS (basic) (winrm http)	Сбор списка пользователей и их групп по протоколу winrm http	Пользователи
Список пользователей и их группы PS (basic) (winrm https)	Сбор списка пользователей и их групп по протоколу winrm https	Пользователи
Список пользователей и их группы PS (winrm http)	Сбор списка пользователей и их групп по протоколу winrm http	Пользователи
Список пользователей и их группы PS (winrm https)	Сбор списка пользователей и их групп по протоколу winrm https	Пользователи
Список процессов (basic) (winrm http)	Список процессов Windows по протоколу winrm http	Процессы
Список процессов (basic) (winrm https)	Список процессов Windows по протоколу winrm https	Процессы
Список процессов (winexe 0.8)	Список процессов Windows по протоколу winexe 0.8	Процессы
Список процессов (nodiff) (winexe 0.8)	Список процессов Windows по протоколу winexe 0.8	Процессы
Список процессов (winexe 1.0)	Список процессов Windows по протоколу winexe 1.0	Процессы
Список процессов (nodiff) (winexe 1.0)	Список процессов Windows по протоколу winexe 1.0	Процессы
Список процессов (winrm http)	Список процессов Windows по протоколу winrm http	Процессы
Список процессов (nodiff) (winrm http)	Список процессов Windows по протоколу winrm http	Процессы
Список процессов (winrm https)	Список процессов Windows по протоколу winrm https	Процессы

Табл. 184. Python-скрипты для сбора данных ОС Windows

НАИМЕНОВАНИЕ	ОПИСАНИЕ	
Список процессов (nodiff) (winrm https)	Список процессов Windows по протоколу winrm https	Процессы
Список процессов (wmi)	Список процессов Windows по протоколу wmi	Процессы
Список процессов (nodiff) (wmi)	Список процессов Windows по протоколу wmi	Процессы
Список процессов без PID (wmi)	Список процессов Windows без PID по протоколу wmi	Процессы
Список процессов без PID (nodiff) (wmi)	Список процессов Windows без PID по протоколу wmi	Процессы
Список устройств (basic) (winrm http)	Сбор списка устройств Windows по протоколу winrm http	Устройства
Список устройств (basic) (winrm https)	Сбор списка устройств Windows по протоколу winrm https	Устройства
Список устройств (winexe 0.8)	Сбор списка устройств Windows по протоколу winexe 0.8	Устройства
Список устройств (winexe 1.0)	Сбор списка устройств Windows по протоколу winexe 1.0	Устройства
Список устройств (winrm http)	Сбор списка устройств Windows по протоколу winrm http	Устройства
Список устройств (winrm https)	Сбор списка устройств Windows по протоколу winrm https	Устройства
Список устройств (wmi)	Сбор списка устройств Windows по протоколу wmi	Устройства
Список устройств powershell (basic) (winrm http)	Сбор списка устройств Windows по протоколу winrm http	Устройства
Список устройств powershell (basic) (winrm https)	Сбор списка устройств Windows по протоколу winrm https	Устройства
Список устройств powershell (winrm http)	Сбор списка устройств Windows по протоколу winrm http	Устройства
Список устройств powershell (winrm https)	Сбор списка устройств Windows по протоколу winrm https	Устройства

Табл. 184. Python-скрипты для сбора данных ОС Windows

НАИМЕНОВАНИЕ	ОПИСАНИЕ	
Статус системы DEP (basic) (winrm http)	Сканер для сбора статуса DEP (Data execution prevention) системы Windows по протоколу winrm http	Статус системы
Статус системы DEP (basic) (winrm https)	Сканер для сбора статуса DEP (Data execution prevention) системы Windows по протоколу winrm https	Статус системы
Статус системы DEP (winexe 0.8)	Сканер для сбора статуса DEP (Data execution prevention) системы Windows по протоколу winexe 0.8	Статус системы
Статус системы DEP (winexe 1.0)	Сканер для сбора статуса DEP (Data execution prevention) системы Windows по протоколу winexe 1.0	Статус системы
Статус системы DEP (winrm http)	Сканер для сбора статуса DEP (Data execution prevention) системы Windows по протоколу winrm http	Статус системы
Статус системы DEP (winrm https)	Сканер для сбора статуса DEP (Data execution prevention) системы Windows по протоколу winrm https	Статус системы
Таблица маршрутизации (basic) (winrm http)	Сканер для сбора таблицы маршрутизации Windows по протоколу winrm http	Таблица маршрутизаци
Таблица маршрутизации (basic) (winrm https)	Сканер для сбора таблицы маршрутизации Windows по протоколу winrm https	Таблица маршрутизаци
Таблица маршрутизации (winexe 0.8)	Сканер для сбора таблицы маршрутизации Windows по протоколу winexe 0.8	Таблица маршрутизаци
Таблица маршрутизации (winexe 1.0)	Сканер для сбора таблицы маршрутизации Windows по протоколу winexe 1.0	Таблица маршрутизаци
Таблица маршрутизации (winrm http)	Сканер для сбора таблицы маршрутизации Windows по протоколу winrm http	Таблица маршрутизаци
Таблица маршрутизации (winrm https)	Сканер для сбора таблицы маршрутизации Windows по протоколу winrm https	Таблица маршрутизаци
Установленное ПО (basic) (winrm http)	Сканер для сбора установленного ПО x64 Windows по протоколу winrm http	Установленное ПО
Установленное ПО (basic) (winrm https)	Сканер для сбора установленного ПО x64 Windows по протоколу winrm https	Установленное ПО
Установленное ПО (winexe 0.8)	Сканер для сбора установленного ПО x64 Windows по протоколу winexe 0.8	Установленное ПО

Табл. 184. Python-скрипты для сбора данных ОС Windows

НАИМЕНОВАНИЕ	ОПИСАНИЕ	
Установленное ПО (winexe 1.0)	Сканер для сбора установленного ПО x64 Windows по протоколу winexe 1.0	Установленное ПО
Установленное ПО (winrm http)	Сканер для сбора установленного ПО x64 Windows по протоколу winrm http	Установленное ПО
Установленное ПО (winrm https)	Сканер для сбора установленного ПО x64 Windows по протоколу winrm https	Установленное ПО
Установленное ПО Windows Installer (basic) (winrm http)	Сканер для сбора установленного ПО x64 Windows Installer по протоколу winrm http	Установленное ПО
Установленное ПО Windows Installer (basic) (winrm https)	Сканер для сбора установленного ПО x64 Windows Installer по протоколу winrm https	Установленное ПО
Установленное ПО Windows Installer (winrm http)	Сканер для сбора установленного ПО x64 Windows Installer по протоколу winrm http	Установленное ПО
Установленное ПО Windows Installer (winrm https)	Сканер для сбора установленного ПО x64 Windows Installer по протоколу winrm https	Установленное ПО
Установленное ПО Windows Installer (wmi)	Сканер для сбора установленного ПО x64 Windows Installer по протоколу wmi	Установленное ПО
Установленное ПО Windows Installer powershell (basic) (winrm http)	Сканер для сбора установленного ПО x64 Windows Installer по протоколу winrm http	Установленное ПО
Установленное ПО Windows Installer powershell (basic) (winrm https)	Сканер для сбора установленного ПО x64 Windows Installer по протоколу winrm https	Установленное ПО
Установленное ПО Windows Installer powershell (winrm http)	Сканер для сбора установленного ПО x64 Windows Installer по протоколу winrm http	Установленное ПО
Установленное ПО Windows Installer powershell (winrm https)	Сканер для сбора установленного ПО x64 Windows Installer по протоколу winrm https	Установленное ПО
Установленное ПО x32 (basic) (winrm http)	Сканер для сбора установленного ПО x32 Windows по протоколу winrm http	Установленное ПО
Установленное ПО x32 (basic) (winrm https)	Сканер для сбора установленного ПО x32 Windows по протоколу winrm https	Установленное ПО

Табл. 184. Python-скрипты для сбора данных ОС Windows

НАИМЕНОВАНИЕ	ОПИСАНИЕ	
Установленное ПО x32 (winexe 0.8)	Сканер для сбора установленного ПО x32 Windows по протоколу winexe 0.8	Установленное ПО
Установленное ПО x32 (winexe 1.0)	Сканер для сбора установленного ПО x32 Windows по протоколу winexe 1.0	Установленное ПО
Установленное ПО x32 (winrm http)	Сканер для сбора установленного ПО x32 Windows по протоколу winrm http	Установленное ПО
Установленное ПО x32 (winrm https)	Сканер для сбора установленного ПО x32 Windows по протоколу winrm https	Установленное ПО
Установленные обновления Windows (basic) (winrm http)	Сканер для сбора установленных обновлений Windows по протоколу winrm http	Обновления ОС
Установленные обновления Windows (basic) (winrm https)	Сканер для сбора установленных обновлений Windows по протоколу winrm https	Обновления ОС
Установленные обновления Windows (winexe 0.8)	Сканер для сбора установленных обновлений Windows по протоколу winexe 0.8	Обновления ОС
Установленные обновления Windows (winexe 1.0)	Сканер для сбора установленных обновлений Windows по протоколу winexe 1.0	Обновления ОС
Установленные обновления Windows (winrm http)	Сканер для сбора установленных обновлений Windows по протоколу winrm http	Обновления ОС
Установленные обновления Windows (winrm https)	Сканер для сбора установленных обновлений Windows по протоколу winrm https	Обновления ОС
Установленные обновления Windows (wmi)	Сканер для сбора установленных обновлений Windows по протоколу wmi	Обновления ОС
Файл hosts (basic) (winrm http)	Сканер для сбора файла hosts Windows по протоколу winrm http	Файл hosts
Файл hosts (basic) (winrm https)	Сканер для сбора файла hosts Windows по протоколу winrm https	Файл hosts
Файл hosts (winexe 0.8)	Сканер для сбора файла hosts Windows по протоколу winexe 0.8	Файл hosts
Файл hosts (winexe 1.0)	Сканер для сбора файла hosts Windows по протоколу winexe 1.0	Файл hosts
Файл hosts (winrm http)	Сканер для сбора файла hosts Windows по протоколу winrm http	Файл hosts

Табл. 184. Python-скрипты для сбора данных ОС Windows

НАИМЕНОВАНИЕ	ОПИСАНИЕ	
Файл hosts (winrm https)	Сканер для сбора файла hosts Windows по протоколу winrm https	Файл hosts
Читатели журнала событий (basic) (winrm http)	Сканер для сбора списка пользователей, имеющих доступ к журналам Windows по протоколу winrm http	Пользователи
Читатели журнала событий (basic) (winrm https)	Сканер для сбора списка пользователей, имеющих доступ к журналам Windows по протоколу winrm https	Пользователи
Читатели журнала событий (winexe 0.8)	Сканер для сбора списка пользователей, имеющих доступ к журналам Windows по протоколу winexe 0.8	Пользователи
Читатели журнала событий (winexe 1.0)	Сканер для сбора списка пользователей, имеющих доступ к журналам Windows по протоколу winexe 1.0	Пользователи
Читатели журнала событий (winrm http)	Сканер для сбора списка пользователей, имеющих доступ к журналам Windows по протоколу winrm http	Пользователи
Читатели журнала событий (winrm https)	Сканер для сбора списка пользователей, имеющих доступ к журналам Windows по протоколу winrm https	Пользователи

Табл. 185. Python-скрипты для сбора данных ОС Windows CC

НАИМЕНОВАНИЕ	ОПИСАНИЕ	
WinCC6 Группы (SQL, noport)	Сканер для сбора списка групп WINCC 6 по протоколу MS SQL (no port)	Группы
WinCC6 Конфи-гурация (SQL, noport)	Сканер для сбора конфигурации WINCC 6 по протоколу MS SQL (no port)	Конфигурации
WinCC6 Пользо-ватели (SQL, noport)	Сканер для сбора списка пользователей WINCC 6 по протоколу MS SQL (no port)	Пользователи
WinCC6 Права групп (SQL, noport)	Сканер для сбора прав групп WINCC 6 по протоколу MS SQL (no port)	Права групп
WinCC6 Права пользо-вателей (SQL, noport)	Сканер для сбора прав пользователей WINCC 6 по протоколу MS SQL (no port)	Права пользователей
Авторизация WinCC7 (SQL)	Сканер для сбора списка событий авторизации WINCC 7 по протоколу MS SQL	События
Авторизация WinCC7 (SQL, noport)	Сканер для сбора списка событий авторизации WINCC 7 по протоколу MS SQL (no port)	События

Табл. 185. Python-скрипты для сбора данных ОС Windows CC

НАИМЕНОВАНИЕ	ОПИСАНИЕ	
WinCC7-группы (SQL)	Сканер для сбора списка групп WINCC 7 по протоколу MS SQL	Группы
WinCC7-группы (SQL, noport)	Сканер для сбора списка групп WINCC 7 по протоколу MS SQL (no port)	Группы
События запуска/ останова WinCC7 (winexe)	Сканер для сбора списка событий запуска и останова WINCC 7 по протоколу winexe	События
События запуска/останова WinCC7 (winrm/http)	Сканер для сбора списка событий запуска и останова WINCC 7 по протоколу winrm/http	События
События запуска/останова WinCC7 (winrm/https)	Сканер для сбора списка событий запуска и останова WINCC 7 по протоколу winrm/https	События
WinCC7-конфигурация (SQL)	Сканер для сбора списка конфигураций WINCC 7 по протоколу MS SQL	Конфигурации
WinCC7-конфи- гурация (SQL, noport)	Сканер для сбора списка конфигураций WINCC 7 по протоколу MS SQL (noport)	Конфигурации
WinCC7-пользователи (SQL)	Сканер для сбора списка пользователей WINCC 7 по протоколу MS SQL	Пользователи
WinCC7-пользо- ватели (SQL, noport)	Сканер для сбора списка пользователей WINCC 7 по протоколу MS SQL (noport)	Пользователи
WinCC7-права групп (SQL)	Сканер для сбора списка прав групп WINCC 7 по протоколу MS SQL	Права групп
WinCC7-права групп (SQL, noport)	Сканер для сбора списка прав групп WINCC 7 по протоколу MS SQL (noport)	Права групп
WinCC7-права поль- зователей (SQL)	Сканер для сбора списка прав пользователей WINCC 7 по протоколу MS SQL	Права пользователей
WinCC7-права пользо- вателей (SQL, noport)	Сканер для сбора списка прав пользователей WINCC 7 по протоколу MS SQL (noport)	Права пользователей
Проверка настроек проекта визуализации, реализованного на ПО Siemens WinCC (winrm http)	Сканер для проверки настроек проекта визуализации WinCC, реализованного на ПО Siemens по протоколу winrm http	Настройки ПО

Табл. 185. Python-скрипты для сбора данных ОС Windows CC

НАИМЕНОВАНИЕ	ОПИСАНИЕ	
Проверка настроек проекта визуализации, реализованного на ПО Siemens WinCC (winrm https)	Сканер для проверки настроек проекта визуализации WinCC, реализованного на ПО Siemens по протоколу winrm https	Настройки ПО

Табл. 186. Python-скрипты для инвентаризации объектов Windows

НАИМЕНОВАНИЕ	ОПИСАНИЕ	
ECI_WIN_DEVICES (winrm http)	Сканер для сбора списка устройств Windows по протоколу winrm http	Устройства
ECI_WIN_DEVICES (winrm https)	Сканер для сбора списка устройств Windows по протоколу winrm https	Устройства
ECI_WIN_DEVICES (wmi)	Сканер для сбора списка устройств Windows по протоколу wmi	Устройства
ECI_WIN_DEVICES_-CDROM (winexe 0.8)	Сканер для сбора списка CD-ROM'ов Windows по протоколу winexe 0.8	CD-ROM
ECI_WIN_DEVICES_-CDROM (winrm http)	Сканер для сбора списка CD-ROM'ов Windows по протоколу winrm http	CD-ROM
ECI_WIN_DEVICES_-CDROM (winrm https)	Сканер для сбора списка CD-ROM'ов Windows по протоколу winrm https	CD-ROM
ECI_WIN_DEVICES_-CDROM (wmi)	Сканер для сбора списка CD-ROM'ов Windows по протоколу wmi	CD-ROM
ECI_WIN_DEVICES_-CPU (winexe 0.8)	Сканер для сбора списка процессоров Windows по протоколу winexe 0.8	
ECI_WIN_DEVICES_-CPU (winrm http)	Сканер для сбора списка процессоров Windows по протоколу winrm http	
ECI_WIN_DEVICES_-CPU (winrm https)	Сканер для сбора списка процессоров Windows по протоколу winrm https	
ECI_WIN_DEVICES_CPU (wmi)	Сканер для сбора списка процессоров Windows по протоколу wmi	
ECI_WIN_DEVICES_-HDD (winexe 0.8)	Сканер для сбора списка физических дисков Windows по протоколу winexe 0.8	Процессоры

Табл. 186. Python-скрипты для инвентаризации объектов Windows

НАИМЕНОВАНИЕ	ОПИСАНИЕ	
ECI_WIN_DEVICES_-HDD (winrm http)	Сканер для сбора списка физических дисков Windows по протоколу winrm http	Процессоры
ECI_WIN_DEVICES_-HDD (winrm https)	Сканер для сбора списка физических дисков Windows по протоколу winrm https	Процессоры
ECI_WIN_DEVICES_HDD (wmi)	Сканер для сбора списка физических дисков Windows по протоколу wmi	Процессоры
ECI_WIN_DEVICES_-LAN (winexe 0.8)	Сканер для сбора списка сетевых адаптеров Windows по протоколу winexe 0.8	Диски
ECI_WIN_DEVICES_-LAN (winrm http)	Сканер для сбора списка сетевых адаптеров Windows по протоколу winrm http	Сетевые адаптеры
ECI_WIN_DEVICES_-LAN (winrm https)	Сканер для сбора списка сетевых адаптеров Windows по протоколу winrm https	Сетевые адаптеры
ECI_WIN_DEVICES_LAN (wmi)	Сканер для сбора списка сетевых адаптеров Windows по протоколу wmi	Сетевые адаптеры
ECI_WIN_DEVICES_-MB (winexe 0.8)	Сканер для сбора списка материнских плат Windows по протоколу winexe 0.8	Материнские платы
ECI_WIN_DEVICES_-MB (winrm http)	Сканер для сбора списка материнских плат Windows по протоколу winrm http	Материнские платы
ECI_WIN_DEVICES_-MB (winrm https)	Сканер для сбора списка материнских плат Windows по протоколу winrm https	Материнские платы
ECI_WIN_DEVICES_MB (wmi)	Сканер для сбора списка материнских плат Windows по протоколу wmi	Материнские платы
ECI_WIN_DEVICES_-RAM (winexe 0.8)	Сканер для сбора списка физической памяти Windows по протоколу winexe 0.8	Физическая память
ECI_WIN_DEVICES_-RAM (winrm http)	Сканер для сбора списка физической памяти Windows по протоколу winrm http	Физическая память
ECI_WIN_DEVICES_-RAM (winrm https)	Сканер для сбора списка физической памяти Windows по протоколу winrm https	Физическая память
ECI_WIN_DEVICES_RAM (wmi)	Сканер для сбора списка физической памяти Windows по протоколу wmi	Физическая память

Табл. 186. Python-скрипты для инвентаризации объектов Windows

НАИМЕНОВАНИЕ	ОПИСАНИЕ	
ECI_WIN_DEVICES_-VIDEO (winexe 0.8)	Сканер для сбора списка видеоадаптеров Windows по протоколу winexe 0.8	Видеоадаптеры
ECI_WIN_DEVICES_-VIDEO (winrm http)	Сканер для сбора списка видеоадаптеров Windows по протоколу winrm http	Видеоадаптеры
ECI_WIN_DEVICES_-VIDEO (winrm https)	Сканер для сбора списка видеоадаптеров Windows по протоколу winrm https	Видеоадаптеры
ECI_WIN_DEVICES_VIDEO (wmi)	Сканер для сбора списка видеоадаптеров Windows по протоколу wmi	Видеоадаптеры
ECI_WIN_DEVICES_-VOLUME (winexe 0.8)	Сканер для сбора списка логических дисков Windows по протоколу winexe 0.8	Логические диски
ECI_WIN_DEVICES_-VOLUME (winrm http)	Сканер для сбора списка логических дисков Windows по протоколу winrm http	Логические диски
ECI_WIN_DEVICES_-VOLUME (winrm https)	Сканер для сбора списка логических дисков Windows по протоколу winrm https	Логические диски
ECI_WIN_DEVICES_-VOLUME (wmi)	Сканер для сбора списка логических дисков Windows по протоколу wmi	Логические диски
ECI_WIN_INVENTORY (winexe 0.8)	Сканер для сбора информации о системе Windows по протоколу winexe 0.8	Информация об ОС
ECI_WIN_INVENTORY (winrm http)	Сканер для сбора информации о системе Windows по протоколу winrm http	Информация об ОС
ECI_WIN_INVENTORY (winrm https)	Сканер для сбора информации о системе Windows по протоколу winrm https	Информация об ОС
ECI_WIN_PROGRAMS PS (winrm http)	Сканер для сбора списка установленного ПО Windows по протоколу winrm http (PS)	Информация о ПО
ECI_WIN_PROGRAMS PS (winrm https)	Сканер для сбора списка установленного ПО Windows по протоколу winrm https (PS)	Информация о ПО
ECI_WIN_PROGRAMS WI (winrm http)	Сканер для сбора списка установленного ПО Windows по протоколу winrm http (WI)	Информация о ПО
ECI_WIN_PROGRAMS WI (winrm https)	Сканер для сбора списка установленного ПО Windows по протоколу winrm https (WI)	Информация о ПО

Табл. 186. Python-скрипты для инвентаризации объектов Windows

НАИМЕНОВАНИЕ	ОПИСАНИЕ	
ECI_WIN_PROGRAMS WI (wmi)	Сканер для сбора списка установленного ПО Windows по протоколу wmi (WI)	Информация о ПО
ECI_WIN_PROGRAMS WI PS (winrm http)	Сканер для сбора списка установленного ПО Windows по протоколу winrm http (WI+PS)	Информация о ПО
ECI_WIN_PROGRAMS WI PS (winrm https)	Сканер для сбора списка установленного ПО Windows по протоколу winrm https (WI+PS)	Информация о ПО
ECI_WIN_USERS (local, winrm http)	Сканер для сбора списка пользователей Windows по протоколу winrm http	Пользователи
ECI_WIN_USERS (local, winrm http, PS)	Сканер для сбора списка пользователей Windows по протоколу winrm http (PS)	Пользователи
ECI_WIN_USERS (local, winrm https)	Сканер для сбора списка пользователей Windows по протоколу winrm https	Пользователи
ECI_WIN_USERS (local, winrm https, PS)	Сканер для сбора списка пользователей Windows по протоколу winrm https (PS)	Пользователи
ECI_WIN_USERS (local, wmi)	Сканер для сбора списка пользователей Windows по протоколу wmi	Пользователи

Табл. 187. Python-скрипты для сбора данных о ПЛК Regul

НАИМЕНОВАНИЕ	ОПИСАНИЕ	ТИП СОБИРАЕМЫХ ДАННЫХ	ТЕГ
Конфигурация ПЛК Regul (snmp3)	Сканер для сбора информации о конфигурации ПЛК Regul по протоколу SNMPv3	Конфигурации	snmp3, auth, priv
Контрольная сумма программы ПЛК Regul (opcua)	Сканер для сбора информации о контрольной сумме ПЛК Regul по протоколу OPC UA	Контрольные суммы	opcua
Контрольная сумма программы ПЛК Regul (ftp)	Сканер для сбора информации о контрольной сумме ПЛК Regul по протоколу FTP	Контрольные суммы	ftp, program_filename

22.16. Сетевые взаимодействия Комплексов

Порты назначения указаны в формате: `[TCP или UDP] [номер порта TCP или UDP] ([протокол или сервис назначения])`

Табл. 188. Сетевые взаимодействия Комплексов

ИСТОЧНИК ТРАФИКА	ПОРТ НАЗНАЧЕНИЯ (ДЛЯ ВНЕШНИХ АКТИВОВ И СИСТЕМ ПРИВЕДЕНЫ ПОРТЫ ПО УМОЛЧАНИЮ)	УЗЕЛ НАЗНАЧЕНИЯ	НАЗНАЧЕНИЕ ТРАФИКА
UDV DATAPK уровня Sensor	TCP 135 (MSRPC) TCP 139 TCP 445 (Winexe) TCP 1024-5000 (MSRPC в Windows XP) TCP 49152-65535 (MSRPC в Windows Vista и новее) TCP 5985 TCP 5986 (WinRM) TCP 3306 (MySQL) TCP 1433 (MSSQL)	Активы на базе ОС Windows, СУБД	Взаимодействие с активом (режим опроса)
	TCP 22 (SSH) TCP 23 (Telnet)	Активы на базе ОС Unix, АСО	
	UDP 161 (SNMP) TCP 102 (S7) TCP 502 (Modbus) TCP 44818 (EthernetIP)	ПЛК	
Активы, поддержи-вающие передачу событий через	UDP 514 (Syslog 3164) UDP 515 (Syslog 5424) TCP 514 (Syslog 3164 TCP)	UDV DATAPK уровня Sensor	Пассивный сбор событий от активов

Табл. 188. Сетевые взаимодействия Комплексов

ИСТОЧНИК ТРАФИКА	ПОРТ НАЗНАЧЕНИЯ (ДЛЯ ВНЕШНИХ АКТИВОВ И СИСТЕМ ПРИВЕДЕНЫ ПОРТЫ ПО УМОЛЧАНИЮ)	УЗЕЛ НАЗНАЧЕНИЯ	НАЗНАЧЕНИЕ ТРАФИКА
стандарт syslog/SNMP-trap	TCP 515 (Syslog 5424 TCP) UDP 162 (SNMP-trap)		
UDV DATAPK уровня Sensor	TCP 16379 (redis) — синхронизация настроек TCP 19091 (prometheus) — метрики TCP 15673 (rabbitmq) — получение данных UDP 123 (если Management выступает в роли NTP-сервера для Sensor)	UDV DATAPK уровня Management	Взаимодействие уровня Sensor с уровнем Management. Инициирует соединения всегда сенсор, поэтому его действительный IP-адрес допускается скрывать по технологии NAT (SNAT). Если межсетевой экран стоит уже после SNAT, доступы к уровню Management нужно открывать с использованием виртуального адреса сенсора
UDV DATAPK уровня Sensor	TCP 20085 — получение pcap-файлов сетевого трафика	UDV DATAPK уровня Management	Получение данных с сенсора
	TCP 20044 — получение архива с файлами		
	TCP 20104 — получение данных о сетевых соединениях		
UDV DATAPK уровня Sensor	UDP 123 (NTP)	NTP-серверы	Синхронизация времени

Табл. 188. Сетевые взаимодействия Комплексов

ИСТОЧНИК ТРАФИКА	ПОРТ НАЗНАЧЕНИЯ (ДЛЯ ВНЕШНИХ АКТИВОВ И СИСТЕМ ПРИВЕДЕНЫ ПОРТЫ ПО УМОЛЧАНИЮ)	УЗЕЛ НАЗНАЧЕНИЯ	НАЗНАЧЕНИЕ ТРАФИКА
Внимание: Взаимодействие сенсора с портом `UDP 123` не требуется, если синхронизация времени настроена через UDV DATAPK уровня Management. UDV DATAPK уровня Management			
UDV DATAPK уровня Management	UDP 514 TCP 514 TCP 25 (SMTP) TCP 465 (SMTPS)	Смежная система	Отправка событий и почтовых уведомлений в смежные системы
UDV DATAPK уровня Management	TCP 389 (LDAP) или TCP 636 (LDAPS)	LDAP-сервер	Для возможности авторизации пользователей UDV DATAPK через службу каталогов
АРМ административного персонала	TCP 443 (HTTPS) TCP 22 (SSH)	UDV DATAPK уровня Management	Администрирование UDV DATAPK.

Табл. 188. Сетевые взаимодействия Комплексов

ИСТОЧНИК ТРАФИКА	ПОРТ НАЗНАЧЕНИЯ (ДЛЯ ВНЕШНИХ АКТИВОВ И СИСТЕМ ПРИВЕДЕНЫ ПОРТЫ ПО УМОЛЧАНИЮ)	УЗЕЛ НАЗНАЧЕНИЯ	НАЗНАЧЕНИЕ ТРАФИКА
			SSH — для сервисного обслуживания в терминале операционной системы
	TCP 22 (SSH)	UDV DATAPK уровня Sensor	Администрирование UDV DATAPK (сервисное обслуживание)

22.17. Поддерживаемые типы событий

В Комплексе доступны следующие типы событий:

- События, генерируемые Комплексом:
  - аутентификация (`appliance_authentication`);
  - инциденты (`incident_control`);
  - события сканирования контролируемой сети (`home_net`);
  - события управления конфигурациями активов (`host_config`);
  - события о настройке, запуске и остановке сбора данных (`host_connection`);
  - события об изменениях интерфейсов активов (`host_interface_status_changed`);
  - действия пользователей в Комплексе (`user_action_control`);
  - действия пользователей над активами (`host_user_action_detected`);
  - изменение статуса доступности актива (`availability_control`);
  - результаты проверок на соответствие требованиям ИБ (`oval_event`);
  - обнаружение неизвестного актива (`unknown_host_detected`);
  - события модуля «Контроль версий ПЛК» (`version_control`);
  - обнаружение и контроль сессий (`session_control`);
  - контроль параметров технологического процесса (`tag_control`);
  - события службы обнаружения вторжений (`ids_event`);
  - события ML Control (`ml_notice`);
  - события DPI (`dpi_notice`);
  - системные события Комплекса (`system_event`).
- События KICS4Net (`kics4net_event`)
- События Linux (`linux_event`)
- События Cisco (`cisco_event`)
- События RuggedCOM (`ruggedcom_event`)
- События Eltex (`eltex_event`)
- События FortiGate (`fortigate_event`)
- События Hirschmann (`hirschmann_event`)
- События Enterasys (`enterasys_event`)
- События Windows (`windows_event`)
- События, полученные по SNMP (`snmp_event`)
- События, полученные по Syslog (`unknown_syslog_event`)

22.17.1. Поля внутренних событий Комплекса

Общие поля для событий Комплекса

Общие поля для внутренних событий Комплекса приведены в таблице ниже. (Таблица 189. Общие поля для событий Комплекса)

Табл. 189. Общие поля для событий Комплекса

ПОЛЕ	ОПИСАНИЕ
observer_name	Сетевое имя регистратора события: актива, сенсора или Комплекса

Табл. 189. Общие поля для событий Комплекса

ПОЛЕ	ОПИСАНИЕ
observer_ip	IP-адрес регистратора события: актива, сенсора или Комплекса
event_code	Идентификатор события
event_type	Тип события

Аутентификация (appliance_authentication)

Поля для событий аутентификации в Комплексе приведены в таблице ниже (Таблица 192. Поля для событий управления конфигурациями активов).

Табл. 190. Поля для событий об аутентификации

ПОЛЕ	ОПИСАНИЕ
action	Произведенное действие. Возможны следующие варианты: `login` или `exit`
category	Категория события аутентификации Возможны следующие варианты: `success`, `failure` или `token_expired`
description	Описание события
source_ip	IP-адрес, с которого совершена попытка аутентификации
user	Имя пользователя, который выполнял попытку аутентификации

События контроля инцидентов (incident_control)

Поля для контроля инцидентов приведены в таблице ниже (Таблица 191. Поля для событий контроля инцидентов).

Табл. 191. Поля для событий контроля инцидентов

ПОЛЕ	ОПИСАНИЕ
additional_information	Служебные поля инцидента (например, наименование правила корреляции)
description	Описание выполненного действия
justification	Обоснование выполненного действия
incident_id	Идентификатор созданного или измененного инцидента
link	Все id событий, на основе которых сформирован инцидент

Табл. 191. Поля для событий контроля инцидентов

ПОЛЕ	ОПИСАНИЕ
target_ip	Все IP-адреса из событий, на основе которых сформирован инцидент Внимание: Отображаются, только если это явно указано в правилах корреляции.
target_id	Идентификатор регистратора события: актива, сенсора или Комплекса
target_hostname	Сетевое имя регистратора события: актива, сенсора или Комплекса
user	Имя пользователя, который выполнил действие
priority	Текущий приоритет созданного или измененного инцидента

События управления конфигурациями активов (host_config)

Возможны следующие изменения эталонного состояния конфигурации:

- `datapk_host_config_changed` — Нарушено эталонное состояние конфигурации;
- `datapk_reference_config_changed` — Изменено эталонное состояние конфигурации;
- `datapk_host_config_restored` — Восстановлено эталонное состояние конфигурации.

Поля для событий изменения эталонного состояния конфигурации активов приведены в таблице ниже (Таблица 192. Поля для событий управления конфигурациями активов).

Табл. 192. Поля для событий управления конфигурациями активов

ПОЛЕ	ОПИСАНИЕ
additional_information	Список изменений в конфигурации, либо обоснование изменения эталонной конфигурации
category	Категория конфигурации (совпадает с названием сканера сбора конфигурации)
description	Описывает событие изменения конфигурации актива
target_hostname	Сетевое имя актива, на котором обнаружено нарушение эталонного состояния конфигурации
user	Имя пользователя, который изменил эталонную конфигурацию

Действие пользователя (user_action_detected)

Поля для событий действий пользователя приведены в таблице ниже (Таблица 193. Поля для событий о действиях пользователя).

Табл. 193. Поля для событий о действиях пользователя

ПОЛЕ	ОПИСАНИЕ
additional_information	Обоснование действия (комментарий) и изменившееся значение
category	Результат (статус выполненного действия) например: `OK`, `cert_error`, `access_denied`
description	Описание выполненного действия
user	Пользователь Комплекса, который выполнил действие
target_hostname	Сетевое имя Комплекса
target_id	Идентификатор Комплекса

События о настройке, запуске и остановке сбора данных (host_connection)

Поля для событий о команде запуска и остановки сбора данных приведены в таблице ниже (Таблица 194. Поля для событий о подключениях к активу).

Табл. 194. Поля для событий о подключениях к активу

ПОЛЕ	ОПИСАНИЕ
additional_information	Дополнительные данные (что изменено, ошибки запуска)
description	Описание и перечень активов, для которых изменяется состояние сбора данных
observer_id	Идентификатор сенсора, выполнившего сбор данных
observer_name	Сетевое имя сенсора, выполнившего сбор данных
source_hostname	Сетевое имя сенсора, выполнившего сбор данных
source_id	Идентификатор сенсора, выполнившего сбор данных
target_hostname	Сетевое имя Комплекса, получающего команду
target_id	Идентификатор актива, с которого осуществлялся сбор данных
target_ip	IP-адрес актива, с которого осуществлялся сбор данных

Табл. 194. Поля для событий о подключениях к активу

ПОЛЕ	ОПИСАНИЕ
user	Имя пользователя, который производит действия с задачами

Обнаружение действий пользователей с активами (host_user_action_detected)

Поля для событий о действиях пользователей с активами приведены в таблице ниже (Таблица 195. Поля для событий о действиях пользователя с активом).

Табл. 195. Поля для событий о действиях пользователя с активом

ПОЛЕ	ОПИСАНИЕ
action	Произведенное действие (варианты: `create`, `change`, `change_-interface` или `delete`)
additional_information	Дополнительные данные об активе
target_ip	IP-адрес актива, с которым производят манипуляции
target_hostname	Сетевое имя актива, с которым производят манипуляции
target_mac	MAC-адрес актива, с которым производят манипуляции Внимание: MAC-адрес актива указывается заглавными буквами.

Изменение статуса доступности актива (availability_control)

Поля для событий о статусе доступности активов приведены в таблице ниже (Таблица 196. Поля для событий статуса доступности актива).

Табл. 196. Поля для событий статуса доступности актива

ПОЛЕ	ОПИСАНИЕ
description	Описание доступности интерфейса
target_ip	IP-адрес актива, у которого происходит изменение статуса доступности
target_hostname	Сетевое имя актива, у которого происходит изменение статуса доступности
target_mac	MAC-адрес актива, у которого происходит изменение статуса доступности

Табл. 196. Поля для событий статуса доступности актива

ПОЛЕ	ОПИСАНИЕ
	Внимание: MAC-адрес указывается заглавными буквами.

Результат проверок на соответствие требованиям ИБ (oval_event)

Поля для событий о проверках OVAL приведены в таблице ниже (Таблица 197. Поля для событий о результатах проверок на соответствие требованиям ИБ).

Табл. 197. Поля для событий о результатах проверок на соответствие требованиям ИБ

ПОЛЕ	ОПИСАНИЕ
action	Статус действия проверки Возможны следующие варианты: `oval_check_success` или `oval_check_error`
additional_information	Статус завершенного действия (например, «Проверка завершена») или вывод ошибки
category	Название группы OVAL-определений
description	Описание проверки на соответствие требованиям ИБ
target_ip	IP-адрес проверяемого актива
target_hostname	Сетевое имя проверяемого актива
target_mac	MAC-адрес проверяемого актива Внимание: MAC-адрес указывается заглавными буквами.
user	Имя пользователя, который производит проверку на соответствие требованиям ИБ

Обнаружение неизвестного актива (unknown_host_detected)

Поля для событий обнаружения неизвестных активов приведены в таблице ниже (Таблица 198. Поля для событий обнаружения неизвестного актива).

Табл. 198. Поля для событий обнаружения неизвестного актива

ПОЛЕ	ОПИСАНИЕ
description	Описание события
target_ip	IP-адрес обнаруженного актива
target_mac	MAC-адрес обнаруженного актива **Внимание:** MAC-адрес обнаруженного актива указывается заглавными буквами.

События службы обнаружения вторжений (ids_event)

Поля для событий службы обнаружения вторжений приведены в таблице ниже (Таблица 199. Поля для событий службы обнаружения вторжений).

Табл. 199. Поля для событий службы обнаружения вторжений

ПОЛЕ	ОПИСАНИЕ
action	Действие службы обнаружения вторжений. **Подсказка:** Берется из поля `action` правила службы обнаружения вторжений.
category	Категория события службы обнаружения вторжений. **Подсказка:** Берется из поля `event_type` правила службы обнаружения вторжений.
description	Описание правила срабатывания сигнатуры (IDS)
event_code	Значение поля `signature_id` правила службы обнаружения вторжений
protocol	Протокол срабатывания правила службы обнаружения вторжений.

Табл. 199. Поля для событий службы обнаружения вторжений

ПОЛЕ	ОПИСАНИЕ
	Подсказка: Берется из поля `app_proto` правила службы обнаружения вторжений.
source_ip	IP-адрес отправителя сетевых пакетов. Внимание: В событиях от службы обнаружения вторжений (поле `event_type` в таких событиях имеет значение `ids_event`) Комплекс может менять местами IP-адреса отправителя и получателя. Корректный адрес можно посмотреть по ссылке **Сессия** вверху карточки интересующего события на странице **События**.
source_port	Порт, по которому отправлены сетевые пакеты
target_ip	IP-адрес получателя сетевых пакетов. Внимание: В событиях от службы обнаружения вторжений (поле `event_type` в таких событиях имеет значение `ids_event`) Комплекс может менять местами IP-адреса отправителя и получателя. Корректный адрес можно посмотреть по ссылке **Сессия** вверху карточки интересующего события на странице **События**.
target_port	Порт, на который отправлены сетевые пакеты

Контроль системных событий Комплекса (event_control)

Поля для контроля событий Комплекса приведены в таблице ниже (Таблица 200. Поля для контроля событий Комплекса).

Табл. 200. Поля для контроля событий Комплекса

ПОЛЕ	ОПИСАНИЕ
description	Описание события Комплекса
protocol	Идентификатор источника
source_hostname	Сетевое имя актива

Табл. 200. Поля для контроля событий Комплекса

ПОЛЕ	ОПИСАНИЕ
source_ip	IP-адрес актива
target_hostname	Сетевое имя объекта, над которым выполнялось действие: актива, сенсора или Комплекса
target_id	ID объекта, над которым выполнялось действие: актива, сенсора или Комплекса

22.17.2. Поля событий KICS4Net

События KICS4Net (kics4net_event)

Поля для событий KICS4Net приведены в таблице ниже (Таблица 201. Поля для событий KICS4Net).

Табл. 201. Поля для событий KICS4Net

ПОЛЕ	ОПИСАНИЕ
additional_information	Название сработавшего правила или значение noTrafficDuration.
category	Наименование точки мониторинга.
description	Описание потока.
event_code	Идентификатор типа события в KICS4Net.
hostname	Сетевое имя сервера KICS4Net.
ip	IP-адрес KICS4Net.
protocol	Название протокола.
source_ip	IP-адрес источника потока данных.
source_mac	MAC-адрес источника. Внимание: MAC-адрес указывается заглавными буквами.
source_port	Порт источника потока данных.
target_ip	IP-адрес получателя потока данных.
target_mac	MAC-адрес получателя.

Табл. 201. Поля для событий KICS4Net

ПОЛЕ	ОПИСАНИЕ
	Внимание: MAC-адрес указывается заглавными буквами.
target_port	Порт получателя потока данных.

22.17.3. Поля событий Linux

Доступные для событий Linux поля приведены в таблице ниже (Таблица 202. Поля для событий Linux).

Табл. 202. Поля для событий Linux

ПОЛЕ	ОПИСАНИЕ
event_code	Уникальный идентификатор события. Представляет собой facility+severity из protocol_specific_data.
category	Название журнала или процесса Linux.
ip	IP-адрес актива.
Дополнительные поля	
description	Описание события.
protocol	Протокол, использованный в событии Linux.
source_ip	IP-адрес источника события при воздействии на Linux.
source_port	Порт источника события при воздействии на Linux.
user	Пользователь, инициировавший событие.

22.17.4. Поля событий Cisco

Доступные для событий Cisco поля приведены в таблице ниже (Таблица 203. Поля для событий Cisco).

Табл. 203. Поля для событий Cisco

ПОЛЕ	ОПИСАНИЕ
action	Произведенное действие. Содержит значение из facility_mnemonic (кроме ASA).

Табл. 203. Поля для событий Cisco

ПОЛЕ	ОПИСАНИЕ
additional_information	Развернутое значение facility (из словаря), либо название политики для firepower.
category	Категория важности события. Содержит читаемое значение severity (из словаря).
description	Описание события.
event_code	Уникальный идентификатор события. Составляется из Facility-Severity-Mnemonic.
ip	IP-адрес актива.
target_ip	IP-адрес получателя (IP-адрес Cisco или IP-адрес для SNMP).
target_port	Порт получателя или подключения.
Дополнительные поля	
protocol	Протокол событий ACL и протокол доступа событий, связанных с пользователями.
source_ip	IP-адрес источника события (при воздействии на Cisco).
source_port	Порт источника события.
hostname	Сетевое имя актива, с которого пришло событие (если включена отправка hostname на Cisco).
user	Пользователь, инициировавший событие.

22.17.5. Поля событий RuggedCOM

Доступные для событий RuggedCOM поля приведены в таблице ниже (Таблица 204. Поля для событий RuggedCOM).

Табл. 204. Поля для событий RuggedCOM

ПОЛЕ	ОПИСАНИЕ
event_code	Уникальный идентификатор события. Составляется из facility+severity из protocol_specific_data.
ip	IP-адрес актива.

Табл. 204. Поля для событий RuggedCOM

ПОЛЕ	ОПИСАНИЕ
Дополнительные поля	
user	Пользователь, инициировавший событие.

22.17.6. Поля событий Eltex

Доступные для событий поля приведены в таблице ниже (Таблица 205. Поля для событий Eltex).

Табл. 205. Поля для событий Eltex

ПОЛЕ	ОПИСАНИЕ
action	Тип выполняемого действия.
category	Группа логирования.
description	Описание события.
event_code	Идентификатор типа события, состоит из category-action.
ip	IP-адрес актива.
protocol	Протокол подключения (только в событиях подключения).
source_ip	IP-адрес источника действия.
target_ip	IP-адрес коммутатора.
user	Имя пользователя, если есть в событии.
Дополнительные поля	
additional_information	Выполненная команда. Внимание: Только для событий с фиксацией команд.

22.17.7. Поля событий FortiGate

Доступные для событий FortiGate поля приведены в таблице ниже (Таблица 206. Поля для событий FortiGate).

Табл. 206. Поля для событий FortiGate

ПОЛЕ	ОПИСАНИЕ
action	Значение поля action события.
additional_information	Поле msg или название vpn-тоннеля.
category	Тип события.
description	Описание события.
event_code	Значение поля logid.
observer_name	Сетевое имя регистратора события: актива (МЭ fortigate), сенсора или Комплекса.
observer_ip	IP-адрес регистратора события: актива (МЭ fortigate), сенсора или Комплекса.
protocol	Наименование протокола из события.
source_ip	Значение поля srcip или locip.
source_port	Значение поля srcport или locport.
target_ip	Значение поля dstip или remip.
target_port	Значение поля dstport или remport.
user	Значение поля user.

22.17.8. Поля событий Hirschmann

Доступные для событий Hirschmann поля приведены в таблице ниже (Таблица 207. Поля для событий Hirschmann).

Табл. 207. Поля для событий Hirschmann

ПОЛЕ	ОПИСАНИЕ
category	Категория (например: TRAPMGR, HM_HPL_FDB, DOT1S, UNKN).
description	Описание события.
event_code	Уникальный идентификатор события. Состоит из Facility+severity из protocol_specific_data.
ip	IP-адрес актива.

22.17.9. Поля событий Enterasys

Доступные для событий Enterasys поля приведены в таблице ниже (Таблица 208. Поля для событий Enterasys).

Табл. 208. Поля для событий Enterasys

ПОЛЕ	ОПИСАНИЕ
description	Описание события.
event_code	Уникальный идентификатор событий. Состоит из Facility +severity из protocol_specific_data.
ip	IP-адрес актива.
protocol	Протокол подключения (только в событиях подключения).
source_ip	IP-адрес источника событий.
user	Имя пользователя в событии.

22.17.10. Поля событий Windows

Доступные для событий Windows поля приведены в таблице ниже (Таблица 209. Поля для событий Windows).

Табл. 209. Поля для событий Windows

ПОЛЕ	ОПИСАНИЕ
action	Произведенное действие или категория события.
category	Название журнала событий.
description	Описание события.
event_code	Идентификатор события в журнале событий.
observer_name	Имя регистратора события: актива, сенсора или Комплекса.
observer_ip	IP-адрес регистратора события: актива, сенсора или Комплекса.
user	Пользователь, инициировавший событие.
Дополнительные поля	
additional_information	Описание события из внутренней библиотеки Комплекса в соответствии с данными от Microsoft.
source_ip	IP-адрес источника события.

Табл. 209. Поля для событий Windows

ПОЛЕ	ОПИСАНИЕ
user	Пользователь. Используется поле targetUserName из события.

22.17.11. Поля событий SNMP

Доступные для событий SNMP поля приведены в таблице ниже (Таблица 210. Поля для событий SNMP).

Табл. 210. Поля для событий SNMP

ПОЛЕ	ОПИСАНИЕ
action	Имя переменной SNMP (snmpTrapOID).
category	Ключевое слово, которое определяет имя объединения для взаимодействия (community_name).
ip	IP-адрес отправителя сообщения.
target_ip	IP-адрес актива, с которого пришло событие.

22.17.12. Поля событий Syslog

Доступные для событий Syslog поля приведены в таблице ниже (Таблица 211. Поля для событий Syslog).

Табл. 211. Поля для событий Syslog

ПОЛЕ	ОПИСАНИЕ
event_code	Уникальный идентификатор события. Используется facility+severity из protocol_specific_data.
ip	IP-адрес актива.

22.18. Синтаксис правил корреляции событий

Синтаксис языка EPL схож с SQL-запросами, и его можно описать следующим образом:

Select→ поля → из → тип события→ фильтр(опционально).

В правилах используются поля нормализованных событий — подробнее см. раздел «Нормализация событий».

Синтаксис на языке EPL на основе популярной конструкции представлен ниже:

```
SELECT [необходимые поля] FROM [тип события]([фильтр событий]).win:time([отслеживаемое время]) GROUP BY [поле для группировки событий] HAVING COUNT([поле по которому ведется счет]) = [порог для появления инцидента]
```

Описание используемых команд и функций приведено в таблице (Таблица 212. Команды, используемые в примере синтаксиса EPL).

Табл. 212. Команды, используемые в примере синтаксиса EPL

КОМАНДА	ПЕРЕВОД НАЗВАНИЯ	ОПИСАНИЕ
SELECT	Выбрать	Выбор некоторых полей для вывода информации в сообщении об инциденте, а также используются агрегирующие функции, примененные к данным полям, и метки. После оператора идут требуемые поля. **Внимание:** Для корректного функционирования правила корреляции после команды SELECT требуется обязательно указать поля, содержащие следующую семантику: • идентификаторы событий в рамках комплекса (например, `id`); • идентификатор сенсора, сформировавшего событие (например, `appliance_node_id`); • идентификаторы активов, участвующих в инциденте (например, `source_id`, `observer_id` или `target_id`).
FROM	Из	Указание источника – откуда выбирать вышеуказанные поля.
GROUP BY	Группировать по	Группировка событий по определенному полю, указанному после команды. Так, например, можно разделить события по хостам или по обнаруживающему средству, чтобы исключить ложные срабатывания правила.
HAVING	Содержит	Команда для работы с групповыми записями, которая вводит критерий отбора событий, указанный после команды.
COUNT()	Количество	Подсчитывает количество вхождений событий с указанным внутри нее полем. **Внимание:** Для корректной работы порога количества условно обнаруженных событий требуется также указать временное окно, иначе счетчик будет увеличиваться перманентно и пересечет порог единожды.
.win:time()	Время	Условие определяет временной промежуток, обозреваемый от обнаруженного по условию события.

В составлении данных запросов необходимо использовать только те поля, которые соответствуют классу события. Описание полей для разных классов приведено далее.

22.18.1. Ключевые поля событий для создания правил корреляции

Следующие поля (Таблица 213. Обязательные поля) являются обязательными при создании правила корреляции, так как данная информация необходима для создания инцидента.

Табл. 213. Обязательные поля

ПОЛЕ	ОПИСАНИЕ
observer_id	Уникальный идентификатор регистратора события: сенсора, зафиксировавшего событие, либо актива, либо Комплекса
id	Уникальный идентификатор события

22.18.2. Фильтр событий

В правилах корреляции заложена возможность установки двух параметров – условий инцидента и фильтра событий.

В данном пункте рассматривается фильтр событий. Его возможно задать после указания типа события. Указанное условие размещается в круглых скобках и должно использовать поля того типа события, которое было задано за скобками.

Пример

Например,

```
windows_event(event_code ="4625" OR event_code ="529")
```

В данном случае происходит условная фильтрация событий ресурса (типа windows_event) по идентификаторам самого ресурса.

Данное условие возможно составить, используя поля поддерживаемых типов, логические операторы и требуемые значения полей, указанные в двойных кавычках.

22.18.3. Временное окно

Для выявления инцидента, основанного на цепочке событий в течение временного диапазона, рекомендуется использовать конструкцию:

```
[тип события]([фильтр событий]).win:time([отслеживаемое время])
```

Пример

Например,

```
windows_event(event_code="4625" OR event_code="529").win:time(180 sec)
```

Поэлементно данное выражение означает следующее:

- точка «.» после описания типа событий и фильтров подразумевает использование какого-либо свойства;
- «win:» - в данном случае пространство имен обозначает «data window» или окно данных;
- «time()» - функция, принимающая значение временного диапазона окна данных, по умолчанию принимает значение в секундах.

Функция time может принимать явно указанные значения:

- дни (days или day);
- часы (hours или hour);
- минуты (min);
- секунды (sec);
- миллисекунды (msec).

Работа функции представлена на рисунке.

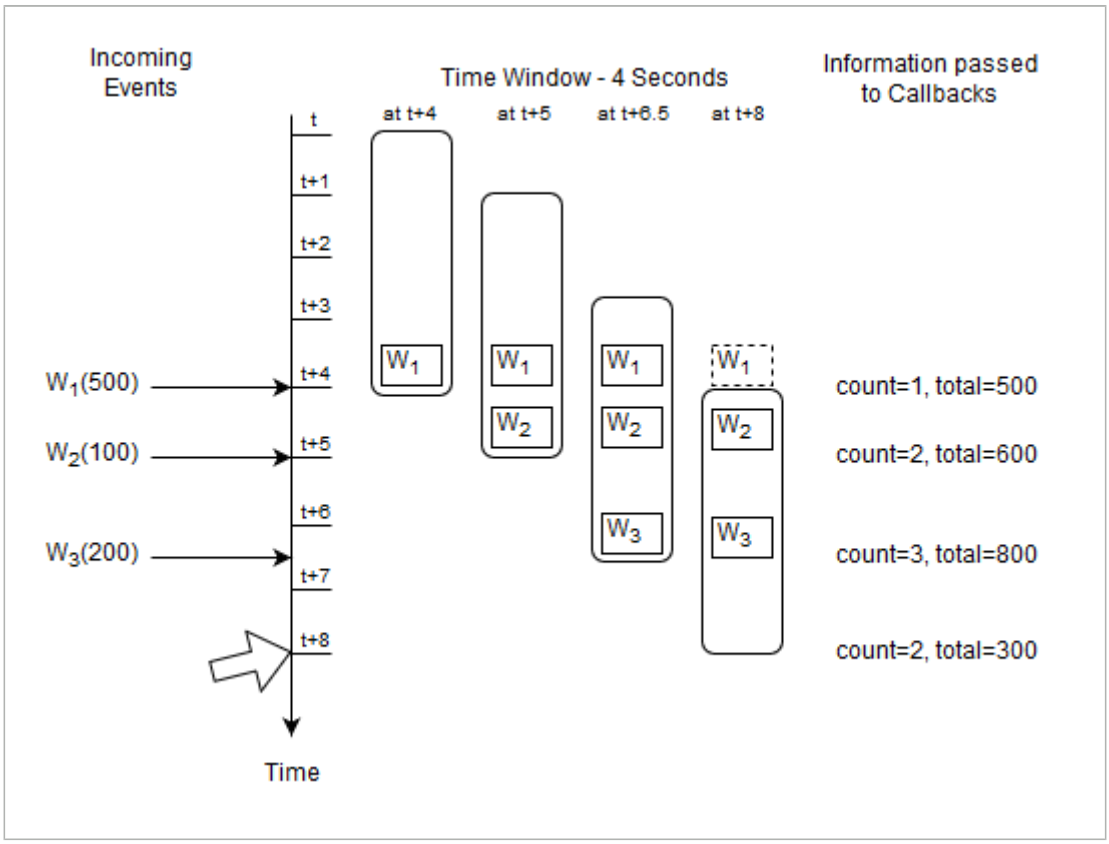


Рис. 573. Работа функции time()

На данном рисунке отображены приходящие события (Incoming Events) в виде символов «W_n», где n – номер события. По временному отрезку движется окно данных с диапазоном в 4 секунды и ведет счет полученных событий. Так, на восьмой секунде отбрасывается первое пришедшее событие, и число событий становится на единицу меньше.

22.18.4. Группировка

В связи с тем, что события бывают от разных объектов, применяют механизм группировки событий для разделения их по активам, исключая ложные срабатывания механизма корреляции.

Так, при использовании команды: `GROUP BY observer_name` несколько одинаковых событий от разных активов не будут образовывать цепочку атаки и приводить к инциденту ИБ.

Особенность данного режима заключается в дальнейшем описании условия возникновения инцидента (при его наличии). Вместо «WHERE», который применяется для описания единичных событий, используется «HAVING». Отсюда, при использовании примера, указанного выше, конструкция принимает вид:

```
GROUP BY observer_name HAVING …
```

Группировать можно только по тем полям, которые принадлежат выбранному типу событий.

22.18.5. Условие инцидента

Действия, описанные в данной части конструкции правила, вариативные. В качестве примера была отображена функция «COUNT()» и логический оператор «=».

> **Пример**
>
> Например, используя данное условие, возможно вести подсчет событий, пока их количество не превысит заданное:
>
> ```
> COUNT(event_code) = 3
> ```

Вместо данной функции можно использовать различные агрегаторы:

- Сумма значений (sum);
- Среднее значение (avg);
- Максимальное значение (max);
- Минимальное значение (min);
- Медианное значение (median);
- Стандартное отклонение значений (stddev);
- Среднее отклонение значений (avedev).

При необходимости глубокого изучения возникновения ошибок, проверки состояния службы и валидации правил в модуле корреляции возможно использовать данные log-записей сервиса `udv-esper`, используя команду, описанную в начале подраздела.

22.18.6. Шаблоны обработки сложных событий

В этом разделе:

- Команда «PATTERN»
- Оператор «EVERY»

С помощью правил корреляции можно создавать модели поведения злоумышленников. Для реализации этого существует такой инструмент, как шаблоны обработки сложных событий.

> **Пример**
>
> Пример использования шаблона:
>
> ```
> SELECT df.user, df.source_ip, df.target_ip FROM PATTERN@SuppressOverlappingMatches [EVERY df=cisco_event(df.description="Login Success" OR df.action = "LOGIN_SUCCESS") AND EVERY c=datapk_data_flow(c.action="detect" AND c.protocol="ssh" AND df.source_ip=c.source_ip)].win:time(180 sec)
> ```

Далее рассмотрим применение самого шаблона «PATTERN» и используемый оператор «EVERY».

22.18.6.1. Команда «PATTERN»

Ключевым словом «PATTERN» для модуля обозначают начало шаблона, описание которого происходит в квадратных скобках далее.

Отсюда, синтаксис для составления шаблона следующий:

```
PATTERN [[первое событие] →[второе событие] AND …]
```

Подсказка:

Оператор между событиями может быть любой из поддерживаемых языком EPL.

В качестве дополнений шаблонов могут использоваться аннотации. Полный список аннотаций представлен в справочной информации Esper.

Аннотации в шаблонах указываются сразу после ключевого слова «PATTERN» и отличаются знаком «@» в начале обозначения.

Пример

В данном случае рассмотрен пример аннотации «@SuppressOverlappingMatches», означающий подавление совпадений с одним и тем же событием.

Допустим, у нас есть последовательность событий «A_1 A_2 B_1» и правило, которое просматривает каждое совпадение событий A → B (оператор для данного правила рассмотрен ниже). Следовательно, в данном случае мы получим два срабатывания на один инцидент, что в определенной ситуации (например, большого потока событий в один момент времени) сделает оповещения неинформативными. Если же применить аннотацию «@SuppressOverlappingMatches», то в случае последовательности «A_1 A_2 B_1» произойдет одно срабатывание на инцидент ИБ.

См. также

http://esper.espertech.com/release-8.4.0/reference-esper/html_single/index.html

22.18.6.2. Оператор «EVERY»

Рассмотренное в разделе «Команда «PATTERN»» правило «каждое совпадение событий A → B» представляется возможным благодаря оператору «EVERY».

Пример

Для примера возьмем поток событий: «A_1 B_1 C_1 B_2 A_2 D_1 A_3 B_3 E_1 A_4 F_1 B_4», где буква обозначает событие, а индекс — номер события данного типа.

При написании следующей конструкции:

```
EVERY ( A → B )
```

совпадения будут в следующих комбинациях:

```
{A 1 , B 1 }; {A 2 , B 3 }; {A 4 , B 4 }
```

При конструкции:

```
EVERY A → B
```

будут комбинации:

```
{A 1 , B 1 }; {A 2 , B 3 }; {A 3 , B 3 }; {A 4 , B 4 }
```

Следующая конструкция:

```
A → EVERY B
```

выберет данные комбинации:

```
{A 1 , B 1 }; {A 1 , B 2 }; {A 1 , B 3 }; {A 1 , B 4 }
```

И при заключительном варианте:

```
EVERY A → EVERY B
```

результат будет следующим:

```
{A 1 , B 1 }; {A 1 , B 2 }; {A 1 , B 3 }; {A 2 , B 3 }; {A 3 , B 3 }; {A 1 , B 4 };
 {A 2 , B 4 }; {A 3 , B 4 }; {A 4 , B 4 }
```

22.18.7. Сообщение инцидента

При создании правила корреляции требуется обозначить текст, отображаемый оператору в случае возникновения инцидента. Чтобы сообщение было более информативным, рекомендуется индивидуализировать его посредством внесения переменных.

Переменными в сообщении могут являться только те поля, которые были «выбраны» командой `SELECT`.

Пример

Например, при указании данного правила:

```
SELECT event_code, observer_name, user, ip FROM windows_event(event_code ="4625" OR event_code
 ="529").win:time(180 sec) GROUP BY observer_name HAVING COUNT(event_code) = 3
```

возможно использование следующего сообщения оператору:

```
На активе ${observer_name} (${observer_ip}) обнаружен подбор пароля к учетной записи пользователя
 ${user}
```

В случае наименования хоста — «GasStation», IP-адреса — `192.168.0.100`, атакуемого пользователя «Администратор», по прошествии трех неудачных попыток ввода пароля оператор ИБ получит сообщение об инциденте следующего вида:

```
На активе GasStation ( 192.168.0.100) обнаружен подбор пароля к учетной записи пользователя
 Администратор
```

Для образования информативных сообщений необходимо воспользоваться следующим синтаксисом написания переменных:

```
${ [наименование выводимого поля] }
```

22.18.8. Приоритет и активность правил

Заключительным этапом в создании правила является определение критичности выявляемого инцидента и указание статуса работы правила (активно или неактивно).

Критичность выявляемого инцидента задается в поле «Приоритет» и имеет следующую градацию:

- Низкий
- Средний
- Высокий
- Очень высокий

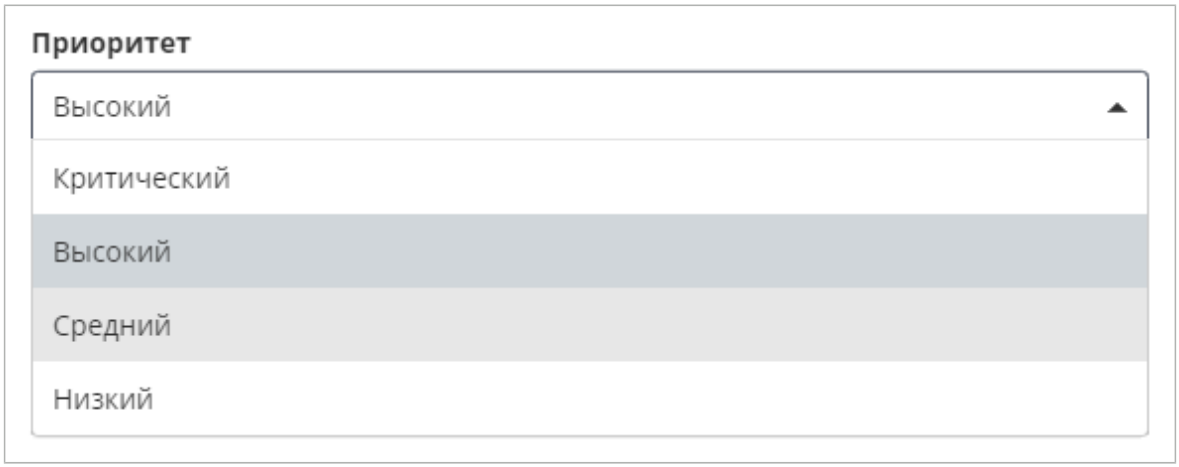


Рис. 574. Градация критичности выявляемого инцидента

Статус правила задается чекбоксами («☑») «Применять в текущем анализе» и «Применять в ретроспективном анализе».

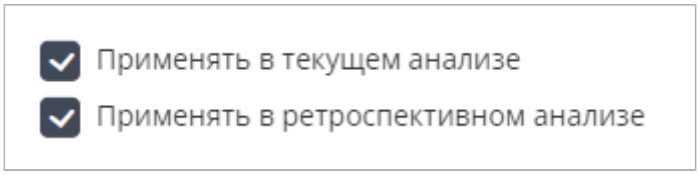


Рис. 575. Активные статусы правила корреляции

22.19. Список внутренних правил корреляции событий

Перечень внутренних правил корреляции событий представлен в таблице ниже.

Табл. 214. Внутренние правила корреляции событий

НОМЕР	НАЗВАНИЕ ПРАВИЛА	СОБЫТИЕ/ИНЦИДЕНТ, ГЕНЕРИРУЕМЫЙ ПРАВИЛОМ КОРРЕЛЯЦИИ
0001	Подбор пароля пользователя Комплекса	Подбор пароля пользователя `{user}` на Комплексе (`{appliance_node_name}`, `{observer_ip}`) с хоста `{source_-ip}`
0002	Обнаружен новый актив	Обнаружен новый актив ip: `{target_ip}`, mac: `{target_mac}`

Табл. 214. Внутренние правила корреляции событий

НОМЕР	НАЗВАНИЕ ПРАВИЛА	СОБЫТИЕ/ИНЦИДЕНТ, ГЕНЕРИРУЕМЫЙ ПРАВИЛОМ КОРРЕЛЯЦИИ
0003	Изменение конфигурации актива	На активе `{target_hostname}` изменилась конфигурация `{category}`
0004	События IDS по группам	Обнаружено `{count}` срабатываний сигнатуры `{description}`
0005	Применение эксплоита	Применение эксплоита `{description}`. Сторона 1: `{source_hostname}` (`{source_ip}`), сторона 2: `{target_hostname}` (`{target_ip}`)
0006	Обнаружена подозрительная активность, похожая на MALWARE	Подозрение на `{description}`. Сторона 1: `{source_hostname}` (`{source_ip}`), сторона 2: `{target_hostname}` (`{target_ip}`)
0007	Обнаружение EICAR	Обнаружен EICAR на активе `{target_hostname}` (`{target_ip}`) с узла `{source_hostname}` (`{source_ip}`).
0008	Обнаружена подозрительная активность, похожая на TROJAN	Подозрение на `{description}`. Сторона 1: `{source_hostname}` (`{source_ip}`), сторона 2: `{target_hostname}` (`{target_ip}`)
0009	Обнаружена подозрительная активность, похожая на WORM	Подозрение на `{description}`. Сторона 1: `{source_hostname}` (`{source_ip}`), сторона 2: `{target_hostname}` (`{target_ip}`)
0010	События IDS с высоким приоритетом с группировкой по Комплексам-источникам событий	Обнаружено `{count}` срабатываний IDS с высоким приоритетом на Комплексе `{observer_name}`

Табл. 214. Внутренние правила корреляции событий

НОМЕР	НАЗВАНИЕ ПРАВИЛА	СОБЫТИЕ/ИНЦИДЕНТ, ГЕНЕРИРУЕМЫЙ ПРАВИЛОМ КОРРЕЛЯЦИИ
0011	Получение учетных данных (Тактика: TA0006)	Обнаружена активность по тактике `{category}` от `{source_ip}` в сторону `{target_ip}`. Использована техника `{description}`. Выполнена команда `{action}` через RPC-интерфейс `{additional_information}`.
0012	Первоначальный доступ (Тактика: TA0001)	Обнаружена активность Log4J от `{source_ip}` в сторону `{target_ip}`. Использована техника `{description}`. Полезная нагрузка: `{justification}`.
0013	Исследование (Тактика: TA0007)	Обнаружена активность по тактике `{category}` от `{source_ip}`. Количество попыток 5.
0014	Предотвращение обнаружения (Тактика: TA0005)	Обнаружена активность по тактике `{category}` от `{source_ip}` в сторону `{target_ip}`. Использована техника `{description}`. Выполнена команда `{action}` через RPC-интерфейс `{additional_information}`.
0015	Перемещение внутри периметра (Тактика: TA0008). Семейство эксплойтов Eternal	Обнаружена активность по тактике `{category}` от `{source_ip}` в сторону `{target_ip}`. Использована техника `{description}`. Применен эксплоит: `{additional_information}`.
0016	Перемещение внутри периметра (Тактика: TA0008). Передача файла	Обнаружена активность по тактике `{category}` от `{source_ip}` в сторону `{target_ip}`. Передача файла `{justification}`. FUID: `{additional_information}`.

Табл. 214. Внутренние правила корреляции событий

НОМЕР	НАЗВАНИЕ ПРАВИЛА	СОБЫТИЕ/ИНЦИДЕНТ, ГЕНЕРИРУЕМЫЙ ПРАВИЛОМ КОРРЕЛЯЦИИ
		Использована техника `{description}`.
0017	Вредоносное ПО в сети	`{description}` при передаче от `{source_ip}` в сторону `{target_ip}`. Детальная информация: `{justification}`. FUID: `{additional_information}`.
0019	Выполнение (Тактика: TA0002)	Обнаружена активность по тактике `{category}` от `{source_ip}` в сторону `{target_ip}`. Использована техника `{description}`. Выполнена команда `{action}` через RPC-интерфейс `{additional_information}`.
0020	Получение учетных данных (Тактика: TA0006)	Обнаружена активность по тактике `{category}` от `{source_ip}` в сторону `{target_ip}`. Использована техника `{description}`. Украденная учетная запись: `{user}`. Получен доступ до сервиса: `{additional_information}`.
0021	Закрепление (Тактика: TA0003)	Обнаружена активность по тактике `{category}` от `{source_ip}` в сторону `{target_ip}`. Использована техника `{description}`. Выполнена команда `{action}` через RPC-интерфейс `{additional_information}`.
0022	Перемещение внутри периметра (Тактика: TA0008)	Обнаружена активность по тактике `{category}` от `{source_ip}` в сторону `{target_ip}`. Использована техника

Табл. 214. Внутренние правила корреляции событий

НОМЕР	НАЗВАНИЕ ПРАВИЛА	СОБЫТИЕ/ИНЦИДЕНТ, ГЕНЕРИРУЕМЫЙ ПРАВИЛОМ КОРРЕЛЯЦИИ
		`{additional_information}`. `{description}`.
0023	Перемещение внутри периметра (Тактика: TA0008). Множественные попытки	Обнаружена активность по тактике `{category}` от `{source_ip}`. Количество попыток 10. `{description}`.
0024	Воздействие (Тактика: TA0040)	Обнаружена активность по тактике `{category}` от `{source_ip}` в сторону `{target_ip}`. Использована техника `{description}`. Выполнена команда `{action}` через RPC-интерфейс `{additional_information}`.
0025	Управление и контроль (Тактика: TA0011)	Обнаружен DNS-туннель при запросе `{justification}` от `{source_ip}` в сторону `{target_ip}`. `{additional_information}`. Использована техника `{description}`.
0027	Разведка (Тактика: TA0043)	Обнаружена активность по тактике Разведка от `{source_ip}` в сторону `{target_ip}`. Использована техника T1595.001: Сканирование блоков IP-адресов.
0028	Разведка (Тактика: TA0043). Перебор URL Web-сервера	На активе `{source_ip}` обнаружено большое количество 404 ответов к активу `{target_ip}`. Использована техника T1595.003: Сканирование по списку слов.

См. также

Управление внутренними правилами корреляции событий

22.20. Отображение времени в Комплексе

Дата и время в Комплексе хранится во временной зоне UTC, а при отображении в интерфейсе адаптируется под часовой пояс клиента. Это позволяет пользователям просматривать события и другую информацию в своем часовом поясе.

На страницах раздела **Мониторинг** и **События** время отображается в соответствии со временем на АРМ пользователя. В случае расхождения времени между АРМ клиента и операционной системой Комплекса могут обнаруживаться несоответствия при которых события отображаются «в будущем» или «в прошлом». Такое расхождение не следует принимать за сбой работы системы регистрации событий.

Подобное поведение также наблюдается при получении событий от актива, на котором некорректно настроено время. При сортировке по полю `create_time` такое событие может отображаться «в прошлом» или «в будущем» относительно событий, полученных в то же время.

См. также

Время на Комплексе отличается от времени получения события

22.21. Структура директорий Комплекса

Список общих директорий и файлов настроек, а также их описание представлены в таблице ниже (Таблица 215. Общие директории и файлы настроек).

Табл. 215. Общие директории и файлы настроек

ДИРЕКТОРИЯ (ФАЙЛ)	НАЗНАЧЕНИЕ
`/usr/share/udv`	Основная директория Комплекса
`/usr/share/udv/scripts-certs`	Директория для хранения сертификата для верификации сканеров сбора данных
`/usr/share/udv/scripts-certs/datapk_script.crt`	Сертификат для верификации сканеров сбора данных
`/usr/share/udv/certs/ca.crt`	Корневой сертификат

Список директорий и основных файлов Комплекса уровня Management, а также их описание представлены в таблице ниже (Таблица 216. Директории и основные файлы настроек Комплекса уровня Management).

Табл. 216. Директории и основные файлы настроек Комплекса уровня Management

ДИРЕКТОРИЯ (ФАЙЛ)	НАЗНАЧЕНИЕ
`/usr/share/udv/datapk/manager.env`	Основные настройки Комплекса
`/var/cache/udv/nginx/certs`	Серверные сертификаты

Табл. 216. Директории и основные файлы настроек Комплекса уровня Management

ДИРЕКТОРИЯ (ФАЙЛ)	НАЗНАЧЕНИЕ
`/usr/share/udv/nginx`	Шаблоны `nginx`
`/usr/share/udv/frontend`	Настройки меню (интерфейса)
`/etc/logstash`	Правила нормализации
`/var/backups`	Директория для хранения резервных копий. Содержит tar-архивы с резервными копиями (`dtpk-backup-version-timestamp.tar`)
`/var/backups/elasticsearch`	Директория для хранения резервных копий событий
`/var/backups/elasticsearch/indices`	Архивированные индексы событий
`/var/backups/elasticsearch/uploads`	Индексы событий для импорта
`/usr/share/udv/vulnerability-backend`	Директория для хранения импортированного справочника ПО и уязвимостей (CPE и CVE), импортированной базы сопоставления собранного сканерами ПО со справочником CPE и отчета с последними результатами поиска уязвимостей
`/var/opt/udv`, `/var/cache/udv`	Служебные директории Комплекса

Список директорий и основных файлов Комплекса уровня Sensor, а также их описание представлены в таблице ниже (Таблица 217. Директории и основные файлы настроек Комплекса уровня Sensor).

Табл. 217. Директории и основные файлы настроек Комплекса уровня Sensor

ДИРЕКТОРИЯ (ФАЙЛ)	НАЗНАЧЕНИЕ
`/usr/share/udv/datapk/sensor.env`	Основные настройки Комплекса
`/usr/share/udv/snmp-connector/snmp_mibs`	Словари SNMP

22.22. Работа с контрольными суммами исполняемых файлов сертифицированного Комплекса

Проверка контрольных сумм исполняемых файлов Комплекса выполняется двумя способами:

- Автоматическая проверка контрольных сумм
- Ручная проверка контрольных сумм

Расположение исполняемых файлов сертифицированного Комплекса

После первичной установки и запуска сервисов Комплекса автоматически создается пустой текстовый файл `packets.txt` для дальнейшего заполнения их эталонными наборами пакетов сервисов Комплекса.

> Прим.:
>
> Эталонные наборы сервисных пакетов Комплекса и их эталонных контрольных сумм для дальнейших автоматических и ручных проверок предоставляются пользователям в комплекте дистрибутива.

В зависимости от принадлежности пакетов компонентам Комплекса эти файлы хранятся в двух директориях:

- `/usr/share/udv/datapk/checksums/management` — директория с эталонными файлами для компонента Management;
- `/usr/share/udv/datapk/checksums/sensor` — директория с эталонными файлами для компонента Sensor.

В этих директориях файлы также разделены по модулям Комплекса:

- `nta` — директория с эталонными файлами для сервисов модуля «Анализ промышленного сетевого трафика»;
- `vc` — директория с эталонными файлами для сервисов модуля «Управление проектами ПЛК»;
- `core` — директория с эталонными файлами для сервисов остальных модулей.

Для того, чтобы можно было выполнять проверки контрольных сумм исполняемых файлов, каждая такая директория должна содержать следующие текстовые файлы:

- `packets.txt` — список отслеживаемых пакетов сервиса (пустой файл создается автоматически после установки Комплекса);
- `checksums.txt` — список контрольных сумм исполняемых файлов отслеживаемых пакетов (пустой файл необходимо создать вручную для дальнейшего заполнения).

  > Прим.:
  >
  > Подробнее о подготовке эталонных файлов для дальнейшей проверки контрольных сумм см. в разделе «Создание эталонных контрольных сумм исполняемых файлов Комплекса вручную».

> Прим.:
>
> Пример содержания заполненного файла `packets.txt`:

```
python3-aio-pika-7.1.0
python3-aiohttp-apiset-0.9.15
python3-aiormq-6.2.3
```

Пример содержания заполненного файла `checksums.txt`:

```
5fea6b9e03acccadf847f495009adad9c19fa9a2c9857e1f4f4d608f84a08d32      /usr/lib/python3/site-packages/aio_pika/abc.py
cd7a4c00b489a2852def8823c7b535163dbc596edbbf9479fb90b8bf298eb6fc      /usr/lib/python3/site-packages/aio_pika/channel.py
566922cfd68b53c7fa3b45cec86015c0ffe186152cfd6a5bcbbf8ed6248fe7ad      /usr/lib/python3/site-packages/aio_pika/connection.py
```

Пример структуры хранения эталонных файлов в директории `/usr/share/udv/datapk/checksums`:

```
+-> management/
|         +-> vc/
|         |      +-> packets.txt
|         |      +-> checksums.txt
|         +-> core/
|         |       +-> packets.txt
|         |       +-> checksums.txt
|         ...
|
+-> sensor/
|         +-> core/
|         |       +-> packets.txt
|         |       +-> checksums.txt
|         ...
...
```

Пример полного пути до файлов для модуля «Управление проектами ПЛК» компонента Management:

```
/usr/share/udv/datapk/checksums/management/vc/packets.txt
/usr/share/udv/datapk/checksums/management/vc/checksums.txt
```

Автоматическая проверка контрольных сумм

По умолчанию Комплекс автоматически выполняет проверку контрольных сумм собственных исполняемых файлов. Контрольные суммы проверяются для всех модулей UDV DATAPK. Автоматическая проверка контрольных сумм выполняется после каждого запуска сервисов Комплекса.

Проверка выполняется для контрольных сумм эталонных файлов `packets.txt`и `checksums.txt`, расположенных в директории `/usr/share/udv/datapk/checksums/management` или `/usr/share/udv/datapk/checksums/sensor`, в зависимости от компонента Комплекса.

Подробнее о структуре хранения эталонных файлов см. в разделе «Расположение исполняемых файлов сертифицированного Комплекса».

После каждого запуска сервисов Комплекса автоматически запускается скрипт проверки контрольных сумм, который сверяет контрольные суммы модулей Комплекса со значениями, указанными в эталонных файлах. При наличии отклонений в контрольных суммах формируется отчет по результатам проверки. Готовый отчет хранится в директории `/var/log/` сенсора, наименование отчета — `udv-checksums_*.log`, где `*` — уровень

Комплекса (Management или Sensor). В отчете указывается директория файла, контрольные суммы которого не соответствуют эталонному значению.

После завершения проверки контрольных сумм Комплекс формирует одно из следующих событий:

- `1180032 Успешная проверка контрольных сумм исполняемых файлов: целостность файлов не нарушена`;
- `1180033 Обнаружено нарушение целостности исполняемых файлов в результате проверки их контрольных сумм`.

Ручная проверка контрольных сумм

Также пользователь может вручную выполнять расчет и проверку контрольных сумм исполняемых файлов Комплекса.

Расчет контрольных сумм выполняется в соответствии с инструкцией «Создание эталонных контрольных сумм исполняемых файлов Комплекса вручную», а проверка контрольных сумм выполняется в соответствии с инструкцией «Проверка контрольных сумм исполняемых файлов Комплекса вручную».

22.22.1. Создание эталонных контрольных сумм исполняемых файлов Комплекса вручную

В данном разделе приведена инструкция для создания эталонных контрольных сумм исполняемых файлов Комплекса, которые будут применяться для дальнейших проверок целостности исполняемых файлов. Инструкция не предназначена для расчета контрольных сумм иных файлов, в том числе файлов дистрибутива Комплекса. Инструкция предназначена для разработчиков или специалистов, выполняющих внедрение Комплекса.

> Прим.:
>
> Эталонные наборы сервисных пакетов Комплекса и их эталонных контрольных сумм для дальнейших автоматических и ручных проверок предоставляются пользователям в комплекте дистрибутива.

Для расчета эталонных контрольных сумм исполняемых файлов одного модуля выбранного компонента Комплекса:

1. Перейдите в директорию, в которой будут располагаться эталонные текстовые файлы со списком пакетов и контрольными суммами их исполняемых файлов:

   ```
   cd /usr/share/udv/datapk/checksums/[компонент]/[модуль]/
   ```

   Для параметра `[компонент]` возможны следующие значения:
   - `management` — директория с эталонными файлами для компонента Management;
   - `sensor` — директория с эталонными файлами для компонента Sensor.

   Для параметра `[модуль]` возможны следующие значения:
   - `nta` — директория с эталонными файлами для сервисов модуля «Анализ промышленного сетевого трафика»;
   - `vc` — директория с эталонными файлами для сервисов модуля «Управление проектами ПЛК»;
   - `core` — директория с эталонными файлами для сервисов остальных модулей.

> **Внимание:**
>
> Подробнее о структуре расположения файлов см. в разделе Работа с контрольными суммами исполняемых файлов сертифицированного Комплекса.

Пример

Полный путь до файлов для модуля «Управление проектами ПЛК» компонента Management:

```
/usr/share/udv/datapk/checksums/management/vc
```

2. Откройте на редактирование файл `packets.txt`:

```
mcedit packets.txt
```

3. Укажите в файле список пакетов модуля.

Пример

Содержание заполненного файла `packets.txt`:

```
python3-aio-pika-7.1.0
python3-aiohttp-apiset-0.9.15
python3-aiormq-6.2.3
```

4. Сохраните изменения в файле, нажав клавишу **F10**, и подтвердите сохранение изменений, выбрав **Yes**.
5. В той же директории создайте пустой файл `checksums.txt`:

```
touch checksums.txt
```

6. Запустите расчет контрольных сумм модуля командой:

```
udv-checksums create [компонент].[модуль]
```

Пример

команда для расчета контрольных сумм модуля `core` компонента `management`:

```
udv-checksums create management.core
```

- **Результат шага:** контрольные суммы модуля выбранного компонента будут рассчитаны и сохранены в файл `/usr/share/udv/datapk/checksums/[компонент]/[модуль]/checksums.txt`.

22.22.2. Проверка контрольных сумм исполняемых файлов Комплекса вручную

В данном разделе приведена инструкция для проверки контрольных сумм исполняемых файлов Комплекса. Инструкция не предназначена для проверки иных файлов, в том числе файлов дистрибутива Комплекса.

Перед выполнением:

Перед началом проверки убедитесь, что файлы `packets.txt` и `checksums.txt` присутствуют в директориях Комплекса. Подробнее о директориях см. в разделе «Расположение исполняемых файлов сертифицированного Комплекса».

> Прим.:
>
> Эталонные наборы сервисных пакетов Комплекса и их эталонных контрольных сумм для дальнейших автоматических и ручных проверок предоставляются пользователям в комплекте дистрибутива.

Для проверки контрольных сумм исполняемых файлов Комплекса:

1. Перейдите в директорию, в которой располагаются эталонные текстовые файлы со списком пакетов и контрольными суммами их исполняемых файлов:

   ```
   cd /usr/share/udv/datapk/checksums/[компонент]/[модуль]/
   ```

   > Внимание:
   >
   > Подробнее о структуре расположения эталонных файлов см. в разделе Работа с контрольными суммами исполняемых файлов сертифицированного Комплекса.

2. Выполните команду для проверки контрольных сумм:

   ```
   udv-checksums verify [компонент или компонент.модуль] --report-path [директория]
   ```

   где:

   - `[компонент или компонент.модуль]` — список целиком проверяемых компонентов или отдельных модулей в компонентах. Элементы списка разделяются пробелом;
   - `[директория]` — путь и название файла, в которой будет сохранен файл отчета с результатом проверки файлов. По умолчанию результат проверки сохраняется в файл `verdicts.txt` в текущую директорию.

   ▸ **Результат шага:** По завершении проверки будет создан отчет по пути `[директория]`, в котором будет отображаться список найденных и не найденных исполняемых файлов Комплекса, их текущие контрольные суммы и результат их соответствия эталонным контрольным суммам.
   Пример отчета:

   ```
   /usr/lib64/python3/site-packages/pystemd/__init__.py    CORRECT
   /usr/lib64/python3/site-packages/pystemd/__version__.py CORRECT
   /usr/lib64/python3/site-packages/pystemd/base.py    CORRECT
   ```

   Результаты могут быть следующими:

   - `ADDED` — исполняемый файл присутствует в текущем Комплексе, но не был найден в эталонном файле `checksums.txt`;
   - `REMOVED` — исполняемый файл был найден в файле `checksums.txt`, но отсутствует в текущем Комплексе;
   - `CORRECT` — исполняемый файл присутствует в Комплексе, его контрольная сумма соответствует сумме, указанной в файле `checksums.txt`;
   - `INVALID` — исполняемый файл присутствует в Комплексе, но его контрольная сумма не соответствует сумме, указанной в файле `checksums.txt`.

22.23. Справочная информация о модуле «Анализ промышленного сетевого трафика»

В этом разделе:

- Переменные файла белого списка
- Возможные состояния сессий
- Поддерживаемые протоколы передачи данных
- Поддерживаемые функции промышленных протоколов

22.23.1. Переменные файла белого списка

В Комплексе файл с белым списком `general.dat` по умолчанию находится в директории `/usr/share/udv/zeek-wrapper/configs/`

Перечень переменных, доступных для использования в нем, представлен в таблицах ниже.

Табл. 218. Переменные, используемые для DNS

ПЕРЕМЕННАЯ	ТАКТИКА АТАКИ	НАЗНАЧЕНИЕ
DNS::whitelist_names	Управление и контроль	Имена запросов и ответов
DNS::whitelist_orig_names	Управление и контроль	Имена запросов
DNS::whitelist_resp_names	Управление и контроль	Имена ответов

Табл. 219. Переменные, используемые для BZAR

ПЕРЕМЕННАЯ	ТАКТИКА АТАКИ (ЖИРНЫМ)[5] ТЕХНИКА АТАКИ	НАЗНАЧЕНИЕ
BZAR::t1003_006_whitelist_orig_-addrs	**Получение учетных данных** Получение дампа учетных данных: DCSync	IP-адреса запросов
BZAR::t1003_006_whitelist_resp_-addrs	**Получение учетных данных** Получение дампа учетных данных: DCSync	IP-адреса ответов
BZAR::t1003_006_whitelist_orig_-subnets	**Получение учетных данных** Получение дампа учетных данных: DCSync	Подсети запросов
BZAR::t1003_006_whitelist_resp_-subnets	**Получение учетных данных** Получение дампа учетных данных: DCSync	Подсети ответов
BZAR::t1003_006_whitelist_orig_-names	**Получение учетных данных** Получение дампа учетных данных: DCSync	Имена запросов

Табл. 219. Переменные, используемые для BZAR

ПЕРЕМЕННАЯ	ТАКТИКА АТАКИ (ЖИРНЫМ)[5] ТЕХНИКА АТАКИ	НАЗНАЧЕНИЕ
BZAR::t1003_006_whitelist_resp_-names	**Получение учетных данных** Получение дампа учетных данных: DCSync	Имена ответов
BZAR::t1070_001_whitelist_orig_-addrs	**Обход защиты** Удаление индикатора: Очистка журналов событий Windows	IP-адреса запросов
BZAR::t1070_001_whitelist_resp_-addrs	**Обход защиты** Удаление индикатора: Очистка журналов событий Windows	IP-адреса ответов
BZAR::t1070_001_whitelist_orig_-subnets	**Обход защиты** Удаление индикатора: Очистка журналов событий Windows	Подсети запросов
BZAR::t1070_001_whitelist_resp_-subnets	**Обход защиты** Удаление индикатора: Очистка журналов событий Windows	Подсети ответов
BZAR::t1070_001_whitelist_orig_-names	**Обход защиты** Удаление индикатора: Очистка журналов событий Windows	Имена запросов
BZAR::t1070_001_whitelist_resp_-names	**Обход защиты** Удаление индикатора: Очистка журналов событий Windows	Имена ответов
BZAR::t1569_002_whitelist_orig_-addrs	**Выполнение/эксплуатация** Диспетчер управления службами	IP-адреса запросов
BZAR::t1569_002_whitelist_resp_-addrs	**Выполнение/эксплуатация** Диспетчер управления службами	IP-адреса ответов
BZAR::t1569_002_whitelist_orig_-subnets	**Выполнение/эксплуатация** Диспетчер управления службами	Подсети запросов
BZAR::t1569_002_whitelist_resp_-subnets	**Выполнение/эксплуатация**	Подсети ответов

Табл. 219. Переменные, используемые для BZAR

ПЕРЕМЕННАЯ	ТАКТИКА АТАКИ (ЖИРНЫМ)[5] ТЕХНИКА АТАКИ	НАЗНАЧЕНИЕ
	Диспетчер управления службами	
BZAR::t1569_002_whitelist_orig_-names	**Выполнение/эксплуатация** Диспетчер управления службами	Имена запросов
BZAR::t1569_002_whitelist_resp_-names	**Выполнение/эксплуатация** Диспетчер управления службами	Имена ответов
BZAR::t1047_whitelist_orig_addrs	**Выполнение/эксплуатация** Windows Management Instrumentation	IP-адреса запросов
BZAR::t1047_whitelist_resp_addrs	**Выполнение/эксплуатация** Windows Management Instrumentation	IP-адреса ответов
BZAR::t1047_whitelist_orig_-subnets	**Выполнение/эксплуатация** Windows Management Instrumentation	Подсети запросов
BZAR::t1047_whitelist_resp_-subnets	**Выполнение/эксплуатация** Windows Management Instrumentation	Подсети ответов
BZAR::t1047_whitelist_orig_-names	**Выполнение/эксплуатация** Windows Management Instrumentation	Имена запросов
BZAR::t1047_whitelist_resp_-names	**Выполнение/эксплуатация** Windows Management Instrumentation	Имена ответов
BZAR::t1053_002_whitelist_orig_-addrs	**Выполнение/эксплуатация** Запланированная задача (задание): Утилита at (Windows)	IP-адреса запросов
BZAR::t1053_002_whitelist_resp_-addrs	**Выполнение/эксплуатация** Запланированная задача (задание): Утилита at (Windows)	IP-адреса ответов

Табл. 219. Переменные, используемые для BZAR

ПЕРЕМЕННАЯ	ТАКТИКА АТАКИ (ЖИРНЫМ)[5] ТЕХНИКА АТАКИ	НАЗНАЧЕНИЕ
BZAR::t1053_002_whitelist_orig_-subnets	**Выполнение/эксплуатация** Запланированная задача (задание): Утилита at (Windows)	Подсети запросов
BZAR::t1053_002_whitelist_resp_-subnets	**Выполнение/эксплуатация** Запланированная задача (задание): Утилита at (Windows)	Подсети ответов
BZAR::t1053_002_whitelist_orig_-names	**Выполнение/эксплуатация** Запланированная задача (задание): Утилита at (Windows)	Имена запросов
BZAR::t1053_002_whitelist_resp_-names	**Выполнение/эксплуатация** Запланированная задача (задание): Утилита at (Windows)	Имена ответов
BZAR::t1053_005_whitelist_orig_-addrs	**Выполнение/эксплуатация** Запланированная задача (задание): Планировщик заданий Windows	IP-адреса запросов
BZAR::t1053_005_whitelist_resp_-addrs	**Выполнение/эксплуатация** Запланированная задача (задание): Планировщик заданий Windows	IP-адреса ответов
BZAR::t1053_005_whitelist_orig_-subnets	**Выполнение/эксплуатация** Запланированная задача (задание): Планировщик заданий Windows	Подсети запросов
BZAR::t1053_005_whitelist_resp_-subnets	**Выполнение/эксплуатация** Запланированная задача (задание): Планировщик заданий Windows	Подсети ответов
BZAR::t1053_005_whitelist_orig_-names	**Выполнение/эксплуатация** Запланированная задача (задание): Планировщик заданий Windows	Имена запросов
BZAR::t1053_005_whitelist_resp_-names	**Выполнение/эксплуатация**	Имена ответов

Табл. 219. Переменные, используемые для BZAR

ПЕРЕМЕННАЯ	ТАКТИКА АТАКИ (ЖИРНЫМ)[5] ТЕХНИКА АТАКИ	НАЗНАЧЕНИЕ
	Запланированная задача (задание): Планировщик заданий Windows	
BZAR::t1529_whitelist_orig_addrs	**Воздействие** Завершение работы или перезагрузка системы	IP-адреса запросов
BZAR::t1529_whitelist_resp_addrs	**Воздействие** Завершение работы или перезагрузка системы	IP-адреса ответов
BZAR::t1529_whitelist_orig_-subnets	**Воздействие** Завершение работы или перезагрузка системы	Подсети запросов
BZAR::t1529_whitelist_resp_-subnets	**Воздействие** Завершение работы или перезагрузка системы	Подсети ответов
BZAR::t1529_whitelist_orig_-names	**Воздействие** Завершение работы или перезагрузка системы	Имена запросов
BZAR::t1529_whitelist_resp_-names	**Воздействие** Завершение работы или перезагрузка системы	Имена ответов
BZAR::t1021_002_t1570_-whitelist_orig_addrs	**Перемещение внутри периметра** • Общие SMB-ресурсы или ресурсы администраторов Windows • Передача инструментов внутри периметра	IP-адреса запросов
BZAR::t1021_002_t1570_-whitelist_resp_addrs	**Перемещение внутри периметра** • Общие SMB-ресурсы или ресурсы администраторов Windows	IP-адреса ответов

Табл. 219. Переменные, используемые для BZAR

ПЕРЕМЕННАЯ	ТАКТИКА АТАКИ (ЖИРНЫМ)[5] ТЕХНИКА АТАКИ	НАЗНАЧЕНИЕ
	• Передача инструментов внутри периметра	
BZAR::t1021_002_t1570_-whitelist_orig_subnets	**Перемещение внутри периметра** • Общие SMB-ресурсы или ресурсы администраторов Windows • Передача инструментов внутри периметра	Подсети запросов
BZAR::t1021_002_t1570_-whitelist_resp_subnets	**Перемещение внутри периметра** • Общие SMB-ресурсы или ресурсы администраторов Windows • Передача инструментов внутри периметра	Подсети ответов
BZAR::t1021_002_t1570_-whitelist_orig_names	**Перемещение внутри периметра** • Общие SMB-ресурсы или ресурсы администраторов Windows • Передача инструментов внутри периметра	Имена запросов
BZAR::t1021_002_t1570_-whitelist_resp_names	**Перемещение внутри периметра** • Общие SMB-ресурсы или ресурсы администраторов Windows • Передача инструментов внутри периметра	Имена ответов
BZAR::t1021_002_whitelist_orig_-addrs	**Перемещение внутри периметра** Общие SMB-ресурсы или ресурсы администраторов Windows	IP-адреса запросов

Табл. 219. Переменные, используемые для BZAR

ПЕРЕМЕННАЯ	ТАКТИКА АТАКИ (ЖИРНЫМ)[5] ТЕХНИКА АТАКИ	НАЗНАЧЕНИЕ
BZAR::t1021_002_whitelist_resp_-addrs	**Перемещение внутри периметра** Общие SMB-ресурсы или ресурсы администраторов Windows	IP-адреса ответов
BZAR::t1021_002_whitelist_orig_-subnets	**Перемещение внутри периметра** Общие SMB-ресурсы или ресурсы администраторов Windows	Подсети запросов
BZAR::t1021_002_whitelist_resp_-subnets	**Перемещение внутри периметра** Общие SMB-ресурсы или ресурсы администраторов Windows	Подсети ответов
BZAR::t1021_002_whitelist_orig_-names	**Перемещение внутри периметра** Общие SMB-ресурсы или ресурсы администраторов Windows	Имена запросов
BZAR::t1021_002_whitelist_resp_-names	**Перемещение внутри периметра** Общие SMB-ресурсы или ресурсы администраторов Windows	Имена ответов
BZAR::t1570_whitelist_orig_addrs	**Перемещение внутри периметра** Передача инструментов внутри периметра	IP-адреса запросов
BZAR::t1570_whitelist_resp_addrs	**Перемещение внутри периметра** Передача инструментов внутри периметра	IP-адреса ответов
BZAR::t1570_whitelist_orig_-subnets	**Перемещение внутри периметра** Передача инструментов внутри периметра	Подсети запросов
BZAR::t1570_whitelist_resp_-subnets	**Перемещение внутри периметра** Передача инструментов внутри периметра	Подсети ответов
BZAR::t1570_whitelist_orig_-names	**Перемещение внутри периметра**	Имена запросов

Табл. 219. Переменные, используемые для BZAR

ПЕРЕМЕННАЯ	ТАКТИКА АТАКИ (ЖИРНЫМ)[5] ТЕХНИКА АТАКИ	НАЗНАЧЕНИЕ
	Передача инструментов внутри периметра	
BZAR::t1570_whitelist_resp_-names	**Перемещение внутри периметра** Передача инструментов внутри периметра	Имена ответов
BZAR::t1021_002_multiple_-attempts_whitelist_orig_addrs	**Перемещение внутри периметра** Службы удаленного доступа: Общие SMB-ресурсы или ресурсы администраторов Windows (многократные попытки)	IP-адреса запросов
BZAR::t1021_002_multiple_-attempts_whitelist_resp_addrs	**Перемещение внутри периметра** Службы удаленного доступа: Общие SMB-ресурсы или ресурсы администраторов Windows (многократные попытки)	IP-адреса ответов
BZAR::t1021_002_multiple_-attempts_whitelist_orig_subnets	**Перемещение внутри периметра** Службы удаленного доступа: Общие SMB-ресурсы или ресурсы администраторов Windows (многократные попытки)	Подсети запросов
BZAR::t1021_002_multiple_-attempts_whitelist_resp_subnets	**Перемещение внутри периметра** Службы удаленного доступа: Общие SMB-ресурсы или ресурсы администраторов Windows (многократные попытки)	Подсети ответов
BZAR::t1021_002_multiple_-attempts_whitelist_orig_names	**Перемещение внутри периметра** Службы удаленного доступа: Общие SMB-ресурсы или ресурсы администраторов Windows (многократные попытки)	Имена запросов
BZAR::t1021_002_multiple_-attempts_whitelist_resp_names	**Перемещение внутри периметра** Службы удаленного доступа: Общие SMB-ресурсы или ресурсы админи-	Имена ответов

Табл. 219. Переменные, используемые для BZAR

ПЕРЕМЕННАЯ	ТАКТИКА АТАКИ (ЖИРНЫМ)[5] ТЕХНИКА АТАКИ	НАЗНАЧЕНИЕ
	страторов Windows (многократные попытки)	
BZAR::attack_lm_ex_whitelist_-orig_addrs	**Перемещение внутри периметра и выполнение команд**	IP-адреса запросов
BZAR::attack_lm_ex_whitelist_-resp_addrs	**Перемещение внутри периметра и выполнение команд**	IP-адреса ответов
BZAR::attack_lm_ex_whitelist_-orig_subnets	**Перемещение внутри периметра и выполнение команд**	Подсети запросов
BZAR::attack_lm_ex_whitelist_-resp_subnets	**Перемещение внутри периметра и выполнение команд**	Подсети ответов
BZAR::attack_lm_ex_whitelist_-orig_names	**Перемещение внутри периметра и выполнение команд**	Имена запросов
BZAR::attack_lm_ex_whitelist_-resp_names	**Перемещение внутри периметра и выполнение команд**	Имена ответов
BZAR::attack_lm_extracted_file_-whitelist_orig_addrs	**Извлечение файла тактикой перемещения внутри периметра**	IP-адреса запросов
BZAR::attack_lm_extracted_file_-whitelist_resp_addrs	**Извлечение файла тактикой перемещения внутри периметра**	IP-адреса ответов
BZAR::attack_lm_extracted_file_-whitelist_orig_subnets	**Извлечение файла тактикой перемещения внутри периметра**	Подсети запросов
BZAR::attack_lm_extracted_file_-whitelist_resp_subnets	**Извлечение файла тактикой перемещения внутри периметра**	Подсети ответов
BZAR::attack_lm_extracted_file_-whitelist_orig_names	**Извлечение файла тактикой перемещения внутри периметра**	Имена запросов
BZAR::attack_lm_extracted_file_-whitelist_resp_names	**Извлечение файла тактикой перемещения внутри периметра**	Имена ответов
BZAR::t1547_004_whitelist_orig_-addrs	**Закрепление**	IP-адреса запросов

Табл. 219. Переменные, используемые для BZAR

ПЕРЕМЕННАЯ	ТАКТИКА АТАКИ (ЖИРНЫМ)[5] ТЕХНИКА АТАКИ	НАЗНАЧЕНИЕ
	Автозапуск при загрузке или входе в систему: DLL-библиотеки, загружаемые с помощью Winlogon	
BZAR::t1547_004_whitelist_resp_addrs	**Закрепление** Автозапуск при загрузке или входе в систему: DLL-библиотеки, загружаемые с помощью Winlogon	IP-адреса ответов
BZAR::t1547_004_whitelist_orig_subnets	**Закрепление** Автозапуск при загрузке или входе в систему: DLL-библиотеки, загружаемые с помощью Winlogon	Подсети запросов
BZAR::t1547_004_whitelist_resp_subnets	**Закрепление** Автозапуск при загрузке или входе в систему: DLL-библиотеки, загружаемые с помощью Winlogon	Подсети ответов
BZAR::t1547_004_whitelist_orig_names	**Закрепление** Автозапуск при загрузке или входе в систему: DLL-библиотеки, загружаемые с помощью Winlogon	Имена запросов
BZAR::t1547_004_whitelist_resp_names	**Закрепление** Автозапуск при загрузке или входе в систему: DLL-библиотеки, загружаемые с помощью Winlogon	Имена ответов
BZAR::t1547_010_whitelist_orig_addrs	**Закрепление** Автозапуск при загрузке или входе в систему: Мониторы портов	IP-адреса запросов
BZAR::t1547_010_whitelist_resp_addrs	**Закрепление** Автозапуск при загрузке или входе в систему: Мониторы портов	IP-адреса ответов
BZAR::t1547_010_whitelist_orig_subnets	**Закрепление**	Подсети запросов

Табл. 219. Переменные, используемые для BZAR

ПЕРЕМЕННАЯ	ТАКТИКА АТАКИ (ЖИРНЫМ)[5] ТЕХНИКА АТАКИ	НАЗНАЧЕНИЕ
	Автозапуск при загрузке или входе в систему: Мониторы портов	
BZAR::t1547_010_whitelist_resp_-subnets	**Закрепление** Автозапуск при загрузке или входе в систему: Мониторы портов	Подсети ответов
BZAR::t1547_010_whitelist_orig_-names	**Закрепление** Автозапуск при загрузке или входе в систему: Мониторы портов	Имена запросов
BZAR::t1547_010_whitelist_resp_-names	**Закрепление** Автозапуск при загрузке или входе в систему: Мониторы портов	Имена ответов
BZAR::attack_discovery_-whitelist_orig_addrs	**Исследование**	IP-адреса запросов
BZAR::attack_discovery_-whitelist_resp_addrs	**Исследование**	IP-адреса ответов
BZAR::attack_discovery_-whitelist_orig_subnets	**Исследование**	Подсети запросов
BZAR::attack_discovery_-whitelist_resp_subnets	**Исследование**	Подсети ответов
BZAR::attack_discovery_-whitelist_orig_names	**Исследование**	Имена запросов
BZAR::attack_discovery_-whitelist_resp_names	**Исследование**	Имена ответов

См. также

Уменьшение количества ложных срабатываний модулей анализа сетевых данных с использованием белого списка

22.23.2. Возможные состояния сессий

Внутренние идентификаторы, которые использует сервис `zeek_wrapper` модуля «Анализ промышленного сетевого трафика» для определения состояния отслеживаемых сессий:

ИДЕНТИФИКАТОР	СОСТОЯНИЕ
S0	Обнаружен запрос подключения, но ответа нет
S1	Соединение установлено, но не завершено
SF	Соединение штатно установлено и завершено
REJ	Запрос на подключение отклонен
S2	Соединение установлено, и обнаружена попытка закрытия соединения от отправителя, но ответа от получателя нет
S3	Соединение установлено, и обнаружена попытка закрытия соединения от получателя, но ответа от отправителя нет
RSTO	Соединение установлено, но отправитель перестал быть доступным (отправлен TCP-флаг RST)
RSTR	Соединение установлено, но получатель перестал быть доступным (отправлен TCP-флаг RST)
RSTOS0	Отправитель отправил флаг SYN, за которым последовал флаг RST, но в период между ними получатель не отправлял флаг SYN ACK
RSTRH	Получатель отправил флаг SYN ACK после флага RST от отправителя, но отправитель не отправлял начальный запрос с флагом SYN
SH	Отправитель отправил флаг SYN, за которым последовал флаг FIN, но в период между ними получатель не отправлял SYN ACK (соединение установлено частично)
SHR	Получатель отправил флаг SYN ACK, за которым последовал флаг FIN, но отправитель не отправлял начальный запрос с флагом SYN
OTH	Отправитель не отправлял начальный запрос с флагом SYN (соединение установлено частично и не закрыто)

22.23.3. Поддерживаемые протоколы передачи данных

Модуль «Анализ промышленного сетевого трафика» способен разбирать различные данные в трафике активов на следующих уровнях:

- индикация — базовое распознавание протокола в трафике: его наличие и наименование без дополнительной информации о содержании его полей. Такие протоколы отображаются в столбце **Протоколы** вкладки **Сессии** и в поле **Протоколы** карточки сессии;
- анализ событий ИБ — выявление в трафике подозрительных или вредоносных действий с определением использованной техники атаки — доступно на страницах **События** и **Инциденты**;

- подробный анализ полей протоколов — подробный анализ и отображение детальной информации о содержании полей протокола. Список таких протоколов представлен в группе вкладок **Протоколы** на странице **Сетевые соединения**;
- контроль параметров технологического процесса — мониторинг и валидация значений, критичных для техпроцесса, с целью выявления несанкционированных изменений;
- выявление аномалий ПЛК — выявление отклонений в поведении программируемых логических контроллеров — например, появление новых узлов в контролируемой сети, запуск на узлах новой службы;
- извлечение файлов из трафика — обнаружение, анализ и сохранение файлов, передаваемых в рамках сессий — доступно на вкладке **Файлы** страницы **Сетевые соединения**.

В таблице ниже представлена информация о поддерживаемых протоколах и уровнях их разбора. Протоколы сгруппированы по назначению: общие и промышленные. Наличие галочки (✓) означает поддержку соответствующего уровня анализа, крестик (×) — отсутствие.

Табл. 220. Разбор протоколов, поддерживаемых модулем «Анализ промышленного сетевого трафика»

ПРОТОКОЛ	ИНДИКАЦИЯ	АНАЛИЗ СОБЫТИЙ ИБ	ПОДРОБНЫЙ АНАЛИЗ ПОЛЕЙ ПРОТОКОЛОВ	КОНТРОЛЬ ПАРАМЕТРОВ ТЕХНОЛОГИЧЕСКОГО ПРОЦЕССА	ВЫЯВЛЕНИЕ АНОМАЛИЙ ПЛК	ИЗВЛЕЧЕНИЕ ФАЙЛОВ ИЗ ТРАФИКА
Протоколы общего назначения						
ARP (Address Resolution Protocol)	×	✓	×	Неприменимо	Неприменимо	×
AYIYA (Anything In Anything)	✓	×	×			×
DCE/RPC (Distributed Computing Environment / Remote Procedure Calls)	✓	✓	✓			×
DHCP (Dynamic Host Configuration Protocol)	✓	×	×			×

Табл. 220. Разбор протоколов, поддерживаемых модулем «Анализ промышленного сетевого трафика»

ПРОТОКОЛ	ИН-ДИКАЦИЯ	АНАЛИЗ СОБЫТИЙ ИБ	ПО-ДРОБНЫЙ АНАЛИЗ ПОЛЕЙ ПРО-ТОКОЛОВ	КОНТРОЛЬ ПАРА-МЕТРОВ ТЕХНОЛО-ГИЧЕСКОГО ПРОЦЕССА	ВЫЯВЛЕНИЕ АНОМАЛИЙ ПЛК	ИЗ-ВЛЕЧЕНИЕ ФАЙЛОВ ИЗ ТРАФИКА
DNS (Domain Name System)	✓	✓	✓			×
DTLS (Datagram Transport Layer Security)	✓	×	×			×
Finger	✓	×	×			×
FTP (File Transfer Protocol) — Control connection	✓	×	×			✓
Geneve	✓	×	×			×
GSSAPI (Generic Security Service Application Program Interface)	✓	×	×			×
GTPV1 (GPRS Tunneling Protocol Version 1)	✓	×	×			×
HTTP (Hyper Text Transfer Protocol)	✓	✓	✓			✓

Табл. 220. Разбор протоколов, поддерживаемых модулем «Анализ промышленного сетевого трафика»

ПРОТОКОЛ	ИН-ДИКАЦИЯ	АНАЛИЗ СОБЫТИЙ ИБ	ПО-ДРОБНЫЙ АНАЛИЗ ПОЛЕЙ ПРО-ТОКОЛОВ	КОНТРОЛЬ ПАРА-МЕТРОВ ТЕХНОЛО-ГИЧЕСКОГО ПРОЦЕССА	ВЫЯВЛЕНИЕ АНОМАЛИЙ ПЛК	ИЗ-ВЛЕЧЕНИЕ ФАЙЛОВ ИЗ ТРАФИКА
ICMP (Internet Control Message Protocol)	✓	✓	×			×
IMAP (Internet Message Access Protocol)	✓	×	×			×
IRC (Internet Relay Chat)	✓	×	×			✓
Kerberos	✓	×	✓			✓
LDAP (Lightweight Directory Access Protocol)	✓	×	×			×
LLMNR (Link-local Multicast Name Resolution)	×	✓	×			×
MDNS (Multicast Domain Name System)	×	✓	×			×
MQTT (Message Queue	✓	×	×			×

Табл. 220. Разбор протоколов, поддерживаемых модулем «Анализ промышленного сетевого трафика»

ПРОТОКОЛ	ИНДИКАЦИЯ	АНАЛИЗ СОБЫТИЙ ИБ	ПОДРОБНЫЙ АНАЛИЗ ПОЛЕЙ ПРОТОКОЛОВ	КОНТРОЛЬ ПАРАМЕТРОВ ТЕХНОЛОГИЧЕСКОГО ПРОЦЕССА	ВЫЯВЛЕНИЕ АНОМАЛИЙ ПЛК	ИЗВЛЕЧЕНИЕ ФАЙЛОВ ИЗ ТРАФИКА
Telemetry Transport)						
MySQL	✓	×	×			×
NBNS (Network Basic Input/ Output System Name Service)	✓	×	×			×
NTLM (New Technology LAN Manager)	✓	✓	✓			×
NTP (Network Time Protocol)	✓	×	×			×
POP3 (Post Office Protocol Version 3)	✓	×	×			×
PGSQL (PostgreSQL)	✓	×	×			×
QUIC	✓	×	×			×
RADIUS (Remote Authentication Dial-In User Service)	✓	×	×			×

Табл. 220. Разбор протоколов, поддерживаемых модулем «Анализ промышленного сетевого трафика»

ПРОТОКОЛ	ИН-ДИКАЦИЯ	АНАЛИЗ СОБЫТИЙ ИБ	ПО-ДРОБНЫЙ АНАЛИЗ ПОЛЕЙ ПРО-ТОКОЛОВ	КОНТРОЛЬ ПАРА-МЕТРОВ ТЕХНОЛО-ГИЧЕСКОГО ПРОЦЕССА	ВЫЯВЛЕНИЕ АНОМАЛИЙ ПЛК	ИЗ-ВЛЕЧЕНИЕ ФАЙЛОВ ИЗ ТРАФИКА
RDP (Remote Desktop Protocol)	✓	×	✓			✓[6]
RFB/VNC (Remote Framebuffer)	✓	×	×			×
SIP (Session Initiation Protocol)	✓	×	×			×
SMB (Server Message Block)	✓	✓	✓			✓
SMTP (Simple Mail Transfer Protocol)	✓	×	✓			✓
SNMP (Simple Network Management Protocol)	✓	×	×			×
SOCKS	✓	×	×			×
SSH (Secure Shell)	✓	✓	✓			×
SSL (Secure Sockets Layer)	✓	×	✓			✓
SYSLOG	✓	×	×			×

6. Извлеченные файлы содержат только данные об использованном в соединении сертификате SSL/TLS.

Табл. 220. Разбор протоколов, поддерживаемых модулем «Анализ промышленного сетевого трафика»

ПРОТОКОЛ	ИН-ДИКАЦИЯ	АНАЛИЗ СОБЫТИЙ ИБ	ПО-ДРОБНЫЙ АНАЛИЗ ПОЛЕЙ ПРО-ТОКОЛОВ	КОНТРОЛЬ ПАРА-МЕТРОВ ТЕХНОЛО-ГИЧЕСКОГО ПРОЦЕССА	ВЫЯВЛЕНИЕ АНОМАЛИЙ ПЛК	ИЗ-ВЛЕЧЕНИЕ ФАЙЛОВ ИЗ ТРАФИКА
TDS (Tabular Data Stream)	✓	×	×			×
TELNET	✓	×	×			×
TFTP	✓	×	×			×
TNS (Transparent Network Substrate)	✓	×	×			×
TPKT/COTP (Connection-Oriented Transport Protocol)	✓	×	×			×
VXLAN (Virtual Extensible LAN)	✓	×	×			×
WS DISCOVERY (Web Services Dynamic Discovery)	✓	×	×			×
XMPP (Extensible Messaging and Presence Protocol)	✓	×	×			×
Протоколы промышленного назначения						

Табл. 220. Разбор протоколов, поддерживаемых модулем «Анализ промышленного сетевого трафика»

ПРОТОКОЛ	ИН-ДИКАЦИЯ	АНАЛИЗ СОБЫТИЙ ИБ	ПО-ДРОБНЫЙ АНАЛИЗ ПОЛЕЙ ПРО-ТОКОЛОВ	КОНТРОЛЬ ПАРА-МЕТРОВ ТЕХНОЛО-ГИЧЕСКОГО ПРОЦЕССА	ВЫЯВЛЕНИЕ АНОМАЛИЙ ПЛК	ИЗ-ВЛЕЧЕНИЕ ФАЙЛОВ ИЗ ТРАФИКА
DNP3 (Distributed Network Protocol 3)	✓	✓	×	×	×	×
Emerson DeltaV	✓	✓	✓	✓	×	×
ENIP/CIP (Ethernet Industrial Protocol/ Common Industrial Protocol)	✓	✓	×	×	✓	×
IEC 60870-5-104	✓	✓	×	×	✓	×
IEC 61850 MMS (Manufacturing Message Specification)	✓	×	×	×	✓	×
Modbus	✓	×	✓	✓	✓	×
OPC UA (Open Platform Communications Unified Architecture)	✓	×	✓	✓	✓	×
S7 Communication	✓	✓	×	×	✓	×

Табл. 220. Разбор протоколов, поддерживаемых модулем «Анализ промышленного сетевого трафика»

ПРОТОКОЛ	ИНДИКАЦИЯ	АНАЛИЗ СОБЫТИЙ ИБ	ПОДРОБНЫЙ АНАЛИЗ ПОЛЕЙ ПРОТОКОЛОВ	КОНТРОЛЬ ПАРАМЕТРОВ ТЕХНОЛОГИЧЕСКОГО ПРОЦЕССА	ВЫЯВЛЕНИЕ АНОМАЛИЙ ПЛК	ИЗВЛЕЧЕНИЕ ФАЙЛОВ ИЗ ТРАФИКА
S7 Plus Communication	✓	✓	×	×	✓	×
UMAS (Unified Messaging Application Services)	✓	✓	×	×	×	×

22.23.4. Поддерживаемые функции промышленных протоколов

В данном разделе приведен перечень функций техпроцесса, обнаруживаемых модулем «Анализ промышленного сетевого трафика». Функции сгруппированы по поддерживаемым промышленным протоколам. Для каждого протокола функции разделены на «Управляющие» и «Критичные». Функции из группы «Критичные» по умолчанию заданы в конфигурационном файле `ics-function.dat`, который можно настроить в соответствии со своими задачами (см. раздел «Изменение списка критичных функций»).

Функции протокола CIP

Управляющие:

- Find Next Object Instance
- Get Instance Attribute List
- Get Instance Attribute List Reply
- Group Sync
- Mask
- Read/Modify/Write Tag
- Read/Modify/Write Tag Reply
- Read Tag
- Read Tag Fragmented
- Read Tag Fragmented Reply
- Read Tag Reply
- Response Mask
- Write Tag
- Write Tag Fragmented
- Write Tag Fragmented Reply
- Write Tag Reply

Критичные:

- Apply Attributes
- Create
- Delete
- Error Response
- Execute PCCC Service
- Forward Open
- Forward Open Reply
- Get Attribute List
- Get Attribute List Reply
- Get Attributes All
- Get Attributes All Reply
- Get Attribute Single Reply
- Get Attributes Single
- Get Connection Point Member List
- Get Member
- Insert Member
- Multiple Service Packet
- Multiple Service Packet Reply
- No Forward Open
- Remove Member
- Reset
- Restore
- Save
- Set Attribute List
- Set Attributes All
- Set Attributes Single
- Set Member
- Start
- Stop

Функции протокола DeltaV

Управляющие:

- Close module session
- Create subscription
- Get config card info
- Get phys card info
- Get running modules
- Open device session
- Open module session
- Switchover
- Write tag

Критичные:

- Debug force module input
- Debug start

- Debug stop
- Download
- Online mode enable
- Select mode
- Upgrade
- Upload parameters

Функции протокола DNP3

Управляющие

- ASSIGN_CLASS
- AUTHENTICATE_RESP
- CONFIRM
- DELAY_MEASURE
- DIRECT_OPERATE
- DIRECT_OPERATE_NR
- FREEZE_AT_TIME
- FREEZE_AT_TIME_NR
- FREEZE_CLEAR
- FREEZE_CLEAR_NR
- IMMED_FREEZE
- IMMED_FREEZE_NR
- OPERATE
- READ
- RECORD_CURRENT_TIME
- RESPONSE
- SELECT
- UNSOLICITED_RESPONSE
- WRITE

Критичные:

- ABORT_FILE
- ACTIVATE_CONFIG
- AUTHENTICATE_FILE
- AUTHENTICATE_REQ
- AUTHENTICATE_REQ_NR
- CLOSE_FILE
- COLD_RESTART
- DELETE_FILE
- DISABLE_UNSOLICITED
- ENABLE_UNSOLICITED
- GET_FILE_INFO
- INITIALIZE_APPL
- INITIALIZE_DATA
- OPEN_FILE
- SAVE_CONFIG

- START_APPL
- STOP_APPL
- WARM_RESTART

Функции протокола IEC104

Табл. 221. Управляющие функции протокола IEC104, поддерживаемые модулем «Анализ промышленного сетевого трафика»

ФУНКЦИЯ (ОБОЗНАЧЕНИЕ В КОНФИГУРАЦИИ)	ОПИСАНИЕ (ОБОЗНАЧЕНИЕ В СОБЫТИИ)
C_BO_NA_1	bit string 32 bit
C_BO_TA_1	bit string 32 bit with time tag CP56Time2a
C_CD_NA_1	delay acquisition command
C_CI_NA_1	counter interrogation command
C_CS_NA_1	clock synchronization command
C_DC_TA_1	double command with time tag CP56Time2a
C_IC_NA_1	(general-) interrogation command
C_RC_NA_1	regulating step command
C_RC_TA_1	regulating step command with time tag CP56Time2a
C_RD_NA_1	read command
C_SC_TA_1	single command with time tag CP56Time2a
C_SE_NA_1	setpoint command; normalized value
C_SE_NB_1	setpoint command; scaled value
C_SE_NC_1	setpoint command; short floating point value
C_SE_TA_1	setpoint command; normalized value with time tag CP56Time2a
C_SE_TB_1	setpoint command; scaled value with time tag CP56Time2a
C_SE_TC_1	setpoint command; short floating point value with time tag CP56Time2a
C_TS_NA_1	test command

Табл. 221. Управляющие функции протокола IEC104, поддерживаемые модулем «Анализ промышленного сетевого трафика»

ФУНКЦИЯ (ОБОЗНАЧЕНИЕ В КОНФИГУРАЦИИ)	ОПИСАНИЕ (ОБОЗНАЧЕНИЕ В СОБЫТИИ)
C_TS_TA_1	test command with time tag CP56Time2a
F_AF_NA_1	ack file; ack section
F_DR_TA_1	directory
F_FR_NA_1	file ready
F_LS_NA_1	last section; last segment
F_SC_NB_1	queryLog - request archive file
F_SG_NA_1	segment
F_SR_NA_1	section ready
M_BO_NA_1	bit string of 32 bit
M_BO_TA_1	bit string of 32 bit with time tag
M_BO_TB_1	bit string of 32 bit with time tag CP56Time2a
M_DP_NA_1	double point information
M_DP_TA_1	double point information with time tag
M_DP_TB_1	double point information with time tag CP56Time2a
M_EI_NA_1	end of initialization
M_EP_TA_1	event of protection equipment with time tag
M_EP_TB_1	packed start events of protection equipment with time tag
M_EP_TC_1	packed output circuit information of protection equipment with time tag
M_EP_TD_1	event of protection equipment with time tag CP56Time2a
M_EP_TE_1	packed start events of protection equipment with time tag CP56time2a
M_EP_TF_1	packed output circuit information of protection equipment with time tag CP56Time2a

Табл. 221. Управляющие функции протокола IEC104, поддерживаемые модулем «Анализ промышленного сетевого трафика»

ФУНКЦИЯ (ОБОЗНАЧЕНИЕ В КОНФИГУРАЦИИ)	ОПИСАНИЕ (ОБОЗНАЧЕНИЕ В СОБЫТИИ)
M_IT_NA_1	integrated totals
M_IT_TA_1	integrated totals with time tag
M_IT_TB_1	integrated totals with time tag CP56Time2a
M_ME_NA_1	measured value; normalized value
M_ME_NB_1	measured value; scaled value
M_ME_NC_1	measured value; short floating point value
M_ME_ND_1	measured value; normalized value without quality descriptor
M_ME_TA_1	measured value; normalized value with time tag
M_ME_TB_1	measured value; scaled value with time tag
M_ME_TC_1	measured value; short floating point value with time tag
M_ME_TD_1	measured value; normalized value with time tag CP56Time2a
M_ME_TE_1	measured value; scaled value with time tag CP56Time2a
M_ME_TF_1	measured value; short floating point value with time tag CP56Time2a
M_PS_NA_1	packed single-point information with status change detection
M_SP_NA_1	single point information
M_SP_TA_1	single point information with time tag
M_SP_TB_1	single point information with time tag CP56Time2a
M_ST_NA_1	single point information
M_ST_TA_1	step position information with time tag
M_ST_TB_1	step position information with time tag CP56Time2a
P_AC_NA_1	parameter activation

Табл. 221. Управляющие функции протокола IEC104, поддерживаемые модулем «Анализ промышленного сетевого трафика»

ФУНКЦИЯ (ОБОЗНАЧЕНИЕ В КОНФИГУРАЦИИ)	ОПИСАНИЕ (ОБОЗНАЧЕНИЕ В СОБЫТИИ)
P_ME_NA_1	parameter of measured value; normalized value
P_ME_NB_1	parameter of measured value; scaled value
P_ME_NC_1	parameter of measured value; short floating point value

Табл. 222. Критичные функции протокола IEC104, поддерживаемые модулем «Анализ промышленного сетевого трафика»

ФУНКЦИЯ (ОБОЗНАЧЕНИЕ В КОНФИГУРАЦИИ)	ОПИСАНИЕ (ОБОЗНАЧЕНИЕ В СОБЫТИИ)
C_DC_NA_1	double command
C_RP_NA_1	reset process command
C_SC_NA_1	single command
Change_Value_Command	IEC104_change_value_command in netpdl.xml
F_SC_NA_1	call directory; select file; call file; call section
Insert_Command	IEC104_insert_command and IEC104_insert_off_command in netpdl.xml

Функции протокола Modbus

Управляющие:

- DIAGNOSTICS
- ENCAP_INTERFACE_TRANSPORT
- GET_COMM_EVENT_COUNTER
- GET_COMM_EVENT_LOG
- MASK_WRITE_REGISTER
- READ_COILS
- READ_DISCRETE_INPUTS
- READ_EXCEPTION_STATUS
- READ_FIFO_QUEUE
- READ_FILE_RECORD
- READ_HOLDING_REGISTERS
- READ_INPUT_REGISTERS
- READ_WRITE_MULTIPLE_REGISTERS
- REPORT_SLAVE_ID
- WRITE_FILE_RECORD

- WRITE_MULTIPLE_COILS
- WRITE_MULTIPLE_REGISTERS
- WRITE_SINGLE_COIL
- WRITE_SINGLE_REGISTER

Критичные:

- не заданы

Функции протокола S7 Communication

Управляющие:

- CPU Services
- Mode Transition
- Read Variable
- Setup Communication
- Write Variable

Критичные:

- Download Block
- Download Ended
- End Upload
- PLC Control
- PLC Stop
- Request Download
- Start Upload
- Upload

Функции протокола S7 Plus Communication

Управляющие:

- HW_Config_Change

Критичные:

- Program_Transfer_From_Plc
- Program_Transfer_To_Plc
- Start_CPU
- Stop_CPU

Функции протокола UMAS

Управляющие:

- RESPONSE_ERROR
- RESPONSE_OK
- UMAS_CHECK_PLC
- UMAS_GET_STATUS_MODULE
- UMAS_INIT_COMM

- UMAS_KEEP_ALIVE
- UMAS_MONITOR_PLC
- UMAS_READ_CARD_INFO
- UMAS_READ_COILS_REGISTERS
- UMAS_READ_ETH_MASTER_DATA
- UMAS_READ_ID
- UMAS_READ_IO_OBJECT
- UMAS_READ_MEMORY_BLOCK
- UMAS_READ_PLC_INFO
- UMAS_READ_PROJECT_INFO
- UMAS_READ_VARIABLES
- UMAS_RELEASE_PLC_RESERVATION
- UMAS_REPEAT
- UMAS_TAKE_PLC_RESERVATION
- UMAS_WRITE_COILS_REGISTERS
- UMAS_WRITE_IO_OBJECT
- UMAS_WRITE_VARIABLES

Критичные:

- UMAS_END_TRANSFER_PROJECT_FROM_PLC
- UMAS_END_TRANSFER_PROJECT_TO_PLC
- UMAS_INITIALIZE_TRANSFER_PROJECT_FROM_PLC
- UMAS_INITIALIZE_TRANSFER_PROJECT_TO_PLC
- UMAS_START_PLC
- UMAS_STOP_PLC
- UMAS_TRANSFER_PROJECT_FROM_PLC
- UMAS_TRANSFER_PROJECT_TO_PLC

См. также

Управление сервисом регистрации событий техпроцесса

Изменение списка критичных функций

22.23.5. Детектируемые тактики и техники атак

Группы и идентификаторы атак указаны в соответствии с классификацией, принятой в MITRE ATT&CK.

- Разведка:
  - T1592 — Сбор информации об атакуемых узлах
  - T1595 — Активное сканирование
- Первоначальный доступ:
  - T1190 — Недостатки в общедоступном приложении
- Выполнение/эксплуатация:
  - T1047 — Инструментарий управления Windows
  - T1053.005 — Запланированная задача (задание): Планировщик заданий Windows
  - T1059.001 — Интерпретаторы командной строки: PowerShell
  - T1569.002 — Системные службы: Диспетчер управления службами

- Закрепление:
    - T1047 — Инструментарий управления Windows
    - T1053.005 — Запланированная задача (задание): Планировщик заданий Windows
    - T1204 — Выполнение с участием пользователя
    - T1547.004 — Автозапуск при загрузке или входе в систему: DLL-библиотеки загружаемые с помощью Winlogon
    - T1547.010 — Автозапуск при загрузке или входе в систему: Мониторы портов
    - T1569 — Системные службы
- Повышение привилегий:
    - T1053.005 — Запланированная задача (задание): Планировщик заданий Windows
- Предотвращение обнаружения:
    - T1070.001 — Удаление признаков активности из системы: Очистка журналов событий Windows
    - T1542.005 — Загрузка раньше ОС: Загрузка по TFTP
- Получение учетных данных:
    - T1003.004 — Получение дампа учетных данных: Секреты LSA
    - T1003.006 — Получение дампа учетных данных: DCSync
    - T1003.008 — Получение дампа учетных данных: Содержимое файлов /etc/passwd и /etc/shadow
    - T1557.001 — «Человек посередине»: Подмена LLMNR/NBT-NS-ответа и ретрансляция SMB
    - T1558.003 — Кража или подделка билетов Kerberos: «Прожарка» Kerberos
- Исследование:
    - T1012 — Запросы к реестру
    - T1016 — Изучение конфигурации сети
    - T1018 — Изучение удаленных систем
    - T1033 — Исследование владельца или пользователей системы
    - T1046 — Сканирование сетевых служб
    - T1049 — Изучение сетевых подключений
    - T1069 — Изучение групп разрешений
    - T1082 — Изучение системы
    - T1083 — Изучение файлов и каталогов
    - T1087 — Изучение учетных записей
    - T1124 — Изучение системного времени
    - T1135 — Исследование общих сетевых ресурсов
- Перемещение внутри периметра:
    - T1021.001 — Службы удаленного доступа: Протокол удаленного рабочего стола
    - T1021.002 — Службы удаленного доступа: Общие SMB-ресурсы или ресурсы администраторов Windows
    - T1021.004 — Службы удаленного доступа: SSH
    - T1021.005 — Службы удаленного доступа: VNC
    - T1210 — Эксплуатация удаленных служб
    - T1570 — Передача инструментов внутри периметра
- Сбор данных:
    - T1039 — Данные с общих сетевых дисков
    - T1602.001 — Данные из репозитория конфигураций: SNMP (дамп MIB)
- Управление и контроль:
    - T1071.004 — Протокол прикладного уровня: DNS
    - T1095 — Протоколы (кроме прикладного уровня)
- Эксфильтрация данных:

    - T1041 — Эксфильтрация через канал управления
    - T1048.003 — Эксфильтрация по протоколу без шифрования
- Воздействие:
    - T1496 — Несанкционированное использование ресурсов
    - T1529 — Завершение работы или перезагрузка системы

22.24. Справочная информация о модуле «Управление проектами ПЛК»

В этом разделе:

- Общая информация о модуле «Управление проектами ПЛК»
- Статусы репозиториев
- Системные журналы Version Control Desktop App
- Шаблоны для настройки исключений

22.24.1. Общая информация о модуле «Управление проектами ПЛК»

- Архитектура модуля «Управление проектами ПЛК»
- Спецсимволы
- Подключенные активы
- Блокировка проекта

Version Control помогает специалистам АСУ ТП и экспертам по кибербезопасности решить задачу централизованного хранения проектов ПЛК и отслеживания изменений в них. При необходимости Version Control предоставляет возможность быстро отследить цепочку изменений и восстановить требуемую версию проекта ПЛК.

Решаемые задачи:

- Централизованное хранение проектов ПЛК.
- Ведение истории изменений проектов ПЛК, сравнение версий и отображение различий.
- Контроль легитимности изменений ПО и конфигураций ПЛК.
- Резервное копирование и восстановление проектов ПЛК.
- Мониторинг, аналитика и отчетность по проектам ПЛК.

В этом разделе:

22.24.1.1. Архитектура модуля «Управление проектами ПЛК»

Архитектура модуля «Управление проектами ПЛК» (Version Control) описывается следующими уровнями:

- **Supervision**. Верхний уровень серверной архитектуры, предназначенный для централизованного мониторинга и управления всей системой. На этом уровне осуществляется:
    - Централизованное управление решением, получение данных со всех площадок.
    - Централизованное хранение копий проектов.
    - Просмотр панелей мониторинга, отчетов, инфографики по всем объектам предприятия.
- **Management**. Реализован как Version Control Management. Серверная часть, которая устанавливается отдельно и хранит всю информацию об изменениях исходного кода версий ПЛК. На этом уровне осуществляется:

- Учет и контроль изменений в ПО (проекты ПЛК/АСУ ТП), в том числе сравнение версий проекта.
- Хранение резервных копий ПО и восстановление ПО.
- Формирование и отправка событий ИБ в сторонние системы.

- **Sensor**. На этом уровне осуществляется сбор данных с ПЛК для контроля неизменности ПО и конфигураций ПЛК.
- **Desktop App**. Реализован как приложение Version Control Desktop App.Возможности этого уровня:
  - Устанавливается на инженерные станции.
  - Позволяет загружать проекты в Version Control Management.
  - Позволяет скачивать проекты с Version Control Management.
  - Позволяет вносить обоснования изменений проектов ПЛК и просматривать историю изменений.
  - Проверяет соответствие версий проектов ПЛК в Version Control Desktop App и Version Control Management.

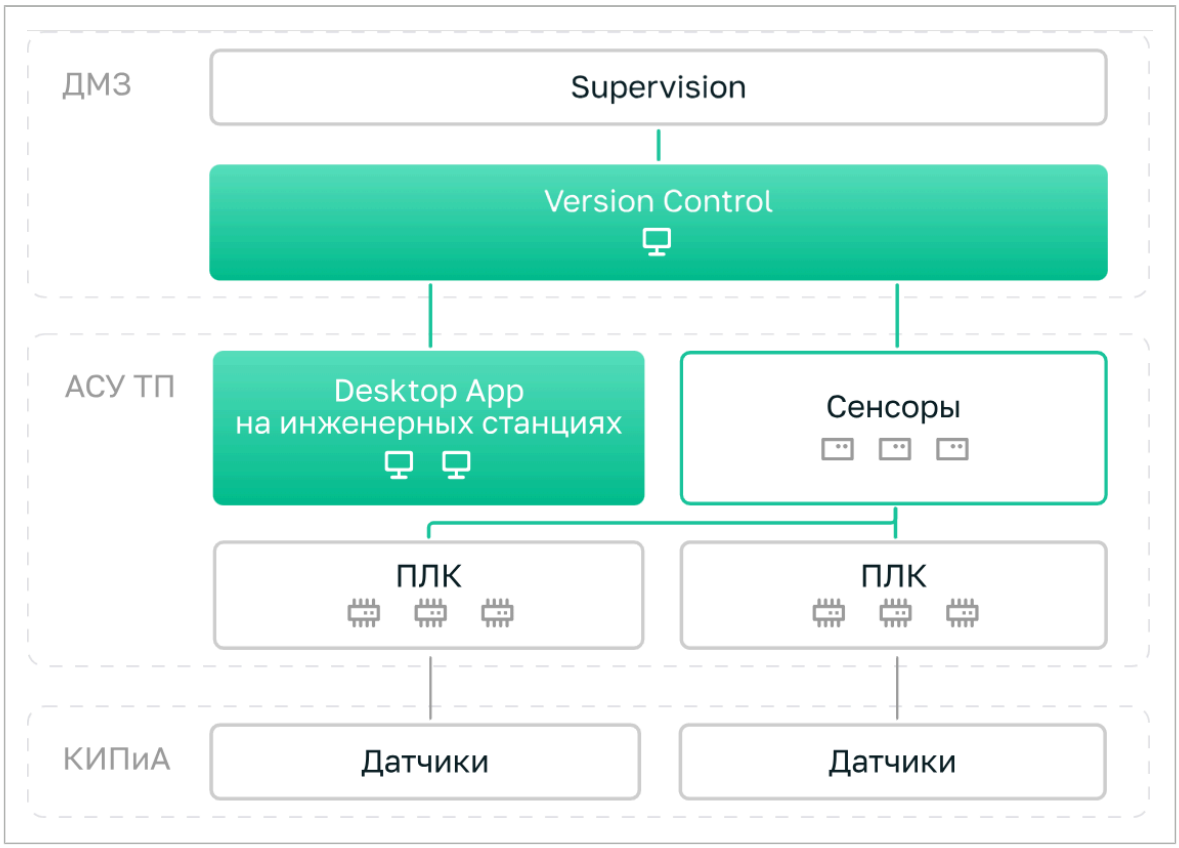


Рис. 577. Архитектура Version Control

22.24.1.2. Спецсимволы

Включить отображение спецсимволов можно в области с содержимым файла с помощью кнопки ⋮.

Табл. 223. Отображаемые спецсимволы

СПЕЦСИМВОЛ	КОД СИМВОЛА	ОПИСАНИЕ
Перевод строки	ASCII 10	Завершает текущую строку и переводит курсор на следующую строку
Возврат каретки	ASCII 13	Возвращает курсор в начало текущей строки

Табл. 223. Отображаемые спецсимволы

СПЕЦСИМВОЛ	КОД СИМВОЛА	ОПИСАНИЕ
Табуляция	ASCII 9	Добавляет горизонтальный отступ
Конец файла	ASCII 26	Сигнализирует о завершении файла в старых системах. Этот символ указывает, что больше нет данных для чтения
Обычный пробел	ASCII 32	—
Неразрывный пробел	Unicode U+00A0	Предотвращает перенос текста на новую строку. Выглядит как обычный пробел
Тонкий пробел	Unicode U+2009	—
Широкий пробел	Unicode U+2003	—

22.24.1.3. Подключенные активы

К репозиториям можно подключить до 10 ПЛК, которые еще не имеют привязки к репозиториям.

На странице репозитория отображается следующая информация о подключенных ПЛК:

- Наименование — название ПЛК. При нажатии на наименование ПЛК открывается его страница в Version Control Management.
- Сбор данных — информация об успешности сбора данных.
- Конфигурации — статус отклонения последней собранной с ПЛК конфигурации от эталона.

Сбор данных

В столбце `Сбор данных` содержится следующая информация:

- Первое число — количество сканеров сбора, выполненных успешно.
- Второе число — количество сканеров сбора, которые не удалось выполнить из-за ошибок соединения.
- Третье число — количество сканеров сбора, которые не удалось выполнить из-за ошибок сбора.

Содержимое ячейки изменяет цвет в зависимости от успешности сбора данных:

- Серый цвет — сбор данных не выполнялся.
- Черный цвет — все сканеры сбора выполнены успешно.
- Желтый цвет — хотя бы один сканер сбора не удалось выполнить из-за ошибок соединения.
- Красный цвет — хотя бы один сканер сбора не удалось выполнить из-за ошибок сбора.

При наведении на содержимое столбца отображается:

- Дата и время последнего обновления.
- Количество выполненных попыток сбора данных с ПЛК по категориям.

Конфигурации

В столбце `Конфигурации` могут быть следующие значения:

- Нет отклонений — конфигурации ПЛК соответствуют эталону в данный момент. Выделено черным цветом.
- Были отклонения — Конфигурации ПЛК соответствует эталону в данный момент, но в их предыдущих версиях были отклонения. Выделено желтым цветом.
- Есть отклонения — Конфигурации ПЛК не соответствуют эталону в данный момент. Выделено красным цветом.
- Символ `–` — сбор конфигураций не выполнялся.

При наведении на содержимое столбца отображается:

- Дата и время последнего обновления.
- Количество собранных конфигураций, сгруппированных по статусу их отклонения.

22.24.1.4. Блокировка проекта

Блокирование проекта — отключение возможности внесения изменений в проект другими пользователями, кроме пользователя, который выполнил блокировку.

Права на блокировку и разблокировку проектов различаются в зависимости от роли пользователя:

- Пользователь с ролью `Администратор` может разблокировать любые проекты и блокировать любые не заблокированные.
- Пользователь с ролью `Инженер` может блокировать любые не заблокированные проекты, но разблокировать может только те проекты, которые заблокировал сам.

У пользователя, заблокировавшего проект, остаются доступны все сценарии работы с проектом. У других пользователей будут доступны все сценарии работы с этим проектом, кроме следующих:

- Создание и загрузка новых версий проекта.
- Редактирование репозитория.
- Блокировка и разблокировка проекта.
- Восстановление версии проекта.

22.24.2. Статусы репозиториев

В левом боковом меню возле имени репозитория может отображаться значок статуса репозитория. Возможные статусы репозиториев отображены в таблице ниже.

Табл. 224. Статусы репозиториев

ЗНАЧОК СТАТУСА	ОБОЗНАЧЕНИЕ СТАТУСА	НЕОБХОДИМЫЕ ДЕЙСТВИЯ	ИНСТРУКЦИЯ
—	Серверная и локальная версии проекта равны	Действия не требуются	—
	Репозиторий не подключен к локальному хранилищу	Необходимо подключить репозиторий	Подключение репозитория

Табл. 224. Статусы репозиториев

ЗНАЧОК СТАТУСА	ОБОЗНАЧЕНИЕ СТАТУСА	НЕОБХОДИМЫЕ ДЕЙСТВИЯ	ИНСТРУКЦИЯ
	Серверная версия проекта новее локальной	Необходимо скачать новую версию проекта с сервера	—
	Локальная версия проекта новее серверной	Необходимо загрузить новую версию проекта на сервер	Загрузка версии проекта на сервер
	Репозиторий не найден на сервере	Ранее подключенный репозиторий был удален на сервере. Необходимо забыть проект	Удаление связи между локальным и серверным хранилищем
	Обнаружен конфликт версий	Необходимо исправить конфликт версий	Обнаружен конфликт версий проектов ПЛК
	Обнаружена ошибка	Необходимо исправить ошибку	—
	Идет процесс импорта или экспорта	Действия не требуются	—
	Идет процесс подключения репозитория	Действия не требуются	—
	Локальное хранилище изменено	Необходимо создать новую версию проекта	Создание и загрузка версии проекта на сервер

Для отображения блокировки проекта используются статусы блокировки проекта. Возможные статусы блокировки проекта отображены в таблице ниже.

Табл. 225. Статусы блокировки проекта

ЗНАЧОК СТАТУСА	ОБОЗНАЧЕНИЕ СТАТУСА	ОПИСАНИЕ
—	Проект не заблокирован	Проект может заблокировать любой пользователь
	Проект заблокирован самим пользователем	Для работы с проектом его должен разблокировать сам пользователь

Табл. 225. Статусы блокировки проекта

ЗНАЧОК СТАТУСА	ОБОЗНАЧЕНИЕ СТАТУСА	ОПИСАНИЕ
	Проект заблокирован другим пользователем	Для работы с проектом его должен разблокировать пользователь, заблокировавший его, или пользователь с ролью `Администратор`

22.24.3. Системные журналы Version Control Desktop App

Для каждого пользователя Version Control Desktop App создается свой кэш.

В ОС Windows данные приложения хранятся в папке **C:\Users\[имя пользователя]\AppData\Local\VersionControl**. Системные журналы Version Control Desktop App записываются в **C:\Users\[имя пользователя]\AppData\Local\VersionControl\logs**.

В ОС Astra Linux и РЕД ОС данные приложения и системные журналы хранятся в **/home/[имя пользователя]/.local/share/**.

Ротация системных журналов происходит каждый день. Срок хранения журналов — 7 дней.

22.24.4. Шаблоны для настройки исключений

ШАБЛОН	ПРИМЕРЫ СООТВЕТСТВИЯ	ПОЯСНЕНИЕ

`**/logs`	`logs/debug.log`
	`logs/monday/foo.bar`
	`build/logs/debug.log`
		Добавьте символы `**` в начало шаблона, чтобы сопоставлять каталоги в любом месте репозитория

`**/logs/debug.log`	`logs/debug.log`
	`build/logs/debug.log`
	но не
	`logs/build/debug.log`
		Символы `**` сопоставляют файлы на основе их имени и имени родительского каталога

`*.log`	`debug.log`
	`foo.log`
	`.log`
	`logs/debug.log`
		Символ `*` — это подстановочный знак, который может соответствовать как нескольким символам, так и ни одному

`*.log` `!important.log`	`debug.log` но не	Добавление символа `!` в начало шаблона отменяет действие шаблона. Если файл соответствует шаблону исключения и ука-

ШАБЛОН	ПРИМЕРЫ СО-ОТВЕТСТВИЯ	ПОЯСНЕНИЕ
	`logs/debug.log`	занному после отменяющему шаблону, то такой файл не будет исключен

`/debug.log`	`debug.log`
	но не
	`logs/debug.log`
		Шаблоны исключения, указанные после отменяющего шаблона, снова будут помечать файлы как исключаемые, даже если ранее исключение этих файлов было отменено

`debug.log`	`debug.log` `logs/debug.log`	Символ `/` перед именем файла соответствует файлу в корневом каталоге репозитория

`debug?.log`	`debug0.log`
	`debugg.log`
	но не
	`debug10.log`
		Символ `?` соответствует строго одному символу

`debug[0-9].log`	`debug0.log`
	`debug1.log`
	но не
	`debug10.log`
		Символы в имени файла соответствуют одному символу из заданного диапазона в `[...]`

`debug[01].log`	`debug0.log`
	`debug1.log`
	но не
	`debug2.log`
	`debug01.log`
		Символы в имени файла соответствуют одному символу из указанного набора в `[...]`

`debug[!01].log`	`debug2.log`
	но не
	`debug0.log`
	`debug1.log`
	`debug01.log`
		Символы в имени файла не соответствуют символам, указанным в `[!...]`

`debug[a-z].log`	`debuga.log`
	`debugb.log`
	но не
	`debug1.log`
		Символы в имени файла соответствуют одному символу из заданного диапазона в `[...]`

ШАБЛОН	ПРИМЕРЫ СО-ОТВЕТСТВИЯ	ПОЯСНЕНИЕ

`logs`	`logs`
	`logs/debug.log`
	`logs/latest/foo.bar`
	`build/logs`
	`build/logs/debug.log`
		Без символа `/` в конце этот шаблон будет соответствовать и файлам, и содержимому каталогов с таким именем

`logs/`	`logs/debug.log`
	`logs/latest/foo.bar`
	`build/logs/foo.bar`
	`build/logs/latest/debug.log`
		Символ `/` в конце шаблона означает каталог. Все содержимое любого каталога репозитория, соответствующего этому имени, будет игнорироваться

`logs/!logs/important.log`	`logs/debug.log` `logs/important.log`	Файл `logs/important.log` исключен, так как из-за особенностей Git нельзя отменить исключение файла, которое задано шаблоном соответствия каталогу

`logs/**/debug.log`	`logs/debug.log`
	`logs/monday/debug.log`
	`logs/monday/pm/debug.log`
		Символы `**` соответствуют множеству каталогов или ни одному

`logs/*day/debug.log`	`logs/monday/debug.log`
	`logs/tuesday/debug.log`
	но не
	`logs/latest/debug.log`
		Подстановочные символы `*` можно использовать в именах каталогов

`logs/debug.log`	`logs/debug.log`
	но не
	`debug.log`
		Шаблоны, указывающие на файл в определенном каталоге, задаются относительно корневого каталога репозитория

ШАБЛОН	ПРИМЕРЫ СО-ОТВЕТСТВИЯ	ПОЯСНЕНИЕ
	`build/logs/debug.log`	

См. также

Настройка исключений

22.25. Справочная информация о модуле «EDR for PLC»

В этом разделе:

- Общие сведения о модуле «EDR for PLC»
- Типы моделей модуля «EDR for PLC»;
- Модель на основе временного автомата;
- Модель на основе иерархического словаря;
- Модель на основе гибридного автомата.

22.25.1. Общие сведения о модуле «EDR for PLC»

Модуль UDV DATAPK EDR for PLC формирует комплексную Модель системы, в том числе схему ее работы, и выявляет отклонения в работе ее компонентов. Совместим с любыми автоматизированными системами, не требует информации о топологии, особенностях применяемых протоколов и алгоритмов.

Модуль UDV DATAPK EDR for PLC выявляет признаки инцидента на ранней стадии и формирует подробную информацию о затронутых процессах и компонентах.

Принципы работы модуля:

- применение технологий машинного обучения для раннего выявления аномалий;
- инвентаризация компонентов системы и их взаимодействие;
- поведенческий анализ компонентов системы;
- автоматизированное моделирование системы.

Алгоритмы построения модели основан на пассивном наблюдении за работой каждого компонента защищаемой системы и не требует активного взаимодействия с ней.

22.25.2. Типы моделей модуля «EDR for PLC»

Модуль UDV DATAPK EDR for PLC использует три типа моделей:

- модель на основе временного автомата;
- модель на основе иерархического словаря;
- модель на основе гибридного автомата.

Для каждого представления существует свой способ формирования модели. Для формирования модели на основе временного автомата используется алгоритм `OTALA`. Модель на основе иерархического словаря формируется с использованием алгоритма `Q-dict`, а модель на основе гибридного автомата формируется с помощью алгоритма `hybrid_automation`.

22.25.2.1. Жизненный цикл модели

Жизненный цикл модели в рамках модуля UDV DATAPK EDR for PLC состоит из следующих этапов:

1. Обучение.
2. Валидация.

> Прим.:
>
> Данный этап доступен только для моделей на основе иерархического словаря и гибридного автомата.

3. Детектирование.
4. Дообучение.

> Прим.:
>
> Данный этап доступен только для моделей на основе иерархического словаря и временного автомата.

5. Пауза.

Основным этапом является детектирование, которому соответствует режим детектирования аномалий.

Обучение завершается в двух случаях: при достижении условий сходимости модели или при ручном переводе модели в режим детектирования через API.

Если обучение модели на основе иерархического словаря и гибридного автомата завершено по условию сходимости, выполняется переход к процессу валидации. Цель валидации — проверить качество обучения. Для проверки в конфигурации задается минимальное значение, которое модель должна достичь на валидационной выборке, чтобы перейти в режим детектирования. Если значение не достигнуто, модель возвращается на этап обучения.

Валидационная выборка формируется из актуальных данных, поступающих с начала валидации, и не включает данные обучения.

Схема жизненного цикла модели представлена на рисунке ниже.

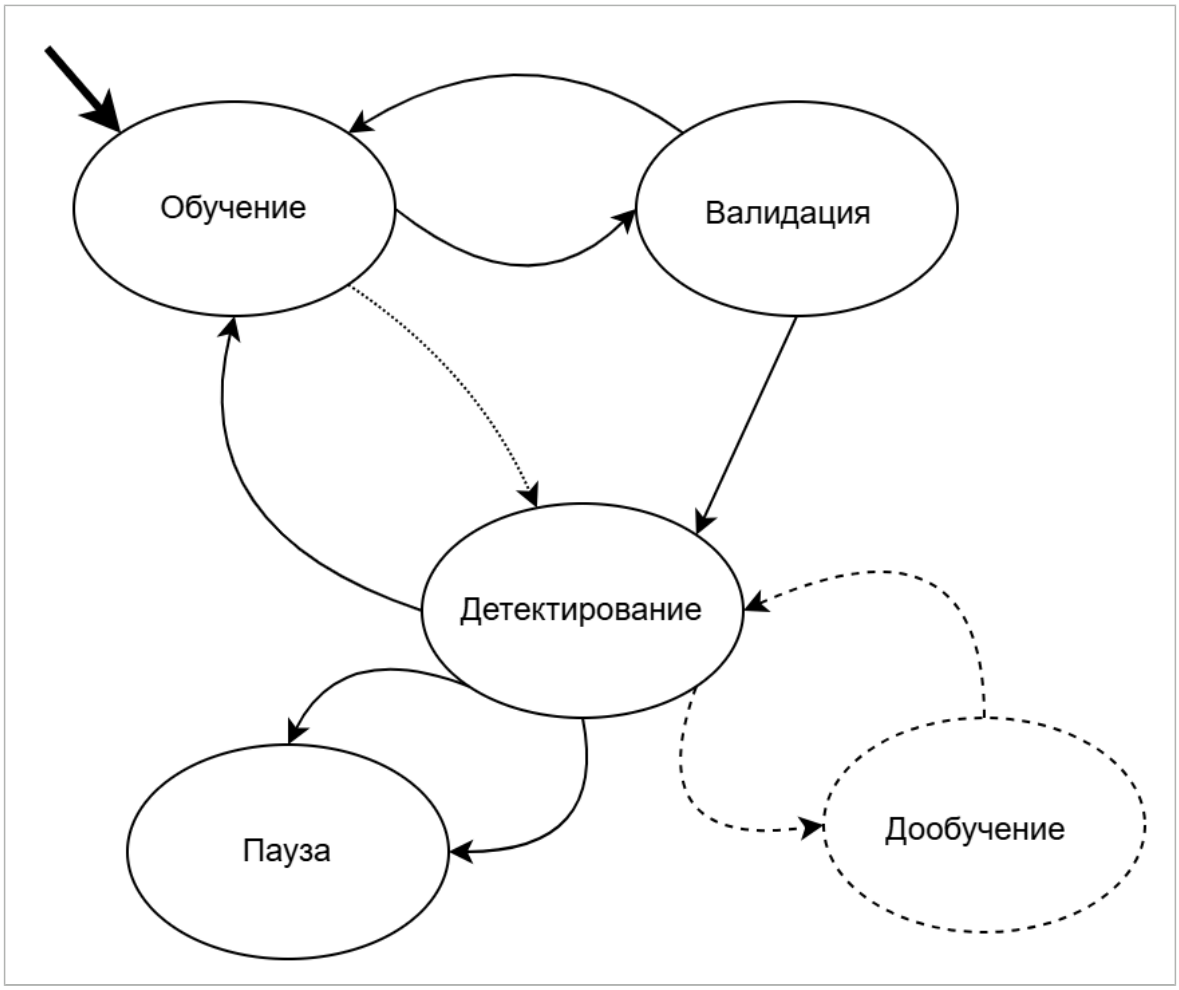


Рис. 578. Жизненный цикл модели в рамках модуля «EDR for PLC»

22.25.2.2. Модель на основе иерархического словаря

Данный тип модели представляет собой структуру данных, в которой каждый ключ `k` содержит значение `v`. При этом ключ может содержать несколько вложенных пар «ключ-значение». Глубина вложенности ограничена размером буфера (FIFO), который хранит последние пары «вход-выход». Изменении размера буфера запущенной модели приведет к переобучению модели.

Процесс обучения модели на основе иерархического словаря выглядит следующим образом:

1. Входные (k_i) и выходные (v_i) данные попадают в буфер.
2. Если иерархический словарь может предсказать v_i по k_i, то выполняется сравнение предсказанных данных с v_i.
    a. При совпадении предсказанных и фактических данных начинается анализ последующих взаимодействий.
    b. При несовпадении ключ расширяется за счет предыдущих пар из буфера:

- Формируется новый составной ключ $[\{k_{i-1}, v_{i-1}\}, k_i]$.

> Прим.:
>
> Значения k_{i-1} и v_{i-1} подставляются из буфера.

- Если коллизия сохраняется, ключ расширяется дальше (но не больше размера буфера).

3. Если ключа нет в словаре — добавляется новая запись.

Автоматический переход на этап валидации/детектирования происходит, если подряд идущие пары «вход-выход» не добавляют новые записи.

На этапе валидации выполняется проверка модели на новых данных. В случае достижения заданного порога «предсказательной способности» выполняется переход на этап детектирования. При недостижении порога выполняется повторное обучение модели.

На этапе детектирования модель предсказывает выходные данные на основе входных. В случае несовпадения предсказанных данных с фактическими формируется событие.

Кроме того, на этапе детектирования можно дообучить модель в ручном режиме, через API-интерфейс. Дообучение происходит при добавлении нового элемента словаря, данные для создания элемента словаря берутся из события модели, которое обработано пользователем и считается ложно-положительным.

Схема обучения модели на основе иерархического словаря представлена ниже.

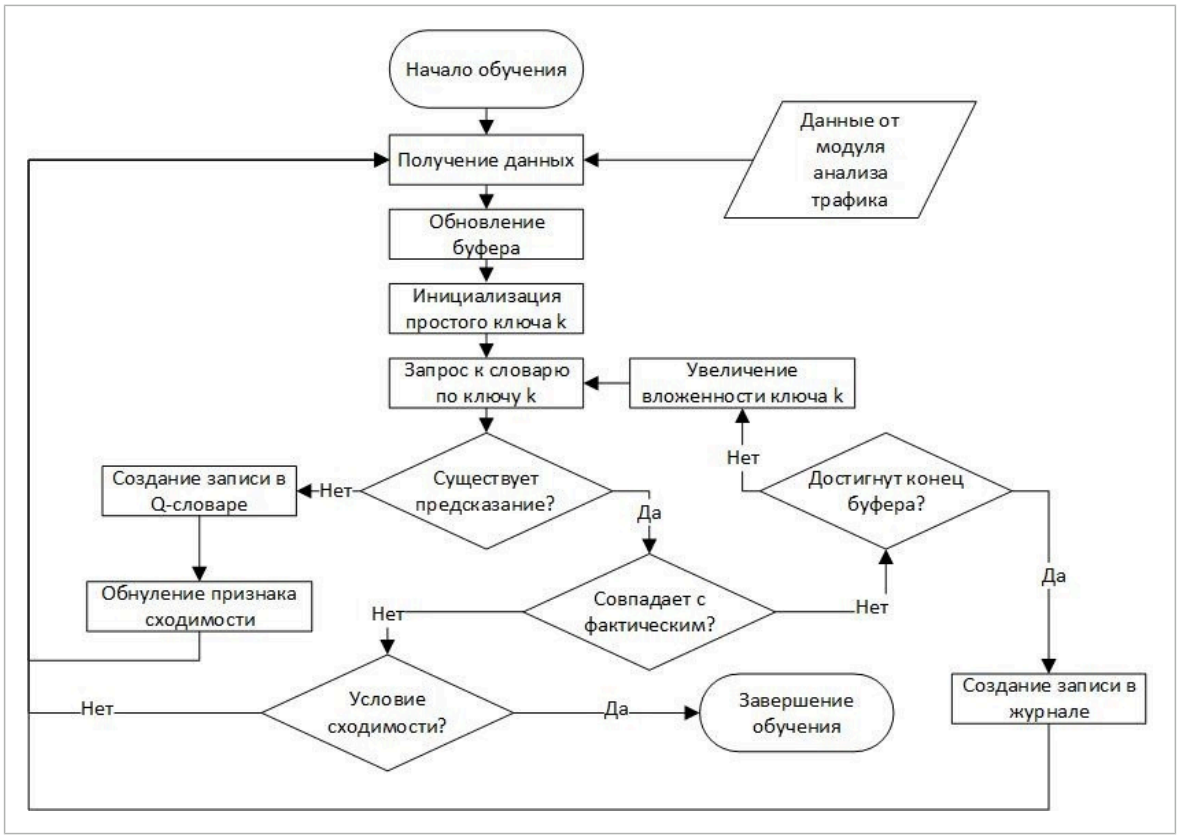


Рис. 579. Схема обучения модели на основе иерархического словаря

22.25.2.3. Модель на основе гибридного автомата

Модель на основе гибридного автомата позволяет моделировать как дискретные, так и непрерывные данные в сетевом взаимодействии, обеспечивая более точное (но и более сложное) описание процессов.

> Внимание:
>
> На текущий момент модель на основе гибридного автомата может быть построена только для протокола Modbus.

Входной вектор модели определяет, какие области памяти Modbus-устройства анализируются (конфигурируется заранее). Данные накапливаются до полного заполнения вектора (или передаются с задержкой, при этом подставляются предыдущие значения).

Описание этапов обучения модели на основе гибридного автомата представлено в таблице ниже.

Табл. 226. Этапы обучения модели на основе гибридного автомата

ЭТАП	ОПИСАНИЕ ЭТАПА	МЕТОДЫ/АЛГОРИТМЫ	ЦЕЛИ
Подготовка обучающей выборки	Накопление входных векторов данных	-	Формирование объема данных для обучения (рекомендуется ≥5 циклов работы системы)

Табл. 226. Этапы обучения модели на основе гибридного автомата

ЭТАП	ОПИСАНИЕ ЭТАПА	МЕТОДЫ/АЛГОРИТМЫ	ЦЕЛИ
Сегментация данных	Разделение данных на участки с разным поведением	• Вычисление производных; • Анализ бинарных изменений.	Выделение сегментов, соответствующих дискретным операциям и изменениям в системе
Кластеризация сегментов	Группировка схожих сегментов	Самоорганизующаяся карта Кохонена (SOM)	Определение состояния гибридного автомата
Расчет уравнений состояний	Построение математических моделей для каждого состояния	• Линейная регрессия с регуляризацией; • Минимизация MSE.	Получение дифференциальных уравнений, описывающих поведение системы в каждом состоянии
Выявление переходов	Определение правил смены состояний	• SVM-классификатор; • Линейная регрессия для reset-выражений.	Построение модели переходов между состояниями
Расчет допустимой ошибки	Определение пороговых значений для детектирования аномалий	Статистический анализ ошибок	Формирование критериев для обнаружения отклонений

На этапе валидации модель проверяется на валидационной выборке. В случае достижения порога предсказательной способности выполняется переход к этапу детектирования. В противном случае выполняется повторное обучение модели

На этапе детектирования обученная модель определяет следующее состояние автомата. Если следующее состояние отличается от текущего, данные следующего вектора предсказываются при помощи LR-модели. Если текущее и следующее состояния одинаковые, данные вектора предсказываются с помощью модели, обученной на данных внутри текущего состояния.

Если предсказанное значение превышает порог ошибки, то генерируется сообщение об аномалии.

Также в рамках модели на основе гибридного автомата дополнительно реализованы детекторы для протокола Modbus, позволяющие определять отклонения на уровне самого протокола. Ниже представлен перечень этих детекторов:

- `detector_new_tags` – детектор для контроля используемых областей памяти в рамках обмена по протоколу Modbus;
- `detector_exception` – детектор для сигнализации о возникновении исключений на уровне протокола Modbus;
- `detector_event_type` – детектор для выявления Modbus-запросов без ответов и/или Modbus-ответов без запросов;
- `detector_empty_request_address` – детектор для выявления неправильно сформированных запросов;

- `detector_stacked_coils_request` – детектор для выявления неверного формата данных (например, передача строки в бинарном регистре);
- `detector_unknown_func` – детектор для выявления отсутствующих в режиме обучения функций протокола Modbus;
- `detector_long_delay_in_requests` – детектор для выявления задержек между запросами, превосходящих предельные значения режима обучения;
- `detector_large_number_of_requests_over_time` – детектор для выявления слишком частых запросов (относительно режима обучения).

Активность каждого детектора определяется в конфигурации. Режима валидации для детекторов не существует, поэтому они сразу переходят в режим детектирования.

22.25.2.4. Модель на основе временного автомата

Данный тип модели представляет собой временной автомат, который формируется на основании наблюдаемых данных. Формально временной автомат представляет собой систему, состоящую из 4-х элементов (`S`, `∑`, `T`, `δ`), где:

- `S` - конечный набор состояний системы;
- `∑` - алфавит, состоящий из входных и выходных данных;
- `T` - набор допустимых переходов;
- `δ` - функция, характеризующая допустимый временной интервал для каждого из переходов.

Этап обучения включает создание алфавита `∑`, набора состояний `S` и переходов `T` временного автомата с сохранением временных интервалов.

Состояние автомата определяется уникальной комбинацией входных и выходных данных (допускается отсутствие одного из них, например, при одностороннем взаимодействии). Этот метод эффективен, когда входные и выходные сигналы четко идентифицируют состояние системы.

Функция `δ` задает минимальное и максимальное допустимое время для каждого перехода.

Автоматический переход к детектированию происходит при выполнении условий сходимости — заданного числа подряд идущих пар вход-выход без изменений в структуре автомата (т. е. без добавления состояний, переходов или корректировки временных интервалов).

Данная модель обучается по алгоритму `OTALA`. Схема обучения представлена ниже.

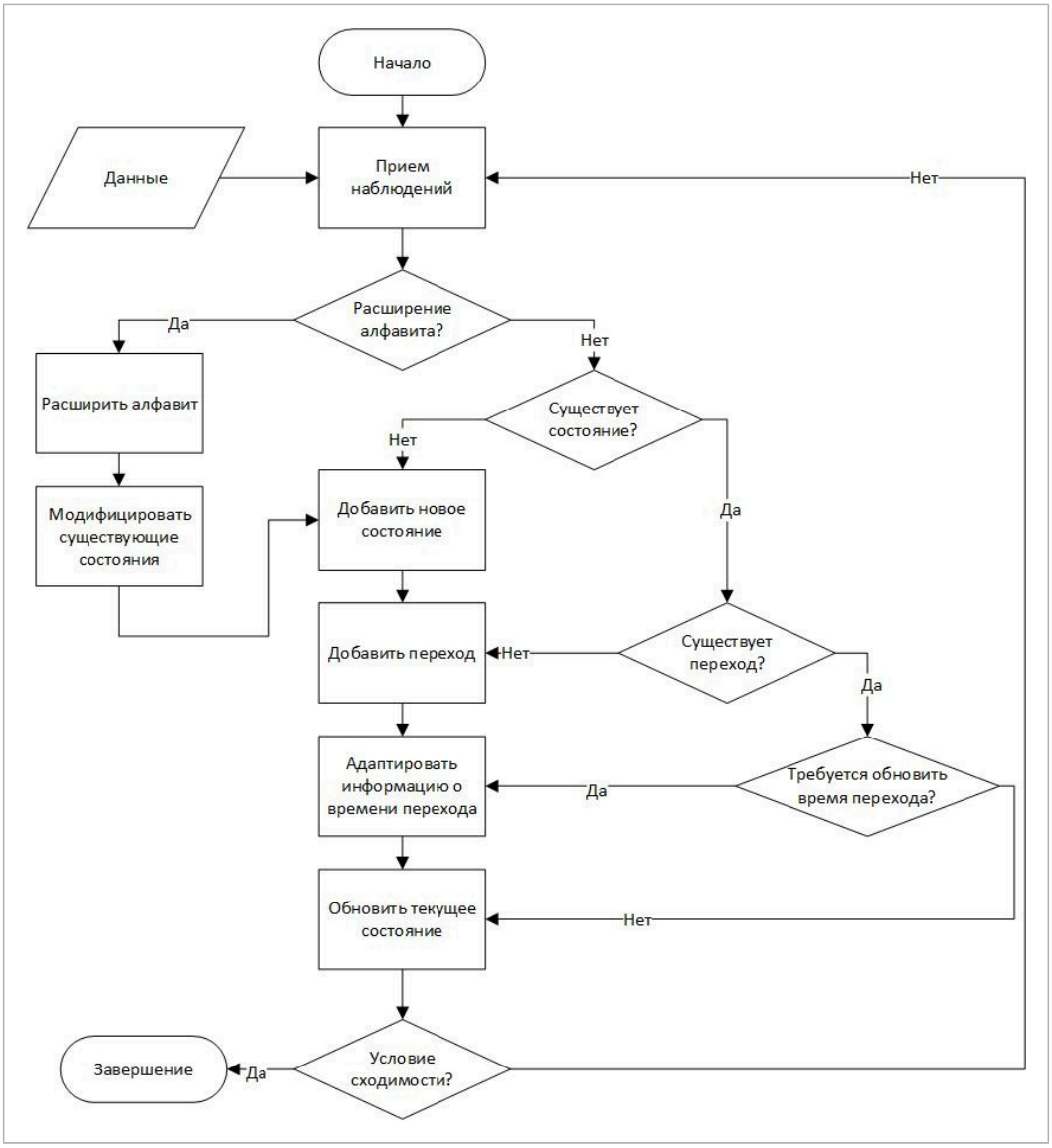


Рис. 580. Схема обучения модели на основе временного автомата

На этапе детектирования выполняется анализ пары «вход-выход». Ниже представлен порядок анализа:

1. Определяется новое состояние автомата и проверяется допустимость перехода.
2. Если данные неизвестны (новое состояние) или переход отсутствует в автомате — генерируется событие «Несуществующий переход».
3. Если переход допустим, но время выходит за рамки интервала, заданного при обучении — фиксируется событие «Нарушение временного интервала».

22.26. Справочная информация о компоненте Supervision

В этом разделе:

- Статусы компонентов Management;
- Роли пользователей Supervision.

22.26.1. Статусы компонентов Management

Подключенные к системе Менеджменты могут находиться в статусах `Подключен`, `Ошибка` и `Отключен`. Эти статусы отображаются в виде иконки в поле **Статус** в таблице на странице **Менеджменты** и в боковой панели выбранного Менеджмента — подробнее см. «Просмотр сведений о компоненте Management».

Табл. 227. Статусы Менеджментов

СТАТУС	ОПИСАНИЕ
`Подключен`	Менеджмент успешно подключен к Супервижн. Сервисы, отвечающие за сетевое соединение и обмен данными, работают стабильно и без ошибок. Сервисы, отвечающие за обмен данных, работают стабильно и без ошибок
`Ошибка`	Отсутствует сетевое соединение на стороне Менеджмента или Супервижн. Некорректная работа сервисов, отвечающих за обмен данными. Прим.: Для устранения причин ошибок см. раздел «Действия по восстановлению комплекса при сбойных ситуациях и ошибках в данных»
`Отключен`	Сетевое соединение с Менеджментом не выполняется, так как он был вручную отключен от Супервижн — подробнее об отключении Менеджмента см. раздел «Отключение компонента Management»

Супервижн также отслеживает следующие состояния взаимодействия с каждым Менеджментом: `Соединение`, `Репликация`, `Сбор метрик`. Эти состояния отображаются в боковой панели выбранного Менеджмента в блоке **Состояние Менеджмента** — подробнее см. «Просмотр сведений о компоненте Management».

Табл. 228. Состояния взаимодействия Менеджментов с Супервижн

СОСТОЯНИЕ	ОПИСАНИЕ	ВОЗМОЖНЫЕ ЗНАЧЕНИЯ
`Соединение`	Активность соединения между Менеджментом и Супервижн. Прим.: Если статус Менеджмента и состояние соединения имеют значение `Ошибка`, то состояния репликации и сбора метрик	1. `Установлено` — соединение работает в обычном режиме. 2. `Ошибка` — соединение прервано из-за возникшей ошибки. 3. `Недоступно` — соединение недоступно, так как Менеджмент был принудительно отключен от Супервижн.

Табл. 228. Состояния взаимодействия Менеджментов с Супервижн

СОСТОЯНИЕ	ОПИСАНИЕ	ВОЗМОЖНЫЕ ЗНАЧЕНИЯ
	от Менеджмента также будут иметь значение `Ошибка`.	
`Репликация`	Статус репликации (отправки) данных с Менеджмента на Супервижн и статус работы сервисов, отвечающих за репликацию данных. Прим.: Состояние репликации зависит от состояния соединения и не зависит от состояния сбора метрик с Менеджмента.	1. `Активно` — сервисы работают в обычном режиме. 2. `Ошибка` — сервисы перестали работать из-за возникшей ошибки. 3. `Недоступно` — сервисы недоступны, так как Менеджмент был принудительно отключен от Супервижн.
`Сбор метрик`	Статус работы сервисов, отвечающих за сбор метрик с Менеджментов, которые затем отображаются на виджетах Супервижн. Прим.: Состояние сбора метрик зависит от состояния соединения и не зависит от состояния репликации данных с Менеджмента.	

Действия над Менеджментами, доступные пользователям

В таблице ниже указано, какие действия могут выполнять пользователи с Менеджментами в Супервижн и какие статусы назначаются Менеджментам в зависимости от выполняемых действий.

Прим.:

Состоянием `Нет статуса` в таблице ниже обозначено состояние Менеджмента, если его подключение ранее не выполнялось и записей о нем нет на странице **Мониторинг**, либо Менеджмент был отключен и удален из Супервижн.

Табл. 229. Связь статусов Менеджментов и пользовательских действий над Менеджментами

СТАТУСЫ МЕНЕДЖМЕНТОВ	ДЕЙСТВИЯ ПОЛЬЗОВАТЕЛЕЙ НАД МЕНЕДЖМЕНТАМИ				
	ПОДКЛЮЧЕНИЕ	ПОВТОРНОЕ ПОДКЛЮЧЕНИЕ	РЕДАКТИРОВАНИЕ	ОТКЛЮЧЕНИЕ	УДАЛЕНИЕ
Нет статуса	Да	Нет	Нет	Нет	Нет
`Подключен`	Нет	Да	Да	Да	Нет
`Ошибка`	Нет	Да	Да	Да	Нет
`Отключен`	Да	Да	Нет	Нет	Да

Условия перехода между статусами Менеджментов

В таблице ниже описываются условия, при которых Менеджменты переходят из одного статуса в другой. В ячейках, связанных с переходом в статус `Ошибка`, также перечисляются причины такого поведения. Эту информацию можно использовать для устранения неполадок — подробнее о возможных нештатных ситуациях и способах их устранения см. раздел «Нештатные ситуации при взаимодействии компонентов Management и Supervision».

Табл. 230. Условия перехода между статусами Менеджментов

ПЕРЕХОД	УСЛОВИЯ
Нет статуса → `Ошибка` → `Подключен`	Менеджмент переходит в состояние `Подключен` только после успешного прохождения этапов, приведенных ниже. Во время этих этапов на протяжении 10–20 секунд Менеджмент находится в статусе `Ошибка`: 1. Менеджмент подключается впервые или через некоторое время после полного удаления Менеджмента вместе с его данными с Супервижн. 2. VPN-соединение с Менеджментом установлено успешно (состояние соединения — `Активно`). 3. Репликация данных с Менеджмента работает через 10–20 секунд после подключения (состояние репликации — `Активно`). 4. Сбор метрик с Менеджмента работает через 10–20 секунд после подключения (состояние сбора метрик — `Активно`).

Табл. 230. Условия перехода между статусами Менеджментов

ПЕРЕХОД	УСЛОВИЯ
Нет статуса → `Ошибка`	1. Менеджмент подключается впервые или через некоторое время после полного удаления Менеджмента вместе с его данными с Супервижн. 2. VPN-соединение с Менеджментом не установлено (состояние соединения — `Ошибка`) по следующим причинам: • Менеджмент не успел подключиться к Супервижн; • в конфигурации сети между Менеджментом и Супервижн возникли ошибки; • у Менеджмента нет сетевого доступа к Супервижн; • на Менеджменте остановлен или отсутствует сервис `udv-supervision-backend`
	И (если состояние соединения — `Ошибка`) ИЛИ (если состояние соединения другое) репликация данных с Менеджмента не работает (состояние репликации — `Ошибка`) по следующим причинам: • сервисы не успели запуститься; • используется некорректная конфигурация VPN; • используется некорректный сетевой адрес подписки на репликацию; • используется неправильная конфигурация на стороне Супервижн;; • возникли внутренние ошибки репликации в сервисе Менеджмента `udv-postgres`; • схемы реплицируемых данных отличаются на Супервижн и Менеджменте; • дубликаты данных Менеджмента хранятся на Супервижн; • используется медленное или нестабильное интернет-соединение; • в Супервижн остановлен или отсутствует сервис `udv-managements-backend`
	И (если состояние соединения — `Ошибка`) ИЛИ (если состояние соединения другое) сбор метрик с Менеджмента не работает (состояние сбора — `Ошибка`) по следующим причинам: • сервисы не успели запуститься; • используется некорректная конфигурация VPN;

Табл. 230. Условия перехода между статусами Менеджментов

ПЕРЕХОД	УСЛОВИЯ
	• используется некорректный сетевой адрес сбора метрик; • используется неправильная конфигурация на стороне Супервижн; • возникли ошибки сбора метрик в сервисе Менеджмента `udv-prometheus`; • на Менеджменте остановлен или отсутствует сервис `udv-prometheus`; • в Супервижн остановлен или отсутствует сервис `udv-sv-prometheus` • в Супервижн остановлен или отсутствует сервис `udv-sv-prometheus-wrapper`
`Подключен` → `Отключен` → Нет статуса	Пользователь отключил Менеджмент от Супервижн и удалил запись о Менеджменте с полным удалением его данных — подробнее см.: 1. Отключение компонента Management 2. Удаление компонента Management
`Подключен` → `Ошибка`	VPN-соединение с Менеджментом прервано из-за внутренней ошибки сети (состояние соединения — `Ошибка`) по следующим причинам: • возникли проблемы конфигурации сети между Менеджментом и Супервижн; • у Менеджмента нет сетевого доступа к Супервижн; • на Менеджменте остановлен или отсутствует сервис `udv-supervision-backend`
	И (если состояние соединения — `Ошибка`) ИЛИ (если состояние соединения другое) репликация данных автоматически приостановлена из-за внутренней ошибки (состояние репликации — `Ошибка`) по следующим причинам: • используется некорректная конфигурация VPN; • используется некорректный сетевой адрес подписки на репликацию; • используется неправильная конфигурация на стороне Супервижн; • возникли внутренние ошибки репликации в сервисе Менеджмента `udv-postgres`;

Табл. 230. Условия перехода между статусами Менеджментов

ПЕРЕХОД	УСЛОВИЯ
	• схемы реплицируемых данных отличаются на Супервижн и Менеджменте; • в Супервижн хранятся дубликаты данных Менеджмента; • используется медленное или нестабильное интернет-соединение; • в Супервижн остановлен или отсутствует сервис `udv-managements-backend`
	И (если состояние соединения — `Ошибка`) ИЛИ (если состояние соединения другое) сбор метрик автоматически приостановлен из-за внутренней ошибки (состояние сбора метрик — `Ошибка`) по следующим причинам: • используется некорректная конфигурация VPN; • используется некорректный сетевой адрес сбора метрик; • используется неправильная конфигурация на стороне Супервижн; • возникли ошибки сбора метрик в сервисе Менеджмента `udv-prometheus`; • на Менеджменте остановлен или отсутствует сервис `udv-prometheus`; • в Супервижн остановлен или отсутствует сервис `udv-sv-prometheus` • в Супервижн остановлен или отсутствует сервис `udv-sv-prometheus-wrapper`
`Подключен` → `Отключен`	Пользователь отключил Менеджмент от Супервижн с сохранением метрик и событий в течение времени, установленного политикой хранения данных
`Ошибка` → `Отключен` → Нет статуса	Пользователь отключил Менеджмент от Супервижн с полным удалением данных (реплик, метрик и событий)

Табл. 230. Условия перехода между статусами Менеджментов

ПЕРЕХОД	УСЛОВИЯ
`Ошибка` → `Подключен`	1. VPN-соединение с Менеджментом успешно установлено или восстановлено (состояние соединения — `Установлено`); 2. репликация данных с Менеджмента успешно работает или восстановлена (состояние репликации — `Активно`); 3. сбор метрик с Менеджмента успешно работает или восстановлен (состояние сбора метрик — `Активно`
`Ошибка` → `Отключен`	Пользователь отключил Менеджмент от Супервижн с сохранением метрик и событий в течение времени, установленного политикой хранения данных
`Отключен` → Нет статуса	Пользователь удалил отключенный раннее Менеджмент с удалением записи о нем, а также хранившихся в Супервижн данных
`Отключен` → `Ошибка` → `Подключен`	Менеджмент переходит в состояние `Подключен` только после успешного прохождения этапов, приведенных ниже. Во время этих этапов на протяжении 10–20 секунд Менеджмент находится в статусе `Ошибка`: 1. Менеджмент подключается после его отключения от Супервижн; 2. VPN-соединение с Менеджментом установлено успешно (состояние соединения — `Активно`); 3. репликация данных с Менеджмента работает (состояние репликации — `Активно`); 4. сбор метрик с Менеджмента работает (состояние сбора метрик — `Активно`)
`Отключен` → `Ошибка`	1. Менеджмент подключается после его отключения от Супервижн; 2. VPN-соединение с Менеджментом не установлено (состояние соединения — `Ошибка`) по следующим причинам: • Менеджмент не успел подключиться к Супервижн; • в конфигурации сети между Менеджментом и Супервижн возникли ошибки;

Табл. 230. Условия перехода между статусами Менеджментов

ПЕРЕХОД	УСЛОВИЯ
	• у Менеджмента нет сетевого доступа к Супервижн; • на Менеджменте остановлен или отсутствует сервис `udv-supervision-backend`
	И (если состояние соединения — `Ошибка`) ИЛИ (если состояние соединения другое) репликация данных с Менеджмента не работает (состояние репликации — `Ошибка`) по следующим причинам: • сервисы не успели запуститься; • используется некорректная конфигурация VPN; • используется некорректный сетевой адрес подписки на репликацию; • используется неправильная конфигурация на стороне Супервижн; • возникли внутренние ошибки репликации в сервисе Менеджмента `udv-postgres`; • схемы реплицируемых данных отличаются на Супервижн и Менеджменте; • в Супервижн хранятся дубликаты данных Менеджмента; • используется медленное или нестабильное интернет-соединение; • в Супервижн остановлен или отсутствует сервис `udv-managements-backend`
	И (если состояние соединения — `Ошибка`) ИЛИ (если состояние соединения другое) сбор метрик с Менеджмента не работает (состояние сбора метрик — `Ошибка`) по следующим причинам: • сервисы не успели запуститься; • используется некорректная конфигурация VPN; • используется некорректный сетевой адрес сбора метрик; • используется неправильная конфигурация на стороне Супервижн; • возникли ошибки сбора метрик в сервисе Менеджмента `udv-prometheus`; • на Менеджменте остановлен или отсутствует сервис `udv-prometheus`;

Табл. 230. Условия перехода между статусами Менеджментов

ПЕРЕХОД	УСЛОВИЯ
	• в Супервижн остановлен или отсутствует сервис `udv-sv-prometheus`; • в Супервижн остановлен или отсутствует сервис `udv-sv-prometheus-wrapper`.

22.26.2. Роли пользователей Supervision

Пользователям системы можно назначить одну из следующих ролей:

1. `Администратор`. Пользователи с этой ролью могут выполнять любые действия, связанные с настройкой и использованием Супервижн.
2. `Просмотр веб-интерфейса`. Пользователи с этой ролью могут изучать информацию о сервисе, выполнять поиск нужных данных и просматривать их, а также использовать другие доступные функции, которые не требуют изменения состояния системы.