



UDV NTA Network Traffic Analyzer v.1.0

Руководство по эксплуатации

cyberlympa.ru

support@cyberlympa.com

Содержание

1. Глоссарий.....	7
2. Первичная настройка Комплекса.....	13
2.1. Подключение Комплекса.....	13
2.1.1. Подключение к веб-интерфейсу по протоколу HTTPS.....	13
2.1.2. Первоначальная настройка.....	16
2.2. Импорт справочников из архива.....	19
2.3. Настройка сенсоров.....	21
2.3.1. Настройка контролируемой сети.....	21
2.3.2. Первичная настройка UDV NTA.....	22
2.3.3. Запуск обнаружения вторжений и синхронизация правил с сенсорами.....	24
2.4. Настройка парольной политики.....	25
2.5. Изменение сведений о Комплексе и сенсорах.....	27
2.6. Проверка работоспособности Комплекса.....	28
2.6.1. Проверка работоспособности системы передачи данных по иерархии.....	29
2.6.2. Проверка работоспособности UDV NTA.....	29
3. Инспекция сети.....	31
3.1. Управление сетевыми соединениями.....	31
3.1.1. Просмотр сессий и пакетов.....	31
3.1.2. Поиск по списку сессий.....	36
3.1.3. Фильтрация списка сессий.....	38
3.1.4. Экспорт копии сетевого трафика.....	39
3.1.5. Экспорт файлов, обнаруженных в сетевом трафике.....	41
3.2. Служба обнаружения вторжений.....	43
3.2.1. Создание правил обнаружения вторжений.....	45
3.2.2. Управление службой обнаружения вторжений.....	46
3.2.3. Экспорт и импорт правил службы обнаружения вторжения.....	49
4. Мониторинг событий.....	54
4.1. Поиск и просмотр событий в упрощенном режиме.....	56
4.2. Просмотр событий и создание запросов в экспертном режиме.....	61
4.3. Просмотр главной панели мониторинга «Статус защищенности».....	64
4.4. Импортируемые панели мониторинга.....	66
4.4.1. Принцип работы с мониторингом.....	67
4.4.2. Действия в случае обнаружения событий в панели мониторинга.....	67
4.4.3. Создание фильтров на панелях мониторинга.....	68

4.4.4. Выбор периода отображения событий на панели мониторинга.....	70
4.4.5. Главный дашборд.....	72
4.4.6. Экспорт событий из панели мониторинга.....	73
4.5. Настройка сбора событий.....	73
4.5.1. Экспорт и импорт правил нормализации событий.....	74
4.5.2. Экспорт и импорт источников событий.....	75
4.5.3. Включение и отключение служебных источников.....	76
4.5.4. Создание источника событий.....	78
4.5.5. Управление источниками событий.....	79
4.5.6. Выгрузка событий Комплекса в архив.....	80
4.6. Настройка и управление мониторингом.....	81
4.6.1. Создание шаблона индекса.....	81
4.6.2. Удаление шаблона индекса.....	83
4.6.3. Создание и настройка виджета.....	84
4.6.4. Просмотр и управление виджетами.....	86
4.6.5. Создание и настройка панели мониторинга.....	87
4.6.6. Настройка пользовательских правил нормализации событий.....	90
4.6.7. Настройка форматирования чисел и дат в разделе «Мониторинг».....	91
4.6.8. Экспорт и импорт объектов раздела «Мониторинг».....	92
5. Анализ и настройка инцидентов.....	98
5.1. Анализ инцидентов.....	99
5.2. Изменение параметров инцидента.....	102
5.3. Удаление инцидента.....	104
5.4. Групповые операции над инцидентами.....	104
5.5. Настройка инцидентов.....	105
5.5.1. Экспорт и импорт политики корреляции и статусов инцидентов.....	107
5.5.2. Управление службой корреляции событий.....	112
5.5.3. Управление схемой корреляции.....	113
5.5.4. Управление правилами корреляции событий.....	118
5.5.5. Анализ событий для генерации инцидентов.....	120
5.5.6. Настройка оповещений при появлении инцидентов.....	126
5.5.7. Управление статусами инцидентов.....	132
6. Работа с активами.....	134
6.1. Экспорт и импорт активов и их групп.....	136
6.1.1. Экспорт активов.....	137
6.1.2. Экспорт групп активов.....	137

6.1.3. Импорт активов.....	137
6.1.4. Импорт групп активов.....	138
6.2. Управление активами.....	139
6.2.1. Кнопки управления активами.....	139
6.2.2. Фильтрация списка активов.....	140
6.3. Создание актива.....	141
6.4. Группировка активов.....	142
6.4.1. Создание группы активов.....	143
6.4.2. Добавление активов в группу.....	144
6.4.3. Управление группами активов.....	147
6.5. Редактирование актива.....	150
6.6. Удаление активов.....	154
6.7. Выгрузка отчета по активам.....	156
6.8. Настройки активов.....	157
6.8.1. Настройка классификаторов.....	157
7. Управление Комплексом.....	163
7.1. Изменение сведений о Комплексе и сенсорах.....	163
7.2. Сканирование сети и определение интерфейсов активного сетевого оборудования.....	165
7.2.1. Интерпретация результатов пассивного сканирования сети.....	166
7.3. Настройка контролируемой сети.....	167
7.4. Управление пользователями.....	168
7.4.1. Управление учетными записями пользователей.....	171
7.4.2. Настройка парольной политики.....	177
7.4.3. Отключение ограничения на количество сессий пользователей.....	179
7.5. Экспорт отдельных справочников.....	179
7.6. Диагностика состояния системы Комплекса.....	180
7.7. Удаление сенсора.....	183
8. Нештатные ситуации и действия по их устранению.....	184
8.1. Действия по восстановлению комплекса при сбойных ситуациях и ошибках в данных.....	184
8.1.1. Веб-интерфейс не загружается.....	185
8.1.2. Соединение с главной страницей веб-интерфейса осуществляется по протоколу HTTP вместо HTTPS.....	187
8.1.3. Время на Комплексе отличается от времени получения события.....	187
8.1.4. После запуска Комплекса при попытке загрузки веб-интерфейса открывается пустая страница..	188
8.1.5. 502-я ошибка при загрузке страницы авторизации, 500-е ошибки сразу после авторизации.....	189
8.1.6. Не обнаруживаются новые сессии.....	191

8.1.7. Комплекс не обнаруживает активы в автоматическом режиме.....	193
8.1.8. Комплекс не обнаруживает активы без IP-адреса.....	194
8.1.9. Два актива с одинаковым IP-адресом.....	195
8.1.10. Отсутствуют события, генерируемые Комплексом.....	196
8.1.11. Не принимаются Syslog-сообщения от активов.....	198
8.1.12. Не принимаются сообщения от служб корреляции и обнаружения вторжений.....	199
8.1.13. Не принимаются сообщения от службы корреляции.....	200
8.1.14. Не инициализируется стек udv-opensearch, udv-opensearch-dashboards, udv-logstash.....	200
8.1.15. Не создается индекс в экспертном режиме страницы «События».....	201
8.1.16. Не удастся отфильтровать записи на странице «События» по новым значениям полей после нормализации.....	201
8.1.17. Объекты мониторинга и визуализации импортируются с ошибкой.....	202
8.1.18. Не удастся импортировать сканер сбора данных в веб-интерфейсе.....	202
8.1.19. Не выполняется архивация событий при превышении размера или времени хранения индекса.....	203
8.1.20. Ошибка «An HTTP request took too long to complete» при запуске контейнеров.....	204
8.1.21. Ошибки вида «<...>Cannot start service <...>. Bind for <ip_address>:<TCP/UDP_port> is ready allocated» при попытке запуска контейнеров.....	205
8.1.22. Недоступен сервис корреляции событий.....	205
8.1.23. При бездействии в веб-интерфейсе сеанс завершается раньше, чем через 10 минут.....	205
8.1.24. Не устанавливается соединение с сенсором.....	207
8.1.25. Потери при передаче данных через ERSPAN.....	209
8.2. Действия в случаях несанкционированного доступа к данным.....	210
8.2.1. Просмотр журнала действий пользователей Комплекса.....	210
8.2.2. Изменение статуса активности учетной записи пользователя Комплекса.....	211
8.3. Действия в других аварийных ситуациях.....	211
8.4. Анкета при обращении в сервисный центр.....	212
9. Справочная информация.....	217
9.1. Условные обозначения.....	217
9.2. Разделение функций по администрированию.....	218
9.3. Интерфейс Комплекса.....	219
9.3.1. Страницы интерфейса.....	219
9.3.2. Управляющие элементы.....	248
9.3.3. Элементы управления таблицами.....	253
9.3.4. Цветовая индикация и виды уведомлений.....	257
9.4. Дополнительные функции Комплекса.....	264
9.4.1. Выгрузка отчетов.....	264

9.4.2. Групповые операции.....	265
9.4.3. Нормализация событий.....	267
9.4.4. Фильтры.....	269
9.4.5. Представления.....	270
9.5. Условия эксплуатации Комплекса.....	272
9.6. Описание служебных источников событий.....	273
9.7. Описание полей событий.....	275
9.8. Переменные Комплекса.....	278
9.8.1. Переменные Комплекса уровня Management.....	278
9.8.2. Переменные Комплекса уровня Sensor.....	287
9.8.3. Рекомендации по использованию переменных файла .env.....	289
9.9. Основные переменные файла environment.json.....	290
9.10. Отображение времени в Комплексе.....	293
9.11. Работа с импортируемыми панелями мониторинга.....	293
9.11.1. Навигация в разделах мониторинга.....	293
9.11.2. Средства управления панелями мониторинга.....	293
9.11.3. Элементы управления интерфейсом визуализации.....	295
9.11.4. Диаграммы и таблицы на панелях мониторинга.....	296
9.12. Сетевые взаимодействия Комплексов.....	303
9.13. Синтаксис правил корреляции событий.....	306
9.13.1. Поддерживаемые типы событий.....	307
9.13.2. Фильтр событий.....	325
9.13.3. Временное окно.....	325
9.13.4. Группировка.....	327
9.13.5. Условие инцидента.....	327
9.13.6. Шаблоны обработки сложных событий.....	327
9.13.7. Сообщение инцидента.....	329
9.13.8. Приоритет и активность правил.....	330
9.14. События, попадающие в разделы мониторинга.....	331
9.15. Структура директорий Комплекса.....	369
9.16. Признаки неактивности сессий.....	370
9.17. Протоколы, обнаруживаемые UDV NTA в режиме индикации.....	372
9.18. Сетевые атаки, обнаруживаемые UDV NTA.....	373
9.19. Переменные файла белого списка.....	374

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.

1.3. 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

1.4. Виджет

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

1.5. Глобальная сеть

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

1.6. Индекс событий

Индекс событий — совокупность событий за сутки.

1.7. 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

1.8. Источник событий

Источник событий — объект или сервис от которого поступают события.

1.9. Карта сети

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

1.10. Классификатор

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

1.11. Контролируемая сеть

Контролируемая сеть — список подсетей, настраиваемый вручную на странице [Сенсоры](#). Узлы этих подсетей автоматически обнаруживаются Комплексом как контролируемые активы. Взаимодействие контролируемой сети с локальной сетью регистрируется как событие, с глобальной сетью — как инцидент.

1.12. 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 snmp 7 на соответствие эталонным настройкам системы, ее версии и контрольным суммам блоков.

1.13. Корреляция

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

1.14. Локальная сеть

Локальная сеть — список подсетей, зарезервированных для локального использования.

1.15. Несанкционированный доступ

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



Прим.:

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

Аббревиатура: НСД

1.16. Нормализация событий

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

1.18. Операционная система

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

Аббревиатура: ОС

1.19. Панель мониторинга

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

Синонимы: Dashboard

1.20. Политика корреляции событий

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

1.21. 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.

1.22. Программно-техническое средство

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

Аббревиатура: ПТС

1.23. Программное обеспечение

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

Аббревиатура: ПО

1.24. Программный комплекс

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

Аббревиатура: ПК

1.25. Программируемый логический контроллер

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

Аббревиатура: ПЛК

1.26. 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.

1.27. Роль пользователя

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

1.28. 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

1.29. 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 UDV NTA для каждого протокола транспортного уровня.

См. также

[Просмотр сессий и пакетов](#)

1.30. Система обнаружения вторжений

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

Аббревиатура: COB

1.31. Сканер

Сканер — исполняемый скрипт сбора данных.

1.32. Скрипт

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

1.33. Справочник

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

1.34. 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.

1.35. Средство защиты информации

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

Аббревиатура: СрЗИ

1.36. 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.

1.37. Технические условия

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

Аббревиатура: ТУ

1.38. 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

1.39. 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

1.40. Узел

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

1.41. 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.

1.42. 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

1.43. Фильтрация

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

1.44. 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

1.45. Common Platform Enumeration

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

Аббревиатура: CPE

1.46. Common Vulnerabilities and Exposures

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

Аббревиатура: CVE

1.47. Sensor

UDV NTA с базовым набором функций по получению информации с активов технологического комплекса.

Аббревиатура: Sensor

1.48. Management

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

Аббревиатура: Management

1.49. UDV NTA уровня Sensor

UDV NTA с базовым набором функций по получению информации о сетевой активности с активов корпоративного комплекса.

Аббревиатура: Sensor

1.50. UDV NTA уровня Management

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

Аббревиатура: Management

2. Первичная настройка Комплекса

В этом разделе:

1. **Подключение Комплекса**
2. **Импорт справочников из архива**
3. **Настройка сенсоров**
4. **Настройка парольной политики**
5. **Изменение сведений о Комплексе и сенсорах**
6. **Проверка работоспособности Комплекса**

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

Рекомендуется выполнять первичную настройку в предложенном порядке:

1. Подключение Комплекса
2. Импорт справочников из архива
3. Настройка сенсоров
4. Настройка парольной политики
5. Изменение сведений о Комплексе и сенсорах
6. Проверка работоспособности Комплекса

2.1. Подключение Комплекса

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.

2.1.1. Подключение к веб-интерфейсу по протоколу HTTPS

Для подключения к веб-интерфейсу Комплекса по протоколу HTTPS:

1. Проверьте возможность подключения к Management по протоколу HTTPS. Для этого:
 - а. Откройте веб-браузер на клиентской машине.
 - б. Введите адрес для подключения в веб-интерфейсу в формате `https://[IP-адрес]`, где [IP-адрес] – IP-адрес интерфейса управления Management.
- **Результат шага:** отобразится окно входа в веб-интерфейс UDV NTA.



Рис. 1. Окно входа в веб-интерфейс UDV NTA

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

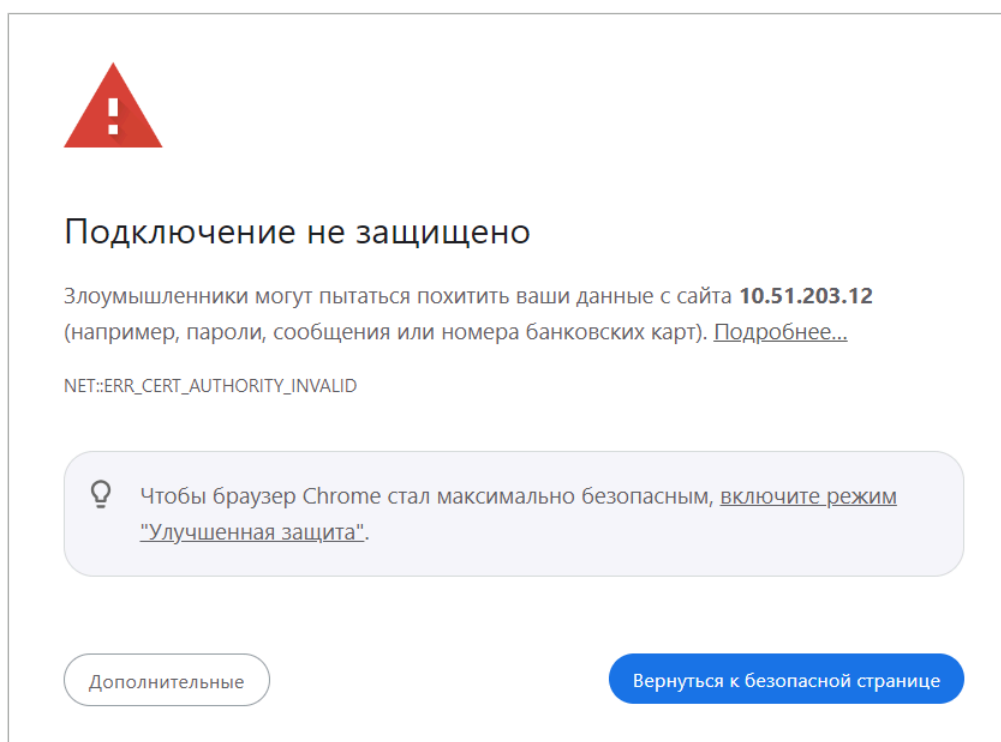


Рис. 2. Окно предупреждения о незащищенном подключении

- **Результат шага:** открыты дополнительные настройки для подключения к веб-интерфейсу UDV NTA в браузере.
- б. Для продолжения подключения к UDV NTA нажмите ссылку **Перейти на сайт [IP-адрес] (небезопасно)**.

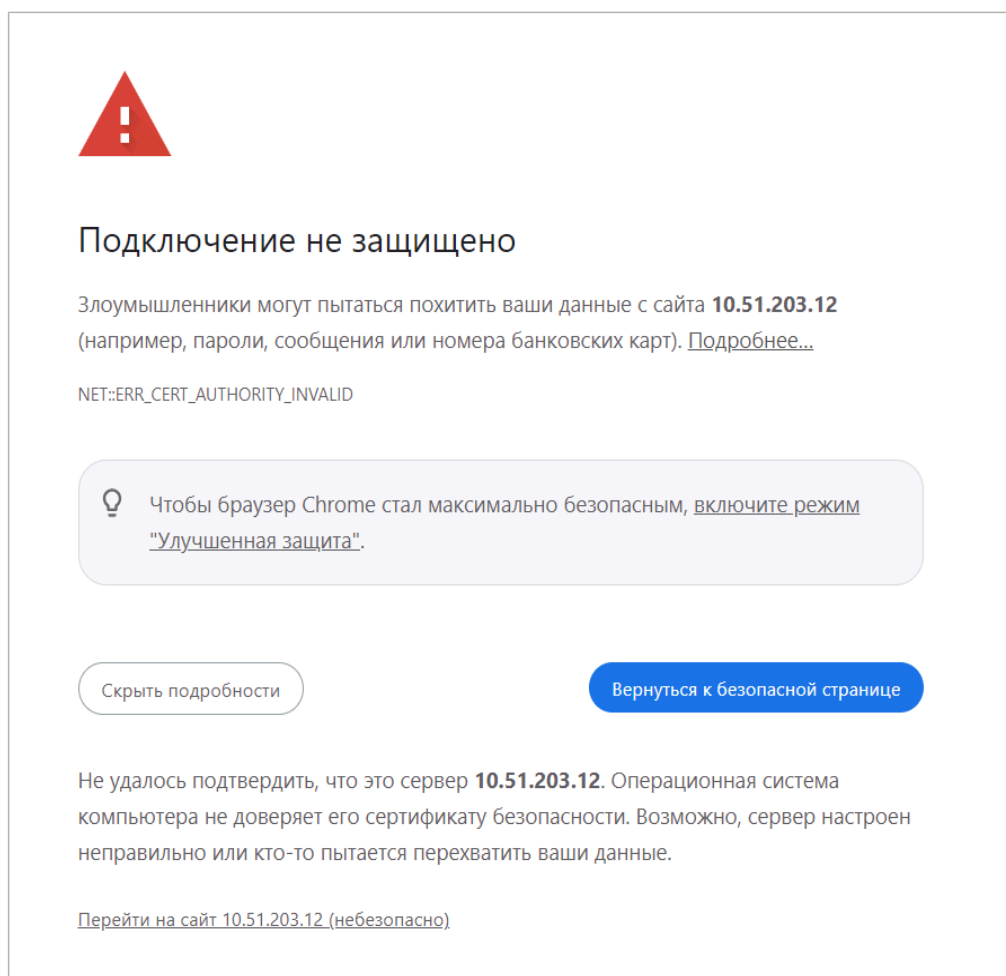


Рис. 3. Подключение к UDV NTA по HTTPS

► **Результат шага:** отобразится окно входа в веб-интерфейс UDV NTA.

- 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 900 секунд (15 минут).

Количество неудачных попыток и время блокировки регулируются администратором на странице [Парольная политика](#).

 **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.

См. также

[Настройка парольной политики](#)

2.1.2. Первоначальная настройка

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



Прим.:

Обязательными шагами являются только принятие лицензионного соглашения и настройка встроенной учетной записи. 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:
 - а. 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»

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

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

3. Импортируйте справочники. Для этого:

- Нажмите кнопку **Выбрать файл**.
- Выберите архив формата **.tar**, содержащий справочники, и нажмите кнопку **Открыть**.

**Внимание:**

Если результат импорта вас не устраивает или файл был выбран ошибочно, то можно сразу отменить импорт, нажав кнопку **Сбросить**. Импортировать справочники архивом или по отдельности можно после первоначальной настройки — см. раздел [«Импорт справочников из архива»](#).

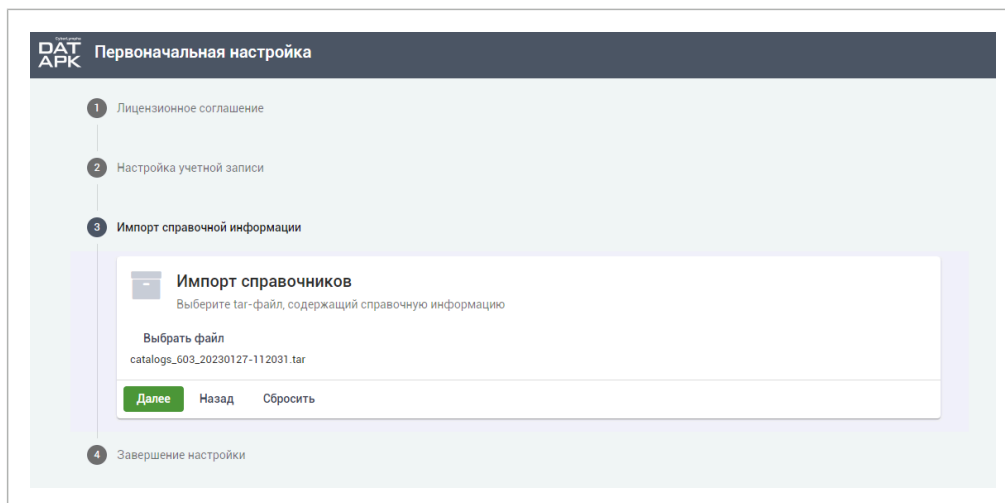


Рис. 6. Окно «Импорт справочников»

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

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

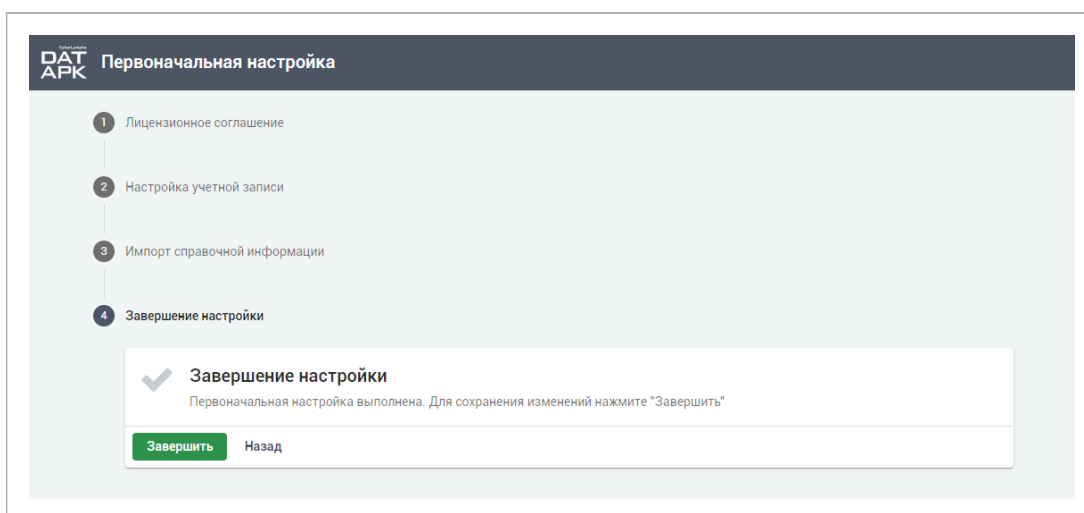


Рис. 7. Окно «Завершение настройки»

5. Войдите в веб-интерфейс Комплекса с новым логином и паролем.

► **Результат шага:** откроется страница **Статус защищенности**.

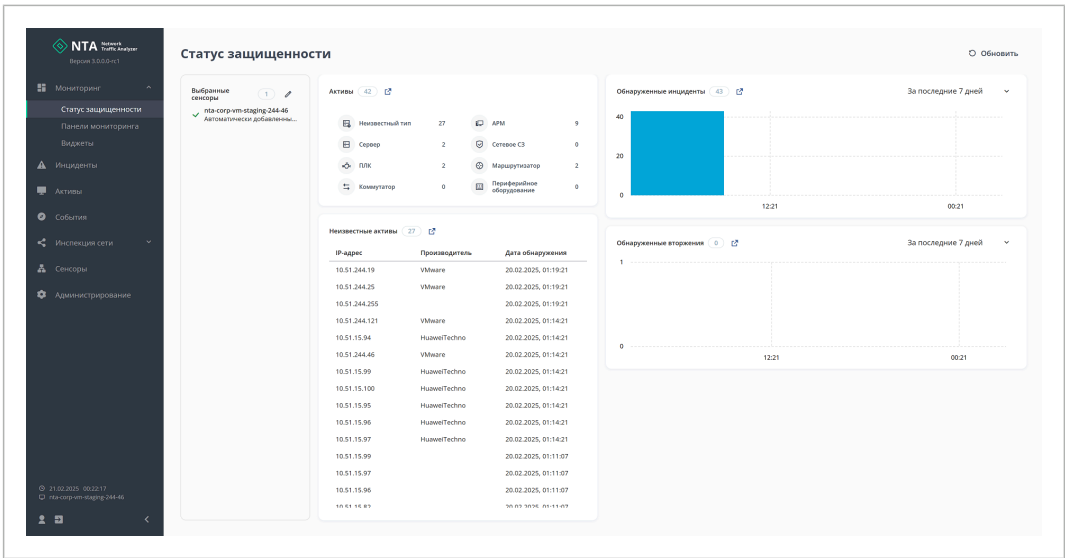


Рис. 8. Страница «Статус защищенности»

6. Если в правом верхнем углу отобразится ошибка: Непредвиденная ошибка. Перезапустить синхронизацию, нажмите на ссылку **Перезапустить синхронизацию** для перезапуска синхронизации сенсоров с Комплексом.

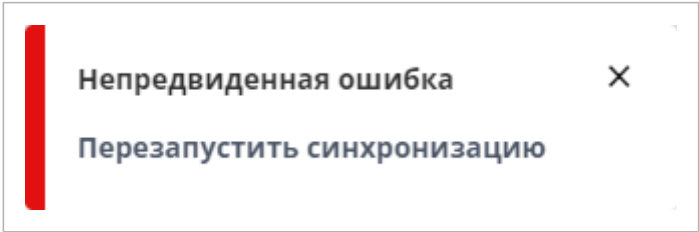


Рис. 9. Ошибка синхронизации сенсоров с Комплексом

2.2. Импорт справочников из архива

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



Прим.:

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 1. Справочники, доступные для импорта).

Табл. 1. Справочники, доступные для импорта

НАЗВАНИЕ СПРАВОЧНИКА		РАЗДЕЛ
События		
Правила разбора событий	Импорт правил разбора событий	

Табл. 1. Справочники, доступные для импорта

НАЗВАНИЕ СПРАВОЧНИКА	РАЗДЕЛ
Правила обогащений событий	Импорт правил обогащений событий
Схема событий	Импорт схемы событий
Элементы иерархии	
Иерархия меток активов	Импорт меток
Группы активов	
Корреляция событий	
Правила корреляции	Импорт правил корреляции
Схема корреляции	Импорт схемы корреляции
Политика корреляции	Импорт политики корреляции
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

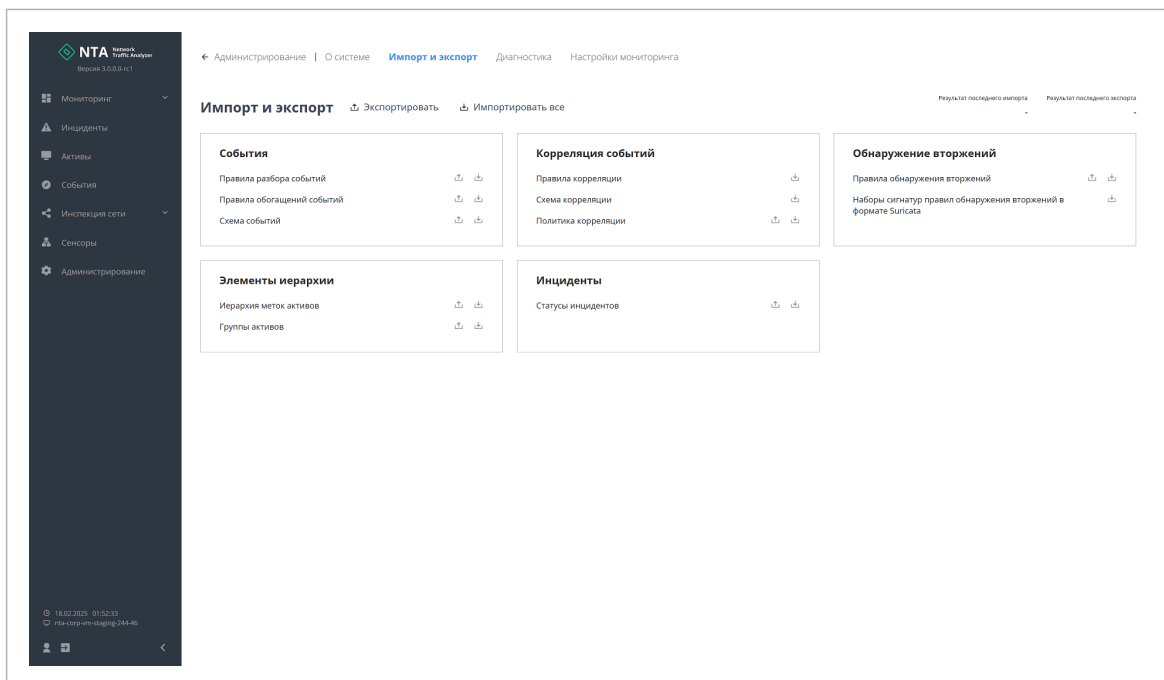


Рис. 10. Страница «Импорт и экспорт»

2.3. Настройка сенсоров

Настройка сенсоров выполняется на странице **Сенсоры** и включает в себя следующие действия:

- **Настройка контролируемой сети** для отображения активов и сессий, входящих в контролируемые сети.
- **Первичная настройка UDV NTA**, которая включает в себя управление списком распознаваемых протоколов и сетевых атак, настройку объемов хранимых дампов трафика и распознанных файлов.
- **Запуск обнаружения вторжений и синхронизация правил с сенсорами**

2.3.1. Настройка контролируемой сети

Настройка контролируемой сети необходима для отображения на странице **Активы** активов, IP-адреса которых входят в контролируемую сеть. 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:** откроется карточка выбранного сенсора.
3. В открывшейся панели в блоке **Контролируемая сеть** нажмите кнопку  (**Редактировать**).
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**).

▼ **Контролируемая сеть**

Адрес * 10.51.244.0/24 X

Адрес * 10.51.15.0/24 X

Адрес * 10.51.33.0/24 X

+ Добавить сеть

Применить Отменить

Рис. 11. Блок «Контролируемая сеть» в настройках сенсора

5. Нажмите кнопку **Применить**.

► **Результат шага:** Появится окно с предупреждением: При смене контролируемой сети активы, 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.

2.3.2. Первичная настройка UDV NTA

На странице **Сенсоры** для каждого сенсора доступны следующие настройки UDV NTA, которые рекомендуется выполнить перед началом работы:

- **Управление анализаторами трафика.**
- **Настройка хранения записей трафика** — включение или отключение записи на диск трафика, обнаруживаемого UDV NTA. При включении записи доступен выбор максимального объема диска, при достижении которого более ранние записи трафика будут удалены.
- **Настройка хранения обнаруженных файлов** — включение или отключение записи на диск файлов, которые обнаруживает UDV NTA в сетевом трафике. При включении записи доступен выбор максимального объема диска, при достижении которого более ранние хранимые файлы будут удалены.

Управление анализаторами трафика

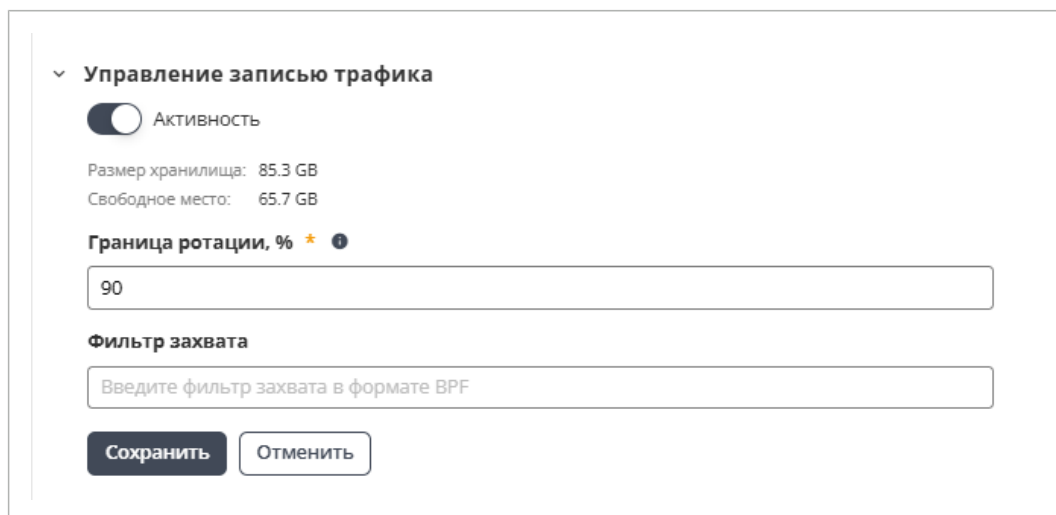
Для настройки списка протоколов и сетевых атак, которые будет распознавать сенсор UDV NTA:

1. Выберите сенсор на странице **Сенсоры**.
 - **Результат шага:** откроется карточка выбранного сенсора.
2. В карточке сенсора раскройте блок **Управление логированием**.
3. В открывшейся панели включите или выключите необходимые анализаторы с помощью переключателей: если переключатель в состоянии  — анализатор включен.

Настройка хранения записей трафика

Для настройки хранения записей трафика на сенсоре:

1. Выберите сенсор на странице **Сенсоры**.
 - **Результат шага:** откроется карточка выбранного сенсора.
2. В блоке **Управление записью трафика** нажмите кнопку  (**Редактировать**).
 - **Результат шага:** Откроется панель настроек **Управление записью трафика**.



Панель настроек «Управление записью трафика» содержит следующие элементы:

- Заголовок: **Управление записью трафика**
- Переключатель **Активность** (включен).
- Размер хранилища: 85.3 GB
- Свободное место: 65.7 GB
- Граница ротации, %  
 - Вводное поле со значением 90.
- Фильтр захвата
 - Вводное поле с подсказкой: Введите фильтр захвата в формате BPF.
- Кнопки: **Сохранить** и **Отменить**.

Рис. 12. Панель настроек «Управление записью трафика»

3. В открывшейся панели включите или выключите запись трафика с помощью переключателя **Активность**: если переключатель в состоянии  — запись будет включена.
4. Если на предыдущем шаге запись была включена, введите в поле **Граница ротации** максимальный объем диска для хранения трафика. Значение задается в процентах от 1 до 100.

**Внимание:**

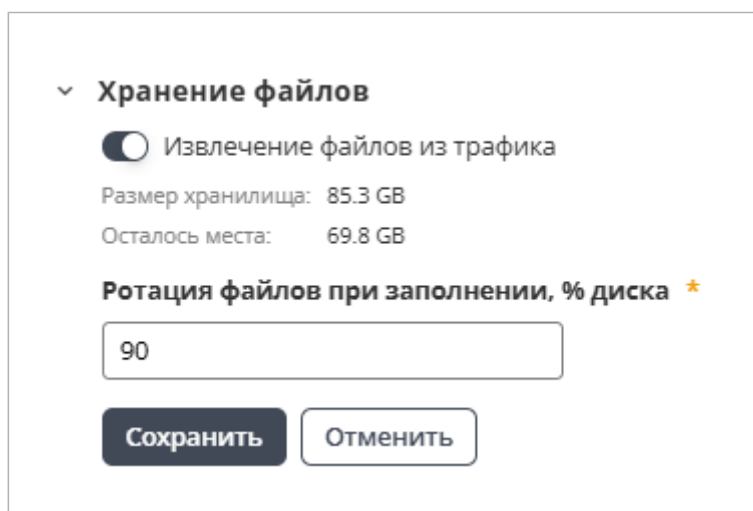
При достижении границ ротации более ранние записи трафика будут заменены новыми записями.

5. В поле **Фильтр захвата** введите параметры фильтра захвата трафика на языке фильтрации BPF .
6. Нажмите кнопку **Сохранить**.
 - **Результат шага:** если запись трафика включена, записи будут доступны для скачивания на вкладке **Пакеты** страницы **Инспекция сети** → **Сетевые соединения**. Подробнее см. инструкцию **Экспорт копии сетевого трафика**

Настройка хранения обнаруженных файлов

Для настройки хранения файлов на сенсоре:

1. Выберите сенсор на странице **Сенсоры**.
 - **Результат шага:** откроется карточка выбранного сенсора.
2. В блоке **Хранение файлов** нажмите кнопку  (**Редактировать**).
 - **Результат шага:** Откроется панель настроек **Хранение файлов**.



▼ **Хранение файлов**

☐ Извлечение файлов из трафика

Размер хранилища: 85.3 GB

Осталось места: 69.8 GB

Ротация файлов при заполнении, % диска ★

90

Сохранить **Отменить**

Рис. 13. Панель настроек «Хранение файлов»

3. В открывшейся панели включите или выключите запись файлов с помощью переключателя **Извлечение файлов из трафика**: если переключатель в состоянии  — запись будет включена.
4. Если на предыдущем шаге запись была включена, введите в поле **Ротация трафика при заполнении** максимальный объем диска для хранения файлов. Значение задается в процентах от 1 до 100.
5. Нажмите кнопку **Сохранить**.
 - **Результат шага:** если запись файлов включена, файлы будут доступны для скачивания на вкладке **Файлы** на странице **Инспекция сети** → **Сетевые соединения**. Подробнее см. инструкцию **Экспорт файлов, обнаруженных в сетевом трафике**.

2.3.3. Запуск обнаружения вторжений и синхронизация правил с сенсорами

Убедитесь, что в Комплексе на странице **Импорт и экспорт** импортированы правила обнаружения вторжений из архива при первоначальной настройке.

Если архив не был импортирован, для возможности обнаружения вторжений предварительно импортируйте правила обнаружения согласно одной из инструкций:

- [Импорт правил обнаружения вторжений в формате *.json](#)
- [Импорт правил обнаружения вторжений в формате *.rules](#)

После импорта правил обнаружения необходимо включить сервис обнаружения вторжений на сенсорах и передать на сенсоры 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:** откроется карточка выбранного сенсора.
3. В открывшейся панели включите или выключите службу обнаружения вторжений сенсора с помощью переключателя **Служба обнаружения вторжений**: если переключатель в состоянии  — служба включена.
4. Если служба обнаружения вторжений включена, перейдите на страницу [Администрирование](#) → [Сигнатурный анализ](#) → [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.

2.4. Настройка парольной политики

Для настройки единой парольной политики для всех пользователей:

1. Перейдите на страницу [Администрирование](#) → [Пользователи](#) → [Парольная политика](#).

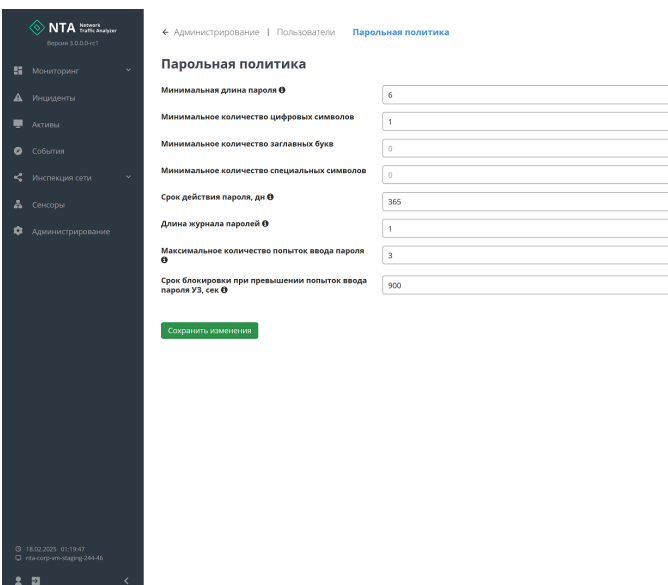


Рис. 14. Страница «Парольная политика»

2. Настройте следующие параметры парольной политики:

- общее минимальное количество символов, которое должен содержать пароль;



Прим.:

Доступен ввод значений в диапазоне от 6 до 14. 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);



Прим.:

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;



Прим.:

Доступен ввод значений в диапазоне от 1 до 24.

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



Прим.:

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.



Прим.:

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).

2.5. Изменение сведений о Комплексе и сенсорах

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.

The screenshot shows the 'О системе' (About System) page in the NTA CyberLympha interface. The page is divided into two main sections: 'Сведения о Комплексе' (System Information) and 'Информация об изготовителе' (Manufacturer Information).

Сведения о Комплексе

- Наименование**: nta-corp-ym-staging-244-46
- Описание**: необходимо заполнить
- Эксплуатирующая организация**: необходимо заполнить
- Место установки**: необходимо заполнить

Информация об изготовителе

- CyberLympha DATAPK
- Разработчик: ООО «СайберЛимфа»
- www.CyberLympha.ru
- Версия: 3.0.0.0-rc1

Buttons: [Сохранить](#) (Save), [Отмена](#) (Cancel)

Рис. 15. Страница «О системе»

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

Изменение сведений о сенсорах, подключенных к Комплексу

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

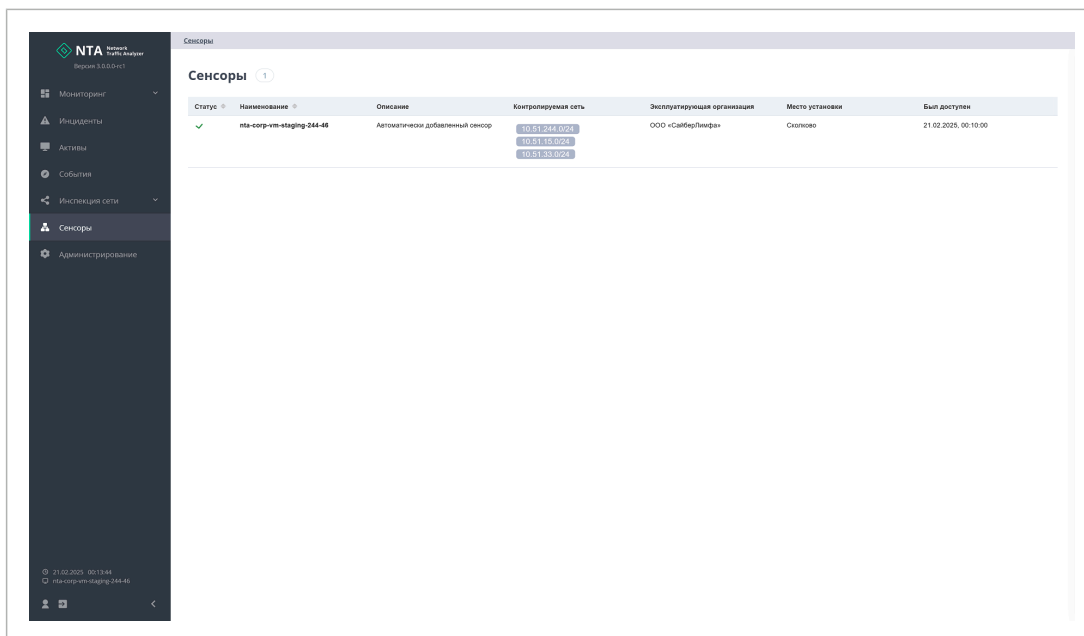


Рис. 16. Страница «Сенсоры»

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

nta-corp-vm-staging-244-46

Описание

Эксплуатирующая организация

Место установки

Рис. 17. Блок редактирования информации о сенсоре

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

2.6. 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 UDV NTA. Подробнее см. в разделе «[Проверка работоспособности UDV NTA](#)».

2.6.1. Проверка работоспособности системы передачи данных по иерархии

Для проверки работоспособности системы передачи данных по иерархии выполните следующие действия:

1. На Management перейдите на страницу [Сенсоры](#).
2. Выберите сенсор.
 - **Результат шага:** появится боковая панель с описанием и настройками выбранного сенсора.
3. Просмотрите статусы синхронизации настроек и получения данных с сенсора.

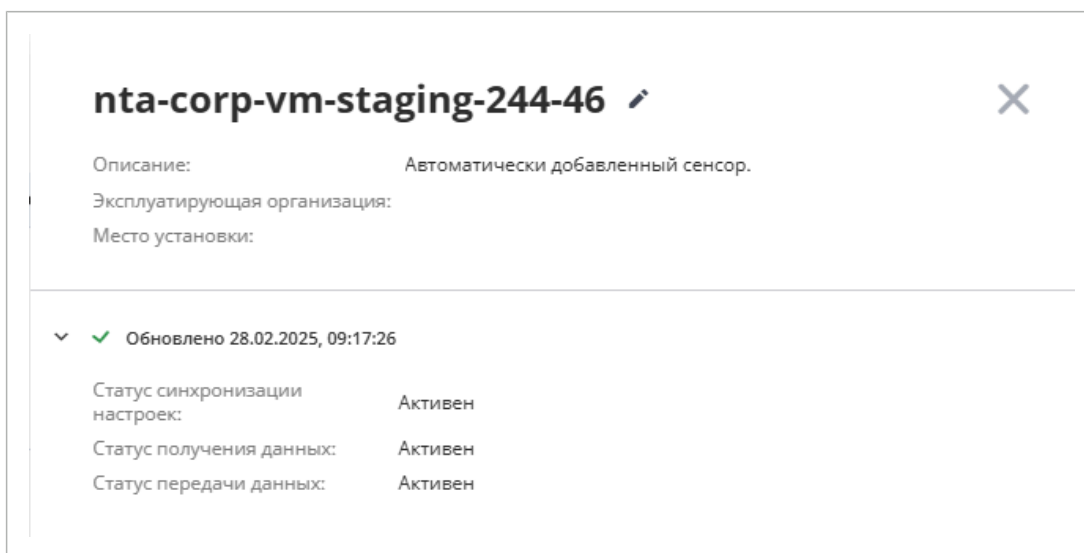


Рис. 18. Статусы исправной синхронизации настроек и получения данных с сенсора

2.6.2. Проверка работоспособности UDV NTA

Для проверки работоспособности UDV NTA:

1. Перейдите на страницу [Инспекция сети](#) → [Сетевые соединения](#).
 - **Результат шага:** откроется вкладка [Сессии](#).

Инциденты сети > Сетевые соединения

Сетевые соединения 4748 Сессии Пакеты Файлы Протоколы

Нажмите ввести поисковый запрос

Обновлено: 18.02.2025 00:00:00.000 - 18.02.2025 23:59:59.999 Сенсор: Вкл Активность: Вкл Протоколы: Вкл IP-адрес отправителя: Вкл IP-адрес получателя: Вкл + Очистить

Обновлено	Обнаружено	Сенсор	Состояние	UID сессии	Протоколы	Транспортный пр...	IP-адрес отправит...	Порт отправит...	IP-адрес получе...
18.02.2025, 11:35:54	18.02.2025, 11:32:54	nta-corporate-staging...	S0	● C2b5n2u03Nmp...	NBNS	udp	10.51.244.121	137	10.51.244.255
18.02.2025, 11:35:51	18.02.2025, 11:33:51	nta-corporate-staging...	S1	● CkRfP24G0V0b5...	SSL	tcp	10.199.0.23	62426	10.51.244.46
18.02.2025, 11:35:51	18.02.2025, 11:32:51	nta-corporate-staging...	S0	● CkVnH2wmt3C...		udp	10.51.244.121	138	10.51.244.255
18.02.2025, 11:35:50	18.02.2025, 11:35:50	nta-corporate-staging...	S0	● CkA9K0Cvdyb2Bj	NBNS	udp	10.51.244.19	137	10.51.244.255
18.02.2025, 11:35:50	18.02.2025, 11:35:40	nta-corporate-staging...	SF	● CkzrCj7BnqR04...	DNS	udp	10.51.244.46	55119	10.55.10.10
18.02.2025, 11:35:45	18.02.2025, 11:35:40	nta-corporate-staging...	SF	● CkZbZu3v5N7aY...	SSL	tcp	10.199.0.23	55017	10.51.244.46
18.02.2025, 11:35:44	18.02.2025, 11:33:22	nta-corporate-staging...	SF	● CkPQZ2Wdyk7Bj	SSL	tcp	10.199.0.23	62387	10.51.244.46
18.02.2025, 11:35:44	18.02.2025, 11:33:25	nta-corporate-staging...	SF	● CkN4A2gZpC0p...	SSL	tcp	10.199.0.23	62410	10.51.244.46
18.02.2025, 11:35:44	18.02.2025, 11:33:25	nta-corporate-staging...	SF	● CkE1C1tWkHk6W...	SSL	tcp	10.199.0.23	62413	10.51.244.46
18.02.2025, 11:35:44	18.02.2025, 11:33:25	nta-corporate-staging...	SF	● CkERZP7nRbqM...	SSL	tcp	10.199.0.23	62411	10.51.244.46
18.02.2025, 11:35:44	18.02.2025, 11:33:25	nta-corporate-staging...	SF	● CkM8ngl6OFR79	SSL	tcp	10.199.0.23	62412	10.51.244.46
18.02.2025, 11:35:41	18.02.2025, 01:00:32	nta-corporate-staging...	S0	● CkGQMT6w6Bq...	NBNS	udp	10.51.244.16	137	10.51.244.255
18.02.2025, 11:35:33	18.02.2025, 11:34:33	nta-corporate-staging...	SF	● CkVnH2wmt3C...	NTP	udp	10.51.244.46	33246	217.170.87.229
18.02.2025, 11:35:25	18.02.2025, 11:33:25	nta-corporate-staging...	S1	● CkN7Gz0bANB8W	SSL	tcp	10.199.0.23	62414	10.51.244.46
18.02.2025, 11:35:00	18.02.2025, 11:30:00	nta-corporate-staging...	S1	● CkVnH2wmt3C...	DCE_RPC NTLM	tcp	10.51.244.46	52788	10.51.244.26
18.02.2025, 11:35:00	18.02.2025, 11:34:00	nta-corporate-staging...	S1	● CkVnH2wmt3C...	DCE_RPC NTLM	tcp	10.51.244.46	42118	10.51.244.26
18.02.2025, 11:35:00	18.02.2025, 11:32:00	nta-corporate-staging...	S1	● CkVnH2wmt3C...	DCE_RPC NTLM	tcp	10.51.244.46	54268	10.51.201.146
18.02.2025, 11:35:00	18.02.2025, 11:34:00	nta-corporate-staging...	S1	● CkVnH2wmt3C...	DCE_RPC NTLM	tcp	10.51.244.46	52170	10.51.201.146
18.02.2025, 11:34:52	18.02.2025, 11:31:52	nta-corporate-staging...	S0	● CkZbZu3v5N7aY...		udp	10.51.244.16	138	10.51.244.255
18.02.2025, 11:34:24	18.02.2025, 11:31:24	nta-corporate-staging...	S0	● CkVnH2wmt3C...		udp	10.51.244.26	138	10.51.244.255

Рис. 19. Страница «Сетевые соединения»

- Сбросьте фильтр **Время обнаружения**.
- Убедитесь, что UDV NTA обнаруживает новые сессии: в столбце **Время обнаружения** есть записи с текущим временем.
- Убедитесь, что UDV NTA отображает активные сессии: в столбце **Сессия (UID)** активные сессии имеют иконку зеленого цвета.

3. Инспекция сети

В этом разделе:

1. Управление сетевыми соединениями

2. Служба обнаружения вторжений

В UDV NTA для отслеживания сетевых взаимодействий активов в домашней 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 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**.

3.1. Управление сетевыми соединениями

В этом разделе:

- Просмотр сессий и пакетов
- Поиск по списку сессий
- Фильтрация списка сессий
- Создание единого виртуального интерфейса (bond) для прослушивания трафика с нескольких физических интерфейсов
- Экспорт копии сетевого трафика
- Экспорт файлов, обнаруженных в сетевом трафике

3.1.1. 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**.

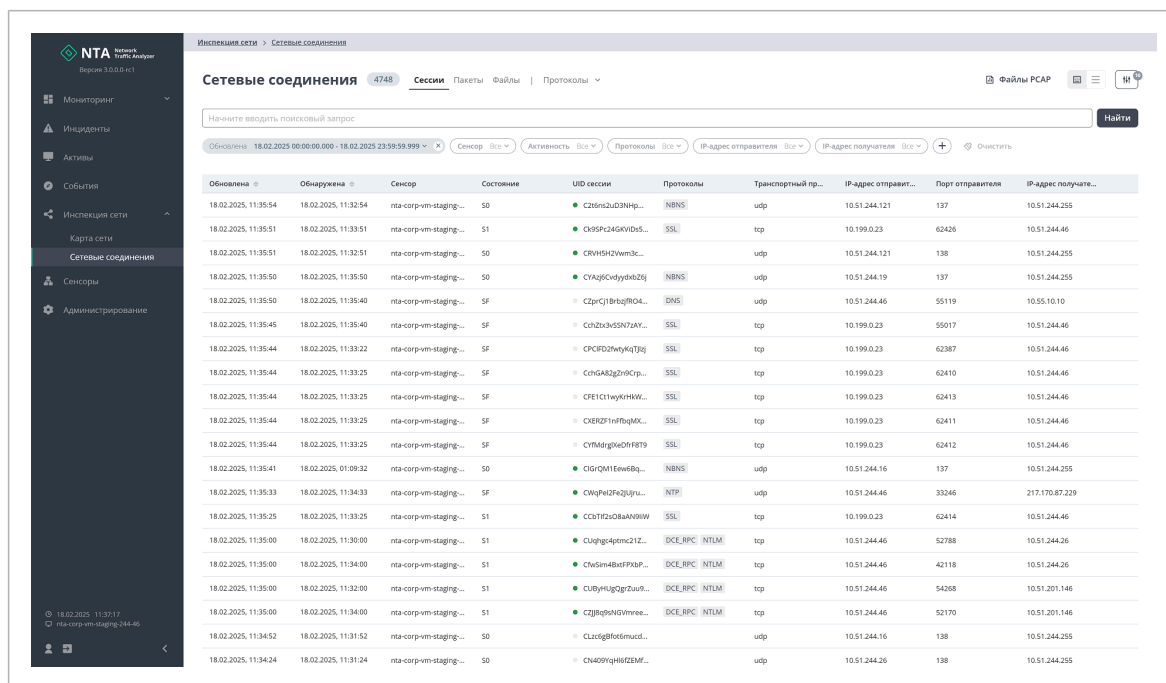
Для навигации по списку сессий используется область фильтров над таблицей. По умолчанию отображаются сессии, обнаруженные за текущие сутки.

**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**.



Обновлена	Обнаружена	Сенсор	Состояние	UID сессии	Протоколы	Транспортный пр...	IP-адрес отправит...	Порт отправителя	IP-адрес получате...
18.02.2025, 11:35:54	18.02.2025, 11:32:54	nta-corp-vim-staging...	S0	C26ns2u3DhHr...	NBNS	udp	10.51.244.121	137	10.51.244.255
18.02.2025, 11:35:51	18.02.2025, 11:33:51	nta-corp-vim-staging...	S1	CK9SP24GKVDb5...	SSL	tcp	10.199.0.23	62426	10.51.244.46
18.02.2025, 11:35:51	18.02.2025, 11:32:51	nta-corp-vim-staging...	S0	CRVH924Wm3c...		udp	10.51.244.121	138	10.51.244.255
18.02.2025, 11:35:50	18.02.2025, 11:35:50	nta-corp-vim-staging...	S0	CYAG5Cdydhb2q...	NBNS	udp	10.51.244.19	137	10.51.244.255
18.02.2025, 11:35:50	18.02.2025, 11:35:40	nta-corp-vim-staging...	SF	C2prCj1BrbzjR04...	DNS	udp	10.51.244.46	55119	10.55.10.10
18.02.2025, 11:35:45	18.02.2025, 11:35:40	nta-corp-vim-staging...	SF	CcnZx3x5SN7AY...	SSL	tcp	10.199.0.23	55017	10.51.244.46
18.02.2025, 11:35:44	18.02.2025, 11:33:22	nta-corp-vim-staging...	SF	CPCFD2fWeykTjR...	SSL	tcp	10.199.0.23	62387	10.51.244.46
18.02.2025, 11:35:44	18.02.2025, 11:33:25	nta-corp-vim-staging...	SF	CcnZx3x5SN7AY...	SSL	tcp	10.199.0.23	62410	10.51.244.46
18.02.2025, 11:35:44	18.02.2025, 11:33:25	nta-corp-vim-staging...	SF	CPE1C1wykHwK...	SSL	tcp	10.199.0.23	62413	10.51.244.46
18.02.2025, 11:35:44	18.02.2025, 11:33:25	nta-corp-vim-staging...	SF	CXERZFIrRqMC...	SSL	tcp	10.199.0.23	62411	10.51.244.46
18.02.2025, 11:35:44	18.02.2025, 11:33:25	nta-corp-vim-staging...	SF	CYMDrg4x6ofrR9...	SSL	tcp	10.199.0.23	62412	10.51.244.46
18.02.2025, 11:35:41	18.02.2025, 01:09:32	nta-corp-vim-staging...	S0	CIGQM1Eew6Bq...	NBNS	udp	10.51.244.16	137	10.51.244.255
18.02.2025, 11:35:33	18.02.2025, 11:34:33	nta-corp-vim-staging...	SF	CWqPeI2Fe2Jyru...	NTP	udp	10.51.244.46	33246	217.170.87.229
18.02.2025, 11:35:25	18.02.2025, 11:33:25	nta-corp-vim-staging...	S1	CC0Tf2a0BAN0W...	SSL	tcp	10.199.0.23	62414	10.51.244.46
18.02.2025, 11:35:00	18.02.2025, 11:30:00	nta-corp-vim-staging...	S1	CUghg4pmc2IZ...	DCE_RPC, NTLM	tcp	10.51.244.46	52788	10.51.244.26
18.02.2025, 11:35:00	18.02.2025, 11:34:00	nta-corp-vim-staging...	S1	CNeSim4BxFPkP...	DCE_RPC, NTLM	tcp	10.51.244.46	42118	10.51.244.26
18.02.2025, 11:35:00	18.02.2025, 11:32:00	nta-corp-vim-staging...	S1	CUBhNug2gZuu9...	DCE_RPC, NTLM	tcp	10.51.244.46	54268	10.51.201.146
18.02.2025, 11:35:00	18.02.2025, 11:34:00	nta-corp-vim-staging...	S1	CZJlR6pN6Vmee...	DCE_RPC, NTLM	tcp	10.51.244.46	52170	10.51.201.146
18.02.2025, 11:34:52	18.02.2025, 11:31:52	nta-corp-vim-staging...	S0	CLx0gBf06mud...		udp	10.51.244.16	138	10.51.244.255
18.02.2025, 11:34:24	18.02.2025, 11:31:24	nta-corp-vim-staging...	S0	CN40YqH0ZEMF...		udp	10.51.244.26	138	10.51.244.255

Рис. 20. Вкладка «Сессии» на странице «Сетевые соединения»

UDV NTA 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 UDV NTA. 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 UDV NTA для поиска информации, связанной с сессией.

Обнаружение протоколов в UDV NTA возможно в двух режимах:

- индикации;
- подробного анализа.

UDV NTA обнаруживает большинство протоколов в пакетах в режиме индикации — это значит, что UDV NTA отображает наименование протокола без дополнительной информации о содержании полей этого протокола.

Протоколы, обнаруживаемые в режиме индикации, можно увидеть только в столбце **Протоколы** вкладки **Сессии** и в поле **Протоколы** карточки сессии.



Подсказка:

Описание всех сетевых протоколов, обнаруживаемых UDV NTA в режиме индикации, вы можете найти в разделе «**Протоколы, обнаруживаемые UDV NTA в режиме индикации**».

Для некоторых протоколов прикладного уровня UDV NTA 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

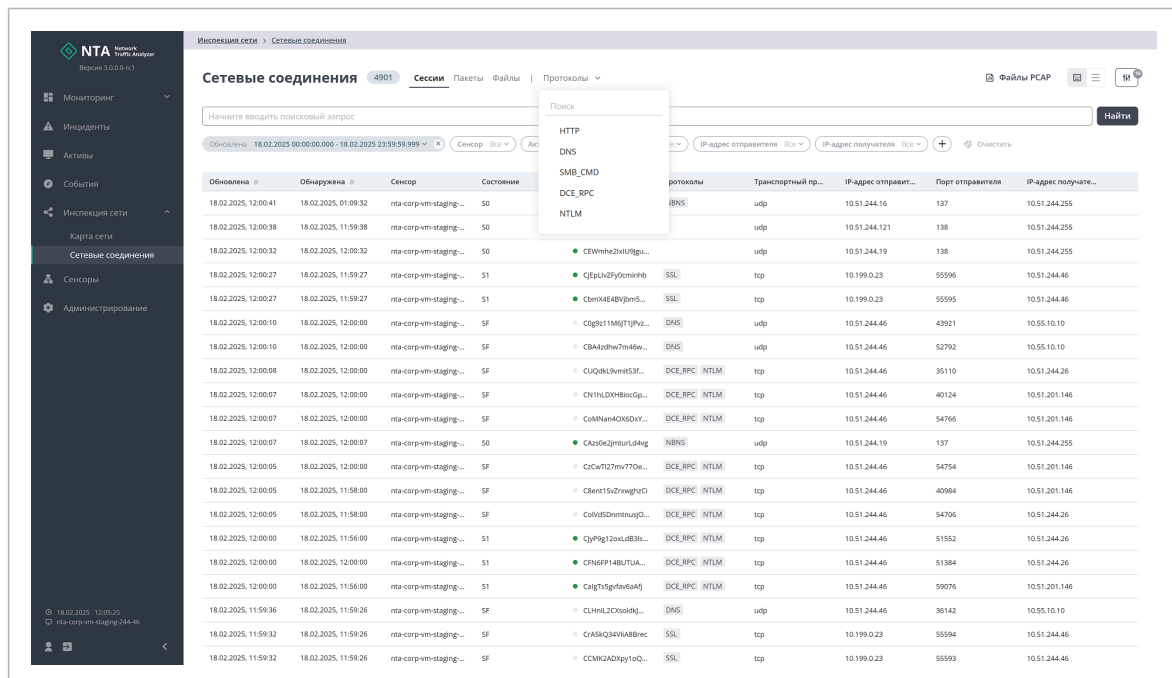


Рис. 21. Группа вкладок «Протоколы» на странице «Сетевые соединения»

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**.

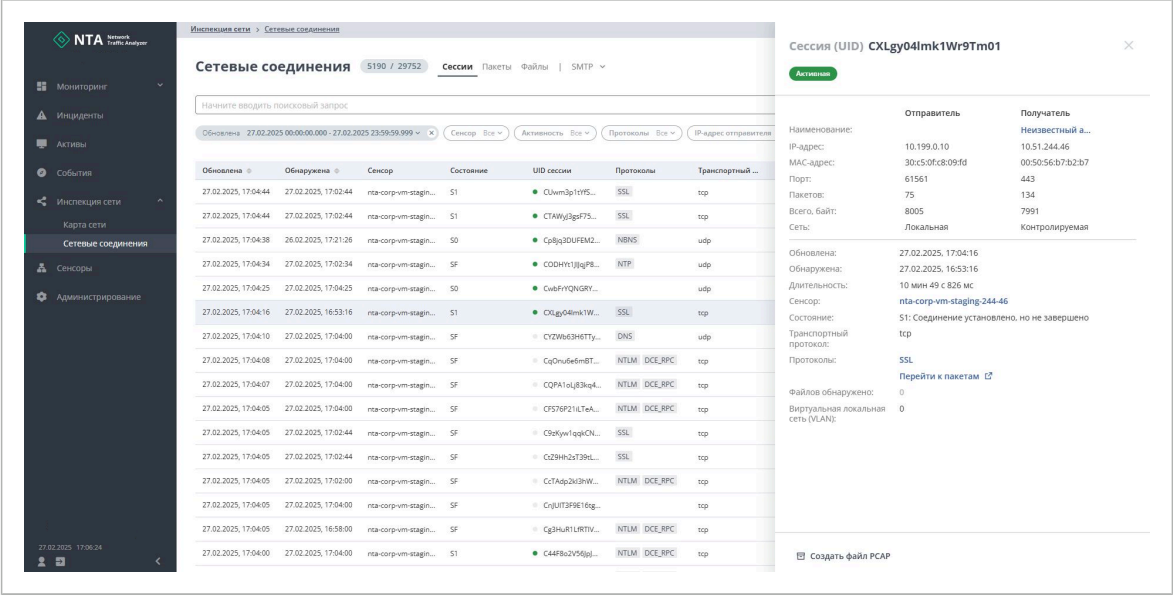


Рис. 22. Карточка сессии

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.

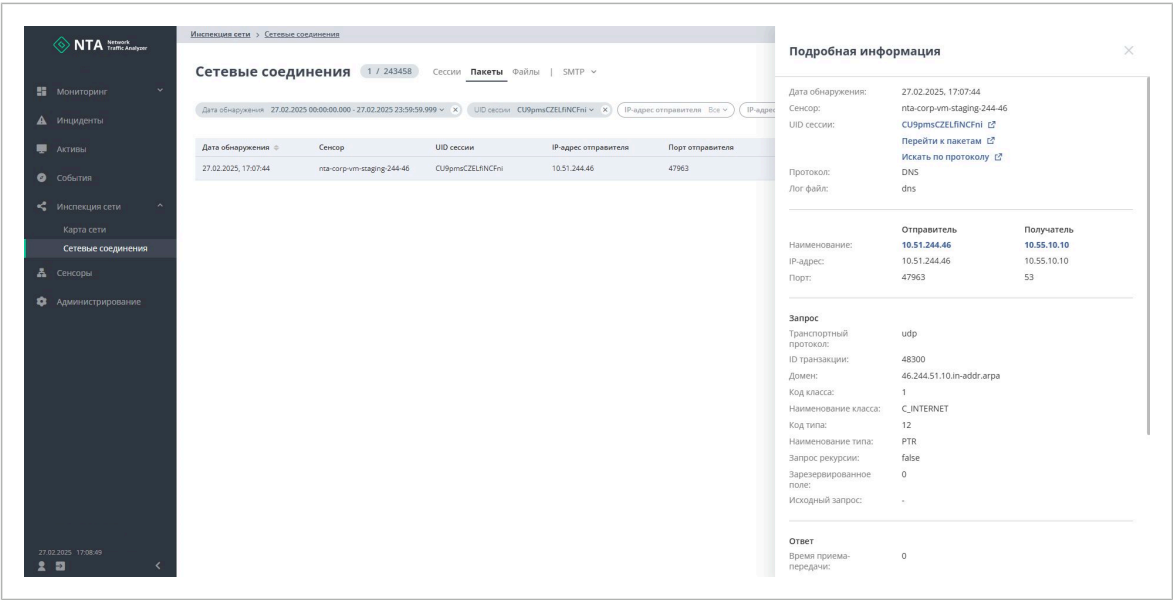


Рис. 23. Подробная информация о выбранных пакетах сессии на вкладке Пакеты

На вкладке **Пакеты** для навигации по записям используется область фильтров над таблицей. Для настройки отображения столбцов используется кнопка  в верхнем правом углу.

Сенсоры UDV NTA 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 UDV NTA**».

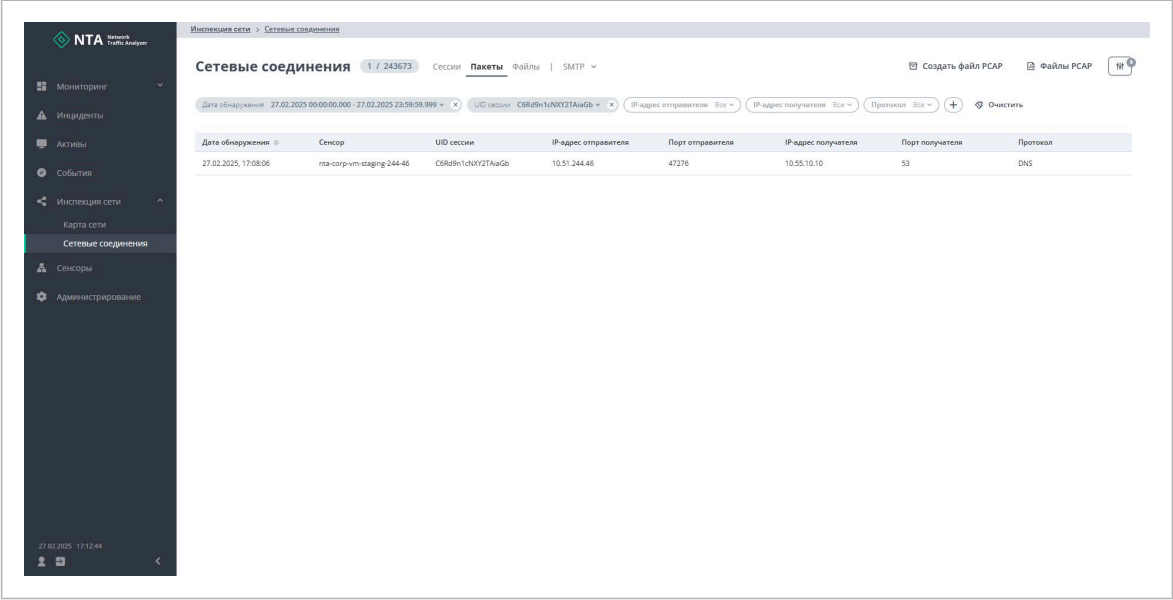


Рис. 24. Пакеты сессии на вкладке «Пакеты»

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**.

NTA

Версия 3.0.0.0-rc1

Мониторинг

Инциденты

Активы

События

Инспекция сети

Карта сети

Сетевые соединения

Сенсоры

Администрирование

Инспекция сети > Сетевые соединения

Сетевые соединения 170 Сессии Пакеты Файлы SMB_CMD

Время обнаружения: 24.02.2025 00:00:00.000 - 24.02.2025 23:59:59.999

UID Все IP-адрес отправителя Все IP-адрес получателя + Очистить

Время обнаружения	Сенсор	UID	Отправитель	IP-адрес о...	Порт отпр...	Получатель	IP-адрес п...	Порт полу...	Протокол	command	sub_comm...	argument	status
24.02.2025, 15:37:01	datapk-vm-d...	CK7vH32gl...	10.51.244.3	10.51.244.3	51506	10.51.244.16	10.51.244.16	445	smb_cmd	LOGOFF			USER_SESSIO...
24.02.2025, 15:37:01	datapk-vm-d...	CK7vH32gl...	10.51.244.3	10.51.244.3	51506	10.51.244.16	10.51.244.16	445	smb_cmd	LOGOFF			SUCCESS
24.02.2025, 15:37:01	datapk-vm-d...	CK7vH32gl...	10.51.244.3	10.51.244.3	51506	10.51.244.16	10.51.244.16	445	smb_cmd	TREE_DISCO...			SUCCESS
24.02.2025, 15:37:01	datapk-vm-d...	CK7vH32gl...	10.51.244.3	10.51.244.3	51506	10.51.244.16	10.51.244.16	445	smb_cmd	READ			SUCCESS
24.02.2025, 15:37:01	datapk-vm-d...	CK7vH32gl...	10.51.244.3	10.51.244.3	51506	10.51.244.16	10.51.244.16	445	smb_cmd	WRITE			SUCCESS
24.02.2025, 15:37:01	datapk-vm-d...	CK7vH32gl...	10.51.244.3	10.51.244.3	51506	10.51.244.16	10.51.244.16	445	smb_cmd	READ			SUCCESS
24.02.2025, 15:37:01	datapk-vm-d...	CK7vH32gl...	10.51.244.3	10.51.244.3	51506	10.51.244.16	10.51.244.16	445	smb_cmd	WRITE			SUCCESS
24.02.2025, 15:37:01	datapk-vm-d...	CK7vH32gl...	10.51.244.3	10.51.244.3	51506	10.51.244.16	10.51.244.16	445	smb_cmd	READ			SUCCESS
24.02.2025, 15:37:01	datapk-vm-d...	CK7vH32gl...	10.51.244.3	10.51.244.3	51506	10.51.244.16	10.51.244.16	445	smb_cmd	WRITE			SUCCESS
24.02.2025, 15:37:01	datapk-vm-d...	CK7vH32gl...	10.51.244.3	10.51.244.3	51506	10.51.244.16	10.51.244.16	445	smb_cmd	READ			SUCCESS
24.02.2025, 15:37:01	datapk-vm-d...	CK7vH32gl...	10.51.244.3	10.51.244.3	51506	10.51.244.16	10.51.244.16	445	smb_cmd	WRITE			SUCCESS
24.02.2025, 15:37:01	datapk-vm-d...	CK7vH32gl...	10.51.244.3	10.51.244.3	51506	10.51.244.16	10.51.244.16	445	smb_cmd	CREATE			SUCCESS
24.02.2025, 15:37:01	datapk-vm-d...	CK7vH32gl...	10.51.244.3	10.51.244.3	51506	10.51.244.16	10.51.244.16	445	smb_cmd	TREE_CONNE...	\\10.51.244.1...		SUCCESS
24.02.2025, 15:37:01	datapk-vm-d...	CK7vH32gl...	10.51.244.3	10.51.244.3	51506	10.51.244.16	10.51.244.16	445	smb_cmd	SESSION_SET...			SUCCESS
24.02.2025, 15:37:01	datapk-vm-d...	CK7vH32gl...	10.51.244.3	10.51.244.3	51506	10.51.244.16	10.51.244.16	445	smb_cmd	NEGOTIATE...			SUCCESS
24.02.2025, 15:37:01	datapk-vm-d...	Cae2761yuv3...	10.51.244.3	10.51.244.3	51498	10.51.244.16	10.51.244.16	445	smb_cmd	LOGOFF			USER_SESSIO...
24.02.2025, 15:37:01	datapk-vm-d...	Cae2761yuv3...	10.51.244.3	10.51.244.3	51498	10.51.244.16	10.51.244.16	445	smb_cmd	LOGOFF			SUCCESS
24.02.2025, 15:37:01	datapk-vm-d...	Cae2761yuv3...	10.51.244.3	10.51.244.3	51498	10.51.244.16	10.51.244.16	445	smb_cmd	TREE_DISCO...			SUCCESS
24.02.2025, 15:37:01	datapk-vm-d...	Cae2761yuv3...	10.51.244.3	10.51.244.3	51498	10.51.244.16	10.51.244.16	445	smb_cmd	READ			SUCCESS
24.02.2025, 15:37:01	datapk-vm-d...	Cae2761yuv3...	10.51.244.3	10.51.244.3	51498	10.51.244.16	10.51.244.16	445	smb_cmd	READ			SUCCESS

Рис. 25. 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 ручную фильтр **Обновлена**.

При нажатии на запись о пакетах открывается карточка с той же информацией о пакетах, которую можно просматривать в карточке на вкладке **Пакеты**.

3.1.2. 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.

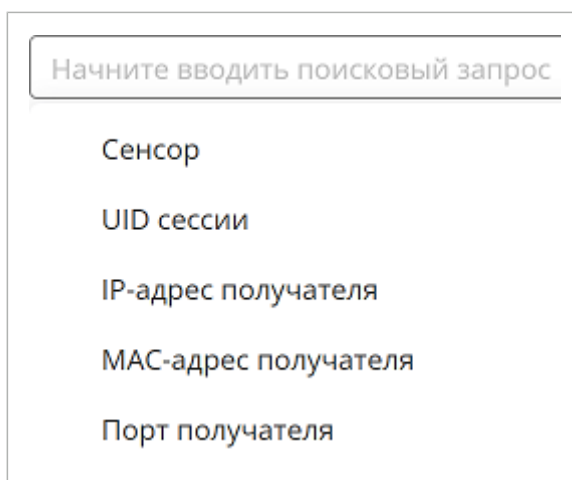


Рис. 26. Список доступных параметров сессии

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.

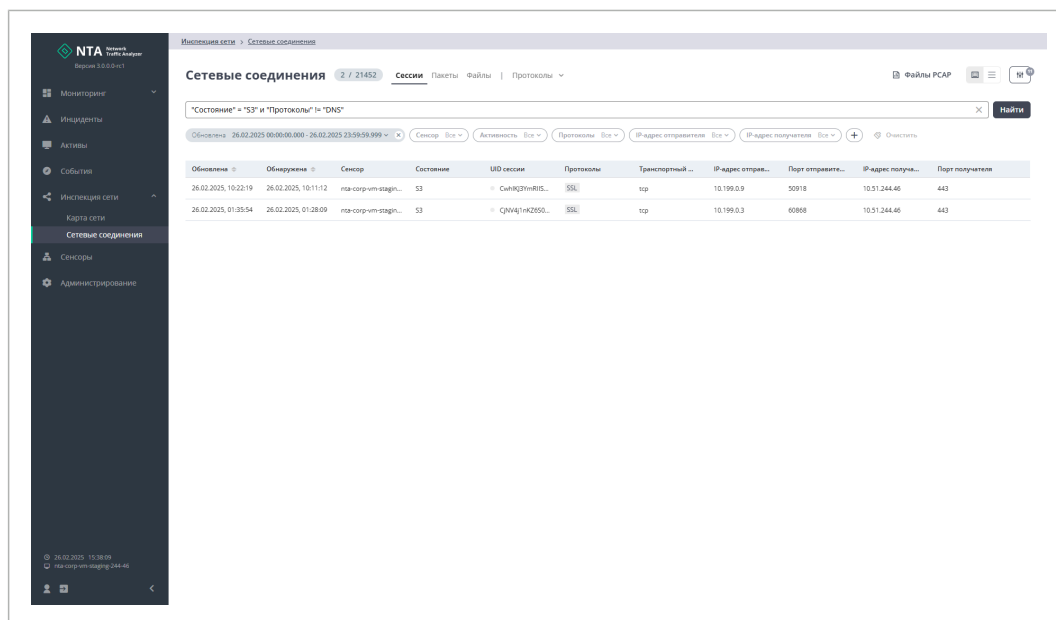


Рис. 27. Отображение результатов поиска в строке поиска на вкладке «Сессии»

3.1.3. 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.

3.1.4. 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.

Убедитесь, что на сенсорах включено сохранение копии трафика — подробнее см. инструкцию «[Первичная настройка UDV NTA](#)».

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:
 - а. 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.

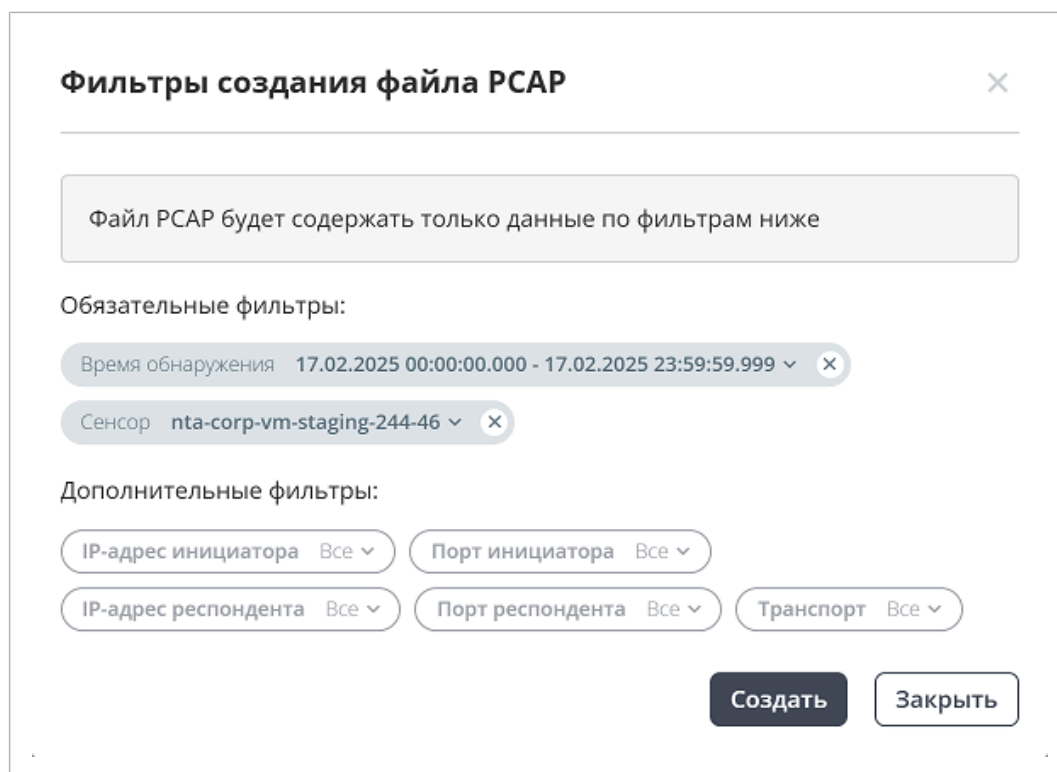


Рис. 28. Окно «Фильтры создания файла PCAP»

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 экспортируемого файла и нажмите кнопку **Сохранить**.

► **Результат шага:** файл `traffic_[дата_и_время].pcap` будет загружен на компьютер.

3.1.5. Экспорт файлов, обнаруженных в сетевом трафике

Убедитесь, что на сенсорах включено сохранение файлов из трафика — подробнее см. инструкцию «Первичная настройка UDV NTA».

Экспорт одного файла, обнаруженного в рамках сессии

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**.

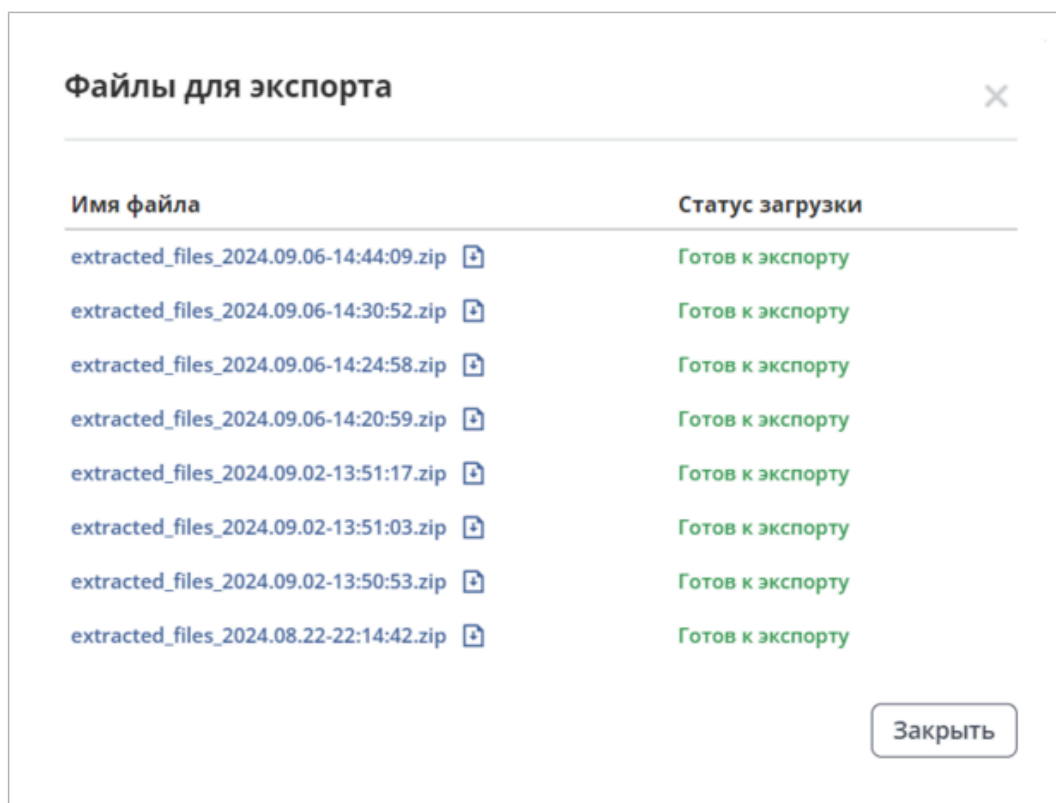


Рис. 29. Окно «Файлы для экспорта»

- 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](#)».

- В открывшемся окне укажите расположение экспортируемого файла 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.

Экспорт нескольких файлов

Для экспорта нескольких файлов со страницы **Файлы**:

- При необходимости отфильтруйте список всех обнаруженных файлов на странице **Файлы**.
- Установите чекбоксы слева от файлов, которые нужно экспортировать.
- 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.
- 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**.

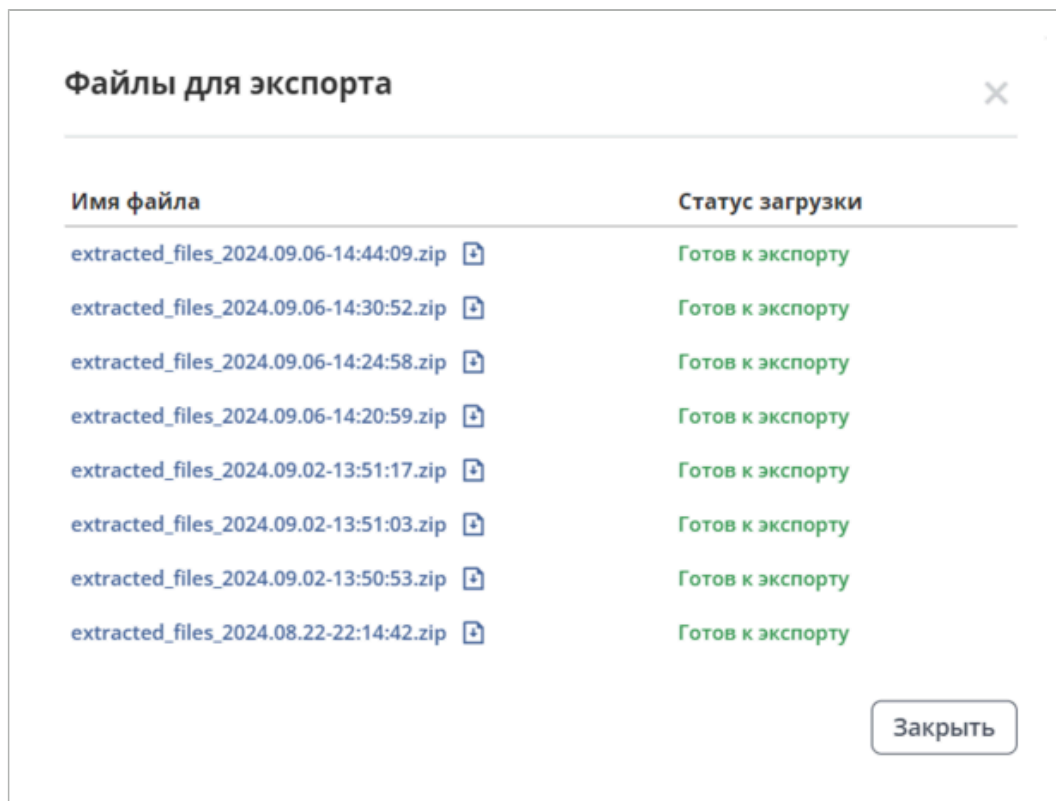


Рис. 30. Окно «Файлы для экспорта»

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 экспортируемого файла 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.

3.2. 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

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

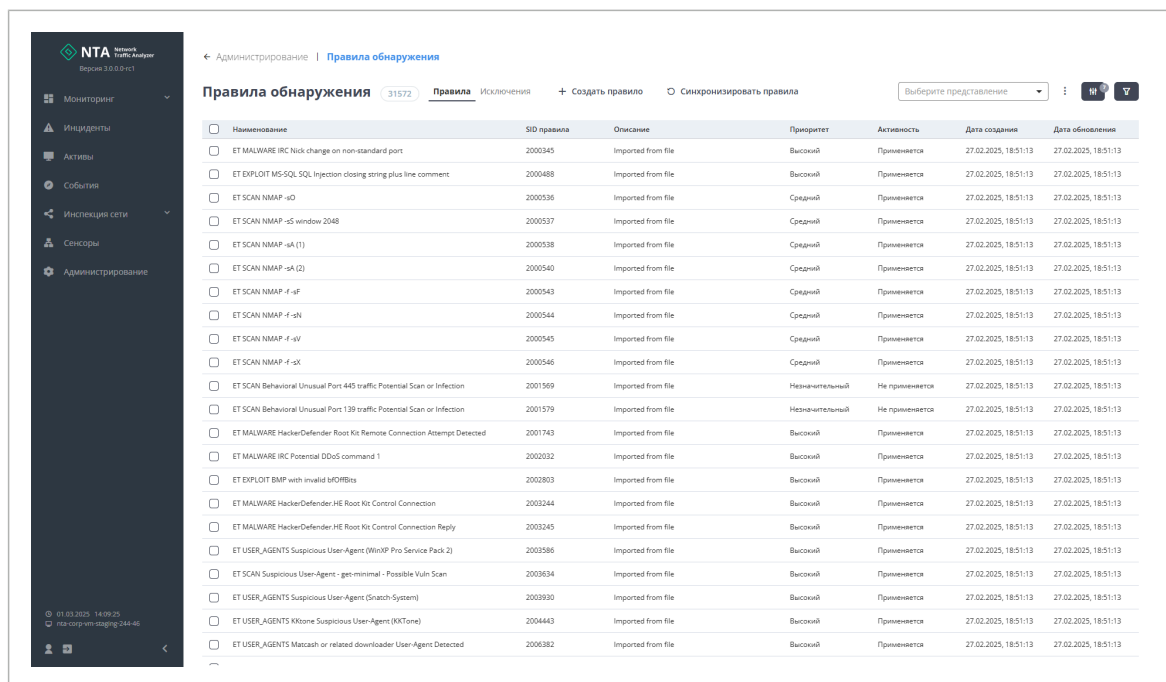


Рис. 31. Страница «Обнаружение вторжений»

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:

```
# 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](#)».

3.2.1. Создание правил обнаружения вторжений

Для создания правил обнаружения в веб-интерфейсе Комплекса.

1. Перейдите на страницу [Администрирование](#) → [Сигнатурный анализ](#) → [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.

- чекбокс **Активность** для активации правила.

Создание правила обнаружения вторжений

Наименование *

Описание

Условие *

☒ Активность

Создать

Отменить

Рис. 32. Окно «Создание правила обнаружения вторжения»

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

3.2.2. Управление службой обнаружения вторжений

Службу обнаружения вторжений можно остановить и запустить на сенсорах. Правила службы обнаружения вторжений доступны для редактирования после создания, также возможен запуск и остановка всех доступных правил. После изменения правила необходимо синхронизировать с сенсорами.

- Для запуска или остановки службы на сенсорах:
 - Перейдите на страницу [Сенсоры](#).
 - Нажмите на строку с сенсором, для которого нужно проверить статус службы обнаружения вторжений.
 - **Результат шага:** откроется боковая панель настроек выбранного сенсора.
 - В открывшейся панели включите или выключите службу обнаружения вторжений сенсора с помощью переключателя **Служба обнаружения вторжений**: если переключатель в состоянии  — служба включена.
- Для активации и деактивации правил:

- а. Перейдите на страницу [Администрирование](#) → [Сигнатурный анализ](#) → [Правила обнаружения](#).
 - б. Для включения нескольких правил воспользуйтесь фильтрами и нажмите кнопку ✓ **Активировать** в верхней части страницы.
 - в. Для отключения нескольких правил воспользуйтесь фильтрами и нажмите кнопку ✕ **Деактивировать** в верхней части страницы.
3. Для редактирования правила:
- а. Нажмите  (**Редактировать**) напротив интересующего правила.
 - **Результат шага:** появится окно **Редактирование правила обнаружения вторжений**.
 - б. Измените необходимые параметры в окне **Редактирование правила обнаружения вторжений**.

i

Прим.:

Не рекомендуется редактирование правил с sid в диапазоне, отличающемся от пользовательского (94000000-94999999), так как такие правила могут быть заменены при импорте.

Редактирование правила обнаружения

✕

Наименование *

Описание

Условие *

☒ **Активность**

Рис. 33. Окно редактирования правила обнаружения вторжения

4. Для изменения правила с sid в диапазоне, отличающемся от пользовательского (94000000-94999999):
 - а. Нажмите  (**Редактировать**) напротив интересующего правила.
 - **Результат шага:** появится окно **Редактирование правила обнаружения вторжений**.
 - б. Скопируйте значения полей окна.
 - в. При необходимости отмените выбор чекбокса **Активность** и нажмите **Сохранить**.

- г. Нажмите **Создать правило**.
- д. Вставьте скопированные ранее значения полей окна в соответствующие поля окна создания правила.
- е. Измените sid так, чтобы он входил в пользовательский диапазон (94000000-94999999) и не совпадал с другими правилами.
- ж. Измените необходимые параметры правила.



Подсказка:

Для ограничения срабатывания правила 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.

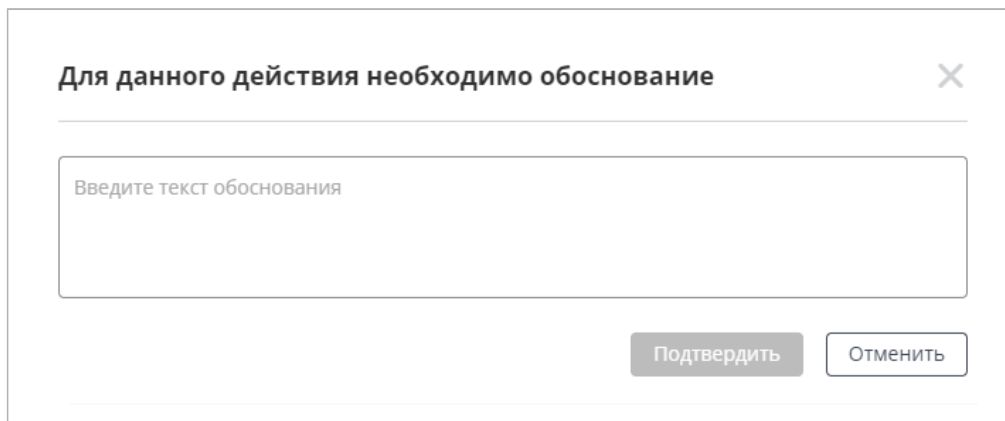
- 3. Установите чекбокс **Активность**;

и. 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.

5. Для удаления правила:

- а. Нажмите  (**Удалить правило**) напротив интересующего правила.
- б. Введите текст обоснования удаления правила и нажмите кнопку **Подтвердить**.



Для данного действия необходимо обоснование

Введите текст обоснования

Подтвердить Отменить

Рис. 34. Обоснование удаления правила обнаружения вторжений

6. Для синхронизации измененных правил с сенсорами нажмите  **Синхронизировать правила**.

3.2.3. 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**.

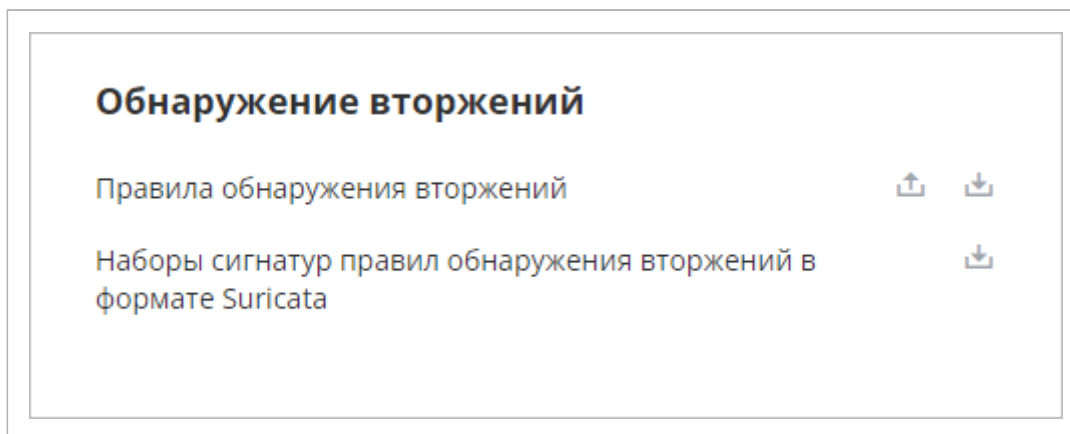


Рис. 35. Панель «Обнаружение вторжений» на странице «Импорт и экспорт»

3.2.3.1. Импорт правил обнаружения вторжений в формате *.json

Перед импортом обратите 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 импортируемого меньше, чем в уже загруженном, новое правило не будет импортировано;
- если rev импортируемого 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** выберите:
 - 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.

Подготовка к импорту

Оставить ⓘ

Удалить ⓘ

Оставить как есть ⓘ

Присвоить старым статус, как в файле ⓘ

При импорте правил выполняется проверка уникальности элемента по sid правила, конфликты разрешаются по номеру ревизии (rev) правила. В случае импорта устаревшего правила (rev меньше текущего), импорт не производится. При успешном разрешении конфликта активность правила может быть сохранена согласно выбранному действию (Статус активности правил после импорта)

Импортировать

Отменить

Рис. 36. 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.

3.2.3.2. Импорт правил обнаружения вторжений в формате *.rules

Перед импортом обратите 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 импортируемого меньше, чем в уже загруженном, новое правило не будет импортировано;
- если rev импортируемого 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 **Наборы 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** выберите:

- 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.

Подготовка к импорту

Оставить ⓘ

Удалить ⓘ

Оставить как есть ⓘ

Присвоить старым статус, как в файле ⓘ

При импорте правил выполняется проверка уникальности элемента по sid правила, конфликты разрешаются по номеру ревизии (rev) правила. В случае импорта устаревшего правила (rev меньше текущего), импорт не производится. При успешном разрешении конфликта активность правила может быть сохранена согласно выбранному действию (Статус активности правил после импорта)

Импортировать

Отменить

Рис. 37. Окно «Подготовка к импорту» при загрузке наборов сигнатур

► **Результат шага:** появится уведомление Правила *suricata* применяются автоматически.

- Убедитесь, что правила были успешно загружены. Для этого перейдите на страницу [Правила обнаружения](#).

3.2.3.3. Экспорт правил службы обнаружения вторжений

Для экспорта правил обнаружения вторжений в файл формата *.json:

- Перейдите на страницу [Администрирование](#) → [Основные настройки](#) → [Импорт и экспорт](#).
- 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](#).

- Для скачивания файла нажмите на название сформированного файла под заголовком **Результат последнего экспорта**.
- В открывшемся окне укажите расположение экспортируемого файла и нажмите кнопку **Сохранить**.

► **Результат шага:** файл *suricata_rules_[дата_и_время].zip* будет загружен на компьютер.

4. Мониторинг событий

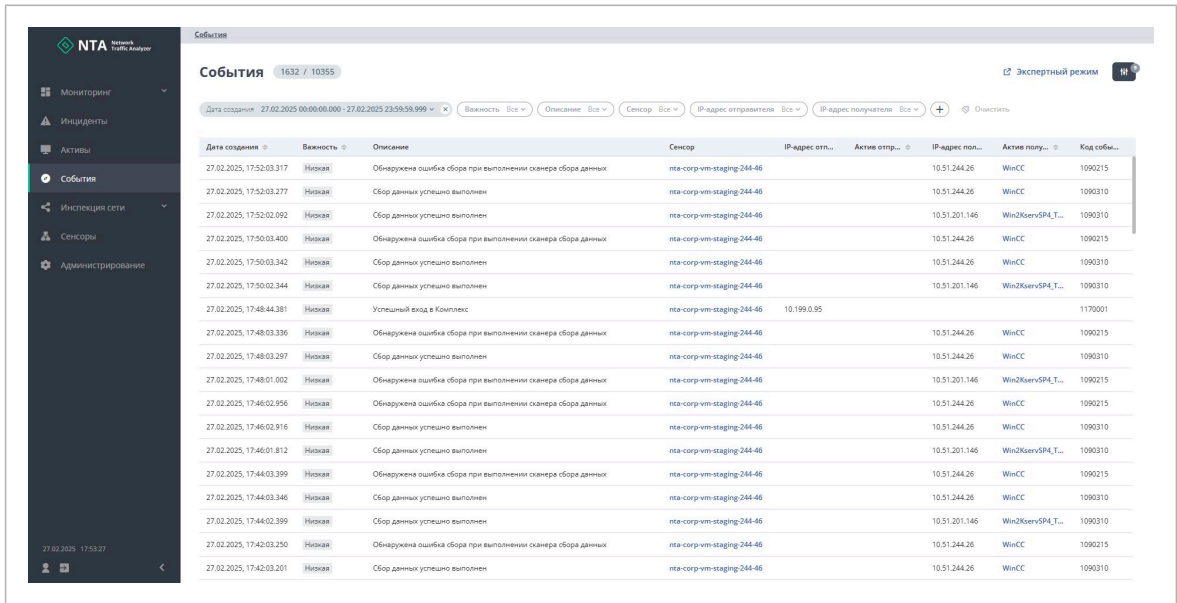
В этом разделе:

- 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

Просмотр и 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, кликните на ячейку **Дата создания** в строке с нужным событием.



Дата создания	Важность	Описание	Сенсор	IP-адрес отп...	Актив отпр...	IP-адрес пол...	Актив полу...	Код собы...
27.02.2025, 17:52:03.317	Низкая	Обнаружена ошибка сбора при выполнении сканера сбора данных	nta-corp-wm-staging-244-46			10.51.244.26	WinCC	1090215
27.02.2025, 17:52:03.277	Низкая	Сбор данных успешно выполнен	nta-corp-wm-staging-244-46			10.51.244.26	WinCC	1090310
27.02.2025, 17:52:02.092	Низкая	Сбор данных успешно выполнен	nta-corp-wm-staging-244-46			10.51.201.146	Win2KservSP4,T...	1090310
27.02.2025, 17:50:03.400	Низкая	Обнаружена ошибка сбора при выполнении сканера сбора данных	nta-corp-wm-staging-244-46			10.51.244.26	WinCC	1090215
27.02.2025, 17:50:03.342	Низкая	Сбор данных успешно выполнен	nta-corp-wm-staging-244-46			10.51.244.26	WinCC	1090310
27.02.2025, 17:50:02.344	Низкая	Сбор данных успешно выполнен	nta-corp-wm-staging-244-46			10.51.201.146	Win2KservSP4,T...	1090310
27.02.2025, 17:48:44.381	Низкая	Успешный вход в Комплекс	nta-corp-wm-staging-244-46	10.190.0.95				1170001
27.02.2025, 17:48:03.336	Низкая	Обнаружена ошибка сбора при выполнении сканера сбора данных	nta-corp-wm-staging-244-46			10.51.244.26	WinCC	1090215
27.02.2025, 17:48:03.297	Низкая	Сбор данных успешно выполнен	nta-corp-wm-staging-244-46			10.51.244.26	WinCC	1090310
27.02.2025, 17:48:01.002	Низкая	Обнаружена ошибка сбора при выполнении сканера сбора данных	nta-corp-wm-staging-244-46			10.51.201.146	Win2KservSP4,T...	1090215
27.02.2025, 17:46:02.956	Низкая	Обнаружена ошибка сбора при выполнении сканера сбора данных	nta-corp-wm-staging-244-46			10.51.244.26	WinCC	1090215
27.02.2025, 17:46:02.916	Низкая	Сбор данных успешно выполнен	nta-corp-wm-staging-244-46			10.51.244.26	WinCC	1090310
27.02.2025, 17:46:01.812	Низкая	Сбор данных успешно выполнен	nta-corp-wm-staging-244-46			10.51.201.146	Win2KservSP4,T...	1090310
27.02.2025, 17:44:03.399	Низкая	Обнаружена ошибка сбора при выполнении сканера сбора данных	nta-corp-wm-staging-244-46			10.51.244.26	WinCC	1090215
27.02.2025, 17:44:03.346	Низкая	Сбор данных успешно выполнен	nta-corp-wm-staging-244-46			10.51.244.26	WinCC	1090310
27.02.2025, 17:44:02.399	Низкая	Сбор данных успешно выполнен	nta-corp-wm-staging-244-46			10.51.201.146	Win2KservSP4,T...	1090310
27.02.2025, 17:42:03.250	Низкая	Обнаружена ошибка сбора при выполнении сканера сбора данных	nta-corp-wm-staging-244-46			10.51.244.26	WinCC	1090215
27.02.2025, 17:42:03.201	Низкая	Сбор данных успешно выполнен	nta-corp-wm-staging-244-46			10.51.244.26	WinCC	1090310

Рис. 38. Список событий на странице «События»

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.

Поиск и просмотр событий

Поиск и просмотр событий выполняются на странице **События**.

Поиск событий возможен с помощью панели фильтров над списком событий.

В каждом событии расположены поля, для которых генерируются уникальные данные. Подробнее о полях событий см. в разделе «[Описание полей событий](#)».

Инструменты для работы с запросами (создание нового запроса, сохранение текущего запроса, открытие сохраненного результата) находятся в [экспертном режиме](#) страницы [События](#).

Генерация событий

Комплекс предоставляет возможности по выявлению критичных событий ИБ, называемых инцидентами. Подробнее см. в главе «[Анализ и настройка инцидентов](#)».

Комплекс в результате работы генерирует собственные события автоматически. Также возможно получение событий от настроенных источников и в результате активного сбора событий 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.

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. Перечень доступных для настройки переменных находится в разделе «[Описание служебных источников событий](#)».



Прим.:

Служебные источники не отображаются на странице [Администрирование](#) → [Настройка активов](#) → [Источники](#).

Генерация событий UDV NTA

UDV NTA генерирует собственные события по результатам анализа прослушиваемого трафика. UDV NTA генерирует события со следующими типами (поле `event_type`):

- `dpi_notice` — события обнаружения сетевых атак (список сетевых атак, которые обнаруживает UDV NTA, приведены в справочном разделе «[Сетевые атаки, обнаруживаемые UDV NTA](#)»);
- `ml_notice` — события обнаружения DNS-туннелирования.

Хранение событий

События, которые доступны к просмотру через веб-интерфейс, хранятся в оперативном архиве — индексе. 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. Чтобы просмотреть эти события, их нужно восстановить из архива — подробнее см. раздел «[Восстановление индексов событий](#)».

Внутренние события, сгенерированные Комплексом, хранятся отдельно от событий, полученных из внешних источников:

- `datapk-events-internal-[дата_создания_индекса]` — индексы для внутренних событий;
- `datapk-events-external-[дата_создания_индекса]` — индексы для внешних событий.

Общий объем зарегистрированных событий ограничен значениями, указанными в переменных файла `manager.env` Комплекса уровня Management. Регистрацию новых событий при переполнении оперативного архива можно отключить с помощью переменной `DATAPK_EVENT_MANAGER_EVENTS_ACTION_MORE_SIZE`. См. подробнее в разделах «Переменные Комплекса уровня Management», «Рекомендации по использованию переменных файла .env».

4.1. Поиск и просмотр событий в упрощенном режиме

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

Просмотр событий

Для просмотра события:

1. Для просмотра информации о событии в строке интересующего события кликните в ячейке **Дата создания**.

► **Результат шага:** откроется карточка с подробной информацией о выбранном событии.

1090215 host_connection

Дата создания: 26.02.2025, 23:58:03.233

Активы

	Отправитель	Получатель
Актив:	—	WinCC
IP-адрес:	—	10.51.244.26
Порт:	—	—
MAC-адрес:	—	—
Идентификатор:	—	2e0b48ed-1117-485e-a3d3-cbef12280985

Событие

Важность: Низкая
Категория события: Arp-таблица (test winexe 0.8)
Протокол: —
Сообщение: Обнаружена ошибка сбора при выполнении сканера сбора данных: Актив: WinCC (2e0b48ed-1117-485e-a3d3-cbef12280985); Сканер: Arp-таблица (test winexe 0.8); Задачи: Задача winexe 0.8; Ошибка: winexe-0.8 is not...
[Показать полностью](#)
Действие: —
Дополнительная информация: winexe-0.8 is not installed on the sensor by default
Обоснование: —
Идентификатор события: 3bb3a1c0-f286-40aa-a3b0-b1a727cb1003
Источник события: datapk_sensor
Пользователь: —
Приоритет инцидента: —
Идентификатор инцидента: —
Идентификатор запроса: —

Сенсор

Сенсор: nta-corp-vm-staging-244-46
Идентификатор сенсора: fc30d73435387abbfbb61c10676106ae

Регистратор

Регистратор: nta-corp-vm-staging-244-46
IP-адрес регистратора: 10.51.244.46
Идентификатор регистратора: fc30d73435387abbfbb61c10676106ae

Рис. 39. Карточка события

2. Для перехода к активам, связанным с событием, нажмите в карточке события кнопку  **Активы**.

**Внимание:**

Кнопка 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 активов, связанных с событием.

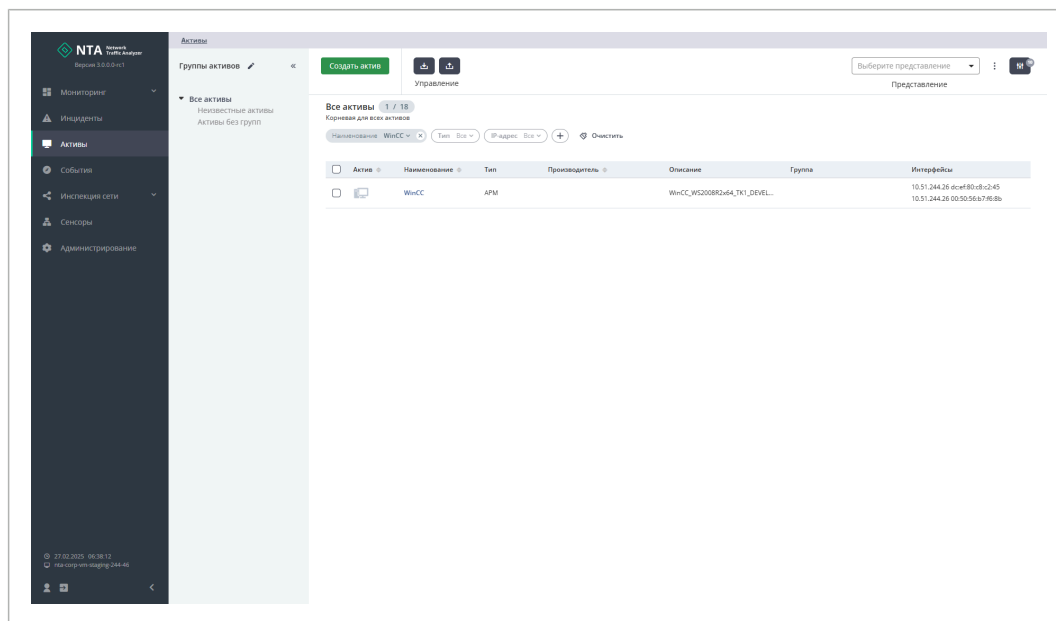


Рис. 40. Активы, связанные с событием, на странице «Активы»

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, за исключением следующих фильтров:

- фильтр **Важность**, в котором по умолчанию заданы значения Низкая или Критическая;
- фильтр **Тип события**, в котором заданы значения типов событий;
- фильтр **Сенсор**, в котором заданы наименования сенсоров, подключенных к Комплексу;
- фильтры **Актив отправителя** и **Актив получателя**, в которых заданы наименования обнаруженных Комплексом или созданных вручную активов.
- фильтр **Протокол**, в котором заданы значения протоколов, обнаруживаемых Комплексом.

Фильтры расположены вверху страницы.

**Подсказка:**

Для более точного поиска событий можно использовать одновременно несколько фильтров.

Для поиска события с помощью фильтра:

1. Выберите необходимый фильтр.

► **Результат шага:** отобразится поле ввода значения в выбранный фильтр.

Рис. 41. Поле ввода значения в фильтр «Описание»

2. Введите значение в фильтр.
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.
5. Для очистки результатов поиска по одному из фильтров нажмите кнопку справа от выбранного фильтра.
- ▶ **Результат шага:** результаты поиска будут автоматически обновлены на странице.

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. 42. Календарь выбора временного периода регистрации событий

2. Выберите начальную дату.

► **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.

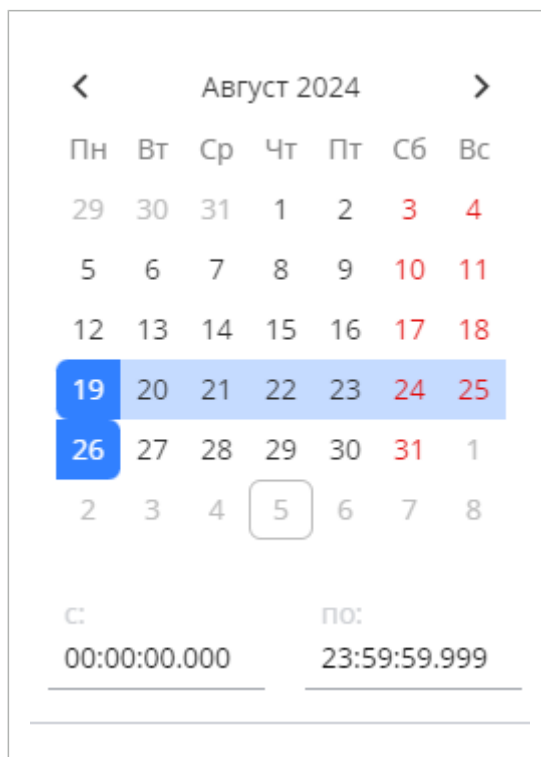


Рис. 43. Выбранные даты в календаре

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:** указывается время для начальной даты;
- в поле **по:** указывается время для конечной даты.

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

Дата создания	Важность	Описание	Сенсор	IP-адрес от...	Актив от...	IP-адрес пол...	Актив пол...	Код собы...
23.02.2025, 01:02:26.979	Критическая	Запущен сервис регистрации событий	nta-corp-vm-staging-244-46					1070001
23.02.2025, 01:06:36.114	Критическая	Деактивированы правила обнаружения вторжений	nta-corp-vm-staging-244-46					1280006
26.02.2025, 21:26:35.903	Критическая	Несоответствие полезной нагрузки ICMP (между who и reply)	nta-corp-vm-staging-244-46	10.51.244.46		10.51.15.1		1230040
26.02.2025, 21:26:37.204	Критическая	Несоответствие полезной нагрузки ICMP (между who и reply)	nta-corp-vm-staging-244-46	10.51.244.46		10.51.15.10		1230040
23.02.2025, 01:02:26.979	Низкая	Обнаружено нарушение целостности исполняемых файлов в результате прове...	nta-corp-vm-staging-244-46					1180033
23.02.2025, 01:02:15.694	Низкая	Обнаружено нарушение целостности исполняемых файлов в результате прове...	nta-corp-vm-staging-244-46					1180033
23.02.2025, 01:06:09.395	Низкая	Успешный вход в Комплекс	nta-corp-vm-staging-244-46	10.51.20.115				1170001
23.02.2025, 01:06:13.311	Низкая	Запущено сканирование сети	nta-corp-vm-staging-244-46					1220001
23.02.2025, 01:06:13.396	Низкая	Добавлены учетные данные активов	nta-corp-vm-staging-244-46					1080026
23.02.2025, 01:06:13.459	Низкая	Добавлены учетные данные активов	nta-corp-vm-staging-244-46					1080026
23.02.2025, 01:06:13.528	Низкая	Добавлены учетные данные активов	nta-corp-vm-staging-244-46					1080026
23.02.2025, 01:06:13.599	Низкая	Добавлены учетные данные активов	nta-corp-vm-staging-244-46					1080026
23.02.2025, 01:06:13.694	Низкая	Добавлены учетные данные активов	nta-corp-vm-staging-244-46					1080026
23.02.2025, 01:06:13.782	Низкая	Добавлены учетные данные активов	nta-corp-vm-staging-244-46					1080026
23.02.2025, 01:06:13.871	Низкая	Добавлены учетные данные активов	nta-corp-vm-staging-244-46					1080026
23.02.2025, 01:06:13.945	Низкая	Добавлены учетные данные активов	nta-corp-vm-staging-244-46					1080026
23.02.2025, 01:06:14.022	Низкая	Добавлены учетные данные активов	nta-corp-vm-staging-244-46					1080026
23.02.2025, 01:06:14.091	Низкая	Добавлены учетные данные активов	nta-corp-vm-staging-244-46					1080026
23.02.2025, 01:06:14.176	Низкая	Добавлены учетные данные активов	nta-corp-vm-staging-244-46					1080026
23.02.2025, 01:06:14.251	Низкая	Добавлены учетные данные активов	nta-corp-vm-staging-244-46					1080026

Рис. 44. 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.

Добавление фильтров

Для добавления фильтров на страницу **События**:

1. Нажмите кнопку , расположенную на панели фильтров.

► **Результат шага:** Отобразится выпадающий список с доступными фильтрами. Фильтры, уже выбранные для отображения на странице, выделены серым цветом и имеют иконку  слева от названия.

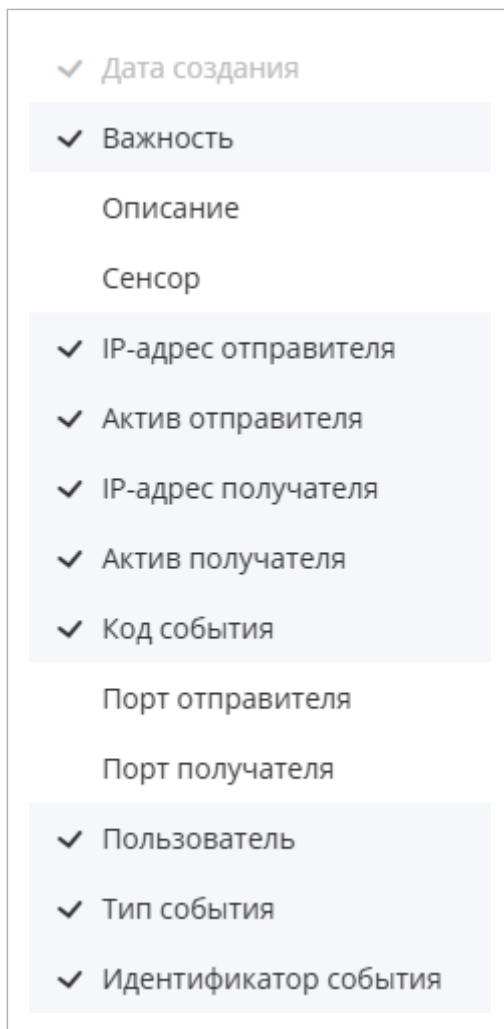


Рис. 45. Список доступных фильтров

2. В выпадающем списке выберите необходимые фильтры.

► **Результат шага:** выбранные фильтры отобразятся на панели фильтров.

Удаление фильтров

Для удаления фильтров со страницы **События**:

1. Нажмите кнопку , расположенную на панели фильтров.

2. В выпадающем списке отмените выбор необходимых фильтров.

► **Результат шага:** фильтры перестанут отображаться на панели фильтров.

4.2. Просмотр событий и создание запросов в экспертном режиме

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](#)».

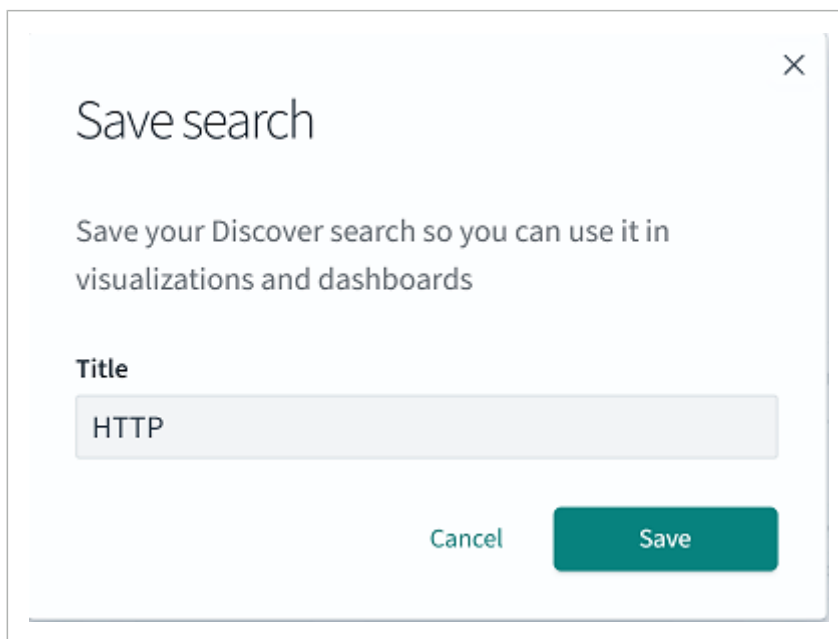
Для создания нового запроса:

1. Перейдите на страницу [События](#).
2. Нажмите кнопку  [Экспертный режим](#) 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.

Time ▾	description	listener
> Dec 27, 2023 @ 06:20:31.831	ET SCAN Potential SSH Scan	intrusion_detection
> Dec 27, 2023 @ 06:20:07.983	ET SCAN NMAP -sS window 1024	intrusion_detection

Рис. 46. 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.



Save search

Save your Discover search so you can use it in visualizations and dashboards

Title

HTTP

Cancel Save

Рис. 47. 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.

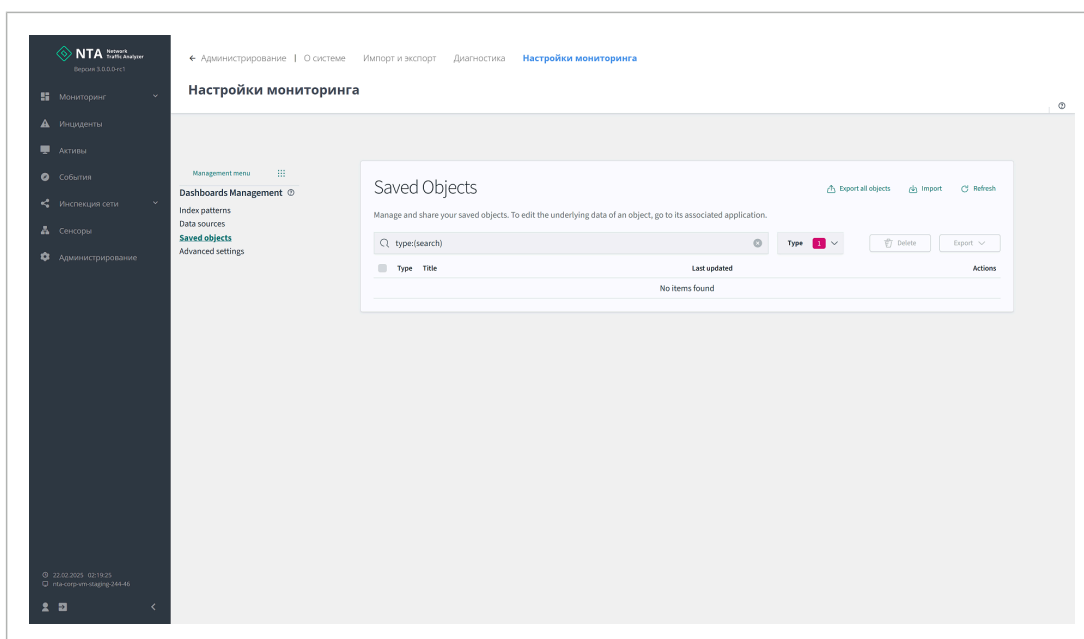


Рис. 48. Выбор типа «search» в разделе «Saved objects» страницы «Настройки мониторинга»

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.

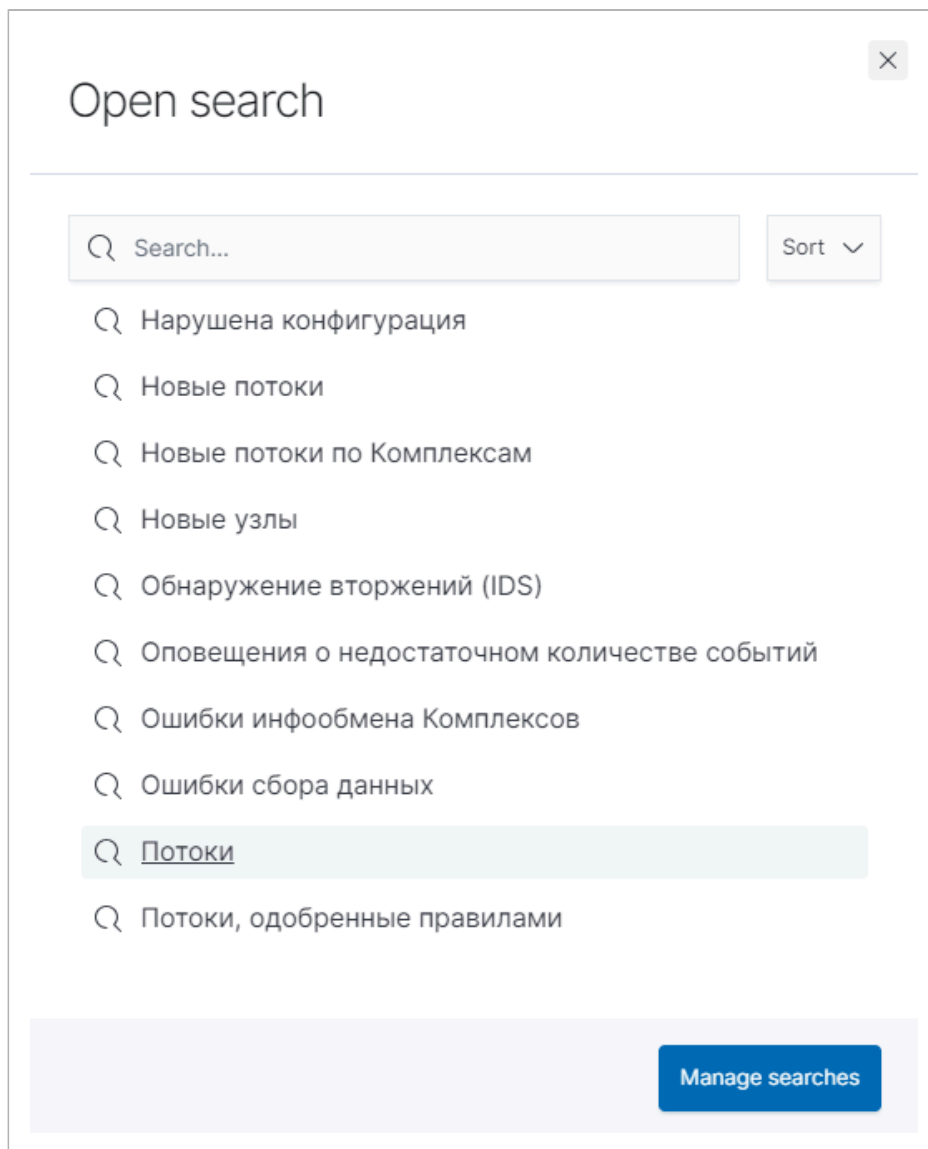


Рис. 49. Окно выбора поискового запроса

4.3. 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.

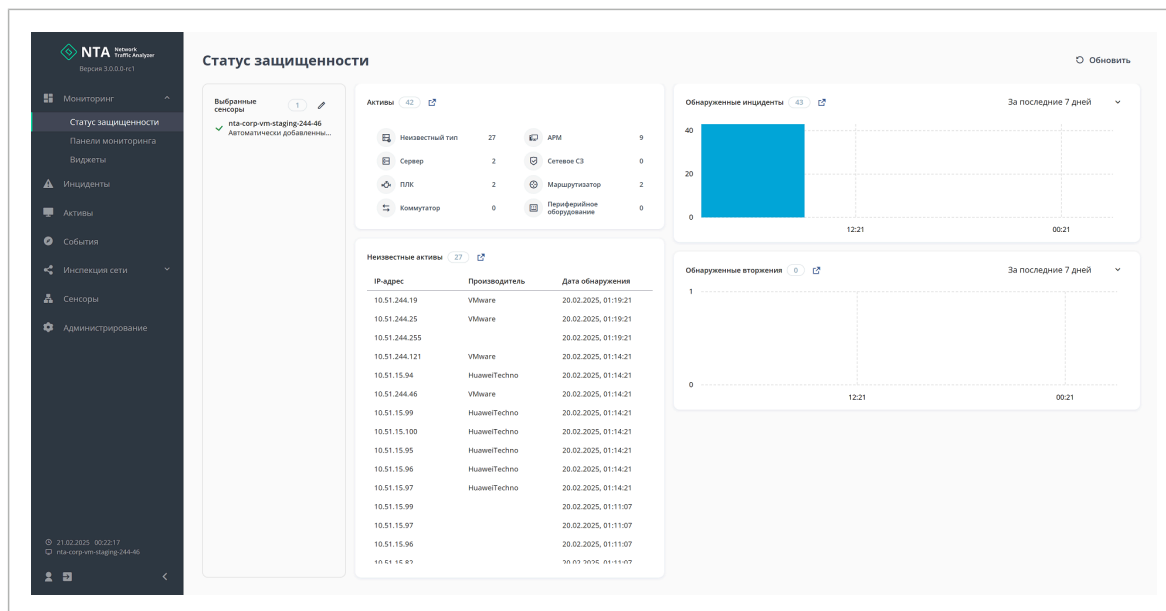


Рис. 50. Страница «Статус защищенности»

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.



Прим.:

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.** В виджете отображается количество всех обнаруженных активов, сгруппированных по типам.



Прим.:

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, Обнаруженные вторжения** — графики с количеством инцидентов и вторжений, обнаруженных в выбранный период времени до текущего момента.



Прим.:

Над каждым графиком отображается примерное количество обнаруженных объектов за период, которое рассчитывается с учетом аппроксимации и исторических данных обнаружения.

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.

4.4. 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](#)

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 в виде файла формата *.ndjson 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 сетевых узлов.**
 - **Обнаружение вторжений.**
 - **Контроль событий:**
 - **События активов.**
 - **Инциденты ИБ.**
- **События управления комплексами** — список всех событий доступа и управления экземпляра Комплекса.
- **Эксплуатационный мониторинг** — содержит три списка событий, относящихся к непосредственному функционированию Комплекса.

4.4.1. 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 состояния актива) на графике.
4. Переходит по ссылке **Контроль сетевых узлов** в разделе аналитики.
5. Находит нужный пик на графике **Изменения во времени**, выделяет его.
6. На странице видит всю необходимую для проверки информацию: Комплекс, наименование сенсора, которому принадлежит актив, наименование узла, описание событие, MAC- и IP-адрес актива, дата и время появления события.

4.4.2. 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.

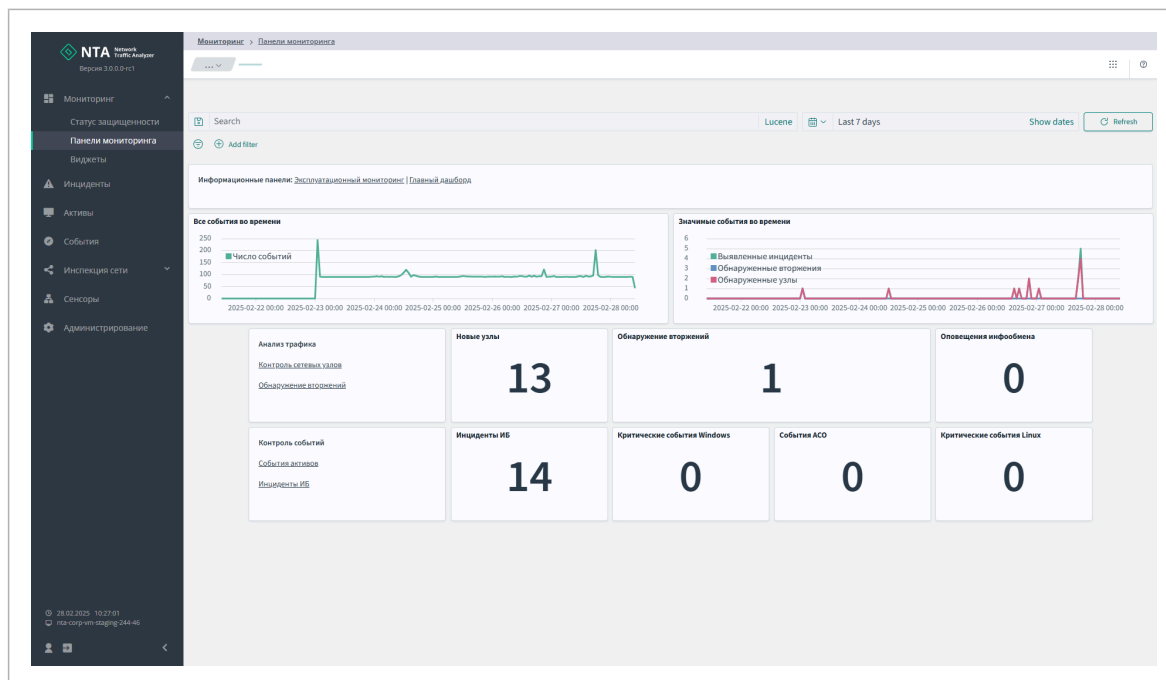


Рис. 51. Главный дашборд

4.4.3. 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.

4.4.3.1. 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 ⊖.

Изменения конфигураций объектов защиты

Комплекс	ОЗ	Название конфигурации	Описание	Кол-во
udv-datapk-с	cisco	ECI_CISCO_IOS_SHOW_RUNNING_CONFIG (ssh-en)	Нарушено эталонное со	3
udv-datapk-с	cisco	ECI_CISCO_IOS_SHOW_STARTUP_CONFIG (ssh-en)	Нарушено эталонное со	1
udv-datapk-с	WIN-SC697B1T31	Компоненты Windows (winrm https-basic)	Нарушено эталонное со	2

**Рис. 52. Создание фильтра по значению таблицы
«Изменения конфигураций объектов защиты»**

**Подсказка:**

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

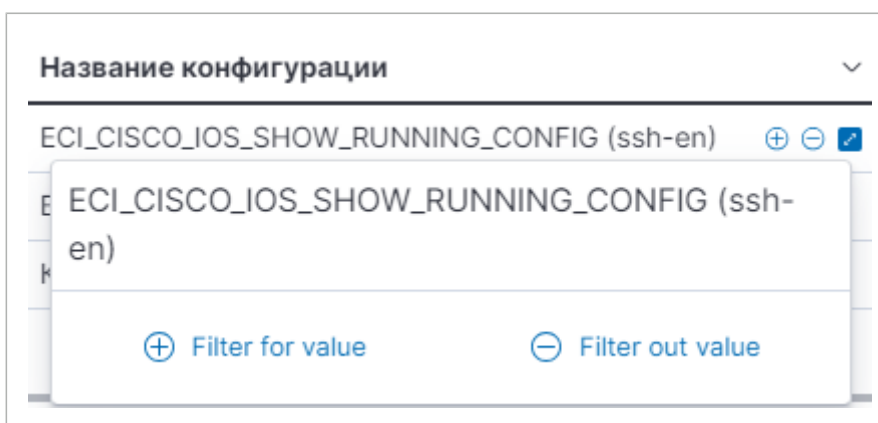


Рис. 53. Отображение значения, выбранного для фильтрации

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.

4.4.4. Выбор периода отображения событий на панели мониторинга

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

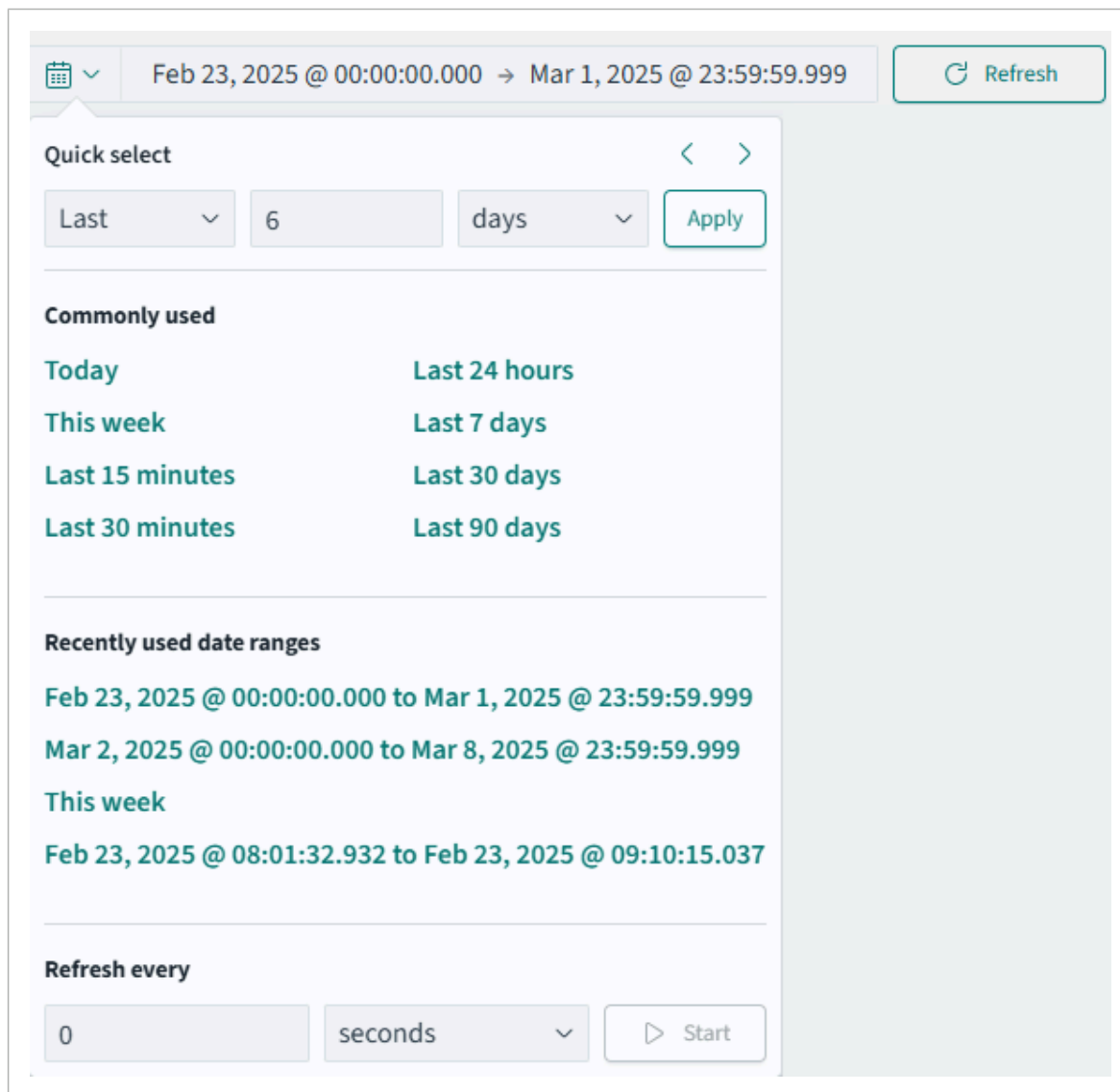


Рис. 54. Выбор периода отображения событий

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;

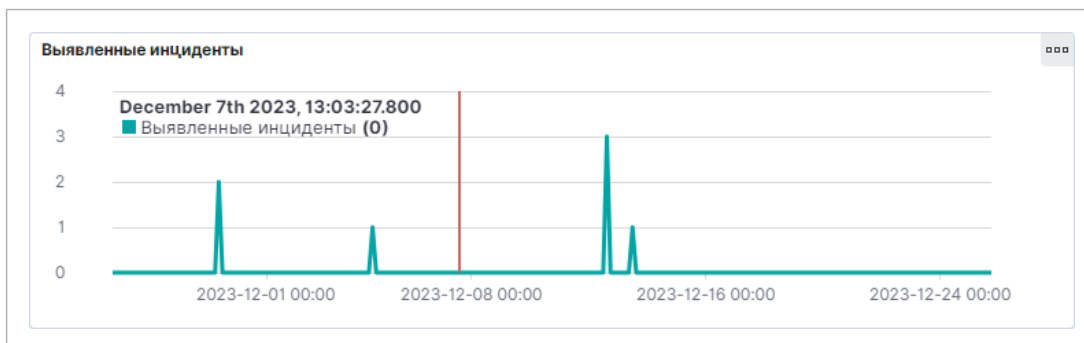


Рис. 55. Выбор начала периода отображения событий

- а. Зажмите левую клавишу мыши.
- б. Не отпуская, ведите до окончания интересующего периода. Область выбора времени на графике станет серой.

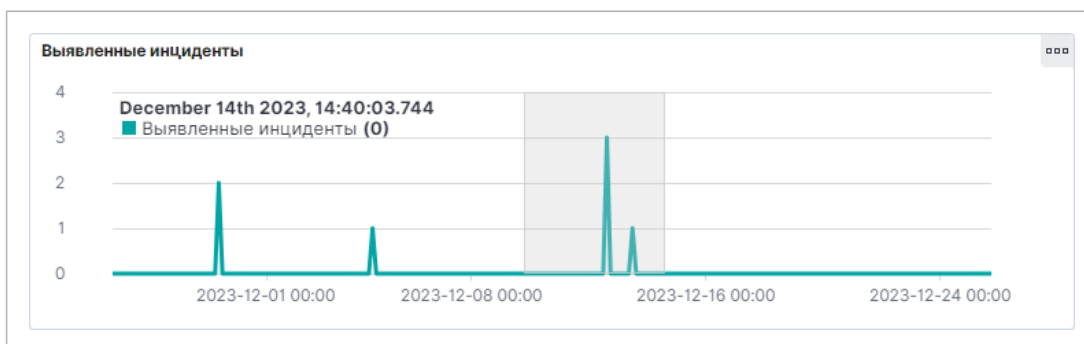


Рис. 56. Выбор окончания периода отображения событий

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.

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. 57. Выбор интервала автообновления

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

4.4.5. Главный дашборд

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.

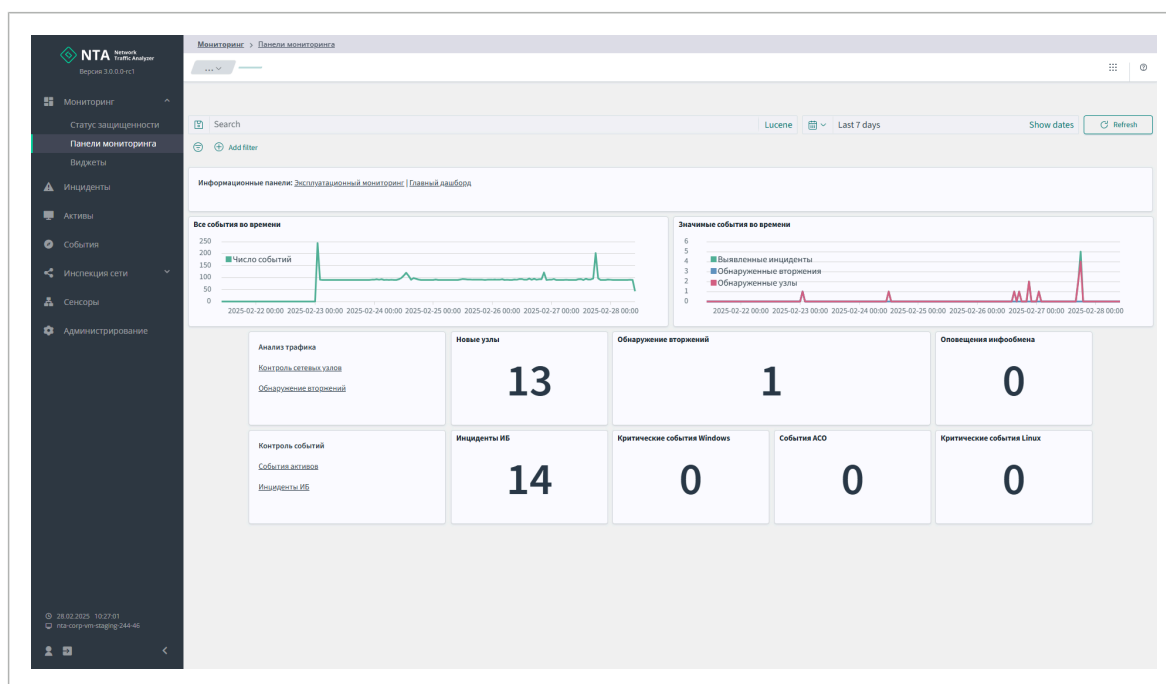


Рис. 58. Главный дашборд

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 событий.**

Графики главного дашборда

Основным средством отслеживания количества событий на главном дашборде являются графики.

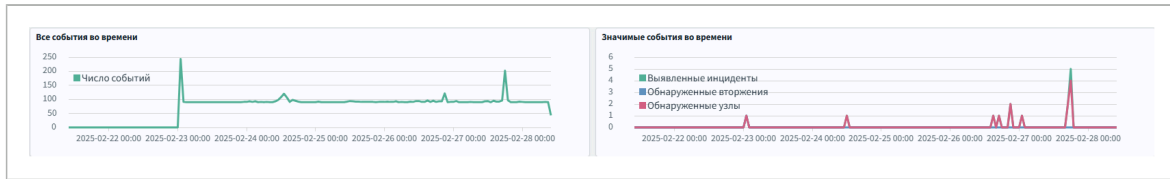


Рис. 59. Графики главного дашборда

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;**
 - **Обнаруженные вторжения;**
 - **Обнаруженные узлы.**

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

4.4.6. 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.

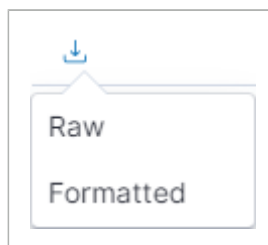


Рис. 60. Типы экспорта событий

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

4.5. 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 событий Комплекса в архив

4.5.1. 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 обогащений событий
- Импорт схемы событий

4.5.1.1. 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.

4.5.1.2. 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.

4.5.1.3. Экспорт схемы событий

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.

4.5.1.4. 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.

4.5.1.5. Импорт правил обогащений событий

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

1. Перейдите на страницу [Администрирование](#) → [Основные настройки](#) → [Импорт и экспорт](#).
2. На панели **События** в строке **Правила обогащений 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.

4.5.1.6. Импорт схемы событий

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.

4.5.2. Экспорт и импорт источников событий

В этом разделе:

- [Экспорт источников событий](#)
- [Импорт источников событий](#)

4.5.2.1. Экспорт источников событий

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

1. Перейдите на страницу [Администрирование](#) → [Настройка активов](#) → [Источники](#).
2. На панели управления под заголовком страницы нажмите кнопку  (**Экспортировать**).
 - **Результат шага:** файл `sources[дата_и_время].json` будет загружен.

4.5.2.2. 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 объект защиты. Если объект защиты, указанный в импортируемом источнике, отсутствует, то такой источник будет пропущен при импорте.

Подготовка к импорту

✕

Перед обработкой выберите:

Действие для элементов, которые отсутствуют в новом справочнике :

☒ Оставить ⓘ

☐ Удалить ⓘ

Источники для отсутствующих ОЗ не будут импортированы

Импортировать

Отменить

Рис. 61. Окно «Подготовка к импорту» при импорте источников событий объектов защиты

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

4.5.3. Включение и отключение служебных источников

По умолчанию все служебные источники Комплекса активны, имеют низкую критичность (low).

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 (5-7 минут).

события от включенных источников будут регистрироваться на странице [События](#).

4.5.4. Создание источника событий

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

1. Перейдите на страницу [Администрирование](#) → [Настройка активов](#) → [Источники](#).

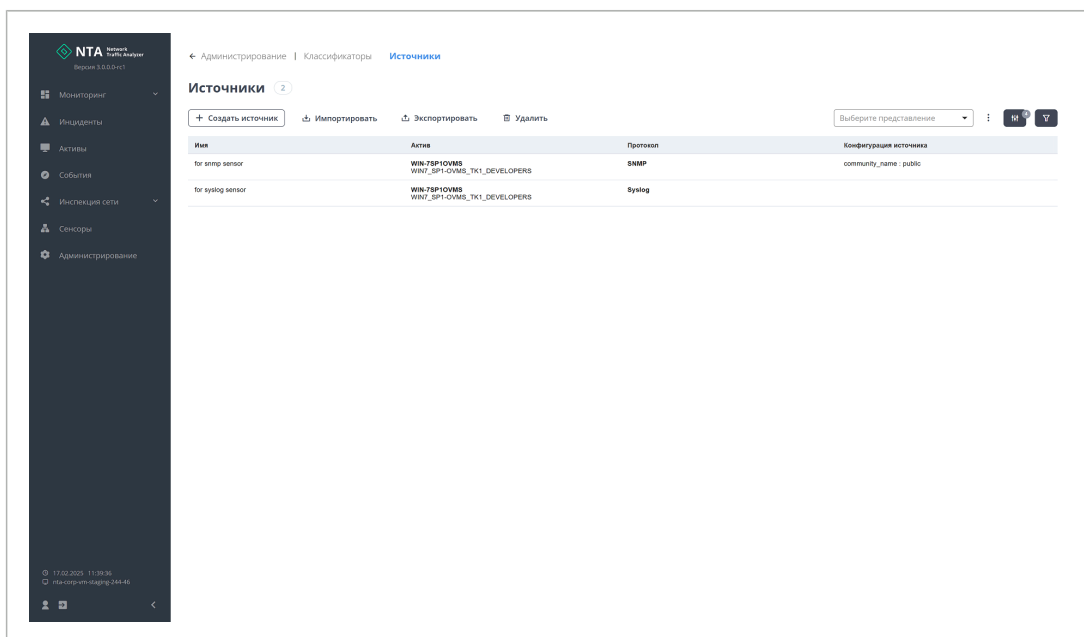
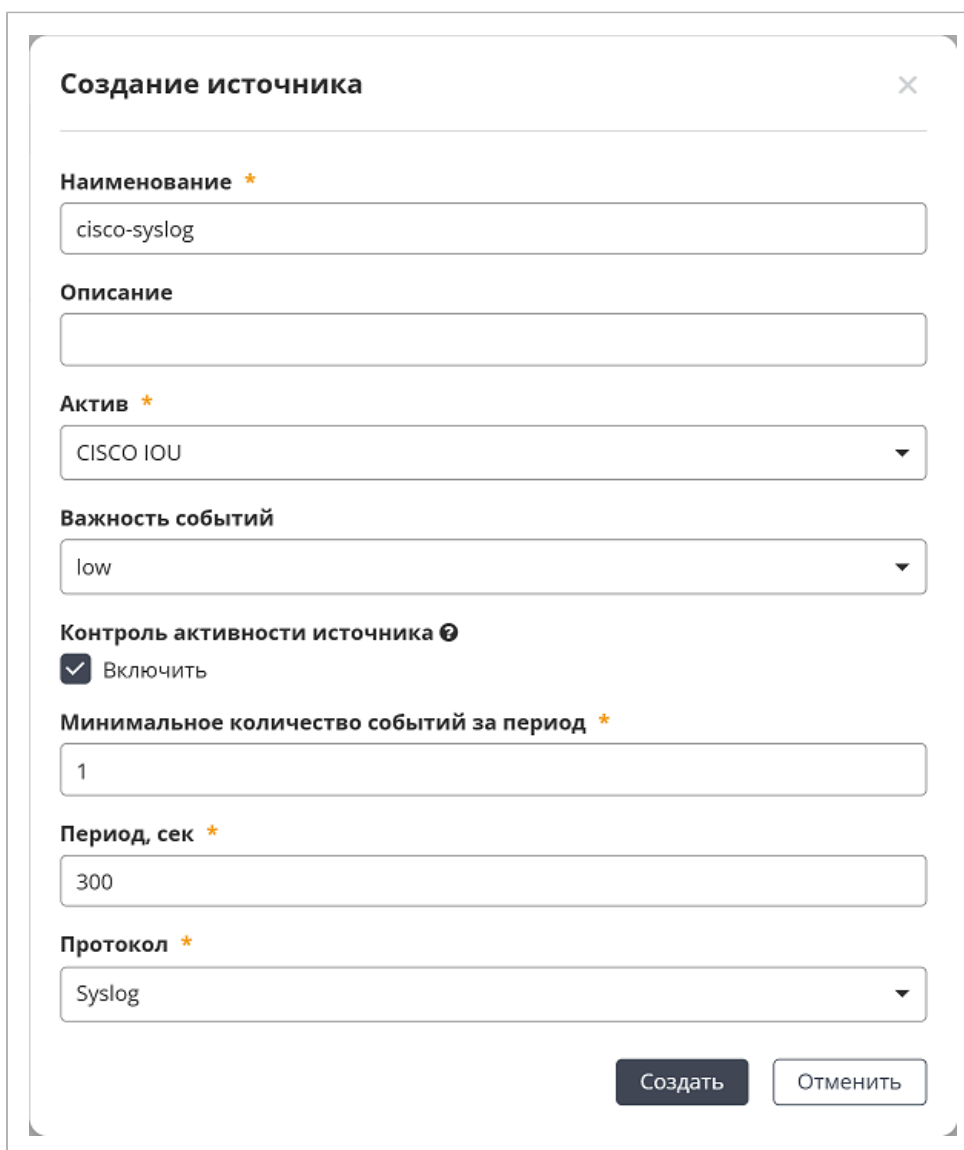


Рис. 62. Страница «Источники»

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. критичность 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.



Создание источника

Наименование *
cisco-syslog

Описание

Актив *
CISCO IOU

Важность событий
low

Контроль активности источника ?
☒ Включить

Минимальное количество событий за период *
1

Период, сек *
300

Протокол *
Syslog

Создать Отменить

Рис. 63. Окно «Создание источника» при создании источника syslog_rfc3164_sensor

4. Нажмите кнопку **Создать** для подтверждения изменений.

► **Результат шага:** будет создан новый источник событий.

4.5.5. Управление источниками событий

Для управления источниками событий присутствуют следующие возможности:

1. Запуск сбора событий от источника. Для возобновления процесса получения событий от определенного источника:
 - а. 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:
 - а. 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:

- а. Перейдите на страницу [Администрирование](#) → [Настройка активов](#) → [Источники](#).
- б. Нажмите кнопку  (**Удалить источник**).
- в. Введите текст обоснования удаления источника.

4.5.6. Выгрузка событий Комплекса в архив

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

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](#).

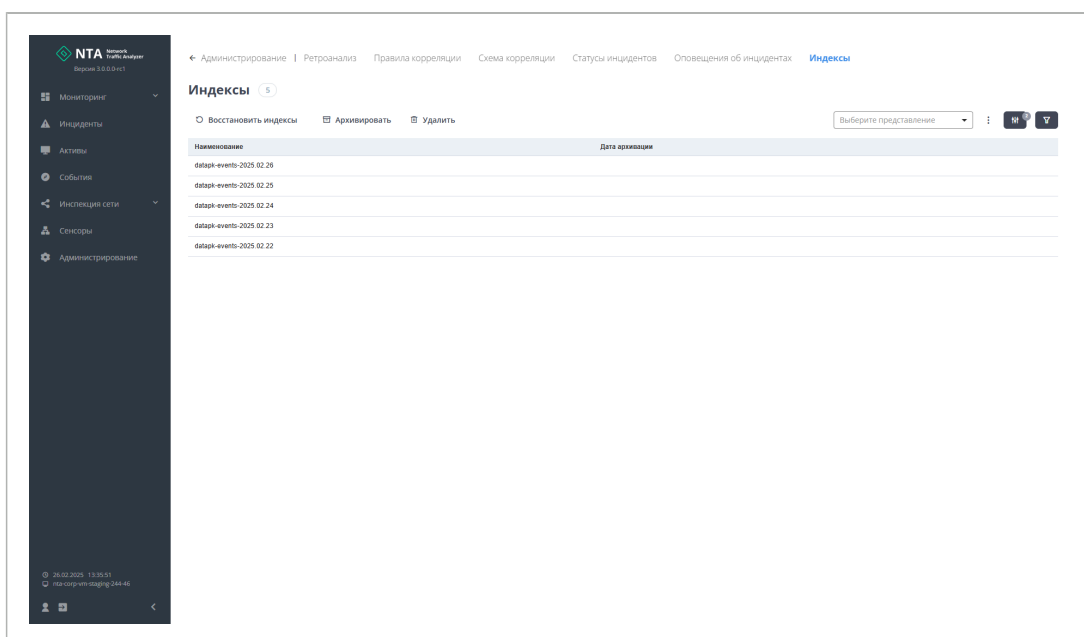


Рис. 64. Страница «Индексы»

2. Нажмите кнопку  (**Архивировать**) справа от выбранного индекса.
 - **Результат шага:** архив с событиями `datapk_events_[тип_индекса]_[дата_индекса]` будет загружен в директорию `indices` в операционной системе Комплекса (путь по умолчанию `/var/backups/elasticsearch/indices`).

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 `indices` в операционной системе Комплекса (путь по умолчанию `/var/backups/elasticsearch/indices`).

4.6. 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»

4.6.1. Создание шаблона индекса

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».

Для создания шаблона индекса:

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

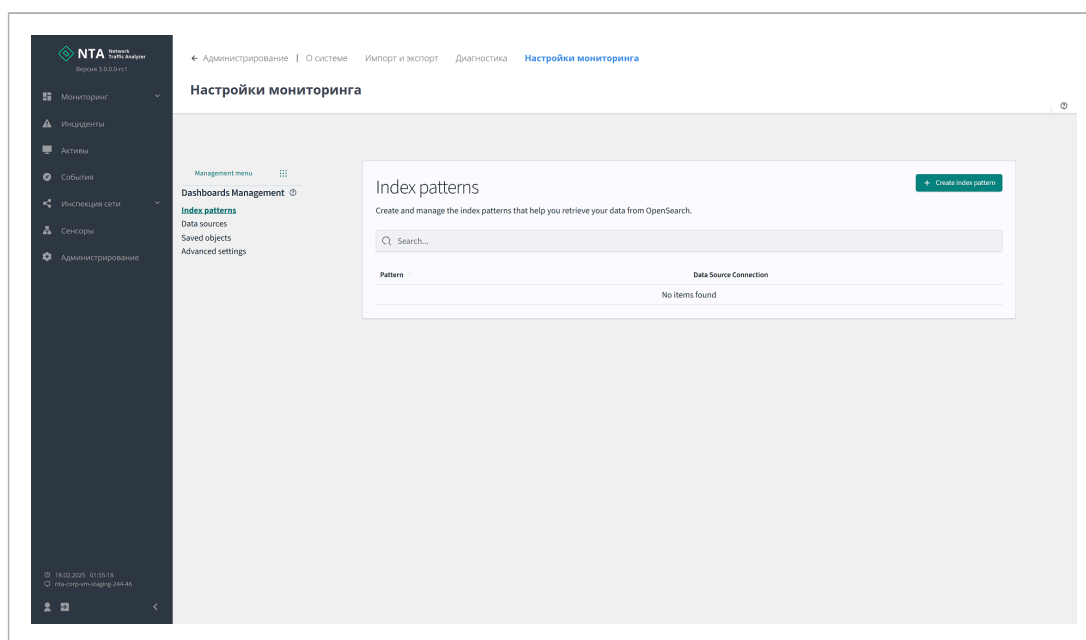


Рис. 65. Страница «Настройки мониторинга»

2. Нажмите **Create index pattern**.

► **Результат шага:** Откроется окно **Create index pattern**.

3. В окне **Create index pattern**:

- а. Введите название предустановленного шаблона `datapk-events-*` в поле **Index pattern name**.
- б. Нажмите **Next step**.

Create index pattern

An index pattern can match a single source, for example, `filebeat-4-3-22`, or **multiple** data sources, `filebeat-*`.
[Read documentation](#)

Step 1 of 2: Define an index pattern

Index pattern name

index-name-*

Use an asterisk (*) to match multiple indices. Spaces and the characters `\, /, ?, %, <, >, |` are not allowed.

☐ Include system and hidden indices

Your index pattern can match your 1 source.

datapk-events-2025.02.18	Index
--------------------------	-------

Rows per page: 10

Рис. 66. 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`).

Create index pattern

An index pattern can match a single source, for example, `filebeat-4-3-22`, or **multiple** data sources, `filebeat-*`.
[Read documentation](#)

Step 2 of 2: Configure settings

Specify settings for your **datapk-*** index pattern.

Select a primary time field for use with the global time filter.

Time field Refresh

create_time

[Show advanced settings](#)

[Back](#)
[Create index pattern](#)

Рис. 67. Окно настройки атрибута временного фильтра в интерфейсе визуализации

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

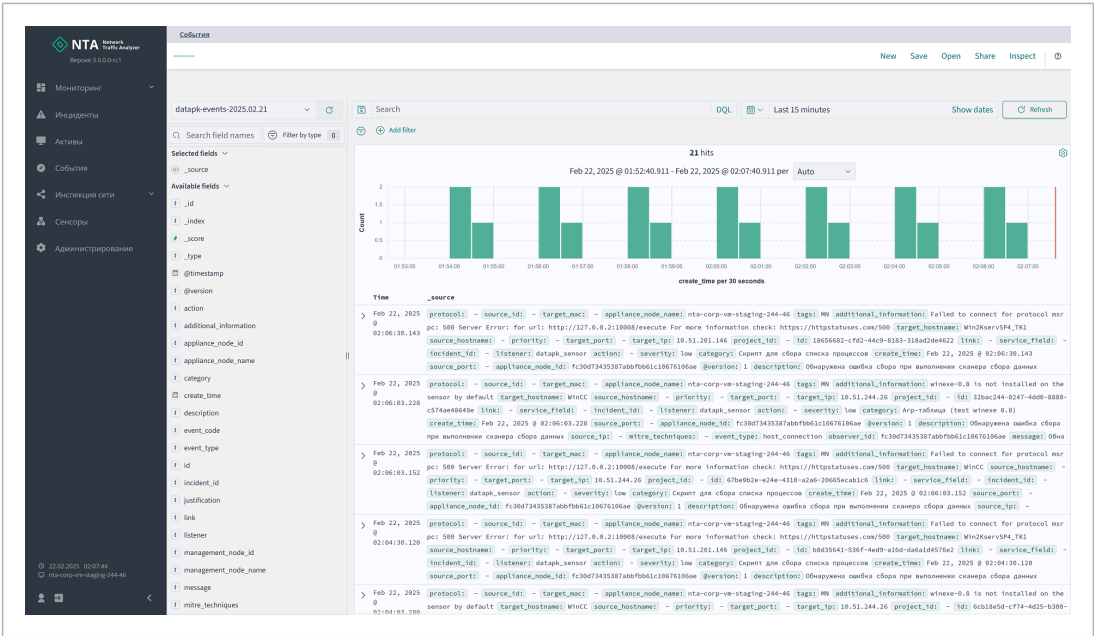


Рис. 68. Страница «События» → «Экспертный режим»

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

4.6.2. 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.

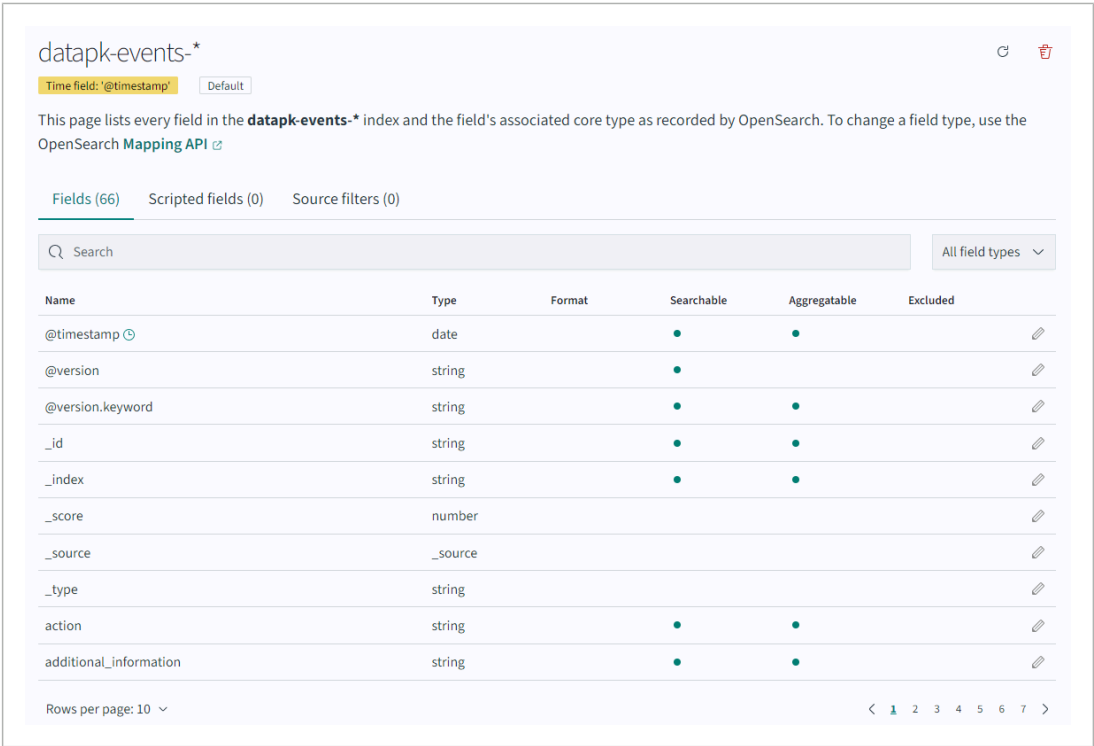


Рис. 69. Внешний вид страницы шаблона индекса

3. Нажмите  в правом верхнем углу.
4. В открывшемся окне нажмите **Delete**.

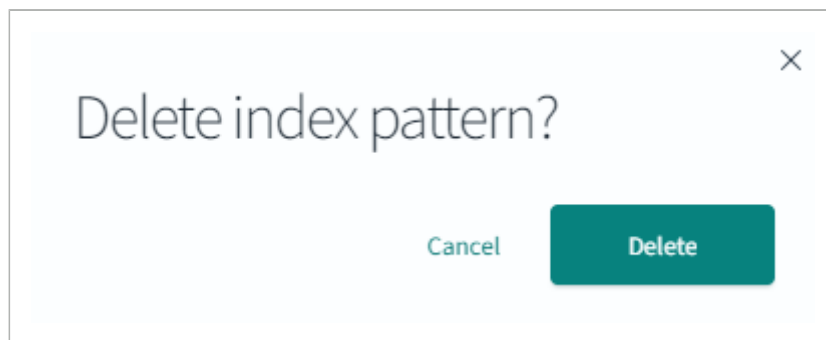


Рис. 70. Окно подтверждения удаления шаблона индекса

- **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](#).

4.6.3. Создание и настройка виджета

Для создания и настройки виджета (визуализации):

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

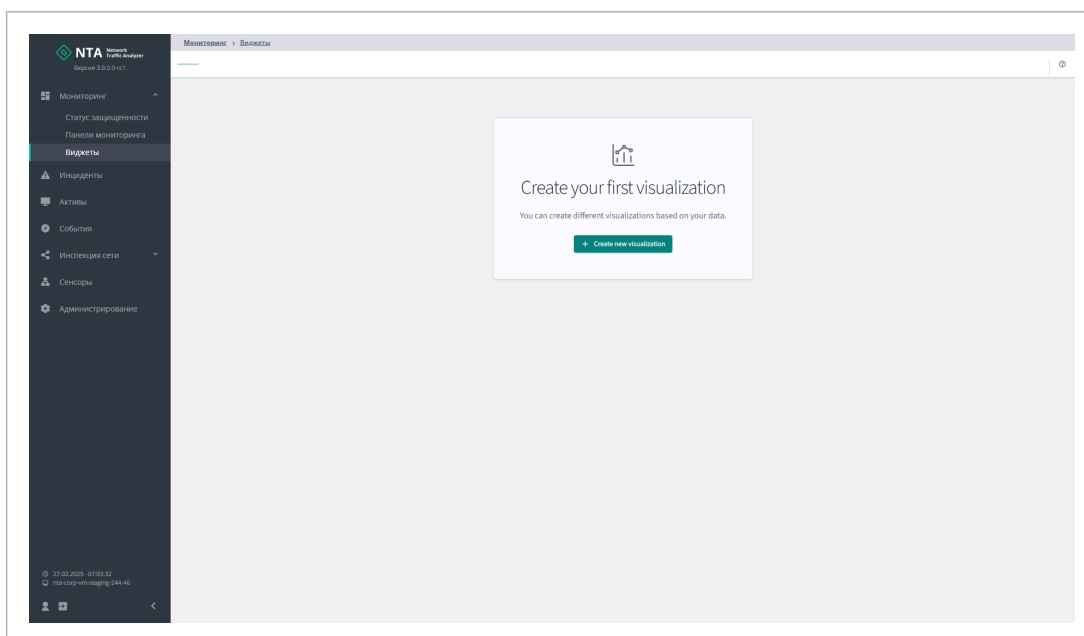


Рис. 71. Страница «Виджет»

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

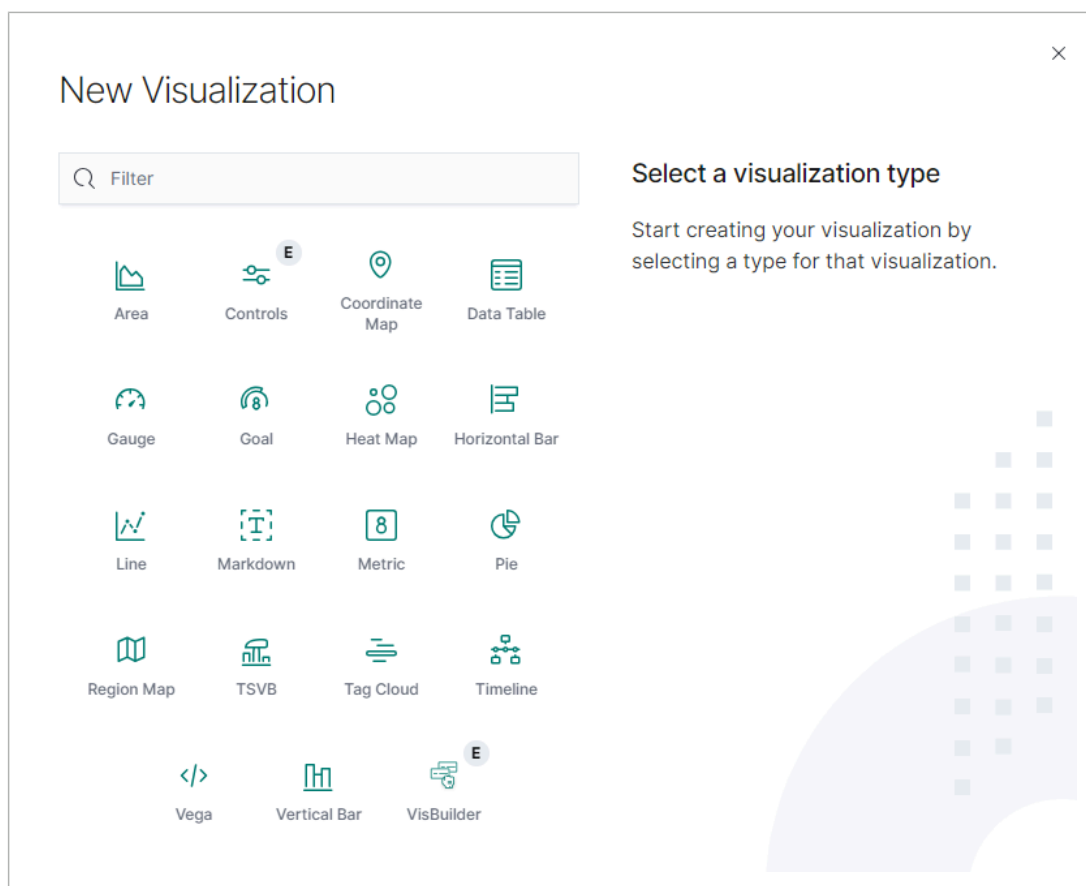


Рис. 72. Окно «New visualization»

4. Выберите источник данных для графического представления.

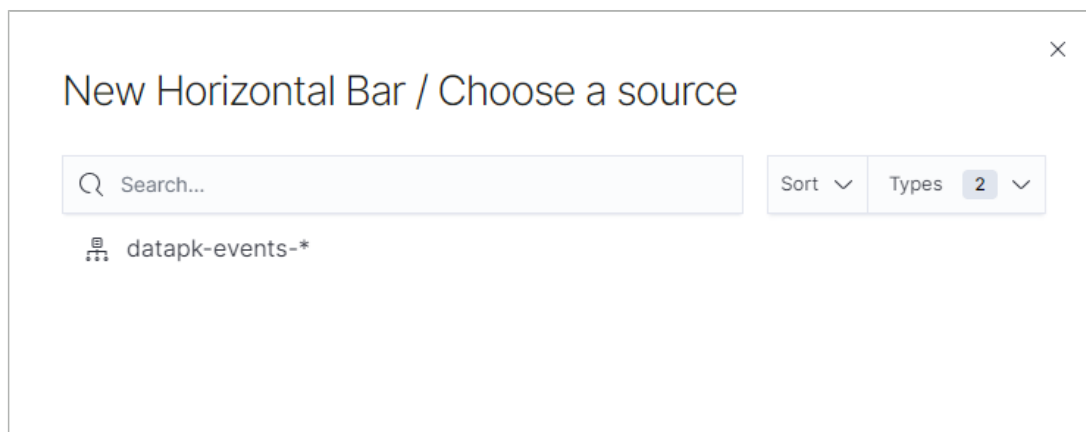


Рис. 73. Выбор источника данных для визуализации

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

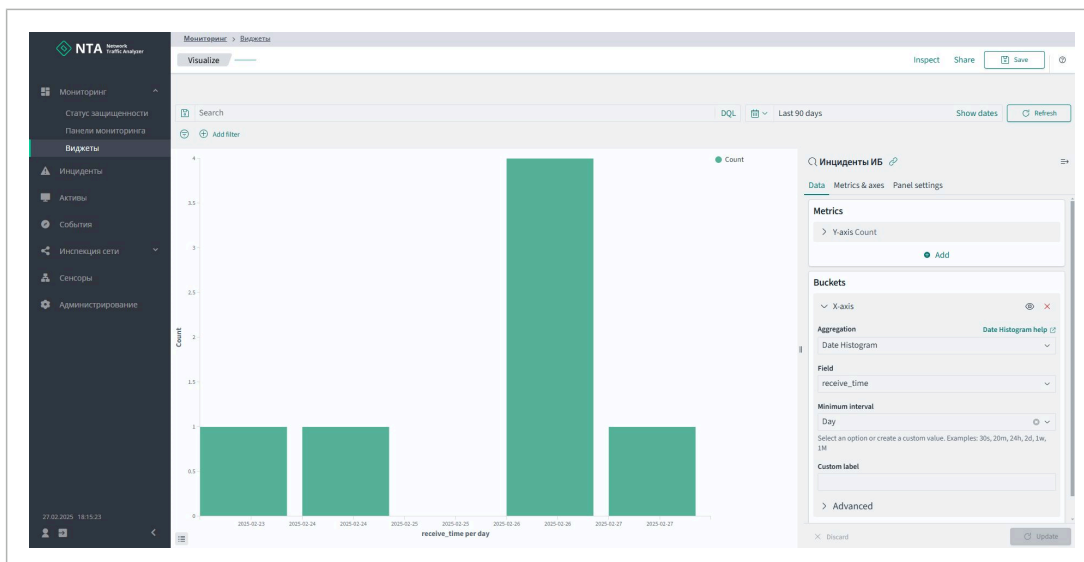


Рис. 74. Виджет типа «Вертикальная диаграмма» с разбивкой событий по временным интервалам

6. Для сохранения визуализации:

- нажмите кнопку **Refresh** в верхней части страницы;
- нажмите кнопку **Save** в верхней части страницы;
- в появившемся окне в поле **Title** введите название сохраняемого объекта;
- нажмите кнопку **Save**.

7. Перейдите на страницу **Администрирование** → **Основные настройки** → **Настройки мониторинга**, вкладка **Saved Objects**.

8. Убедитесь, что в списке присутствует сохраненный объект.

4.6.4. Просмотр и управление виджетами

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

1. Просмотр виджета. Для просмотра:

- Перейдите на страницу **Мониторинг** → **Виджеты**.
- Нажмите на название виджета.
► **Результат шага:** произойдет переход к режиму редактирования визуализации.

2. Редактирование визуализаций. Для редактирования:

- Перейдите на страницу **Мониторинг** → **Виджеты**.
- Нажмите  (**Edit**).
- Измените параметры визуализации.
- Нажмите кнопку **Update** в нижнем правом углу страницы, чтобы применить изменения.
- Нажмите кнопку **Save** в верхнем правом углу страницы.
- 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.

4.6.5. 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.

Создание панели мониторинга

Для создания панели мониторинга:

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

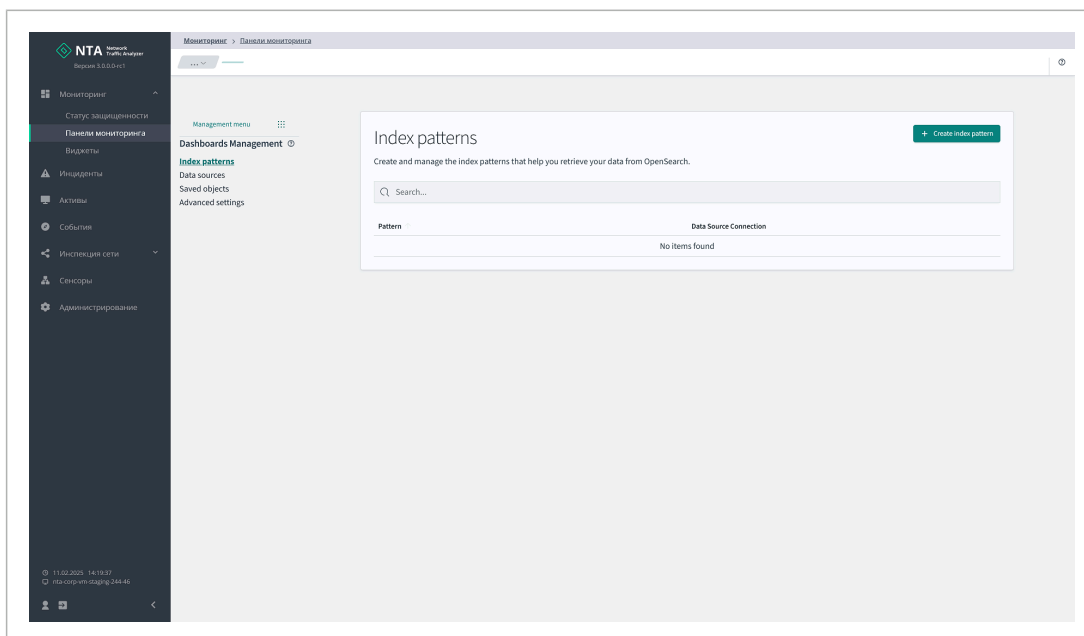


Рис. 75. Страница «Панели мониторинга»

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.

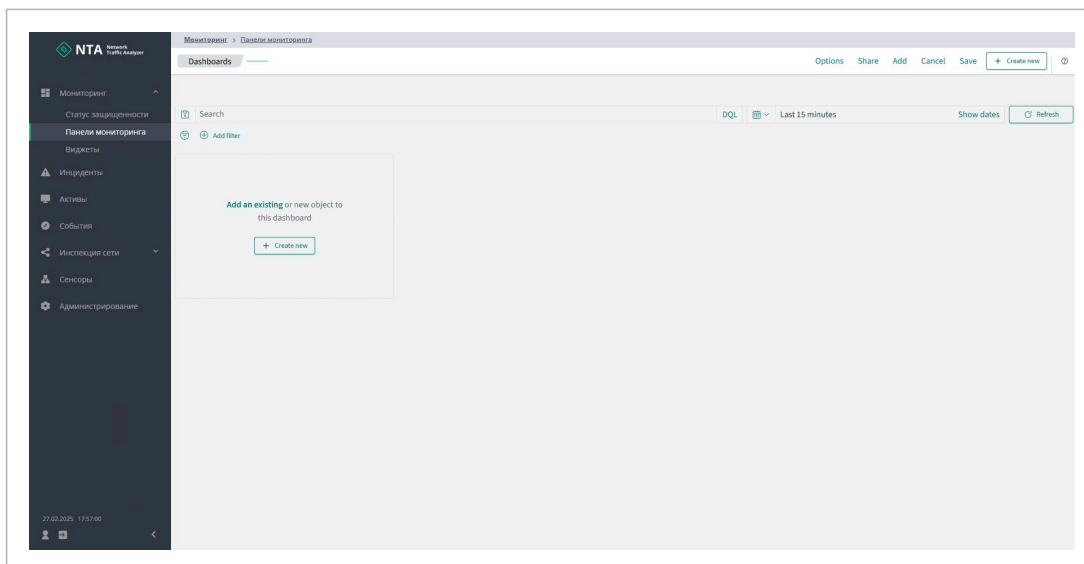


Рис. 76. Страница добавления новой визуализации на панель мониторинга

4. Для добавления существующей визуализации:
 - а. Нажмите кнопку **Add an existing**.
 - б. В появившемся окне выберите один или несколько виджетов.
 - в. Нажмите **X**, 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:
 - а. 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.

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:
 - а. 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:

- а. 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**.

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**.

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**.

4.6.6. Настройка пользовательских правил нормализации событий

Для настройки пользовательских правил нормализации событий:

1. Создайте конфигурационный файл, содержащий пользовательский фильтр grok.
2. Скопируйте файл в директорию `/logstash/config/plugins/pipeline` в рабочей директории Комплекса.
3. Перейдите на страницу [Администрирование](#) → [Основные настройки](#) → [Настройки мониторинга](#).
4. Откройте вкладку **Шаблоны индексов**.

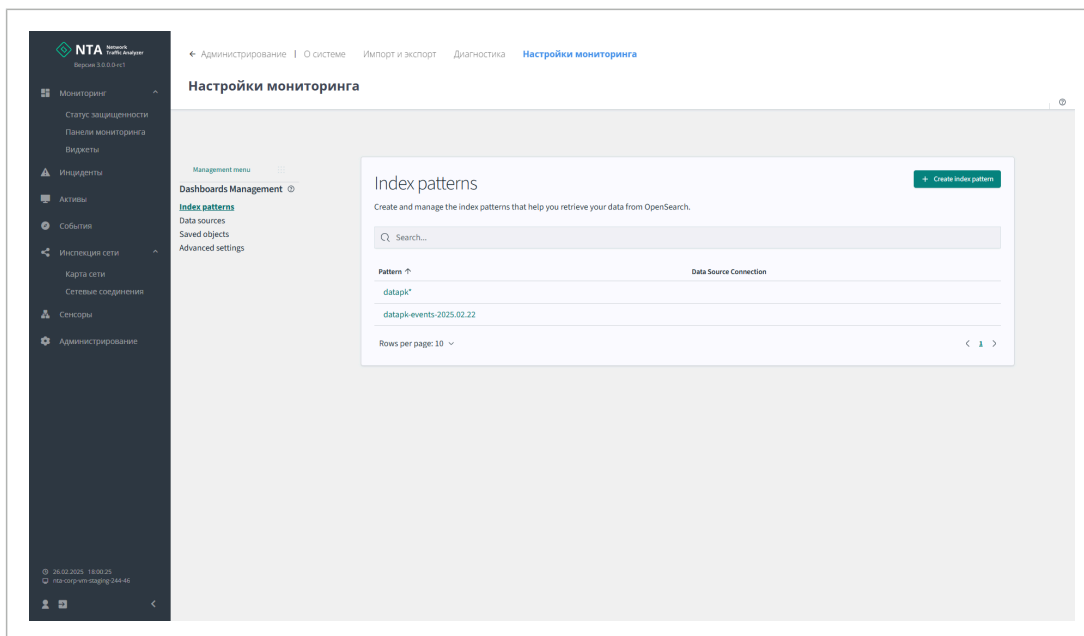


Рис. 77. Вкладка управления мониторингом «Шаблоны индексов»

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

См. также

[Нормализация событий](#)

4.6.7. 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**.

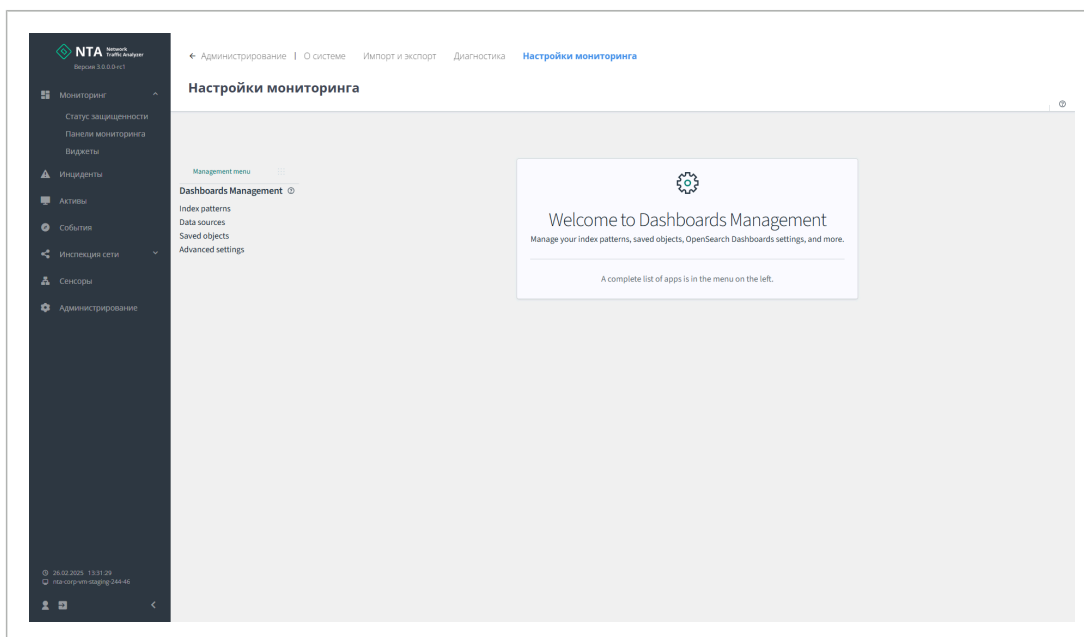


Рис. 78. Страница «Настройки мониторинга»

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

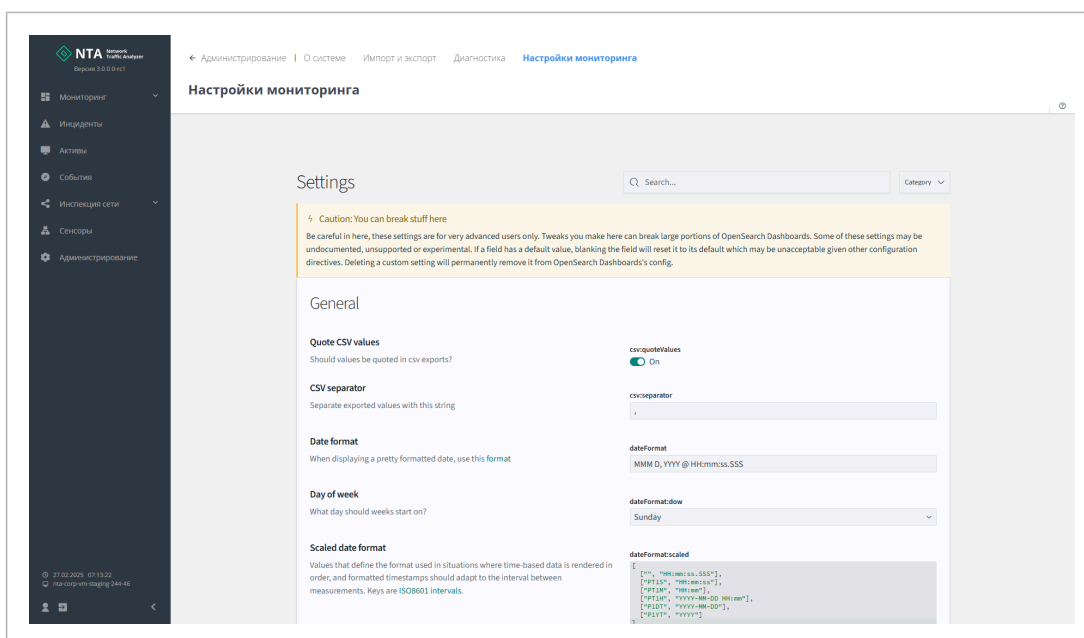


Рис. 79. Вкладка «Advanced Settings»

3. Найдите в списке следующие настройки:

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



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.

4.6.8. Экспорт и импорт объектов раздела «Мониторинг»

В этом разделе:

- [Экспорт сохраненных объектов](#)
- [Импорт сохраненных объектов](#)

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

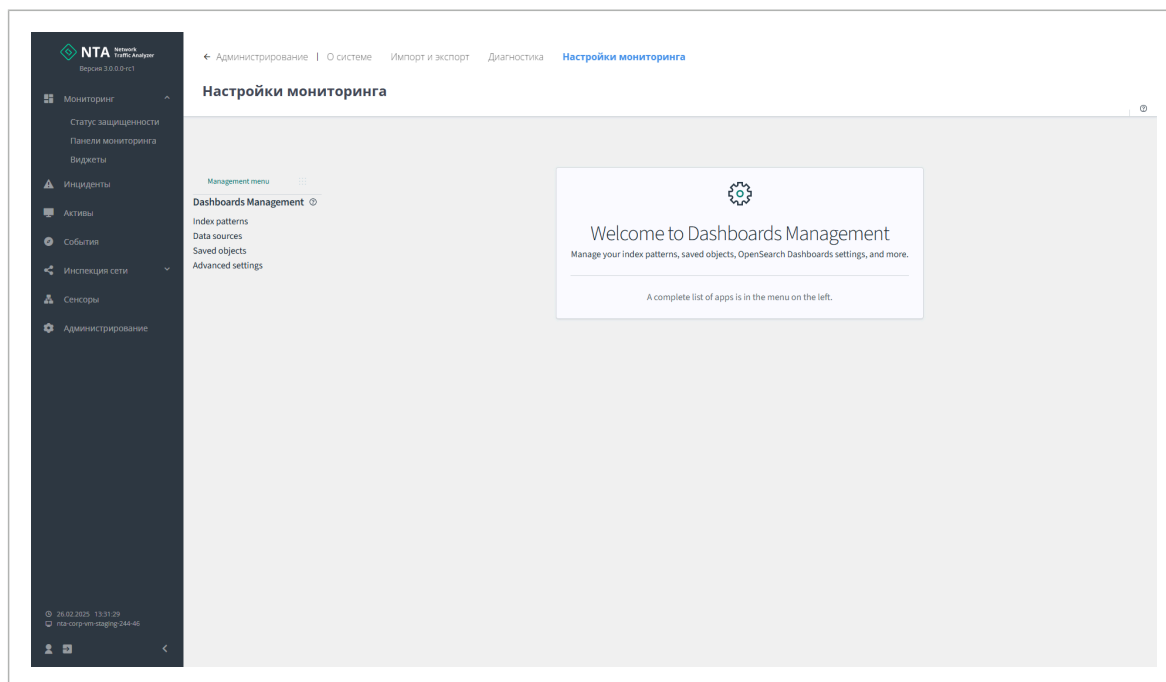


Рис. 80. Страница «Настройки мониторинга»

4.6.8.1. Экспорт сохраненных объектов

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

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

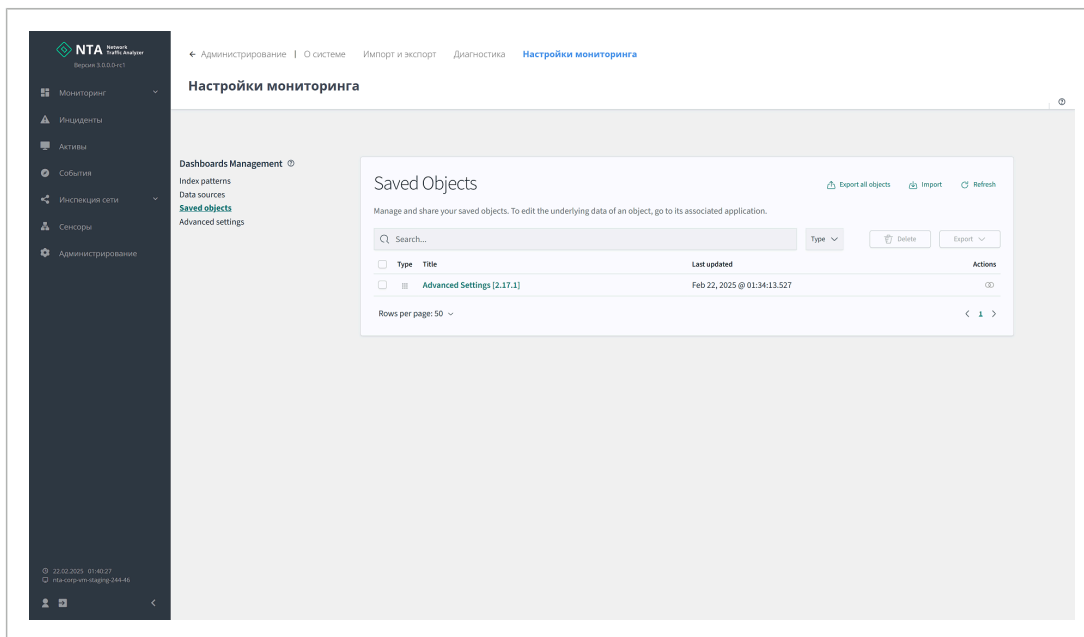


Рис. 81. Вкладка «Saved Objects»

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.

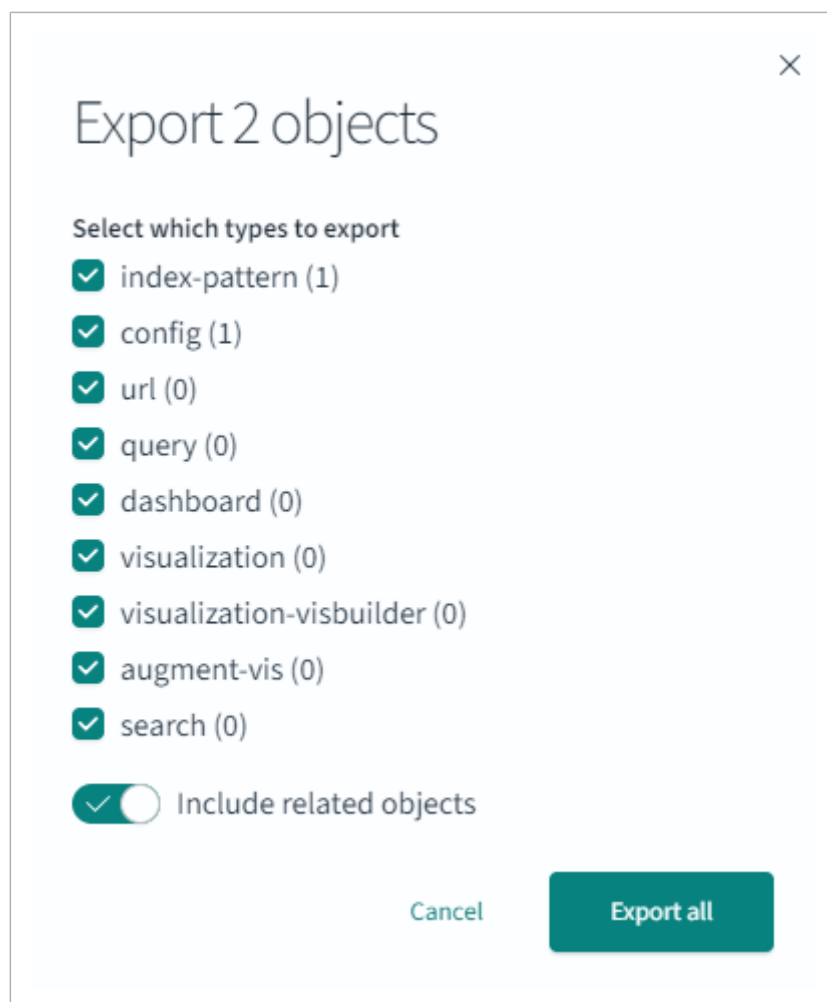


Рис. 82. Окно экспорта объектов

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.

4.6.8.2. Импорт сохраненных объектов

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

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



Прим.:

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. Выберите вкладку **Saved Objects**.

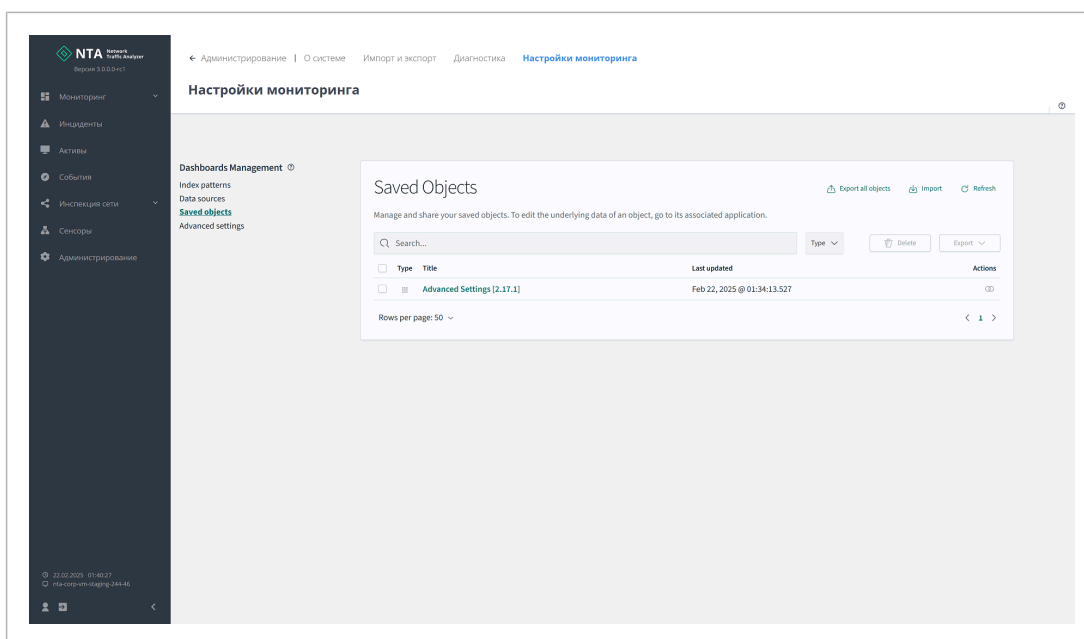


Рис. 83. Вкладка «Saved Objects»

4. Нажмите кнопку **Import**.

► **Результат шага:** появится окно импорта сохраненных объектов.

5. В открывшемся окне:

- Оставьте включенным переключатель **Automatically overwrite conflicts**.
- Перетащите или выберите по нажатию на **Import** файл формата `*.ndjson` с объектами раздела **Мониторинг**.

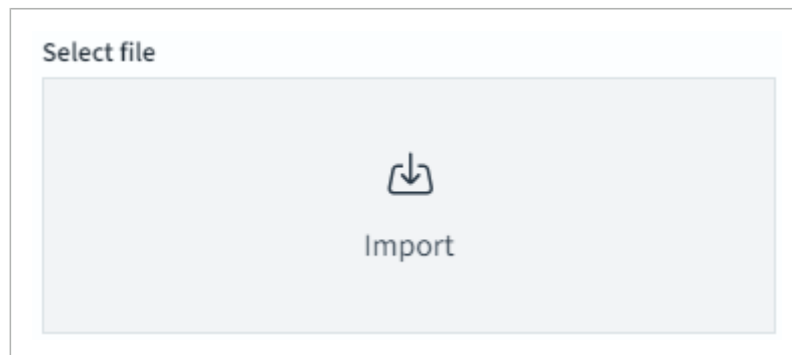


Рис. 84. Область выбора файла для импорта

6. Нажмите **Import**.

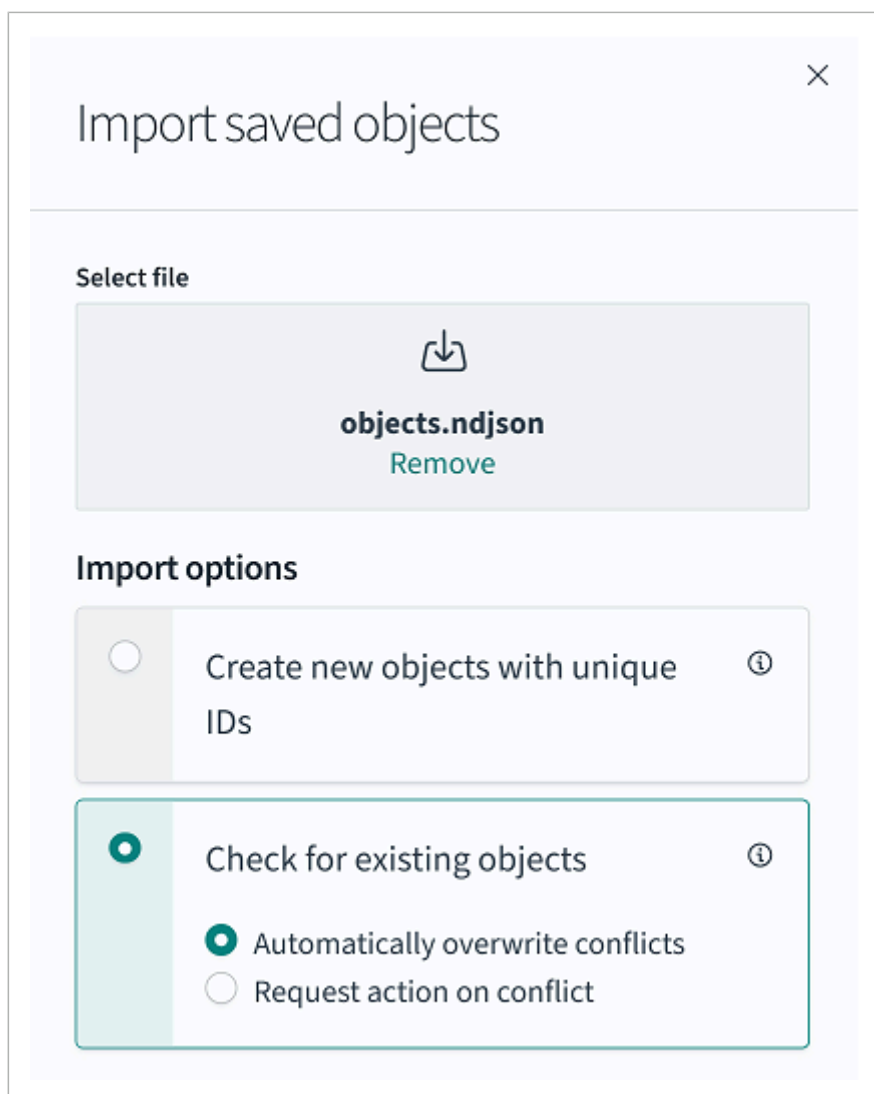


Рис. 85. Окно импорта сохраненных объектов

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**.

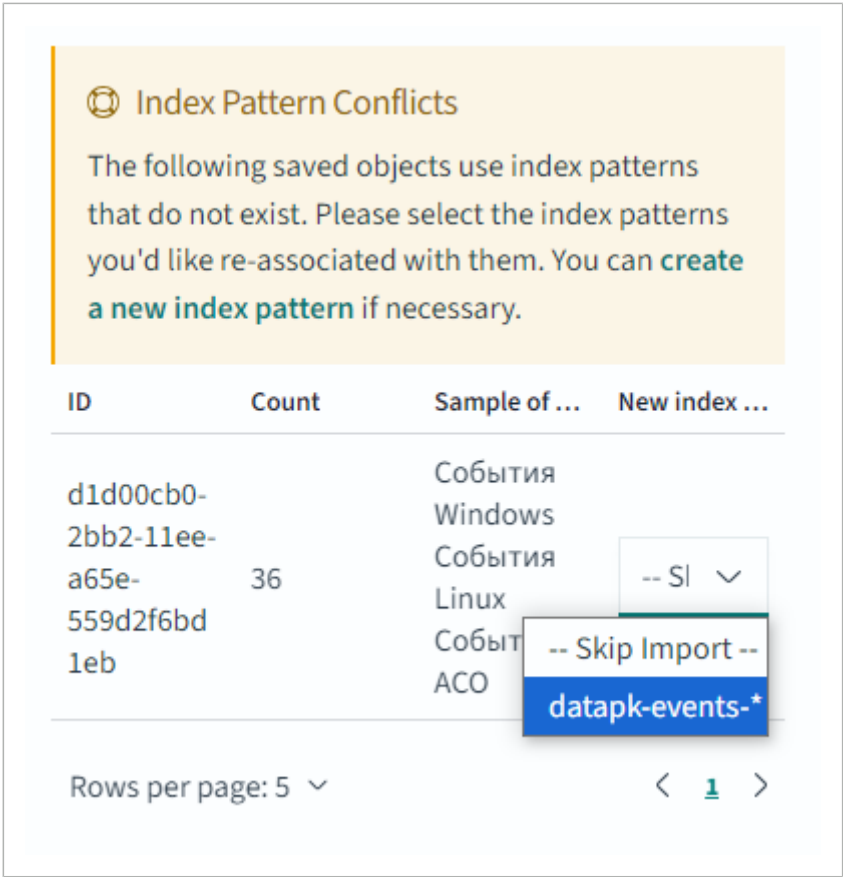


Рис. 86. Список шаблонов индекса в столбце «New Index Pattern»

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

5. Анализ и настройка инцидентов

В этом разделе:

1. [Анализ инцидентов](#)
2. [Изменение параметров инцидента](#)
3. [Удаление инцидента](#)
4. [Групповые операции над инцидентами](#)
5. [Настройка инцидентов](#)

На основе событий Комплекс создает записи об инцидентах.

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](#), а также событий, имеющих приоритет `critical`. Для просмотра списка инцидентов перейдите на страницу [Инциденты](#).

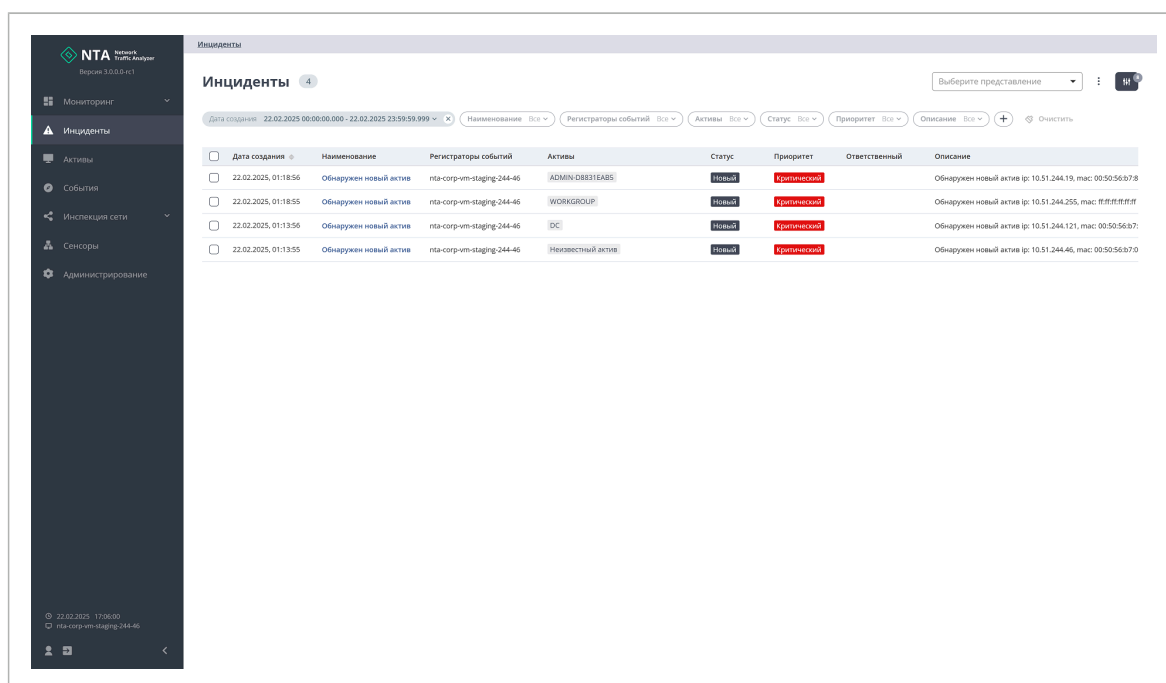


Рис. 87. Страница «Инциденты»

Поиск инцидентов

Для фильтрации воспользуйтесь панелью фильтров над списком инцидентов. Доступны фильтры по дате получения инцидента, обновления статуса, названию актива, содержанию сообщения и статусу инцидента. При фильтрации по статусу можно выбрать ранее удаленные статусы инцидентов — такие статусы имеют отметку (удалено).

При нажатии на название актива можно просмотреть краткую информацию о нем в окне **Информация об активе** и перейти на страницу актива с подробной информацией по ссылке **Подробнее**.

Информация об активе

Наименование: WORKGROUP

Описание:

Производитель:

Тип: Неизвестный тип

Дата создания: 24.02.2025, 12:04:33

Был доступен: 24.02.2025, 12:03:07

Сетевые атрибуты

Название	IP-адрес	MAC-адрес
	10.51.244.255	ff:ff:ff:ff:ff:ff

Подробнее

Закреть

Рис. 88. Просмотр краткой информации об активе

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 на странице [Администрирование](#) → [События и инциденты](#) → [Статусы инцидентов](#).

5.1. Анализ инцидентов

Подробности о выявленных службой корреляции инцидентах можно просматривать на странице [Инциденты](#). Сотрудник, расследующий инцидент информационной безопасности, может воспользоваться следующими возможностями:

1. Просмотр детальной информации об инциденте. Для просмотра детальной информации о конкретном инциденте нажмите в таблице на его наименование:
 - **Результат шага:** Откроется окно [Инцидент \[имя_инцидента\]](#).

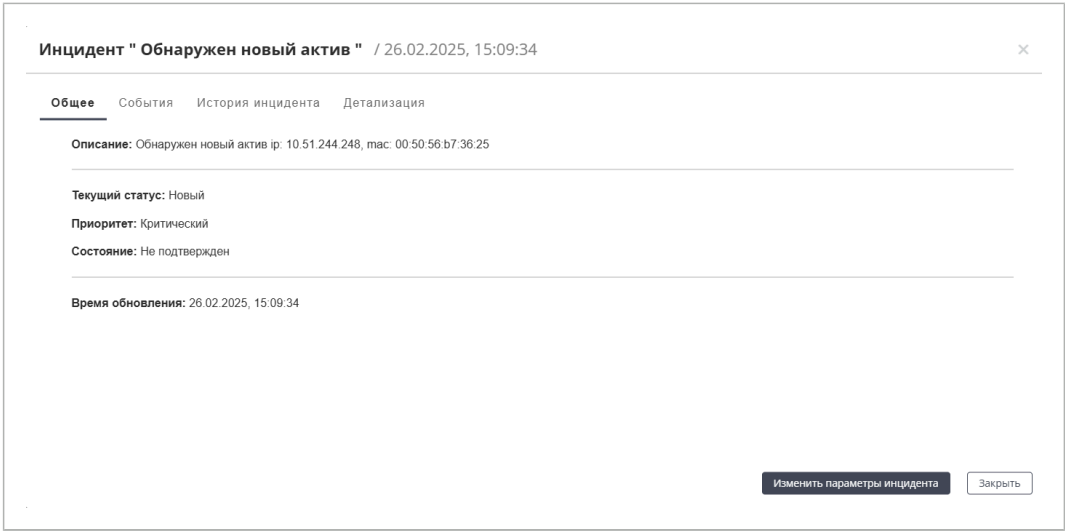


Рис. 89. Детальная информация об инциденте

2. Просмотр событий. Для просмотра списка событий, относящихся к инциденту:

- а. Откройте окно просмотра детальной информации об инциденте.
- б. Перейдите на вкладку **События**.
- **Результат шага:** Появится список событий, относящихся к инциденту.

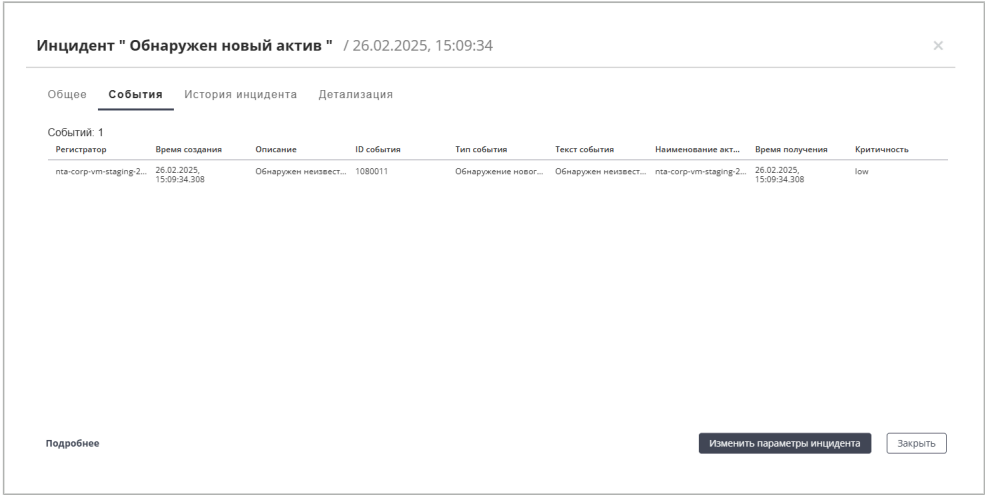


Рис. 90. События инцидента

- в. Нажмите **Подробнее** внизу вкладки, чтобы перейти на страницу **События**.

► **Результат шага:** Откроется страница **События**.

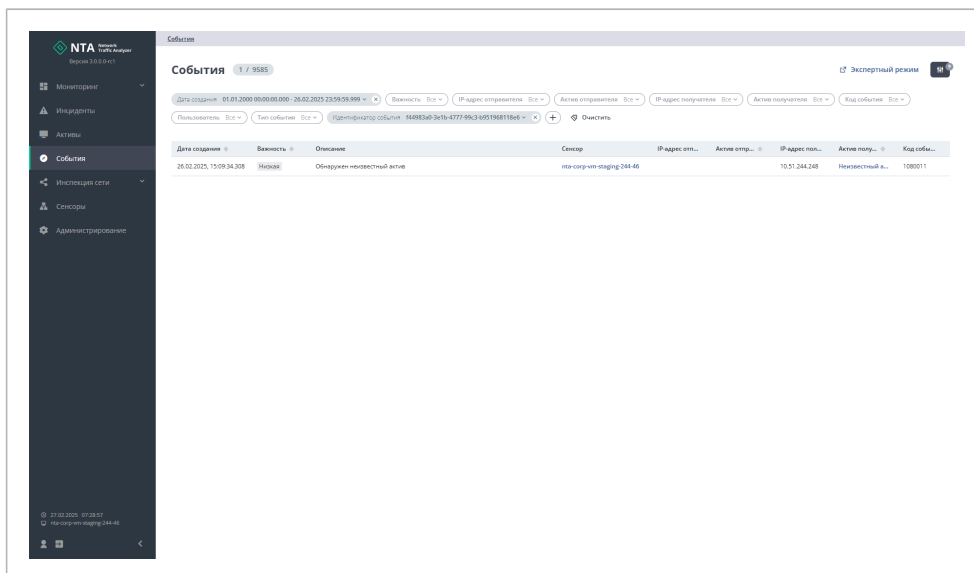


Рис. 91. Страница «События», содержащая список событий инцидента

а. Для отображения событий в экспертном режиме нажмите  **Экспертный режим** в правом верхнем углу.

► **Результат шага:** Откроется страница **Экспертный режим**.

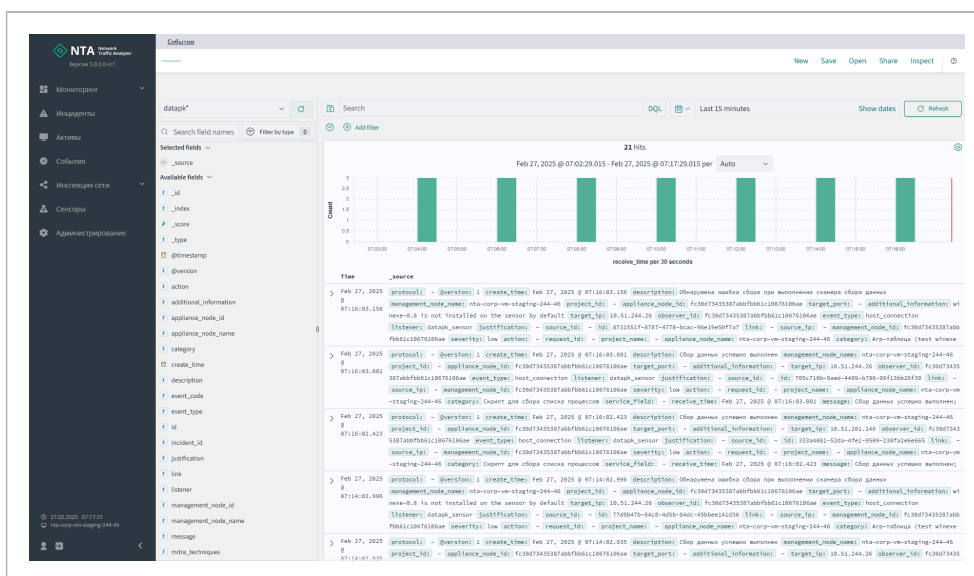


Рис. 92. Страница «Экспертный режим», содержащая список событий инцидента в экспертном режиме

3. Просмотр истории изменений инцидента. Для просмотра истории:

- Откройте окно просмотра детальной информации об инциденте.
- Перейдите на вкладку **История инцидента**.

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

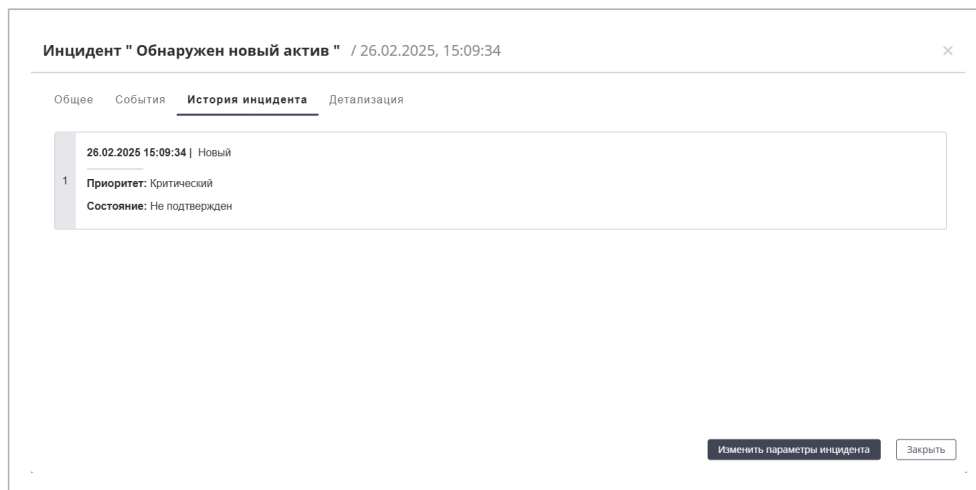


Рис. 93. История инцидента

4. Просмотр события, созданного службой корреляции. Для просмотра события корреляции:

- Откройте окно просмотра детальной информации об инциденте.
- Перейдите на вкладку **Детализация**.

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

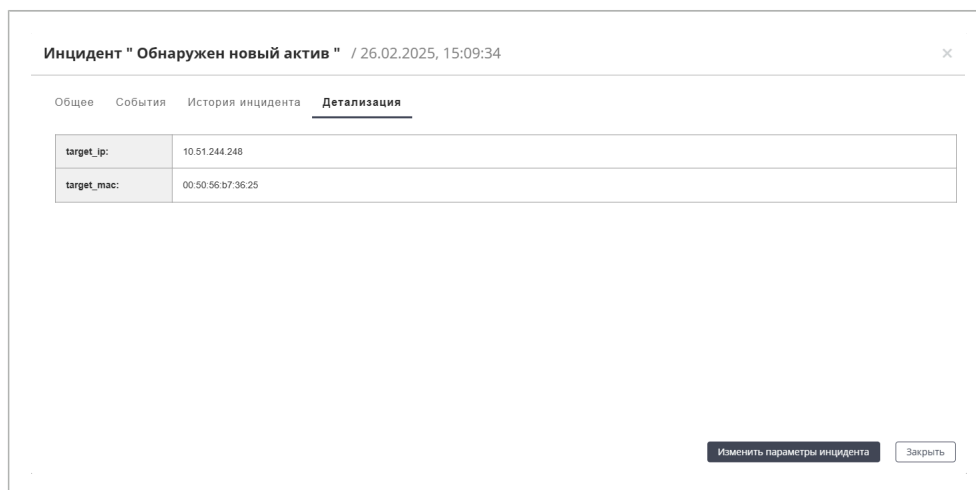


Рис. 94. Подробности события корреляции

5.2. Изменение параметров инцидента

В веб-интерфейсе Комплекса есть возможность подтвердить инцидент, изменить приоритет и статус инцидента, создать отчет. Для этого:

- Перейдите на страницу **Инциденты**.
- Слева от инцидента, который хотите изменить, установите чекбокс. Вы можете отметить сразу несколько инцидентов для выполнения операции над группой инцидентов.

- **Результат шага:** внизу страницы появится панель управления выбранным инцидентом.

- В появившейся панели нажмите кнопку нужного действия:

- **Статус** — изменить статус выбранных инцидентов;
- **Приоритет** — изменить приоритет выбранных инцидентов;
- **Отчет** — создать отчет по выбранным инцидентам в одном из доступных форматов: `html`, `xlsx`;
- **Подтвердить** — подтвердить обнаружение выбранных инцидентов;

- **Отменить подтверждение** — отменить подтверждение выбранных инцидентов;
- **Удалить** — удалить выбранные инциденты;
- **Выбрать все доступные строки** — выбрать все доступные строки с инцидентами.

4. Нажмите **Изменить параметры инцидента**.

► **Результат шага:** откроется окно **Изменение параметров инцидента**.

5. Заполните следующие обязательные поля:

- Статус** — этап работы над инцидентом (Новый, В работе, Закрыт);
- Приоритет** — степень важности и срочности работы над инцидентом;
- Обоснование** — пояснение произведенных операций над инцидентом.

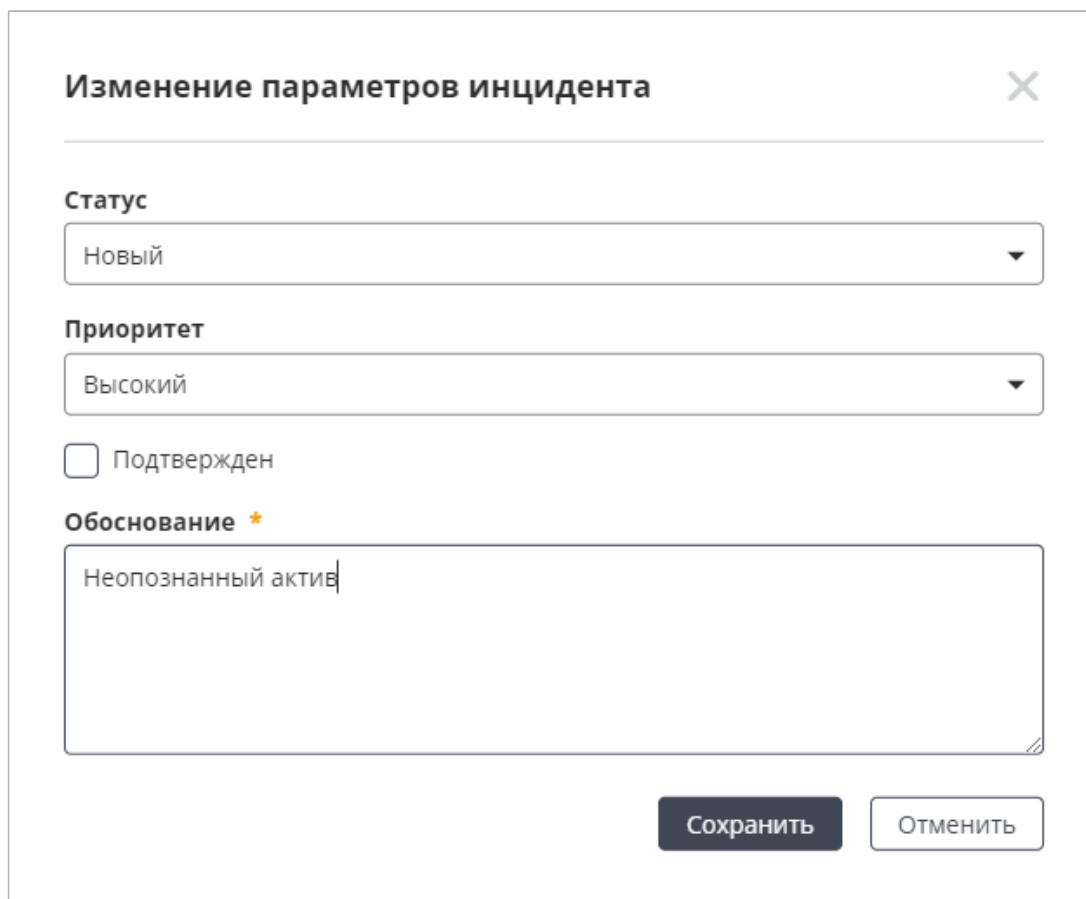


Рис. 95. Окно «Изменение параметров инцидента»

6. При необходимости установите чекбокс **Подтвержден**.



Подсказка:

Чтобы подтвердить инцидент без изменения статуса и обоснования, установите чекбокс **Подтвержден** в соответствующей колонке на странице **Инциденты**. Для того, чтобы воспользоваться возможностью, отрегулируйте отображение столбцов в правом верхнем углу страницы.

7. Нажмите **Обновить**.

► **Результат шага:** будет зафиксировано событие с данными о пользователе и заполненных полях.

5.3. Удаление инцидента

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

1. Перейдите на страницу [Инциденты](#).
2. Наведите курсор на неактуальный более инцидент.
3. Нажмите кнопку  (**Удалить инцидент**).
 - **Результат шага:** появится окно подтверждения удаления инцидента.
4. Во всплывающем окне введите обоснование удаления и нажмите **Удалить**.


Внимание:

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

Для данного действия необходимо обоснование

×

Введите текст обоснования

Подтвердить

Отменить

Рис. 96. Окно обоснования удаления инцидента

5. После удаления инцидента будет зафиксировано соответствующее событие, в котором будет отображено обоснование удаления.

5.4. Групповые операции над инцидентами

Комплекс позволяет выполнять групповые операции над инцидентами, используя фильтры, а именно:

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

Групповые действия применяются ко всем инцидентам, которые были выбраны фильтром, с помощью чекбокса слева от инцидента или с помощью кнопки **Выбрать все** в панели управления под списком инцидентов. Также применение групповых действий будет работать на всех уровнях, где инцидент существует. При этом предыдущее значение статуса или приоритета заменяется, а в истории фиксируется действие и обоснование. Для удаленных инцидентов обоснование будет сохранено в событиях.

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.



Прим.:

Подробнее о статусах см. в разделе «[Цветовая индикация и виды уведомлений](#)».

5.5. Настройка инцидентов

В этом разделе:

- [Экспорт и импорт политики корреляции и 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](#)

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. Служба корреляции событий работает на основе инструмента Esper. Для выполнения корреляции создаются правила обработки событий на языке EPL (Event Processing Language).

Механизм корреляции 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.

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 объектов защиты:

```
@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.

Примеры правил для корреляции событий:

- 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](#)».

Веб-интерфейс Комплекса позволяет [создавать](#) правила корреляции событий, либо [загружать](#) готовый список правил из файла формата *.json.

5.5.1. Экспорт и импорт политики корреляции и статусов инцидентов

В этом разделе:

- Импорт правил корреляции
- Импорт схемы корреляции
- Импорт политики корреляции
- Импорт статусов инцидентов
- Экспорт политики корреляции
- Экспорт статусов инцидентов

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

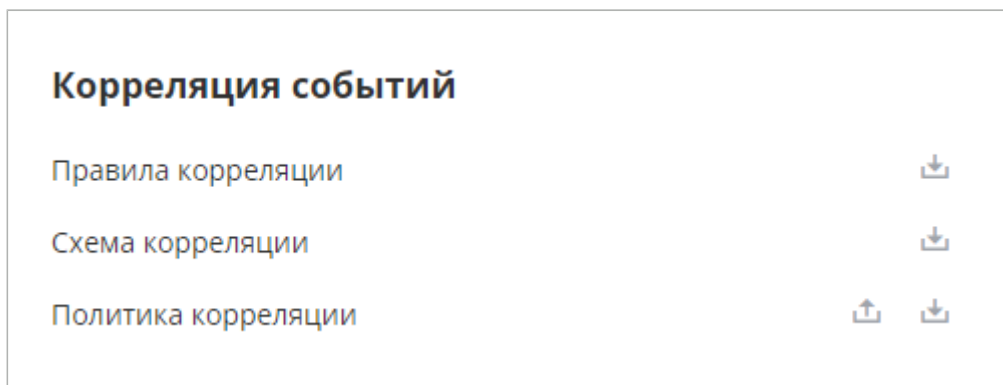


Рис. 97. Панель «Корреляция событий» на странице «Импорт и экспорт»

Управление экспортом и импортом Комплексы статусов инцидентов осуществляется на панели **Инциденты**.

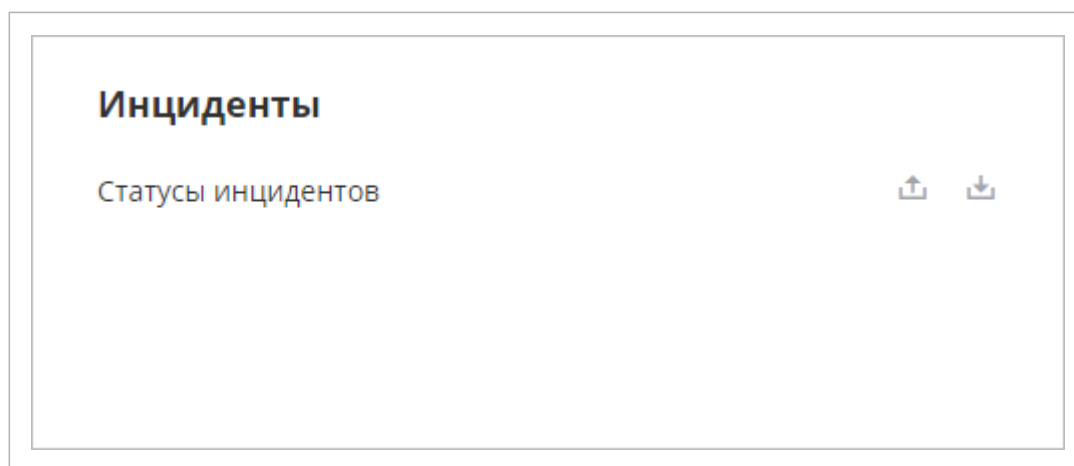


Рис. 98. Панель «Инциденты» на странице «Импорт и экспорт»

5.5.1.1. Импорт правил корреляции



Прим.:

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:
 - а. Действие для элементов, которые отсутствуют в новом справочнике:
 - **Оставить** — новые элементы будут добавлены к уже существующим;
 - **Удалить** — старые элементы будут удалены и добавлены новые
 - б. 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.

Подготовка к импорту

Перед обработкой выберите:

Действие для элементов, которые отсутствуют в новом справочнике :

☒ Оставить *i*

☐ Удалить *i*

Статус активности элементов справочника после импорта:

☒ Оставить как есть *i*

☐ Присвоить старым статус, как в файле *i*

Импортировать **Отменить**

Рис. 99. Окно импорта правил корреляции

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

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

5.5.1.2. Импорт схемы корреляции

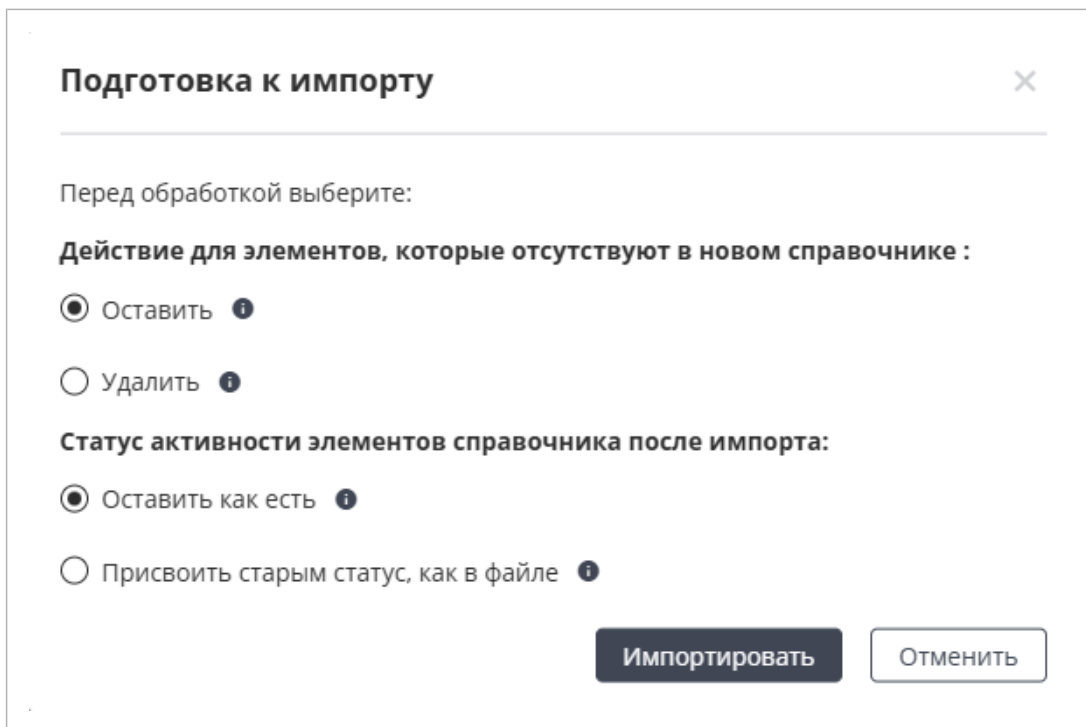


Прим.:

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:

- Перейдите на страницу **Администрирование** → **Основные настройки** → **Импорт и экспорт**.
- На панели Корреляция **событий** в строке **Схема корреляции** нажмите кнопку (**Импортировать**).
- В открывшемся окне укажите расположение импортируемого файла формата *.json и подтвердите выбор.
- В 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
 - 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.
- Нажмите **Импортировать** для запуска процедуры импорта.



Подготовка к импорту ✕

Перед обработкой выберите:

Действие для элементов, которые отсутствуют в новом справочнике :

☒ Оставить ⓘ

☐ Удалить ⓘ

Статус активности элементов справочника после импорта:

☒ Оставить как есть ⓘ

☐ Присвоить старым статус, как в файле ⓘ

Импортировать Отменить

Рис. 100. 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](#).

5.5.1.3. 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 справочнике:
 - **Оставить** — новые элементы будут добавлены к уже существующим;
 - **Удалить** — старые элементы будут удалены и добавлены новые
 - б. 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.

Подготовка к импорту

Перед обработкой выберите:

Действие для элементов, которые отсутствуют в новом справочнике :

☒ Оставить *i*

☐ Удалить *i*

Статус активности элементов справочника после импорта:

☒ Оставить как есть *i*

☐ Присвоить старым статус, как в файле *i*

Импортировать **Отменить**

Рис. 101. Окно импорта политики корреляции

► **Результат шага:** появится уведомление Список «Политика корреляции» успешно обновлен, и на страницах [Схема корреляции](#) и [Правила корреляции](#) появятся загруженные элементы.

- Убедитесь, что политика корреляции была успешно загружена. Для этого перейдите на страницы [Схема корреляции](#) и [Правила корреляции](#).

5.5.1.4. Импорт статусов инцидентов

Для импорта файла формата *.json со статусами инцидентов в Комплекс:

- Перейдите на страницу [Администрирование](#) → [Основные настройки](#) → [Импорт и экспорт](#).
- На панели «Инциденты» в строке «Статусы инцидентов» нажмите кнопку «Загрузить из файла».
- 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
- Убедитесь, что статусы были успешно загружены.

5.5.1.5. Экспорт политики корреляции

В составе политики корреляции экспортируются правила корреляции и схема корреляции.

Для экспорта политики корреляции событий в файл формата .json:

- Перейдите на страницу [Администрирование](#) → [Основные настройки](#) → [Импорт и экспорт](#).
- 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 экспортируемого файла и нажмите кнопку **Сохранить**.
 - **Результат шага:** файл `policy_correlation_[дата_и_время].json` будет загружен на компьютер.

5.5.1.6. 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 экспортируемого файла и нажмите кнопку **Сохранить**.
 - **Результат шага:** файл `policy_correlation_[дата_и_время].json` будет загружен на компьютер.

5.5.2. 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:
 - а. Нажмите  (**Состояние службы корреляции**).
 - **Результат шага:** откроется окно **Состояние службы корреляции**.
 - б. Ознакомьтесь со списком событий службы корреляции.

Состояние службы корреляции

Время создания	Описание
28.08.2024, 18:49:35	Перезапуск службы текущего анализа
28.08.2024, 18:49:35	Схема текущего анализа имеет ошибки компилирования или пуста, правила не применены, текущий ...
28.08.2024, 18:49:35	Ошибка в схеме корреляции для ретроспективного анализа: com.espertech.esper.compiler.client.EPCom...
28.08.2024, 18:49:30	Ошибка в схеме корреляции для текущего анализа: com.espertech.esper.compiler.client.EPCompileExcep...
28.08.2024, 17:55:09	Перезапуск службы текущего анализа
28.08.2024, 17:55:09	Схема текущего анализа успешно применена
28.08.2024, 17:55:08	Перезапуск службы текущего анализа
28.08.2024, 17:55:08	Схема текущего анализа успешно применена
28.08.2024, 17:55:08	Перезапуск службы текущего анализа
28.08.2024, 17:55:08	Схема текущего анализа успешно применена
28.08.2024, 17:48:37	Схема текущего анализа успешно применена
28.08.2024, 17:48:37	Запуск службы текущего анализа
28.08.2024, 17:48:37	Схема корреляции для ретроспективного анализа не содержит выражений
28.08.2024, 17:48:37	Схема корреляции для текущего анализа не содержит выражений

Заккрыть

Рис. 102. Окно «Состояние службы корреляции»



Прим.:

В случае появления ошибок в работе компонентов службы корреляции можно просмотреть подробности в колонке **Описание**.

5.5.3. 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:
 - а. На странице **Схема корреляции** нажмите **Создать элемент схемы**.

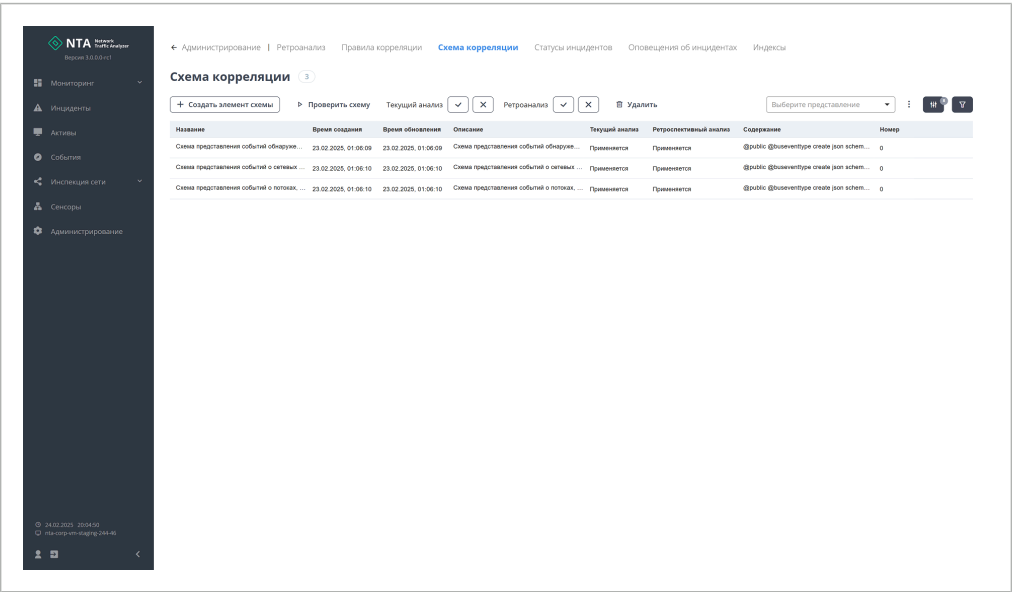


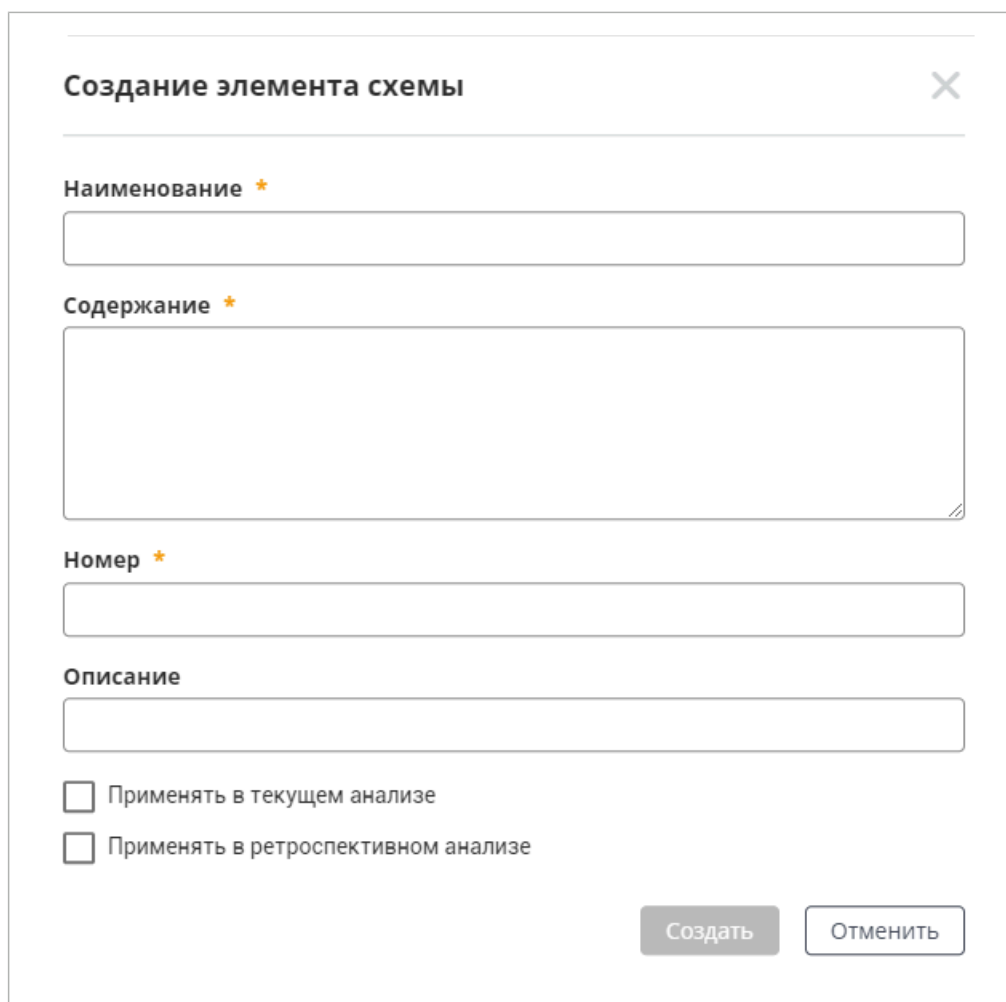
Рис. 103. Страница «Схема корреляции»

► **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.



Создание элемента схемы ✕

Наименование *

Содержание *

Номер *

Описание

☐ Применять в текущем анализе

☐ Применять в ретроспективном анализе

Создать **Отменить**

Рис. 104. Окно «Создание элемента схемы»

в. При необходимости введите описание и установите чекбоксы для применения в текущем или ретроспективном анализах.


Прим.:

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:

- Наведите курсор на строку с элементом схемы, который нужно отредактировать.
 - В правой части страницы нажмите  (**Редактировать**).
- **Результат шага:** откроется окно **Редактирование элемента схемы**.
- Измените необходимые параметры и нажмите **Сохранить**.

Редактирование элемента схемы

✕

Наименование *

Содержание *

```
@public @buseventtype create json schema unknown_host_detected as (action
string, additional_information string, appliance_node_id string,
appliance_node_name string, category string, create_time string, description
string, event_code string, observer_id string, observer_name string, id string,
observer_ip string, justification string, protocol string, receive_time string,
```

Номер *

Описание

☒ Применять в текущем анализе

☒ Применять в ретроспективном анализе

Сохранить

Отменить

Рис. 105. Окно «Редактирование элемента схемы»

4. Удаление. Для удаления одного элемента схемы:

- Наведите курсор на строку с элементом, который нужно удалить.
 - Нажмите  (**Удалить элемент схемы**).
- **Результат шага:** появится окно подтверждения удаления.

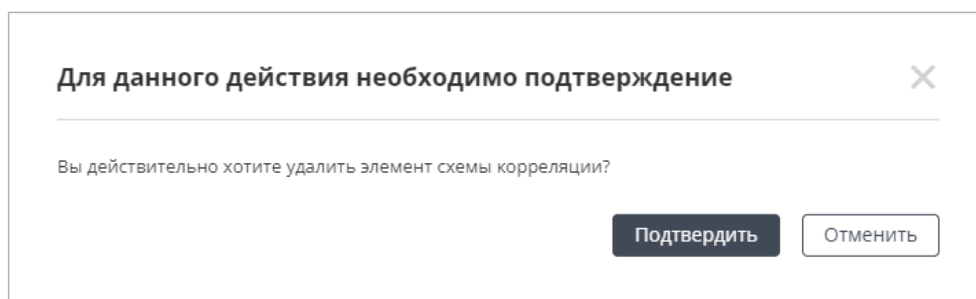


Рис. 106. Окно подтверждения удаления элемента схемы корреляции

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.

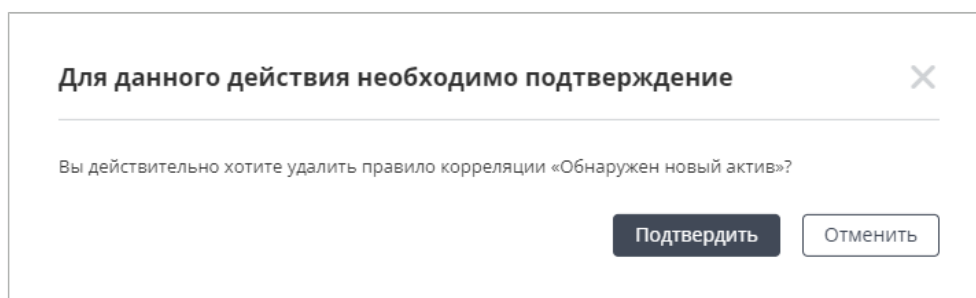


Рис. 107. Окно подтверждения удаления элементов схемы корреляции

в. Нажмите **Подтвердить**.

5.5.4. Управление правилами корреляции событий

Для управления правилами корреляции в веб-интерфейсе Комплекса предусмотрены следующие возможности:

- 1. Создание правил корреляции. Для создания:
 - а. Перейдите на страницу **Администрирование** → **События и инциденты** → **Правила корреляции**.

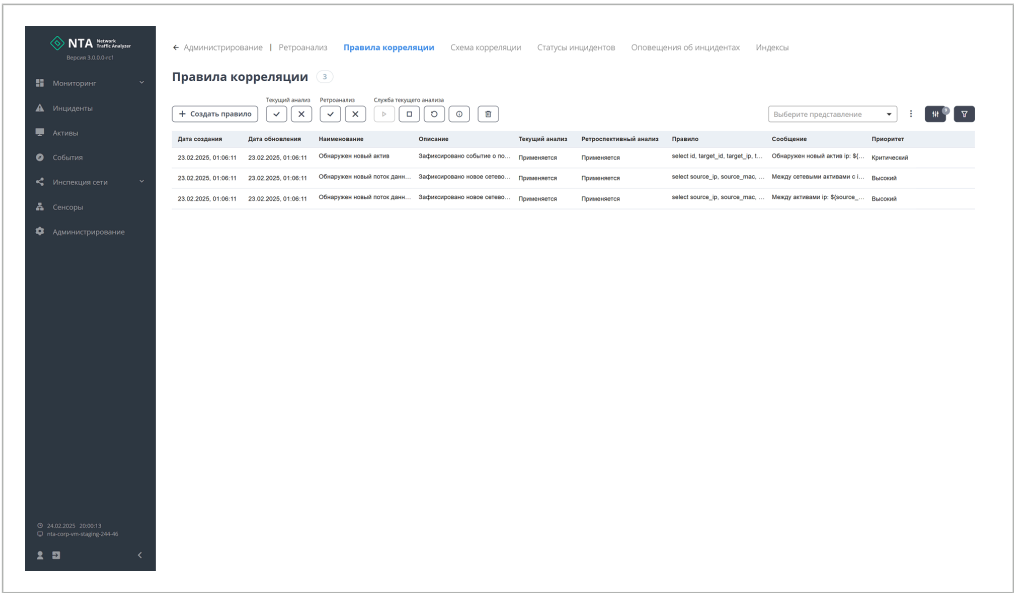


Рис. 108. Страница «Правила корреляции»

- б. Нажмите кнопку **Создать правило**. В открывшемся окне настройте следующие параметры:
 - наименование и описание;

 Прим.:

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.

Создание правила корреляции

✕

Наименование *

Описание

Правило *

Сообщение *

Приоритет *

Средний

▼

☐

Применять в текущем анализе

☐

Применять в ретроспективном анализе

Создать

Отменить

Рис. 109. Окно «Создание правила корреляции»

в. Нажмите кнопку **Создать** для подтверждения изменений.

i

Прим.:

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.

2. Редактирование правила корреляции. Для редактирования:

- а. Перейдите на страницу [Правила корреляции](#).
- б. В правой части страницы нажмите  (**Редактировать**).

► **Результат шага:** откроется окно **Редактирование правила корреляции**.

в. Измените необходимые параметры и нажмите **Сохранить**.

Редактирование правила корреляции

Наименование *
Обнаружен новый актив

Описание
Зафиксировано событие о появлении неизвестного активаТактика: TA0001 Пер

Правило *
select id, target_id, target_ip, target_mac, appliance_node_id from
unknown_host_detected

Сообщение *
Обнаружен новый актив ip: \${target_ip}, mac: \${target_mac}

Приоритет *
Критический

☒ Применять в текущем анализе
☒ Применять в ретроспективном анализе

Сохранить **Отменить**

Рис. 110. Окно «Редактирование правила корреляции»

3. Удаление правила корреляции. Для удаления:
 - а. Наведите курсор на строку с правилом, которое нужно удалить.
 - б. Нажмите (**Удалить правило**).
 - **Результат шага:** появится окно ввода обоснования удаления.
 - в. Введите обоснование удаления и нажмите **Подтвердить**.
4. Удаление нескольких правил корреляции. Для группового удаления правил:
 - а. Воспользуйтесь фильтрами на странице [Правила корреляции](#).
 - б. В верхней части страницы нажмите (**Удалить правила**).
 - **Результат шага:** появится окно ввода обоснования удаления.
 - в. Введите обоснование и нажмите **Удалить**.

5.5.5. 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 ранее (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. 111. 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.

5.5.5.1. 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:
 - а. 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:

- В верхней части страницы **Правила корреляции** нажмите  (**Состояние службы корреляции**).
- 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**).

5.5.5.2. 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:

- Нажмите кнопку  в верхнем правом углу страницы и воспользуйтесь представленными фильтрами.
- 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:

- Воспользуйтесь фильтрами на странице **Правила корреляции**.
- 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**.
- в. В открывшемся окне задайте следующие обязательные параметры анализа:

- название;
- период, за который будут проанализированы события;

Рис. 112. Окно запуска ретроспективного анализа

- г. При необходимости введите описание и фильтр в формате Lucene.
- д. Нажмите **Запустить**.



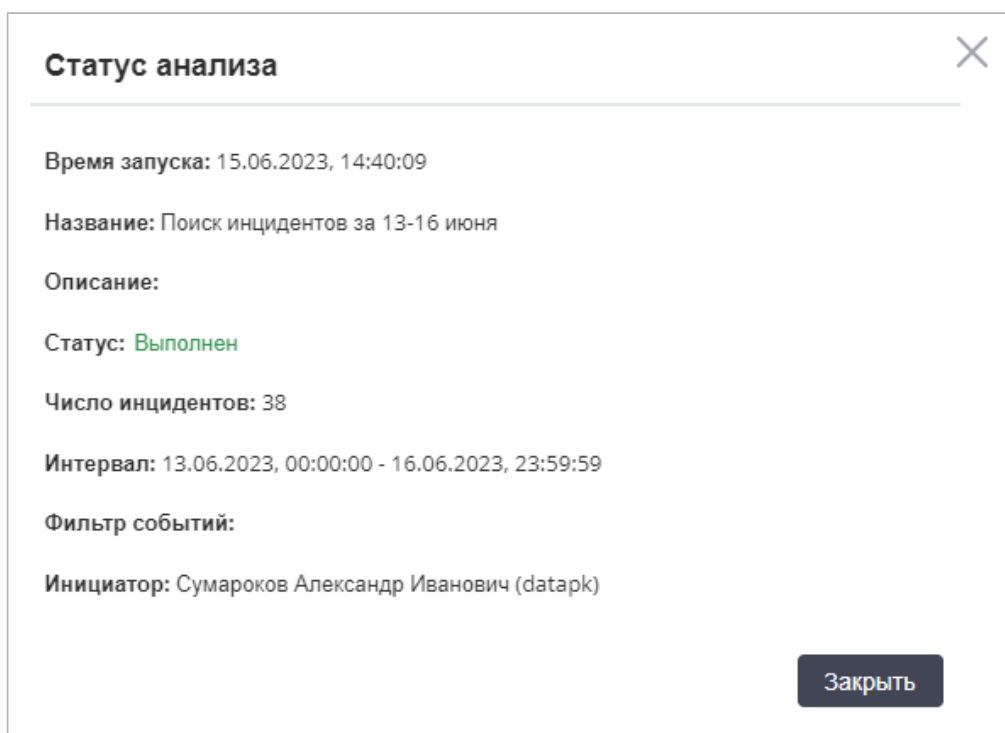
Подсказка:

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.

- е. 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:
 - а. 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. 113. Окно «Статус анализа»****См. также**[Недоступен сервис корреляции событий](#)

5.5.5.3. 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:

- а. 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.

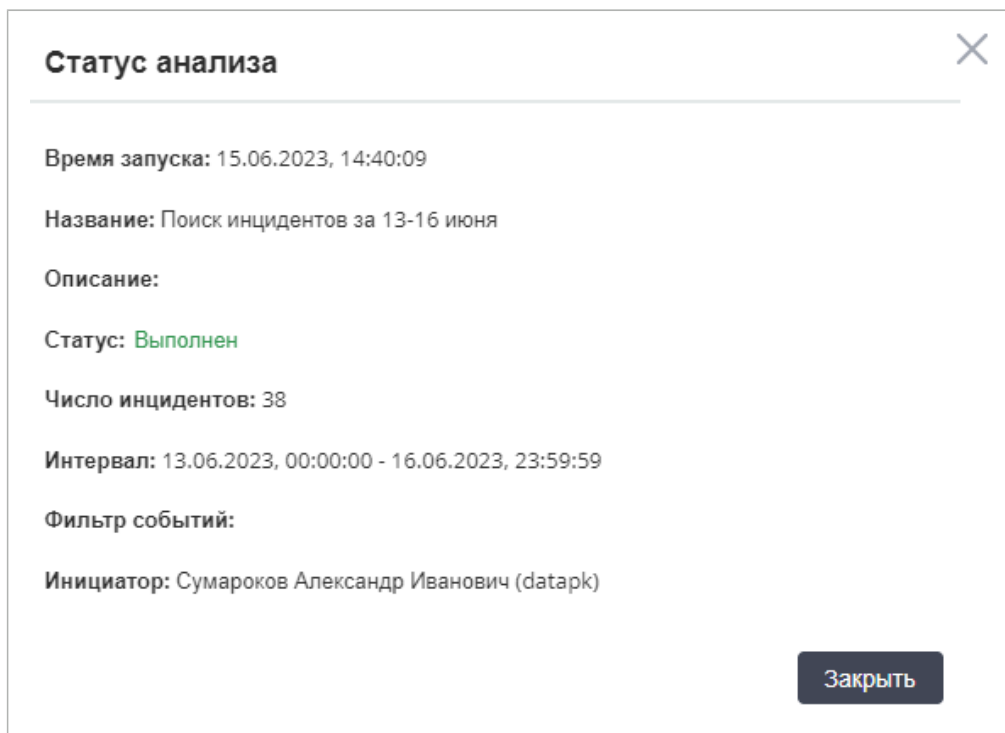


Рис. 114. Окно «Статус анализа»

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**.

Название	Время запуска	Статус	Число инцидентов
Поиск инцидентов за 13-16 июня	15.06.2023, 14:40:09	Выполнен	<u>38</u>

Рис. 115. 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](#)

5.5.6. 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](#).

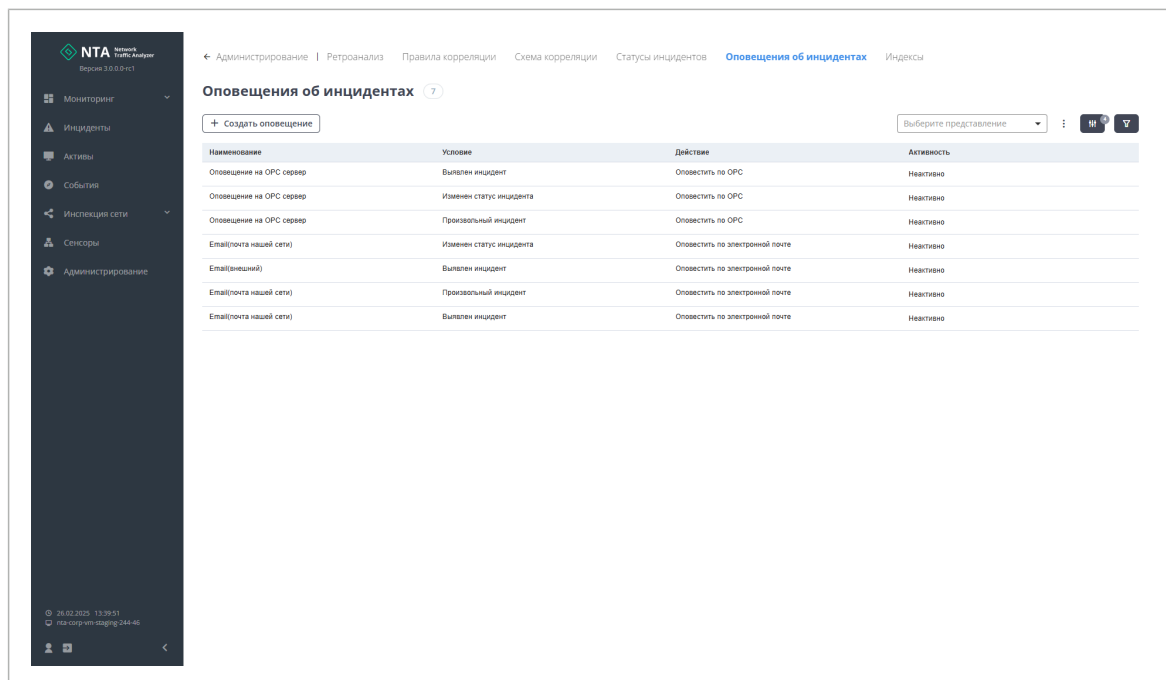


Рис. 116. Страница «Оповещения об инцидентах»

5.5.6.1. 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.

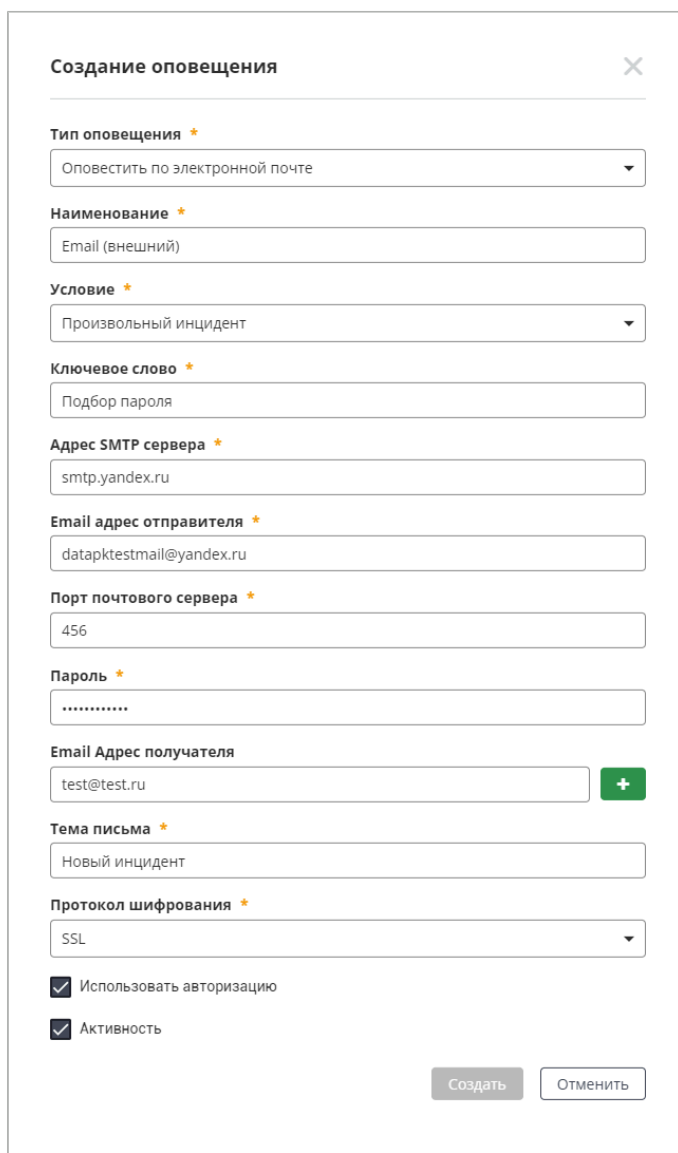


Прим.:

Доступен ввод значения только одного поля инцидента в одном ключевом слове. При этом допускается ввести строку из нескольких слов, которая целиком содержится в названии или описании инцидента.

- д. IP-адрес почтового сервера;
- е. Email-адрес почтового сервера;

- 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.



Создание оповещения

Тип оповещения *

Оповестить по электронной почте

Наименование *

Email (внешний)

Условие *

Произвольный инцидент

Ключевое слово *

Подбор пароля

Адрес SMTP сервера *

smtp.yandex.ru

Email адрес отправителя *

datapctestmail@yandex.ru

Порт почтового сервера *

456

Пароль *

.....

Email Адрес получателя

test@test.ru 

Тема письма *

Новый инцидент

Протокол шифрования *

SSL

☒ Использовать авторизацию

☒ Активность

Создать Отменить

Рис. 117. Окно «Создание оповещения» при настройке оповещения о любых инцидентах по электронной почте

4. Для проверки нажмите **Отправить тестовое оповещение**.

Пример

Оповещения будут приходить в следующем формате:

```
Описание события: [описание события].
Инцидент: [наименование инцидента].
Дата создания: [дата и время с указанием часового пояса в формате UTC].
Комплекс: [идентификатор Комплекса].
Объекты защиты: [наименования объектов защиты].
Описание инцидента: [текст с описанием].
Ссылка на инцидент: https://[IP-адрес текущего Комплекса]/app/incidents/[идентификатор инцидента]
```

5. Нажмите кнопку **Сохранить**.

5.5.6.2. 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.



Прим.:

Доступен ввод значения только одного поля инцидента в одном ключевом слове. При этом допускается ввести строку из нескольких слов, которая целиком содержится в названии или описании инцидента.

- д. IP-адрес 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;
- 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**;



Прим.:

Если выбран тип **String**, в качестве сообщения будет отправлено стандартное сообщение; если выбран тип **Boolean**, в качестве сообщения может быть отправлено только значение **true** или **false**.

- н. установите чекбокс **Активность** для включения активности правила.

Создание оповещения

Тип оповещения *
Оповестить по OPC

Наименование *
Оповещение на OPC сервер

Условие *
Выявлен инцидент

Адрес OPC сервера *
10.51.244.16

Порт OPC сервера *
55000

URL-путь

NamespaceIndex *
4

IdentifierType *
STRING

Identifier *
SCRIPT.script.datapk-string

Логин
test

Пароль
.....

Тип тега *
String

☒ Активность

Создать Отменить

Рис. 118. Окно «Создание оповещения» при настройке оповещения об инцидентах по протоколу OPC

4. Для проверки нажмите **Отправить тестовое оповещение**.

Пример

При выборе типа тега `String` оповещения будут приходить в следующем формате:

Описание события: [описание события].
 Инцидент: [наименование инцидента].
 Дата создания: [дата и время с указанием часового пояса в формате UTC].
 Комплекс: [идентификатор Комплекса].
 Объекты защиты: [наименования объектов защиты].
 Описание инцидента: [текст с описанием].
 Ссылка на инцидент: [ссылка].

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

5.5.7. Управление статусами инцидентов

Для изменения состава статусов инцидентов:

1. Перейдите на страницу [Администрирование](#) → [События и инциденты](#) → [Статусы инцидентов](#).
2. Для создания нового статуса инцидента:
 - а. 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. 119. 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. 120. 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.

в. Введите обоснование удаления статуса и нажмите **Подтвердить**.

6. 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, страница актива с детальной информацией, события, инциденты, источники, активы на карте сети), кнопки экспорта, импорта, создания отчетов, создания и удаления активов, столбцы статусов и статистики по доступности активов и инцидентам.

Актив	Наименование	Тип	Пром...	Описание	Группа	Интерфейсы	Инцид...	Метки	Доступ...	Дата соз...	Последн...	Провиде...	ОС
ADMIN-08831EAB5	ADMIN-08831EAB5	Неизвестный	VMware			10.51.244.19 00...	Критический		Недоступен	20.02.2025...	20.02.2025...		
CISCO-10U	CISCO-10U	Маршрутизатор		CISCO-10U...		10.51.244.22 00...		Тестировать	Недоступен	20.02.2025...			
CISCO-ASA-BRANCH	CISCO-ASA-BRANCH	Маршрутизатор		ciscoasa		10.51.201.9 005...		Тестировать	Недоступен	20.02.2025...			
DC	Неизвестный	VMware				10.51.244.121 0...	Критический		Недоступен	20.02.2025...	20.02.2025...		
Manager	Manager	APM		Хост на кот...		10.51.244.46 00...			Недоступен	20.02.2025...			
S7	S7	ПЛК		PLC-S7_TK1		10.51.201.141 0...		Тестировать	Недоступен	20.02.2025...			
SE-CE14	SE-CE14	ПЛК		SE-CE14_D...		10.51.202.28 00...		Тестировать	Недоступен	20.02.2025...			
WIN-75P10VMS	WIN-75P10VMS	APM		WN7_SP1...		10.51.244.16 00...		win7m...	Недоступен	20.02.2025...		Microsoft C...	Microsoft ...
WIN-98W5J3ACT	WIN-98W5J3ACT	Неизвестный	VMware			10.51.244.25 00...	Неизвестный		Недоступен	20.02.2025...	20.02.2025...		
WIN10_TK2	WIN10_TK2	APM		DESKTOP-C...		10.51.202.19 00...		Рабочая...	Недоступен	20.02.2025...			
Win2003P2_TK1	Win2003P2_TK1	Сервер		Win2003_S...		10.51.201.145 0...		Сервер	Недоступен	20.02.2025...			

Рис. 121. 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 обнаруженным инцидентам.

Подсказка:
Подробнее о статусах активов см. разделы «[Статусы активов](#)» и «[Индикация активов](#)».

☐	Актив	Наименование	Тип	Прои...	Описание	Доступн...	Инцид...	Интерфейсы	Метки	Группа	Дата соз...
☐		Win2KSP4_TK1	APM		Win2000_S...	Недоступен		10.51.201.147 0...	Сервер		23.02.2025,...
☐		Win2003SP2_TK1	Сервер		Win2003_S...	Недоступен		10.51.201.145 0...	Сервер		23.02.2025,...
☐		Неизвестный актив	Неизвестный ...	VMware		Недоступен	Критическ...	10.51.244.46 00:...			23.02.2025,...
☐		WIN10_TK2	APM		DESKTOP-C...	Недоступен		10.51.202.19 00:...	Рабочая...		23.02.2025,...
☐		WIN_7_Company	APM		Win7-SP1.c...	Недоступен		10.51.200.133 0...	Рабочая...		23.02.2025,...
☐		Manager	APM		Хост на кот...	Недоступен		10.51.244.46 00:...			23.02.2025,...
☐		WORKGROUP	Неизвестный ...			Недоступен	Критическ...	10.51.244.255 ff...			24.02.2025,...
☐		WINDOWS-XP-SP2_T...	APM		WINDOWS-...	Недоступен		10.51.201.139 0...	Рабочая...		23.02.2025,...
☐		SE_CE14	ПЛК		SE_CE14_D...	Недоступен		10.51.202.28 00:...	Технол...		23.02.2025,...

Рис. 122. 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.

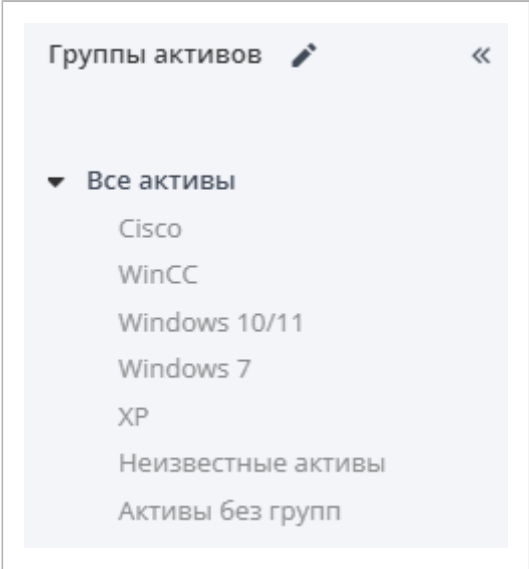


Рис. 123. Панель управления группами активов

По нажатию на иконку актива или его наименование появляется **Страница актива**, отображающая:

- описание актива: наименование, описание, производитель, тип, группа, дата и время создания, дата и время, когда актив последний раз был доступен;
- 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 инцидентам;
- связанные данные, позволяющие просмотреть данные об активе в других разделах:
 - инциденты;
 - события;
 - источники.

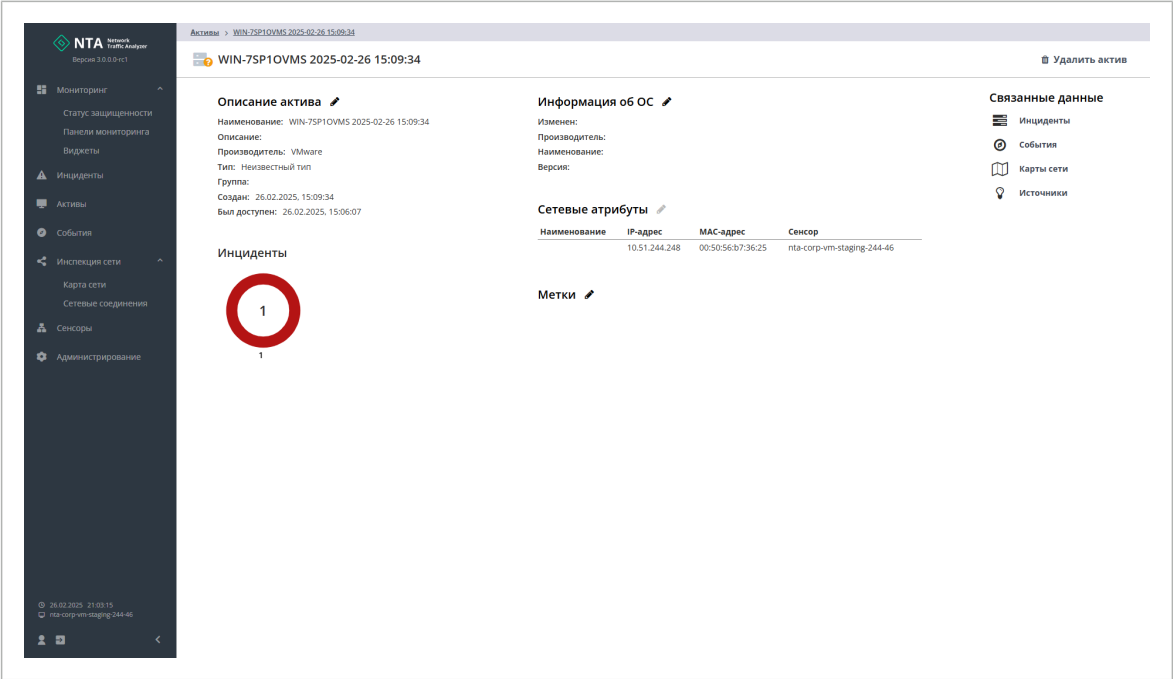


Рис. 124. Карточка актива

6.1. 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**.

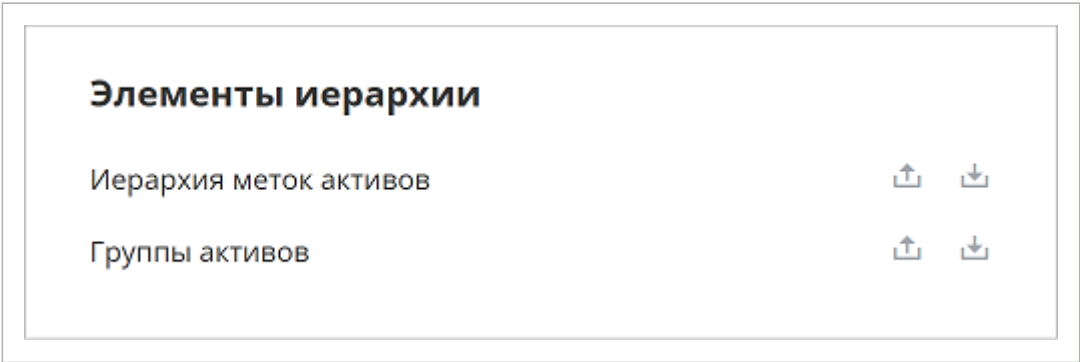


Рис. 125. Панель «Элементы иерархии» на странице «Импорт и экспорт»

6.1.1. Экспорт 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:** файл со списком активов, их групп, меток с названием `hosts_[дата_и_время].json` будет загружен на компьютер в директорию загрузки по умолчанию.
3. В открывшемся окне укажите расположение экспортируемого файла и нажмите кнопку **Сохранить**.
 - **Результат шага:** файл `hosts_[дата_и_время].json` будет загружен на компьютер.



ОСТОРОЖНО:

В файл `hosts_[дата_и_время].json` будут добавлены все активы, независимо от выбора и фильтрации активов.

6.1.2. Экспорт групп активов

Для экспорта справочника с иерархией 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 `host_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 название сформированного файла под заголовком **Результат последнего экспорта**.
4. В открывшемся окне укажите расположение экспортируемого файла и нажмите кнопку **Сохранить**.
 - **Результат шага:** файл `host_groups_[дата_и_время].json` будет загружен на компьютер.

6.1.3. Импорт активов

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 перенесите файл из проводника. В открывшемся окне укажите расположение импортируемого файла формата *.json и подтвердите выбор.

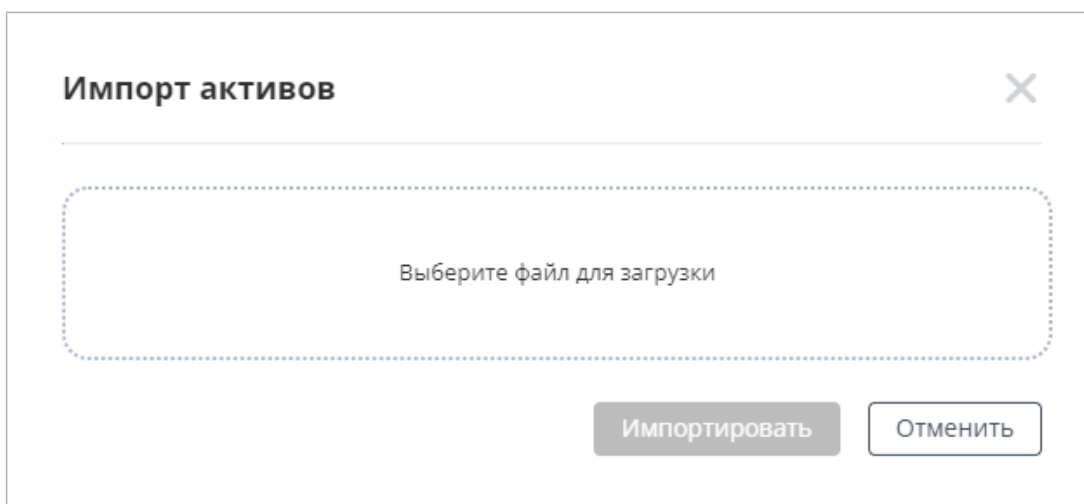


Рис. 126. Окно «Импорт активов»

4. Нажмите кнопку **Импортировать** для выполнения импорта списка активов.
5. Убедитесь, что на странице **Активы** активы успешно импортированы из файла.

6.1.4. Импорт групп активов

Для импорта справочника с пользовательской иерархией 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**.

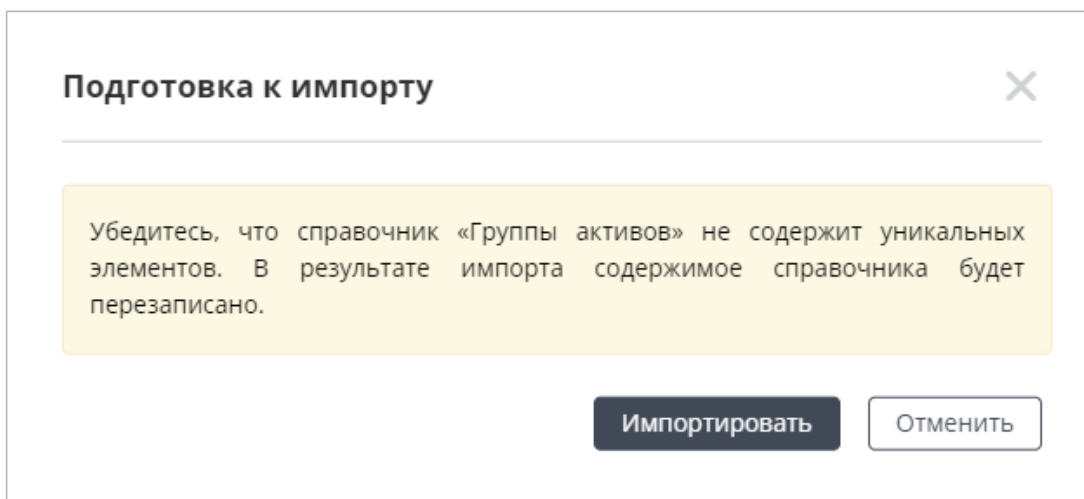


Рис. 127. Окно «Подготовка к импорту» при импорте групп активов

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.

6.2. Управление активами

В этом разделе:

- [Кнопки управления активами](#)
- [Фильтрация списка активов](#)

6.2.1. Кнопки управления активами

В верхней части страницы [Активы](#) расположен ряд кнопок для управления выбранными активами. При выборе с помощью чекбокса ☒ одного актива внизу страницы также появляется панель с кнопками управления.

Ознакомиться со списком кнопок вы можете в таблице ниже ([Таблица 2. Кнопки управления активами](#)).

Табл. 2. Кнопки управления активами

КНОПКА	ДЕЙСТВИЕ	СТРАНИЦА	УСЛОВИЯ ДОСТУПНОСТИ
	Создание актива	Создание актива	—
	Удаление выбранных активов	Удаление активов	Кнопки доступны, если выбран хотя бы один актив
	Создание отчета по выбранным активам	Выгрузка отчетов	
	Экспорт активов	Экспорт активов	Выполняется для всех активов независимо от того, какие активы были выбраны или отфильтрованы
	Импорт активов	Импорт активов	—

При клике в строке выбранного актива в любой ячейке, не содержащей гиперссылку, появляется карточка с информацией об активе. Кнопки перехода на смежные страницы доступны в блоке **Связанные данные**.

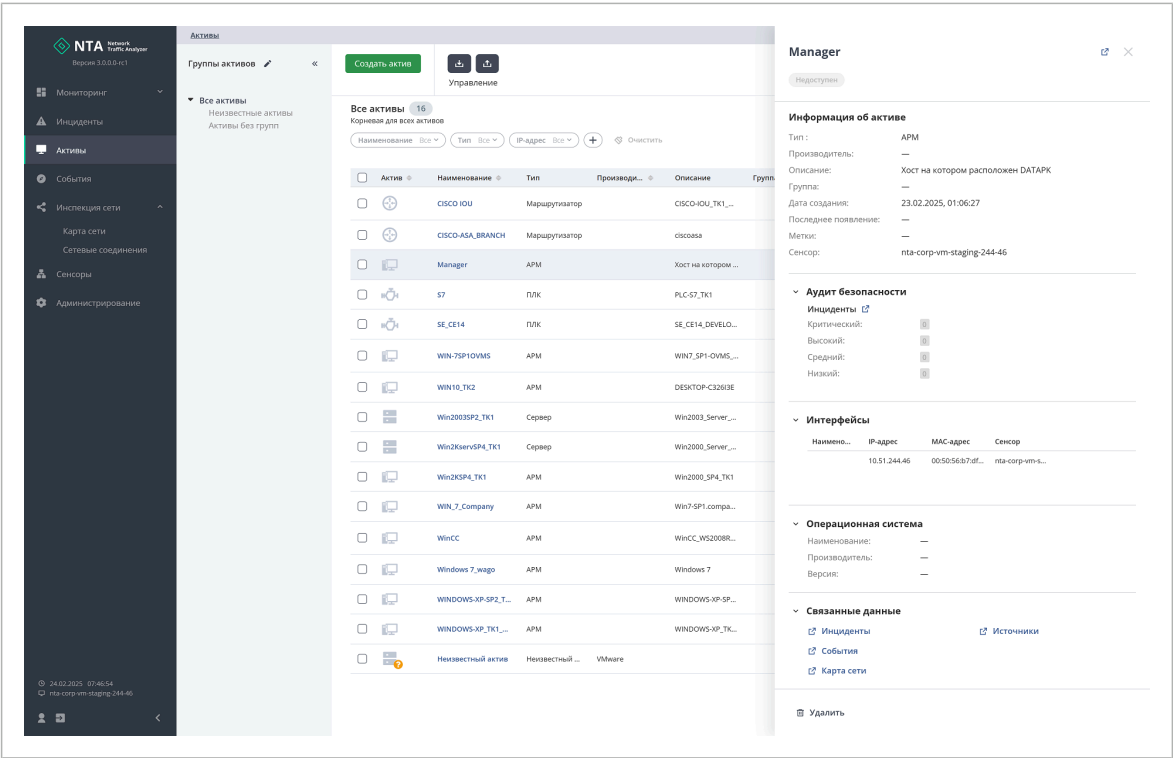


Рис. 128. Карточка выбранного актива

6.2.2. Фильтрация списка активов

Комплекс позволяет фильтровать обнаруженные активы. На странице **Активы** над списком активов расположена панель фильтрации.

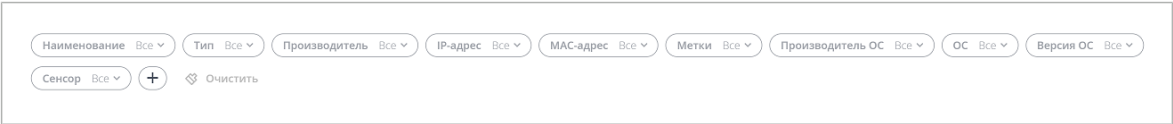


Рис. 129. Панель фильтров на странице «Активы»

Доступны следующие фильтры:

1. **Наименование.** Фильтрация выполняется по наименованиям обнаруженных активов. Можно выбирать несколько наименований.
2. **Тип.** Фильтрация выполняется по типам, назначенным активам. Можно выбирать сразу несколько типов активов.
3. **Производитель.** Фильтрация выполняется по наименованиям производителей аппаратного обеспечения актива, информация о которых получена Комплексом. Можно выбирать сразу несколько наименований.
4. **IP-адрес.** Фильтрация выполняется по IP-адресам, привязанным к сетевым атрибутам активов. Для выбора нескольких IP-адресов:
 - а. Полностью введите IP-адрес в поле.



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.

- б. Нажмите **Добавить** в строке ниже для подтверждения выбора.
 - с. Повторите пункты 4.a-4.b для других IP-адресов, по которым необходимо отфильтровать активы.
5. **MAC-адрес.** Фильтрация выполняется по ключевому слову среди MAC-адресов, привязанных к сетевым атрибутам активов. Для ввода в поле разрешены цифры и английские символы.



Внимание:

Для октетов MAC-адресов допускается использовать следующие разделители: ., -, :, либо не использовать разделители.

6. **Метки.** Фильтрация выполняется по меткам, назначенным активам. В раскрывающемся списке можно выбирать сразу несколько меток с помощью чекбоксов.
7. **Производитель ОС.** Фильтрация выполняется по ключевому слову среди наименований производителей ОС или прошивок, информация о которых получена Комплексом.
8. **ОС.** Фильтрация выполняется по ключевому слову среди наименований ОС или прошивок, информация о которых получена Комплексом.
9. **Версия ОС.** Фильтрация выполняется по ключевому слову среди версий ОС или прошивок, информация о которых получена Комплексом.
10. **Сенсор.** Фильтр содержит наименования сенсоров, подключенных к Комплексу. Можно выбирать сразу несколько наименований. При применении фильтра отобразятся активы, чьи интерфейсы сбора данных привязаны к выбранным сенсорам.



Внимание:

Фильтрация может повлиять на доступность кнопки  (**Групповое удаление**). Кнопка становится недоступна при следующих условиях:

- Применен хотя бы один из фильтров: **Производитель ОС, ОС, Версия ОС**;
- По результатам фильтрации получилось больше 100 записей;
- Применено действие **Выбрать все записи (>100) в данной таблице**.

6.3. 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**.
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 наименование производителя.



Внимание:

При создании актива невозможно автоматическое распознавание производителя по нажатию кнопки **определить**.

Создание актива ×

Тип *

Неизвестный тип ▾

Наименование *

Неизвестный актив

Описание

Производитель

определить

Группа

Не выбрано ▾

Создать

Отменить

Рис. 130. Окно создания нового актива

4. Нажмите кнопку **Создать** для подтверждения изменений.

6.4. 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 для упрощения управления активами.

По умолчанию доступны следующие группы:

- **Неизвестные активы** — группа, в которую автоматически добавляются все Активы с типом «неизвестный»;
- **Активы без групп** — группа, в которую автоматически добавляются все Активы, у которых не заполнено поле **Группа**.

Удаление и редактирование этих групп, а также добавление Актив в эти группы вручную и удаление Актив из этих групп недоступно.

Список групп отображается на панели в левой части экрана. Если в списке выбрана конкретная группа Актива, то фильтры будут применяться только для элементов этой группы.

6.4.1. Создание группы активов

Для создания группы активов:

1. Перейдите на страницу [Активы](#).
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.

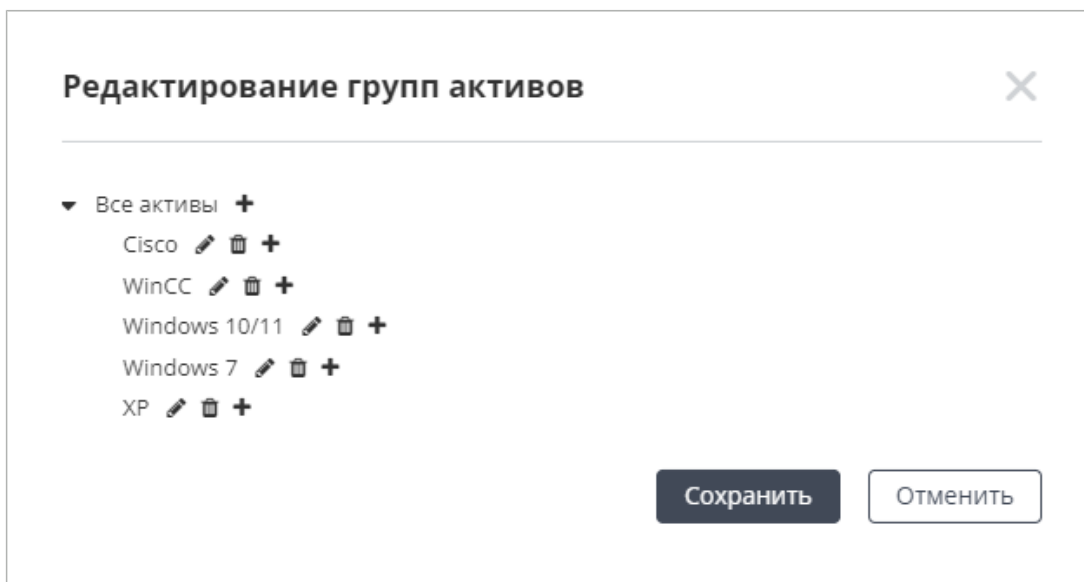


Рис. 131. Окно «Редактирование групп активов»

- **Результат шага:** появится окно **Создание группы активов**.
4. В окне создания задайте наименование и описание новой группы. При необходимости выберите другую вышестоящую группу.

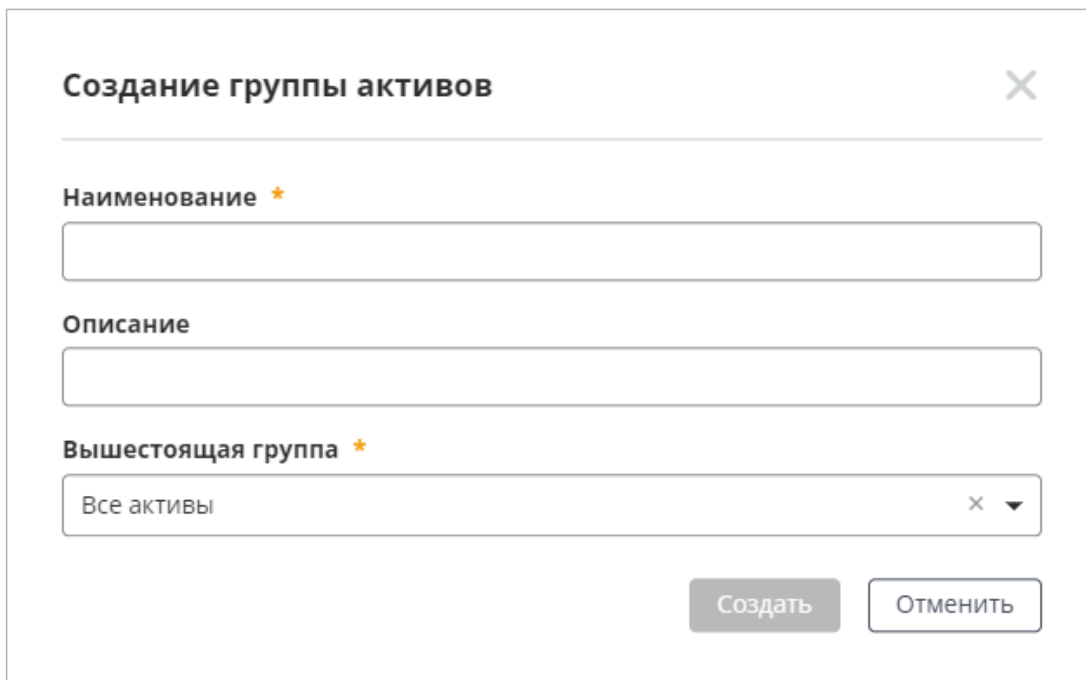


Рис. 132. Окно «Создание группы активов»

5. Нажмите кнопку **Создать** для подтверждения локальных изменений.

 **Внимание:**

Без сохранения в окне редактирования групп 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 будут сохранены, окно редактирования групп будет закрыто, появится уведомление Список "Группы активов" успешно обновлен.

6.4.2. 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, выбрав настройки в панели фильтрации.
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, нажмите левую кнопку мыши и немного сдвиньте курсор.

► **Результат шага:** появится прямоугольник 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.

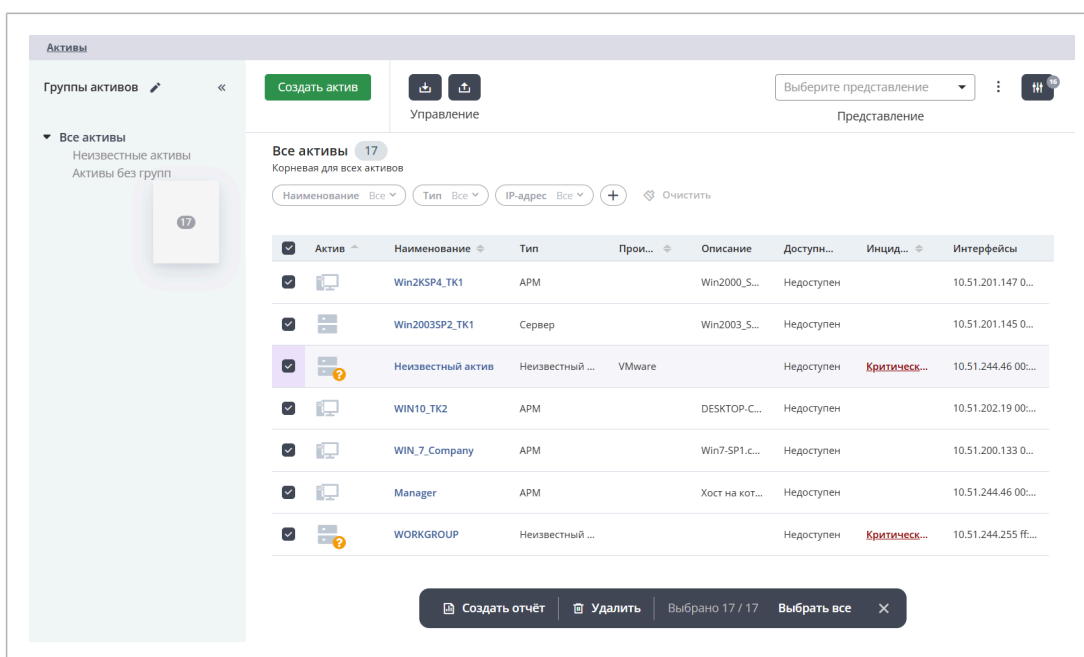


Рис. 133. Добавление активов в группу

► **Результат шага:** появится окно подтверждения добавления активов в группу.

5. Для подтверждения переноса нажмите **Подтвердить**.

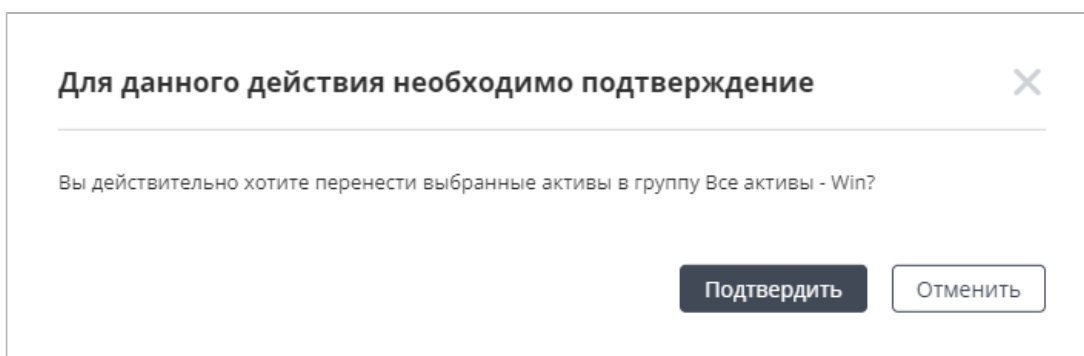


Рис. 134. Окно подтверждения перемещения актива

- **Результат шага:** активы будут перенесены в группу. В правом верхнем углу экрана появится уведомление Перемещение актива прошло успешно.

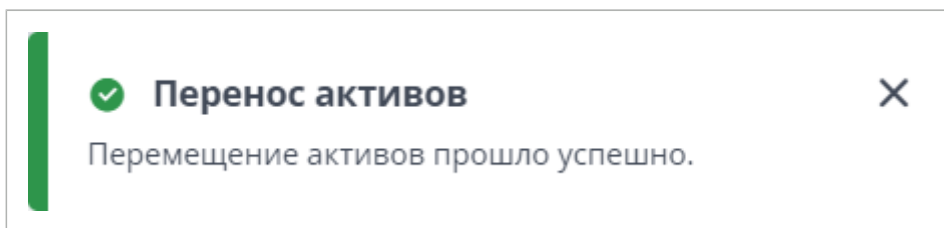


Рис. 135. Уведомление «Перемещение актива прошло успешно»

6. При необходимости группу можно также изменить 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.

Если необходимо исключить актив из группы, измените соответствующее поле в окне **Основная информация об активе**.

Основная информация об активе ✕

Тип *

APM ▼

Наименование *

Win2KSP4_TK1

Описание

Win2000_SP4_TK1

Производитель

определить

Группа

Не выбрано ▼

Сохранить **Отменить**

Рис. 136. Окно редактирования основной информации об активе

6.4.3. Управление группами активов

Управление группами активов может осуществляться на странице [Активы](#). 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.

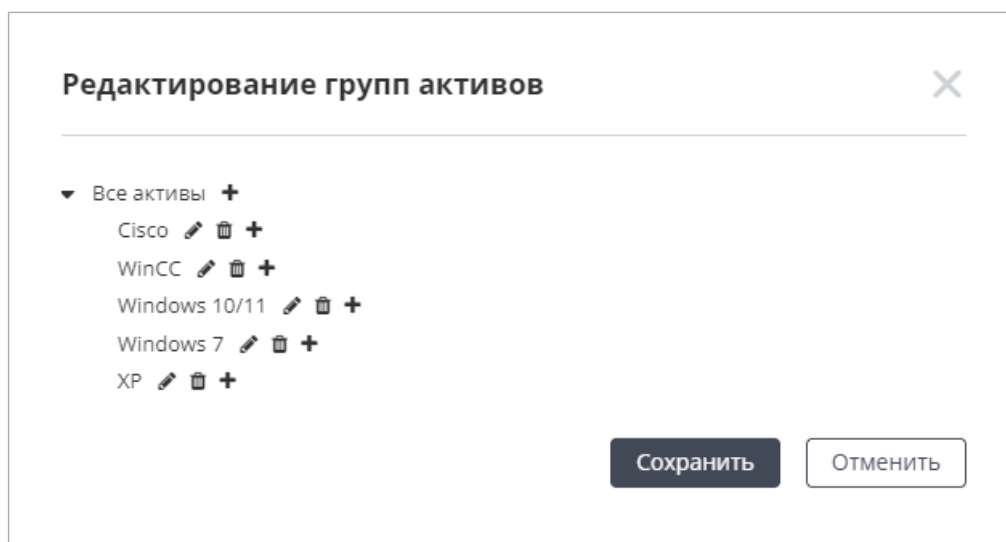


Рис. 137. Окно «Редактирование групп активов»

- **Результат шага:** появится окно **Редактирование группы активов**.

в. Измените необходимые параметры группы активов.

Рис. 138. 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.

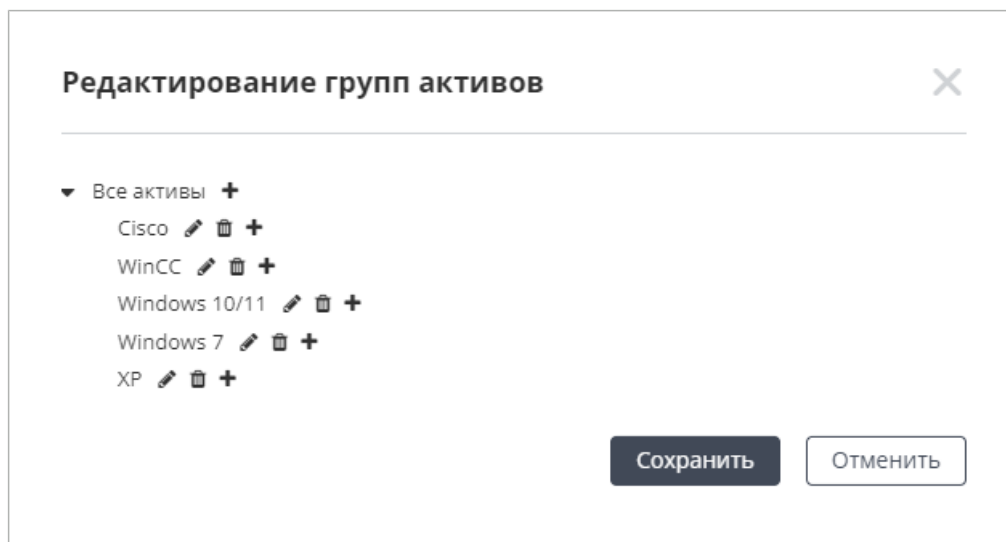


Рис. 139. Окно «Редактирование групп активов»

► **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.

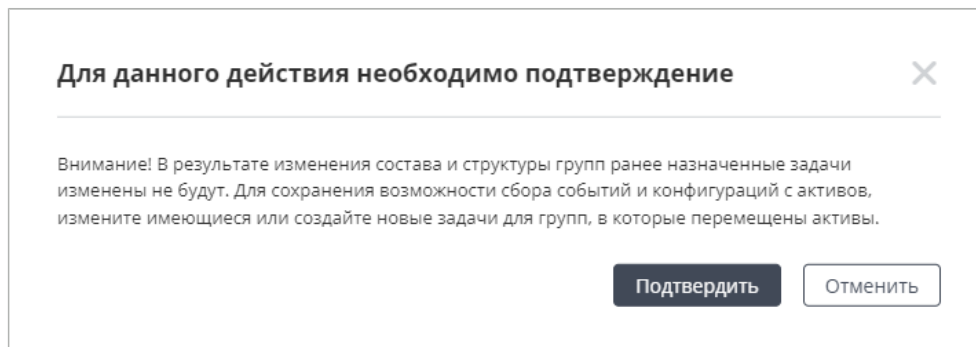


Рис. 140. Окно подтверждения изменений групп

д. Нажмите **Подтвердить** для сохранения изменения состава групп.

► **Результат шага:** изменения будут сохранены, окно редактирования групп будет закрыто.

6.5. Редактирование актива

Для редактирования актива:

1. Перейдите на страницу [Активы](#).
2. Нажмите на иконку или наименование актива.



Рис. 141. Переход на страницу актива

► **Результат шага:** откроется [Страница актива](#).

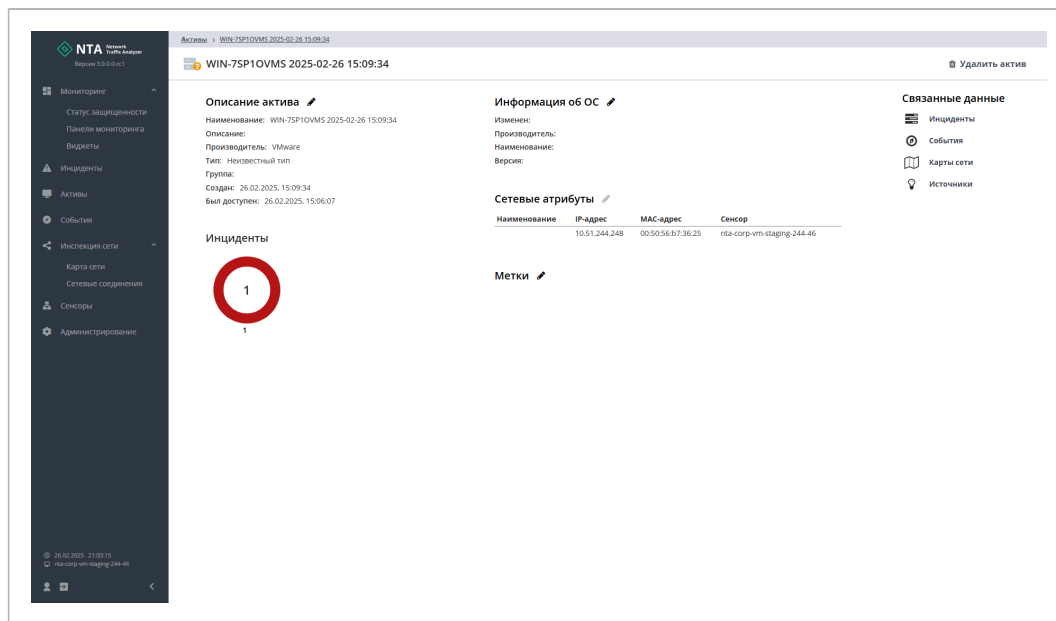


Рис. 142. Карточка актива

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»](#).

Описание актива

Наименование: WIN-7SP1OVMS 2025-02-26 15:09:34

Описание:

Производитель: VMware

Тип: Неизвестный тип

Группа:

Создан: 26.02.2025, 15:09:34

Был доступен: 26.02.2025, 15:06:07

Рис. 143. Содержание полей блока «Описание актива»

4. Для редактирования общей информации об активе:

а. 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 5 после редактирования общей информации.

- описание;
- 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. 144. Окно «Основная информация об активе»

5. 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**.

- в. При необходимости отключите автообновление данных об операционной системе при сборе задачами сбора данных. Для этого нажмите **Автообновление доступно**.

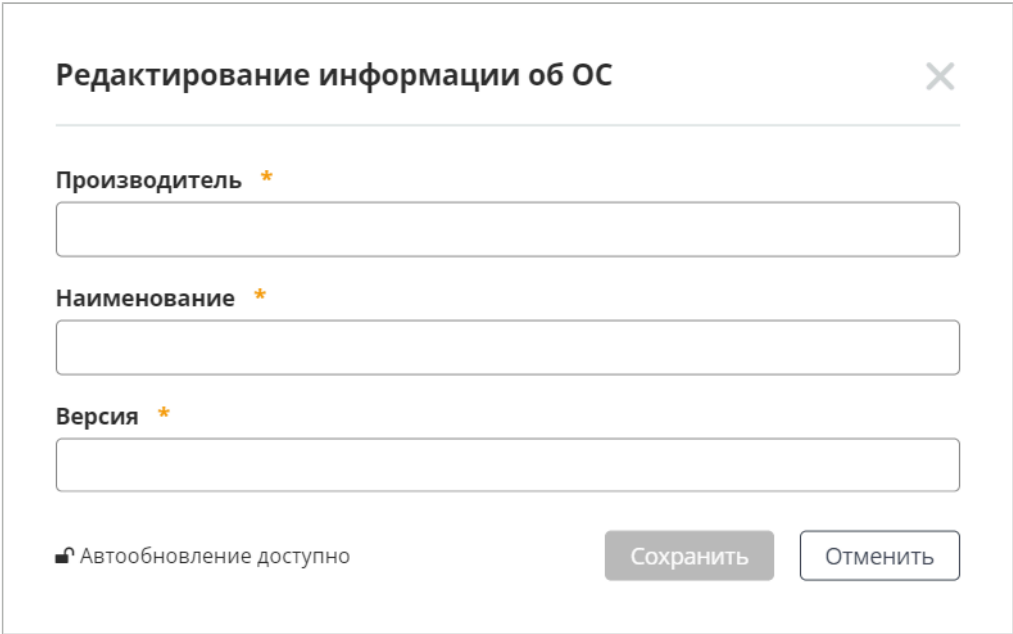


Рис. 145. Окно «Редактирование информации об ОС»

- **Результат шага:** появится надпись **Автообновление заблокировано**.
- г. Нажмите кнопку **Сохранить**.
- б. 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:

Для октетов MAC-адресов допускается использовать следующие разделители: ., -, :, либо не использовать разделители.

- 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.



Прим.:

- 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.

Редактирование сетевых атрибутов актива

Наименование	IP-адрес	MAC-адрес	Сенсор
	10.51.201.11	00:50:56:b7:84:b9	nta-corp-vm-staging-...x
			Выберите сенсор

☐ Выбрать сетевой атрибут неизвестного актива

Заккрыть

Рис. 146. Окно «Редактирование сетевых атрибутов актива»

7. Для изменения списка меток, которым принадлежит редактируемый актив:
 - а. Нажмите кнопку  напротив блока **Метки**.
 - **Результат шага:** появится окно **Редактирование меток**.
 - б. Измените состав присвоенных активу меток и нажмите **Сохранить**.

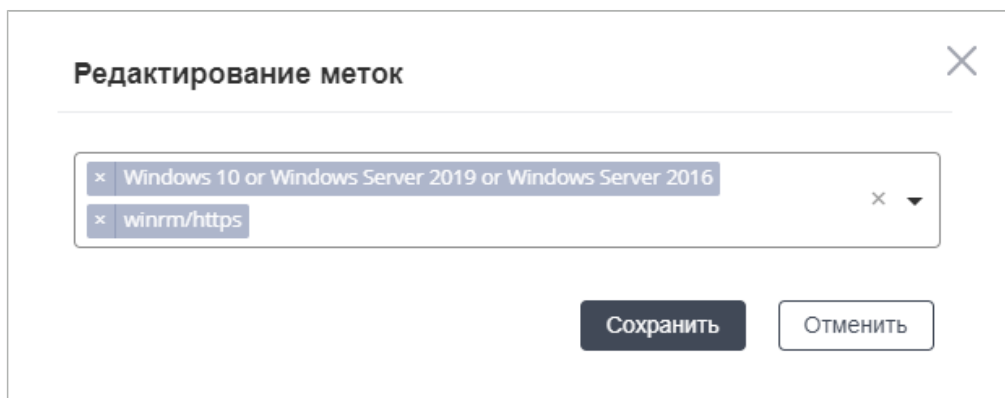


Рис. 147. Окно «Редактирование меток»

6.6. Удаление активов



ОСТОРОЖНО:

При удалении одного или нескольких активов с Комплекса будут удалены все связанные с ними данные: сессии и данные об операционной системе.

Удаление актива

Для удаления актива:

1. Перейдите на страницу **Активы**.
2. Нажмите на иконку или наименование актива.
 - **Результат шага:** откроется **Страница актива**.
3. Нажмите кнопку  **Удалить актив** в правом верхнем углу.

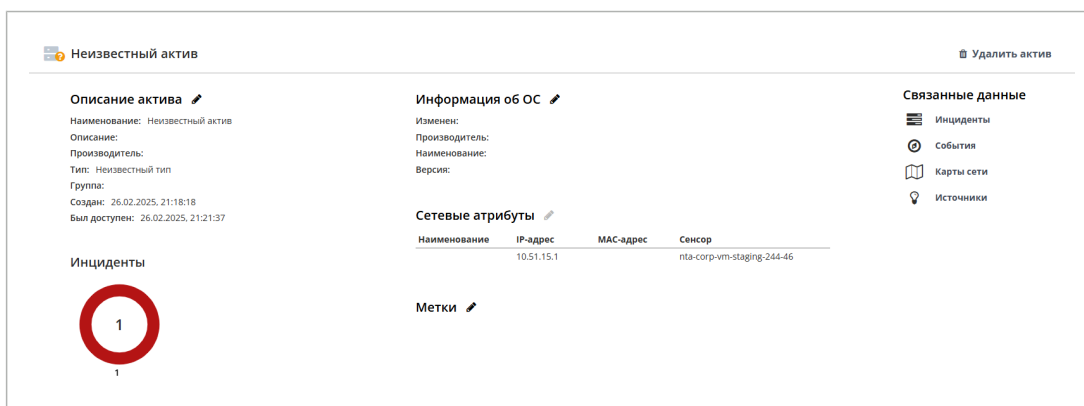


Рис. 148. Кнопка «Удалить актив» на странице актива

4. В открывшемся окне введите обоснование удаления актива и нажмите кнопку **Подтвердить**.

Для данного действия необходимо обоснование ✕

Вместе с активом будут удалены связанные конфигурации. Вы действительно хотите удалить актив?

Введите текст обоснования

Подтвердить **Отменить**

Рис. 149. Окно обоснования удаления актива

- **Результат шага:** актив будет удален. Откроется страница **Активы**.

Групповое удаление активов

Для удаления нескольких активов:

1. Перейдите на страницу **Активы**.
2. Получите необходимую выборку активов:
 - а. Выберите группу активов в левой части страницы.
 - б. На панели фильтров настройте параметры фильтрации списка Актив и нажмите кнопку **Применить**.

Внимание:

Если выбрана группа Актив, параметры фильтрации и групповые операции будут применяться только к активам из группы.

- в. Отметьте все отфильтрованные активы на удаление с помощью чекбокса в заголовке таблицы, либо отметьте отдельные активы с помощью чекбоксов рядом с активами. Для выбора всех активов в таблице отметьте один актив, затем нажмите в появившейся внизу страницы панели управления **Выбрать все**.
3. На панели управления внизу страницы нажмите кнопку (**Удалить**).

Создать отчёт
Удалить
Выбрано 18 / 18
Выбрать все
✕

Рис. 150. Кнопка «Удалить» на панели управления активами

**Внимание:**

Кнопка **(Удалить)** недоступна, если после применения действия **Выбрать все** выбрано более 100 активов.

4. В открывшемся окне введите обоснование удаления активов и нажмите кнопку **Подтвердить**.

► **Результат шага:** появится всплывающее уведомление об успешном удалении: Удаление активов запущено.

6.7. 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** в панели под таблицей.

► **Результат шага:** откроется окно **Создание отчета**.

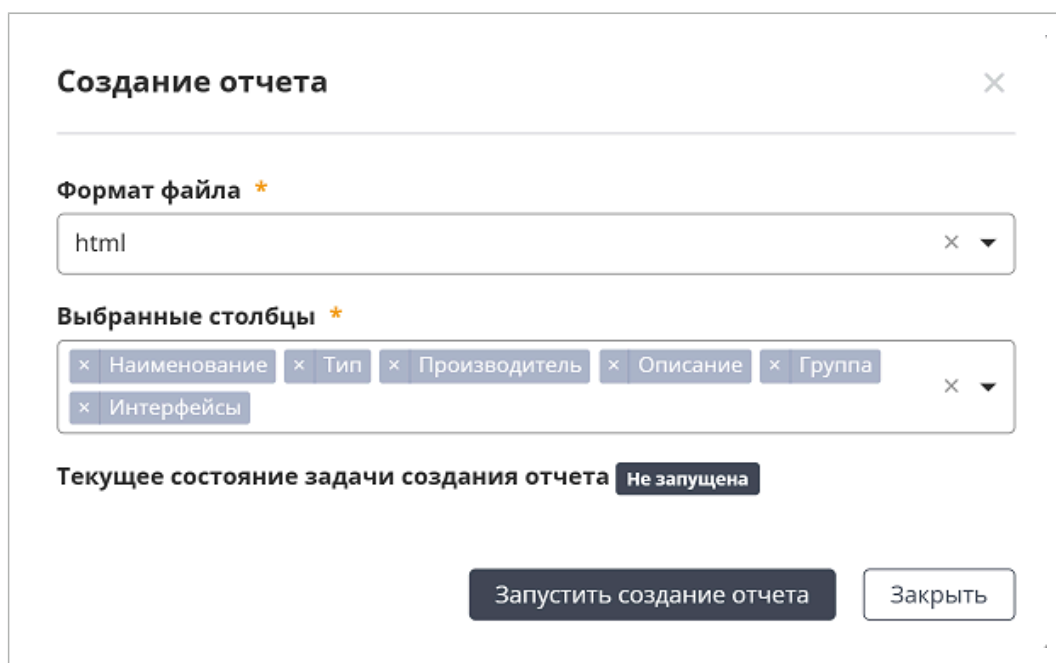


Рис. 151. Окно «Создание отчета»

4. Выберите формат файла отчета из выпадающего списка **Формат файла**. Для выбора доступны форматы **html** и **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**. В том же окне **Создание отчета**, по завершении создания отчета, появится ссылка с названием файла в выбранном формате — например, `hosts.html`.

7. Для сохранения отчета нажмите на ссылку с названием файла отчета.

6.8. Настройки активов

В этом разделе:

- **Настройка классификаторов**
 - **Создание метки**
 - **Редактирование и удаление классификаторов**
 - **Экспорт и импорт классификаторов**

Для работы с активами в Комплексе предусмотрено создание, редактирование и удаление групп классификаторов.

6.8.1. 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 3. Редактируемые классификаторы Комплекса](#)).

Табл. 3. Редактируемые классификаторы Комплекса

КЛАССИФИКАТОР	ХАРАКТЕРИСТИКА КЛАССИФИКАТОРА	ОТНОШЕНИЕ К АКТИВАМ
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. 4. Встроенные классификаторы Комплекса

КЛАССИФИКАТОР	ХАРАКТЕРИСТИКА КЛАССИФИКАТОРА	ОТНОШЕНИЕ К АКТИВАМ
Комплекс	предустановленный, автоматически дополняемый с добавлением Комплексов не редактируемый	обязательный атрибут классификации активов, появляется при наличии иерархии Комплексов
Производители	предустановленный не редактируемый	обязательный атрибут классификации активов

Табл. 4. Встроенные классификаторы Комплекса

КЛАССИФИКАТОР	ХАРАКТЕРИСТИКА КЛАССИФИКАТОРА	ОТНОШЕНИЕ К АКТИВАМ
Активы	предустановленный, автоматически дополняемый с добавлением Актив не редактируемый	обязательный атрибут классификации активов
Типы активов	предустановленный не редактируемый	обязательный атрибут классификации активов
Операционные системы, распознанные Комплексом	предустановленный, автоматически дополняемый не редактируемый	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.

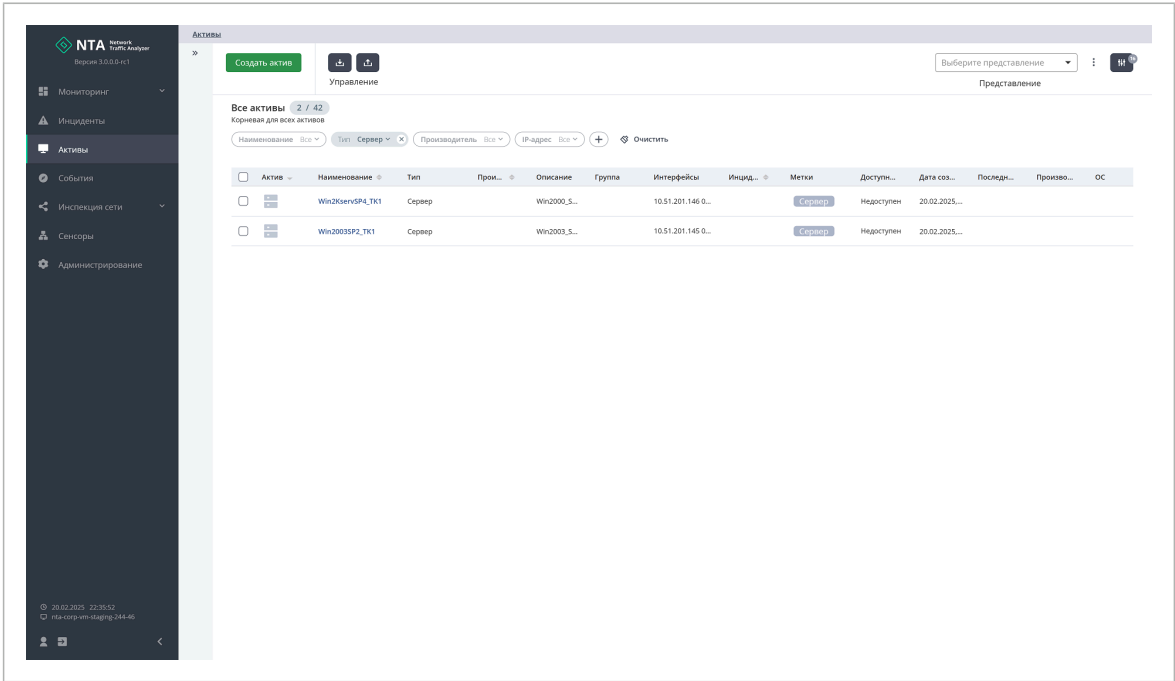


Рис. 152. Список активов с типом «Сервер» из классификатора «Типы активов»

6.8.1.1. Создание метки

Для создания метки:

 **Внимание:**

Максимальная вложенность при создании дочерних классификаторов равна 10.

1. Перейдите на страницу [Администрирование](#) → [Настройка активов](#) → [Классификаторы](#).
2. Нажмите кнопку **Создать метку**. В открывшемся окне **Создание метки** задайте следующие параметры:
 - а. наименование новой метки;
 - б. вышестоящую метку.

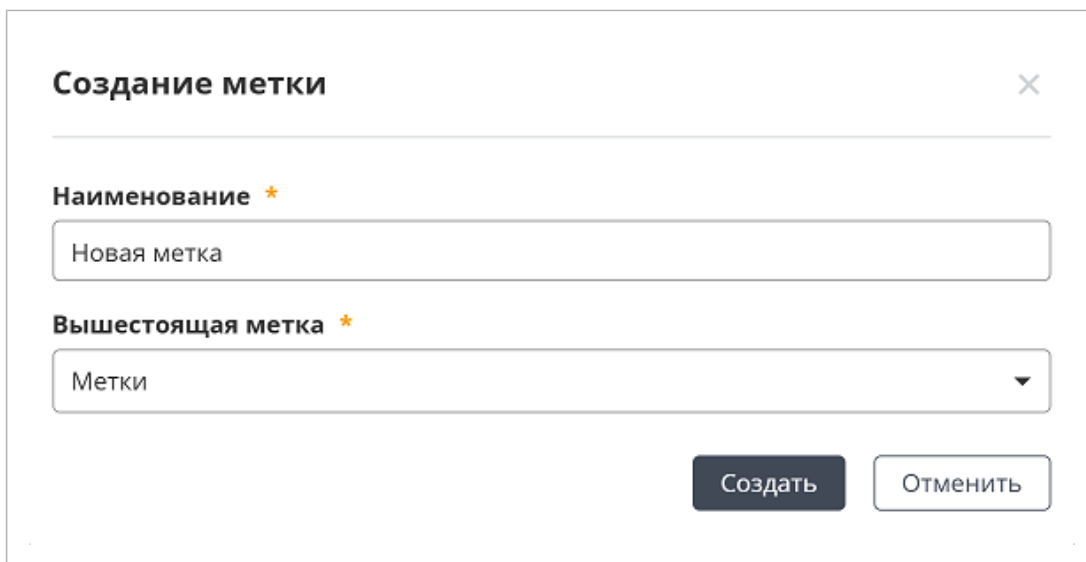


Рис. 153. Окно «Создание метки»

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

6.8.1.2. Редактирование и удаление классификаторов

Для управления созданными ранее классификаторами доступны следующие возможности:

1. Редактирование. Для редактирования классификатора:
 - а. Перейдите на страницу [Администрирование](#) → [Настройка активов](#) → [Классификаторы](#).
 - б. Напротив классификатора, который необходимо изменить, нажмите  (**Редактировать**).



Рис. 154. Кнопка редактирования классификатора

- **Результат шага:** появится окно [Редактирование метки](#).
- в. В окне редактирования классификатора измените необходимые параметры.

Рис. 155. Окно «Редактирование метки»

- г. Нажмите **Сохранить**.
2. Удаление. Для удаления классификатора:
- Перейдите на страницу [Классификаторы](#).
 - Напротив классификатора, который необходимо удалить, нажмите (**Удалить**).
- **Результат шага:** появится окно подтверждения удаления метки.

Рис. 156. Окно подтверждения удаления метки

Рис. 157. Окно подтверждения удаления вышестоящей метки

- в. Нажмите **Подтвердить**.

6.8.1.3. Экспорт и импорт классификаторов

В этом разделе:

- Экспорт меток
- Импорт меток

Экспорт и импорт справочников с иерархической структурой, содержащих метки и группы активов, осуществляется на странице [Администрирование](#) → [Основные настройки](#) → [Импорт и экспорт](#).

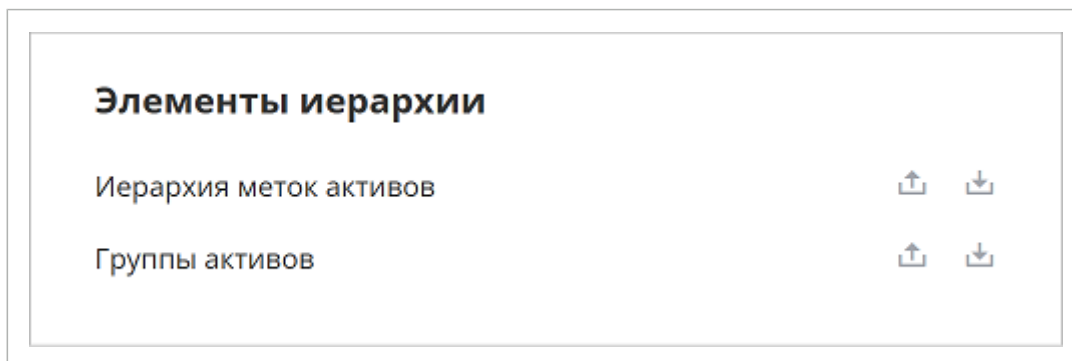


Рис. 158. Панель «Элементы иерархии» на странице «Импорт и экспорт»

6.8.1.3.1. Экспорт меток

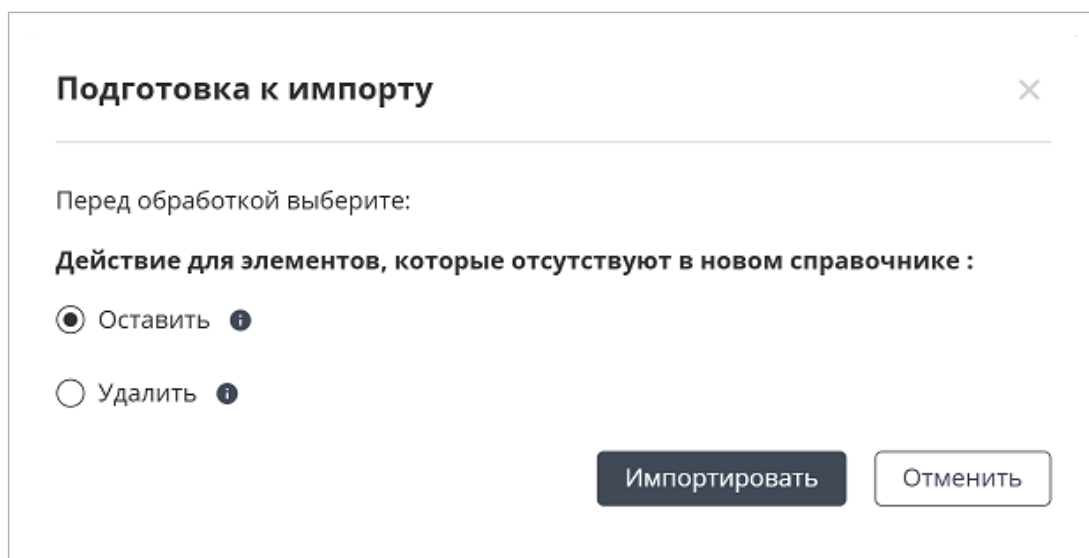
Для экспорта справочника с метками и их иерархией в файл формата *.json:

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:** в правом верхнем углу страницы появится уведомление **Запущен экспорт справочника** и начнется процесс экспорта. По окончании 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 экспортируемого файла и нажмите кнопку **Сохранить**.
 - **Результат шага:** файл `tags_[дата_и_время].json` будет загружен на компьютер.

6.8.1.3.2. Импорт меток

Для импорта справочника с пользовательской иерархией групп и меток из файла формата *.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.



Подготовка к импорту ✕

Перед обработкой выберите:

Действие для элементов, которые отсутствуют в новом справочнике :

☒ Оставить ⓘ

☐ Удалить ⓘ

Импортировать **Отменить**

Рис. 159. Окно «Подготовка к импорту»

5. Убедитесь, что метки были успешно загружены.

- **Результат шага:** на странице [Администрирование](#) → [Настройка активов](#) → [Классификаторы](#) появится импортированный справочник.

7. 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. [Удаление сенсора](#)

На страницах управления выполняется настройка параметров использования Комплекса: сведения о текущем Комплексе, контролируемая сеть, пользователи, экспорт данных и диагностика.

7.1. Изменение сведений о Комплексе и сенсорах

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.

The screenshot shows the 'О системе' (About System) page in the NTA CyberLympha interface. The page has a dark sidebar on the left with navigation links: Мониторинг, Инциденты, Активы, События, Инспекция сети, Сенсоры, and Администрирование. The main content area is titled 'О системе' and contains two sections: 'Сведения о Комплексе' (Complex Information) and 'Информация об изготовителе' (Manufacturer Information). The 'Сведения о Комплексе' section has four input fields: 'Наименование' (Name) with the value 'nta-corp-vm-staging-244-46', 'Описание' (Description) with the placeholder 'необходимо заполнить' (must be filled), 'Эксплуатирующая организация' (Operating Organization) with the placeholder 'необходимо заполнить' (must be filled), and 'Место установки' (Installation Location) with the placeholder 'необходимо заполнить' (must be filled). Below these fields are 'Сохранить' (Save) and 'Отмена' (Cancel) buttons. The 'Информация об изготовителе' section displays the following information: 'CyberLympha DATAPK', 'Разработчик: ООО «СайберЛимфа»' (Developer: LLC 'CyberLympha'), 'www.CyberLympha.ru', and 'Версия: 3.0.0.0-rc1'.

Рис. 160. Страница «О системе»

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

Изменение сведений о сенсорах, подключенных к Комплексу

1. Перейдите на страницу [Сенсоры](#).
2. Выберите сенсор из списка.
 - **Результат шага:** откроется карточка выбранного сенсора.

3. В открывшейся панели нажмите кнопку  (**Редактировать**) напротив наименования сенсора.

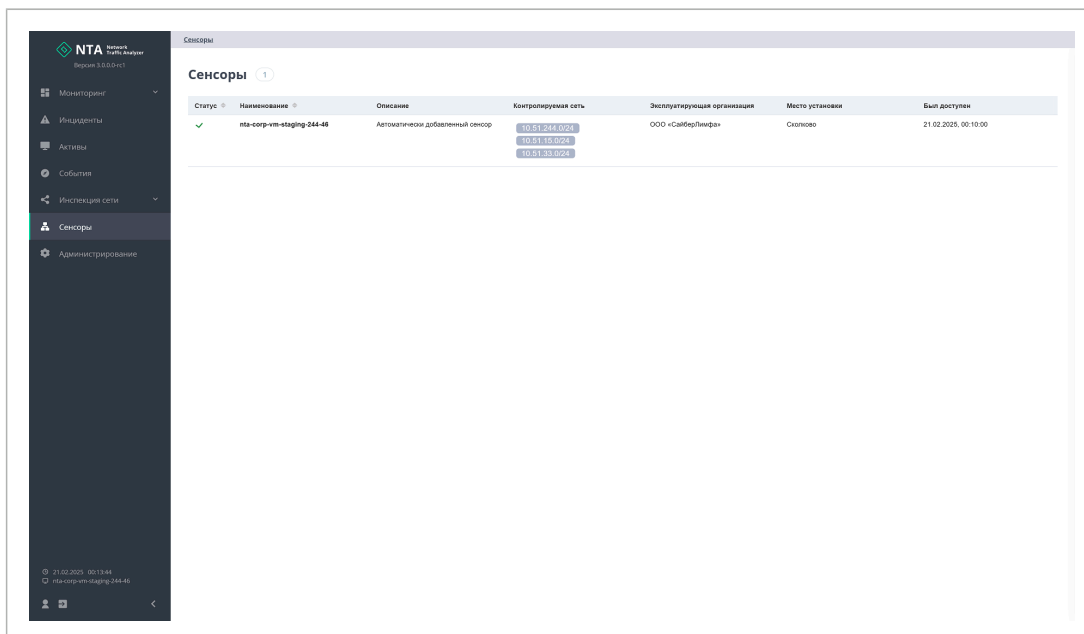
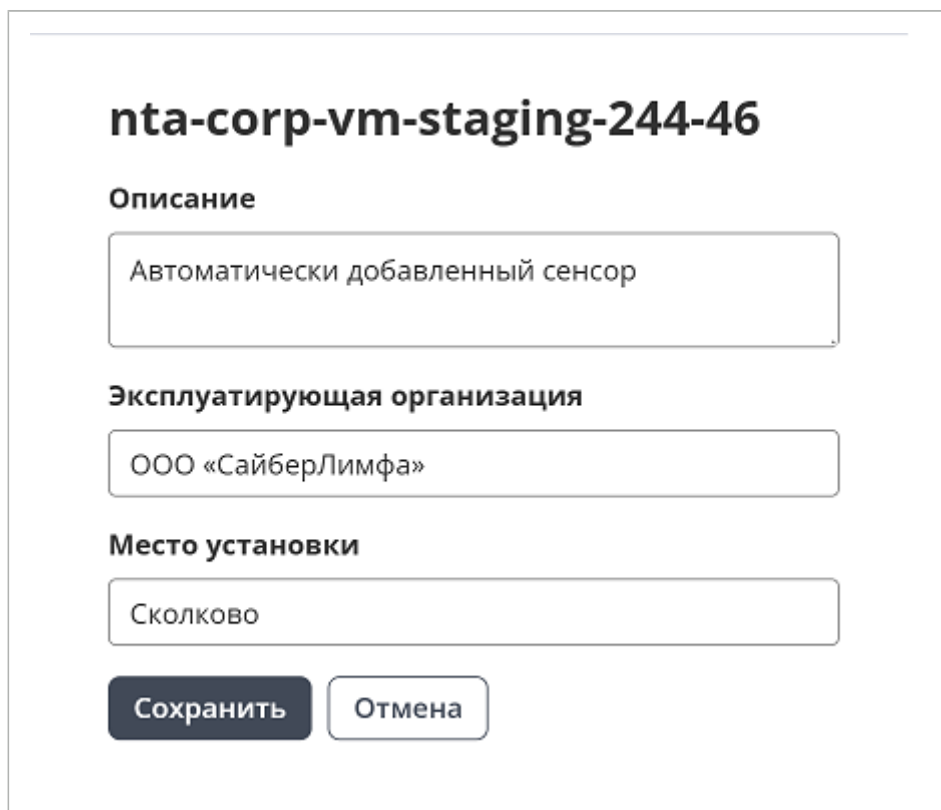


Рис. 161. Страница «Сенсоры»

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



nta-corp-vm-staging-244-46

Описание

Автоматически добавленный сенсор

Эксплуатирующая организация

ООО «СайберЛимфа»

Место установки

Сколково

Сохранить **Отмена**

Рис. 162. Блок редактирования информации о сенсоре

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

7.2. Сканирование сети и определение интерфейсов активного сетевого оборудования

Комплекс обнаруживает новые активы в автоматическом режиме на основании информации из пакетов сетевого трафика, которые поступают на активный и прослушивающий интерфейсы сенсоров. Такой информацией могут быть IP- и MAC-адреса источников или получателей пакетов. Для некоторых активов возможно определение дополнительной информации об операционной системе: версии ОС, NetBIOS и DNS имени. Вся полученная информация об активах отображается на странице [Активы](#).



Внимание:

Способ обнаружения активов и их отображение зависит от значения переменной `AUTOMATIC_HOST_CREATION_BY_MAC` в конфигурационном файле `manager.env`:

- Если переменная имеет значение `false`, либо она не задана в `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 `true`, 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.

Комплекс способен выполнять сканирование сети для обнаружения новых неизвестных активов и для получения дополнительной информации об операционных системах активов (возможно только для ряда операционных систем).

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). В случае определения сетевого имени узла наименование соответствующего актива в Комплексе меняется на сетевое имя.

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.

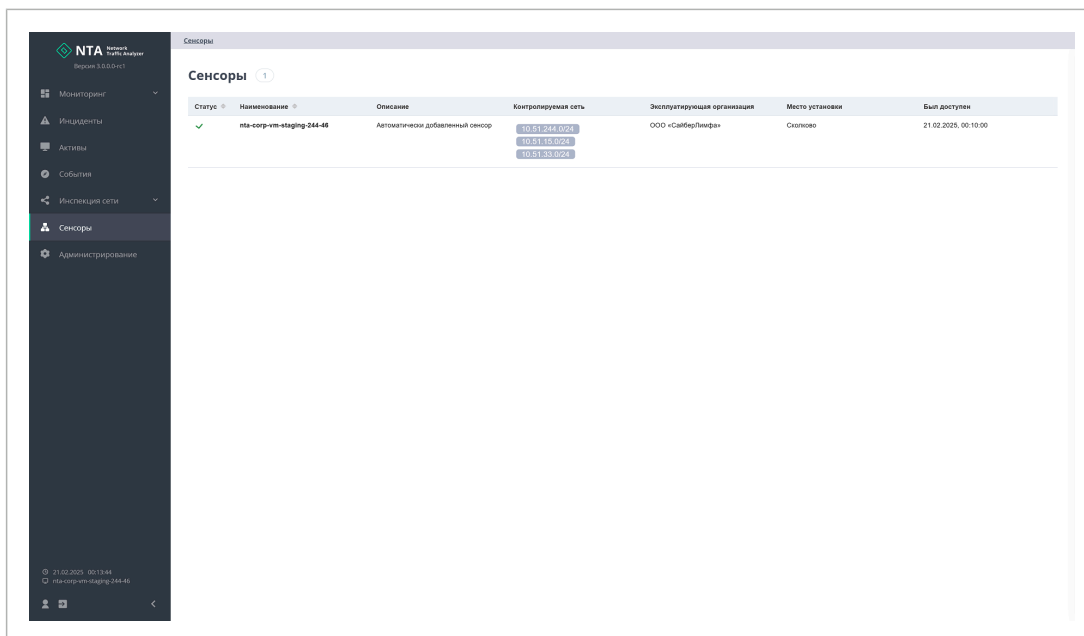


Рис. 163. Панель «Сканирование сети»

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 Сканирование адресов контролируемой сети запущено успешно.

7.2.1. Интерпретация результатов пассивного сканирования сети

В процессе пассивного сканирования сети в Комплексе могут быть получены следующие результаты на странице **Активы**, которые необходимо проверить:

- Объекту защиты может быть присвоен дополнительный интерфейс, который имеет такой же IP-адрес, 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 Актив, 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 объекту защиты, 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 объект защиты и присвойте ему найденный интерфейс — тогда он будет автоматически удален из списка интерфейсов исходного объекта защиты.

- На странице **Активы** могут присутствовать несколько Актив с разными интерфейсами, хотя они должны принадлежать одному Актив (часто такие Актив являются активным сетевым оборудованием). Если на таком Актив открыт доступ по протоколу SNMP, то есть возможность привязать к нему необходимые интерфейсы и удалить лишние Актив с помощью специального сканера сбора данных.

7.3. Настройка контролируемой сети

Настройка контролируемой сети необходима для отображения на странице **Активы** активов, IP-адреса которых входят в контролируемую сеть. 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:** откроется карточка выбранного сенсора.
3. В открывшейся панели в блоке **Контролируемая сеть** нажмите кнопку  (**Редактировать**).
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**).

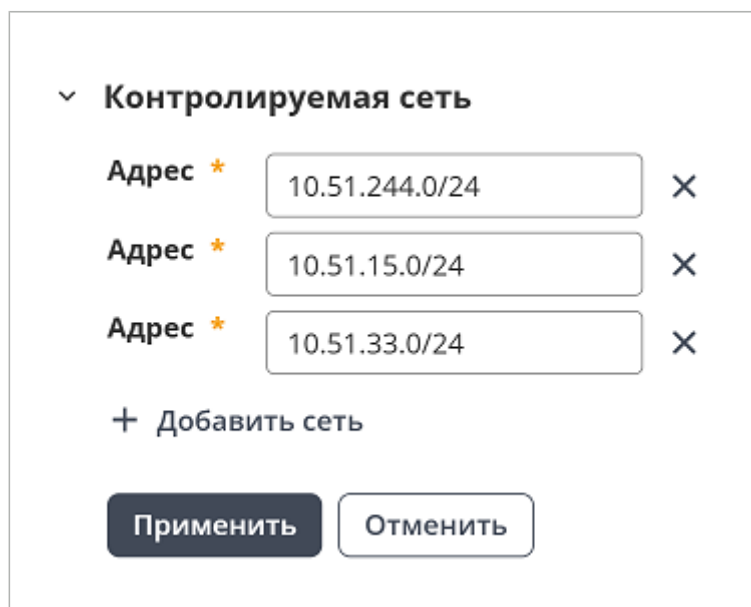


Рис. 164. Блок «Контролируемая сеть» в настройках сенсора

5. Нажмите кнопку **Применить**.
 - **Результат шага:** Появится окно с предупреждением: При смене контролируемой сети активы, 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 активнов 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.

7.4. 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 — хранящаяся 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.

Возможность входа в Комплекс и выхода из него недоступна только заблокированным пользователям.

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 `.env` (подробнее см. раздел «Отключение ограничения на количество сессий пользователей»).

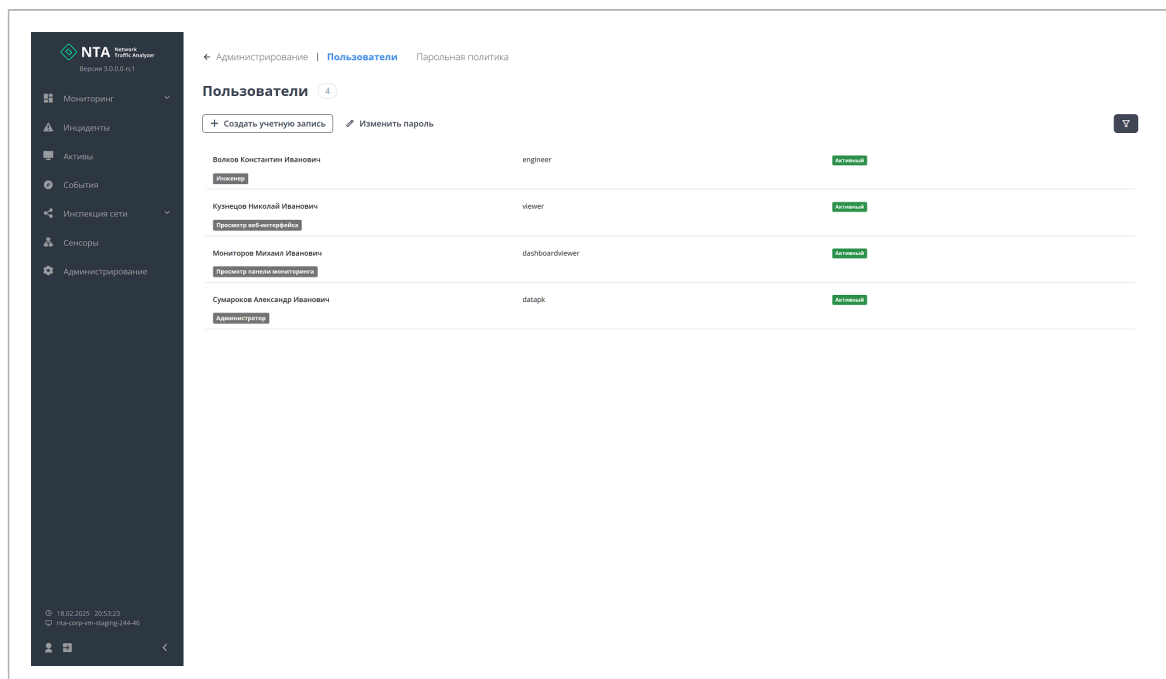


Рис. 165. Страница «Пользователи»

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 5. 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. 5. Пользовательские роли по умолчанию

ФУНКЦИОНАЛЬНАЯ ОБЛАСТЬ / РАЗДЕЛ ВЕБ-ИНТЕРФЕЙСА	ДЕЙСТВИЯ		
	АДМИНИСТРАТОР	ИНЖЕНЕР	ПРОСМОТР ВЕБ-ИНТЕРФЕЙСА
Вкладка Сессии	Просмотр		Просмотр всех страниц UDV NTA
Вкладка Пакеты	Просмотр		
Вкладка Файлы	Просмотр		
	Создание и скачивание архива с файлами PCAP		
Карточка сенсора	Просмотр		
	Изменение настроек ротации файлов	—	
Группа вкладок Протоколы	Просмотр		
Страница Карта сети	Просмотр		
Страница Правила сессий	Просмотр		
	Создание, изменение правила сессий, изменение режима работы правила сессий		
	Групповая активация и деактивации правил сессий		
	Удаление правила сессий, групповое удаление правил сессий	—	

Табл. 5. Пользовательские роли по умолчанию

ФУНКЦИОНАЛЬНАЯ ОБЛАСТЬ / РАЗДЕЛ ВЕБ-ИНТЕРФЕЙСА	ДЕЙСТВИЯ		
	АДМИНИСТРАТОР	ИНЖЕНЕР	ПРОСМОТР ВЕБ-ИНТЕРФЕЙСА
Страница Правила контроля тегов	Просмотр		
	Создание, изменение, удаление правила контроля тегов		
Актив	Просмотр страницы и карточки актива, экспорт и импорт активов, со- здание, изменение, удаление активов		
Источники	Создание, остановка, запуск, редакти- рование, удаление источника событий		
Инциденты	Изменение параметров и удаление инцидента или группы инцидентов		
	Создание статусов инцидентов	Просмотр статусов инцидентов	
Индексы	Создание и удаление шаблонов индекса		
	Архивирование, удаление индексов	Просмотр списка индексов	
Сканирование сети	Запуск	—	
Сенсоры, иерархия	Управление сенсорами	Перезапуск син- хронизации	
События	Просмотр событий и создание запросов		
	Запуск текущего и ретроспективного анализа событий	—	
Карты сети	Просмотр карты сети, настройка представлений на карте		
Страница Статус защи- щенности	Просмотр, переход на страницы Активы , Инциденты , Инспекция сети → Карта сети , События для получения подробной информации		Просмотр

7.4.1. 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.

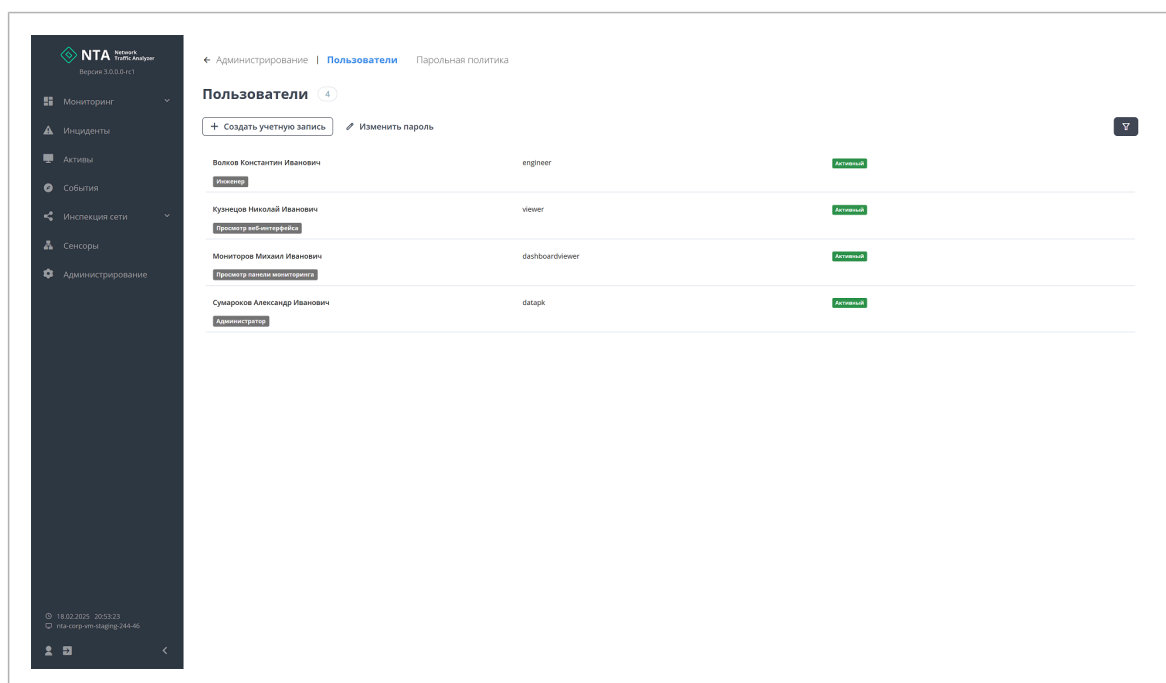


Рис. 166. Страница «Пользователи»

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.

7.4.1.1. 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**;



Прим.:

При отмене выбора данного параметра учетная запись пользователя будет заблокирована.

- при необходимости отметьте чекбокс **Сменить пароль при входе**.

Создание учетной записи

Тип учетной записи *

Локальная

Логин * ⓘ

sverchovensky

Новый пароль *

.....

Подтверждение нового пароля *

.....

Имя учетной записи в службе каталогов

example@domain.local

Фамилия *

Верховенский

Имя *

Степан

Отчество

Трофимович

Роль пользователя *

Инженер

☒ Учетная запись пользователя активна

☐ Сменить пароль при входе

Создать Отменить

Рис. 167. Окно «Создание учетной записи» при создании локальный учетной записи

4. Нажмите кнопку **Создать** для подтверждения изменений.

7.4.1.2. 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 (5-7 минут).
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.

Создание учетной записи

Тип учетной записи *

Служба каталогов

Логин * ⓘ

mlebyadkina

Новый пароль *

Новый пароль

Подтверждение нового пароля *

Подтверждение нового пароля

Имя учетной записи в службе каталогов

mlebyadkina@corp.example.com

Фамилия *

Лебядкина

Имя *

Мария

Отчество

Тимофеевна

Роль пользователя *

Просмотр веб-интерфейса

☒ Учетная запись пользователя активна

☐ Сменить пароль при входе

Создать

Отменить

Рис. 168. Окно «Создание учетной записи» при создании учетной записи службы каталогов

13. Нажмите кнопку **Создать** для подтверждения изменений.

7.4.1.3. 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](#)

7.4.1.3.1. 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**.

✕

Редактирование учетной записи

Тип учетной записи *

Локальная

Логин * 

sverchovensky

Новый пароль *

Новый пароль

Подтверждение нового пароля *

Подтверждение нового пароля

Имя учетной записи в службе каталогов

example@domain.local

Фамилия *

Верховенский

Имя *

Степан

Отчество

Трофимович

Роль пользователя *

Инженер

☒ Учетная запись пользователя активна

☐ Сменить пароль при входе

Сохранить

Отменить

Рис. 169. Окно «Редактирование учетной записи»

4. Для применения изменений выполните повторный вход в веб-интерфейс Комплекса:

- а. Нажмите кнопку  (Выход) в верхнем правом углу страницы веб-интерфейса.
- б. Произведите повторный вход в систему с измененной учетной записью.

7.4.1.3.2. 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.

i

Прим.:

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 символов;
- содержание пароля — не менее одного буквенного и не менее одного числового символа;
- пароль не должен содержать логин учетной записи.

Изменение пароля учетной записи пользователя **datapk**

×

Логин * ⓘ

datapk

Старый пароль *

Старый пароль

Новый пароль *

Новый пароль

Подтверждение нового пароля *

Подтверждение нового пароля

Сохранить

Отменить

Рис. 170. Окно «Изменение пароля учетной записи»

4. Для применения изменений выполните повторный вход в веб-интерфейс Комплекса:

- а. Нажмите кнопку  (**Выход**) в верхнем правом углу страницы веб-интерфейса.
- б. Произведите повторный вход в систему с измененной учетной записью.

7.4.1.3.3. Блокировка и удаление учетной записи

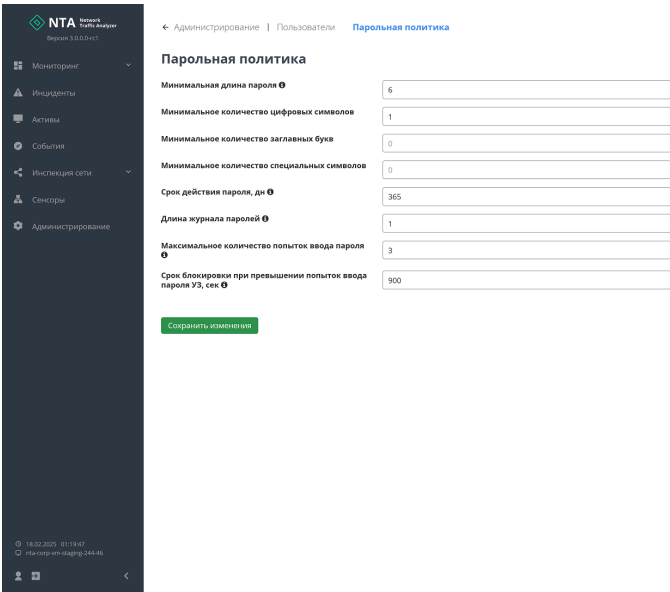
В случае обнаружения несанкционированных действий пользователя (подробнее см. раздел «[Действия в случаях несанкционированного доступа к данным](#)») или в иных случаях, интерфейс Комплекса предоставляет возможность бессечно заблокировать или удалить учетную запись пользователя.

1. Перейдите на страницу [Администрирование](#) → [Пользователи](#).
2. Для блокировки учетной записи пользователя Комплекса:
 - а. Выберите учетную запись в списке пользователей 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:
 - а. Напротив утратившей актуальность учетной записи нажмите кнопку  (**Удалить учетную запись**).
 - б. Во всплывающем окне введите текст обоснования удаления.

7.4.2. Настройка парольной политики

Для настройки единой парольной политики для всех пользователей:

1. Перейдите на страницу [Администрирование](#) → [Пользователи](#) → [Парольная политика](#).



NTA Network Security Manager
Версия 3.0.0.101

← Администрирование | Пользователи | Парольная политика

Парольная политика

Минимальная длина пароля	6
Минимальное количество цифровых символов	1
Минимальное количество заглавных букв	0
Минимальное количество специальных символов	0
Срок действия пароля, дн	365
Длина журнала паролей	1
Максимальное количество попыток ввода пароля	3
Срок блокировки при превышении попыток ввода пароля УЗ, сек	900

[Сохранить изменения](#)

18.02.2025 01:19:47
nta-scp-ntn-lab@192.168.1.40

Рис. 171. Страница «Парольная политика»

2. Настройте следующие параметры парольной политики:

- общее минимальное количество символов, которое должен содержать пароль;



Прим.:

Доступен ввод значений в диапазоне от 6 до 14. 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);



Прим.:

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;



Прим.:

Доступен ввод значений в диапазоне от 1 до 24.

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



Прим.:

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.



Прим.:

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).

7.4.3. 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 (5-7 минут).

7.5. 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 6. Ссылки на разделы документа с описанием экспорта объектов Комплекса) приведены ссылки на разделы с описанием выполнения резервных копий объектов Комплекса путем экспорта.

Табл. 6. 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 меток активов	Экспорт меток	json
Группы активов (без активов)	Экспорт групп активов	json
Политика корреляции	Экспорт политики корреляции	json
Статусы инцидентов	Экспорт статусов инцидентов	json

Табл. 6. Ссылки на разделы документа с описанием экспорта объектов Комплекса

НАИМЕНОВАНИЕ	ССЫЛКА	ФОРМАТ
Правила службы обнаружения вторжений	Экспорт правил службы обнаружения вторжений	json
Источники событий	Экспорт источников событий	json
Сохраненные запросы, визуализации, панели мониторинга	Экспорт сохраненных объектов	json
Активы	Экспорт активов	json



Внимание:

Экспорт следующих справочников недоступен в веб-интерфейсе:

- 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.

7.6. Диагностика состояния системы Комплекса

На странице [Администрирование](#) → [Диагностика](#) вы можете ознакомиться с графиками нагрузки компонентов системы, на которой функционирует текущий Комплекс.

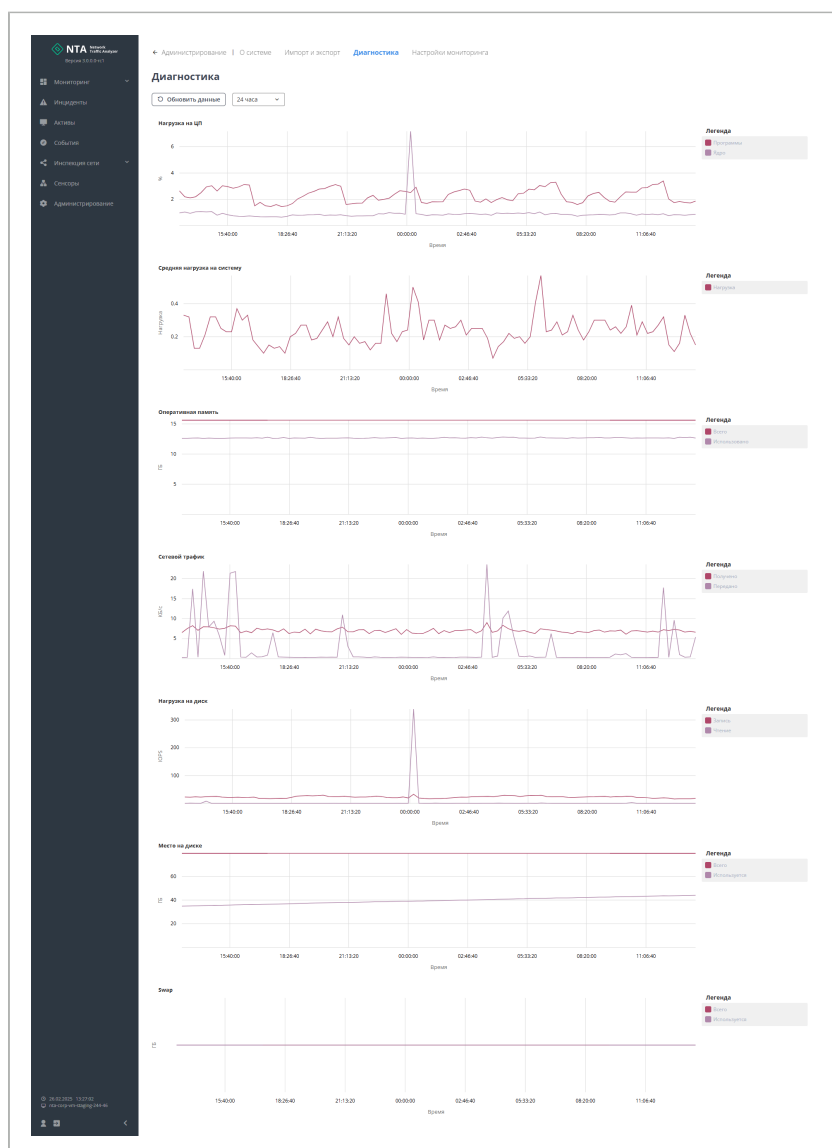


Рис. 172. Страница «Диагностика»

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**.

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.



Прим.:

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.



Прим.:

При превышении заданного в переменной `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.



Прим.:

При превышении заданного в переменной `MAX_RAM_CONSUMED_PERCENTAGE` 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.



Прим.:

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.

Справа от каждого графика можно увидеть легенду, где указано, какие параметры используются на этом графике и цвет их линий.

7.7. 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:** 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 сетевые атрибуты актива.
 - 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**.

Для данного действия необходимо обоснование

Вместе с сенсором будут удалены связанные сетевые атрибуты. Вы действительно хотите удалить сенсор nta-corp-vm-staging-244-46?

Введите текст обоснования

Подтвердить

Отменить

- **Результат шага:** сенсор и связанные с ним данные будут удалены из Комплекса уровня Management.

Если необходимо подключить сенсор к другому Комплексу уровня Management, выполните шаги 7-14 инструкции «Подключение сенсора к другому Комплексу уровня Management» Руководства по внедрению и поддержке.

8. Нештатные ситуации и действия по их устранению

В этом разделе:

1. Действия по восстановлению комплекса при сбойных ситуациях и ошибках в данных
2. Действия в случаях несанкционированного доступа к данным
3. Действия в других аварийных ситуациях
4. Анкета при обращении в сервисный центр

UDV NTA функционирует круглосуточно. В процессе использования UDV NTA возможно появление неполадок, ограничивающих возможности управления защитными механизмами или открывающих возможности для атаки на объекты защиты.

Если вам не удастся самостоятельно устранить нештатную ситуацию, заполните анкету (см. раздел [Анкета при обращении в сервисный центр](#)) и отправьте на адрес сервисного центра ООО «СайберЛимфа»: support@cyberlymph.com.

8.1. 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
- Соединение с главной страницей веб-интерфейса осуществляется по протоколу HTTP вместо HTTPS
- 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
- Комплекс не обнаруживает активы без IP-адреса
- Два актива с одинаковым IP-адресом
- Отсутствуют события, генерируемые Комплексом
- Не принимаются Syslog-сообщения от активов
- Не принимаются сообщения от служб корреляции и обнаружения вторжений
- Не принимаются сообщения от службы корреляции
- Не инициализируется стек udv-opensearch, udv-opensearch-dashboards, udv-logstash
- Не создается индекс в экспертном режиме страницы «События»
- Не удается отфильтровать записи на странице «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 событий при превышении размера или времени хранения индекса
- Ошибка «An HTTP request took too long to complete» при запуске контейнеров
- Ошибки вида «<...>Cannot start service <...>. Bind for <ip_address>:<TCP/UDP_port> is ready allocated» при попытке запуска контейнеров
- Недоступен сервис корреляции событий

- При бездействии в веб-интерфейсе сеанс завершается раньше, чем через 10 минут
- Не устанавливается соединение с сенсором
- Потери при передаче данных через ERSPAN

8.1.1. 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**).

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 (5-7 минут).



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 наименованию серверного сертификата. Для этого выполните команду:

```
cat /usr/share/udv/datapk/manager.env | grep HOST_IP
```

4. Если значение переменной не соответствует наименованию серверного сертификата, 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 **F2**, и закройте файл, нажав клавишу **F10**.
- 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.

8.1.2. Соединение с главной страницей веб-интерфейса осуществляется по протоколу HTTP вместо HTTPS

Причина: отсутствие серверного сертификата и ключа

Способ устранения

Для устранения затруднения:

1. Остановите работу сервисов, выполнив команду:

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

2. 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 их.
3. Убедитесь, что в файле `manager.env`, расположенном в рабочей директории Комплекса, значение переменной `HOST_IP` совпадает с наименованием серверного сертификата.
4. Запустите работу сервисов, выполнив команду:

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

8.1.3. 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](#)

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 SP».

См. также

[Отображение времени в Комплексе](#)

8.1.4. 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-frontent`, выполнив команду:

```
apt-get install --reinstall udv-frontent -y
```

► **Результат шага:** Если файл `environment.json` был изменен или удален, при переустановке сервиса `udv-frontent` он будет восстановлен до состояния по умолчанию.

8.1.5. 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-*
```

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`:
 - правила для уровня Management:

```
*filter
:INPUT DROP [0:0]
:FORWARD DROP [0:0]
:OUTPUT ACCEPT [0:0]

-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
-A INPUT -p icmp -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -p tcp -m state --state NEW -m tcp --dport 22 -j ACCEPT
-A INPUT -p tcp -m state --state NEW -m tcp --dport 443 -j ACCEPT

# Правило, когда М выступает в роли ntp-сервера для S:
-A INPUT -p udp -m udp --dport 123 -j ACCEPT

-A INPUT -p tcp -m tcp --dport 16379 -j ACCEPT
-A INPUT -p tcp -m tcp --dport 19091 -j ACCEPT
-A INPUT -p tcp -m tcp --dport 15673 -j ACCEPT
-A INPUT -j REJECT --reject-with icmp-host-prohibited
-A FORWARD -j REJECT --reject-with icmp-host-prohibited
```

```
COMMIT
```

- правила для уровня Management+Sensor:

```
*filter
:INPUT DROP [0:0]
:FORWARD DROP [0:0]
:OUTPUT ACCEPT [0:0]

-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
-A INPUT -p icmp -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -p tcp -m state --state NEW -m tcp --dport 22 -j ACCEPT
-A INPUT -p tcp -m state --state NEW -m tcp --dport 443 -j ACCEPT
-A INPUT -p udp -m udp --dport 514 -j ACCEPT
-A INPUT -p tcp -m tcp --dport 514 -j ACCEPT
-A INPUT -p udp -m udp --dport 515 -j ACCEPT
-A INPUT -p tcp -m tcp --dport 515 -j ACCEPT
-A INPUT -p udp -m udp --dport 162 -j ACCEPT
-A INPUT -j REJECT --reject-with icmp-host-prohibited
-A FORWARD -j REJECT --reject-with icmp-host-prohibited

COMMIT
```

2. При необходимости настройте правила iptables:

- а. 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.

8.1.6. 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]
```



Подсказка:

Интерфейсы пишутся через запятую без пробелов.

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»](#).

8.1.7. 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 вкладке **Сессии** страницы **Инспекция сети** → **Сетевые соединения** (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](#)».

8.1.8. Комплекс не обнаруживает активы без IP-адреса

Комплекс не обнаруживает активы, все или некоторые интерфейсы которых не имеют IP-адреса (узлы, работающие на канальном уровне модели OSI).

Причина: переменная в файле `manager.env` `AUTOMATIC_HOST_CREATION_BY_MAC` имеет значение `true`

Способ устранения

Для устранения затруднения:

1. Подключитесь к операционной системе 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 `AUTOMATIC_HOST_CREATION_BY_MAC` значение `false`.
5. Запустить работу сервисов командой:

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

6. Дождитесь запуска работы всех сервисов (5-7 минут).
7. Убедитесь, что активы, интерфейсы которых не имеют IP-адреса, обнаруживаются и отображаются на странице **Активы** веб-интерфейса Комплекса.

8.1.9. 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 сетевых узлов»](#)».

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:

1. На странице **Сенсоры** веб-интерфейса Комплекса убедитесь, что добавленные контролируемые сети сенсоров не пересекаются друг с другом.
2. 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](#)».

8.1.10. Отсутствуют события, генерируемые Комплексом

На странице **События** частично или полностью отсутствуют события, генерируемые Комплексом. В качестве причин рассмотрены следующие:

1. [Генерация событий отключена в настройках переменных](#)
2. [Диск операционной системы Комплекса заполнен более, чем на 90%](#)

Генерация событий отключена в настройках переменных

В конфигурационном файле `manager.env` Комплекса уровня Management переменным, отвечающим за отключение и включение генерации 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](#)».

Диск операционной системы Комплекса заполнен более, чем на 90%

Сервис хранения и поиска событий недоступен в результате заполнения дискового пространства 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 пространства.
5. При необходимости измените значения переменных `EVENT_INDICES_MAX_SIZE_GB` и `EVENT_ARCHIVES_MAX_SIZE_GB`:

- а. 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_MANAGER_ARCHIVES_SIZE` 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](#)».

9. Запустите сервисы Комплекса:

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

10. Убедитесь в работоспособности сервиса хранения и поиска событий:

а. 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 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 принимаются сообщения от службы корреляции](#)

8.1.11. 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.

8.1.12. Не принимаются сообщения от служб корреляции и обнаружения вторжений

Причина: наименование служебного объекта защиты 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 контейнеров Комплекса без удаления накопленных данных.
- б. Откройте файл `/etc/profile` в режиме редактирования с помощью редактора `nano`:

```
nano /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 контейнеров Комплекса.
- ж. Убедитесь, что наименование Комплекса совпадает с его сетевым именем на странице [Администрирование](#) → [О системе](#).

8.1.13. Не принимаются сообщения от службы корреляции

Причина: 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 (5-7 минут).

8.1.14. Не инициализируется стек udv-opensearch, udv-opensearch-dashboards, udv-logstash

Возможны следующие причины:

- Некорректное значение системной переменной `vm.max_map_count`
- Ошибки в настройках нормализации

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:
 - а. 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 нормализации

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 (5-7 минут).

8.1.15. 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 с актива.

2. Создайте или включите источники объектов защиты и сгенерируйте на них события.

8.1.16. Не удастся отфильтровать записи на странице «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 [Мониторинг](#) → [Настройки мониторинга](#), вкладка **Шаблоны Индексов**.
2. Убедитесь, что после нормализации было принято событие с новыми полями (помеченными желтым восклицательным знаком).

8.1.17. Объекты мониторинга и визуализации импортируются с ошибкой

Причина: отсутствуют нужные поля в шаблоне индекса

Способ устранения

Для устранения затруднения:

1. Убедитесь в целостности директории `/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.

8.1.18. 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`, который расположен в рабочей директории Комплекса уровня Management. Для этого выполните следующую команду:

```
openssl verify -CAfile /opt/datapk/ca.crt /opt/datapk/scripts-certs/datapk_script.crt
```

- **Результат шага:** если верификация пройдет успешно, в командную строку будет выведена следующая информация:

```
/opt/datapk/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.
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.
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.
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.

8.1.19. Не выполняется архивация 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 `.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 /opt/datapk/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 событий Комплекса в архив»](#)).

В переменной файла .env настроено удаление индексов вместо сохранения в архив

Способ устранения

Для устранения затруднения:

1. Перейдите в рабочую директорию Комплекса уровня Management.
2. Остановите работу контейнеров без удаления данных.
3. В конфигурационном файле `.env` присвойте переменной `DATAPK_EVENT_MANAGER_EVENTS_ACTION_MORE_SIZE` значение `rotate`.
4. Запустите работу контейнеров и дождитесь их запуска (5-7 минут).

8.1.20. Ошибка «An HTTP request took too long to complete» при запуске контейнеров

Возможны следующие причины:

- [Загрузка контейнера обрывается по достижении лимита времени](#)
- [Недостаточный размер оперативной памяти аппаратного комплекса или виртуальной машины, на которой развернут Комплекс](#)

Загрузка контейнера обрывается по достижении лимита времени

Способ устранения

Для устранения затруднения:

1. Добавьте в конфигурационный файл `.env` переменную `COMPOSE_HTTP_TIMEOUT` и присвойте ей значение больше 60.
2. Повторно выполните запуск работы контейнеров.

Недостаточный размер оперативной памяти аппаратного комплекса или виртуальной машины, на которой развернут Комплекс

Способ устранения

Для устранения затруднения:

Увеличьте размер оперативной памяти.

8.1.21. Ошибки вида «<...>Cannot start service <...>. Bind for <ip_address>:<TCP/UDP_port> is ready allocated» при попытке запуска контейнеров

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:

- а. Узнайте наименование сервиса, которым занят порт, с помощью команды:

```
netstat -tulpn | grep [номер_порта]
```

- б. Узнайте номер процесса, к которому относится сервис:

```
pidof [имя-сервиса]
```

- в. Остановите процесс с полученным номером:

```
kill -9 [номер_процесса]
```

- г. При необходимости остановки процесса и его дочерних процессов:

```
killall [номер_процесса]
```

- д. Повторите запуск работы контейнеров Комплекса.

8.1.22. Недоступен сервис корреляции событий

Причина: ретроспективный анализ был удален до того, как проверка была завершена

Способ устранения

Для устранения затруднения:

1. Подключитесь к операционной системе Комплекса уровня Management.
2. Перезапустите сервис корреляции событий. Для этого введите следующую команду:

```
systemctl restart udv-esper.service
```

3. Дождитесь окончания перезапуска сервиса.
4. Убедитесь в работоспособности службы корреляции событий в веб-интерфейсе.

См. также

[Настройка инцидентов](#)

8.1.23. 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 и по умолчанию равно 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 (5-7 минут).

► **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:
 - а. 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 (5-7 минут).

► **Результат шага:** станет возможным вход в веб-интерфейс под любой учетной записью с любого количества устройств.

8.1.24. 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:

а. Убедитесь, что межсетевой экран `efw` не запущен и не будет конфликтовать с `iptables`:

```
cat /etc/net/ifaces/default/options | grep CONFIG_FW
```



Прим.:

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 аппаратных средствах);
- «Установка Комплекса уровня Management+Sensor на одном аппаратном средстве» (при установке сенсора и Комплекса уровня Management на одном аппаратном средстве).

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. 7. 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 <code>udv-rabbitmq</code> , <code>udv-rabbitmq-sensor</code> , <code>udv-redis</code> или <code>udv-redis-sensor</code>	Уровень Sensor: • <code>udv-node-exporter-sensor</code> • <code>udv-pushgateway</code> Уровень Management: • <code>udv-node_exporter</code> • <code>udv-prometheus</code>
Получение данных недоступно	Затруднения в работе сервиса отправки оперативных данных с сенсора	<code>udv-rabbitmq-sensor</code> (уровень Sensor)
	Затруднения в работе сервиса получения оперативных данных с сенсора на Комплексе	<code>udv-rabbitmq</code> (уровень Management)
Синхронизация настроек недоступна	Затруднения в работе сервиса отправки справочников с Комплекса на сенсор	<code>udv-redis</code> (уровень Management)

Табл. 7. Возможные ошибки в процессе работы иерархии

НАИМЕНОВАНИЕ ОШИБКИ	ВОЗМОЖНАЯ ПРИЧИНА	СЕРВИС, ОТВЕЧАЮЩИЙ ЗА РАБОТУ ИЕРАРХИИ
	Затруднения в работе сервиса получения справочников на сенсоре	udv-redis-sensor (уровень Sensor)
Не удастся 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](#)».

8.1.25. Потери при передаче данных через ERSPAN

При передаче трафика на UDV NTA через ERSPAN-туннель могут обнаруживаться следующие признаки потери данных:

- При передаче файла размером больше 1450 байт UDV NTA обнаруживает этот файл с размером меньше фактического. Размер обнаруженных файлов указывается в значении поля `total_bytes` на странице [Файлы](#).
- Ошибки в пакетах протокола IP при записи трафика, поступающего от актива на прослушивающий интерфейс UDV NTA, с помощью анализаторов трафика. Пример ошибки при просмотре записи трафика через Wireshark: Expert Info (Error/Protocol): IPv4 total length exceeds packet length.

Причина: отключенная поддержка Jumbo-кадров и недостаточные значения MTU на интерфейсах, передающих и получающих трафик через ERSPAN-туннель

Для устранения потерь трафика при передаче через ERSPAN-туннель:

1. Активируйте поддержку Jumbo-кадров в настройках сетевого оборудования, который отправляет ERSPAN-трафик на прослушивающий интерфейс UDV NTA уровня Sensor (сенсора).
2. Увеличьте значение MTU на следующих интерфейсах и устройствах из цепочки передачи данных от источника трафика до сенсора:
 - интерфейсе сетевого оборудования, прослушивающего трафик от источника;
 - ERSPAN-интерфейсе сетевого оборудования, на который копируется трафик от источника;
 - интерфейсе сетевого оборудования, отправляющего ERSPAN-трафик на прослушивающий интерфейс сенсора;
 - интерфейсе источника трафика.



Прим.:

Оптимальные значения MTU:

- [максимальный размер MTU на интерфейсах источника] + 50 — для интерфейсов передачи ERSPAN-трафика на сетевом оборудовании и для прослушивающего интерфейса сенсора;
- [максимальный размер MTU на интерфейсах источника] — для ERSPAN-интерфейса сетевого оборудования.

3. Увеличьте значение MTU на прослушивающем интерфейсе сенсора. Для этого:

- а. Подключитесь к операционной системе сенсора.
- б. Откройте на редактирование конфигурационный файл прослушивающего сетевого интерфейса, для которого требуется увеличить MTU, с помощью команды:

```
nano /etc/net/ifaces/[наименование интерфейса]/iplink
```

- в. Добавьте в файл следующую строку:

```
mtu [рассчитанное значение MTU]
```

- г. Сохраните и закройте файл.
- д. Убедитесь, что увеличилось значение MTU прослушивающего интерфейса. Для этого выполните команду:

```
ip a | grep [наименование интерфейса]
```

- **Результат шага:** Значение поля `mtu` совпадает со значением, указанным в конфигурационном файле.

8.2. 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](#)

8.2.1. 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_detected` 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.

8.2.2. 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.

8.3. 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, устраняются путем проверки и исправлений настроек сети управляющего контура комплекса и локальных настроек Комплекса.

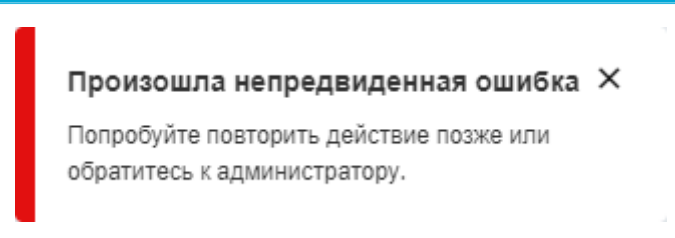
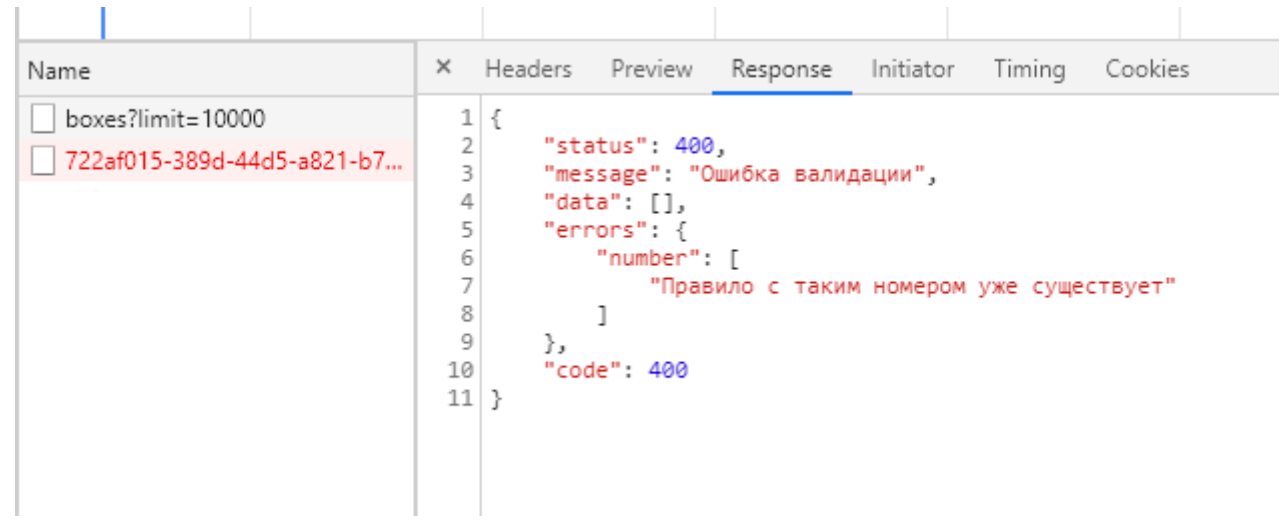
8.4. Анкета при обращении в сервисный центр



Прим.:

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 *		1.0.0.0
Общее количество Активов, сессий, событий в сутки на проблемном UDV NTA (включая полученные снизу)		150 ОЗ, 300 тыс. сессий, 250 тыс. событий в сутки
Количество подчиненных UDV NTA		2 уровня Sensor
Краткое описание ошибки (словесное) *		Не создается правило обнаружения вторжений
Действия, которые привели к ошибке (подробное описание шагов, приведших к ошибке) *		Перешел на страницу правил обнаружений, в окне «Создание правила обнаружения» заполнил все поля, при сохранении появилась 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-suricata-backend, udv-postgresql
Архив всех логов сервисов (скрипт <code>get_logs.bash</code> на файловом сервере)		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 *		Centos 8.1
Вывод таблицы маршрутизации (route -n или ip route show)		<pre> [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 42 8 172.10.0.0/16 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 link down 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]# </pre>

ПАРАМЕТР	ЗНАЧЕНИЕ	ПРИМЕР ЗАПОЛНЕНИЯ																																																																																																																																																																																																												
Свободное место на корневом разделе диска (df -h /)	Свободное место на корневом разделе: 2.5 ТБ	1 [66.8%] 2 [67.8%] 3 [96.4%] Mem [14.0G/15.2G] Swp [7.62G/7.73G] 4 [63.9%] 5 [67.4%] 6 [83.6%] Tasks: 260, 24232 thr; 6 running Load average: 14.47 12.47 11.11 Uptime: 59 days, 05:02:16 <table><thead><tr><th>PID</th><th>USER</th><th>PRI</th><th>NI</th><th>VIRT</th><th>RES</th><th>SHR</th><th>S</th><th>CPU%</th><th>MEM%</th><th>TIME+</th><th>Command</th></tr></thead><tbody><tr><td>22369</td><td>systemd-c</td><td>20</td><td>0</td><td>170G</td><td>216M</td><td>5788</td><td>S</td><td>254.</td><td>1.4</td><td>163h</td><td>python -m alertin</td></tr><tr><td>23531</td><td>root</td><td>20</td><td>0</td><td>1381M</td><td>173M</td><td>131M</td><td>S</td><td>102.</td><td>1.1</td><td>627h</td><td>godpi -i eno1 -af</td></tr><tr><td>23638</td><td>root</td><td>20</td><td>0</td><td>1381M</td><td>173M</td><td>131M</td><td>R</td><td>102.</td><td>1.1</td><td>43h38:56</td><td>godpi -i eno1 -af</td></tr><tr><td>14533</td><td>root</td><td>20</td><td>0</td><td>55468</td><td>18056</td><td>3880</td><td>R</td><td>41.1</td><td>0.1</td><td>0:03.14</td><td>htop</td></tr><tr><td>26342</td><td>systemd-c</td><td>20</td><td>0</td><td>3557M</td><td>205M</td><td>464</td><td>S</td><td>4.3</td><td>1.3</td><td>39h28:27</td><td>/usr/lib/erlang/e</td></tr><tr><td>2598</td><td>root</td><td>20</td><td>0</td><td>10744</td><td>3744</td><td>2588</td><td>S</td><td>0.0</td><td>0.0</td><td>4:59.47</td><td>containerd-shim -</td></tr><tr><td>2589</td><td>root</td><td>20</td><td>0</td><td>10744</td><td>3744</td><td>2588</td><td>S</td><td>0.0</td><td>0.0</td><td>32:22.70</td><td>containerd-shim -</td></tr><tr><td>24969</td><td>systemd-c</td><td>20</td><td>0</td><td>170G</td><td>216M</td><td>5788</td><td>S</td><td>0.0</td><td>1.4</td><td>3:46.89</td><td>python -m alertin</td></tr></tbody></table> Total DISK READ : 0.00 B/s Total DISK WRITE : 55.89 K/s Actual DISK READ: 0.00 B/s Actual DISK WRITE: 63.15 K/s <table><thead><tr><th>TID</th><th>PRI</th><th>USER</th><th>DISK READ</th><th>DISK WRITE</th><th>SWAPIN</th><th>IO></th><th>COMMAND</th></tr></thead><tbody><tr><td>5199</td><td>be/4</td><td>systemd-</td><td>0.00 B/s</td><td>53.65 K/s</td><td>0.00 %</td><td>1.78 %</td><td>mysqld --~le-log-bir</td></tr><tr><td>24390</td><td>be/4</td><td>systemd-</td><td>0.00 B/s</td><td>0.00 B/s</td><td>0.00 %</td><td>1.36 %</td><td>mysqld --~le-log-bir</td></tr><tr><td>12718</td><td>be/4</td><td>root</td><td>0.00 B/s</td><td>0.00 B/s</td><td>0.00 %</td><td>0.10 %</td><td>[kworker/~efficient]</td></tr><tr><td>24392</td><td>be/4</td><td>systemd-</td><td>0.00 B/s</td><td>2.24 K/s</td><td>0.00 %</td><td>0.00 %</td><td>mysqld --~le-log-bir</td></tr><tr><td>1</td><td>be/4</td><td>root</td><td>0.00 B/s</td><td>0.00 B/s</td><td>0.00 %</td><td>0.00 %</td><td>systemd --rialize 18</td></tr><tr><td>2</td><td>be/4</td><td>root</td><td>0.00 B/s</td><td>0.00 B/s</td><td>0.00 %</td><td>0.00 %</td><td>[kthreadd]</td></tr><tr><td>3</td><td>be/0</td><td>root</td><td>0.00 B/s</td><td>0.00 B/s</td><td>0.00 %</td><td>0.00 %</td><td>[rcu_gp]</td></tr><tr><td>4</td><td>be/0</td><td>root</td><td>0.00 B/s</td><td>0.00 B/s</td><td>0.00 %</td><td>0.00 %</td><td>[rcu_par_gp]</td></tr><tr><td>6</td><td>be/0</td><td>root</td><td>0.00 B/s</td><td>0.00 B/s</td><td>0.00 %</td><td>0.00 %</td><td>[kworker/~H-kblockd]</td></tr><tr><td>8</td><td>be/0</td><td>root</td><td>0.00 B/s</td><td>0.00 B/s</td><td>0.00 %</td><td>0.00 %</td><td>[mm_percpu_wq]</td></tr><tr><td>9</td><td>be/4</td><td>root</td><td>0.00 B/s</td><td>0.00 B/s</td><td>0.00 %</td><td>0.00 %</td><td>[ksoftirqd/0]</td></tr></tbody></table>	PID	USER	PRI	NI	VIRT	RES	SHR	S	CPU%	MEM%	TIME+	Command	22369	systemd-c	20	0	170G	216M	5788	S	254.	1.4	163h	python -m alertin	23531	root	20	0	1381M	173M	131M	S	102.	1.1	627h	godpi -i eno1 -af	23638	root	20	0	1381M	173M	131M	R	102.	1.1	43h38:56	godpi -i eno1 -af	14533	root	20	0	55468	18056	3880	R	41.1	0.1	0:03.14	htop	26342	systemd-c	20	0	3557M	205M	464	S	4.3	1.3	39h28:27	/usr/lib/erlang/e	2598	root	20	0	10744	3744	2588	S	0.0	0.0	4:59.47	containerd-shim -	2589	root	20	0	10744	3744	2588	S	0.0	0.0	32:22.70	containerd-shim -	24969	systemd-c	20	0	170G	216M	5788	S	0.0	1.4	3:46.89	python -m alertin	TID	PRI	USER	DISK READ	DISK WRITE	SWAPIN	IO>	COMMAND	5199	be/4	systemd-	0.00 B/s	53.65 K/s	0.00 %	1.78 %	mysqld --~le-log-bir	24390	be/4	systemd-	0.00 B/s	0.00 B/s	0.00 %	1.36 %	mysqld --~le-log-bir	12718	be/4	root	0.00 B/s	0.00 B/s	0.00 %	0.10 %	[kworker/~efficient]	24392	be/4	systemd-	0.00 B/s	2.24 K/s	0.00 %	0.00 %	mysqld --~le-log-bir	1	be/4	root	0.00 B/s	0.00 B/s	0.00 %	0.00 %	systemd --rialize 18	2	be/4	root	0.00 B/s	0.00 B/s	0.00 %	0.00 %	[kthreadd]	3	be/0	root	0.00 B/s	0.00 B/s	0.00 %	0.00 %	[rcu_gp]	4	be/0	root	0.00 B/s	0.00 B/s	0.00 %	0.00 %	[rcu_par_gp]	6	be/0	root	0.00 B/s	0.00 B/s	0.00 %	0.00 %	[kworker/~H-kblockd]	8	be/0	root	0.00 B/s	0.00 B/s	0.00 %	0.00 %	[mm_percpu_wq]	9	be/4	root	0.00 B/s	0.00 B/s	0.00 %	0.00 %	[ksoftirqd/0]
PID	USER		PRI	NI	VIRT	RES	SHR	S	CPU%	MEM%	TIME+	Command																																																																																																																																																																																																		
22369	systemd-c		20	0	170G	216M	5788	S	254.	1.4	163h	python -m alertin																																																																																																																																																																																																		
23531	root		20	0	1381M	173M	131M	S	102.	1.1	627h	godpi -i eno1 -af																																																																																																																																																																																																		
23638	root	20	0	1381M	173M	131M	R	102.	1.1	43h38:56	godpi -i eno1 -af																																																																																																																																																																																																			
14533	root	20	0	55468	18056	3880	R	41.1	0.1	0:03.14	htop																																																																																																																																																																																																			
26342	systemd-c	20	0	3557M	205M	464	S	4.3	1.3	39h28:27	/usr/lib/erlang/e																																																																																																																																																																																																			
2598	root	20	0	10744	3744	2588	S	0.0	0.0	4:59.47	containerd-shim -																																																																																																																																																																																																			
2589	root	20	0	10744	3744	2588	S	0.0	0.0	32:22.70	containerd-shim -																																																																																																																																																																																																			
24969	systemd-c	20	0	170G	216M	5788	S	0.0	1.4	3:46.89	python -m alertin																																																																																																																																																																																																			
TID	PRI	USER	DISK READ	DISK WRITE	SWAPIN	IO>	COMMAND																																																																																																																																																																																																							
5199	be/4	systemd-	0.00 B/s	53.65 K/s	0.00 %	1.78 %	mysqld --~le-log-bir																																																																																																																																																																																																							
24390	be/4	systemd-	0.00 B/s	0.00 B/s	0.00 %	1.36 %	mysqld --~le-log-bir																																																																																																																																																																																																							
12718	be/4	root	0.00 B/s	0.00 B/s	0.00 %	0.10 %	[kworker/~efficient]																																																																																																																																																																																																							
24392	be/4	systemd-	0.00 B/s	2.24 K/s	0.00 %	0.00 %	mysqld --~le-log-bir																																																																																																																																																																																																							
1	be/4	root	0.00 B/s	0.00 B/s	0.00 %	0.00 %	systemd --rialize 18																																																																																																																																																																																																							
2	be/4	root	0.00 B/s	0.00 B/s	0.00 %	0.00 %	[kthreadd]																																																																																																																																																																																																							
3	be/0	root	0.00 B/s	0.00 B/s	0.00 %	0.00 %	[rcu_gp]																																																																																																																																																																																																							
4	be/0	root	0.00 B/s	0.00 B/s	0.00 %	0.00 %	[rcu_par_gp]																																																																																																																																																																																																							
6	be/0	root	0.00 B/s	0.00 B/s	0.00 %	0.00 %	[kworker/~H-kblockd]																																																																																																																																																																																																							
8	be/0	root	0.00 B/s	0.00 B/s	0.00 %	0.00 %	[mm_percpu_wq]																																																																																																																																																																																																							
9	be/4	root	0.00 B/s	0.00 B/s	0.00 %	0.00 %	[ksoftirqd/0]																																																																																																																																																																																																							
Свободная оперативная память, текущий список процессов (htop)	Свободная оперативная память: 1 МБ																																																																																																																																																																																																													
Значение Load Average	Load Average: 14																																																																																																																																																																																																													
Загрузка диска (iotop)																																																																																																																																																																																																														

ПАРАМЕТР	ЗНАЧЕНИЕ	ПРИМЕР ЗАПОЛНЕНИЯ
Наличие сетевых доступов до проблемного Актива/UDV NTA (curl [ip_addr]:[port_number])		<pre> curl: (36) 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><h2>Not Found</h2> <hr><p>HTTP Error 404. The requested resource is not found.</p> </BODY></HTML> </pre>
Запись трафика (pcap-файл) для ошибок, связанных с обнаружением сессий/сетевых соединений/IDS		Во вложении

9. Справочная информация

В этом разделе:

1. Условные обозначения
2. Разделение функций по администрированию
3. Интерфейс Комплекса
4. Дополнительные функции Комплекса
5. Условия эксплуатации Комплекса
6. Описание служебных источников событий
7. Описание полей событий
8. Переменные Комплекса
9. Основные переменные файла `environment.json`
10. Отображение времени в Комплексе
11. Работа с импортируемыми панелями мониторинга
12. Сетевые взаимодействия Комплексов
13. Синтаксис правил корреляции событий
14. События, попадающие в разделы мониторинга
15. Структура директорий Комплекса
16. Признаки неактивности сессий
17. Протоколы, обнаруживаемые UDV NTA в режиме индикации
18. Сетевые атаки, обнаруживаемые UDV NTA
19. Переменные файла белого списка

9.1. Условные обозначения

В настоящем руководстве приняты условные обозначения, ознакомиться с которыми можно в таблице (Таблица 8. Условные обозначения).

Табл. 8. Условные обозначения

ПРИМЕР ТЕКСТА С УСЛОВНЫМ ОБОЗНАЧЕНИЕМ	ОПИСАНИЕ
 ОСТОРОЖНО: Если вы увидите сообщение В период между получением эталонной конфигурации и выбранной было обнаружено отклонение, 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

Табл. 8. Условные обозначения

ПРИМЕР ТЕКСТА С УСЛОВНЫМ ОБОЗНАЧЕНИЕМ	ОПИСАНИЕ
 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.	Важная информация, требующая осмысленного подхода при работе с Комплексом, включая справочные сведения и рекомендации
 Подсказка: 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
<code>cd /opt/datapk</code>	Блок кода. Содержит исполняемые команды или выдержки из кода программ

9.2. Разделение функций по администрированию

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

Табл. 9. Функциональные роли по администрированию Комплекса

НАИМЕНОВАНИЕ ФУНКЦИОНАЛЬНОЙ РОЛИ	КРАТКОЕ ОПИСАНИЕ ОСНОВНЫХ ФУНКЦИЙ
Инженер	• Определение состава активов • Добавление активов в каталог активов • Определение легитимности изменений в составе активов • Определение легитимности сетевых соединений • Редактирование карты сети • Привязывание интерфейсов к активам • Формирование отчетов по событиям и инцидентам ИБ • Анализ событий и инцидентов ИБ

Табл. 9. 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 СЗИ • 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 • Сканирование сети • Управление иерархией
Просмотр веб-интерфейса	Просмотр всех разделов Комплекса
Просмотр панели мониторинга	Непрерывный просмотр страницы Статус защищенности

9.3. Интерфейс Комплекса

В разделе описаны детали работы с веб-интерфейсом Комплекса.

- Страницы интерфейса
- Управляющие элементы
- Элементы управления таблицами
- Цветовая индикация и виды уведомлений

9.3.1. Страницы интерфейса

В подразделе описаны все содержащиеся в интерфейсе страницы.

- Мониторинг
 - Статус защищенности
 - Панели мониторинга
 - Виджеты
- Инциденты

- Активы
- События
 - Экспертный режим
- Инспекция сети
 - Карта сети
 - Сетевые соединения
 - Сессии
 - Пакеты
 - Файлы
 - HTTP
 - DNS
 - SMB_CMD
 - DCE_RPC
 - NTLM
 - SSH
 - SSL
 - Kerberos
 - Modbus
 - RDP
 - SMTP
 - OPC UA
 -
- Сенсоры
- Администрирование
 - Основные настройки
 - О системе
 - Импорт и экспорт
 - Диагностика
 - Настройки мониторинга
 - События и инциденты
 - Ретроанализ
 - Правила корреляции
 - Схема корреляции
 - Статусы инцидентов
 - Оповещения об инцидентах
 - Индексы
 - Пользователи
 - Пользователи
 - Парольная политика
 - Сигнатурный анализ
 - Правила обнаружения
 - Настройка активов
 - Классификаторы
 - Источники
- Страница «Страница не найдена»

9.3.1.1. Мониторинг

Пункт главного меню, содержащий страницы [Статус защищенности](#), [Панели мониторинга](#) и [Виджеты](#).

- См. также
- [Статус защищенности](#)
- [Панели мониторинга](#)
- [Виджеты](#)

9.3.1.1.1. Статус защищенности

Подраздел мониторинга, в котором отображаются статистика и изменения в реальном времени по ключевым оперативным данным Комплекса.

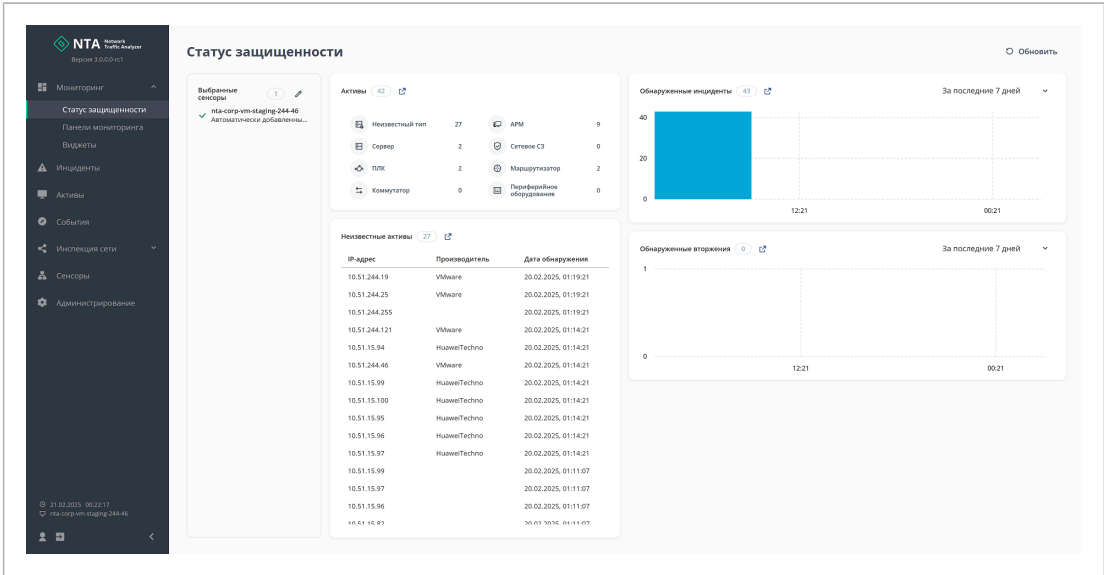


Рис. 173. Страница «Статус защищенности»

- См. также
- [Просмотр главной панели мониторинга «Статус защищенности»](#)

9.3.1.1.2. Панели мониторинга

Подраздел мониторинга, в котором располагаются созданные пользователем или предоставленные производителем Комплекса панели мониторинга. Расположенные в подразделе объекты доступны для редактирования.

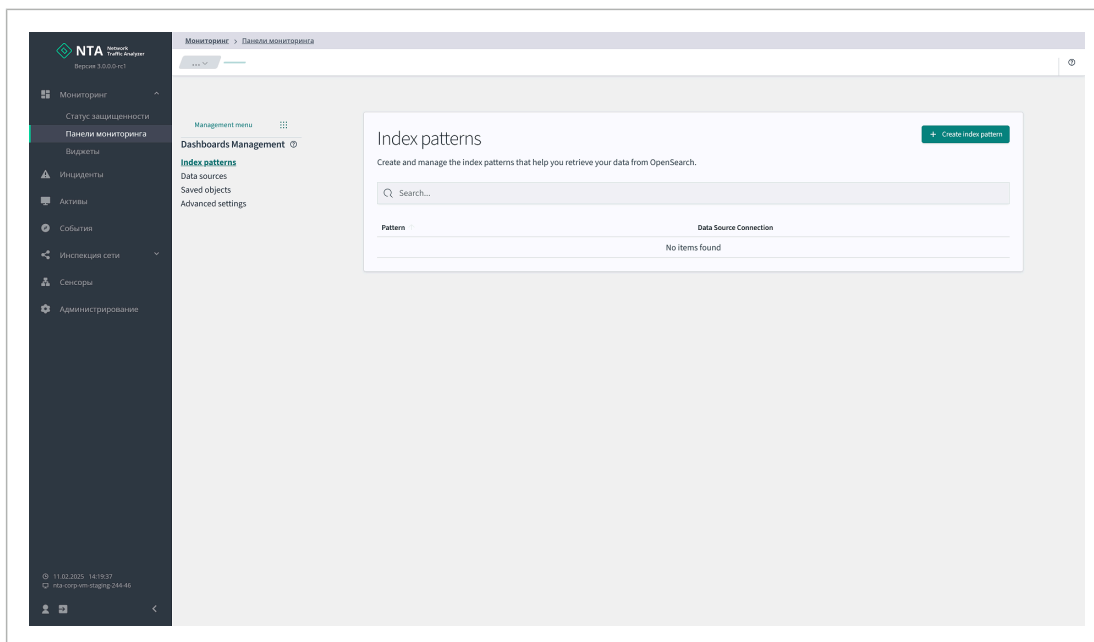


Рис. 174. Страница «Панели мониторинга»

См. также[Создание и настройка панели мониторинга](#)[Импортируемые панели мониторинга](#)[Виджеты](#)**9.3.1.1.3. Виджеты**

Подраздел мониторинга, в котором можно создавать и редактировать визуализации. Из визуализаций состоят панели мониторинга.

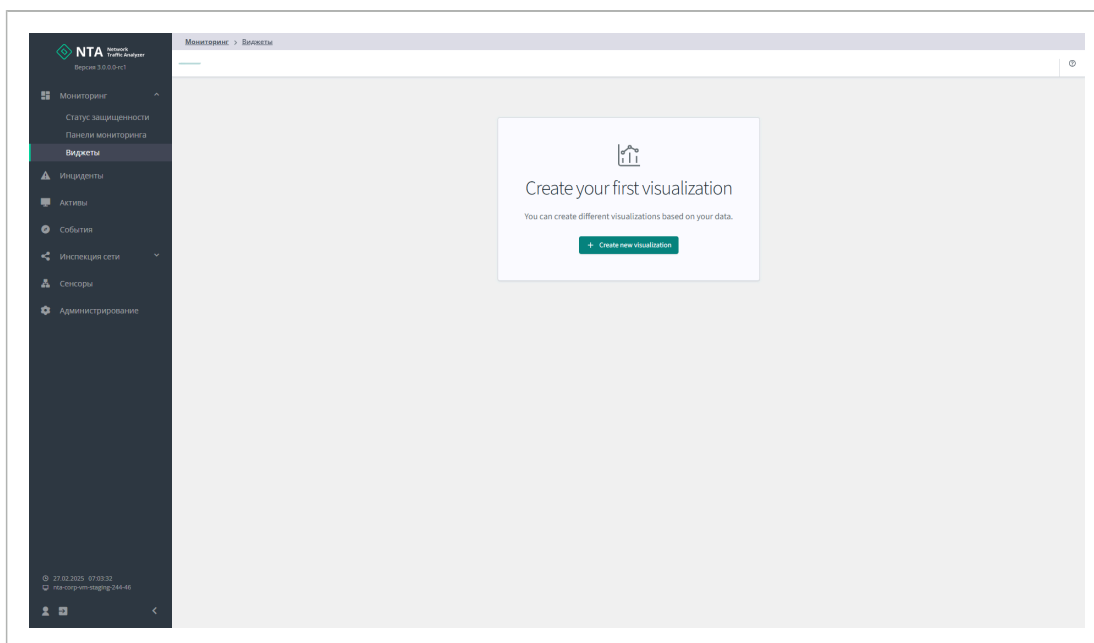


Рис. 175. Страница «Виджеты»

См. также

[Панели мониторинга](#)

[Создание и настройка виджета](#)

9.3.1.2. Инциденты

Пункт главного меню, 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.

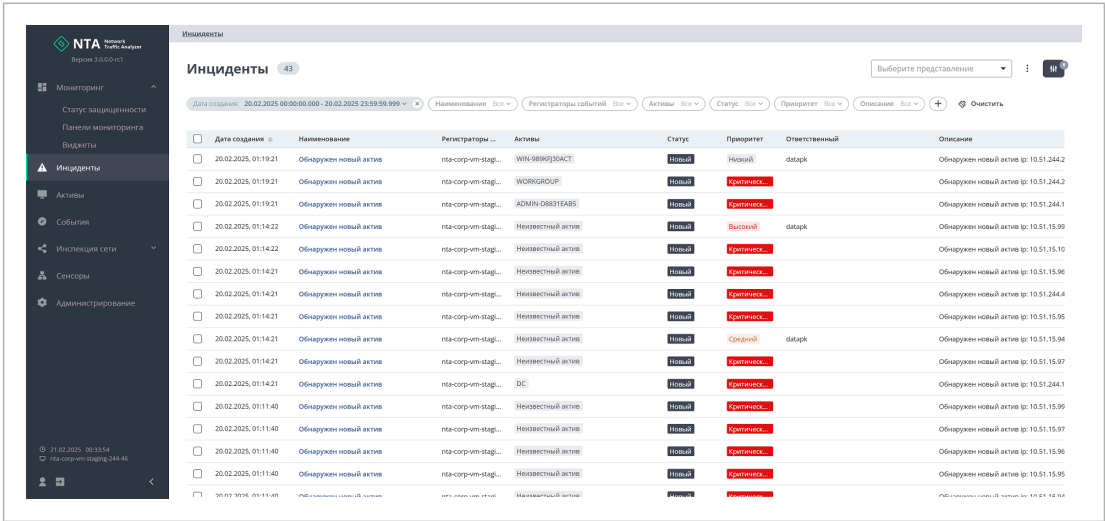


Рис. 176. Страница «Инциденты»

См. также

[Управление статусами инцидентов](#)

[Изменение параметров инцидента](#)

[Удаление инцидента](#)

[Групповые операции над инцидентами](#)

9.3.1.3. 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, страница актива с детальной информацией, события, инциденты, источники, активы на карте сети), кнопки экспорта, импорта, создания отчетов, создания и удаления активов, столбцы статусов и статистики по доступности активов и инцидентам.

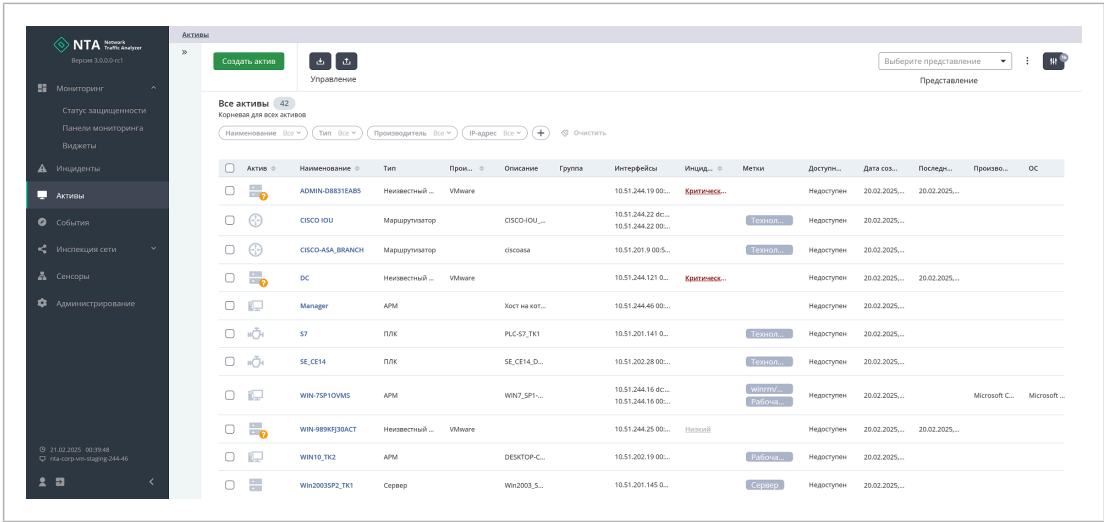


Рис. 177. Страница «Активы»

См. также
Работа с активами

9.3.1.3.1. Страница актива

Не является разделом основного интерфейса. Перейти на страницу актива можно со страниц [Активы](#), [Карта сети](#), [Инциденты](#), [События](#), если в событии определен актив, из карточки актива и карточки сессии при нажатии на иконку  (**Подробнее об активе**) или на название актива. Доступен просмотр в отдельной вкладке. Содержание страницы различается в зависимости от актива, для которого она открыта.

В верхней части страницы расположен заголовок, совпадающий с наименованием просматриваемого актива. В правой части заголовка расположена кнопка удаления актива.

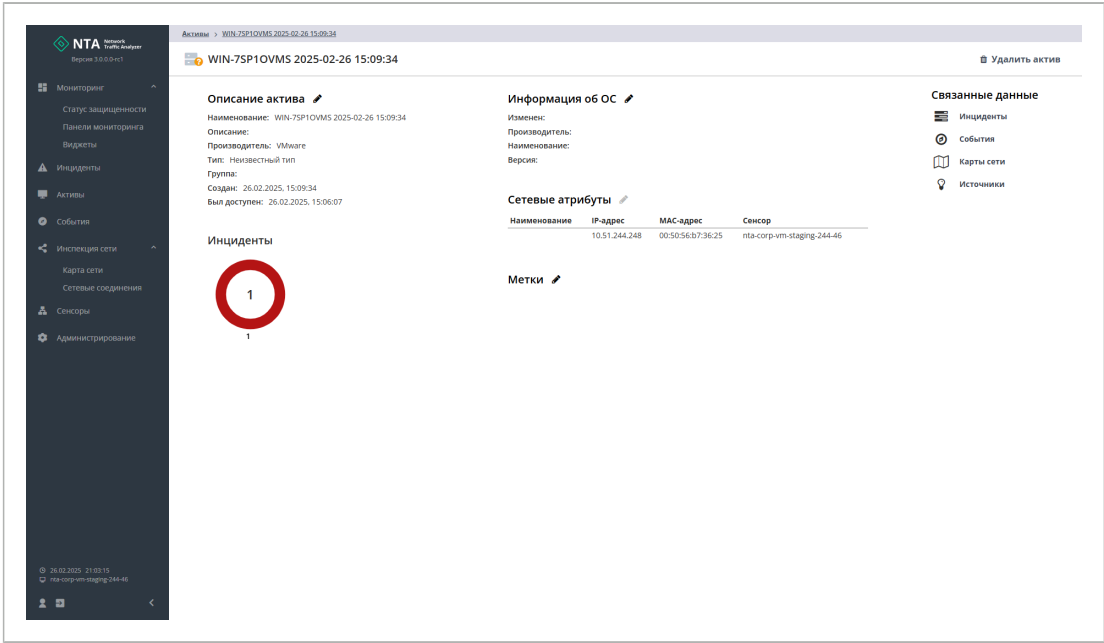


Рис. 178. Страница актива

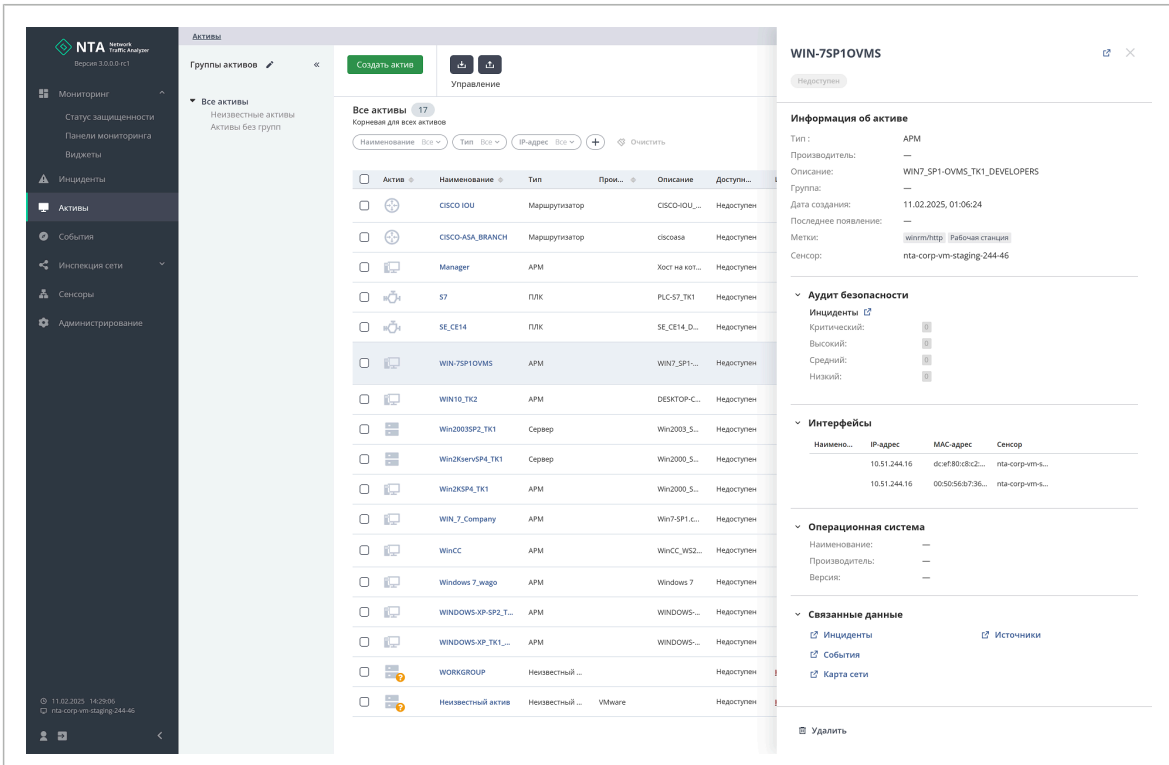
После заголовка расположены следующие блоки с информацией о примененных к активу параметрах:

1. Описание актива. Содержит информацию о Комплексе, к которому относится актив, наименовании, описании, производителе, типе, группе актива, датах создания и появления, IP- и MAC-адресах.
2. Виджет **Инциденты** для отображения состояния компонентов ИБ на активе.
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. **Сетевые атрибуты**. Содержит используемые IP- и MAC-адреса, с которых происходит прослушивание трафика актива, а также содержит информацию о сенсорах, чьим контролируемым сетям принадлежат IP-адреса сетевых атрибутов.
5. **Метки**. Содержит список присвоенных активу меток и кнопку  (**Редактировать**) для присвоения активу ранее созданных меток.
6. **Связанные данные**. Содержит ссылки на разделы, относящиеся к активу.

9.3.1.3.2. Карточка актива

Не является разделом основного интерфейса. Перейти в карточку актива можно со страницы **Активы**, нажав в строке нужного актива в любую ячейку, не содержащую ссылку.

В верхней части карточки расположен заголовок, совпадающий с наименованием просматриваемого актива. В правой части заголовка расположена иконка перехода на страницу актива  и кнопка закрытия карточки актива . Под заголовком расположен статус доступности актива: **Доступен** или **Недоступен**.



The screenshot displays the NTA Network Traffic Analyzer interface. The main panel shows a list of assets under the 'Активы' section. The selected asset, 'WIN-7SP1OVMS', is highlighted. The right sidebar provides detailed information for this asset, including its type (APM), manufacturer (WIN7_SP1-OVMS_TK1_DEVELOPERS), and various attributes like IP and MAC addresses. The sidebar also includes sections for security audit, interfaces, operating system, and related data.

Рис. 179. Карточка актива

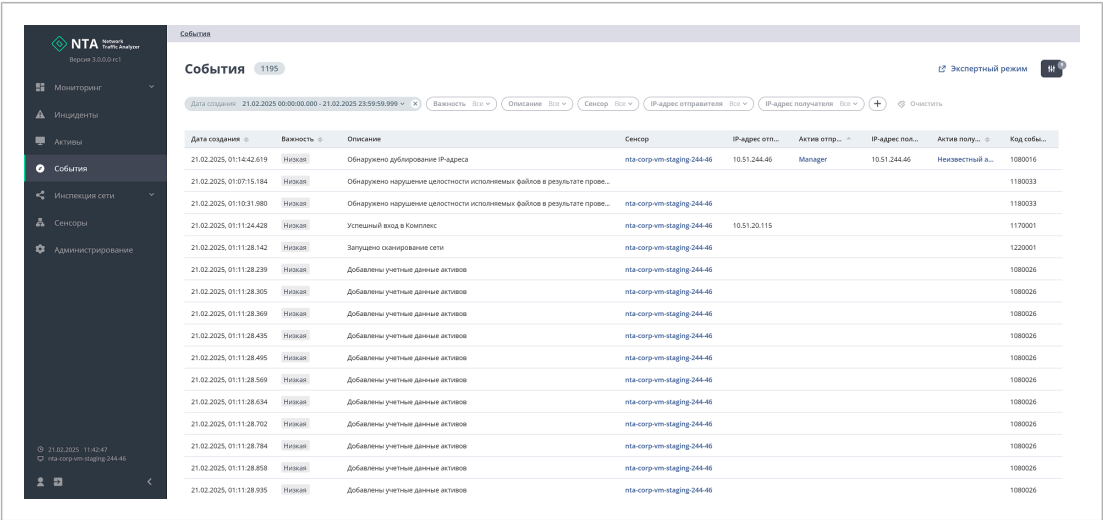
После заголовка расположены следующие блоки с информацией о примененных к активу параметрах:

- 1. **Информация об активе.** Содержит информацию о типе и производителе актива, наименовании Комплекса и группе, к которому относится актив, датах создания и последнего появления, о присвоенных активу метках и наименование сенсора, которому принадлежит актив.
- 2. **Аудит безопасности.** Содержит статистику по приоритетам инцидентов и иконку перехода на страницу [Инциденты](#) с информацией об инцидентах, выявленных на активе.
- 3. **Интерфейсы.** Содержит информацию о сетевых атрибутах актива: используемые IP- и MAC-адреса, с которых происходит прослушивание трафика актива, а также наименования сенсоров, чьим контролируемым сетям принадлежат IP-адреса сетевых атрибутов.
- 4. **Операционная система.** Содержит информацию об ОС: наименовании, производителе и версии.
- 5. **Связанные данные.** Содержит ссылки на разделы, относящиеся к активу.

Внизу карточки актива расположена кнопка удаления актива  **Удалить**.

9.3.1.4. События

Пункт главного меню, содержащий список всех событий Комплекса и набор фильтров для упрощенного поиска событий.



Дата создания	Важность	Описание	Сенсор	IP-адрес отп...	Актив отпр...	IP-адрес полу...	Актив полу...	Код собы...
21.02.2025, 01:14:42.619	Низкая	Обнаружено дублирование IP-адреса	nta-corp-wm-staging-244-46	10.51.244.46	Manager	10.51.244.46	Неизвестный а...	1080016
21.02.2025, 01:07:15.184	Низкая	Обнаружено нарушение целостности исполняемых файлов в результате прове...	nta-corp-wm-staging-244-46					1180033
21.02.2025, 01:10:31.980	Низкая	Обнаружено нарушение целостности исполняемых файлов в результате прове...	nta-corp-wm-staging-244-46					1180033
21.02.2025, 01:11:24.428	Низкая	Успешный вход в Комплекс	nta-corp-wm-staging-244-46	10.51.20.115				1170001
21.02.2025, 01:11:28.142	Низкая	Запущено сканирование сети	nta-corp-wm-staging-244-46					1220001
21.02.2025, 01:11:28.239	Низкая	Добавлены учетные данные активов	nta-corp-wm-staging-244-46					1080026
21.02.2025, 01:11:28.305	Низкая	Добавлены учетные данные активов	nta-corp-wm-staging-244-46					1080026
21.02.2025, 01:11:28.369	Низкая	Добавлены учетные данные активов	nta-corp-wm-staging-244-46					1080026
21.02.2025, 01:11:28.435	Низкая	Добавлены учетные данные активов	nta-corp-wm-staging-244-46					1080026
21.02.2025, 01:11:28.495	Низкая	Добавлены учетные данные активов	nta-corp-wm-staging-244-46					1080026
21.02.2025, 01:11:28.569	Низкая	Добавлены учетные данные активов	nta-corp-wm-staging-244-46					1080026
21.02.2025, 01:11:28.634	Низкая	Добавлены учетные данные активов	nta-corp-wm-staging-244-46					1080026
21.02.2025, 01:11:28.702	Низкая	Добавлены учетные данные активов	nta-corp-wm-staging-244-46					1080026
21.02.2025, 01:11:28.784	Низкая	Добавлены учетные данные активов	nta-corp-wm-staging-244-46					1080026
21.02.2025, 01:11:28.858	Низкая	Добавлены учетные данные активов	nta-corp-wm-staging-244-46					1080026
21.02.2025, 01:11:28.935	Низкая	Добавлены учетные данные активов	nta-corp-wm-staging-244-46					1080026

Рис. 180. Страница «События»

См. также

[Поиск и просмотр событий в упрощенном режиме](#)

9.3.1.4.1. 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](#).

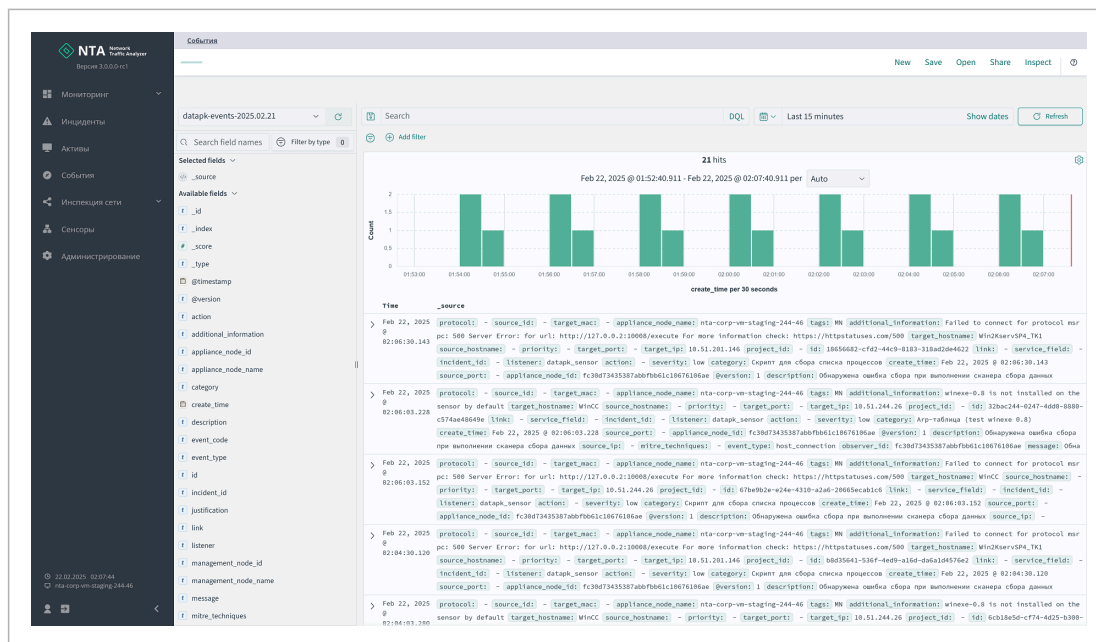


Рис. 181. Страница «Экспертный режим»

См. также

Просмотр событий и создание запросов в экспертном режиме

9.3.1.5. Инспекция сети

Пункт главного меню, содержащий страницы [Карта сети](#) и [Сетевые соединения](#).

См. также

[Карта сети](#)

[Сетевые соединения](#)

9.3.1.5.1. Карта сети

Подраздел инспекции сети, предназначенный для просмотра карты сети и сохраненных представлений.

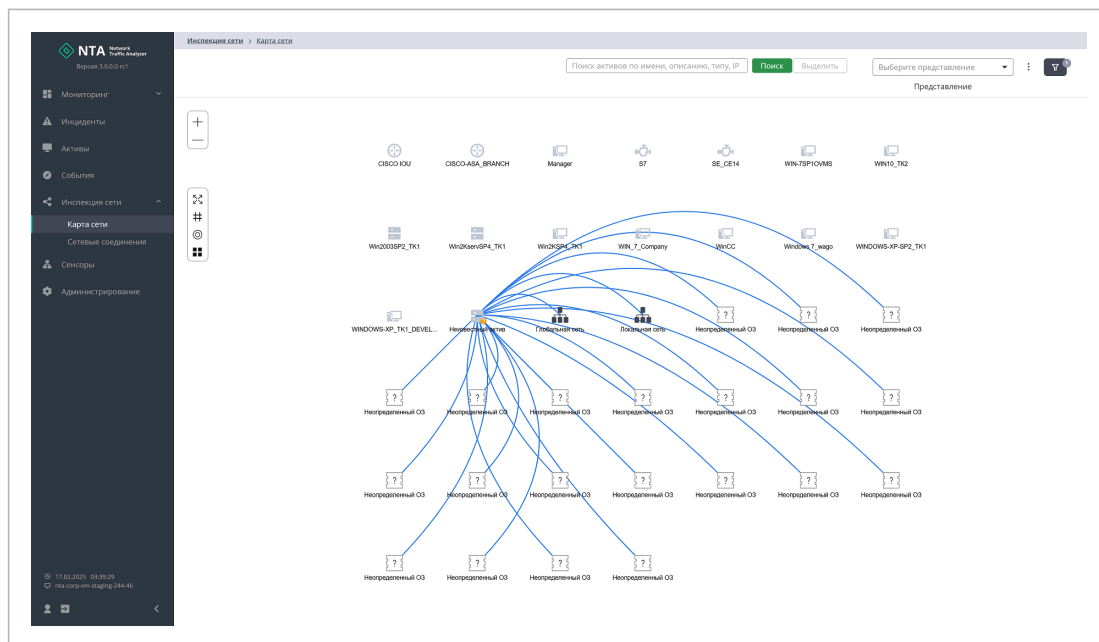


Рис. 182. Страница «Карта сети»

См. также[Просмотр карты сети](#)[Настройка представлений на карте](#)

9.3.1.5.2. Сетевые соединения

Подраздел инспекции сети для просмотра журналов взаимодействия Активов в прослушиваемых сетях. В разделе можно просматривать следующую информацию:

- список сессий, которые обнаруживает UDV NTA, — 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**

9.3.1.5.2.1. Сессии

Вкладка на странице **Сетевые соединения** — для просмотра журнала сетевых сессий, которые обнаруживает UDV NTA.

Обновлена	Обнаружена	Сенсор	Состояние	UID сессии	Протоколы	Транспортный пр...	IP-адрес отправит...	Порт отправителя	IP-адрес получате...
18.02.2025, 11:35:54	18.02.2025, 11:32:54	nta-corp-vm-staging...	SO	CS26n2u3Nhr...	NBNS	udp	10.51.244.121	137	10.51.244.255
18.02.2025, 11:35:51	18.02.2025, 11:33:51	nta-corp-vm-staging...	S1	0x5P9C24GKVD5...	SSL	tcp	10.199.0.23	62426	10.51.244.46
18.02.2025, 11:35:51	18.02.2025, 11:32:51	nta-corp-vm-staging...	SO	SVNHN2Vnm3c...		udp	10.51.244.121	138	10.51.244.255
18.02.2025, 11:35:50	18.02.2025, 11:35:50	nta-corp-vm-staging...	SO	CVK9Cvduy6b2j...	NBNS	udp	10.51.244.19	137	10.51.244.255
18.02.2025, 11:35:50	18.02.2025, 11:35:40	nta-corp-vm-staging...	SF	CDpC1Vb0qR04...	DNS	udp	10.51.244.46	55119	10.55.10.10
18.02.2025, 11:35:45	18.02.2025, 11:35:40	nta-corp-vm-staging...	SF	CoZn3u35N7AY...	SSL	tcp	10.199.0.23	55017	10.51.244.46
18.02.2025, 11:35:44	18.02.2025, 11:33:22	nta-corp-vm-staging...	SF	CPCFD2WuYKq7Jq...	SSL	tcp	10.199.0.23	62387	10.51.244.46
18.02.2025, 11:35:44	18.02.2025, 11:33:25	nta-corp-vm-staging...	SF	CoGAB2g2n6Cp...	SSL	tcp	10.199.0.23	62410	10.51.244.46
18.02.2025, 11:35:44	18.02.2025, 11:33:25	nta-corp-vm-staging...	SF	CPE1C1WuYHwM...	SSL	tcp	10.199.0.23	62413	10.51.244.46
18.02.2025, 11:35:44	18.02.2025, 11:33:25	nta-corp-vm-staging...	SF	CKERZ1fRbqAM...	SSL	tcp	10.199.0.23	62411	10.51.244.46
18.02.2025, 11:35:44	18.02.2025, 11:33:25	nta-corp-vm-staging...	SF	CYUdmgw25F8T9...	SSL	tcp	10.199.0.23	62412	10.51.244.46
18.02.2025, 11:35:41	18.02.2025, 01:09:32	nta-corp-vm-staging...	SO	CGQM1EwYB8...	NBNS	udp	10.51.244.16	137	10.51.244.255
18.02.2025, 11:35:33	18.02.2025, 11:34:33	nta-corp-vm-staging...	SF	CKwRqG2u3u...	NTP	udp	10.51.244.46	33246	217.170.87.229
18.02.2025, 11:35:25	18.02.2025, 11:33:25	nta-corp-vm-staging...	S1	CC3TFSOBANW9W...	SSL	tcp	10.199.0.23	62414	10.51.244.46
18.02.2025, 11:35:00	18.02.2025, 11:30:00	nta-corp-vm-staging...	S1	Cu4hg4p4mC2I...	DCE_RPC	NTLM	10.51.244.46	52788	10.51.244.26
18.02.2025, 11:35:00	18.02.2025, 11:34:00	nta-corp-vm-staging...	S1	CKd5m4BbFP6P...	DCE_RPC	NTLM	10.51.244.46	42118	10.51.244.26
18.02.2025, 11:35:00	18.02.2025, 11:32:00	nta-corp-vm-staging...	S1	CUyHnUq3pZu0...	DCE_RPC	NTLM	10.51.244.46	54268	10.51.201.146
18.02.2025, 11:35:00	18.02.2025, 11:34:00	nta-corp-vm-staging...	S1	CDJkphG0mvee...	DCE_RPC	NTLM	10.51.244.46	52170	10.51.201.146
18.02.2025, 11:34:52	18.02.2025, 11:31:52	nta-corp-vm-staging...	SO	CLzdg8f6tmucl...		udp	10.51.244.16	138	10.51.244.255
18.02.2025, 11:34:24	18.02.2025, 11:31:24	nta-corp-vm-staging...	SO	CM4D9yqR6ZEM...		udp	10.51.244.26	138	10.51.244.255

Рис. 183. Вкладка «Сессии» на странице «Сетевые соединения»

См. также

Сессия

9.3.1.5.2.2. Пакеты

Вкладка на странице **Сетевые соединения** — для просмотра записей о сетевых пакетах, обнаруживаемых UDV NTA 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**.

Дата обнаружения	Сенсор	UID сессии	IP-адрес отправителя	Порт отправителя	IP-адрес получателя	Порт получателя	Протокол
24.02.2025, 19:11:23	nta-corp-vm-staging-244-46	CR52Z2Z1q7qVtE03	10.199.0.60	61656	10.51.244.46	443	SSL
24.02.2025, 19:11:23	nta-corp-vm-staging-244-46	CWwKX71v05970PPQ7	10.199.0.60	61655	10.51.244.46	443	SSL
24.02.2025, 19:11:23	nta-corp-vm-staging-244-46	CYBwX303y0E0x6	10.199.0.60	61654	10.51.244.46	443	SSL
24.02.2025, 19:11:23	nta-corp-vm-staging-244-46	Cu2COLXK3pMwW0p6	10.199.0.60	61653	10.51.244.46	443	SSL
24.02.2025, 19:11:22	nta-corp-vm-staging-244-46	CMpH0991BWw0y0a	10.199.0.60	61650	10.51.244.46	443	SSL
24.02.2025, 19:11:22	nta-corp-vm-staging-244-46	CjwBp2n3QC540K56	10.51.244.46	60062	10.55.10.10	53	DNS
24.02.2025, 19:11:14	nta-corp-vm-staging-244-46	CZC1423R5awV0R75	10.199.0.60	61645	10.51.244.46	443	SSL
24.02.2025, 19:11:14	nta-corp-vm-staging-244-46	Cx05CV1pc3M1f9w	10.51.244.46	44502	10.55.10.10	53	DNS
24.02.2025, 19:10:03	nta-corp-vm-staging-244-46	CTFNC4pCgmvV6p4	10.51.244.46	34100	10.51.244.26	1027	DCE_RPC
24.02.2025, 19:10:03	nta-corp-vm-staging-244-46	CTFNC4pCgmvV6p4	10.51.244.46	34100	10.51.244.26	1027	DCE_RPC
24.02.2025, 19:10:02	nta-corp-vm-staging-244-46	CTFNC4pCgmvV6p4	10.51.244.46	34100	10.51.244.26	1027	DCE_RPC
24.02.2025, 19:10:02	nta-corp-vm-staging-244-46	CTFNC4pCgmvV6p4	10.51.244.46	34100	10.51.244.26	1027	DCE_RPC
24.02.2025, 19:10:02	nta-corp-vm-staging-244-46	CTFNC4pCgmvV6p4	10.51.244.46	34100	10.51.244.26	1027	DCE_RPC
24.02.2025, 19:10:02	nta-corp-vm-staging-244-46	CTFNC4pCgmvV6p4	10.51.244.46	34100	10.51.244.26	1027	DCE_RPC
24.02.2025, 19:10:02	nta-corp-vm-staging-244-46	CTFNC4pCgmvV6p4	10.51.244.46	34100	10.51.244.26	1027	DCE_RPC
24.02.2025, 19:10:02	nta-corp-vm-staging-244-46	CTFNC4pCgmvV6p4	10.51.244.46	34100	10.51.244.26	1027	DCE_RPC
24.02.2025, 19:10:02	nta-corp-vm-staging-244-46	CTFNC4pCgmvV6p4	10.51.244.46	34100	10.51.244.26	1027	DCE_RPC
24.02.2025, 19:10:02	nta-corp-vm-staging-244-46	CTFNC4pCgmvV6p4	10.51.244.46	34100	10.51.244.26	1027	DCE_RPC
24.02.2025, 19:10:02	nta-corp-vm-staging-244-46	CTFNC4pCgmvV6p4	10.51.244.46	34100	10.51.244.26	1027	DCE_RPC
24.02.2025, 19:10:02	nta-corp-vm-staging-244-46	CTFNC4pCgmvV6p4	10.51.244.46	34100	10.51.244.26	1027	DCE_RPC
24.02.2025, 19:10:02	nta-corp-vm-staging-244-46	CTFNC4pCgmvV6p4	10.51.244.46	34100	10.51.244.26	1027	DCE_RPC
24.02.2025, 19:10:02	nta-corp-vm-staging-244-46	CTFNC4pCgmvV6p4	10.51.244.46	34100	10.51.244.26	1027	DCE_RPC
24.02.2025, 19:10:02	nta-corp-vm-staging-244-46	CTFNC4pCgmvV6p4	10.51.244.46	34100	10.51.244.26	1027	DCE_RPC

Рис. 184. Вкладка «Пакеты» на странице «Сетевые соединения»

9.3.1.5.2.3. Файлы

Вкладка на странице **Сетевые соединения** — для просмотра информации о распознанных файлах, переданных в рамках сессий, и скачивания этих файлов.

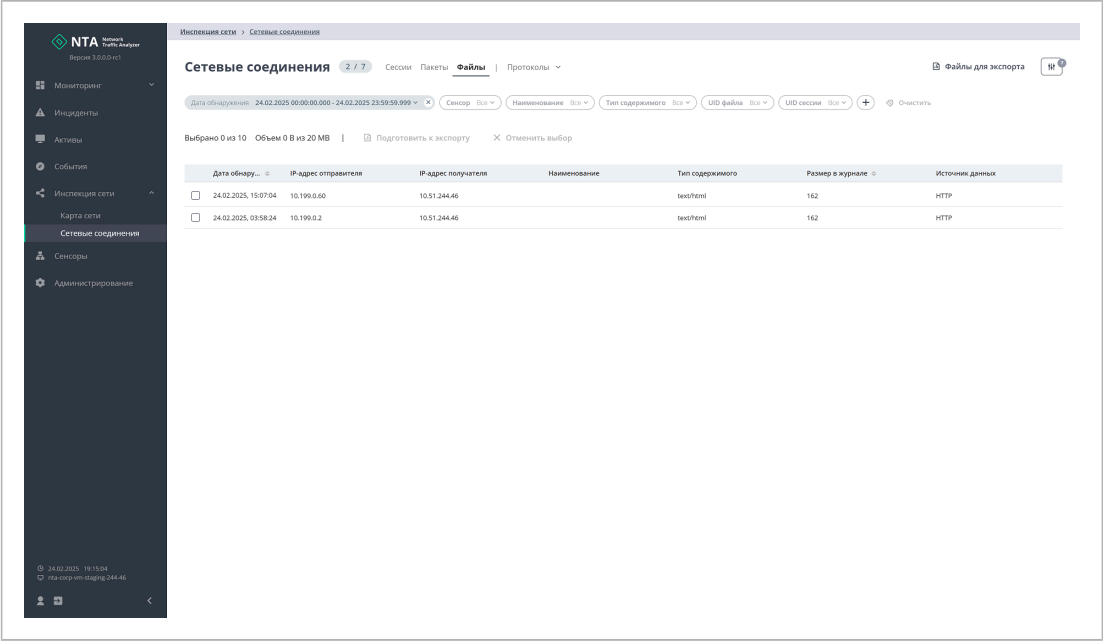


Рис. 185. Страница «Файлы»

См. также
Экспорт файлов, обнаруженных в сетевом трафике

9.3.1.5.2.4. HTTP

Вкладка из группы вкладок **Протоколы** на странице **Сетевые соединения** — для мониторинга HTTP-пакетов, обнаруживаемых UDV NTA в рамках сессий.

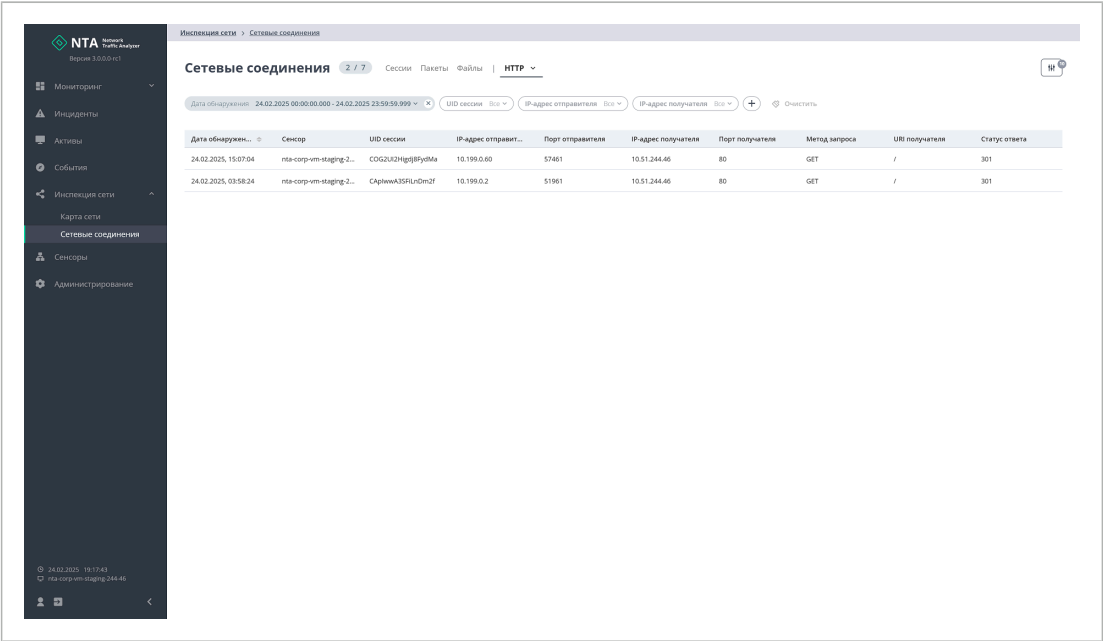
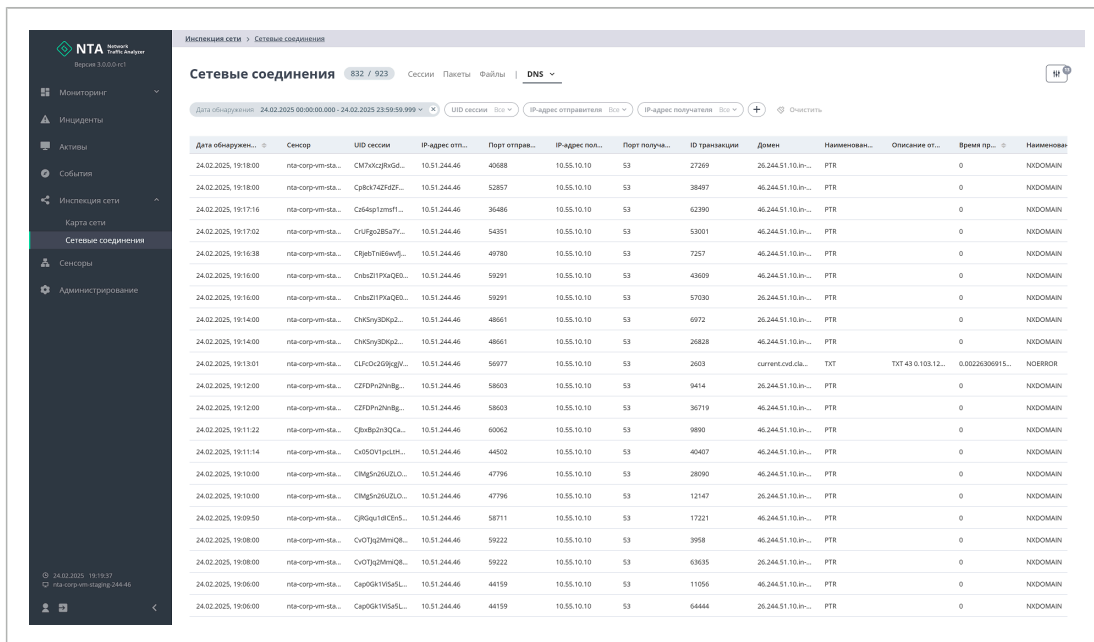


Рис. 186. Вкладка «HTTP» на странице «Сетевые соединения»

9.3.1.5.2.5. DNS

Вкладка из группы вкладок **Протоколы** на странице **Сетевые соединения** — для мониторинга DNS-пакетов, обнаруживаемых UDV NTA в рамках сессий.



Дата обнаружен...	Сенсор	UID сессии	IP-адрес отп...	Порт отправ...	IP-адрес пол...	Порт получ...	ID транзакции	Домен	Наименован...	Описание от...	Время пр...	Наименован...
24.02.2025, 19:18:00	nta-corp-vim-sta...	CM7Xc9RnGd...	10.51.244.46	40688	10.55.10.10	53	27269	25.244.51.10.10...	PTR		0	NIDOMAIN
24.02.2025, 19:18:00	nta-corp-vim-sta...	Cp8x74ZfGZf...	10.51.244.46	52857	10.55.10.10	53	38497	46.244.51.10.10...	PTR		0	NIDOMAIN
24.02.2025, 19:17:16	nta-corp-vim-sta...	C64apt1mstf1...	10.51.244.46	36486	10.55.10.10	53	62390	46.244.51.10.10...	PTR		0	NIDOMAIN
24.02.2025, 19:17:02	nta-corp-vim-sta...	CuIfg2B5a7Y...	10.51.244.46	54351	10.55.10.10	53	53001	46.244.51.10.10...	PTR		0	NIDOMAIN
24.02.2025, 19:16:38	nta-corp-vim-sta...	Cfje1TnE6wJ...	10.51.244.46	49780	10.55.10.10	53	7257	46.244.51.10.10...	PTR		0	NIDOMAIN
24.02.2025, 19:16:00	nta-corp-vim-sta...	Cn8z2fPxaQEB...	10.51.244.46	59291	10.55.10.10	53	43609	46.244.51.10.10...	PTR		0	NIDOMAIN
24.02.2025, 19:16:00	nta-corp-vim-sta...	Cn8z2fPxaQEB...	10.51.244.46	59291	10.55.10.10	53	57030	25.244.51.10.10...	PTR		0	NIDOMAIN
24.02.2025, 19:14:00	nta-corp-vim-sta...	CnK5ny1Ckq2...	10.51.244.46	48661	10.55.10.10	53	6972	25.244.51.10.10...	PTR		0	NIDOMAIN
24.02.2025, 19:14:00	nta-corp-vim-sta...	CnK5ny1Ckq2...	10.51.244.46	48661	10.55.10.10	53	25828	46.244.51.10.10...	PTR		0	NIDOMAIN
24.02.2025, 19:13:01	nta-corp-vim-sta...	CLPcDz1G9gJ...	10.51.244.46	56977	10.55.10.10	53	2603	current.cvd.cda...	TXT	TXT 43 0.103.12...	0.0022036915...	NOERROR
24.02.2025, 19:12:00	nta-corp-vim-sta...	CZTDPh2n8lg...	10.51.244.46	58603	10.55.10.10	53	9414	25.244.51.10.10...	PTR		0	NIDOMAIN
24.02.2025, 19:12:00	nta-corp-vim-sta...	CZTDPh2n8lg...	10.51.244.46	58603	10.55.10.10	53	36719	46.244.51.10.10...	PTR		0	NIDOMAIN
24.02.2025, 19:11:22	nta-corp-vim-sta...	CjwBpzn3QCa...	10.51.244.46	60062	10.55.10.10	53	9890	46.244.51.10.10...	PTR		0	NIDOMAIN
24.02.2025, 19:11:14	nta-corp-vim-sta...	CvK5SVY1pLH...	10.51.244.46	44502	10.55.10.10	53	40407	46.244.51.10.10...	PTR		0	NIDOMAIN
24.02.2025, 19:10:00	nta-corp-vim-sta...	CMg5n5uZU2D...	10.51.244.46	47796	10.55.10.10	53	28090	46.244.51.10.10...	PTR		0	NIDOMAIN
24.02.2025, 19:10:00	nta-corp-vim-sta...	CMg5n5uZU2D...	10.51.244.46	47796	10.55.10.10	53	12147	25.244.51.10.10...	PTR		0	NIDOMAIN
24.02.2025, 19:09:50	nta-corp-vim-sta...	CfG5ay1dCEh...	10.51.244.46	58711	10.55.10.10	53	17221	46.244.51.10.10...	PTR		0	NIDOMAIN
24.02.2025, 19:08:00	nta-corp-vim-sta...	CvOTJz3Mm1Q...	10.51.244.46	59222	10.55.10.10	53	3958	46.244.51.10.10...	PTR		0	NIDOMAIN
24.02.2025, 19:08:00	nta-corp-vim-sta...	CvOTJz3Mm1Q...	10.51.244.46	59222	10.55.10.10	53	63635	25.244.51.10.10...	PTR		0	NIDOMAIN
24.02.2025, 19:06:00	nta-corp-vim-sta...	CepQGR1V5dS...	10.51.244.46	44159	10.55.10.10	53	11056	46.244.51.10.10...	PTR		0	NIDOMAIN
24.02.2025, 19:06:00	nta-corp-vim-sta...	CepQGR1V5dS...	10.51.244.46	44159	10.55.10.10	53	64444	25.244.51.10.10...	PTR		0	NIDOMAIN

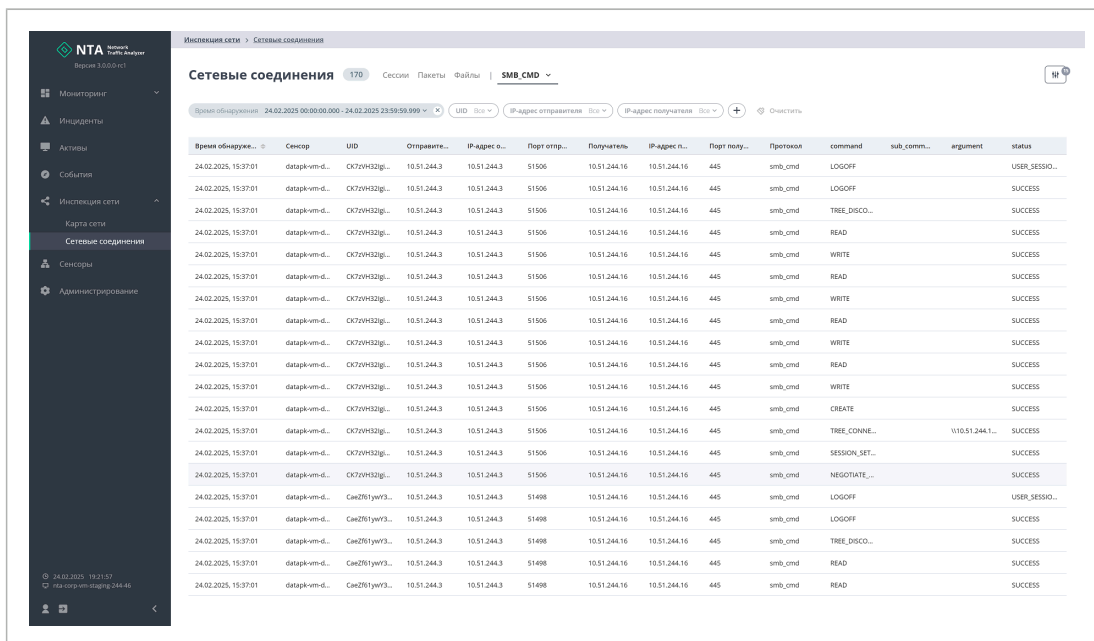
Рис. 187. Вкладка «DNS» на странице «Сетевые соединения»

См. также

Туннелирование DNS

9.3.1.5.2.6. SMB_CMD

Вкладка из группы вкладок **Протоколы** на странице **Сетевые соединения** — для мониторинга пакетов SMB_CMD, обнаруживаемых UDV NTA в рамках сессий.

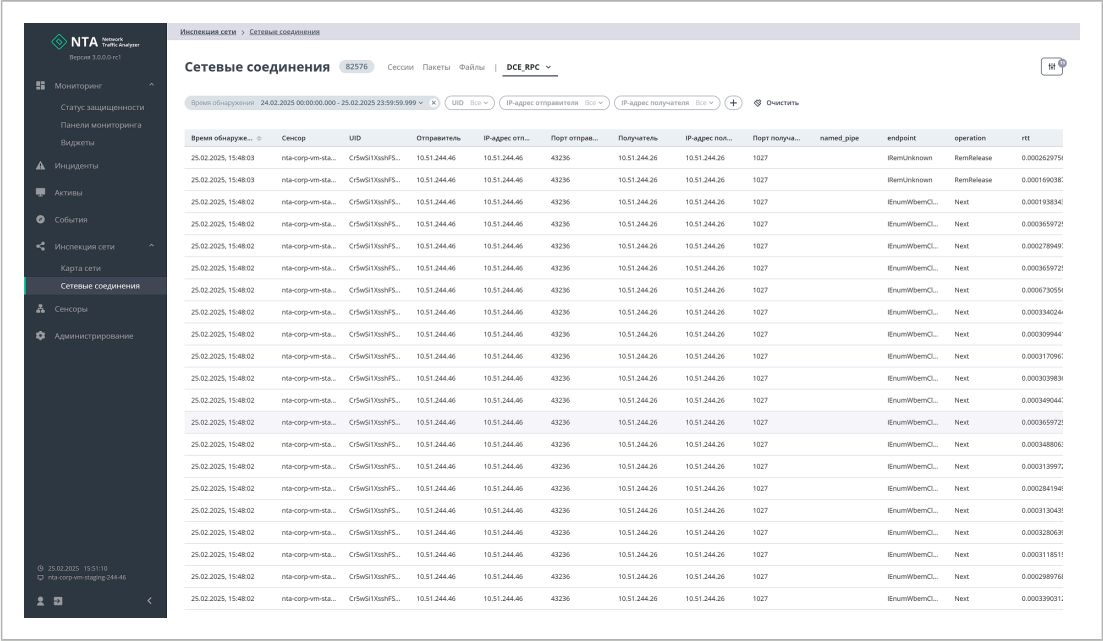


Время обнаружен...	Сенсор	UID	Отправител...	IP-адрес п...	Порт отправ...	Получатель	IP-адрес п...	Порт полу...	Протокол	command	sub_comm...	argument	status
24.02.2025, 15:37:01	data-pk-vim-d...	CK7vH52jgi...	10.51.244.3	10.51.244.3	51506	10.51.244.16	10.51.244.16	445	smb_cmd	LOGOFF			USER_SESSIO...
24.02.2025, 15:37:01	data-pk-vim-d...	CK7vH52jgi...	10.51.244.3	10.51.244.3	51506	10.51.244.16	10.51.244.16	445	smb_cmd	LOGOFF			SUCCESS
24.02.2025, 15:37:01	data-pk-vim-d...	CK7vH52jgi...	10.51.244.3	10.51.244.3	51506	10.51.244.16	10.51.244.16	445	smb_cmd	TREE_DISCO...			SUCCESS
24.02.2025, 15:37:01	data-pk-vim-d...	CK7vH52jgi...	10.51.244.3	10.51.244.3	51506	10.51.244.16	10.51.244.16	445	smb_cmd	READ			SUCCESS
24.02.2025, 15:37:01	data-pk-vim-d...	CK7vH52jgi...	10.51.244.3	10.51.244.3	51506	10.51.244.16	10.51.244.16	445	smb_cmd	WRITE			SUCCESS
24.02.2025, 15:37:01	data-pk-vim-d...	CK7vH52jgi...	10.51.244.3	10.51.244.3	51506	10.51.244.16	10.51.244.16	445	smb_cmd	READ			SUCCESS
24.02.2025, 15:37:01	data-pk-vim-d...	CK7vH52jgi...	10.51.244.3	10.51.244.3	51506	10.51.244.16	10.51.244.16	445	smb_cmd	WRITE			SUCCESS
24.02.2025, 15:37:01	data-pk-vim-d...	CK7vH52jgi...	10.51.244.3	10.51.244.3	51506	10.51.244.16	10.51.244.16	445	smb_cmd	WRITE			SUCCESS
24.02.2025, 15:37:01	data-pk-vim-d...	CK7vH52jgi...	10.51.244.3	10.51.244.3	51506	10.51.244.16	10.51.244.16	445	smb_cmd	READ			SUCCESS
24.02.2025, 15:37:01	data-pk-vim-d...	CK7vH52jgi...	10.51.244.3	10.51.244.3	51506	10.51.244.16	10.51.244.16	445	smb_cmd	WRITE			SUCCESS
24.02.2025, 15:37:01	data-pk-vim-d...	CK7vH52jgi...	10.51.244.3	10.51.244.3	51506	10.51.244.16	10.51.244.16	445	smb_cmd	WRITE			SUCCESS
24.02.2025, 15:37:01	data-pk-vim-d...	CK7vH52jgi...	10.51.244.3	10.51.244.3	51506	10.51.244.16	10.51.244.16	445	smb_cmd	CREATE			SUCCESS
24.02.2025, 15:37:01	data-pk-vim-d...	CK7vH52jgi...	10.51.244.3	10.51.244.3	51506	10.51.244.16	10.51.244.16	445	smb_cmd	TREE_CONN...		\\10.51.244.1...	SUCCESS
24.02.2025, 15:37:01	data-pk-vim-d...	CK7vH52jgi...	10.51.244.3	10.51.244.3	51506	10.51.244.16	10.51.244.16	445	smb_cmd	SESSION_SE...			SUCCESS
24.02.2025, 15:37:01	data-pk-vim-d...	CK7vH52jgi...	10.51.244.3	10.51.244.3	51506	10.51.244.16	10.51.244.16	445	smb_cmd	NEGOTIATE...			SUCCESS
24.02.2025, 15:37:01	data-pk-vim-d...	Cae2R1yWY3...	10.51.244.3	10.51.244.3	51498	10.51.244.16	10.51.244.16	445	smb_cmd	LOGOFF			USER_SESSIO...
24.02.2025, 15:37:01	data-pk-vim-d...	Cae2R1yWY3...	10.51.244.3	10.51.244.3	51498	10.51.244.16	10.51.244.16	445	smb_cmd	LOGOFF			SUCCESS
24.02.2025, 15:37:01	data-pk-vim-d...	Cae2R1yWY3...	10.51.244.3	10.51.244.3	51498	10.51.244.16	10.51.244.16	445	smb_cmd	TREE_DISCO...			SUCCESS
24.02.2025, 15:37:01	data-pk-vim-d...	Cae2R1yWY3...	10.51.244.3	10.51.244.3	51498	10.51.244.16	10.51.244.16	445	smb_cmd	READ			SUCCESS
24.02.2025, 15:37:01	data-pk-vim-d...	Cae2R1yWY3...	10.51.244.3	10.51.244.3	51498	10.51.244.16	10.51.244.16	445	smb_cmd	READ			SUCCESS

Рис. 188. Вкладка «SMB_CMD» на странице «Сетевые соединения»

9.3.1.5.2.7. DCE_RPC

Вкладка из группы вкладок **Протоколы** на странице **Сетевые соединения** — для мониторинга пакетов DCE/RPC, обнаруживаемых UDV NTA в рамках сессий.

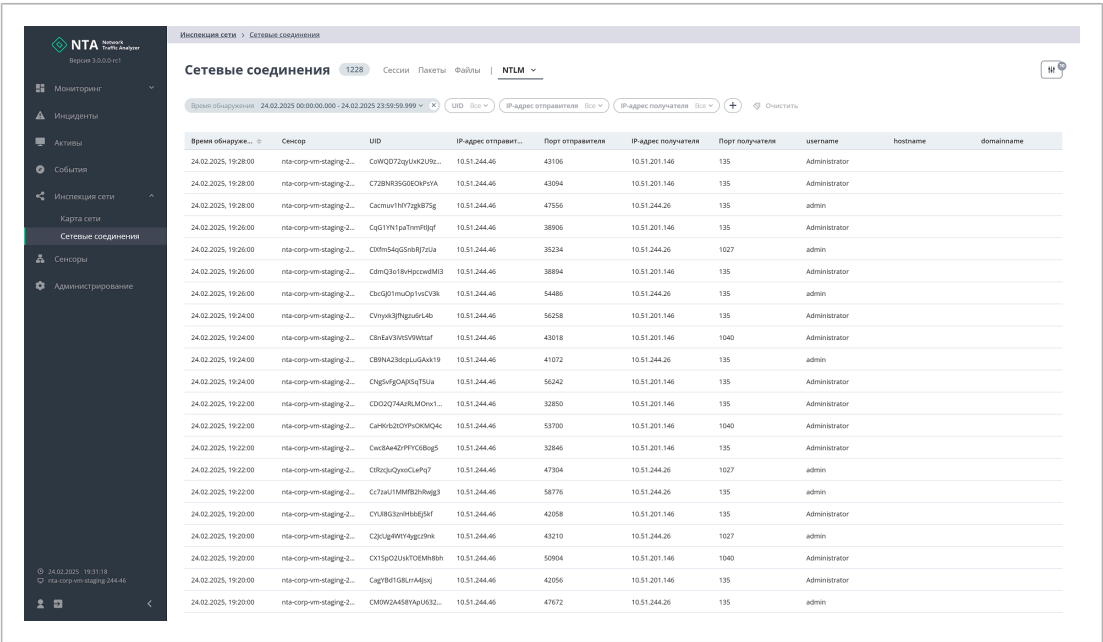


Время обнаруж...	Сенсор	UID	Отправитель	IP-адрес отп...	Порт отправ...	Получатель	IP-адрес пол...	Порт получа...	named_pipe	endpoint	operation	rtt
25.02.2025, 15:48:03	nta-corp-vm-sta...	CfSwS1XoaHPS...	10.51.244.46	10.51.244.46	43236	10.51.244.26	10.51.244.26	1027	IRemUnknown	RemRelease		0.0002629759
25.02.2025, 15:48:03	nta-corp-vm-sta...	CfSwS1XoaHPS...	10.51.244.46	10.51.244.46	43236	10.51.244.26	10.51.244.26	1027	IRemUnknown	RemRelease		0.000169038
25.02.2025, 15:48:02	nta-corp-vm-sta...	CfSwS1XoaHPS...	10.51.244.46	10.51.244.46	43236	10.51.244.26	10.51.244.26	1027	EnumWbemCl...	Next		0.000193834
25.02.2025, 15:48:02	nta-corp-vm-sta...	CfSwS1XoaHPS...	10.51.244.46	10.51.244.46	43236	10.51.244.26	10.51.244.26	1027	EnumWbemCl...	Next		0.000365972
25.02.2025, 15:48:02	nta-corp-vm-sta...	CfSwS1XoaHPS...	10.51.244.46	10.51.244.46	43236	10.51.244.26	10.51.244.26	1027	EnumWbemCl...	Next		0.000278949
25.02.2025, 15:48:02	nta-corp-vm-sta...	CfSwS1XoaHPS...	10.51.244.46	10.51.244.46	43236	10.51.244.26	10.51.244.26	1027	EnumWbemCl...	Next		0.000365972
25.02.2025, 15:48:02	nta-corp-vm-sta...	CfSwS1XoaHPS...	10.51.244.46	10.51.244.46	43236	10.51.244.26	10.51.244.26	1027	EnumWbemCl...	Next		0.000673059
25.02.2025, 15:48:02	nta-corp-vm-sta...	CfSwS1XoaHPS...	10.51.244.46	10.51.244.46	43236	10.51.244.26	10.51.244.26	1027	EnumWbemCl...	Next		0.000334024
25.02.2025, 15:48:02	nta-corp-vm-sta...	CfSwS1XoaHPS...	10.51.244.46	10.51.244.46	43236	10.51.244.26	10.51.244.26	1027	EnumWbemCl...	Next		0.000309944
25.02.2025, 15:48:02	nta-corp-vm-sta...	CfSwS1XoaHPS...	10.51.244.46	10.51.244.46	43236	10.51.244.26	10.51.244.26	1027	EnumWbemCl...	Next		0.000317096
25.02.2025, 15:48:02	nta-corp-vm-sta...	CfSwS1XoaHPS...	10.51.244.46	10.51.244.46	43236	10.51.244.26	10.51.244.26	1027	EnumWbemCl...	Next		0.000303983
25.02.2025, 15:48:02	nta-corp-vm-sta...	CfSwS1XoaHPS...	10.51.244.46	10.51.244.46	43236	10.51.244.26	10.51.244.26	1027	EnumWbemCl...	Next		0.000349044
25.02.2025, 15:48:02	nta-corp-vm-sta...	CfSwS1XoaHPS...	10.51.244.46	10.51.244.46	43236	10.51.244.26	10.51.244.26	1027	EnumWbemCl...	Next		0.000365972
25.02.2025, 15:48:02	nta-corp-vm-sta...	CfSwS1XoaHPS...	10.51.244.46	10.51.244.46	43236	10.51.244.26	10.51.244.26	1027	EnumWbemCl...	Next		0.000348806
25.02.2025, 15:48:02	nta-corp-vm-sta...	CfSwS1XoaHPS...	10.51.244.46	10.51.244.46	43236	10.51.244.26	10.51.244.26	1027	EnumWbemCl...	Next		0.000313997
25.02.2025, 15:48:02	nta-corp-vm-sta...	CfSwS1XoaHPS...	10.51.244.46	10.51.244.46	43236	10.51.244.26	10.51.244.26	1027	EnumWbemCl...	Next		0.000284194
25.02.2025, 15:48:02	nta-corp-vm-sta...	CfSwS1XoaHPS...	10.51.244.46	10.51.244.46	43236	10.51.244.26	10.51.244.26	1027	EnumWbemCl...	Next		0.000313048
25.02.2025, 15:48:02	nta-corp-vm-sta...	CfSwS1XoaHPS...	10.51.244.46	10.51.244.46	43236	10.51.244.26	10.51.244.26	1027	EnumWbemCl...	Next		0.000328063
25.02.2025, 15:48:02	nta-corp-vm-sta...	CfSwS1XoaHPS...	10.51.244.46	10.51.244.46	43236	10.51.244.26	10.51.244.26	1027	EnumWbemCl...	Next		0.000311851
25.02.2025, 15:48:02	nta-corp-vm-sta...	CfSwS1XoaHPS...	10.51.244.46	10.51.244.46	43236	10.51.244.26	10.51.244.26	1027	EnumWbemCl...	Next		0.000286974
25.02.2025, 15:48:02	nta-corp-vm-sta...	CfSwS1XoaHPS...	10.51.244.46	10.51.244.46	43236	10.51.244.26	10.51.244.26	1027	EnumWbemCl...	Next		0.000339031

Рис. 189. Вкладка «DCE_RPC» на странице «Сетевые соединения»

9.3.1.5.2.8. NTLM

Вкладка из группы вкладок **Протоколы** на странице **Сетевые соединения** — для мониторинга NTLM-пакетов, обнаруживаемых UDV NTA в рамках сессий.

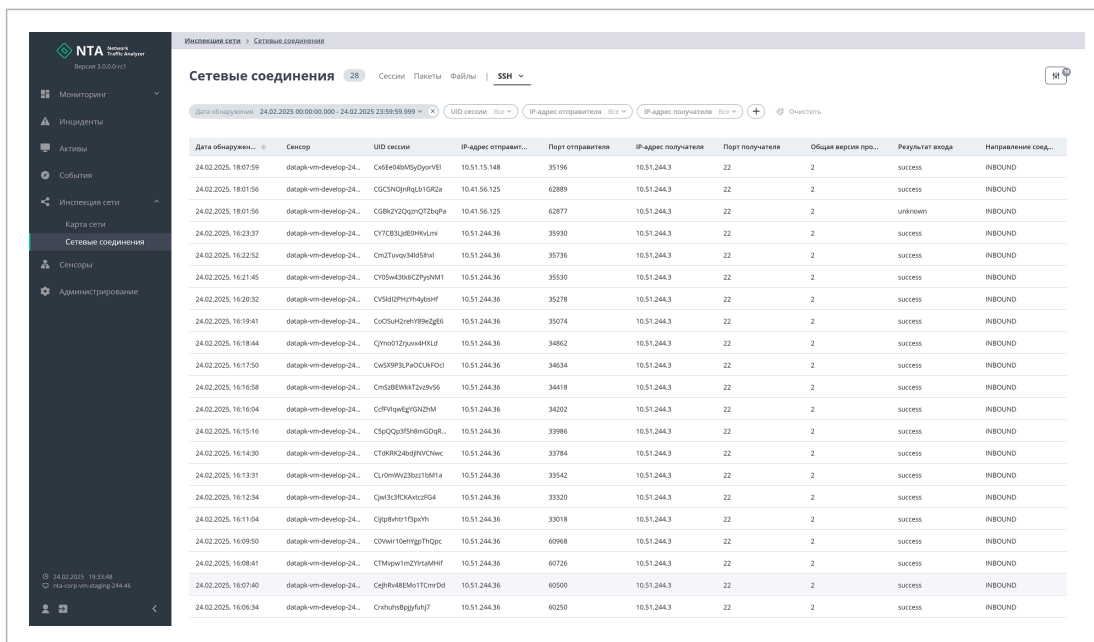


Время обнаруж...	Сенсор	UID	IP-адрес отправит...	Порт отправителя	IP-адрес получателя	Порт получателя	username	hostname	domainname
24.02.2025, 19:28:00	nta-corp-vm-staging-2...	CoWQD72qUvZU9c...	10.51.244.46	43106	10.51.201.146	135	Administrator		
24.02.2025, 19:28:00	nta-corp-vm-staging-2...	CT2BNR25S6EOP5YA	10.51.244.46	43094	10.51.201.146	135	Administrator		
24.02.2025, 19:28:00	nta-corp-vm-staging-2...	SacsmuV1N7zgIB7Sg	10.51.244.46	47556	10.51.244.26	135	admin		
24.02.2025, 19:26:00	nta-corp-vm-staging-2...	CqG1Y1N1pa1rmfHjgJ	10.51.244.46	38906	10.51.201.146	135	Administrator		
24.02.2025, 19:26:00	nta-corp-vm-staging-2...	C0fms5AgZb4hB7Jc0a	10.51.244.46	35234	10.51.244.26	1027	admin		
24.02.2025, 19:26:00	nta-corp-vm-staging-2...	CdmQ3e1f8uHqscowM3	10.51.244.46	38894	10.51.201.146	135	Administrator		
24.02.2025, 19:26:00	nta-corp-vm-staging-2...	CbcQD1msOp1ucV3k	10.51.244.46	54486	10.51.244.26	135	admin		
24.02.2025, 19:24:00	nta-corp-vm-staging-2...	CmYxk3fMgugurL4b	10.51.244.46	56258	10.51.201.146	135	Administrator		
24.02.2025, 19:24:00	nta-corp-vm-staging-2...	CbW4V3M3VWmtaf	10.51.244.46	43018	10.51.201.146	1040	Administrator		
24.02.2025, 19:24:00	nta-corp-vm-staging-2...	CBWNA23kgLuGak19	10.51.244.46	41072	10.51.244.26	135	admin		
24.02.2025, 19:24:00	nta-corp-vm-staging-2...	CHG5uG0ApQ5qTSu4	10.51.244.46	56242	10.51.201.146	135	Administrator		
24.02.2025, 19:22:00	nta-corp-vm-staging-2...	CD0OZQ74AURLMOnx1...	10.51.244.46	32850	10.51.201.146	135	Administrator		
24.02.2025, 19:22:00	nta-corp-vm-staging-2...	CaH6b2ZCPXcXKM24c	10.51.244.46	53700	10.51.201.146	1040	Administrator		
24.02.2025, 19:22:00	nta-corp-vm-staging-2...	Cac8Ae4dFPYCBug5	10.51.244.46	32846	10.51.201.146	135	Administrator		
24.02.2025, 19:22:00	nta-corp-vm-staging-2...	CRQ3u3QyocLefh7	10.51.244.46	47304	10.51.244.26	1027	admin		
24.02.2025, 19:22:00	nta-corp-vm-staging-2...	CS7ax1MMfB2hWdgg3	10.51.244.46	58776	10.51.244.26	135	admin		
24.02.2025, 19:20:00	nta-corp-vm-staging-2...	CYU8G3znHbb6Jsf	10.51.244.46	42058	10.51.201.146	135	Administrator		
24.02.2025, 19:20:00	nta-corp-vm-staging-2...	C2c3u6W7AggczHk	10.51.244.46	43210	10.51.244.26	1027	admin		
24.02.2025, 19:20:00	nta-corp-vm-staging-2...	CX1SpDQ3uATOEIM8sh	10.51.244.46	50904	10.51.201.146	1040	Administrator		
24.02.2025, 19:20:00	nta-corp-vm-staging-2...	Cag7B4fGRLAq3u	10.51.244.46	42056	10.51.201.146	135	Administrator		
24.02.2025, 19:20:00	nta-corp-vm-staging-2...	CMWQ2AS8Yk6U632...	10.51.244.46	47672	10.51.244.26	135	admin		

Рис. 190. Вкладка «NTLM» на странице «Сетевые соединения»

9.3.1.5.2.9. SSH

Вкладка из группы вкладок **Протоколы** на странице **Сетевые соединения** — для мониторинга SSH-пакетов, обнаруживаемых UDV NTA в рамках сессий.

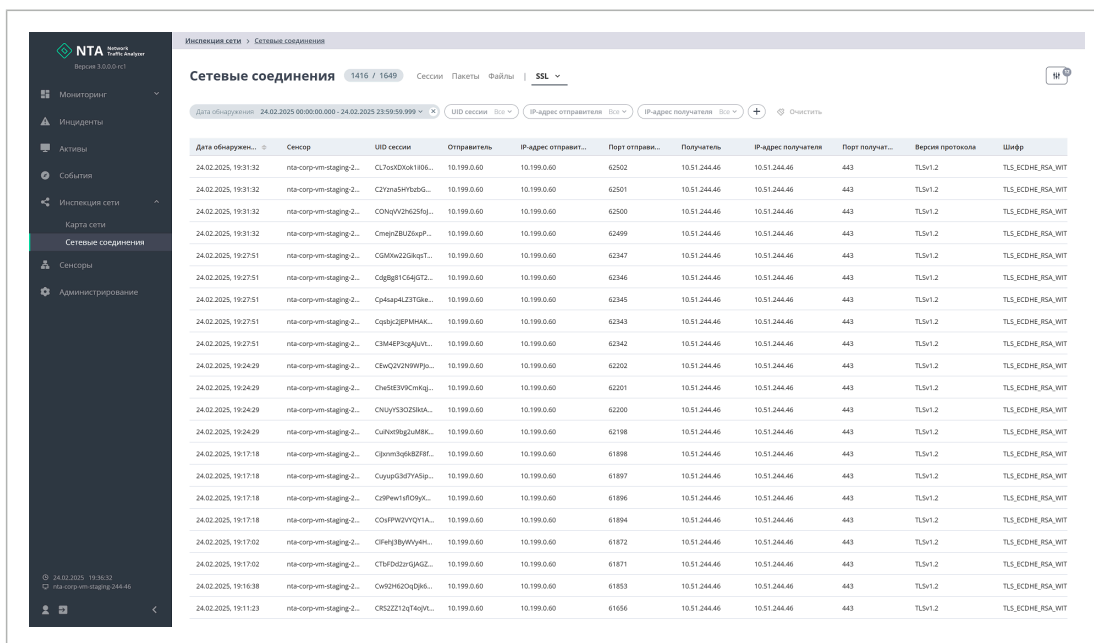


Дата обнаруж...	Сенсор	UID сессии	IP-адрес отправит...	Порт отправителя	IP-адрес получателя	Порт получателя	Общая версия про...	Результат входа	Направление соед...
24.02.2025, 18:07:59	data-lk-vm-develop-24...	CsEE64M45y0y0rV6I	10.51.15.148	35196	10.51.244.3	22	2	success	INBOUND
24.02.2025, 18:01:56	data-lk-vm-develop-24...	CGS3CQ9rkqL3tGR2a	10.41.56.125	62889	10.51.244.3	22	2	success	INBOUND
24.02.2025, 18:01:56	data-lk-vm-develop-24...	CG8kZtQ2qmQ7Z2qfa	10.41.56.125	62877	10.51.244.3	22	2	unknown	INBOUND
24.02.2025, 16:23:37	data-lk-vm-develop-24...	CYTCS3qE0DKMLtL	10.51.244.36	39930	10.51.244.3	22	2	success	INBOUND
24.02.2025, 16:22:52	data-lk-vm-develop-24...	CmZTangp3465Rnl	10.51.244.36	35736	10.51.244.3	22	2	success	INBOUND
24.02.2025, 16:21:45	data-lk-vm-develop-24...	CY5W43X6CZ7y9NM1	10.51.244.36	35530	10.51.244.3	22	2	success	INBOUND
24.02.2025, 16:20:32	data-lk-vm-develop-24...	CV5dI2P4CmThdybHf	10.51.244.36	35278	10.51.244.3	22	2	success	INBOUND
24.02.2025, 16:19:41	data-lk-vm-develop-24...	COo5H2mV89k2Z66	10.51.244.36	35074	10.51.244.3	22	2	success	INBOUND
24.02.2025, 16:18:44	data-lk-vm-develop-24...	CY7m0T2Zjwv4RtDd	10.51.244.36	34862	10.51.244.3	22	2	success	INBOUND
24.02.2025, 16:17:50	data-lk-vm-develop-24...	COv8P3LUCOUCAF0d	10.51.244.36	34634	10.51.244.3	22	2	success	INBOUND
24.02.2025, 16:16:58	data-lk-vm-develop-24...	Cm5d8WMT2v9v56	10.51.244.36	34418	10.51.244.3	22	2	success	INBOUND
24.02.2025, 16:16:04	data-lk-vm-develop-24...	CGFVh9eYGNDZHM	10.51.244.36	34202	10.51.244.3	22	2	success	INBOUND
24.02.2025, 16:15:16	data-lk-vm-develop-24...	CSpQOp3F9h8mQDqL...	10.51.244.36	33986	10.51.244.3	22	2	success	INBOUND
24.02.2025, 16:14:30	data-lk-vm-develop-24...	CT8WQ24b9fWVCwC	10.51.244.36	33784	10.51.244.3	22	2	success	INBOUND
24.02.2025, 16:13:31	data-lk-vm-develop-24...	CLUdHwZ30z10M14	10.51.244.36	33542	10.51.244.3	22	2	success	INBOUND
24.02.2025, 16:12:34	data-lk-vm-develop-24...	CM3Z3C3KzKzG4	10.51.244.36	33320	10.51.244.3	22	2	success	INBOUND
24.02.2025, 16:11:04	data-lk-vm-develop-24...	Cj9bVh8r1D3xvTh	10.51.244.36	33018	10.51.244.3	22	2	success	INBOUND
24.02.2025, 16:09:50	data-lk-vm-develop-24...	COwW10eH7gP1H9f	10.51.244.36	69968	10.51.244.3	22	2	success	INBOUND
24.02.2025, 16:08:41	data-lk-vm-develop-24...	CTMgwaTmZ3v8H9f	10.51.244.36	69726	10.51.244.3	22	2	success	INBOUND
24.02.2025, 16:07:40	data-lk-vm-develop-24...	COjHh48EMoT1CmDd	10.51.244.36	60500	10.51.244.3	22	2	success	INBOUND
24.02.2025, 16:06:34	data-lk-vm-develop-24...	COhUhs8BgJufu7	10.51.244.36	60250	10.51.244.3	22	2	success	INBOUND

Рис. 191. Вкладка «SSH» на странице «Сетевые соединения»

9.3.1.5.2.10. SSL

Вкладка из группы вкладок **Протоколы** на странице **Сетевые соединения** — для мониторинга SSL-пакетов, обнаруживаемых UDV NTA в рамках сессий.



Дата обнаруж...	Сенсор	UID сессии	Отправитель	IP-адрес отправит...	Порт отправ...	Получатель	IP-адрес получателя	Порт получат...	Версия протокола	Шифр
24.02.2025, 19:31:32	nta-corp-vm-staging-2...	CL7o2D2K6A1B96...	10.199.0.60	10.199.0.60	62502	10.51.244.46	10.51.244.46	443	TLSv1.2	TLS_ECDHE_RSA_WIT
24.02.2025, 19:31:32	nta-corp-vm-staging-2...	CZ7m3a5Hb6b5...	10.199.0.60	10.199.0.60	62501	10.51.244.46	10.51.244.46	443	TLSv1.2	TLS_ECDHE_RSA_WIT
24.02.2025, 19:31:32	nta-corp-vm-staging-2...	COHqV2H625faj...	10.199.0.60	10.199.0.60	62500	10.51.244.46	10.51.244.46	443	TLSv1.2	TLS_ECDHE_RSA_WIT
24.02.2025, 19:31:32	nta-corp-vm-staging-2...	CMej8U2U59pP...	10.199.0.60	10.199.0.60	62499	10.51.244.46	10.51.244.46	443	TLSv1.2	TLS_ECDHE_RSA_WIT
24.02.2025, 19:27:51	nta-corp-vm-staging-2...	CGMw2G2GkptT...	10.199.0.60	10.199.0.60	62347	10.51.244.46	10.51.244.46	443	TLSv1.2	TLS_ECDHE_RSA_WIT
24.02.2025, 19:27:51	nta-corp-vm-staging-2...	COjB8b1C64G7Z...	10.199.0.60	10.199.0.60	62346	10.51.244.46	10.51.244.46	443	TLSv1.2	TLS_ECDHE_RSA_WIT
24.02.2025, 19:27:51	nta-corp-vm-staging-2...	CO4ap4L2Z7Gle...	10.199.0.60	10.199.0.60	62345	10.51.244.46	10.51.244.46	443	TLSv1.2	TLS_ECDHE_RSA_WIT
24.02.2025, 19:27:51	nta-corp-vm-staging-2...	COjB3j2F8HAK...	10.199.0.60	10.199.0.60	62343	10.51.244.46	10.51.244.46	443	TLSv1.2	TLS_ECDHE_RSA_WIT
24.02.2025, 19:27:51	nta-corp-vm-staging-2...	CSM4F3Z8gVhV...	10.199.0.60	10.199.0.60	62342	10.51.244.46	10.51.244.46	443	TLSv1.2	TLS_ECDHE_RSA_WIT
24.02.2025, 19:24:29	nta-corp-vm-staging-2...	CEWQ2V2N9W9p...	10.199.0.60	10.199.0.60	62202	10.51.244.46	10.51.244.46	443	TLSv1.2	TLS_ECDHE_RSA_WIT
24.02.2025, 19:24:29	nta-corp-vm-staging-2...	On58E3V9Cmkq...	10.199.0.60	10.199.0.60	62201	10.51.244.46	10.51.244.46	443	TLSv1.2	TLS_ECDHE_RSA_WIT
24.02.2025, 19:24:29	nta-corp-vm-staging-2...	COuYt53C25BKA...	10.199.0.60	10.199.0.60	62200	10.51.244.46	10.51.244.46	443	TLSv1.2	TLS_ECDHE_RSA_WIT
24.02.2025, 19:24:29	nta-corp-vm-staging-2...	COuN9R9g2uMRK...	10.199.0.60	10.199.0.60	62198	10.51.244.46	10.51.244.46	443	TLSv1.2	TLS_ECDHE_RSA_WIT
24.02.2025, 19:17:18	nta-corp-vm-staging-2...	COjvmb3g8B2F8H...	10.199.0.60	10.199.0.60	61898	10.51.244.46	10.51.244.46	443	TLSv1.2	TLS_ECDHE_RSA_WIT
24.02.2025, 19:17:18	nta-corp-vm-staging-2...	COjvmb3g8B2F8H...	10.199.0.60	10.199.0.60	61897	10.51.244.46	10.51.244.46	443	TLSv1.2	TLS_ECDHE_RSA_WIT
24.02.2025, 19:17:18	nta-corp-vm-staging-2...	COjvmb3g8B2F8H...	10.199.0.60	10.199.0.60	61896	10.51.244.46	10.51.244.46	443	TLSv1.2	TLS_ECDHE_RSA_WIT
24.02.2025, 19:17:18	nta-corp-vm-staging-2...	COjvmb3g8B2F8H...	10.199.0.60	10.199.0.60	61894	10.51.244.46	10.51.244.46	443	TLSv1.2	TLS_ECDHE_RSA_WIT
24.02.2025, 19:17:02	nta-corp-vm-staging-2...	COjvmb3g8B2F8H...	10.199.0.60	10.199.0.60	61872	10.51.244.46	10.51.244.46	443	TLSv1.2	TLS_ECDHE_RSA_WIT
24.02.2025, 19:17:02	nta-corp-vm-staging-2...	COjvmb3g8B2F8H...	10.199.0.60	10.199.0.60	61871	10.51.244.46	10.51.244.46	443	TLSv1.2	TLS_ECDHE_RSA_WIT
24.02.2025, 19:16:38	nta-corp-vm-staging-2...	COjvmb3g8B2F8H...	10.199.0.60	10.199.0.60	61853	10.51.244.46	10.51.244.46	443	TLSv1.2	TLS_ECDHE_RSA_WIT
24.02.2025, 19:11:23	nta-corp-vm-staging-2...	COjvmb3g8B2F8H...	10.199.0.60	10.199.0.60	61656	10.51.244.46	10.51.244.46	443	TLSv1.2	TLS_ECDHE_RSA_WIT

Рис. 192. Вкладка «SSL» на странице «Сетевые соединения»

9.3.1.5.2.11. Kerberos

Вкладка из группы вкладок **Протоколы** на странице **Сетевые соединения** — для мониторинга Kerberos-пакетов, обнаруживаемых UDV NTA в рамках сессий.

NTA

интерфейс

NTA

версия 3.0.0.0

Мониторинг

Инциденты

Активы

События

Инспекция сети

Карта сети

Сетевые соединения

Сенсоры

Администрирование

27.02.2025 16:17:32

nta-complex-startup-244-46

Инспекция сети

Сетевые соединения

Сетевые соединения

16

Сессии

Пакеты

Файлы

Kerberos

Время обнаружения

27.02.2025 00:00:00.000 - 27.02.2025 23:59:59.999

UID

IP-адрес отправителя

IP-адрес получателя

Очистить

Время обнаружения	Сенсор	UID	Отправитель	IP-адрес отправителя	Порт отправителя	Получатель	IP-адрес получателя	Порт получателя
27.02.2025, 16:02:24	datapik-vm-develop-15-100	CpyR9K2wVhZpzyh65	10.1.12.2	10.1.12.2	1096	10.5.3.1	10.5.3.1	88
27.02.2025, 16:02:23	datapik-vm-develop-15-100	CGV9v8eCqf969028	10.1.12.2	10.1.12.2	1092	10.5.3.1	10.5.3.1	88
27.02.2025, 16:02:23	datapik-vm-develop-15-100	C8uZ84ysCwDVG4E8	10.1.12.2	10.1.12.2	1090	10.5.3.1	10.5.3.1	88
27.02.2025, 16:02:23	datapik-vm-develop-15-100	C32BphGgRc4t1fPg	10.1.12.2	10.1.12.2	1089	10.5.3.1	10.5.3.1	88
27.02.2025, 16:02:23	datapik-vm-develop-15-100	OM4u84ywlU925YcGb	10.1.12.2	10.1.12.2	1088	10.5.3.1	10.5.3.1	88
27.02.2025, 16:02:22	datapik-vm-develop-15-100	CM4PES37WnBfPh002	10.1.12.2	10.1.12.2	1084	10.5.3.1	10.5.3.1	88
27.02.2025, 16:02:22	datapik-vm-develop-15-100	CEINX2T1x1a5e7H94e	10.1.12.2	10.1.12.2	1083	10.5.3.1	10.5.3.1	88
27.02.2025, 16:02:21	datapik-vm-develop-15-100	Cv4H9VPMjE9Hub	10.1.12.2	10.1.12.2	1076	10.5.3.1	10.5.3.1	88
27.02.2025, 16:02:21	datapik-vm-develop-15-100	CwwfLOIPRYNTAV3	10.1.12.2	10.1.12.2	1074	10.5.3.1	10.5.3.1	88
27.02.2025, 16:02:21	datapik-vm-develop-15-100	CO18TTFvHfSQz5Zn7	10.1.12.2	10.1.12.2	1069	10.5.3.1	10.5.3.1	88
27.02.2025, 16:02:21	datapik-vm-develop-15-100	CT4WZ54kCH85dXnd	10.1.12.2	10.1.12.2	1068	10.5.3.1	10.5.3.1	88
27.02.2025, 16:02:21	datapik-vm-develop-15-100	C3n5RZ1pbmw7TV4u4u	10.1.12.2	10.1.12.2	1067	10.5.3.1	10.5.3.1	88
27.02.2025, 16:02:21	datapik-vm-develop-15-100	CS20m69PMMYkury2	10.1.12.2	10.1.12.2	1065	10.5.3.1	10.5.3.1	88
27.02.2025, 16:02:20	datapik-vm-develop-15-100	CT4hZ3M5pK9j9p8b	10.1.12.2	10.1.12.2	1061	10.5.3.1	10.5.3.1	88
27.02.2025, 16:02:20	datapik-vm-develop-15-100	CwIDQW55SUA7mf	10.1.12.2	10.1.12.2	1060	10.5.3.1	10.5.3.1	88
27.02.2025, 16:02:20	datapik-vm-develop-15-100	CS6j41VY9u4U4U6	10.1.12.2	10.1.12.2	1059	10.5.3.1	10.5.3.1	88

Рис. 193. Вкладка «Kerberos» на странице «Сетевые соединения»

9.3.1.5.2.12. Modbus

Вкладка из группы вкладок **Протоколы** на странице **Сетевые соединения** — для мониторинга Modbus-пакетов, обнаруживаемых UDV NTA в рамках сессий.

NTA

интерфейс

NTA

версия 3.0.0.0

Мониторинг

Инциденты

Активы

События

Инспекция сети

Карта сети

Сетевые соединения

Сенсоры

Администрирование

24.02.2025 19:36:32

nta-complex-startup-244-46

Инспекция сети

Сетевые соединения

Сетевые соединения

6

Сессии

Пакеты

Файлы

Modbus

Время обнаружения

24.02.2025 00:00:00.000 - 24.02.2025 23:59:59.999

UID

IP-адрес отправителя

IP-адрес получателя

Очистить

Время обнаружения	Сенсор	UID	Отправитель	IP-адрес отправителя	Порт отправителя	Получатель	IP-адрес получателя	Порт получателя	function
24.02.2025, 15:55:25	datapik-vm-develop-24...	C6vWQ24P92LdLM7	10.51.244.3	10.51.244.3	54142	10.51.202.28	10.51.202.28	502	unknown-90
24.02.2025, 15:37:02	datapik-vm-develop-24...	CS4uXyZme7P91F1	10.51.244.3	10.51.244.3	45726	10.51.202.28	10.51.202.28	502	unknown-90
24.02.2025, 15:37:02	datapik-vm-develop-24...	CaDAEO3HvngVhWek	10.51.244.3	10.51.244.3	45710	10.51.202.28	10.51.202.28	502	unknown-90
24.02.2025, 15:37:01	datapik-vm-develop-24...	ChZkx6fC4khdg1De	10.51.244.3	10.51.244.3	45708	10.51.202.28	10.51.202.28	502	unknown-90
24.02.2025, 15:37:01	datapik-vm-develop-24...	CQE1YCUgP7Ap8R	10.51.244.3	10.51.244.3	45696	10.51.202.28	10.51.202.28	502	unknown-90
24.02.2025, 15:36:55	datapik-vm-develop-24...	CRHQ6A3y4KZQ5y4u	10.51.244.3	10.51.244.3	45737	10.51.201.138	10.51.201.138	502	READ_HOLDING_REGI...

Рис. 194. Вкладка «Modbus» на странице «Сетевые соединения»

9.3.1.5.2.13. RDP

Вкладка из группы вкладок **Протоколы** на странице **Сетевые соединения** — для мониторинга RDP-пакетов, обнаруживаемых UDV NTA в рамках сессий.

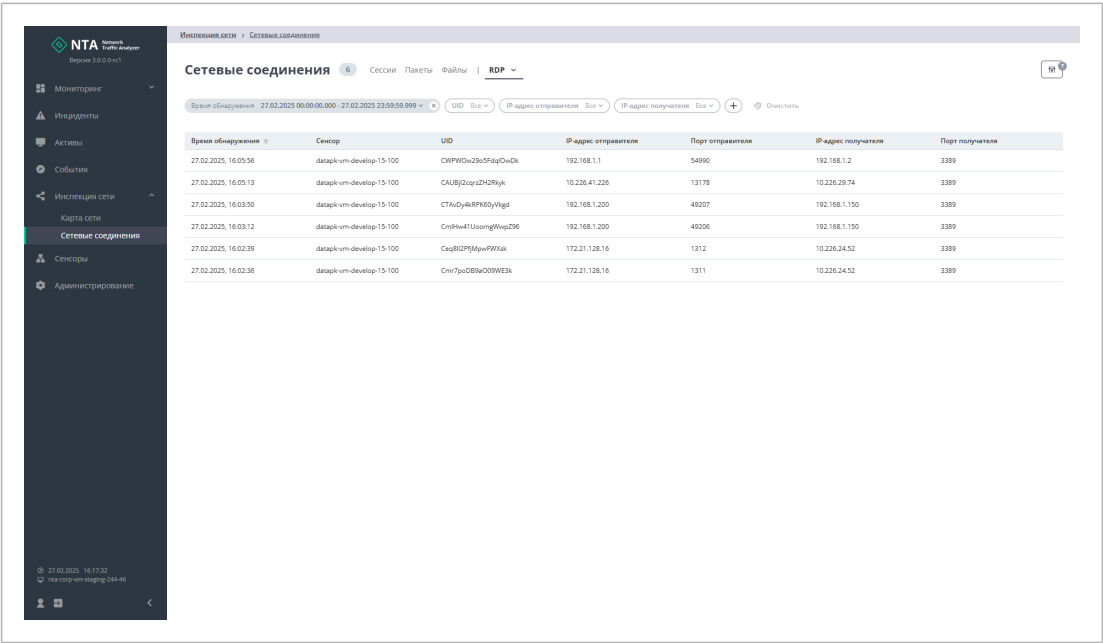


Рис. 195. Вкладка «RDP» на странице «Сетевые соединения»

9.3.1.5.2.14. SMTP

Вкладка из группы вкладок **Протоколы** на странице **Сетевые соединения** — для мониторинга SMTP-пакетов, обнаруживаемых UDV NTA в рамках сессий.

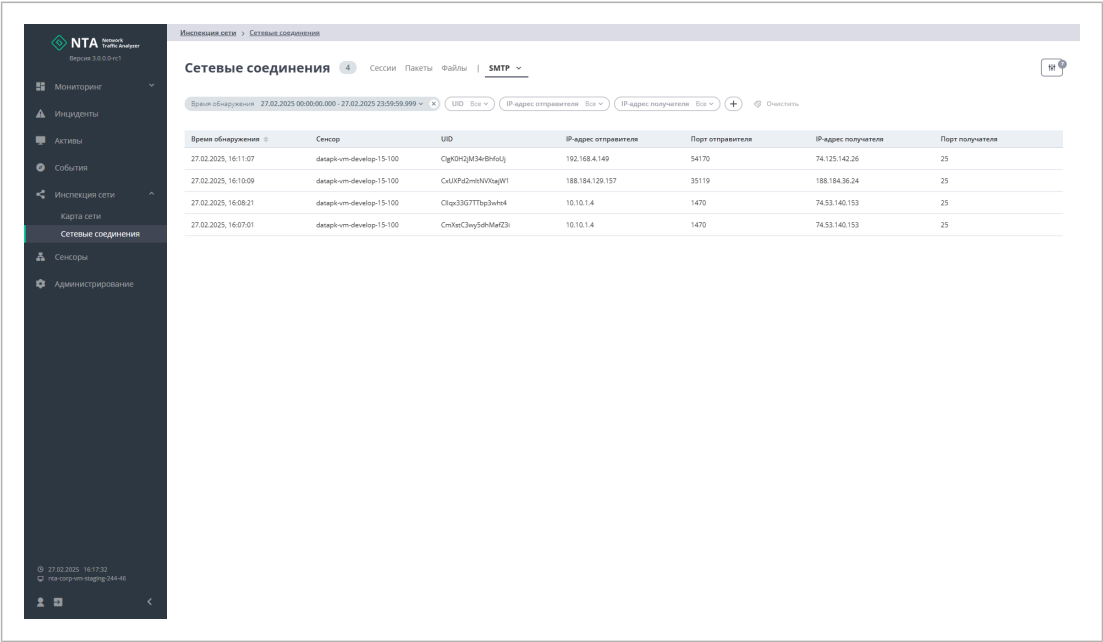


Рис. 196. Вкладка «SMTP» на странице «Сетевые соединения»

9.3.1.5.2.15. OPC UA

Вкладка из группы вкладок **Протоколы** на странице **Сетевые соединения** — для мониторинга пакетов OPC UA, обнаруживаемых UDV NTA в рамках сессий.

- Основные настройки
- События и инциденты
- Пользователи
- Сигнатурный анализ
- Настройка активов

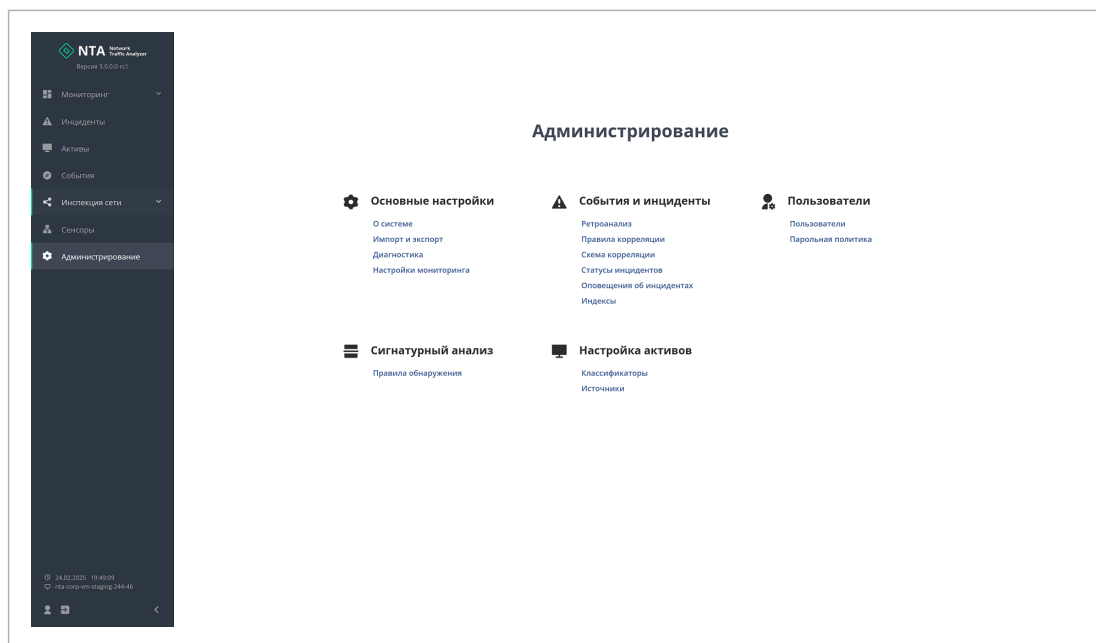


Рис. 199. Страница «Администрирование»

9.3.1.7.1. Основные настройки

9.3.1.7.1.1. 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.

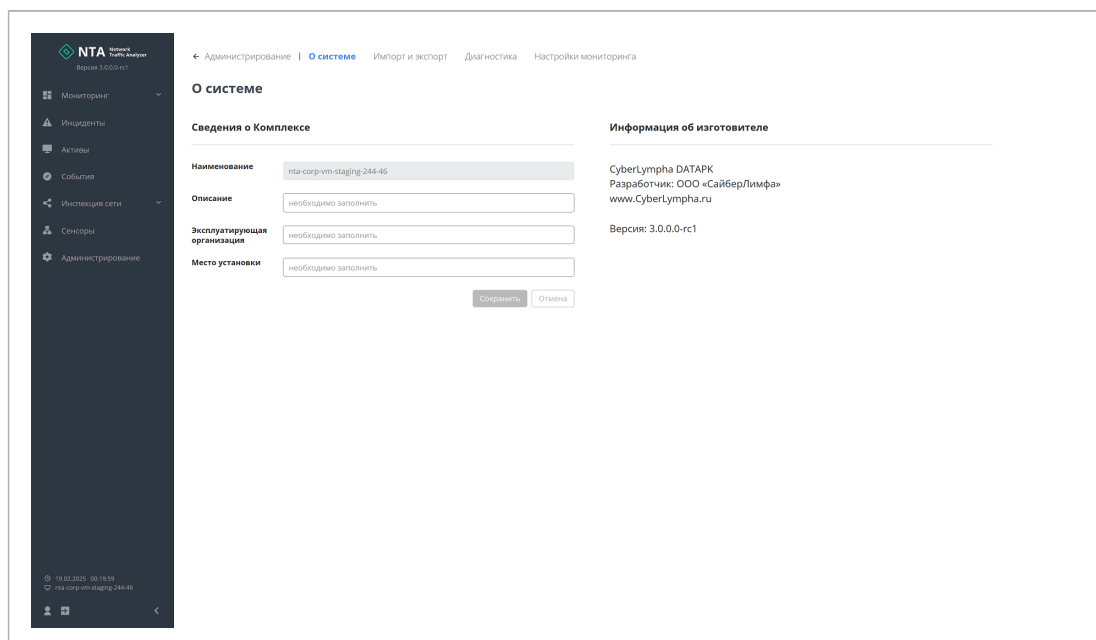


Рис. 200. Страница «О системе»

См. также

[Изменение сведений о Комплексе и сенсорах](#)

9.3.1.7.1.2. Импорт и экспорт

Страница, где можно экспортировать и импортировать справочники.



Подсказка:

Доступен импорт справочников размером до 145 МБ.

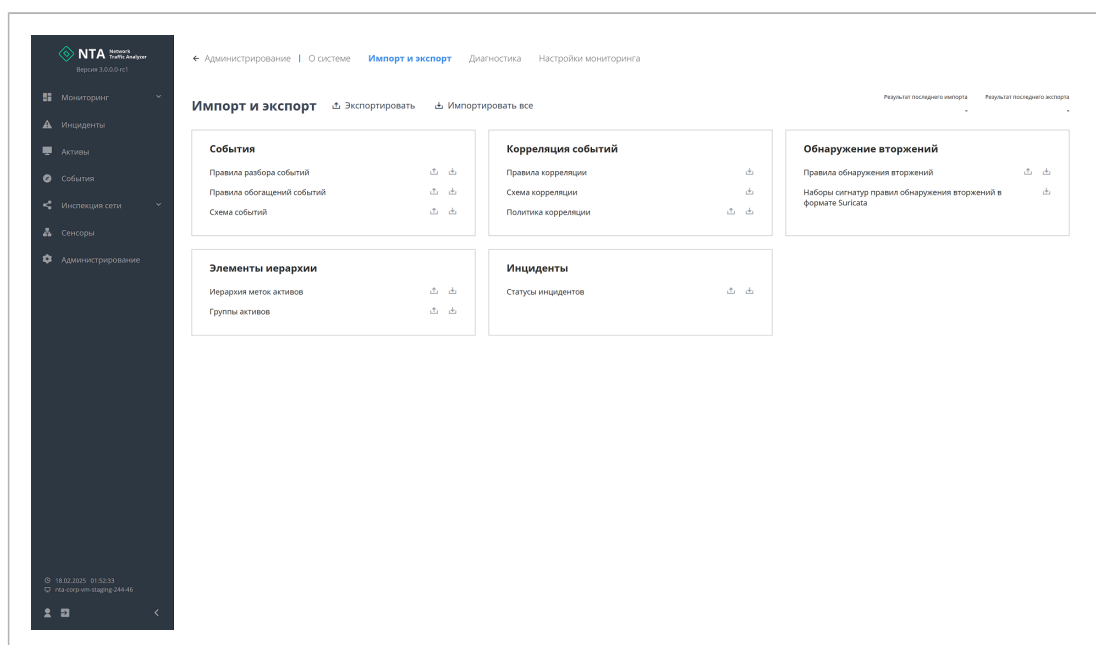


Рис. 201. Страница «Импорт и экспорт»

См. также

[Импорт правил корреляции](#)

[Экспорт и импорт классификаторов](#)

[Импорт меток](#)

[Импорт правил обнаружения вторжений в формате *.rules](#)

[Импорт источников событий](#)

[Экспорт источников событий](#)

[Импорт правил обогащений событий](#)

[Экспорт схемы событий](#)

[Экспорт правил службы обнаружения вторжений](#)

[Экспорт правил разбора событий](#)

[Экспорт правил обогащения событий](#)

[Экспорт меток](#)

[Импорт правил обнаружения вторжений в формате *.json](#)

[Импорт схемы событий](#)

[Импорт правил разбора событий](#)

9.3.1.7.1.3. 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.

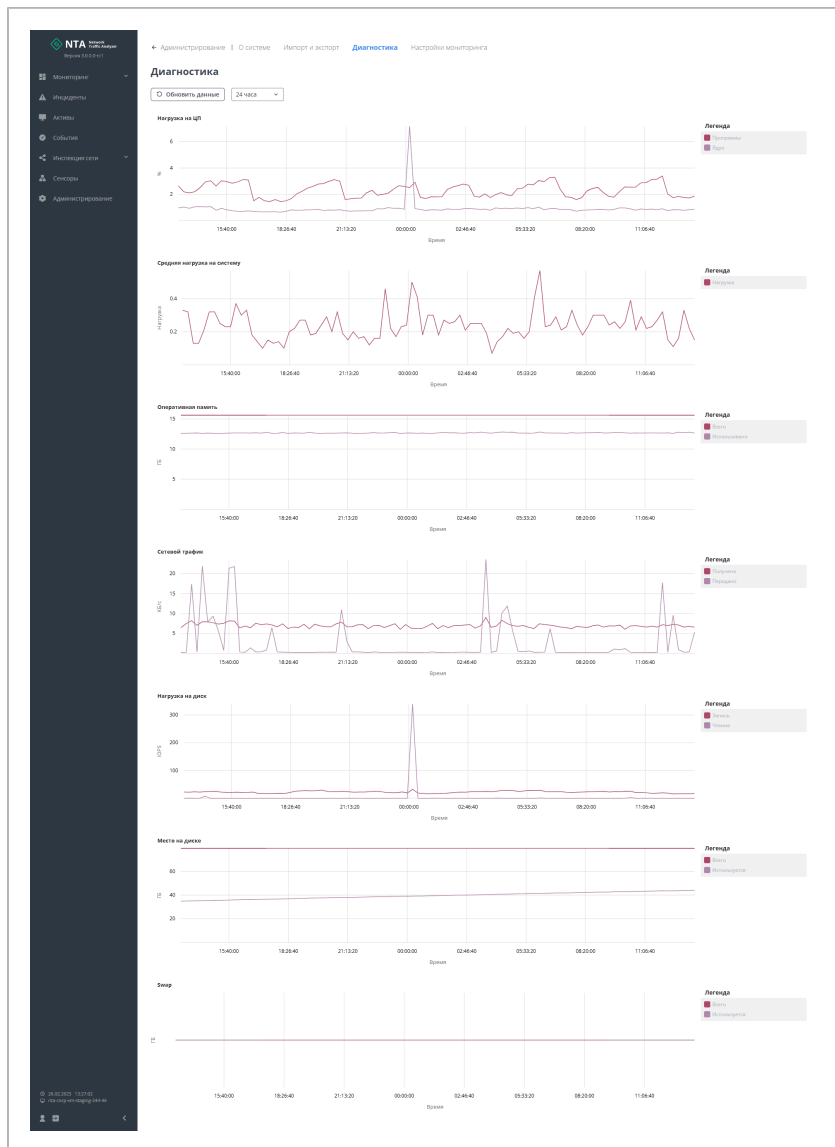


Рис. 202. Страница «Диагностика»

См. также

[Диагностика состояния системы Комплекса](#)

9.3.1.7.1.4. Настройки мониторинга

Подраздел администрирования основных настроек, в котором можно настраивать шаблоны индекса, осуществлять экспорт и импорт, настраивать отображение в подразделах мониторинга.

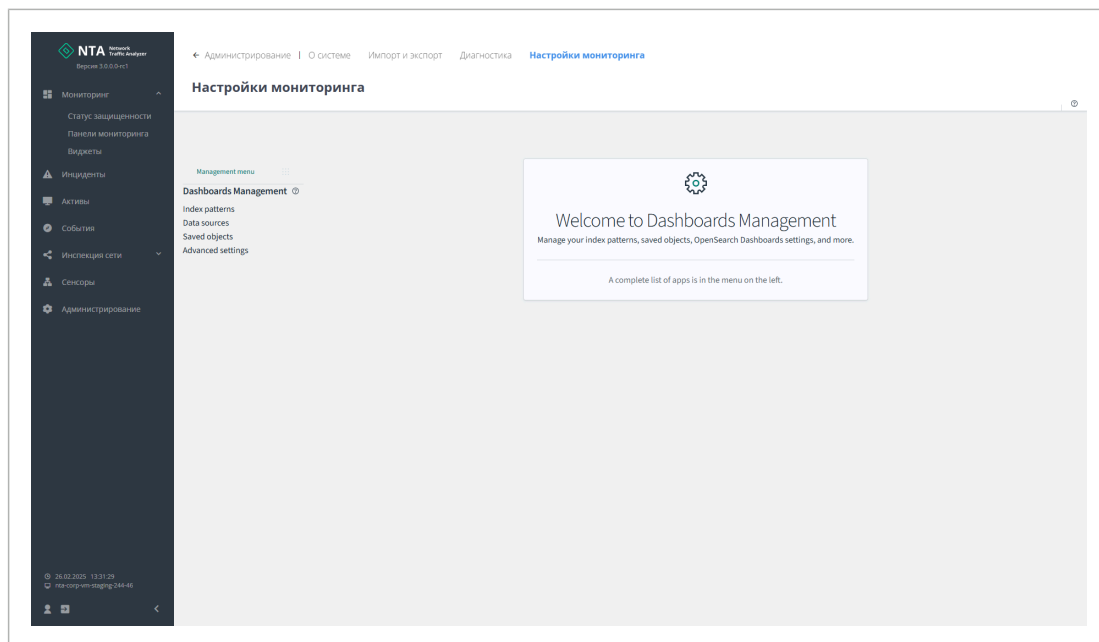


Рис. 203. Страница «Настройки мониторинга»

См. также

[Настройка пользовательских правил нормализации событий](#)

[Настройка форматирования чисел и дат в разделе «Мониторинг»](#)

[Экспорт и импорт объектов раздела «Мониторинг»](#)

9.3.1.7.2. События и инциденты

Пункт раздела **Администрирование**, содержащий подразделы **Ретроанализ**, **Правила корреляции**, **Схема корреляции**, **Статусы инцидентов**, **Оповещения об инцидентах** и **Индексы**.

См. также

[Инциденты](#)

[Статусы инцидентов](#)

[Правила корреляции](#)

[Оповещения об инцидентах](#)

[Схема корреляции](#)

[Ретроанализ](#)

9.3.1.7.2.1. Ретроанализ

Страница, где можно запускать, перезапускать и удалять ретроспективные проверки.

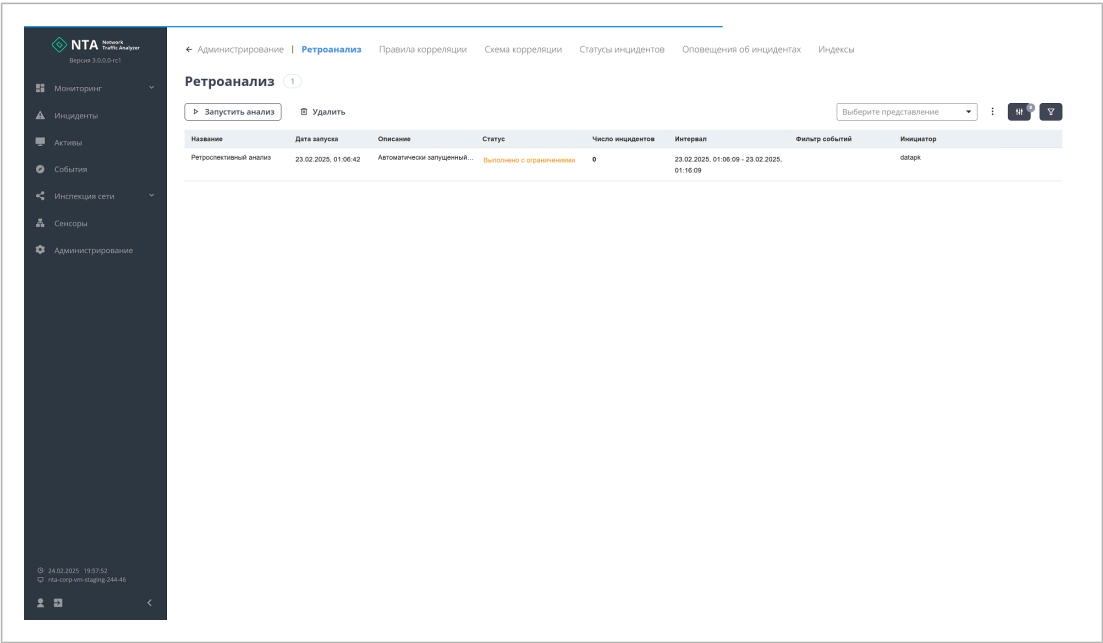


Рис. 204. Страница «Ретроанализ»

См. также
Ретроспективный анализ событий

9.3.1.7.2.2. Правила корреляции

Подраздел настроек инцидентов, в котором можно управлять службой корреляции событий, создавать, редактировать, применять, удалять, активировать и деактивировать правила корреляции.

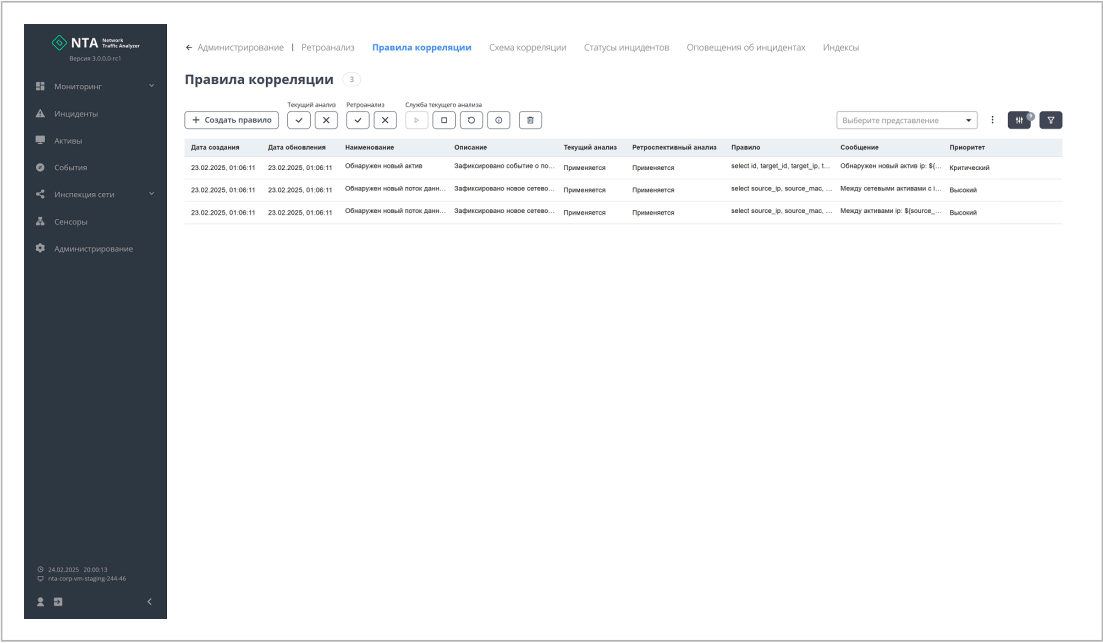


Рис. 205. Страница «Правила корреляции»

См. также
Управление правилами корреляции событий
Управление службой корреляции событий

9.3.1.7.2.3. Схема корреляции

Подраздел настроек инцидентов, в котором можно создавать, редактировать, проверять, ассоциировать с тем или иным видом анализа, удалять элементы схемы корреляции.

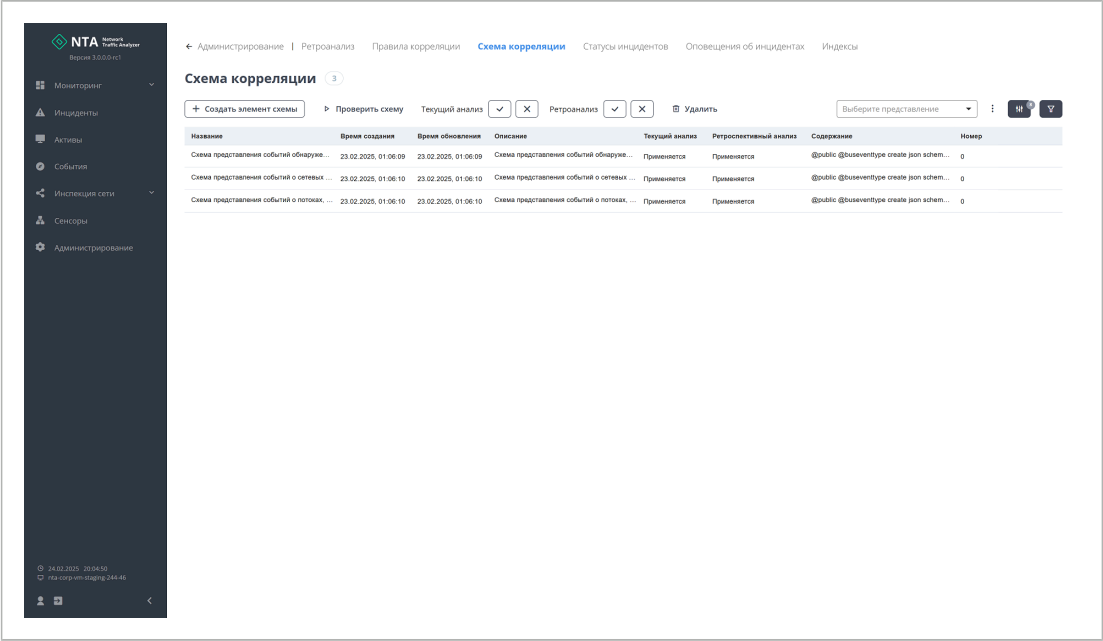


Рис. 206. Страница «Схема корреляции»

- См. также
- Анализ событий для генерации инцидентов
 - Управление схемой корреляции

9.3.1.7.2.4. Статусы инцидентов

Подраздел настроек инцидентов, содержащий доступные для редактирования статусы, которые оператор может присвоить инцидентам. Доступно создание, редактирование и удаление.

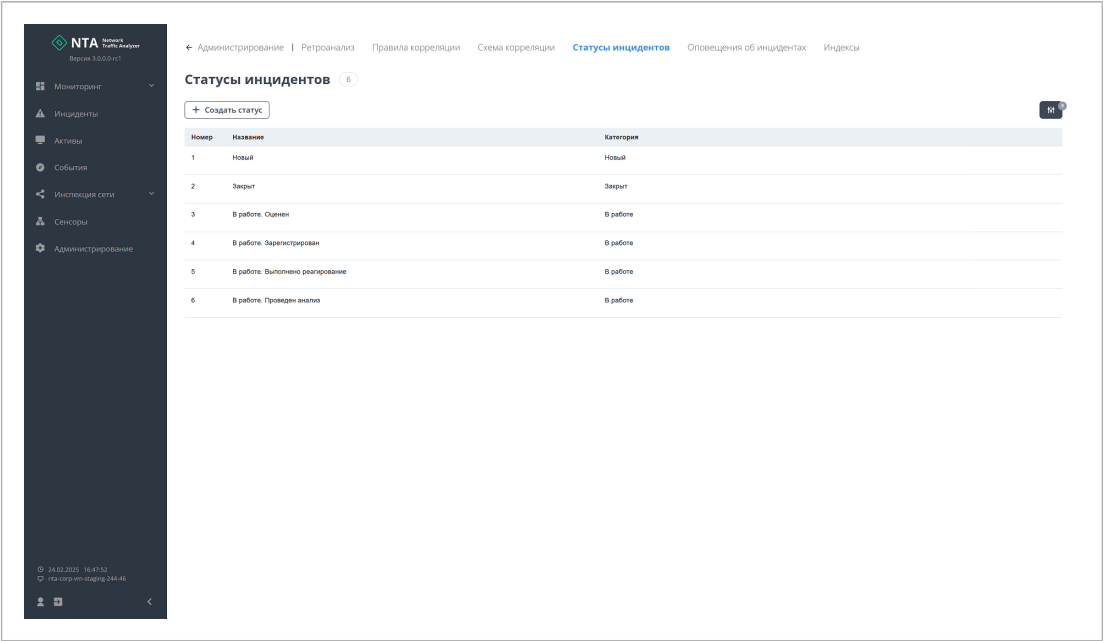


Рис. 207. Страница «Статусы инцидентов»

См. также[Управление статусами инцидентов](#)

9.3.1.7.2.5. Оповещения об инцидентах

Подраздел администрирования событий и инцидентов, в котором можно создавать, редактировать и удалять оповещения об инцидентах, а также отправлять тестовые оповещения об инцидентах.

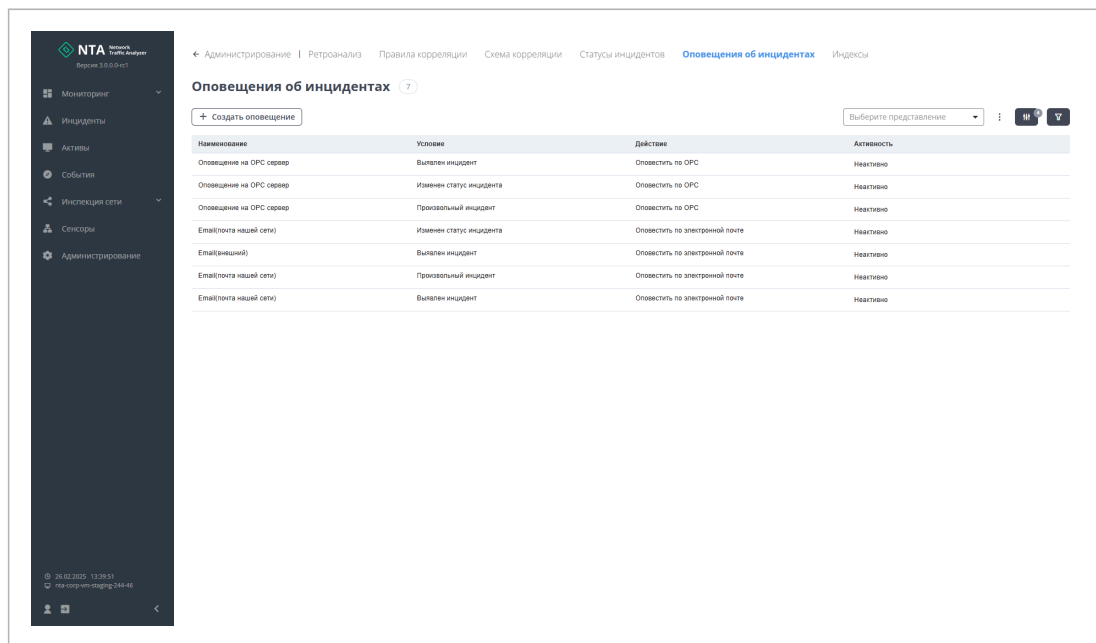


Рис. 208. Страница «Оповещения об инцидентах»

См. также[Настройка оповещений при появлении инцидентов](#)

9.3.1.7.2.6. Индексы

Подраздел администрирования событий и инцидентов, в котором можно восстанавливать, архивировать и удалять индексы событий.

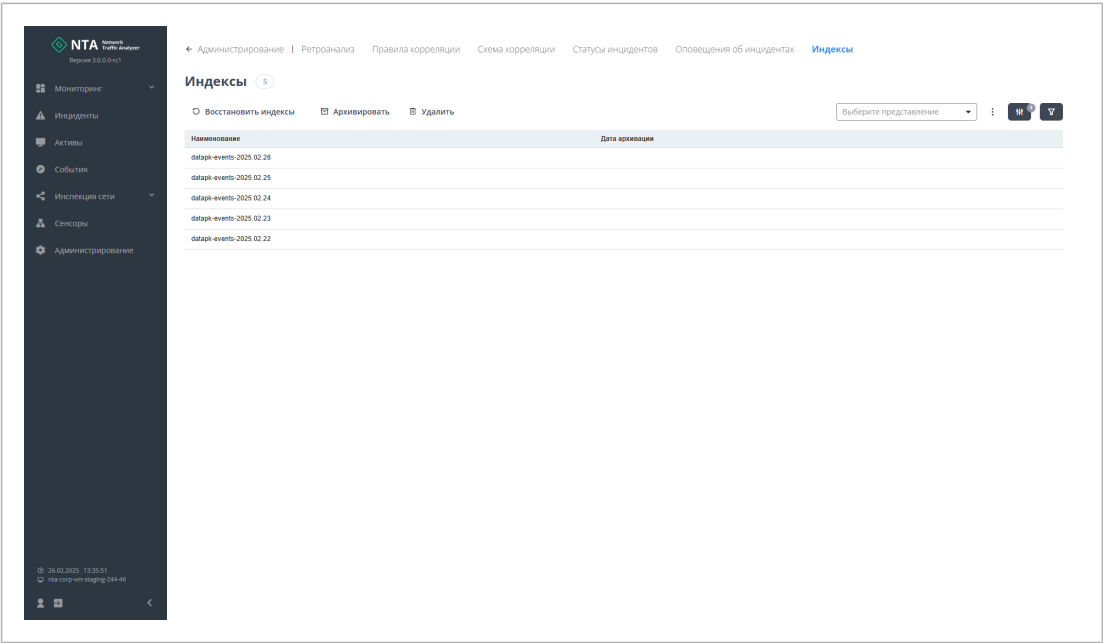


Рис. 209. Страница «Индексы»

См. также

[Выгрузка событий Комплекса в архив](#)

9.3.1.7.3. Пользователи

Подраздел администрирования, содержащий страницы [Пользователи](#) и [Парольная политика](#).

9.3.1.7.3.1. Пользователи

Подраздел администрирования Комплексом, где можно создавать, редактировать, деактивировать и активировать, удалять пользователей.

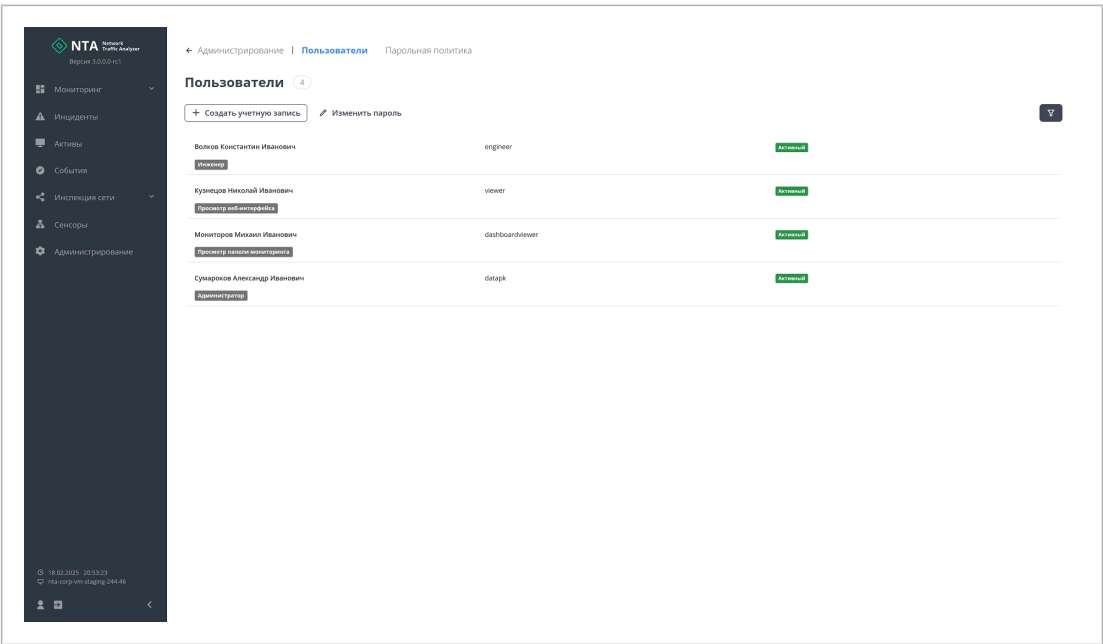


Рис. 210. Страница «Пользователи»

См. также[Создание локальной учетной записи](#)[Редактирование учетных записей пользователей](#)

9.3.1.7.3.2. Парольная политика

Подраздел настроек пользователей, где можно настраивать требования к паролям в Комплексе.

NTA Система комплексной безопасности
Версия 3.0.0.0.17

← Администрирование | Пользователи **Парольная политика**

Парольная политика

Минимальная длина пароля **0**

Минимальное количество цифровых символов

Минимальное количество заглавных букв

Минимальное количество специальных символов

Срок действия пароля, дни **0**

Длина журнала паролей **0**

Максимальное количество попыток ввода пароля **0**

Срок блокировки при превышении попыток ввода пароля УЗ, сек **0**

[Сохранить изменения](#)

18.02.2025 01:19:47
nta-complex@nta.ru 244-46

Рис. 211. Страница «Парольная политика»

См. также[Настройка парольной политики](#)

9.3.1.7.4. Сигнатурный анализ

9.3.1.7.4.1. Правила обнаружения

Страница для работы с правилами обнаружения вторжений, содержащая следующие вкладки:

- [Правила обнаружения вторжений](#);
- [Исключения](#).

См. также[Служба обнаружения вторжений](#)

9.3.1.7.5. Настройка активов

Пункт меню раздела [Администрирование](#), содержащий страницы [Классификаторы](#) и [Источники](#).

См. также

[Классификаторы](#)

[Источники](#)

9.3.1.7.5.1. Классификаторы

Подраздел настроек активов, где можно создавать, редактировать и удалять классификаторы типа **Метки**.

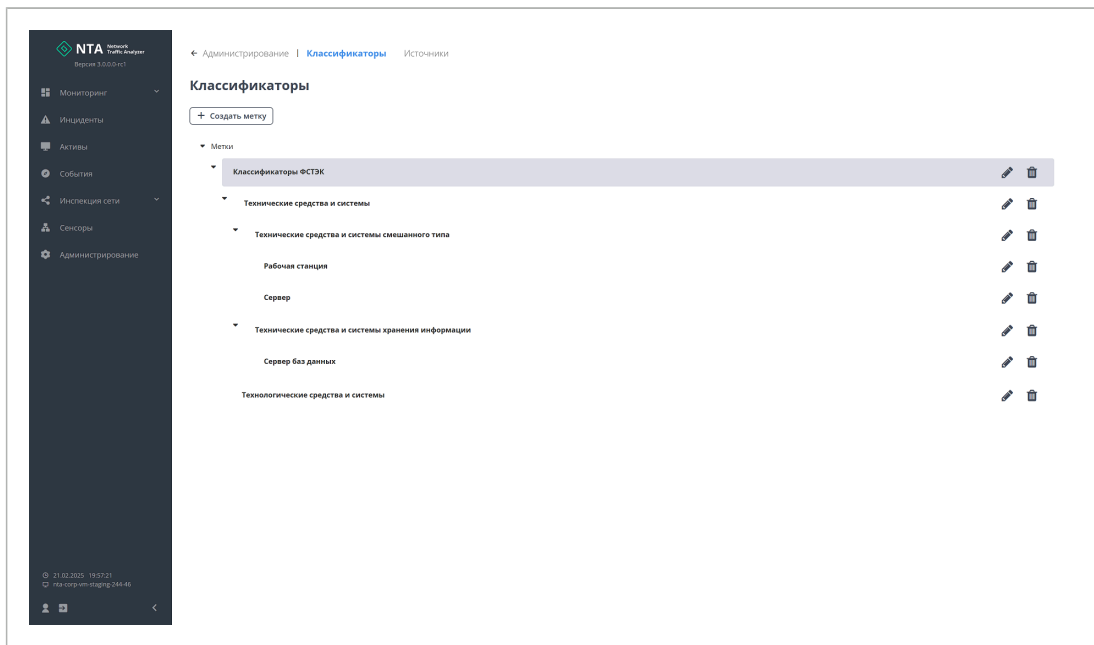


Рис. 212. Страница «Классификаторы»

См. также

[Создание метки](#)

[Редактирование и удаление классификаторов](#)

9.3.1.7.5.2. Источники

Подраздел настроек активов, в котором можно создавать и редактировать источники событий, а также запускать и останавливать прием данных от них.

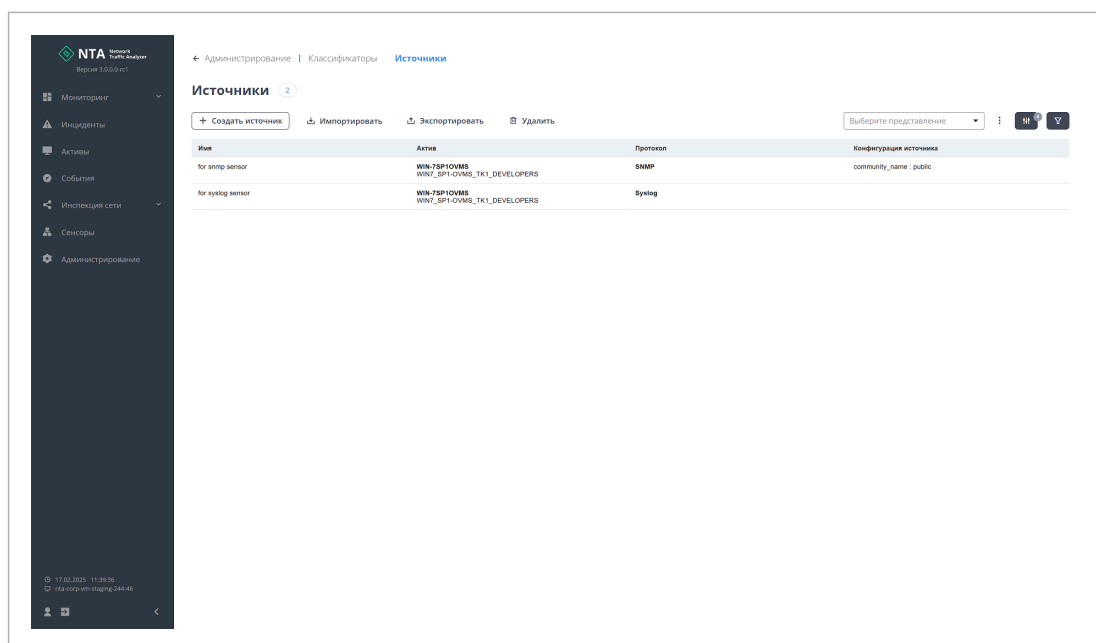


Рис. 213. Страница «Источники»

См. также[Создание источника событий](#)[Управление источниками событий](#)**9.3.1.8. 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](#).

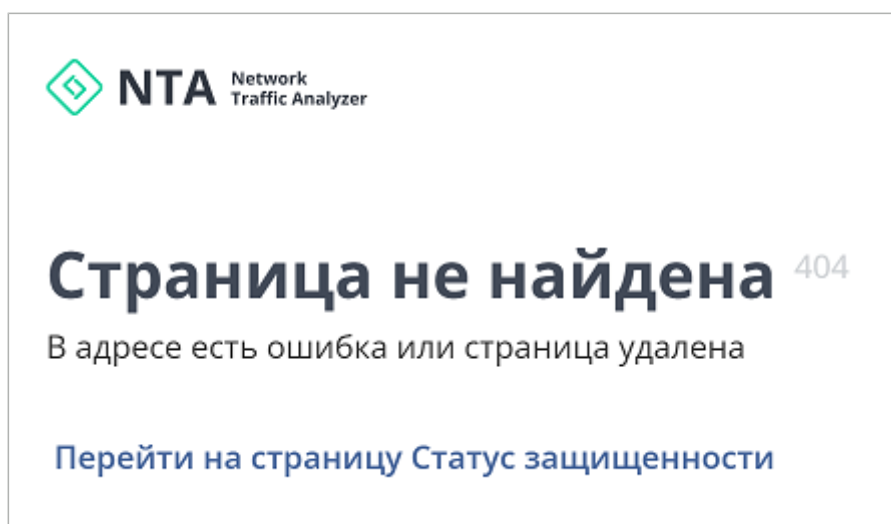


Рис. 214. Страница «Страница не найдена»

См. также[Статус защищенности](#)

9.3.2. Управляющие элементы

В таблице ниже (Таблица 10. Управляющие элементы Комплекса) описаны управляющие элементы — кнопки и иконки, доступные в основном интерфейсе Комплекса.

Табл. 10. Управляющие элементы Комплекса

УПР. ЭЛ-Т	ОПИСАНИЕ	СТРАНИЦЫ ИНТЕРФЕЙСА
	Отфильтровать содержимое страницы	
	Настроить список столбцов таблицы	
	Развернуть	
	Свернуть. Отображается, когда элемент развернут	
	Запустить сбор событий от источника	Источники
	Приостановить сбор событий от источника	
	Запустить службу	Правила корреляции
	Недоступная для использования кнопка запуска службы	
	Остановить службу	
	Перезапустить службу	

Табл. 10. Управляющие элементы Комплекса

УПР. ЭЛ-Т	ОПИСАНИЕ	СТРАНИЦЫ ИНТЕРФЕЙСА
	Перейти к событиям службы	
	Экспортировать источники	Источники
	Экспортировать справочники	Импорт и экспорт
	Импортировать источники	Источники
	Импортировать справочники	Импорт и экспорт
	Сформировать отчет по выбранным активам	Активы
	Импортировать активы	
	Экспортировать активы	
События 	Перейти к событиям актива	Страница актива
Инциденты 	Перейти к инцидентам актива	Страница актива
Источники 	Перейти к источникам актива	Страница актива
	Перейти к источникам выбранных активов	Активы

Табл. 10. Управляющие элементы Комплекса

УПР. ЭЛ-Т	ОПИСАНИЕ	СТРАНИЦЫ ИНТЕРФЕЙСА
 Карты сети	Показать сессии актива на карте сети	Страница актива
	Отвязать сетевые атрибуты от актива	Страница актива, окно настройки сетевых атрибутов
	Сохранить изменения сетевых атрибутов актива	Страница актива, окно настройки сетевых атрибутов
	Глобальная сеть, Локальная сеть	Карта сети
	Удалить элемент	Активы, Инциденты, Индексы, Классификаторы, Источники, Правила корреляции, Оповещения об инцидентах, Правила обнаружения, Пользователи
	Удалить группу элементов	
	Недоступная для использования кнопка группового удаления. Можно увидеть, когда нет элементов для удаления, либо они недоступны	
	Редактировать элемент	Страница актива, Классификаторы, Источники, Правила корреляции, Правила обнаружения, Пользователи
	Редактировать группу элементов	
	Сформировать отчет по содержимому страницы	Активы
	Отменить изменения сетевых атрибутов актива	Страница актива

Табл. 10. Управляющие элементы Комплекса

УПР. ЭЛ-Т	ОПИСАНИЕ	СТРАНИЦЫ ИНТЕРФЕЙСА
	Добавить Email Адрес получателя	Оповещения об инцидентах
	Удалить Email Адрес получателя	
	Архивировать группу индексов событий	Индексы
	Архивировать индекс событий	
	Восстановить индексы из архива	
	Удалить сеть	Сенсоры
	Служба обнаружения вторжений включена (выключить службу)	
	Служба обнаружения вторжений выключена (включить службу)	
	Не применять все выбранные в фильтре элементы	Правила корреляции, Схема корреляции
	Применить все выбранные в фильтре элементы	
	Повысить порядок статуса инцидентов	Статусы инцидентов
	Понизить порядок статуса инцидентов	Статусы инцидентов

Табл. 10. Управляющие элементы Комплекса

УПР. ЭЛ-Т	ОПИСАНИЕ	СТРАНИЦЫ ИНТЕРФЕЙСА
	Просмотреть информацию об элементе (при наведении курсора)	Источники — окно создания источника
	Изменить режим отображения таблицы	Сессии

9.3.3. 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.

Дата создания	Наименование	Регистраторы событий	Активы	Статус	Приоритет	Ответственный	Описание
20.02.2025, 01:19:21	Обнаружен новый актив	nta-corp-vm-stagi...	WIN-989KJ30ACT	Новый	Низкий	dataapk	Обнаружен новый актив ip: 10.51.244.2
20.02.2025, 01:19:21	Обнаружен новый актив	nta-corp-vm-stagi...	WORKGROUP	Новый	Критический		Обнаружен новый актив ip: 10.51.244.2
20.02.2025, 01:19:21	Обнаружен новый актив	nta-corp-vm-stagi...	ADMIN-D8831EAB5	Новый	Критический		Обнаружен новый актив ip: 10.51.244.1
20.02.2025, 01:14:22	Обнаружен новый актив	nta-corp-vm-stagi...	Неизвестный актив	Новый	Высокий	dataapk	Обнаружен новый актив ip: 10.51.15.99
20.02.2025, 01:14:22	Обнаружен новый актив	nta-corp-vm-stagi...	Неизвестный актив	Новый	Критический		Обнаружен новый актив ip: 10.51.15.10
20.02.2025, 01:14:21	Обнаружен новый актив	nta-corp-vm-stagi...	Неизвестный актив	Новый	Критический		Обнаружен новый актив ip: 10.51.15.96
20.02.2025, 01:14:21	Обнаружен новый актив	nta-corp-vm-stagi...	Неизвестный актив	Новый	Критический		Обнаружен новый актив ip: 10.51.244.4
20.02.2025, 01:14:21	Обнаружен новый актив	nta-corp-vm-stagi...	Неизвестный актив	Новый	Критический		Обнаружен новый актив ip: 10.51.15.95
20.02.2025, 01:14:21	Обнаружен новый актив	nta-corp-vm-stagi...	Неизвестный актив	Новый	Средний	dataapk	Обнаружен новый актив ip: 10.51.15.94
20.02.2025, 01:14:21	Обнаружен новый актив	nta-corp-vm-stagi...	Неизвестный актив	Новый	Критический		Обнаружен новый актив ip: 10.51.15.97
20.02.2025, 01:11:40	Обнаружен новый актив	nta-corp-vm-stagi...	DC	Новый	Критический		Обнаружен новый актив ip: 10.51.244.1
20.02.2025, 01:11:40	Обнаружен новый актив	nta-corp-vm-stagi...	Неизвестный актив	Новый	Критический		Обнаружен новый актив ip: 10.51.15.99
20.02.2025, 01:11:40	Обнаружен новый актив	nta-corp-vm-stagi...	Неизвестный актив	Новый	Критический		Обнаружен новый актив ip: 10.51.15.97
20.02.2025, 01:11:40	Обнаружен новый актив	nta-corp-vm-stagi...	Неизвестный актив	Новый	Критический		Обнаружен новый актив ip: 10.51.15.96
20.02.2025, 01:11:40	Обнаружен новый актив	nta-corp-vm-stagi...	Неизвестный актив	Новый	Критический		Обнаружен новый актив ip: 10.51.15.95

Рис. 215. 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. 216. 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.

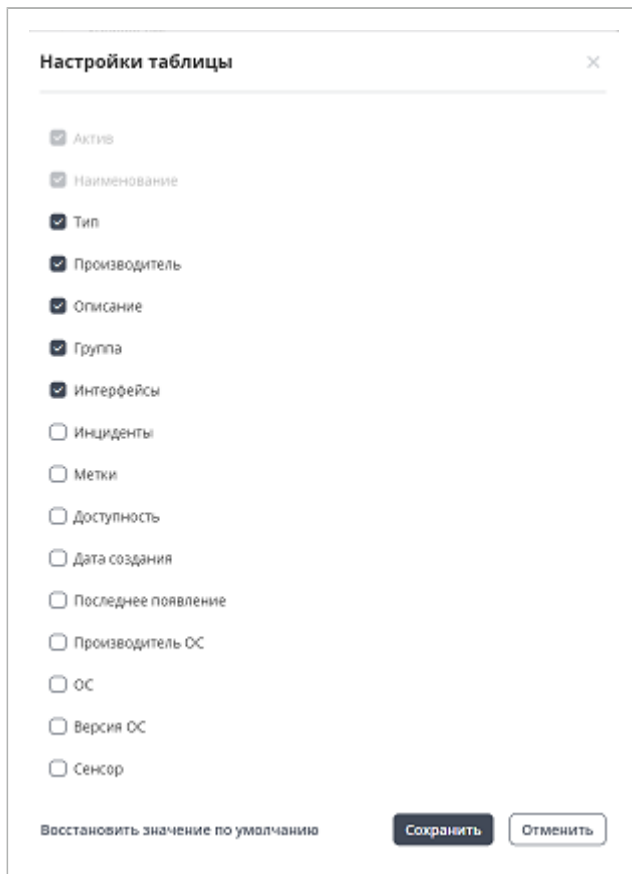


Рис. 217. Окно для выбора столбцов таблицы



Прим.:

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 — . Сортировка доступна не для всех столбцов таблиц.

Множественный выбор элементов

Множественный выбор элементов доступен для таблиц на страницах [Виджеты](#), [Активы](#), [Инциденты](#), [Администрирование](#) → [Сигнатурный анализ](#) → [Правила обнаружения](#), [Инспекция сети](#) → [Сетевые соединения](#) → [Файлы](#).

• 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

Способ 1.

Установите чекбокс в заголовке таблицы — в результате будут установлены чекбоксы во всех строках таблицы.

Способ 2.

1. Установите чекбокс в любой строке — в результате внизу страницы появится панель с кнопками.
2. В появившейся панели нажмите кнопку **Выбрать все** — будут выбраны все доступные строки.

Возможность выбора всех строк отсутствует на странице [Инспекция сети](#) → [Сетевые соединения](#) → [Файлы](#)

- **Отмена выбора всех строк**

При выборе всех строк отметьте чекбокс в заголовке таблицы, чтобы отменить выбор чекбоксов во всех строках.

Возможность отмены выбора всех строк отсутствует на странице [Инспекция сети](#) → [Сетевые соединения](#) → [Файлы](#)

9.3.4. 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:

- [Индикация активов](#)
- [Статусы активов](#)
- [Статусы групповых операций](#)
- [Индикация статусов операций](#)
- [Виды уведомлений](#)

9.3.4.1. Индикация активов

Индикация активов по типу

В интерфейсе Комплекса на странице [Активы](#) присутствует специфическая индикация активов в зависимости от присвоенного им типа. Ознакомиться с ней вы можете в таблице ниже.

Табл. 11. Индикация активов по типу

ИНДИКАТОР	ТИП АКТИВА, ОБОЗНАЧЕНИЕ
	Автоматизированное рабочее место (АРМ)
	Коммутатор
	Маршрутизатор
	Неизвестный тип
	Сервер

Табл. 11. Индикация активов по типу

ИНДИКАТОР	ТИП АКТИВА, ОБОЗНАЧЕНИЕ
	Периферийное оборудование
	Программируемый логический контроллер (ПЛК)
	Средство защиты
	Сенсор
	Комплекс

Цветовая индикация активов

На странице [Активы](#) присутствует специфическая цветовая индикация активов в зависимости от их состояния. Ознакомиться с ней вы можете в таблице ниже.

Табл. 12. Цветовая 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
Индикация активов цветом и спецсимволами <u>не зависят</u> друг от друга		

9.3.4.2. Статусы активов

В таблице на странице [Активы](#) можно просматривать статистику по обнаруженным инцидентам. Столбец таблицы можно выбрать и отобразить по кнопке  в правом верхнем углу страницы.

Описание статусов приведено в таблице ниже.

Табл. 13. 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

Статус **Инциденты** можно сортировать в порядке критичности. Порядок критичности по убыванию: темно-красный, красный, оранжевый, серый.

9.3.4.3. Статусы групповых операций

На многих страницах веб-интерфейса присутствует возможность выполнять групповые операции с элементами таблиц. При их использовании задействуется механизм индикации. В таблице ниже для примера используется индикация статуса временного одобрения потоков данных.

Табл. 14. Цветовая индикация групповых операций

ИНДИКАТОР	ЦВЕТ	ОПИСАНИЕ
	Темно-синий	Групповая операция доступна для использования
	Серый	Групповая операция недоступна для использования
	Оранжевый	Групповая операция находится в очереди. При нажатии выполнение операции будет отменено
	Зеленый	Групповая операция выполняется. При нажатии выполнение операции будет прервано

9.3.4.4. 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. 15. Индикаторы статусов операций

ИН-ДИКАТОР	ОПИСАНИЕ	СТРАНИЦА ИНТЕРФЕЙСА
Ошибка обработки	Операция не была завершена вследствие ошибки. При нажатии на «▼» можно посмотреть детали	Страница актива
Ошибка соединения	Операция была инициирована пользователем, ожидает в очереди на выполнение	Страница актива

Табл. 15. Индикаторы статусов операций

ИН-ДИКАТОР	ОПИСАНИЕ	СТРАНИЦА ИНТЕРФЕЙСА
Успешно завершено	Операция была запущена и выполняется в данный момент	Страница актива
	Операция не была завершена вследствие превышения времени ожидания	Страница актива
	Пользователь активен (не заблокирован)	Пользователи
	Пользователь неактивен (заблокирован)	Пользователи

9.3.4.5. 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. 16. Виды уведомлений в интерфейсе Комплекса

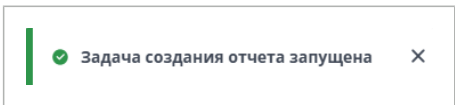
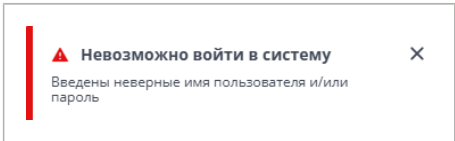
ПРИМЕР УВЕДОМЛЕНИЯ	ОПИСАНИЕ
	Предупреждения. Уведомляет пользователя о специфике работы выбранной операции и ее последствиях.
	Уведомляет пользователя об успешном начале потенциально длительной операции.

Табл. 16. Виды уведомлений в интерфейсе Комплекса

ПРИМЕР УВЕДОМЛЕНИЯ	ОПИСАНИЕ
	Ошибки. Уведомляет пользователя о проблемах при выполнении операции.

9.3.4.6. Статусы подготовки файлов к экспорту

На следующих страницах UDV NTA 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. 17. 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
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

9.4. Дополнительные функции Комплекса

В разделе описаны следующие дополнительные функциональные возможности Комплекса.

- Выгрузка отчетов
- Групповые операции
- Нормализация событий
- Фильтры

9.4.1. Выгрузка отчетов

Комплекс позволяет пользователям выгружать отчеты в форматы **xlsx** и **csv** по содержимому следующих страниц:

СТРАНИЦА	СОДЕРЖАНИЕ ОТЧЕТА	ФОРМАТ ОТЧЕТА
Активы	Активы, выбранные чекбоксами	html, xlsx
Инциденты	Все или отфильтрованные инциденты	html, xlsx

Помимо таблицы, отчеты формата **html** и **xlsx** содержат название, использованные при создании отчета фильтры, дату выгрузки, автора запроса и заголовков.

Отчет "Активы"

Создан: Смирнов Александр Иванович (00000)
История: Активы: CISCO_IOL, CISCO_ASA_BRANCH, Manager, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96, 97, 98, 99, 100, 101, 102, 103, 104, 105, 106, 107, 108, 109, 110, 111, 112, 113, 114, 115, 116, 117, 118, 119, 120, 121, 122, 123, 124, 125, 126, 127, 128, 129, 130, 131, 132, 133, 134, 135, 136, 137, 138, 139, 140, 141, 142, 143, 144, 145, 146, 147, 148, 149, 150, 151, 152, 153, 154, 155, 156, 157, 158, 159, 160, 161, 162, 163, 164, 165, 166, 167, 168, 169, 170, 171, 172, 173, 174, 175, 176, 177, 178, 179, 180, 181, 182, 183, 184, 185, 186, 187, 188, 189, 190, 191, 192, 193, 194, 195, 196, 197, 198, 199, 200, 201, 202, 203, 204, 205, 206, 207, 208, 209, 210, 211, 212, 213, 214, 215, 216, 217, 218, 219, 220, 221, 222, 223, 224, 225, 226, 227, 228, 229, 230, 231, 232, 233, 234, 235, 236, 237, 238, 239, 240, 241, 242, 243, 244, 245, 246, 247, 248, 249, 250, 251, 252, 253, 254, 255, 256, 257, 258, 259, 260, 261, 262, 263, 264, 265, 266, 267, 268, 269, 270, 271, 272, 273, 274, 275, 276, 277, 278, 279, 280, 281, 282, 283, 284, 285, 286, 287, 288, 289, 290, 291, 292, 293, 294, 295, 296, 297, 298, 299, 300, 301, 302, 303, 304, 305, 306, 307, 308, 309, 310, 311, 312, 313, 314, 315, 316, 317, 318, 319, 320, 321, 322, 323, 324, 325, 326, 327, 328, 329, 330, 331, 332, 333, 334, 335, 336, 337, 338, 339, 340, 341, 342, 343, 344, 345, 346, 347, 348, 349, 350, 351, 352, 353, 354, 355, 356, 357, 358, 359, 360, 361, 362, 363, 364, 365, 366, 367, 368, 369, 370, 371, 372, 373, 374, 375, 376, 377, 378, 379, 380, 381, 382, 383, 384, 385, 386, 387, 388, 389, 390, 391, 392, 393, 394, 395, 396, 397, 398, 399, 400, 401, 402, 403, 404, 405, 406, 407, 408, 409, 410, 411, 412, 413, 414, 415, 416, 417, 418, 419, 420, 421, 422, 423, 424, 425, 426, 427, 428, 429, 430, 431, 432, 433, 434, 435, 436, 437, 438, 439, 440, 441, 442, 443, 444, 445, 446, 447, 448, 449, 450, 451, 452, 453, 454, 455, 456, 457, 458, 459, 460, 461, 462, 463, 464, 465, 466, 467, 468, 469, 470, 471, 472, 473, 474, 475, 476, 477, 478, 479, 480, 481, 482, 483, 484, 485, 486, 487, 488, 489, 490, 491, 492, 493, 494, 495, 496, 497, 498, 499, 500, 501, 502, 503, 504, 505, 506, 507, 508, 509, 510, 511, 512, 513, 514, 515, 516, 517, 518, 519, 520, 521, 522, 523, 524, 525, 526, 527, 528, 529, 530, 531, 532, 533, 534, 535, 536, 537, 538, 539, 540, 541, 542, 543, 544, 545, 546, 547, 548, 549, 550, 551, 552, 553, 554, 555, 556, 557, 558, 559, 560, 561, 562, 563, 564, 565, 566, 567, 568, 569, 570, 571, 572, 573, 574, 575, 576, 577, 578, 579, 580, 581, 582, 583, 584, 585, 586, 587, 588, 589, 590, 591, 592, 593, 594, 595, 596, 597, 598, 599, 600, 601, 602, 603, 604, 605, 606, 607, 608, 609, 610, 611, 612, 613, 614, 615, 616, 617, 618, 619, 620, 621, 622, 623, 624, 625, 626, 627, 628, 629, 630, 631, 632, 633, 634, 635, 636, 637, 638, 639, 640, 641, 642, 643, 644, 645, 646, 647, 648, 649, 650, 651, 652, 653, 654, 655, 656, 657, 658, 659, 660, 661, 662, 663, 664, 665, 666, 667, 668, 669, 670, 671, 672, 673, 674, 675, 676, 677, 678, 679, 680, 681, 682, 683, 684, 685, 686, 687, 688, 689, 690, 691, 692, 693, 694, 695, 696, 697, 698, 699, 700, 701, 702, 703, 704, 705, 706, 707, 708, 709, 710, 711, 712, 713, 714, 715, 716, 717, 718, 719, 720, 721, 722, 723, 724, 725, 726, 727, 728, 729, 730, 731, 732, 733, 734, 735, 736, 737, 738, 739, 740, 741, 742, 743, 744, 745, 746, 747, 748, 749, 750, 751, 752, 753, 754, 755, 756, 757, 758, 759, 760, 761, 762, 763, 764, 765, 766, 767, 768, 769, 770, 771, 772, 773, 774, 775, 776, 777, 778, 779, 780, 781, 782, 783, 784, 785, 786, 787, 788, 789, 790, 791, 792, 793, 794, 795, 796, 797, 798, 799, 800, 801, 802, 803, 804, 805, 806, 807, 808, 809, 810, 811, 812, 813, 814, 815, 816, 817, 818, 819, 820, 821, 822, 823, 824, 825, 826, 827, 828, 829, 830, 831, 832, 833, 834, 835, 836, 837, 838, 839, 840, 841, 842, 843, 844, 845, 846, 847, 848, 849, 850, 851, 852, 853, 854, 855, 856, 857, 858, 859, 860, 861, 862, 863, 864, 865, 866, 867, 868, 869, 870, 871, 872, 873, 874, 875, 876, 877, 878, 879, 880, 881, 882, 883, 884, 885, 886, 887, 888, 889, 890, 891, 892, 893, 894, 895, 896, 897, 898, 899, 900, 901, 902, 903, 904, 905, 906, 907, 908, 909, 910, 911, 912, 913, 914, 915, 916, 917, 918, 919, 920, 921, 922, 923, 924, 925, 926, 927, 928, 929, 930, 931, 932, 933, 934, 935, 936, 937, 938, 939, 940, 941, 942, 943, 944, 945, 946, 947, 948, 949, 950, 951, 952, 953, 954, 955, 956, 957, 958, 959, 960, 961, 962, 963, 964, 965, 966, 967, 968, 969, 970, 971, 972, 973, 974, 975, 976, 977, 978, 979, 980, 981, 982, 983, 984, 985, 986, 987, 988, 989, 990, 991, 992, 993, 994, 995, 996, 997, 998, 999, 1000, 1001, 1002, 1003, 1004, 1005, 1006, 1007, 1008, 1009, 1010, 1011, 1012, 1013, 1014, 1015, 1016, 1017, 1018, 1019, 1020, 1021, 1022, 1023, 1024, 1025, 1026, 1027, 1028, 1029, 1030, 1031, 1032, 1033, 1034, 1035, 1036, 1037, 1038, 1039, 1040, 1041, 1042, 1043, 1044, 1045, 1046, 1047, 1048, 1049, 1050, 1051, 1052, 1053, 1054, 1055, 1056, 1057, 1058, 1059, 1060, 1061, 1062, 1063, 1064, 1065, 1066, 1067, 1068, 1069, 1070, 1071, 1072, 1073, 1074, 1075, 1076, 1077, 1078, 1079, 1080, 1081, 1082, 1083, 1084, 1085, 1086, 1087, 1088, 1089, 1090, 1091, 1092, 1093, 1094, 1095, 1096, 1097, 1098, 1099, 1100, 1101, 1102, 1103, 1104, 1105, 1106, 1107, 1108, 1109, 1110, 1111, 1112, 1113, 1114, 1115, 1116, 1117, 1118, 1119, 1120, 1121, 1122, 1123, 1124, 1125, 1126, 1127, 1128, 1129, 1130, 1131, 1132, 1133, 1134, 1135, 1136, 1137, 1138, 1139, 1140, 1141, 1142, 1143, 1144, 1145, 1146, 1147, 1148, 1149, 1150, 1151, 1152, 1153, 1154, 1155, 1156, 1157, 1158, 1159, 1160, 1161, 1162, 1163, 1164, 1165, 1166, 1167, 1168, 1169, 1170, 1171, 1172, 1173, 1174, 1175, 1176, 1177, 1178, 1179, 1180, 1181, 1182, 1183, 1184, 1185, 1186, 1187, 1188, 1189, 1190, 1191, 1192, 1193, 1194, 1195, 1196, 1197, 1198, 1199, 1200, 1201, 1202, 1203, 1204, 1205, 1206, 1207, 1208, 1209, 1210, 1211, 1212, 1213, 1214, 1215, 1216, 1217, 1218, 1219, 1220, 1221, 1222, 1223, 1224, 1225, 1226, 1227, 1228, 1229, 1230, 1231, 1232, 1233, 1234, 1235, 1236, 1237, 1238, 1239, 1240, 1241, 1242, 1243, 1244, 1245, 1246, 1247, 1248, 1249, 1250, 1251, 1252, 1253, 1254, 1255, 1256, 1257, 1258, 1259, 1260, 1261, 1262, 1263, 1264, 1265, 1266, 1267, 1268, 1269, 1270, 1271, 1272, 1273, 1274, 1275, 1276, 1277, 1278, 1279, 1280, 1281, 1282, 1283, 1284, 1285, 1286, 1287, 1288, 1289, 1290, 1291, 1292, 1293, 1294, 1295, 1296, 1297, 1298, 1299, 1300, 1301, 1302, 1303, 1304, 1305, 1306, 1307, 1308, 1309, 1310, 1311, 1312, 1313, 1314, 1315, 1316, 1317, 1318, 1319, 1320, 1321, 1322, 1323, 1324, 1325, 1326, 1327, 1328, 1329, 1330, 1331, 1332, 1333, 1334, 1335, 1336, 1337, 1338, 1339, 1340, 1341, 1342, 1343, 1344, 1345, 1346, 1347, 1348, 1349, 1350, 1351, 1352, 1353, 1354, 1355, 1356, 1357, 1358, 1359, 1360, 1361, 1362, 1363, 1364, 1365, 1366, 1367, 1368, 1369, 1370, 1371, 1372, 1373, 1374, 1375, 1376, 1377, 1378, 1379, 1380, 1381, 1382, 1383, 1384, 1385, 1386, 1387, 1388, 1389, 1390, 1391, 1392, 1393, 1394, 1395, 1396, 1397, 1398, 1399, 1400, 1401, 1402, 1403, 1404, 1405, 1406, 1407, 1408, 1409, 1410, 1411, 1412, 1413, 1414, 1415, 1416, 1417, 1418, 1419, 1420, 1421, 1422, 1423, 1424, 1425, 1426, 1427, 1428, 1429, 1430, 1431, 1432, 1433, 1434, 1435, 1436, 1437, 1438, 1439, 1440, 1441, 1442, 1443, 1444, 1445, 1446, 1447, 1448, 1449, 1450, 1451, 1452, 1453, 1454, 1455, 1456, 1457, 1458, 1459, 1460, 1461, 1462, 1463, 1464, 1465, 1466, 1467, 1468, 1469, 1470, 1471, 1472, 1473, 1474, 1475, 1476, 1477, 1478, 1479, 1480, 1481, 1482, 1483, 1484, 1485, 1486, 1487, 1488, 1489, 1490, 1491, 1492, 1493, 1494, 1495, 1496, 1497, 1498, 1499, 1500, 1501, 1502, 1503, 1504, 1505, 1506, 1507, 1508, 1509, 1510, 1511, 1512, 1513, 1514, 1515, 1516, 1517, 1518, 1519, 1520, 1521, 1522, 1523, 1524, 1525, 1526, 1527, 1528, 1529, 1530, 1531, 1532, 1533, 1534, 1535, 1536, 1537, 1538, 1539, 1540, 1541, 1542, 1543, 1544, 1545, 1546, 1547, 1548, 1549, 1550, 1551, 1552, 1553, 1554, 1555, 1556, 1557, 1558, 1559, 1560, 1561, 1562, 1563, 1564, 1565, 1566, 1567, 1568, 1569, 1570, 1571, 1572, 1573, 1574, 1575, 1576, 1577, 1578, 1579, 1580, 1581, 1582, 1583, 1584, 1585, 1586, 1587, 1588, 1589, 1590, 1591, 1592, 1593, 1594, 1595, 1596, 1597, 1598, 1599, 1600, 1601, 1602, 1603, 1604, 1605, 1606, 1607, 1608, 1609, 1610, 1611, 1612, 1613, 1614, 1615, 1616, 1617, 1618, 1619, 1620, 1621, 1622, 1623, 1624, 1625, 1626, 1627, 1628, 1629, 1630, 1631, 1632, 1633, 1634, 1635, 1636, 1637, 1638, 1639, 1640, 1641, 1642, 1643, 1644, 1645, 1646, 1647, 1648, 1649, 1650, 1651, 1652, 1653, 1654, 1655, 1656, 1657, 1658, 1659, 1660, 1661, 1662, 1663, 1664, 1665, 1666, 1667, 1668, 1669, 1670, 1671, 1672, 1673, 1674, 1675, 1676, 1677, 1678, 1679, 1680, 1681, 1682, 1683, 1684, 1685, 1686, 1687, 1688, 1689, 1690, 1691, 1692, 1693, 1694, 1695, 1696, 1697, 1698, 1699, 1700, 1701, 1702, 1703, 1704, 1705, 1706, 1707, 1708, 1709, 1710, 1711, 1712, 1713, 1714, 1715, 1716, 1717, 1718, 1719, 1720, 1721, 1722, 1723, 1724, 1725, 1726, 1727, 1728, 1729, 1730, 1731, 1732, 1733, 1734, 1735, 1736, 1737, 1738, 1739, 1740, 1741, 1742, 1743, 1744, 1745, 1746, 1747, 1748, 1749, 1750, 1751, 1752, 1753, 1754, 1755, 1756, 1757, 1758, 1759, 1760, 1761, 1762, 1763, 1764, 1765, 1766, 1767, 1768, 1769, 1770, 1771, 1772, 1773, 1774, 1775, 1776, 1777, 1778, 1779, 1780, 1781, 1782, 1783, 1784, 1785, 1786, 1787, 1788, 1789, 1790, 1791, 1792, 1793, 1794, 1795, 1796, 1797, 1798, 1799, 1800, 1801, 1802, 1803, 1804, 1805, 1806, 1807, 1808, 1809, 1810, 1811, 1812, 1813, 1814, 1815, 1816, 1817, 1818, 1819, 1820, 1821, 1822, 1823, 1824, 1825, 1826, 1827, 1828, 1829, 1830, 1831, 1832, 1833, 1834, 1835, 1836, 1837, 1838, 1839, 1840, 1841, 1842, 1843, 1844, 1845, 1846, 1847, 1848, 1849, 1850, 1851, 1852, 1853, 1854, 1855, 1856, 1857, 1858, 1859, 1860, 1861, 1862, 1863, 1864, 1865, 1866, 1867, 1868, 1869, 1870, 1871, 1872, 1873, 1874, 1875, 1876, 1877, 1878, 1879, 1880, 1881, 1882, 1883, 1884, 1885, 1886, 1887, 1888, 1889, 1890, 1891, 1892, 1893, 1894, 1895, 1896, 1897, 1898, 1899, 1900, 1901, 1902, 1903, 1904, 1905, 1906, 1907, 1908, 1909, 1910, 1911, 1912, 1913, 1914, 1915, 1916, 1917, 1918, 1919, 1920, 1921, 1922, 1923, 1924, 1925, 1926, 1927, 1928, 1929, 1930, 1931, 1932, 1933, 1934, 1935, 1936, 1937, 1938, 1939, 1940, 1941, 1942, 1943, 1944, 1945, 1946, 1947, 1948, 1949, 1950, 1951, 1952, 1953, 1954, 1955, 1956, 1957, 1958, 1959, 1960, 1961, 1962, 1963, 1964, 1965, 1966, 1967, 1968, 1969, 1970, 1971, 1972, 1973, 1974, 1975, 1976, 1977, 1978, 1979, 1980, 1981, 1982, 1983, 1984, 1985, 1986, 1987, 1988, 1989, 1990, 1991, 1992, 1993, 1994, 1995, 1996, 1997, 1998, 1999, 2000, 2001, 2002, 2003, 2004, 2005, 2006, 2007, 2008, 2009, 2010, 2011, 2012, 2013, 2014, 2015, 2016, 2017, 2018, 2019, 2020, 2021, 2022, 2023, 2024, 2025, 2026, 2027, 2028, 2029, 2030, 2031, 2032, 2033, 2034, 2035, 2036, 2037, 2038, 2039, 2040, 2041, 2042, 2043, 2044, 2045, 2046, 2047, 2048, 2049, 2050, 2051, 2052, 2053, 2054, 2055, 2056, 2057, 2058, 2059, 2060, 2061, 2062, 2063, 2064, 2065, 2066, 2067, 2068, 2069, 2070, 2071, 2072, 2073, 2074, 2075, 2076, 2077, 2078, 2079, 2080, 2081, 2082, 2083, 2084, 2085, 2086, 2087, 2088, 2089, 2090, 2091, 2092, 2093, 2094, 2095, 2096, 2097, 2098, 2099, 2100, 2101, 2102, 2103, 2104, 2105, 2106, 2107, 2108, 2109, 2110, 2111, 2112, 2113, 2114, 2115, 2116, 2117, 2118, 2119, 2120, 2121, 2122, 2123, 2124, 2125, 2126, 2127, 2128, 2129, 2130, 2131, 2132, 2133, 2134, 2135, 2136, 2137, 2138, 2139, 2140, 2141, 2142, 2143, 2144, 2145, 2146, 2147, 2148, 2149, 2150, 2151, 2152, 2153, 2154, 2155, 2156, 2157, 2158, 2159, 2160, 2161, 2162, 2163, 2164, 2165, 2166, 2167, 2168, 2169, 2170, 2171, 2172, 2173, 2174, 2175, 2176, 2177,

4. Нажмите кнопку **Запустить создание отчета**. В правом верхнем углу вы увидите всплывающее уведомление Задача создания отчета запущена;
5. Для сохранения отчета после того, как он сформирован, нажмите на ссылку с названием файла отчета.

 **Внимание:**

Максимальное количество строк, выгружаемых при формировании отчета – 1000. Если значение переменной `MAX_ROWS_PER_REPORT` более 1000, в отчет выгрузится только 1000 строк.

В окне **Создание отчета** пользователь видит текущее состояние задачи создания отчета и после того, как отчет сформирован, может его сохранить в нужном формате.

Создание отчета

×

Формат файла *

html
×
▼

Выбранные столбцы *

×

Наименование

×

Тип

×

Производитель

×

Описание

×

Группа

×

Интерфейсы

×

Инциденты

×

Метки

×

Доступность

×

Дата создания

×

Последнее появление

×

Производитель ОС

×

ОС

×

Версия ОС

×

Сенсор

×
▼

Текущее состояние задачи создания отчета

Завершена

 hosts.html

Запустить создание отчета

Заккрыть

Рис. 219. Окно «Создание отчета»

Для задачи создания отчета возможны следующие состояния:

- 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.

9.4.2. 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 18. Основные групповые операции).

Табл. 18. Основные групповые операции

НАЗВАНИЕ	СТРАНИЦЫ ИНТЕРФЕЙСА
Удаление	Активы, Инциденты, Индексы, Источники, Правила корреляции, Правила обнаружения, Ретроанализ, Схема корреляции
Включение правил	Правила корреляции, Правила обнаружения
Отключение правил	Правила корреляции, Правила обнаружения



Внимание:

Действие групповой операции применяется ко всем выбранным элементам страницы. Для страниц **Активы**, **Виджеты** 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 19. Операции, доступные только при выборе одного или нескольких элементов.).

Табл. 19. Операции, доступные только при выборе одного или нескольких элементов.

СТРАНИЦА	КНОПКИ ОПЕРАЦИЙ, ДОСТУПНЫЕ ПРИ ВЫБОРЕ ХОТЯ БЫ ОДНОГО ЭЛЕМЕНТА
Виджеты	Удалить визуализации
Активы, Инциденты	 (Удалить),  (Отчет)

Дополнительные групповые операции

Ознакомиться с дополнительными групповыми операциями, которые используются только на одной странице интерфейса, вы можете в таблице ниже.

Табл. 20. Дополнительные групповые операции

НАЗВАНИЕ	СТРАНИЦЫ ИНТЕРФЕЙСА
Изменить параметры инцидентов	Инциденты

Табл. 20. Дополнительные групповые операции

НАЗВАНИЕ	СТРАНИЦЫ ИНТЕРФЕЙСА
Архивировать	Индексы
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

Обоснование групповых операций

При использовании групповых операций необходимо ввести обоснование, чтобы администратор системы мог найти причину серьезных изменений.

Рис. 220. Обоснование групповой операции

9.4.3. 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`, где:

- `${N}` — приоритет применения файла (чем меньше число, тем выше приоритет);
- `${NAME}` — название конфигурации (рекомендуется указывать название сервиса, откуда получено сообщение или для какого сервиса предназначено готовое событие);
- `{TYPE}` — тип конфигурации (`input`, `filter` или `output`). При этом порядок применения `${N}` должен строго соответствовать типу конфигурации: в Комплексе сначала выполняются все файлы `input`, затем — все `filter`, в конце — все `output`.

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} (?<Ver0s>.*)
```

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_source}\""}
      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`.

9.4.4. Фильтры

Для поиска данных по критериям пользователь Комплекса может воспользоваться фильтрами.

На каждой странице, где доступна фильтрация данных, отличается набор, вид и расположение фильтров. На некоторых страницах фильтры доступны по кнопке в правом верхнем углу и открываются в виде карточки.

Время обновления

10.02.2025 x [calendar icon] 00:00:00

14.02.2025 x [calendar icon] 23:59:59

Установить текущие сутки

Название/описание

Введите текст

IP-адреса активов

Введите IP-адреса или диапазоны

Типы активов

Выберите типы

MAC-адреса отправителя

Введите MAC-адреса

☒ Использовать условие "AND"

MAC-адреса получателя

Введите MAC-адреса

IP-адреса отправителя

Введите IP-адреса или диапазоны

☒ Использовать условие "AND"

IP-адреса получателя

Введите IP-адреса или диапазоны

Сеть отправителя

Выберите сеть

Сеть получателя

Выберите сеть

Применить Сбросить

Рис. 221. Пример карточки фильтров на странице «Карта сети»

Также фильтры могут располагаться на панели сверху страницы.

Наименование Все Тип Все Производитель Все IP-адрес Все MAC-адрес Все Метки Все Производитель ОС Все ОС Все Версия ОС Все

Сенсор Все + Очистить

Рис. 222. Пример панели фильтров на странице «Активы»

Фильтры влияют только на отображение записей таблицы: количество и порядок столбцов таблицы можно изменить в окне **Настройка таблицы**. Подробнее см. в разделе «[Элементы управления таблицами](#)».

После настройки фильтров на страницах **Инциденты**, **Активы**, **Карта сети** и страницах раздела **Администрирование** есть возможность сохранить примененный фильтр и другие параметры страницы, такие как расположение узлов на карте или колонок таблиц. Уже созданные представления можно изменить или удалить. Подробнее см. в разделе «[Управление представлениями](#)».

9.4.5. 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 сетевых соединений.

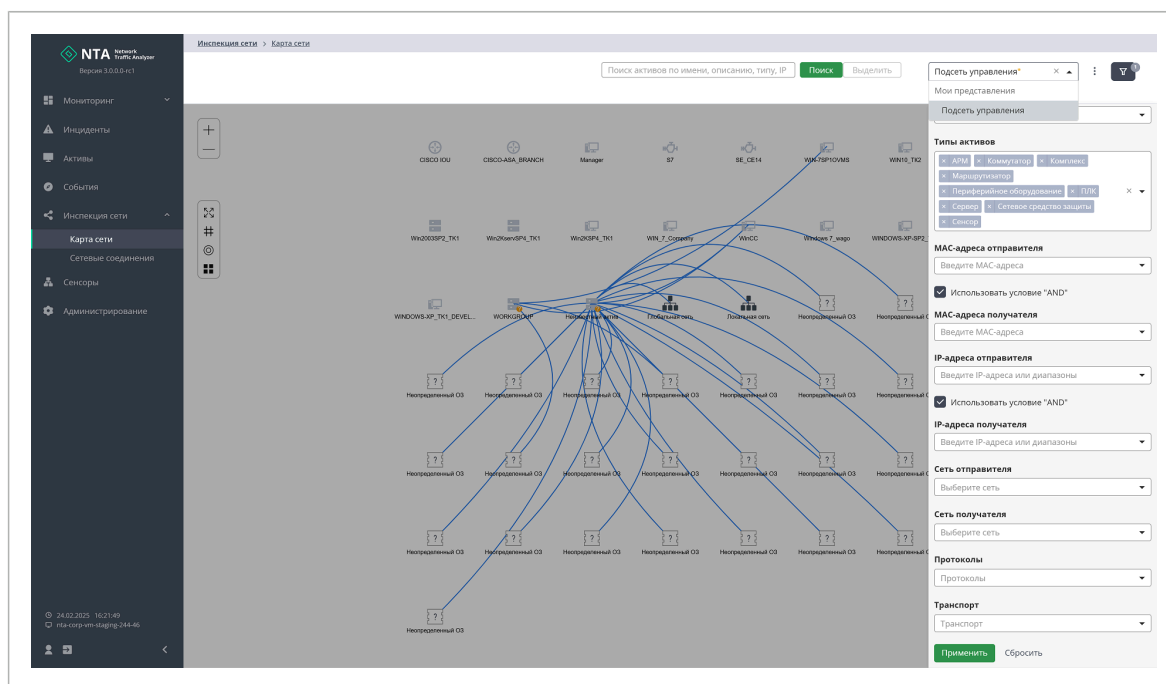


Рис. 223. Представления на странице «Карта сети»

После настройки фильтров, отображаемых колонок или узлов на карте представление можно сохранить. Для сохраненных представлений доступно редактирование и удаление.

9.4.5.1. Управление представлениями

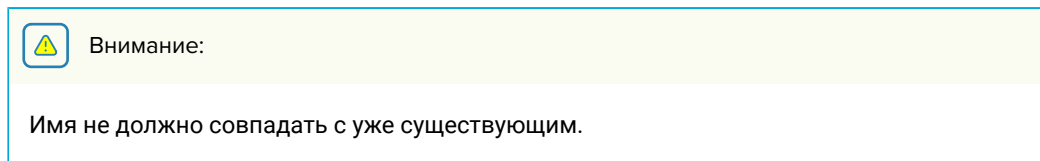
Управление представлениями осуществляется на страницах, где они применяются. Доступны следующие возможности:

1. Сохранение представления. Для сохранения:
 - а. Заполните все необходимые параметры фильтрации, в настройках таблицы 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.



Сохранить представление «Сессии за январь 2025» ✕

Наименование *

Сессии за январь 2025

☒ Сохранить только для меня

☐ Сохранить для всех пользователей

Сохранить Отменить

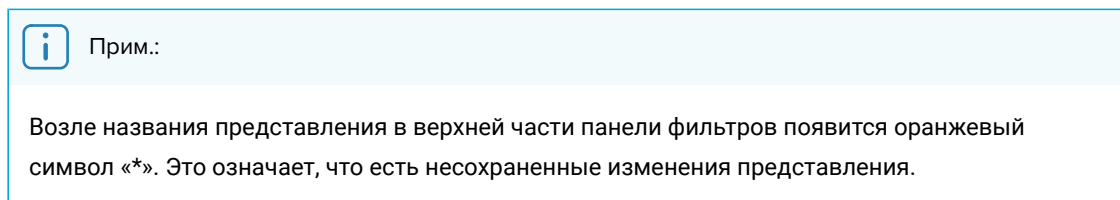
Рис. 224. Окно сохранения представления

д. Нажмите **Сохранить**.

- **Результат шага:** на странице, где было сохранено представление, будет доступно для выбора новое представление.

2. Изменение представления. Для изменения:

- В верхней части панели фильтров выберите из выпадающего списка представление, которое будет изменено.
- Измените параметры фильтрации, отображение столбцов или отображение узлов на карте.



Прим.:

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.

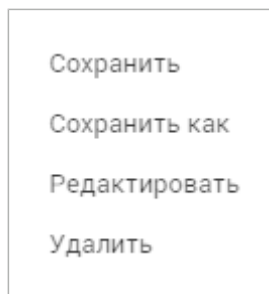


Рис. 225. Меню управления представлением

д. В окне сохранения представления введите имя представления.

Рис. 226. Предупреждение в окне сохранения представления

е. Нажмите **Сохранить**.

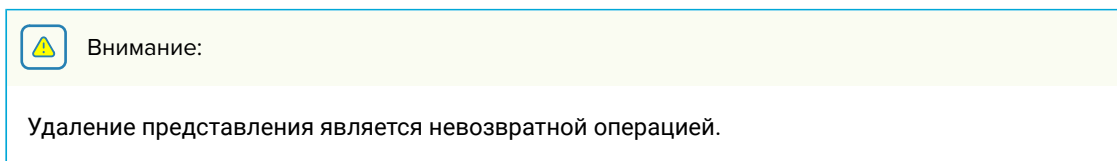
3. Удаление представления. Для удаления представления:

а. 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».



► **Результат шага:** появится всплывающее уведомление: Представление удалено.

9.5. 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.

Клиентское аппаратное и программное обеспечение должно удовлетворять следующим параметрам:

- операционные системы: Microsoft Windows Server 2008 и новее, Microsoft Windows 7 и новее, CentOS 7.6 и новее, Red Hat Enterprise Linux 6.5 и новее, Astra Linux 2.11.5 (Orel) и новее, Astra Linux SE 1.6 (Smolensk) и новее;
- объем оперативной памяти: не менее 1 ГБ;
- процессор: по характеристикам не ниже Pentium IV и с тактовой частотой не менее 2 ГГц;
- дисковое пространство: от 10 ГБ.

9.6. Описание служебных источников событий

Служебные источники событий описаны в таблице ниже ([Таблица 21. Служебные источники событий Комплекса](#)).

Табл. 21. Служебные источники событий Комплекса

НАЗВАНИЕ ИСТОЧНИКА (LISTENER)	ОПИСАНИЕ
Availability control	Изменение доступности активов, невозможность установки соединения с активом
Event control	Запуск или остановка системы регистрации событий
Host control	Создание, удаление и изменение активов, обнаружение неизвестных активов
Incident control	Создание, удаление, изменение инцидентов
User action control	Выполнение действий пользователями
System control	Статус компонентов Комплекса: оперативной памяти, дискового пространства, нагрузки на ЦП, средней нагрузки (Load average)
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 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 22. 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, сгенерированным сенсорами.

Табл. 22. Переменные для управления событиями Комплекса

ПЕРЕМЕННАЯ	ОПИСАНИЕ	ЗНАЧЕНИЕ ПЕРЕМЕННОЙ ПО УМОЛЧАНИЮ
<code>DISABLE_USER_ACTION_- CONTROL_EVENTS</code>	При значении переменной <code>true</code> события о действиях пользователей не собираются	<code>false</code>
<code>DISABLE_HOST_- CONTROL_EVENTS</code>	При значении переменной <code>true</code> события о появлении новых, изменении и удалении узлов не собираются	<code>false</code>
<code>DISABLE_AVAILABILITY_- CONTROL_EVENTS</code>	При значении переменной <code>true</code> события о доступности узлов не собираются	<code>false</code>
<code>DISABLE_INCIDENT_- CONTROL_EVENTS</code>	При значении переменной <code>true</code> события об инцидентах не собираются	<code>false</code>
<code>DISABLE_BACKUP_- CONTROL_EVENTS</code>	При значении переменной <code>true</code> события о резервном копировании не собираются	<code>false</code>
<code>DISABLE_SURICATA_- CONTROL_EVENTS</code>	При значении переменной <code>true</code> события службы обнаружения вторжений не собираются	<code>false</code>
<code>HOST_DATA_COLLECTING_- EVENTS_SEVERITY</code>	Уровень критичности событий сбора и ошибок сбора данных	<code>low</code>
<code>USER_ACTION_CONTROL_- EVENTS_SEVERITY</code>	Уровень критичности событий по действиям пользователей	<code>low</code>
<code>HOST_CONTROL_- EVENTS_SEVERITY</code>	Уровень критичности событий появления новых узлов	<code>low</code>

Табл. 22. Переменные для управления событиями Комплекса

ПЕРЕМЕННАЯ	ОПИСАНИЕ	ЗНАЧЕНИЕ ПЕРЕМЕННОЙ ПО УМОЛЧАНИЮ
AVAILABILITY_CONTROL_ - EVENTS_SEVERITY	Уровень критичности событий доступности узлов	low
INCIDENT_CONTROL_ - EVENTS_SEVERITY	Уровень критичности событий о создании, удалении, изменении инцидентов	low
BACKUP_CONTROL_ - EVENTS_SEVERITY	Уровень критичности событий резервного копирования	low
IDS_CONTROL_ - EVENTS_SEVERITY	Уровень критичности событий службы обнаружения вторжений	low
ESPER_CONTROL_ - EVENTS_SEVERITY	Уровень критичности событий сервиса обработки событий	critical

См. также

[Переменные Комплекса](#)

9.7. Описание полей событий

Для каждого события предусмотрен набор полей, в которых отображается уникальная для события информация.

Табл. 23. 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
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

Табл. 23. Основные поля событий

ПОЛЕ	ОПИСАНИЕ	ПРИМЕРЫ ЗНАЧЕНИЯ ПОЛЯ
recieve_time	Время регистрации события в Комплексе	11.05.2022 @ 18:45:06.123
description	Краткое описание события	Create incoming message
event_code	Идентификатор или классификатор типа события	1170004
event_type	Тип события	info_exchange
observer_id	ID регистратора события: ОЗ, сенсора или Комплекса	9429058a-835a-4f9e-a666-ee5799b33db0
observer_name	Сетевое имя регистратора события: ОЗ, сенсора или Комплекса	datapk-vm-tk2-test-244-36
id	Уникальный идентификатор события	019b35f6-2b98-47de-a3d0-c37c554029a6
observer_ip	IP-адрес регистратора события: ОЗ, сенсора или Комплекса	10.51.203.99
message	Исходное (оригинальное) событие	Выявлена ошибка подключения к активу 192.168.243.80 по MSRPC: rpc_s_access_denied
protocol	Протокол взаимодействия/API/ID канала инфообмена	ssh
receive_time	Время регистрации события на Комплексе	11.05.2022 @ 18:30:11.960
severity	Важность события	critical
listener	Наименование служебного источника событий	event_log_sensor
source_ip	IP-адрес отправителя (актива)	10.51.203.19
source_mac	MAC-адрес отправителя (актива)	00:50:56:B7:2C:3C
source_id	Идентификатор отправителя (актива)	f37b0f20-c1f5-4401-9240-0cfccd9daa58
source_hostname	Наименование отправителя (актива)	datapk-vm-tk2-test-244-36

Табл. 23. Основные поля событий

ПОЛЕ	ОПИСАНИЕ	ПРИМЕРЫ ЗНАЧЕНИЯ ПОЛЯ
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
type	Тип	event
user	Логин пользователя, инициировавшего событие	aivanov

9.8. Переменные Комплекса

Для Комплексов уровней 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. 24. Конфигурационные файлы с переменными и их расположение

ТИП КОМПЛЕКСА	НАБОР ПЕРЕМЕННЫХ	РАСПОЛОЖЕНИЕ ФАЙЛА С НАБОРОМ ПЕРЕМЕННЫХ
Комплекс уровня Management	Переменные файла <code>manager.env</code>	<code>/usr/share/udv/datapk/manager.env</code>
	Переменные сервиса <code>udv-prometheus</code>	<code>/etc/sysconfig/udv-prometheus</code>
	Переменные сервиса <code>udv-logstash</code>	<code>/etc/sysconfig/udv-logstash</code>
	Переменные сервиса <code>udv-opensearch</code>	<code>/etc/sysconfig/udv-opensearch</code>
	Переменные сервиса <code>udv-esper</code>	<code>/etc/sysconfig/udv-esper</code>
Комплекс уровня Sensor	Переменные файла <code>sensor.env</code>	<code>/usr/share/udv/datapk/sensor.env</code>

См. также

[Переменные Комплекса уровня Management](#)

[Переменные Комплекса уровня Sensor](#)

[Переменные службы обнаружения вторжений](#)

9.8.1. Переменные Комплекса уровня Management

Обязательные переменные файла `manager.env`

Переменные файла `manager.env` устанавливаются в директории `/usr/share/udv/datapk/manager.env`

Список обязательных переменных, содержащийся в файле `manager.env` Комплекса уровня Management, представлен в таблице ниже.

Табл. 25. 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
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 (host data collector).  ОСТОРОЖНО: Изменение значения переменной может привести к отсутствию доступа к базе данных.	dJ2ZOZeU0nJhHwjfhq10wF1x

Табл. 25. Обязательные переменные файла `manager.env`

ПЕРЕМЕННАЯ	ОПИСАНИЕ	ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ (ЖИРНЫМ), ЛИБО ПРИМЕР
<code>EVENT_INDICES_MAX_SIZE_GB</code>	Максимально допустимый объем оперативного архива. Суммарный объем с <code>EVENT_MANAGER_ARCHIVES_SIZE</code> 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
<code>EVENT_INDICES_ACTION_SIZE_EXCEEDED</code>	Действие в случае переполнения оперативного архива событий. Возможны два варианта значений переменной: <code>rotate</code> — записывать события в глубокий архив и <code>break</code> — прервать регистрацию событий	rotate
<code>EVENT_INDICES_LIFETIME_DAYS</code>	Время хранения событий в оперативном архиве, задается в днях	30
<code>EVENT_ARCHIVES_LIFETIME_DAYS</code>	Время хранения событий в глубоком архиве, события старше указанного значения удаляются. Значение задается в днях	60
<code>EVENT_ARCHIVES_MAX_SIZE_GB</code>	Максимально допустимый объем глубокого архива. Суммарный объем с <code>EVENT_MANAGER_EVENTS_SIZE</code> должен составлять не более 50-60% объема дискового пространства	5

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. 26. Дополнительные переменные файла manager.env

ПЕРЕМЕННАЯ	ОПИСАНИЕ	ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ (ЖИРНЫМ), ЛИБО ПРИМЕР
API_SKIP_FIRST_INITIALIZATION	Включение первичной инициализации при первом запуске Комплекса при значении переменной true	false
AUTOMATIC_HOST_CREATION_BY_MAC	Включение фильтрации создания неизвестных объектов защиты с IP и MAC-адресом (IP+MAC) при значении переменной true. При значении переменной false неизвестные Актив создаются и без IP-адреса (только MAC)	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 <i>Активы</i> становится серым. Значение задается в секундах.  Внимание: Значение 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

Табл. 26. Дополнительные переменные файла `manager.env`

ПЕРЕМЕННАЯ	ОПИСАНИЕ	ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ (ЖИРНЫМ), ЛИБО ПРИМЕР
<code>LDAP_CONNECTION_STRING</code>	IP-адрес LDAP-сервера Active Directory для создания пользователей из службы каталогов	<code>ldaps://192.168.243.121</code>
<code>LDAP_TLS</code>	Разрешить TLS-шифрование для Active Directory	<code>false</code>
<code>LOG_LEVEL</code>	Минимальная критичность системных событий, которые генерирует Комплекс уровня Management. Возможные значения: <code>CRITICAL</code> , <code>FATAL</code> , <code>ERROR</code> , <code>WARNING</code> , <code>INFO</code> , <code>DEBUG</code> , <code>NOTSET</code>	<code>INFO</code>
<code>MAX_ROWS_PER_REPORT</code>	Максимальное количество строк в отчетах. Значение по умолчанию — <code>1000</code> . Значения меньше или равные <code>1000</code> применяются для отчетов в формате <code>pdf</code> и <code>xls</code> . Значения больше <code>1000</code> применяются только для отчетов в формате <code>xls</code> , в <code>pdf</code> попадает только <code>1000</code> строк	<code>1000</code>
<code>DISABLE_HOST_DATA_COLLECTING_EVENTS</code>	При значении переменной <code>true</code> события сбора данных не собираются	<code>false</code>
<code>DISABLE_USER_ACTION_CONTROL_EVENTS</code>	При значении переменной <code>true</code> события о действиях пользователей не собираются	<code>false</code>
<code>DISABLE_HOST_CONTROL_EVENTS</code>	При значении переменной <code>true</code> события о появлении новых, изменении и удалении узлов не собираются	<code>false</code>
<code>DISABLE_AVAILABILITY_CONTROL_EVENTS</code>	При значении переменной <code>true</code> события о доступности узлов не собираются	<code>false</code>
<code>DISABLE_INCIDENT_CONTROL_EVENTS</code>	При значении переменной <code>true</code> события об инцидентах не собираются	<code>false</code>

Табл. 26. Дополнительные переменные файла `manager.env`

ПЕРЕМЕННАЯ	ОПИСАНИЕ	ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ (ЖИРНЫМ), ЛИБО ПРИМЕР
<code>DISABLE_BACKUP_CONTROL_EVENTS</code>	При значении переменной <code>true</code> события о резервном копировании не собираются	false
<code>USER_ACTION_CONTROL_EVENTS_SEVERITY</code>	Уровень критичности событий по действиям пользователей	low
<code>HOST_CONTROL_EVENTS_SEVERITY</code>	Уровень критичности событий появления новых узлов	low
<code>AVAILABILITY_CONTROL_EVENTS_SEVERITY</code>	Уровень критичности событий доступности узлов	low
<code>INCIDENT_CONTROL_EVENTS_SEVERITY</code>	Уровень критичности событий о создании, удалении, изменении инцидентов	low
<code>BACKUP_CONTROL_EVENTS_SEVERITY</code>	Уровень критичности событий резервного копирования	low
<code>NGINX_HTTPS_PORT</code>	Порт для подключения к Комплексу по протоколу HTTPS	443
<code>DISABLE_SURICATA_CONTROL_EVENTS</code>	При значении переменной <code>true</code> события службы обнаружения вторжений не собираются	false
<code>DISABLE_HOME_NET_SCAN_CONTROL_EVENTS</code>	При значении переменной <code>true</code> события при сканировании контролируемой сети не собираются	false
<code>DISABLE_SYSTEM_CONTROL_EVENTS</code>	При значении переменной <code>true</code> системные события не собираются	false
<code>EVENT_CONTROL_EVENTS_SEVERITY</code>	Уровень критичности для событий, полученных от сервиса регистрации событий	critical
<code>HOME_NET_SCAN_CONTROL_EVENTS_SEVERITY</code>	Уровень критичности для событий, полученных при сканировании контролируемой сети	low

Табл. 26. Дополнительные переменные файла `manager.env`

ПЕРЕМЕННАЯ	ОПИСАНИЕ	ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ (ЖИРНЫМ), ЛИБО ПРИМЕР
<code>SYSTEM_CONTROL_EVENTS_SEVERITY</code>	Уровень критичности для системных событий	low
<code>EVENT_ARCHIVES_ACTION_SIZE_EXCEEDED</code>	Действие, выполняемое при превышении лимита на размер глубокого архива. Возможные значения переменной: • <code>nothing</code> • <code>break</code> • <code>rotate</code>	rotate
<code>USER_SESSION_INACTIVITY_TIMEOUT</code>	Ограничение сессии при отсутствии активности пользователя. Значение переменной задается в секундах	600
<code>ENABLE_DNS_PINNING_PROTECTION</code>	Включение защиты от атаки Anti DNS Pinning. При значении переменной <code>true</code> веб-сервер будет отправлять 404 ошибку, если запрос пришел на адрес, не равный CN серверного сертификата	false

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. 27. Список переменных сервиса `udv-esper`

ПЕРЕМЕННАЯ	ОПИСАНИЕ	ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ (ЖИРНЫМ), ЛИБО ПРИМЕР
<code>ESPER_RMQ_MAX_QUEUE_SIZE</code>	Максимальная длина очереди событий Syslog и событий службы обнаружения вторжений. Задается в байтах	100000

Табл. 27. Список переменных сервиса udv-esper

ПЕРЕМЕННАЯ	ОПИСАНИЕ	ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ (ЖИРНЫМ), ЛИБО ПРИМЕР
ESPER_JAVA_OPTS	Объем оперативной памяти, выделяемой под сервис корреляции событий. Задается в мегабайтах	- Djava.net.preferIPv4Stack=true-Dlog4j2.formatMsgNoLookups=true-Xmx1024m

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. 28. 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
ESPER_PORT	Порт сервиса корреляции событий	517
LS_JAVA_OPTS	Объем оперативной памяти, выделяемой под сервис udv-logstash. Задается в мегабайтах	-Dlog4j2.formatMsgNoLookups=true-Xmx1024m-Xms1024m

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. 29. Список переменных сервиса `udv-opensearch`

ПЕРЕМЕННАЯ	ОПИСАНИЕ	ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ (ЖИРНЫМ), ЛИБО ПРИМЕР
<code>ES_JAVA_OPTS</code>	Объем оперативной памяти, выделяемой под сервис <code>udv-opensearch</code> . Задается в мегабайтах	-Dlog4j2.formatMsgNoLookups=true-Xmx1024m-Xms1024m

Переменные сервиса `udv-vector-manager`

Переменные сервиса `udv-vector-manager` устанавливаются в директории `/etc/sysconfig/udv-vector-manager`

Список переменных сервиса `udv-vector-manager` Комплекса уровня Management представлен в таблице ниже.

Табл. 30. Список переменных сервиса `udv-vector-manager`

ПЕРЕМЕННАЯ	ОПИСАНИЕ	ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ (ЖИРНЫМ), ЛИБО ПРИМЕР
<code>MANAGER_NETWORK_GATEWAY</code>	Адрес для отправки данных в сервис <code>udv-clickhouse</code>	127.0.0.1

Переменные сервиса `udv-vector-sensor`

Переменные сервиса `udv-vector-sensor` устанавливаются в директории `/etc/sysconfig/udv-vector-sensor`

Список переменных сервиса `udv-vector-sensor` Комплекса уровня Management представлен в таблице ниже.

Переменные сервиса `udv-zeek-backend`

Переменные сервиса `udv-zeek-backend` устанавливаются в директории `/etc/sysconfig/udv-zeek-backend`

Список переменных сервиса `udv-zeek-backend` Комплекса уровня Management представлен в таблице ниже.

Табл. 31. Список переменных сервиса `udv-zeek-backend`

ПЕРЕМЕННАЯ	ОПИСАНИЕ	ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ (ЖИРНЫМ), ЛИБО ПРИМЕР
<code>DPI_PASSWORD_CAPTURE</code>	Извлечение паролей из трафика по протоколу HTTP при значении <code>true</code>	false

См. также

Рекомендации по использованию переменных файла `.env`

9.8.2. Переменные Комплекса уровня Sensor

Переменные файла `sensor.env`

Переменные файла `sensor.env` устанавливаются в директории `/usr/share/udv/datapk/sensor.env`

Список переменных, содержащийся в файле `sensor.env` Комплекса уровня Sensor, представлен в таблице ниже.

Табл. 32. Переменные файла `sensor.env`

ПЕРЕМЕННАЯ	ОПИСАНИЕ	ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ (ЖИРНЫМ), ЛИБО ПРИМЕР
<code>ARCHIVE_COMPRESS_LOG</code>	Перевод создаваемых копий журналов событий сервиса <code>udv-zeek</code> в сжатый формат хранения при значении <code>true</code>.  ОСТОРОЖНО: Изменение значения переменной может привести к отказу в работе а.	true

Табл. 32. Переменные файла `sensor.env`

ПЕРЕМЕННАЯ	ОПИСАНИЕ	ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ (ЖИРНЫМ), ЛИБО ПРИМЕР
ARCHIVE_COPY_LOG	Создание копии журналов событий сервиса <code>udv-zeek</code> при значении <code>true</code>.  ОСТОРОЖНО: Изменение значения переменной может привести к отказу в работе а.	false
BUFFER_SIZE	Размер буфера одного обработчика в сервисе <code>udv-vector-manager</code> (один обработчик — один протокол). Задается в байтах	268435488
DEBUG_MODE	Перевод сервиса <code>udv-dns-classifier</code> в debug-режим при значении <code>true</code>. При этом модели сервиса сохраняют на диск датафреймы с результатами работы.  ОСТОРОЖНО: Изменение значения переменной может привести к отказу в работе а.	false
DGA_ANOMALY_THRESHOLD	Граница вероятности, с которой DGA-события отправляются в сервис <code>udv-event-manager</code>	0.75
DGA_LOG_THRESHOLD	Граница вероятности, с которой события считаются DGA	0.75
ENRICH_PROCESSOR_MAC_IP_SEARCH	Переключение режима обогащения: «по MAC + IP» — при значении <code>true</code> ; «только по IP» — при значении <code>false</code>	true
REQUEST_ANOMALY_THRESHOLD	Граница вероятности, с которой события <code>dns_request</code> отправляются в сервис <code>udv-event-manager</code>	0.5

Табл. 32. Переменные файла `sensor.env`

ПЕРЕМЕННАЯ	ОПИСАНИЕ	ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ (ЖИРНЫМ), ЛИБО ПРИМЕР
<code>REQUEST_LOG_THRESHOLD</code>	Граница вероятности, с которой события считаются туннелями для <code>dns-request</code> -модели	0.5
<code>RESPONSE_ANOMALY_THRESHOLD</code>	Граница вероятности, с которой события <code>dns_response</code> отправляются в сервис <code>udv-event-manager</code>	0.75
<code>RESPONSE_LOG_THRESHOLD</code>	Граница вероятности, с которой события считаются туннелями для <code>dns-response</code> -модели	0.75
<code>SESSION_RULES_ENABLED</code>	Статус сервиса правил сессий <code>udv-rules-backend</code> : сервис работает — при значении <code>true</code> ; сервис отключен — при значении <code>false</code>	true

См. также

[Рекомендации по использованию переменных файла `.env`](#)

[Переменные службы обнаружения вторжений](#)

9.8.3. Рекомендации по использованию переменных файла `.env`

Не все доступные для использования переменные, которые могут быть в `env`-файле, 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.

Соблюдение предложенного формата переменных объема обязательно. Варианты написания `10GB` или `10 Gb` некорректны и неизбежно повлекут за собой ошибки. Примеры корректных вариантов:

- `EVENT_INDICES_LIFETIME_DAYS=30d`
- `EVENT_ARCHIVES_LIFETIME_DAYS=45d`
- `EVENT_MANAGER_ARCHIVES_SIZE=500 GB`

Список остальных рекомендаций приведен в таблице ниже ([Таблица 33. Рекомендации по использованию переменных файла .env](#)).

Табл. 33. Рекомендации по использованию переменных файла .env

ПЕРЕМЕННАЯ	РЕКОМЕНДАЦИИ ПО ИСПОЛЬЗОВАНИЮ	ПРИМЕНИМО ДЛЯ УРОВНЯ КОМПЛЕКСА
<code>EVENT_INDICES_MAX_SIZE_GB</code>	Суммарный объем с <code>EVENT_ARCHIVES_MAX_SIZE_GB</code> не должен составлять более 50-60% объема дискового пространства. На ах базового уровня и (или) с HDD — не более 100 ГБ. На ах среднего и верхнего уровней с SSD — не более 300 ГБ	Management
<code>EVENT_ARCHIVES_MAX_SIZE_GB</code>	Суммарный объем с <code>EVENT_INDICES_MAX_SIZE_GB</code> должен составлять не более 50-60% объема дискового пространства	Management
<code>EVENT_INDICES_LIFETIME_DAYS</code>	Установите адекватную системе длительность хранения оперативного архива	Management
<code>EVENT_ARCHIVES_LIFETIME_DAYS</code>	Установите значение на 1-2 дня больше, чем <code>EVENT_INDICES_LIFETIME_DAYS</code>	Management
<code>MANAGER_NODE_ADDRESS</code>	Значение должно совпадать с <code>BACKEND_NETWORK_GATEWAY</code> Комплекса уровня Management	Sensor

См. также

[Переменные Комплекса](#)

9.9. Основные переменные файла environment.json

Список переменных, содержащийся в файле `environment.json`, вы можете видеть в таблице ([Таблица 34. Переменные файла environment.json](#)).

Табл. 34. Переменные файла environment.json

ПЕРЕМЕННАЯ	ОПИСАНИЕ	ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ
mainPage	Ссылка на стартовую страницу.  Прим.: По умолчанию, если значение переменной не заполнено, стартовой будет страница Инспекция сети → Карта сети. Примером изменения стартовой страницы на Активы будет значение переменной <code>"/app/operational_data/hosts"</code>.	нет значения
showMaps	Доступ к странице Карта сети .	true
showKibanaEvents	Доступ к страницам Индексы и События → Экспертный режим .	
showCorrelation	Доступ к странице Правила корреляции.  Внимание: При значении переменной <code>false</code> доступ к странице Администрирование → События и инциденты → Оповещения об инцидентах запрещен вне зависимости от значения переменной <code>showAlerting</code>.	
showIncidentStatuses	Доступ к странице Статусы инцидентов .	

Табл. 34. Переменные файла environment.json

ПЕРЕМЕННАЯ	ОПИСАНИЕ	ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ
<code>showIncidents</code>	Доступ к странице Инциденты .	
<code>showDataFlows</code>	Доступ к странице Администрирование → События и инциденты → Правила корреляции .	
<code>showSuricata</code>	Доступ к странице Правила обнаружения .	
<code>showAlerting</code>	Доступ к странице Администрирование → События и инциденты → Оповещения об инцидентах .	
<code>esperRetroEnabled</code>	Доступ к странице События и инциденты → Ретроанализ .	

9.10. 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](#)

9.11. 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](#)

9.11.1. 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.

Информационные панели: [Эксплуатационный мониторинг](#) | [Главный дашборд](#)

Рис. 227. Информационная панель

9.11.2. 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).

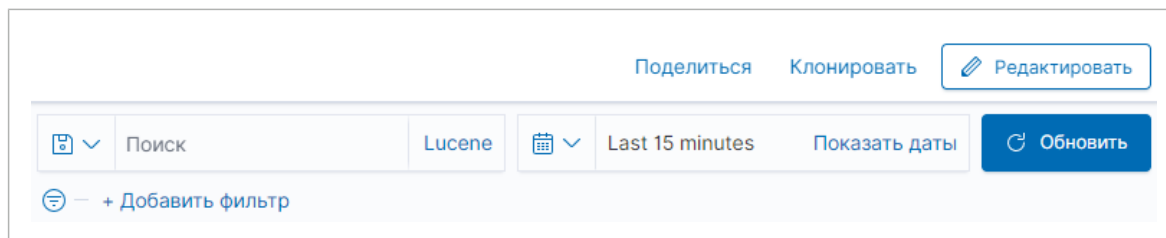


Рис. 228. Инструменты для управления страницами мониторинга

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.

9.11.2.1. 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 -).

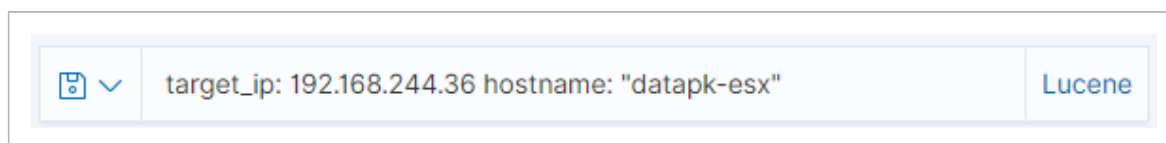


Рис. 229. Пример поискового запроса

9.11.2.2. 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.

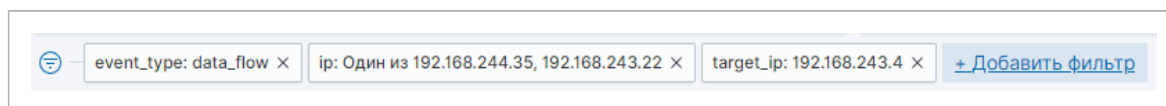


Рис. 230. Панель фильтров

Существует два способа создания фильтра:

1. При помощи кнопки «+Добавить фильтр»;
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 сохраняются.



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.

9.11.3. 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.

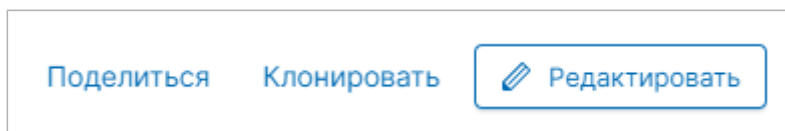


Рис. 231. Кнопки управления интерфейсом визуализации

Их можно увидеть на всех страницах раздела мониторинга:

- **Поделиться** — позволяет поделиться страницей мониторинга в виде элемента iframe или ссылки. Содержимое может быть как интерактивным, так и в виде статичного снимка.

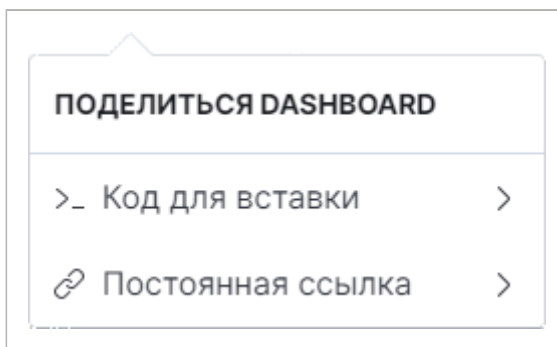


Рис. 232. Меню, позволяющее поделиться содержимым страницы

- **Клонировать** позволяет создать копию страницы панели мониторинга. В настройках можно задать имя скопированной страницы.

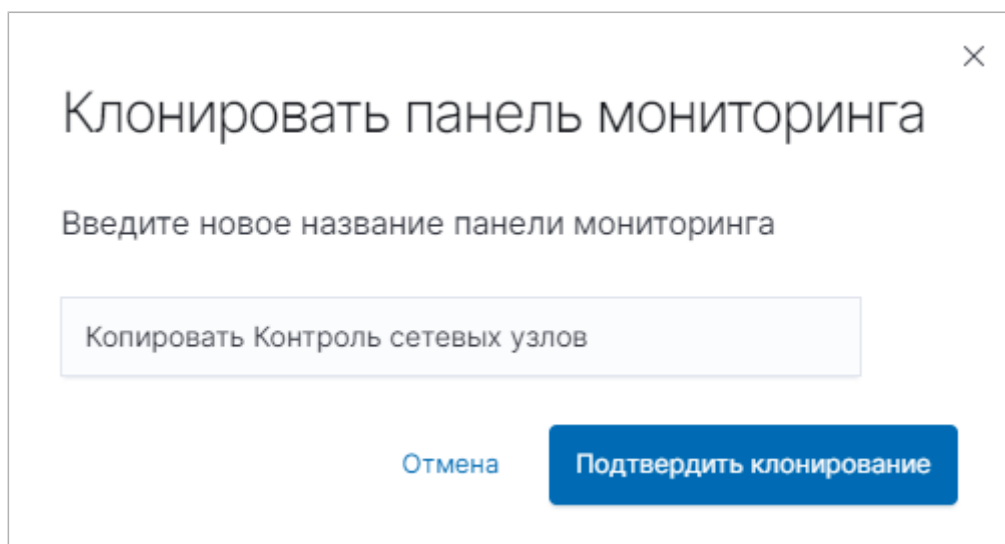


Рис. 233. Окно «Клонировать панель мониторинга»

- **Редактировать** — 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».

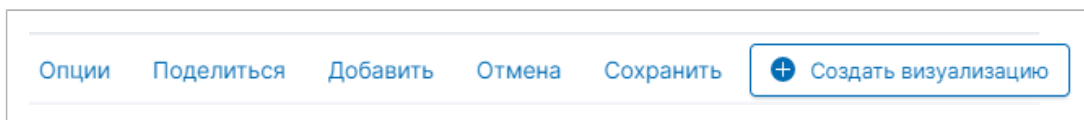


Рис. 234. Редактирование панели мониторинга

9.11.4. 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.

9.11.4.1. Графики

На страницах мониторинга графики помогают отследить появление аномалий по количеству событий во времени.

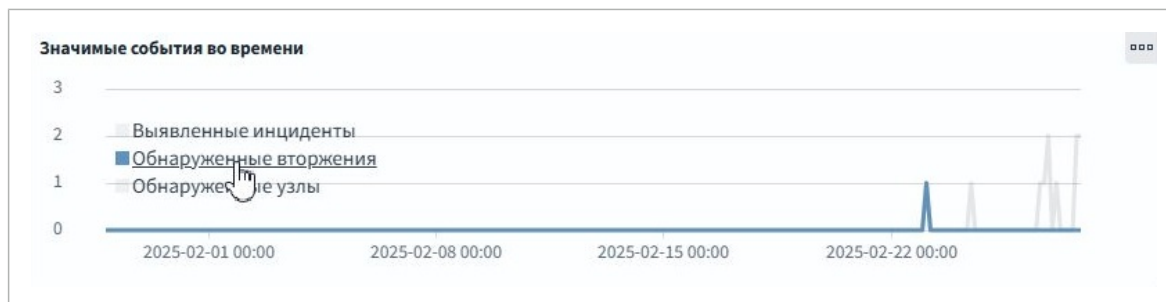


Рис. 235. Пример графика

Графики поддерживают следующие возможности:

- скрывание 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.

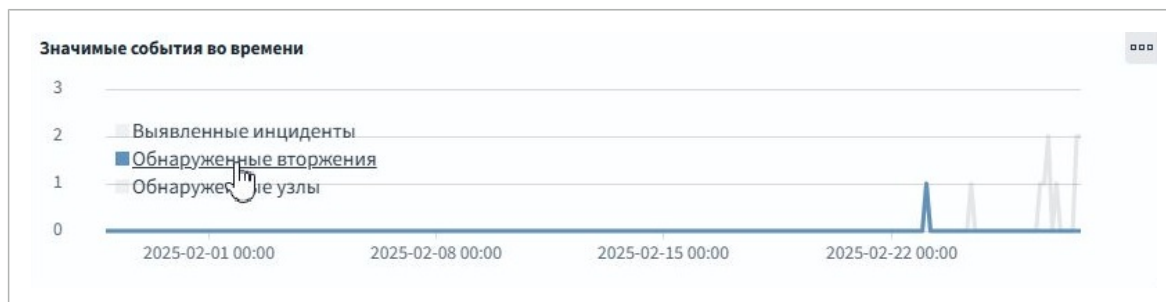


Рис. 236. Выбор одного типа событий для его отображения на графике

Для скрывания 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.

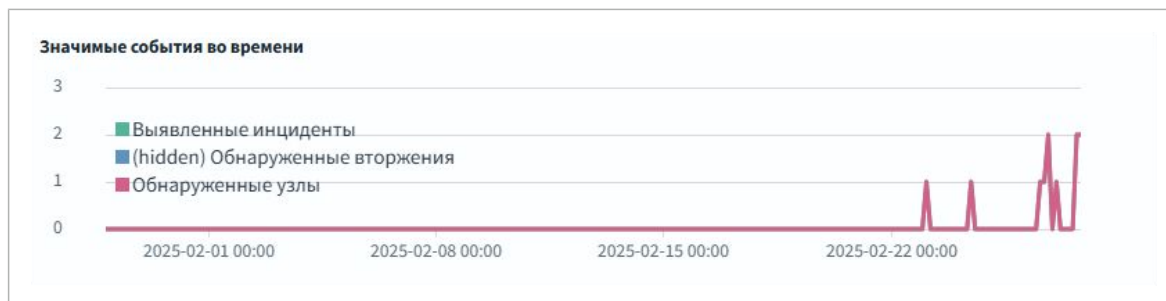


Рис. 237. Вид графика после того, как «Выявленные инциденты» были скрыты

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.

9.11.4.2. Круговые диаграммы

Круговые диаграммы используются для быстрого просмотра изменений в следующих разделах: контроль потоков данных, обнаружение вторжений, контроль конфигураций, инциденты ИБ.

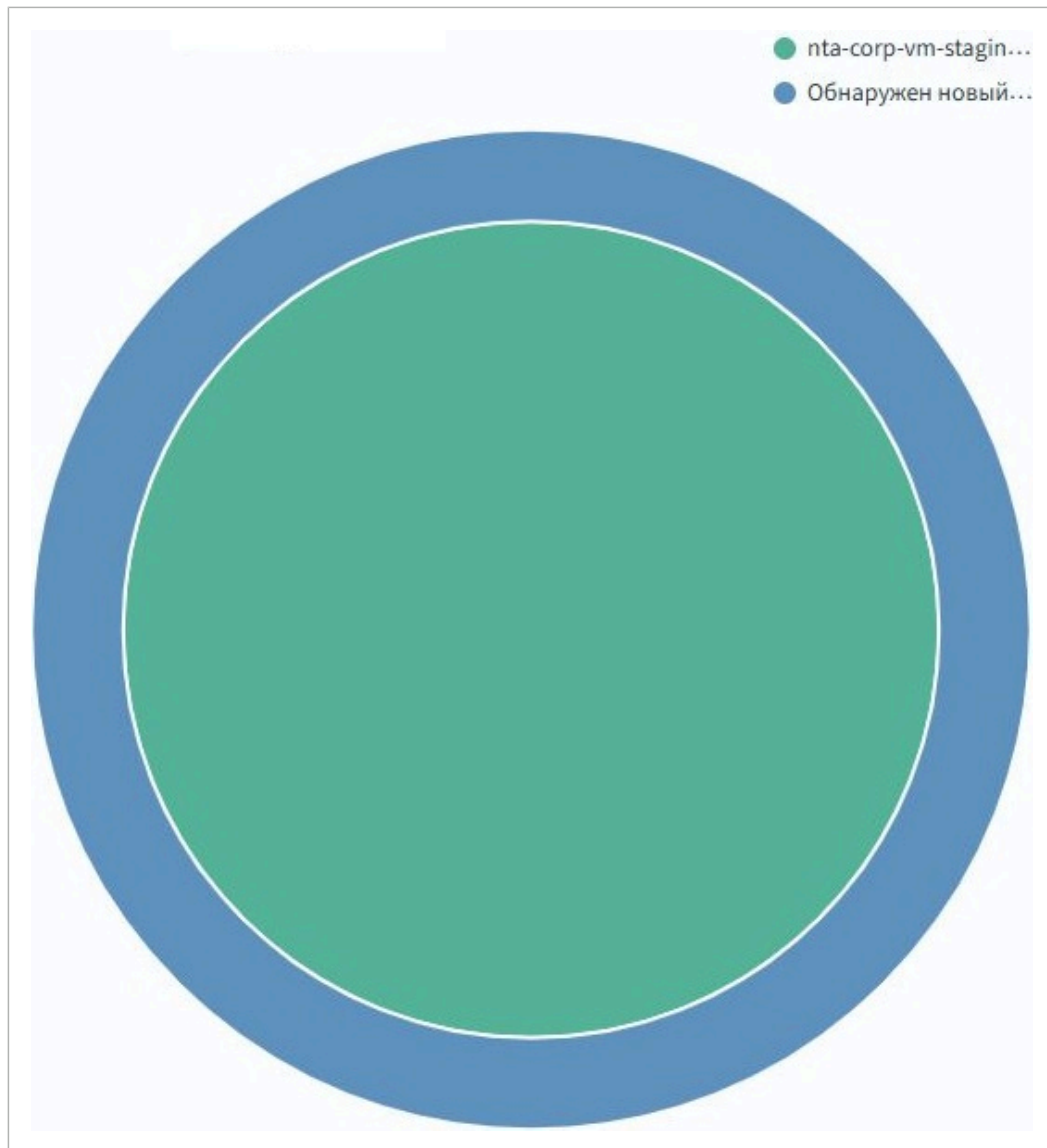


Рис. 238. Пример круговой диаграммы

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 объекта защиты, 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. 239. Просмотр информации об элементе круговой диаграммы

9.11.4.3. Столбчатые диаграммы

Столбчатые диаграммы используются на следующих страницах: обнаружение вторжений, контроль сессий, 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.

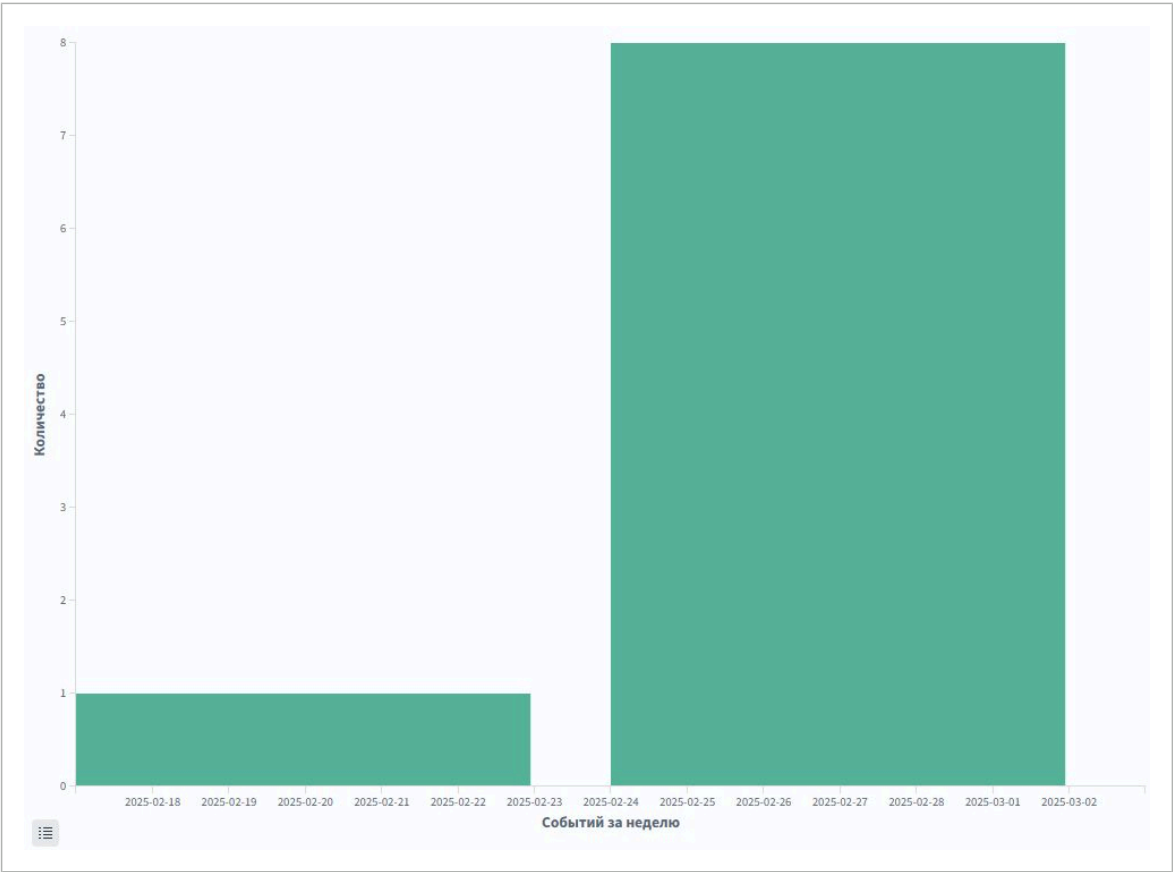


Рис. 240. Пример столбчатой диаграммы

9.11.4.4. Таблицы

В разделе мониторинга событий визуализации в виде таблиц используются для первичного анализа событий по различным критериям. Вид таблиц отличается от основного интерфейса Комплекса.

Изменение состояния актива					
Сенсор	Название узла	Описание	IP адрес	MAC адрес	Кол-во
nta-corp-vm-staging-244-46	Неизвестный актив	Интерфейс недоступен	192.168.2.2	00:50:56:b7:8a:8d	1
nta-corp-vm-staging-244-46	Неизвестный актив	Интерфейс недоступен	192.168.1.4	00:50:56:b7:25:ef	1
nta-corp-vm-staging-244-46	Неизвестный актив	Интерфейс недоступен	192.168.1.3	00:50:56:b7:ce:c6	1
nta-corp-vm-staging-244-46	Неизвестный актив	Интерфейс недоступен	10.51.244.46	00:50:56:b7:b2:b7	5
nta-corp-vm-staging-244-46	Неизвестный актив	Интерфейс недоступен	10.51.15.81	30:c5:0f:c8:09:fd	1
nta-corp-vm-staging-244-46	Неизвестный актив	Доступность интерфейса восст:	10.51.244.46	00:50:56:b7:b2:b7	3
nta-corp-vm-staging-244-46	WinCC	Интерфейс недоступен	10.51.244.26	00:50:56:b7:f6:8b	4
nta-corp-vm-staging-244-46	WinCC	Доступность интерфейса восст:	10.51.244.26	00:50:56:b7:f6:8b	4
nta-corp-vm-staging-244-46	Win2KSP4_TK1	Интерфейс недоступен	10.51.244.255	ff:ff:ff:ff:ff:ff	1

Рис. 241. 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**).

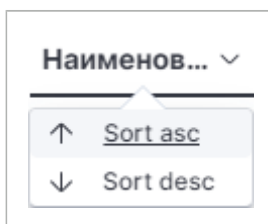


Рис. 242. Выбор в таблице способа сортировки значений столбца

- Создание фильтров по значениям из таблицы. Подробнее см. в разделе «[Фильтр по значениям из таблицы](#)».

9.12. Сетевые взаимодействия Комплексов

В таблице (Таблица 35. Сетевые взаимодействия Комплексов)представлены сетевые взаимодействия Комплексов.

Порты назначения указаны в формате: [TCP или UDP] [номер порта TCP или UDP] ([протокол или сервис назначения])

Табл. 35. Сетевые взаимодействия Комплексов

ИСТОЧНИК ТРАФИКА	ПОРТ НАЗНАЧЕНИЯ (ДЛЯ ВНЕШНИХ АКТИВОВ И СИСТЕМ ПРИВЕДЕНЫ ПОРТЫ ПО УМОЛЧАНИЮ)	УЗЕЛ НАЗНАЧЕНИЯ	НАЗНАЧЕНИЕ ТРАФИКА
UDV NTA уровня Sensor	TCP 20044 (udv-files-backend)	UDV NTA уровня Management	Получение извлеченных из сети файлов
	TCP 20085 (udv-steno-backend)		Получение копии сетевого трафика
	TCP 20104 (udv-vector)		Получение метаданных сетевого трафика
	TCP 16379 (udv-redis) – синхронизация настроек; TCP 19091 (udv-prometheus) – метрики; TCP 15673 (udv-rabbitmq) – получение данных; UDP 123 (если Management выступает в роли NTP-сервера для Sensor)		Взаимодействие уровня Sensor с уровнем Management. Иницирует 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

Табл. 35. Сетевые взаимодействия Комплексов

ИСТОЧНИК ТРАФИКА	ПОРТ НАЗНАЧЕНИЯ (ДЛЯ ВНЕШНИХ АКТИВОВ И СИСТЕМ ПРИВЕДЕНЫ ПОРТЫ ПО УМОЛЧАНИЮ)	УЗЕЛ НАЗНАЧЕНИЯ	НАЗНАЧЕНИЕ ТРАФИКА
Активы, поддерживающие передачу событий через стандарт syslog/SNMP-trap	UDP 514 (Syslog 3164) UDP 515 (Syslog 5424) TCP 514 (Syslog 3164 TCP) TCP 515 (Syslog 5424 TCP) UDP 162 (SNMP-trap)	UDV NTA уровня Sensor	Пассивный сбор событий от активов
UDV NTA уровня Sensor (опционально) UDV NTA уровня Management	UDP 123 (NTP)	NTP-серверы	Синхронизация времени
UDV NTA уровня Management	UDP 514 TCP 514 TCP 25 (SMTP) TCP 465 (SMTPS)	Смежная система	Отправка событий и почтовых уведомлений в смежные системы
UDV NTA уровня Management	TCP 389 (LDAP) или TCP 636 (LDAPS)	LDAP-сервер	Для возможности авторизации пользователей UDV NTA через службу каталогов

Табл. 35. Сетевые взаимодействия Комплексов

ИСТОЧНИК ТРАФИКА	ПОРТ НАЗНАЧЕНИЯ (ДЛЯ ВНЕШНИХ АКТИВОВ И СИСТЕМ ПРИВЕДЕНЫ ПОРТЫ ПО УМОЛЧАНИЮ)	УЗЕЛ НАЗНАЧЕНИЯ	НАЗНАЧЕНИЕ ТРАФИКА
АРМ административного персонала	TCP 443 (HTTPS) TCP 22 (SSH)	UDV NTA уровня Management	Администрирование UDV NTA. SSH — для сервисного обслуживания в терминале операционной системы
	TCP 22 (SSH)	UDV NTA уровня Sensor	Администрирование UDV NTA (сервисное обслуживание)

9.13. 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 36. Команды, используемые в примере синтаксиса EPL).

Табл. 36. 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.
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.

Табл. 36. Команды, используемые в примере синтаксиса EPL

КОМАНДА	ПЕРЕВОД НАЗВАНИЯ	ОПИСАНИЕ
.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.

9.13.1. Поддерживаемые типы событий

Для создания правил корреляции необходимо добавлять поля данных, по которым будут происходить запросы. Доступны следующие типы событий:

- События, генерируемые Комплексом:
 - события сканирования контролируемой сети (home_net);
 - события изменения статуса доступности интерфейсов (host_interface_status_changed);
 - результаты проверок на соответствие требованиям ИБ (oval_event);
 - события контроля тегов промышленных протоколов (tag_control);
 - события правил сессий (session_control);
 - события обнаружения сетевых атак (dpi_notice);
 - события обнаружения DNS-туннелирования (ml_notice);
 - события системы обнаружения вторжений (ids_event);
 - события системы контроля версий (version_control);
 - системные события (system_event);
 - события проверки контрольных сумм (checksum);
- События KICS4Net (kics4net_event);
 - Потоки KICS4Net(kics4net_data_flow);
- События Cisco (cisco_event);
- События Kaspersky (kaspersky_event);
- События DrWeb (drweb_event);
- События RuggedCOM (ruggedcom_event);
- События Eltex (eltex_event);
- События FortiGate (fortigate_event);
- События HoneyPot (honeypot_event);
- События Inzer (inzer_event);
- События Nateks (nateks_event);
- События KICS4Nodes (kics4nodes_event);
- События Huawei (huawei_event);
- События UserGate (usergate_event);
- События БАСТИОН (bastion_event);
- События HP (hp_event);
- События OPNsense (opnsense_event);
- События Zelax (zelax_event);
- События АПКШ «Континент» (kontinent_event)
- События Linux (linux_event);

- События Hirschmann (`hirschmann_event`);
- События Enterasys (`enterasys_event`);
- События MOXA (`moxa_event`);
- События, полученные по Syslog (`unknown_syslog_event`).

9.13.1.1. Ключевые поля для выборки

Следующие поля (Таблица 37. Обязательные поля) являются обязательными при создании правила корреляции, так как данная информация необходима для создания инцидента.

Табл. 37. Обязательные поля

ПОЛЕ	ОПИСАНИЕ
observer_id	Уникальный идентификатор регистратора события: сенсора, зафиксировавшего событие, либо объекта защиты, либо Комплекса
id	Уникальный идентификатор события

9.13.1.2. События Комплекса

Общие поля для событий Комплекса

Общие поля для событий Комплекса приведены в таблице ниже. (Таблица 38. Общие поля для событий Комплекса)

Табл. 38. Общие поля для событий Комплекса

ПОЛЕ	ОПИСАНИЕ
observer_name	Сетевое имя регистратора события: Актив, сенсора или Комплекса
observer_ip	IP-адрес регистратора события: Актив, сенсора или Комплекса
event_code	Идентификатор события
event_type	Тип события

Резервное копирование данных (backup_control)

Поля для событий резервного копирования приведены в таблице ниже (Таблица 39. Поля для событий резервного копирования).

Табл. 39. Поля для событий резервного копирования

ПОЛЕ	ОПИСАНИЕ
additional_information	Обоснование действия (комментарий) и изменившееся значение

Табл. 39. Поля для событий резервного копирования

ПОЛЕ	ОПИСАНИЕ
description	Описание выполненного действия
justification	Обоснование выполненного действия
user	Пользователь Комплекса, который выполнил действие
target_hostname	Сетевое имя Комплекса
target_id	Идентификатор Комплекса

Поток данных (datapk_data_flow)

Поля для событий потоков данных приведены в таблице ниже (Таблица 40. Поля для событий потоков данных).

Табл. 40. Поля для событий потоков данных

ПОЛЕ	ОПИСАНИЕ
action	Произведенное действие. Возможны следующие варианты: detect или delete
additional_information	Дополнительные данные при автоматическом одобрении (состояние, комментарий, наименование правила)
description	Описание события
protocol	Сетевой протокол передачи данных.  Внимание: Сетевой протокол указывается строчными буквами.
source_ip	IP-адрес источника потока данных
source_mac	MAC-адрес источника потока данных.  Внимание: MAC-адрес источника указывается заглавными буквами.
source_port	Порт источника потока данных

Табл. 40. Поля для событий потоков данных

ПОЛЕ	ОПИСАНИЕ
target_ip	IP-адрес получателя потока данных
target_mac	MAC-адрес получателя потока данных.  Внимание: MAC-адрес получателя указывается заглавными буквами.
target_port	Порт получателя потока данных
user	Имя пользователя, выполнившего удаление или создавшего правило одобрения

Действие пользователя (user_action_detected)

Поля для событий действий пользователя приведены в таблице ниже (Таблица 41. Поля для событий о действиях пользователя).

Табл. 41. 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

Аутентификация (appliance_authentication)

Поля для событий аутентификации в Комплексе приведены в таблице ниже (Таблица 43. Поля для событий о состоянии конфигурации актива).

Табл. 42. 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

Действия с эталонным состоянием конфигурации актива (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 43. Поля для событий о состоянии конфигурации актива).

Табл. 43. Поля для событий о состоянии конфигурации актива

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 Актив
target_hostname	Сетевое имя Актив, на котором обнаружено нарушение эталонного состояния конфигурации
user	Имя пользователя, который изменил эталонную конфигурацию

Обнаружение неизвестного актива (datapk_unknown_host_detected)

Поля для событий обнаружения неизвестных активов приведены в таблице ниже (Таблица 44. Поля для событий обнаружения неизвестного актива).

Табл. 44. Поля для событий обнаружения неизвестного актива

ПОЛЕ	ОПИСАНИЕ
description	Описание события
target_ip	IP-адрес обнаруженного Актив
target_mac	MAC-адрес обнаруженного Актив  Внимание: MAC-адрес обнаруженного Актив указывается заглавными буквами.

Обнаружение действия пользователя с активом (host_user_action_detected)

Поля для событий о действиях пользователей с активами приведены в таблице ниже (Таблица 45. Поля для событий о действиях пользователя с активом).

Табл. 45. 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 Актив
target_ip	IP-адрес Актив, с которым производят манипуляции
target_hostname	Сетевое имя Актив, с которым производят манипуляции
target_mac	MAC-адрес Актив, с которым производят манипуляции  Внимание: MAC-адрес Актив указывается заглавными буквами.

Изменение статуса доступности актива (availability_control)

Поля для событий о статусе доступности активов приведены в таблице ниже (Таблица 46. Поля для событий статуса доступности актива).

Табл. 46. Поля для событий статуса доступности актива

ПОЛЕ	ОПИСАНИЕ
description	Описание доступности интерфейса
target_ip	IP-адрес Актив, у которого происходит изменение статуса доступности
target_hostname	Сетевое имя Актив, у которого происходит изменение статуса доступности
target_mac	MAC-адрес Актив, у которого происходит изменение статуса доступности  Внимание: MAC-адрес указывается заглавными буквами.

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 47. Поля для событий о подключениях к активу).

Табл. 47. Поля для событий о подключениях к активу

ПОЛЕ	ОПИСАНИЕ
additional_information	Дополнительные данные (что изменено, ошибки запуска)
description	Описание и перечень Актив, 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
user	Имя пользователя, который производит действия с задачами

Результат проверок на соответствие требованиям ИБ (oval_event)

Поля для событий о проверках приведены в таблице ниже (Таблица 48. Поля для событий о результатах проверок на соответствие требованиям ИБ).

Табл. 48. 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 -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

Верификация импортированного Python-скрипта (script_verification_event)

Поля для событий верификации скриптов приведены в таблице ниже (Таблица 49. Поля для событий верификации Python-скриптов).

Табл. 49. Поля для событий верификации Python-скриптов

ПОЛЕ	ОПИСАНИЕ
additional_information	Вывод ошибки
category	Название сканера, который содержит проверяемый Python-скрипт
description	Описание события Комплекса

Табл. 49. Поля для событий верификации Python-скриптов

ПОЛЕ	ОПИСАНИЕ
request_id	Идентификатор запроса
user	Имя пользователя, который производит манипуляции со сканером
target_hostname	Сетевое имя регистратора события: Актива, сенсора или Комплекса
target_id	ID регистратора события: Актива, сенсора или Комплекса

Контроль событий Комплекса (event_control)

Поля для контроля событий Комплекса приведены в таблице ниже (Таблица 50. Поля для контроля событий Комплекса).

Табл. 50. Поля для контроля событий Комплекса

ПОЛЕ	ОПИСАНИЕ
description	Описание события Комплекса
protocol	Идентификатор источника
source_hostname	Сетевое имя Актива
source_ip	IP-адрес Актива
target_hostname	Сетевое имя объекта, над которым выполнялось действие: Актив, сенсор или Комплекса
target_id	ID объекта, над которым выполнялось действие: Актива, сенсора или Комплекса

События контроля инцидентов (incident_control_event)

Поля для контроля инцидентов приведены в таблице ниже (Таблица 51. Поля для событий контроля инцидентов).

Табл. 51. Поля для событий контроля инцидентов

ПОЛЕ	ОПИСАНИЕ
additional_information	Служебные поля инцидента (например, наименование правила корреляции)
description	Описание выполненного действия
justification	Обоснование выполненного действия

Табл. 51. Поля для событий контроля инцидентов

ПОЛЕ	ОПИСАНИЕ
incident_id	Идентификатор созданного или измененного инцидента
link	Все ID событий, на основе которых сформирован инцидент
target_ip	Все IP-адреса из событий, на основе которых сформирован инцидент.  Прим.: 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 службы обнаружения вторжений (suricata_event)

Поля для событий службы обнаружения вторжений приведены в таблице ниже (Таблица 52. Поля для событий службы обнаружения вторжений).

Табл. 52. Поля для событий службы обнаружения вторжений

ПОЛЕ	ОПИСАНИЕ
action	Действие службы обнаружения вторжений.  Прим.: Берется из поля action правила службы обнаружения вторжений.

Табл. 52. Поля для событий службы обнаружения вторжений

ПОЛЕ	ОПИСАНИЕ
category	Категория события службы обнаружения вторжений.  Прим.: 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.  Прим.: Берется из поля app_proto правила службы обнаружения вторжений.
source_ip	IP-адрес отправителя сетевых пакетов
source_port	Порт, по которому отправлены сетевые пакеты
target_ip	IP-адрес получателя сетевых пакетов
target_port	Порт, на который отправлены сетевые пакеты

9.13.1.3. События KICS4Net

Потоки KICS4Net(kics4net_data_flow)

Поля для событий потоков KICS4Net приведены в таблице ниже (Таблица 53. Поля для событий потоков KICS4Net).

Табл. 53. Поля для событий потоков KICS4Net

ПОЛЕ	ОПИСАНИЕ
category	Наименование точки мониторинга.
description	Описание потока.
event_code	Идентификатор типа события в KICS4Net.

Табл. 53. Поля для событий потоков KICS4Net

ПОЛЕ	ОПИСАНИЕ
observer_name	Сетевое имя регистратора события: ОЗ (сервера KICS4Net), сенсора или Комплекса.
observer_id	IP-адрес регистратора события: ОЗ (сервера KICS4Net), сенсора или Комплекса.
protocol	Название протокола.
source_ip	IP-адрес источника потока данных.
source_mac	MAC-адрес источника потока данных.  Внимание: MAC-адрес указывается заглавными буквами.
source_port	Порт источника потока данных.
target_ip	IP-адрес получателя потока данных.
target_mac	MAC-адрес источника потока данных.  Внимание: MAC-адрес указывается заглавными буквами.
target_port	Порт получателя потока данных.

События KICS4Net (kics4net_event)

Поля для событий KICS4Net приведены в таблице ниже (Таблица 54. Поля для событий KICS4Net).

Табл. 54. Поля для событий KICS4Net

ПОЛЕ	ОПИСАНИЕ
additional_information	Название сработавшего правила или значение noTrafficDuration.
category	Наименование точки мониторинга.
description	Описание потока.

Табл. 54. Поля для событий KICS4Net

ПОЛЕ	ОПИСАНИЕ
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.  Внимание: MAC-адрес указывается заглавными буквами.
target_port	Порт получателя потока данных.

9.13.1.4. События Linux

Доступные для событий Linux поля приведены в таблице ниже (Таблица 55. Поля для событий Linux).

Табл. 55. 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.

Табл. 55. Поля для событий Linux

ПОЛЕ	ОПИСАНИЕ
ip	IP-адрес Актив.
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.

9.13.1.5. События Cisco

Доступные для событий Cisco поля приведены в таблице ниже (Таблица 56. Поля для событий Cisco).

Табл. 56. Поля для событий Cisco

ПОЛЕ	ОПИСАНИЕ
action	Произведенное действие. Содержит значение из facility_mnemonic (кроме ASA).
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 Актив.
target_ip	IP-адрес получателя (IP-адрес Cisco или IP-адрес для SNMP).
target_port	Порт получателя или подключения.
Дополнительные поля	

Табл. 56. Поля для событий Cisco

ПОЛЕ	ОПИСАНИЕ
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 Актив, с которого пришло событие (если включена отправка hostname на Cisco).
user	Пользователь, инициировавший событие.

9.13.1.6. События RuggedCOM

Доступные для событий RuggedCOM поля приведены в таблице ниже (Таблица 57. Поля для событий RuggedCOM).

Табл. 57. Поля для событий RuggedCOM

ПОЛЕ	ОПИСАНИЕ
event_code	Уникальный идентификатор события. Составляется из facility+severity из protocol_specific_data.
ip	IP-адрес Актив.
Дополнительные поля	
user	Пользователь, инициировавший событие.

9.13.1.7. События Eltex

Доступные для событий поля приведены в таблице ниже (Таблица 58. Поля для событий Eltex).

Табл. 58. 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.

Табл. 58. Поля для событий Eltex

ПОЛЕ	ОПИСАНИЕ
ip	IP-адрес Актив.
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.

9.13.1.8. События FortiGate

Доступные для событий FortiGate поля приведены в таблице ниже (Таблица 59. Поля для событий FortiGate).

Табл. 59. 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: ОЗ (МЭ fortigate), сенсора или Комплекса.
observer_ip	IP-адрес регистратора события: ОЗ (МЭ fortigate), сенсора или Комплекса.
protocol	Наименование протокола из события.

Табл. 59. Поля для событий FortiGate

ПОЛЕ	ОПИСАНИЕ
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.

9.13.1.9. События Hirschmann

Доступные для событий Hirschmann поля приведены в таблице ниже (Таблица 60. Поля для событий Hirschmann).

Табл. 60. 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 Актив.

9.13.1.10. События Enterasys

Доступные для событий Enterasys поля приведены в таблице ниже (Таблица 61. Поля для событий Enterasys).

Табл. 61. 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 Актив.
protocol	Протокол подключения (только в событиях подключения).
source_ip	IP-адрес источника событий.

Табл. 61. Поля для событий Enterasys

ПОЛЕ	ОПИСАНИЕ
user	Имя пользователя в событии.

9.13.1.11. События Windows

Доступные для событий Windows поля приведены в таблице ниже (Таблица 62. Поля для событий Windows).

Табл. 62. 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: ОЗ, сенсора или Комплекса.
observer_ip	IP-адрес регистратора события: ОЗ, 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.
user	Пользователь. Используется поле targetUserName из события.

9.13.1.12. События SNMP

Доступные для событий SNMP поля приведены в таблице ниже (Таблица 63. Поля для событий SNMP).

Табл. 63. Поля для событий SNMP

ПОЛЕ	ОПИСАНИЕ
action	Имя переменной SNMP (snmpTrapOID).
category	Ключевое слово, которое определяет имя объединения для взаимодействия (community_name).

Табл. 63. Поля для событий SNMP

ПОЛЕ	ОПИСАНИЕ
ip	IP-адрес отправителя сообщения.
target_ip	IP-адрес Актив, с которого пришло событие.

9.13.1.13. События syslog

Доступные для событий syslog поля приведены в таблице ниже (Таблица 64. Поля для событий syslog).

Табл. 64. Поля для событий syslog

ПОЛЕ	ОПИСАНИЕ
event_code	Уникальный идентификатор события. Используется facility+severity из protocol_specific_data.
ip	IP-адрес Актив.

9.13.2. 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.

9.13.3. 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.

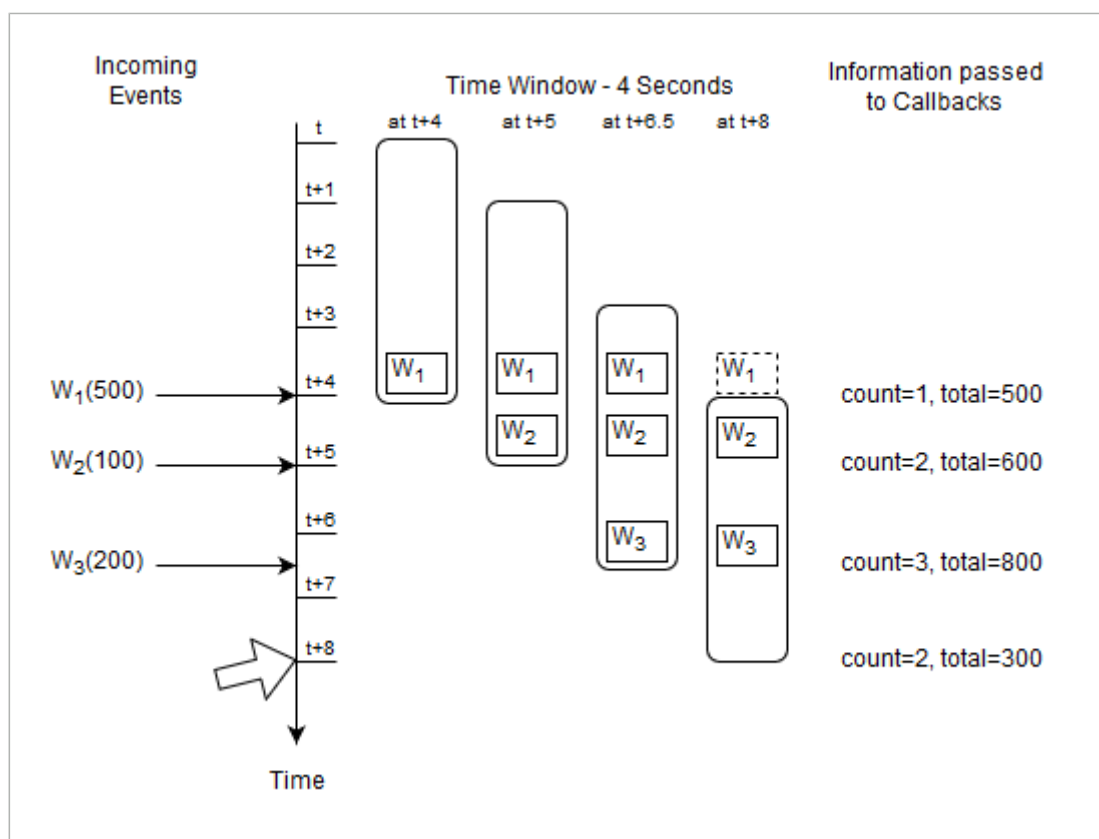


Рис. 243. Работа функции time()

На данном рисунке отображены входящие 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.

9.13.4. 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.

9.13.5. 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).

В случае необходимости глубокого изучения возникновения ошибок, проверки состояния службы и валидации правил в модуле корреляции возможно использование данных log-записей сервиса udv-esper-wrapper, используя команду, описанную в начале подраздела.

9.13.6. 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».

9.13.6.1. 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 ...]
```



Прим.:

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 «A₁ A₂ B₁» 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 «A₁ A₂ B₁» произойдет одно срабатывание на инцидент ИБ.

См. также

http://esper.espertech.com/release-8.4.0/reference-esper/html_single/index.html

9.13.6.2. Оператор «EVERY»

Рассмотренное в разделе «Команда «PATTERN»» правило «каждое совпадение событий A → B» представляется возможным благодаря оператору «EVERY».

Пример

Для примера возьмем поток событий: «A₁ B₁ C₁ B₂ A₂ D₁ A₃ B₃ E₁ A₄ F₁ B₄», где буква обозначает событие, а индекс — номер события данного типа.

При написании следующей конструкции:

```
EVERY ( A → B )
```

совпадения будут в следующих комбинациях:

```
{A1 , B1 }; {A2 , B3 }; {A4 , B4 }
```

При конструкции:

```
EVERY A → B
```

будут комбинации:

```
{A1 , B1 }; {A2 , B3 }; {A3 , B3 }; {A4 , B4 }
```

Следующая конструкция:

```
A → EVERY B
```

выберет данные комбинации:

```
{A1 , B1 }; {A1 , B2 }; {A1 , B3 }; {A1 , B4 }
```

И при заключительном варианте:

```
EVERY A → EVERY B
```

результат будет следующим:

```
{A1 , B1 }; {A1 , B2 }; {A1 , B3 }; {A2 , B3 }; {A3 , B3 }; {A1 , B4 };  
{A2 , B4 }; {A3 , B4 }; {A4 , B4 }
```

9.13.7. 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 Актив ${observer_name} (${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 Актив 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] }
```

9.13.8. 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
- Критический



Приоритет

Высокий

Критический

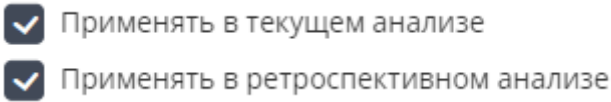
Высокий

Средний

Низкий

Рис. 244. Градация критичности выявляемого инцидента

Статус правила задается чекбоксами («☒») «Применять в текущем анализе» и «Применять в ретроспективном анализе».



☒ Применять в текущем анализе

☒ Применять в ретроспективном анализе

Рис. 245. Активные статусы правила корреляции

9.14. События, попадающие в разделы мониторинга

Так как разделы мониторинга предназначены для первичного анализа, не все события попадают в них. Виды и примеры событий, которые попадают в разделы мониторинга, приведены в таблице (Таблица 65. Основные события Комплекса).

Подсказка:

Виды служебных источников (поле listener) см. в разделе «Описание служебных источников событий».

Помимо событий от сервисов Комплекса и API 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. 65. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИСТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВА- ТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫ- ПОЛНЕНИЕ ФУНКЦИИ
1020001	Сетевое соединение в фоновом режиме помечает доступные интерфейсы	Доступность интерфейса восстановлена	[{ip} - {mac}]: {description} (Актив: {netbios_name})	Availability Control	нет (внутренняя пассивная функция Комплекса)	нет
1020002	Сетевое соединение в фоновом режиме помечает недоступные интерфейсы	Интерфейс недоступен	[{ip} - {mac}]: {description} (Актив: {netbios_name})	Availability Control	нет (внутренняя пассивная функция Комплекса)	нет

Табл. 65. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИСТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВА- ТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫ- ПОЛНЕНИЕ ФУНКЦИИ
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
1030003	Пользователь запустил создание резервной копии	Запущено создание резервной копии	Обоснование: {justification}; Пользователь: {username}	Backup Control	/backup/create POST	Администратор
1070001	Сообщение о запуске регистрации событий	Запущен сервис регистрации событий		Event Control	нет (внутренняя пассивная функция Комплекса)	нет

Табл. 65. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИСТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВА- ТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫ- ПОЛНЕНИЕ ФУНКЦИИ
1070002	Сообщение об остановке регистрации событий	Остановлен сервис регистрации событий		Event Control	нет (внутренняя пассивная функция Комплекса)	нет
1070003	После остановки получения событий журнал был очищен	Сервис регистрации событий запущен после очистки резервированного дискового пространства		Event Control	нет (внутренняя пассивная функция Комплекса)	нет

Табл. 65. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИСТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВА- ТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫ- ПОЛНЕНИЕ ФУНКЦИИ
1070004	Достигнуто предельное значение размера журнала событий	Сервис регистрации событий остановлен в результате переполнения зарезервированного дискового пространства	Объем зарезервированного дискового пространства, заданный в переменной <code>EVENT_INDICES_MAX_SIZE_GB: {size_limit}</code> ГБ	Event Control	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: <code>{source_name}</code> ; Актив: <code>{host_name}</code> (<code>{host_id}</code>); За <code>{delay}</code> секунд было получено <code>{received}</code> событий, ожидалось <code>{threshold}</code> событий.	Event Control	нет (внутренняя пассивная функция Комплекса)	нет

Табл. 65. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИСТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВА- ТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫ- ПОЛНЕНИЕ ФУНКЦИИ
1070006	Новых событий не обнару- жилось в результате вы- полнения задачи	Задача сбора событий успешно вы- полнена, новых событий не обнаружено	Актив: {host_name} ({host_ id}); Наименование сканера: {scanner_name}	Event Control	нет (внутренняя пассивная функция Комплекса)	нет
1070007	Не удалось импортировать события с актива: обна- ружены проблемы с подклю- чением к базе данных	Не удалось импорти- ровать события с актива: обна- ружены проблемы с подклю- чением к базе данных	Актив: {host_name} ({host_ id}); Наименование сканера: {scanner_name}.	Event Control		

Табл. 65. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИСТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВА- ТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫ- ПОЛНЕНИЕ ФУНКЦИИ
1070008	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_name} ({host_id}); Наименование сканера: {scanner_name}.	Event Control		

Табл. 65. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИСТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВА- ТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫ- ПОЛНЕНИЕ ФУНКЦИИ
1070009	Сервис регистрации внутренних событий остановлен в результате переполнения дискового пространства, зарезервированного для событий	Сервис регистрации внутренних событий остановлен в результате переполнения дискового пространства, зарезервированного для событий	Объем зарезервированного дискового пространства, заданный в переменной <code>EVENTS_RETENTION_DISK_CAPACITY_SIZE_MB</code> : {event_size_limit_mb} МБ	Event Control		

Табл. 65. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИСТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВА- ТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫ- ПОЛНЕНИЕ ФУНКЦИИ
1070010	События сервиса регистрации внутренних событий заняли 85% дискового пространства, зарезервированного для событий	События сервиса регистрации внутренних событий заняли 85% дискового пространства, зарезервированного для событий	Объем зарезервированного дискового пространства, заданный в переменной <code>EVENTS_RETENTION_DISK_CAPACITY_SIZE_MB: {event_size_limit_mb}</code> МБ	Event Control		
1080001	Пользователь создает актив	Создан новый актив	id: {id}; Имя: {netbios_name}; Описание: {description}; Тип: {host_type}; ipv4-ipv6- mac: {interfaces_list};	Host Control	<code>/hosts</code> <code>POST</code>	Администратор Инженер

Табл. 65. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИСТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВА- ТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫ- ПОЛНЕНИЕ ФУНКЦИИ
1080002	Пользователь удаляет актив	Удален актив	Обоснование: {justification}; Пользователь: {user} id: {id}; Имя: {netbios_name}; Описание: {description}; Тип: {host_type}; ipv4-ipv6-mac: {interfaces_list}	Host Control	<code>/hosts/[host_id]/delete</code> POST	Администратор

Табл. 65. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИСТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВА- ТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫ- ПОЛНЕНИЕ ФУНКЦИИ
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: {new_interfaces_list}]; Пользователь: {user}	Host Control	/hosts/[host_id] PATCH	Администратор Инженер

Табл. 65. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИСТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВА- ТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫ- ПОЛНЕНИЕ ФУНКЦИИ
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

Табл. 65. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИСТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВА- ТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫ- ПОЛНЕНИЕ ФУНКЦИИ
1080006	Пользователь удалил несколько активов	Удалены активы	Количество активов: {filtered_count}; Типы активов: {host_types}; Метки: {host_labels}; IP-адреса: {ip_filters}; Активы: {hosts}; Производители: {vendors}; Группы активов: {host_groups}; Активы без групп: {outside_tree}; Пользователь: {user}; Обоснование: {justification}	Host Control	/hosts/bulk/delete POST	Администратор
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

Табл. 65. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИСТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВА- ТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫ- ПОЛНЕНИЕ ФУНКЦИИ
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 карточке актива, но нажал Сохранить	Вместе с сенсором удалены сетевые атрибуты актива	Сенсор: {sensor_name} ({sensor_id}); Актив: {host_name} ({host_id}); Сетевые атрибуты: {ip_v4_address}, {mac_address}	Host Control	/hosts/[host_id] PATCH	Администратор Инженер
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

Табл. 65. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИСТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВА- ТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫ- ПОЛНЕНИЕ ФУНКЦИИ
1080011	Комплекс сканирует контролируемую сеть	Обнаружен неизвестный актив	id: {host_id}; ip-mac: [{ip} - {mac}]	Host Control	нет (внутренняя пассивная функция Комплекса)	нет
1080013	Отправлены пустые данные для изменения актива	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. 65. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИСТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВА- ТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫ- ПОЛНЕНИЕ 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	Админи- стратор

Табл. 65. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИСТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВА- ТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫ- ПОЛНЕНИЕ ФУНКЦИИ
1080016	Один и тот же IP-адрес присвоен более, чем одному активу	Обнаружено дубли- рование 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
1080017	Одно и то же наименование присвоено нескольким активам	Обнаружены активы с сов- падающим сетевым именем	Обнаружены активы с сов- падающим 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

Табл. 65. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИСТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВА- ТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫ- ПОЛНЕНИЕ ФУНКЦИИ
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	
1160001	Пользователь удалил одно правило обнаружения вторжений	Удалено правило обнаружения вторжений	Пользователь: {user_login}; Обоснование: {justification}; ID правила: {rule_id}	User Action Control		

Табл. 65. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИСТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВА- ТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫ- ПОЛНЕНИЕ ФУНКЦИИ
1160002	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}	User Action Control		
1160006	Пользователь деактивировал несколько правил обнаружения вторжений	Деактивированы правила обнаружения вторжений	Пользователь: {user}; Правила (ID правила - Сенсор): {rule_sid_ids}; Обоснование: {justification}; Всего деактивировано правил: {len_rule_ids}	User Action Control		
1160007	Пользователь активировал одно правило обнаружения вторжений	Активировано правило обнаружения вторжений	Пользователь: {user}; ID правила: {rule_id}; Сенсор: {node_hostname}	User Action Control		

Табл. 65. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИСТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВА- ТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫ- ПОЛНЕНИЕ ФУНКЦИИ
1160008	Пользователь активировал несколько правил обнаружения вторжений	Активированы правила обнаружения вторжений	Пользователь: {user}; Правил (ID правила - Сенсор): {rule_sid_ids}; Обоснование: {justification}; Всего активировано правил: {len_rule_ids}	User Action Control		
1170001	Пользователь авторизовался	Успешный вход в Комплекс	Пользователь: {user}; IP адрес: {user_ip}	User Action Control	/users/auth_token GET	Все роли
1170002	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

Табл. 65. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИСТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВА- ТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫ- ПОЛНЕНИЕ ФУНКЦИИ
1170003	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
1170006	Пользователь нажал кнопку «Выход»	Успешный выход из Комплекса	Пользователь: {user} IP адрес: {user_ip}	User Action Control	/users/auth_token GET	Все роли

Табл. 65. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИСТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВА- ТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫ- ПОЛНЕНИЕ ФУНКЦИИ
1170007	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. 65. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИСТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВА- ТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫ- ПОЛНЕНИЕ ФУНКЦИИ
1170011	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
1170012	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

Табл. 65. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИСТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВА- ТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫ- ПОЛНЕНИЕ ФУНКЦИИ
1170016	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

Табл. 65. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИСТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВА- ТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫ- ПОЛНЕНИЕ ФУНКЦИИ
1170018	Пользователь редактирует данные учетной записи, оставляя пароль прежним	Изменены данные учетной записи пользователя. Пароль не изменен	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. 65. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИСТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВА- ТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫ- ПОЛНЕНИЕ ФУНКЦИИ
1170026	Пользователь отредактировал парольную политику	Изменена парольная политика	Старые значения: [{old_policy_fields}]; Новые значения [{new_policy_fields}]	User Action Control	/	Администратор
1170027	Пользователь создал учетную запись пользователя Комплекса	Пользователь создан	{self.additional_info}	User Action Control	/users POST	
1170028	Пользователь удалил учетную запись пользователя Комплекса	Пользователь удален	{self.additional_info}	User Action Control	/users/[user_id] DELETE	

Табл. 65. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИСТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВА- ТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫ- ПОЛНЕНИЕ ФУНКЦИИ
1170029	Пользователь выполнил вход в веб-интерфейс Комплекса с нового устройства, не выполнив выход с предыдущего, при условии, что переменная <code>LIMIT_USER_SESSIONS</code> имеет значение true	Обнаружено одновременное использование веб-интерфейса Комплекса более, чем на одном устройстве пользователем <code>{user_login}</code>	Пользователь: <code>{user}</code> ; IP-адрес первого устройства: <code>{old_ip}</code> ; IP-адрес второго устройства: <code>{new_ip}</code>	User Action Control		
1180001	Оперативная память на ОС Комплекса заполнена на значение, превышающее заданное в переменной <code>DATAPK_MAX_RAM_PERCENTAGE_CONSUMED</code>	Обнаружено превышение потребления оперативной памяти (RAM)	Комплекс: <code>{hostname_label}</code> ; Превышен порог в <code>{max_ram_consumed_percentage}%</code>	System Control	нет (внутренняя пассивная функция Комплекса)	нет

Табл. 65. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИСТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВА- ТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫ- ПОЛНЕНИЕ ФУНКЦИИ
1180002	Потребление оперативной памяти снижено до значений, не превышающих заданных в переменной <code>DATAPK_MAX_RAM_PERCENTAGE_CONSUMED</code>	Потребление оперативной памяти (RAM) нормализовано	Комплекс: <code>{hostname_label}</code>	System Control	нет (внутренняя пассивная функция Комплекса)	нет
1180003	Заполненность диска на ОС Комплекса превысило значение, заданное в переменной <code>MAX_DISK_SPACE_CONSUMED_PERCENTAGE</code>	Обнаружено переполнение дискового пространства (HDD/SSD) на Комплексе	Комплекс: <code>{hostname_label}</code> ; Превышен порог в <code>{max_disk_space_consumed_percentage}%</code>	System Control	нет (внутренняя пассивная функция Комплекса)	нет

Табл. 65. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИСТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВА- ТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫ- ПОЛНЕНИЕ ФУНКЦИИ
1180004	Дисковое пространство осво- бождено до значений, не пре- вышающих заданных в пе- ременной MAX_DISK_SPACE_ CONSUMED_PERCENTAGE	Пере- полнение дискового про- странства (HDD, SSD) на Комплексе устранено	Комплекс: {hostname_label}	System Control	нет (внутренняя пассивная функция Комплекса)	нет
1180005	Нагрузка на центральный про- цессор ОС Комплекса пре- высила 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 про- цессор снижена до значений, не превышающих заданных в переменной MAX_CPU_LOAD_ CONSUMED_PERCENTAGE	Нагрузка на центральный процессор (CPU) норма- лизована	Комплекс: {hostname_label}	System Control	нет (внутренняя пассивная функция Комплекса)	нет

Табл. 65. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИСТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВА- ТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫ- ПОЛНЕНИЕ ФУНКЦИИ
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}	System Control	нет (внутренняя пассивная функция Комплекса)	учетная запись администратора ОС
1180010	Пользователь меняет временную зону Комплекса	Временная зона (TZ) Комплекса изменена	Старое значение: {old_value}; Новое значение: {new_value}	System Control	нет (внутренняя пассивная функция Комплекса)	учетная запись администратора ОС

Табл. 65. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИСТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВА- ТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫ- ПОЛНЕНИЕ ФУНКЦИИ
1180011	Брокер сообщений по- требляет больше опера- тивной памяти, чем указано в переменной <code>RMQ_LOW_</code> <code>AVAILABLE_MEMORY_</code> <code>WATERMARK_BYTES</code>	Обнаружено превышение потребления выделенной для брокера сообщений оперативной памяти (RAM)	Комплекс: <code>{hostname_label}</code> ; Лимит RAM: <code>{low_</code> <code>available_memory_</code> <code>watermark_mb}</code> Мбайт	System Control	нет (внутренняя пассивная функция Комплекса)	нет
1180012	Потребление оперативной памяти брокером нормали- зовано до значений, не пре- вышающих указанных в пере- менной <code>RMQ_LOW_AVAILABLE_</code> <code>MEMORY_WATERMARK_BYTES</code>	Потребление выделенной для брокера сообщений оперативной памяти (RAM) нормали- зовано	Комплекс: <code>{hostname_label}</code> ; Лимит RAM: <code>{low_</code> <code>available_memory_</code> <code>watermark_mb}</code> Мбайт	System Control	нет (внутренняя пассивная функция Комплекса)	нет

Табл. 65. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИСТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВА- ТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫ- ПОЛНЕНИЕ ФУНКЦИИ
1180013	Брокер сообщений 1180013 потребляет больше дискового пространства, чем указано в переменной <code>RMQ_LOW_AVAILABLE_DISK_SPACE_WATERMARK_BYTES</code>	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 осво-бождено до значений, не превышающих заданных в переменной <code>RMQ_LOW_AVAILABLE_DISK_SPACE_WATERMARK_BYTES</code>	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

Табл. 65. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИСТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВА- ТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫ- ПОЛНЕНИЕ ФУНКЦИИ
1180015	Запрос к сенсору остался без ответа	Не удастся установить соединение с сенсором	Сенсор: {node_name}({node_id}); Источник данных: {exporter_name}; Был доступен {max_delay:.3f} минут назад;	System Control	нет (внутренняя пассивная функция Комплекса)	нет
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 удастся установить соединение с сервисом получения данных на сенсоре	Не удастся 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

Табл. 65. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИСТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВА- ТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫ- ПОЛНЕНИЕ ФУНКЦИИ
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
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

Табл. 65. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИСТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВА- ТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫ- ПОЛНЕНИЕ ФУНКЦИИ
1180021	Комплексу не удается установить соединение с сервисом синхронизации настроек на сенсоре	Не удастся 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

Табл. 65. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИСТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВА- ТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫ- ПОЛНЕНИЕ ФУНКЦИИ
1180024	Работоспособность сервиса синхронизации настроек на сенсоре восстановлена	Доступность сервиса синхронизации настроек восстановлена	Сенсор: {node_name}({node_id});	System Control	нет (внутренняя пассивная функция Комплекса)	нет
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

Табл. 65. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИСТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВА- ТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫ- ПОЛНЕНИЕ ФУНКЦИИ
1180027	Пользователь удаляет сенсор	Удален сенсор	Наименование сенсора: {node_name}; Идентификатор сенсора: {node_id}; пользо- ватель: {user}; Обоснование: {justification}	System Control	нет (внутренняя пассивная функция Комплекса)	нет
1180028	Сенсор отклоняет сообщения от источника	Сенсор от- клонил входящее со- общение от источника: не удалось обра- ботать текст сообщения	Сенсор: {node_name}({node_ id});	System Control		

Табл. 65. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИСТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВА- ТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫ- ПОЛНЕНИЕ ФУНКЦИИ
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		
1220001	Пользователь запускает сканирование сети	Запущено сканирование сети	Диапазон сканирования: {first_ip} - {last_ip}; Пользователь: {user}	Controlled Net Scan Control	/scan POST	Администратор

Табл. 65. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИСТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВА- ТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫ- ПОЛНЕНИЕ ФУНКЦИИ
1220002	Сеть была успешно проскани- рована	Скани- рование сети успешно за- вершено	Диапазон сканирования: {first_ip} - {last_ip}	Controlled Net Scan Control	нет (внутренняя пассивная функция Комплекса)	нет
1220003	Не удалось завершить скани- рование сети	Обнаружена ошибка при попытке ска- нирования сети	Диапазон сканирования: {first_ip} - {last_ip}; Ошибка: {error}	Controlled Net Scan Control	нет (внутренняя пассивная функция Комплекса)	нет

См. также

[Описание служебных источников событий](#)

9.15. Структура директорий Комплекса

Список общих директорий и файлов настроек, а также их описание представлены в таблице ниже (Таблица 66. Общие директории и файлы настроек).

Табл. 66. Общие директории и файлы настроек

ДИРЕКТОРИЯ (ФАЙЛ)	НАЗНАЧЕНИЕ
<code>/usr/share/udv</code>	Основная директория Комплекса
<code>/usr/share/udv/scripts-certs</code>	Директория для хранения сертификата для верификации сканеров сбора данных
<code>/usr/share/udv/scripts-certs/datapk_script.crt</code>	Сертификат для верификации сканеров сбора данных
<code>/usr/share/udv/certs/ca.crt</code>	Корневой сертификат

Список директорий и основных файлов Комплекса уровня Management, а также их описание представлены в таблице ниже (Таблица 67. Директории и основные файлы настроек Комплекса уровня Management).

Табл. 67. Директории и основные файлы настроек Комплекса уровня Management

ДИРЕКТОРИЯ (ФАЙЛ)	НАЗНАЧЕНИЕ
<code>/usr/share/udv/datapk/manager.env</code>	Основные настройки Комплекса
<code>/var/cache/udv/nginx/certs</code>	Серверные сертификаты
<code>/usr/share/udv/nginx</code>	Шаблоны nginx
<code>/usr/share/udv/frontend</code>	Настройки меню (интерфейса)
<code>/etc/logstash</code>	Правила нормализации
<code>/var/backups</code>	Директория для хранения резервных копий. Содержит tar-архивы с резервными копиями (datapk-backup-version-timestamp.tar)
<code>/var/backups/elasticsearch</code>	Директория для хранения резервных копий событий

Табл. 67. Директории и основные файлы настроек Комплекса уровня Management

ДИРЕКТОРИЯ (ФАЙЛ)	НАЗНАЧЕНИЕ
<code>/var/backups/ elasticsearch/indices</code>	Архивированные индексы событий
<code>/var/backups/ elasticsearch/uploads</code>	Индексы событий для импорта
<code>/usr/share/udv/ vulnerability-backend</code>	Директория для хранения импортированного справочника ПО и уязвимостей (CVE и CVE), импортированной базы сопоставления собранного сканерами ПО со справочником CVE и отчета с последними результатами поиска уязвимостей
<code>/var/opt/udv, /var/ cache/udv</code>	Служебные директории Комплекса

Список директорий и основных файлов Комплекса уровня Sensor, а также их описание представлены в таблице ниже (Таблица 68. Директории и основные файлы настроек Комплекса уровня Sensor).

Табл. 68. Директории и основные файлы настроек Комплекса уровня Sensor

ДИРЕКТОРИЯ (ФАЙЛ)	НАЗНАЧЕНИЕ
<code>/usr/share/udv/ datapk/sensor.env</code>	Основные настройки Комплекса
<code>/usr/share/udv/snmp- connector/snmp_mibs</code>	Словари SNMP

9.16. Признаки неактивности сессий

Признаки, которые использует сервис UDV NTA `zeek_wrapper` для определения неактивности отслеживаемых сессий:

ВНУТРЕННИЙ ИДЕНТИФИКАТОР ПРИЗНАКА	ОПИСАНИЕ ПРИЗНАКА
S0	Обнаружен запрос подключения, но ответа нет
S1	Соединение установлено, но не завершено
SF	Соединение штатно установлено и завершено

ВНУТРЕННИЙ ИДЕНТИФИКАТОР ПРИЗНАКА	ОПИСАНИЕ ПРИЗНАКА
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	 Прим.: Не является признаком неактивности сессии Отправитель отправил флаг SYN, за которым последовал флаг RST, но в период между ними получатель не отправлял флаг SYN ACK
RSTRH	 Прим.: Не является признаком неактивности сессии 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

ВНУТРЕННИЙ ИДЕНТИФИКАТОР ПРИЗНАКА	ОПИСАНИЕ ПРИЗНАКА
OTH	 Прим.: Не является признаком неактивности сессии Отправитель не отправлял начальный запрос с флагом SYN (соединение установлено частично и не закрыто)

9.17. Протоколы, обнаруживаемые UDV NTA в режиме индикации

- AYIYA
- DCE_RPC
- DeltaV
- DHCP
- DNP3
- DNS
- ENIP/CIP
- Finger
- FTP
- FTP-data
- Geneve
- GridFTP
- GridFTP-data
- GSSAPI
- GTPv1
- HTTP
- IEC_61850_MMS
- IMAP
- IRC
- IRC-DCC-data
- KRB (Kerberos TCP)
- LDAP
- Modbus
- MQTT
- MySQL
- NTLM
- NTP
- OPC UA
- PostgreSQL
- POP3
- QUIC
- Radius

- RDP (RDPEUDP)
- RFB (VNC)
- S7comm
- S7commPlus
- SIP (SIP_TCP)
- SMB
- SMTP
- SNMP
- SOCKS
- SSH
- SSL
- Syslog
- Telnet
- Teredo
- TDS
- TNS
- UMAS
- VxLAN
- XMPP

9.18. Сетевые атаки, обнаруживаемые UDV NTA

Группы и идентификаторы атак указаны в соответствии с классификацией, принятой в MITRE ATT&CK.

- Разведка:
 - T1595: Активное сканирование
 - T1592: Сбор информации об атакуемых узлах
- Подготовка ресурсов
- Первоначальный доступ:
 - T1190: Недостатки в общедоступном приложении
- Выполнение/эксплуатация:
 - T1059.001: PowerShell
 - T1047 Windows Management Instrumentation
 - T1569.002 Системные службы: Диспетчер управления службами
 - T1053.002 Запланированная задача (задание): Утилита at (Windows)
 - T1053.005 Запланированная задача (задание): Планировщик заданий Windows
- Закрепление:
 - 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
 - T1204: Выполнение с участием пользователя
 - T1053: Запланированная задача (задание)
 - T1047: Инструментарий управления Windows
 - T1569: Системные службы
- Повышение привилегий
- Предотвращение обнаружения:
 - T1070: Удаление признаков активности из системы
- Получение учетных данных:

- T1003.004 Получение дампа учетных данных: Секреты LSA
- T1003.006 Получение дампа учетных данных: DCSync
- T1558.003 Кража или подделка билетов Kerberos: «Прожарка» Kerberos
- T1557.001 "Человек посередине": Подмена LLMNR/NBT-NS-ответа и ретрансляция SMB
- T1649 Кража или подделка сертификатов аутентификации
- Исследование:
 - T1012 Запросы к реестру
 - T1033 Исследование владельца или пользователей системы
 - T1135 Исследование общих сетевых ресурсов
 - T1201: Исследование парольной политики
 - T1046: Сканирование сетевых служб
- Перемещение внутри периметра:
 - T1021.002 Службы удаленного доступа: Общие SMB-ресурсы или ресурсы администраторов Windows
 - T1570 Передача инструментов внутри периметра
 - T1210 Эксплуатация удаленных служб
 - Сбор данных
 - T1039 Данные с общих сетевых дисков
- Управление и контроль:
 - T1571 Нестандартный порт
 - T1572 Туннелирование протокола
 - T1001.001 Обфускация данных: "Мусорные" данные
 - T1001.002 Обфускация данных: Стеганография
 - T1568.002 Динамическое разрешение: Алгоритмы генерирования доменных имен
- Эксфильтрация данных:
 - T1041: Эксфильтрация через канал управления
- Воздействие:
 - T1529 Завершение работы или перезагрузка системы
 - T1489: Остановка службы

9.19. Переменные файла белого списка

В UDV NTA 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. 69. Переменные, задаваемые 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. 70. Переменные, задаваемые для BZAR

ПЕРЕМЕННАЯ	ТАКТИКА АТАКИ (ЖИРНЫМ) ¹ 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
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

Табл. 70. Переменные, задаваемые для BZAR

ПЕРЕМЕННАЯ	ТАКТИКА АТАКИ (ЖИРНЫМ) ¹ ТЕХНИКА АТАКИ	НАЗНАЧЕНИЕ
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-addr	Выполнение/эксплуатация Диспетчер управления службами	IP-адреса запросов
BZAR::t1569_002_whitelist_resp-addr	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 Диспетчер управления службами	Подсети ответов
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-addr	Выполнение/эксплуатация Windows Management Instrumentation	IP-адреса запросов

Табл. 70. Переменные, задаваемые для BZAR

ПЕРЕМЕННАЯ	ТАКТИКА АТАКИ (ЖИРНЫМ) ¹ ТЕХНИКА АТАКИ	НАЗНАЧЕНИЕ
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
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

Табл. 70. Переменные, задаваемые для BZAR

ПЕРЕМЕННАЯ	ТАКТИКА АТАКИ (ЖИРНЫМ) ¹ ТЕХНИКА АТАКИ	НАЗНАЧЕНИЕ
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-addr	Выполнение/эксплуатация Запланированная задача (задание): Планировщик заданий Windows	IP-адреса запросов
BZAR::t1053_005_whitelist_resp-addr	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 Запланированная задача (задание): Планировщик заданий Windows	Имена ответов
BZAR::t1529_whitelist_orig-addr	Воздействие Завершение работы или перезагрузка системы	IP-адреса запросов

Табл. 70. Переменные, задаваемые для BZAR

ПЕРЕМЕННАЯ	ТАКТИКА АТАКИ (ЖИРНЫМ) ¹ ТЕХНИКА АТАКИ	НАЗНАЧЕНИЕ
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 • Передача инструментов внутри периметра	IP-адреса ответов

Табл. 70. Переменные, задаваемые для BZAR

ПЕРЕМЕННАЯ	ТАКТИКА АТАКИ (ЖИРНЫМ) ¹ ТЕХНИКА АТАКИ	НАЗНАЧЕНИЕ
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. 70. Переменные, задаваемые для BZAR

ПЕРЕМЕННАЯ	ТАКТИКА АТАКИ (ЖИРНЫМ) ¹ ТЕХНИКА АТАКИ	НАЗНАЧЕНИЕ
BZAR::t1021_002_whitelist_resp- addrs	Перемещение внутри периметра Общие SMB-ресурсы или ресурсы ад- министраторов Windows	IP-адреса ответов
BZAR::t1021_002_whitelist_orig_- subnets	Перемещение внутри периметра Общие SMB-ресурсы или ресурсы ад- министраторов Windows	Подсети запросов
BZAR::t1021_002_whitelist_resp_- subnets	Перемещение внутри периметра Общие SMB-ресурсы или ресурсы ад- министраторов Windows	Подсети ответов
BZAR::t1021_002_whitelist_orig_- names	Перемещение внутри периметра Общие SMB-ресурсы или ресурсы ад- министраторов Windows	Имена запросов
BZAR::t1021_002_whitelist_resp_- names	Перемещение внутри периметра Общие SMB-ресурсы или ресурсы ад- министраторов Windows	Имена ответов
BZAR::t1570_whitelist_orig_addrs	Перемещение внутри периметра Передача инструментов внутри пе- риметра	IP-адреса запросов
BZAR::t1570_whitelist_resp_addrs	Перемещение внутри периметра Передача инструментов внутри пе- риметра	IP-адреса ответов
BZAR::t1570_whitelist_orig_- subnets	Перемещение внутри периметра Передача инструментов внутри пе- риметра	Подсети запросов
BZAR::t1570_whitelist_resp_- subnets	Перемещение внутри периметра Передача инструментов внутри пе- риметра	Подсети ответов

Табл. 70. Переменные, задаваемые для BZAR

ПЕРЕМЕННАЯ	ТАКТИКА АТАКИ (ЖИРНЫМ) ¹ ТЕХНИКА АТАКИ	НАЗНАЧЕНИЕ
BZAR::t1570_whitelist_orig_names	Перемещение внутри периметра Передача инструментов внутри периметра	Имена запросов
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

Табл. 70. Переменные, задаваемые для BZAR

ПЕРЕМЕННАЯ	ТАКТИКА АТАКИ (ЖИРНЫМ) ¹ ТЕХНИКА АТАКИ	НАЗНАЧЕНИЕ
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 администраторов Windows (многократные попытки)	Имена ответов
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

Табл. 70. Переменные, задаваемые для BZAR

ПЕРЕМЕННАЯ	ТАКТИКА АТАКИ (ЖИРНЫМ) ¹ ТЕХНИКА АТАКИ	НАЗНАЧЕНИЕ
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 Автозапуск при загрузке или входе в систему: DLL-библиотеки, загружаемые с помощью Winlogon	IP-адреса запросов
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

Табл. 70. Переменные, задаваемые для BZAR

ПЕРЕМЕННАЯ	ТАКТИКА АТАКИ (ЖИРНЫМ) ¹ ТЕХНИКА АТАКИ	НАЗНАЧЕНИЕ
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 Автозапуск при загрузке или входе в систему: Мониторы портов	Подсети запросов
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

Табл. 70. Переменные, задаваемые для BZAR

ПЕРЕМЕННАЯ	ТАКТИКА АТАКИ (ЖИРНЫМ) ¹ ТЕХНИКА АТАКИ	НАЗНАЧЕНИЕ
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