

UDV ITM

Руководство по эксплуатации UDV-ITM-VM версии 1.7.0.0

Версия документа: 1.0
Дата выгрузки: 9.1.2024

Содержание

1. Глоссарий.....	4
2. Что нового?.....	7
2.1. Обновления документации.....	10
3. Введение.....	11
3.1. Область применения.....	11
3.2. Назначение и условия применения.....	11
4. Описание функций.....	13
4.1. Главный экран и элементы веб-интерфейса.....	13
4.1.1. Главное меню веб-интерфейса.....	14
4.1.2. Общие элементы веб-интерфейса.....	15
4.1.3. Подключение к веб-интерфейсу.....	16
4.2. Панель информации.....	17
4.3. Серверы мониторинга.....	24
4.3.1. Подключение нового сервера мониторинга к ITM-VM.....	28
4.3.2. Настройка сбора данных.....	30
4.3.3. Просмотр информации о подключенном сервере мониторинга.....	32
4.3.4. Изменение свойств подключенного сервера мониторинга.....	35
4.3.5. Отключение автоматического сбора данных с сервера мониторинга.....	36
4.3.6. Включение автоматического сбора данных с сервера мониторинга.....	37
4.3.7. Удаление подключенного сервера мониторинга.....	37
4.3.8. Просмотр свойств сервера удаленного мониторинга.....	38
4.3.9. Изменение названия ТО сервера удаленного мониторинга.....	39
4.4. Объекты мониторинга.....	40
4.4.1. Список объектов мониторинга.....	40
4.4.2. Просмотр информации об объекте мониторинга.....	43
4.5. Мониторинг ИТ-услуг.....	45
4.5.1. Просмотр информации об ИТ-услуге.....	47
4.6. Проблемы объектов мониторинга.....	49
4.6.1. Список проблем объектов мониторинга.....	49
4.6.2. Просмотр карточки проблемы.....	53
4.7. Администрирование.....	54

4.7.1. Журнал событий.....	54
4.8. Настройки.....	55
4.8.1. Основные настройки.....	56
4.8.2. Пользователи.....	65
4.8.3. LDAP.....	78
4.8.4. Правила оповещений.....	87
5. Справочная информация.....	96
5.1. Роли пользователей и доступные им интерфейсы.....	96
5.2. Совместимость компонентов решения для UDV-ITM-VM.....	96

1. Глоссарий

1.1. Автоматизированная система управления технологическим процессом

Комплекс программных и программно-аппаратных средств, предназначенных для контроля за технологическим и (или) производственным оборудованием (исполнительными устройствами) и производимыми ими процессами, а также для управления таким оборудованием и процессами.

Аббревиатура: АСУ ТП

1.2. Объект мониторинга

Объект мониторинга (узел сети) – любое устройство, приложение или система, которые подключаются к системе мониторинга для контроля качества их функционирования и предоставляемых услуг.

Аббревиатура: ОМ

1.3. Проблема объекта мониторинга

Состояние контролируемого параметра объекта мониторинга, при котором его значение выходит за пределы диапазона значений при нормальном функционировании объекта мониторинга.

1.4. Система автоматизации процессов обеспечения безопасности

Автоматизированная система, предназначенная для автоматизации процессов управления информационной безопасностью.

Аббревиатура: САОБ

1.5. Система мониторинга безопасности и контроля ресурсов

Комплексная система мониторинга ИТ-ресурсов и компонентов АСУ ТП для реализации требований по защите информации в соответствии с приказом ФСТЭК №239 от 25.12.2017.

Аббревиатура: СМБКР

1.6. Система мониторинга компьютерных инцидентов

Система сбора, анализа и корреляции событий информационной безопасности, созданная на базе решений класса SIEM.

Аббревиатура: СМКИ

1.7. Соглашение об уровне услуг

Соглашение об уровне услуг – установленный уровень качества, который считается приемлемым для данной услуги.

Аббревиатура: SLA

1.8. Технологический комплекс

Технологический комплекс промышленного или производственного предприятия, на котором используется оборудование, управляемое АСУ ТП полевого уровня.

Аббревиатура: ТК

1.9. UDV ITM

UDV ITM – торговое наименование Системы зонтичного мониторинга автоматизированных и информационных систем «Cyberlympha ITM» (свидетельство о регистрации программы для ЭВМ №2022684928, 14.12.2022 г.)

1.10. UDV-ITM-M

UDV-ITM-M – сервер мониторинга.

Применяется для:

- сбора данных о производительности с подключенных объектов мониторинга;
- консолидации данных, в т. ч. полученных с сервера удаленного мониторинга;
- передачи консолидированных данных на сервер визуализации и управления;
- визуализации информации об использовании вычислительных ресурсов и каналов связи объектов мониторинга филиала;
- оповещения ответственных лиц в случае выявления сбоя, либо отклонения показателей функционирования объекта мониторинга от допустимых.

*В ранних версиях использовалось название Сервер консолидации, ITM-K.

1.11. UDV-ITM-RM

UDV-ITM-RM – сервер удаленного мониторинга.

Применяется для:

- сбора данных о производительности с подключенных объектов мониторинга;
- передачи собранных данных на сервер мониторинга.

*В ранних версиях использовалось название Сервер агентов (прокси-сервер), ITM-A.

1.12. UDV-ITM-VM

UDV-ITM-VM – сервер визуализации и управления.

Предназначен для централизованного управления системой мониторинга в целом, консолидации данных мониторинга в масштабах всего предприятия и интеграционного взаимодействия с корпоративными системами обнаружения компьютерных инцидентов и системами автоматизации процессов обеспечения ИБ.

Применяется для:

- сбора данных с серверов консолидации и серверов мониторинга;
- предоставления высокоуровневой информации о состоянии ИТ-ресурсов предприятия пользователям и смежным системам.

2. Что нового?

Основные изменения в ПО сервера UDV-ITM-VM версии 1.7.0.0:

Табл. 2-1 Изменения UDV-ITM-VM версии 1.7.0.0

Категория	Изменения в продукте	Разделы документации
Серверы мониторинга	<p>На странице <i>Серверы мониторинга</i>:</p> <ol style="list-style-type: none"> 1. В таблицу добавлена информация о серверах удаленного мониторинга. 2. Добавлена возможность просмотра карточки сервера удаленного мониторинга. 3. Добавлена возможность свернуть или развернуть сразу все записи в таблице. 4. Добавлена возможность внеочередного сбора данных с сервера мониторинга. 5. Добавлена возможность настройки сбора данных. В связи с этим исключен раздел «Настройки» → «Сбор данных». 6. Добавлено автоматическое обновление до новой версии серверов мониторинга, подключенных к UDV-ITM-VM. После обновления сбор данных с серверов мониторинга продолжится. 7. Исправлена ошибка, при которой можно было добавить несколько одинаковых серверов при повторном нажатии кнопки «Подключить» в окне «Подключение сервера мониторинга». 8. Исправлена ошибка в названии версии UDV-ITM-M, при которой некорректно работала сортировка в столбце «Версия ПО». <p>В карточке сервера мониторинга:</p> <ol style="list-style-type: none"> 1. Добавлена таблица с параметрами конфигурации сервера мониторинга. 2. Добавлена ссылка для перехода на страницу этого сервера мониторинга. <p>Во всплывающем окне со статусами синхронизаций на странице параметр «Системные свойства» переименован в «Свойства сервера мониторинга»</p>	4.3.3 Просмотр информации о подключенном сервере мониторинга (32), 4.3 Серверы мониторинга (24), 4.3.2 Настройка сбора данных (30), 4.3.1 Подключение нового сервера мониторинга к ITM-VM (28), 4.8 Настройки (55), 4 Описание функций (13)
Объекты мониторинга	<p>На странице <i>Объекты мониторинга</i>:</p> <ol style="list-style-type: none"> 1. Исключено дерево филиалов и ТК, теперь по умолчанию в списке отображаются все ОМ. 2. Добавлена возможность фильтрации ОМ по филиалу и ТК. 3. В таблицу со списком ОМ добавлены столбцы «Тип ОМ» и «Ссылки». 4. Добавлен счетчик количества ОМ. 5. Добавлена возможность просмотра наиболее критичных проблем выбранного ОМ при нажатии на значение в столбце «Проблемы». 6. Столбец таблицы «Филиал/ТО» разделен на два: «Филиал» и «ТК». 7. Добавлена возможность сортировки по филиалу. 8. Изменены настройки сортировки по умолчанию. <p>В карточке ОМ:</p> <ol style="list-style-type: none"> 1. Параметр «Состояние» переименован в «Статус». 2. Добавлены параметры «Обновление статуса» и «Обновление свойств ОМ». 3. Исключен параметр «Дата обновления». 	4.4 Объекты мониторинга (40), 4.4.1 Список объектов мониторинга (40), 4.4.2 Просмотр информации об объекте мониторинга (43)

Табл. 2-1 Изменения UDV-ITM-VM версии 1.7.0.0

Категория	Изменения в продукте	Разделы документации
	<p>4. Добавлена возможность отображения внешних ссылок, добавленных в качестве значения полей «URL A», «URL B», «URL C» в инвентарных данных UDV-ITM-M или Zabbix.</p> <p>5. Исправлено отображение IP-адресов с 12 символами.</p> <p>6. Изменено отображение состояния для объектов мониторинга на техническом обслуживании</p>	
Объекты мониторинга, серверы мониторинга, проблемы	<p>Добавлена возможность просмотра окон «Свойства сервера удаленного мониторинга» и «Свойства сервера мониторинга» на страницах <i>Объекты мониторинга</i>, <i>Проблемы</i>.</p> <p>Добавлена возможность просмотра окна «Свойства сервера удаленного мониторинга» при нажатии в любом месте строки конкретного ТК на странице <i>Серверы мониторинга</i>.</p> <p>Изменено поведение на странице <i>Проблемы</i>:</p> <ul style="list-style-type: none"> • При нажатии на значение в столбце «Филиал, ТК» выводится окно просмотра свойств сервера мониторинга. • При нажатии на значение в столбце «Объект» выводится окно просмотра информации об объекте мониторинга 	4.3.3 Просмотр информации о подключенном сервере мониторинга (32), 4.3 Серверы мониторинга (24), 4.4 Объекты мониторинга (40), 4.4.1 Список объектов мониторинга (40), 4.3.8 Просмотр свойств сервера удаленного мониторинга (38), 4.3.9 Изменение названия ТО сервера удаленного мониторинга (39), 4.6.1 Список проблем объектов мониторинга (49), 4.6.2 Просмотр карточки проблемы (53), 4.4.2 Просмотр информации об объекте мониторинга (43)
Проблемы	<p>На странице <i>Проблемы</i>:</p> <ul style="list-style-type: none"> • Изменен счетчик записей. • Добавлена возможность сортировки по длительности проблем. • Добавлена возможность фильтрации списка по состоянию проблем и по объектам мониторинга. • Добавлена возможность поиска Ом в фильтре «Объект» 	4.6.1 Список проблем объектов мониторинга (49)
Отчет о проблемах	<p>Изменен шаблон письма с отчетом о проблемах:</p> <ul style="list-style-type: none"> • Добавлены столбцы с нумерацией строк и состоянием проблемы. • Добавлена строка с информацией об общем количестве событий и о количестве нерешенных проблем. • Добавлено наименование оповещения 	4.8.4.1 Создание правила оповещений (89)
ИТ-услуги	<ol style="list-style-type: none"> 1. Исправлена ошибка, возникавшая при попытке пользователя включить ИТ-услугу, отключенную администратором. 2. Исправлена ошибка, при которой на странице <i>ИТ-услуги</i> отключалось несколько услуг вместо одной 	—
Роли пользователей	<ol style="list-style-type: none"> 1. Для авторизованных пользователей исключена возможность перехода на страницу авторизации без завершения текущей сессии. 2. Для роли «Пользователь» добавлены следующие возможности: <ul style="list-style-type: none"> • просмотр списка и карточек правил оповещений на странице <i>Настройки</i> → <i>Правила оповещений</i>; • создание, изменение, включение, выключение и удаление собственных правил оповещений на странице <i>Настройки</i> → <i>Правила оповещений</i> 	5.1 Роли пользователей и доступные им интерфейсы (96)
Email-оповещения, внешний вид	<p>Добавлен индикатор состояния подключения к SMTP-серверу на странице <i>Настройки</i> → <i>Основные</i></p>	4.8.1 Основные настройки (56)

Табл. 2-1 Изменения UDV-ITM-VM версии 1.7.0.0

Категория	Изменения в продукте	Разделы документации
Переменные, основные настройки	На страницу <i>Настройки</i> → <i>Основные</i> добавлена возможность настройки параметров: <ul style="list-style-type: none"> • Период хранения истории проблем, дней; • Период хранения истории синхронизаций, дней 	4.8.1 Основные настройки (56), 4.8.1.1 Изменение основных свойств сервера (60)
Оповещения	Добавлен вывод оповещений о внутренних ошибках сервера	—
Администрирование, журнал событий	Добавлен раздел основного меню <i>Администрирование</i> , куда перенесен раздел <i>Журнал событий</i> . Изменен внешний вид иконок для отображения важности событий	4.7.1 Журнал событий (54), 4.7 Администрирование (54)
Панель информации	На странице <i>Панель информации</i> : <ol style="list-style-type: none"> 1. Добавлена возможность изменения размера графиков: <ul style="list-style-type: none"> • «Количество объектов мониторинга по статусу»; • «Количество объектов мониторинга по проблемности»; • «Изменение количества объектов мониторинга»; • «Количество нерешенных проблем по важности»; • «Изменение количества проблем». 2. Изменен внешний вид графиков: <ul style="list-style-type: none"> • «Количество нерешенных проблем по важности»; • «Изменение количества объектов мониторинга»; • «Изменение количества проблем». 3. Изменен тип графиков «Количество объектов мониторинга по статусу» и «Количество объектов мониторинга по проблемности», а также пояснения к этим графикам. 4. Добавлена возможность выбора отображаемых графиков. 5. Добавлена возможность перемещения графиков. 6. Исправлена ошибка, при которой некорректно отображались подписи к графикам 	4.2 Панель информации (17), 4.1 Главный экран и элементы веб-интерфейса (13)
Внешний вид	<ol style="list-style-type: none"> 1. Изменено отображение процесса загрузки данных на следующих страницах: <ul style="list-style-type: none"> • <i>Объекты мониторинга</i>; • <i>Журнал событий</i>; • <i>Проблемы</i>; • <i>Панель информации</i>; • <i>LDAP</i>; • страница авторизации. 2. Исправлено отображение полосы прокрутки при загрузке данных. 3. Изменен внешний вид таблиц при отсутствии данных и при возникновении ошибки 502. 4. Добавлено оповещение «Сервер не отвечает» при отсутствии ответа от сервера в течение 30 секунд. 5. Обновлен внешний вид ряда всплывающих окон: <ul style="list-style-type: none"> • окно удаления правила оповещения; • окно удаления сервера; • окно очистки настроек LDAP; • окно свойств сервера мониторинга; • окно изменения свойств сервера мониторинга; • окно информации об ИТ-услуге; • окно настройки сбора данных; • окно просмотра информации об объекте мониторинга; 	4.8.4.2 Управление правилами оповещений (92), 4.3.7 Удаление подключенного сервера мониторинга (37), 4.8.3.3 Очистка настроек LDAP (86), 4.3.3 Просмотр информации о подключенном сервере мониторинга (32), 4.3.4 Изменение свойств подключенного сервера мониторинга (35), 4.5.1 Просмотр информации об ИТ-услуге (47), 4.3.2 Настройка сбора данных (30), 4.4.2 Просмотр информации об объекте мониторинга (43), 4.8.1.3 Очистка настроек Email-оповещений (63), 4.8.2.4 Управление учетной записью пользователя (73), 4.8.1.1 Изменение основных свойств сервера (60), 4.6.2 Просмотр карточки проблемы (53)

Табл. 2-1 Изменения UDV-ITM-VM версии 1.7.0.0

Категория	Изменения в продукте	Разделы документации
	<ul style="list-style-type: none"> • окно очистки настроек email-оповещений; • окно подтверждения удаления пользователя; • окно подтверждения изменения периода неактивности пользователя для блокировки сеанса; • карточка проблемы. <p>6. Исправлена ошибка во всплывающей подсказке к полю «Пароль» в окне «Добавление пользователя»</p>	
Фильтры, панель информации	Изменен фильтр по филиалам и ТК на странице <i>Панель информации</i>	4.2 Панель информации (17)
Фильтры, объекты мониторинга, проблемы	<p>Добавлена возможность отмены сразу всех фильтров на страницах:</p> <ul style="list-style-type: none"> • <i>Объекты мониторинга</i>; • <i>Проблемы</i> 	4.4.1 Список объектов мониторинга (40), 4.6.1 Список проблем объектов мониторинга (49)
Фильтры, проблемы	Добавлена возможность фильтрации по ТК на странице <i>Проблемы</i>	4.6.1 Список проблем объектов мониторинга (49)
Правила оповещений	Добавлена иконка, которая показывает состояние работоспособности канала Email-оповещений на странице <i>Правила оповещений</i>	4.8.4 Правила оповещений (87)
Синхронизация	Исправлена ошибка синхронизации метаданных	—
Настройки, SIEM	Добавлена возможность настройки подключения к SIEM на странице <i>Настройки</i> → <i>Основные</i>	4.8.1 Основные настройки (56), 4.8.1.4 Настройка интеграции с SIEM (64)

2.1. Обновления документации

Обновления в текущей версии документации:

- Добавлены разделы:
 - 4.1.3 Подключение к веб-интерфейсу (16)
- Обновлены разделы:
 - 4.5 Мониторинг ИТ-услуг (45)
 - 4.1.2 Общие элементы веб-интерфейса (15)
 - 4.3.4 Изменение свойств подключенного сервера мониторинга (35)
 - 4.6.2 Просмотр карточки проблемы (53)
 - 4.8.2 Пользователи (65)

3. Введение

В этом разделе:

- 3.1 Область применения (11)
- 3.2 Назначение и условия применения (11)
- 4.1.3 Подключение к веб-интерфейсу (16)

3.1. Область применения

UDV-ITM-VM – сервер визуализации и управления, который используется в корпоративных вертикально-интегрированных решениях по мониторингу и контролю ИТ-ресурсов. UDV-ITM-VM работает на верхнем уровне иерархии, как правило, в администрации предприятия.

3.2. Назначение и условия применения

Сервер визуализации и управления UDV-ITM-VM предназначен для осуществления контроля предоставляемых вычислительных ресурсов и каналов связи в автоматизированных системах управления путем реализации следующих функций:

- Предоставление сводной информации о состоянии функционирования контролируемых ИТ-ресурсов АСУ ТП в филиалах и на технологических объектах предприятия.
- Передача консолидированных данных о свойствах и состоянии функционирования контролируемых ресурсов в смежные корпоративные системы: систему автоматизации процессов обеспечения безопасности (САОБ) и систему мониторинга компьютерных инцидентов (СМКИ).

Сервер визуализации и управления UDV-ITM-VM используется в составе комплексной системы мониторинга и контроля ИТ-ресурсов АСУ ТП UDV ITM.

Архитектура системы UDV ITM приведена на рисунке.

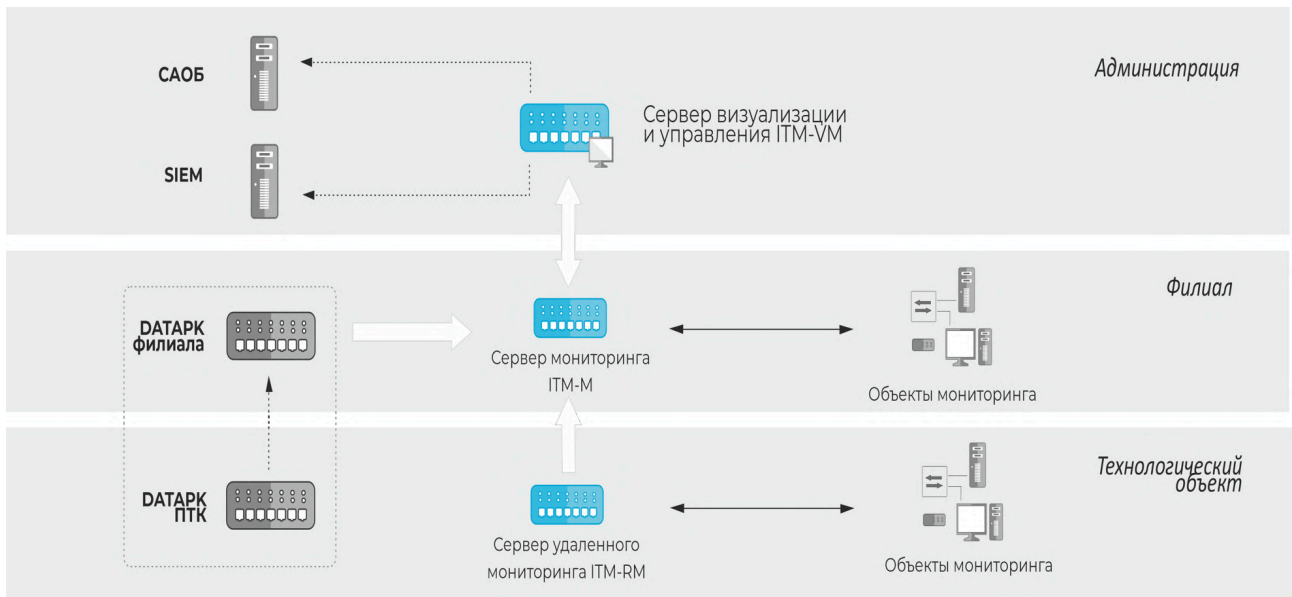


Рис. 3-1 Архитектура системы UDV ITM

4. Описание функций

В этом разделе:

- 4.1 Главный экран и элементы веб-интерфейса (13)
- 4.2 Панель информации (17)
- 4.3 Серверы мониторинга (24)
- 4.4 Объекты мониторинга (40)
- 4.5 Мониторинг ИТ-услуг (45)
- 4.6 Проблемы объектов мониторинга (49)
- 4.7 Администрирование (54)
 - 4.7.1 Журнал событий (54)
- 4.8 Настройки (55)
 - 4.8.1 Основные настройки (56)
 - 4.8.2 Пользователи (65)
 - 4.8.3 LDAP (78)
 - 4.8.4 Правила оповещений (87)

4.1. Главный экран и элементы веб-интерфейса

Главный экран веб-интерфейса сервера визуализации и управления UDV-ITM-VM состоит из основного (бокового) меню и раздела для отображения контента соответствующего раздела.

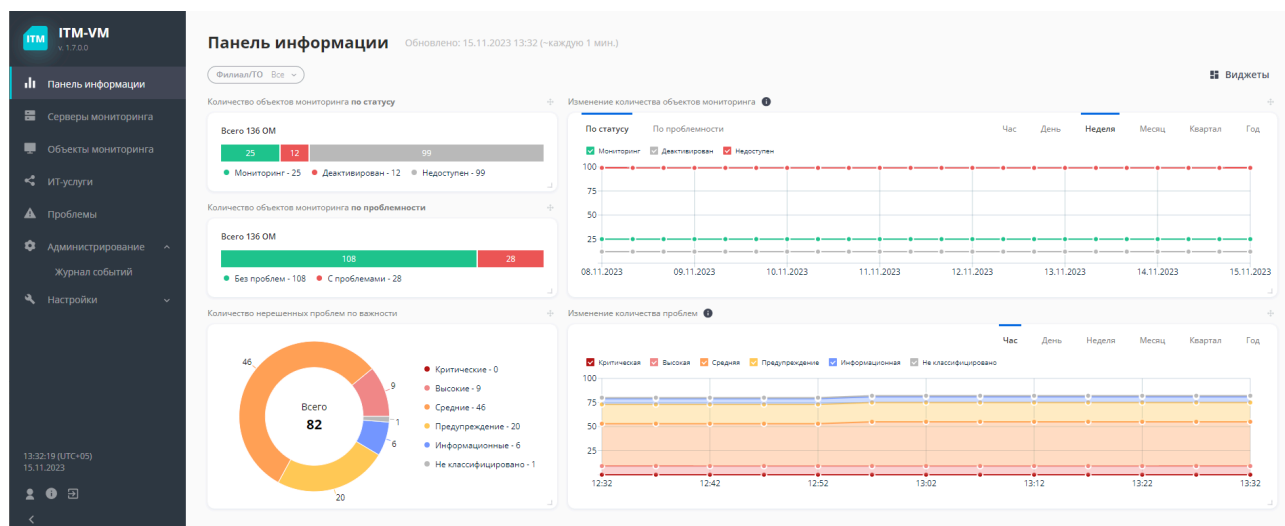


Рис. 4-3 Главный экран интерфейса сервера UDV-ITM-VM

В этом разделе:



- 4.1.1 Главное меню веб-интерфейса (14)
- 4.1.2 Общие элементы веб-интерфейса (15)
- 4.1.3 Подключение к веб-интерфейсу (16)

4.1.1. Главное меню веб-интерфейса



Главное (боковое) меню веб-интерфейса содержит следующие разделы:

1. *Панель информации*. Содержит функции просмотра обобщенной информации об объектах мониторинга и нерешенных проблемах в виде графиков (см. раздел 4.2 Панель информации (17)).
2. *Серверы мониторинга*. Содержит функции подключения серверов мониторинга уровня филиалов и управления ими (подключение, отключение и т.п.) (см. раздел 4.3 Серверы мониторинга (24)).
3. *Объекты мониторинга*. Содержит функции просмотра списков объектов мониторинга, подключенных к серверам мониторинга (см. раздел 4.4 Объекты мониторинга (40)).
4. *ИТ-услуги*. Содержит функции просмотра и настройки списка ИТ-услуг (см. раздел 4.5 Мониторинг ИТ-услуг (45)).
5. *Проблемы*. Содержит функции просмотра списков проблем объектов мониторинга (см. раздел 4.6 Проблемы объектов мониторинга (49)).
6. *Журнал событий*. Содержит функции просмотра списка событий (см. раздел 4.7.1 Журнал событий (54)).
7. *Настройки*. Содержит функции по настройке сервера UDV-ITM-VM (см. раздел 4.8 Настройки (55)).

Боковое меню имеет две формы – полную и свернутую. По умолчанию боковое меню развернуто.

Чтобы свернуть боковое меню, нажмите на кнопку  вверху боковой панели. Чтобы развернуть боковое меню, нажмите на кнопку  вверху боковой панели. Настроенное состояние свернутости меню сохраняется локально для браузера.

В нижней части боковой панели отображается дата и время на сервере с указанием часового пояса, ФИО и подразделение текущего пользователя и кнопки:

-  («Перейти в профиль пользователя») – при нажатии на кнопку откроется окно со свойствами текущего пользователя, в котором можно изменить пароль или данные пользователя. Подробнее см. в разделе 4.8.2.5 Изменение пароля пользователя (76).
-  («О системе») – при нажатии на кнопку откроется окно, которое содержит информацию о системе: название и версию продукта, информацию о производителе.

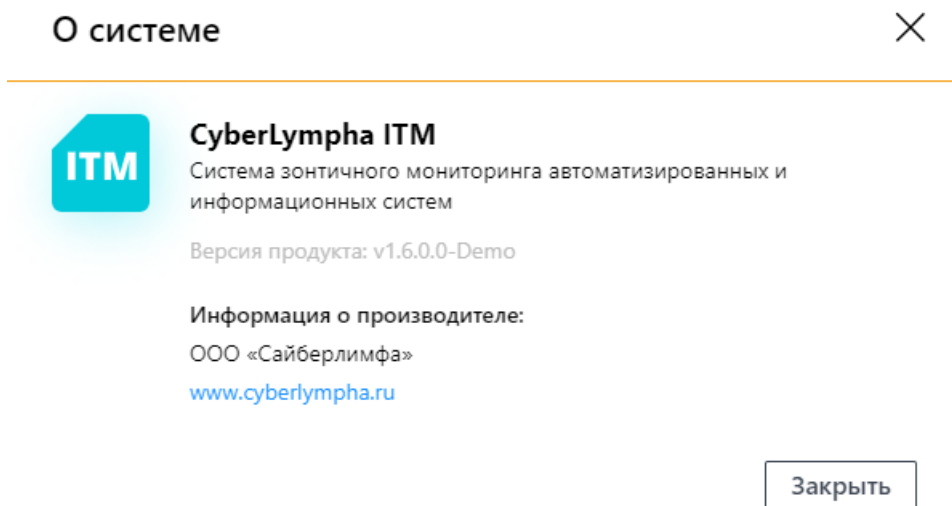



Рис. 4-4 Окно с информацией о системе

-  («Выйти») — при нажатии на кнопку текущая сессия пользователя будет завершена, на экране появится форма авторизации.

4.1.2. Общие элементы веб-интерфейса

Кнопка «Отменить»

Во всех редактируемых экранных формах веб-интерфейса при нажатии на кнопку «Отменить» форма закрывается без сохранения данных. В случае наличия несохраненных данных в форме выводится предупреждение.

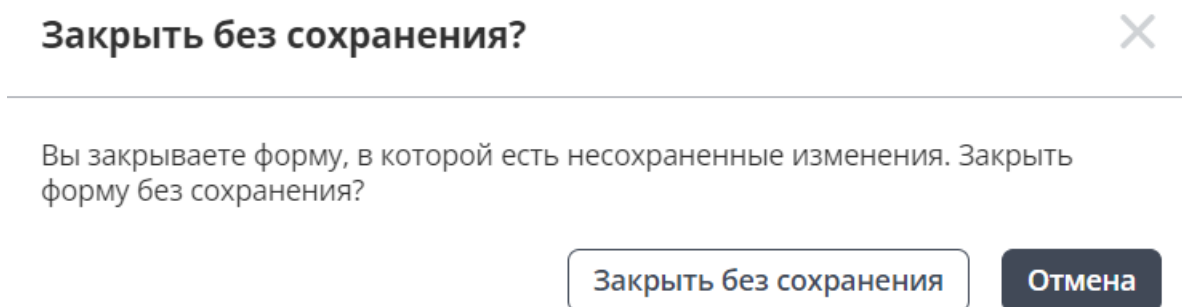







Рис. 4-5 Предупреждение о наличии несохраненных изменений

В редактируемых экранных формах нажатие на кнопку  соответствует действию нажатия на кнопку «Отменить». Это значит, что при нажатии на  редактируемая форма также закрывается без сохранения данных, при этом в случае наличия несохраненных данных в форме выводится предупреждение.

Сортировка значений в таблицах

В таблицах реализована возможность сортировки записей по определенным столбцам.

Для сортировки записей кликните левой кнопкой мыши по названию интересующего столбца таблицы.

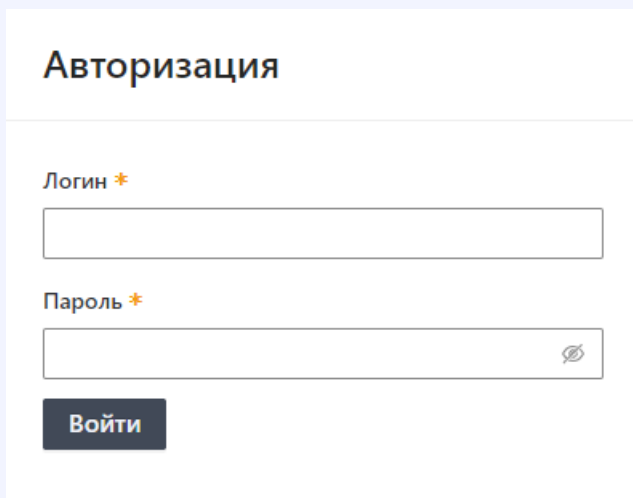
- По первому клику осуществляется сортировка по возрастанию, иконка рядом с названием столбца имеет вид .
- По второму клику – сортировка по убыванию, иконка рядом с названием столбца имеет вид .
- По третьему клику – возврат к сортировке по умолчанию, иконка рядом с названием столбца имеет вид .

4.1.3. Подключение к веб-интерфейсу

Для подключения к веб-интерфейсу UDV-ITM-VM:

1. В браузере в адресной строке введите IP-адрес UDV-ITM-VM.

Результат шага: отобразится окно входа в веб-интерфейс UDV-ITM-VM.



The screenshot shows a white rectangular window with a light blue border. At the top, the title 'Авторизация' is centered in a bold, dark blue font. Below the title, there are two input fields. The first is labeled 'Логин *' in a dark blue font, with an asterisk indicating it is required. The second is labeled 'Пароль *' in a dark blue font, also with an asterisk. To the right of the password field is a small icon of an eye with a slash through it, used for toggling password visibility. Below the input fields is a dark blue button with the white text 'Войти'.

Рис. 4-6 Окно авторизации

2. В окне входа введите логин и пароль учетной записи.


 **Внимание:**

При вводе неправильного логина или пароля 5 раз IP-адрес, с которого пользователь пытается авторизоваться, блокируется на 5 минут.

3. Нажмите на кнопку «Войти».

Результат шага: выполнен вход на главную страницу веб-интерфейса UDV-ITM-VM.

Подсказка:

Чтобы завершить сеанс работы в веб-интерфейсе UDV-ITM-VM, нажмите на кнопку  («Выйти») в нижней части главного меню.

4.2. Панель информации

Раздел основного меню *Панель информации* содержит информацию об объектах мониторинга и нерешенных проблемах в виде графиков. Данные графиков собираются суммарно по всем серверам мониторинга.

Данные графиков автоматически обновляются каждую минуту. В верхнем правом углу страницы указана дата и время последнего обновления.

В фильтре «Филиал/ТК» в верхнем левом углу можно выбрать филиалы и ТК, для которых будут отображаться все графики на странице. Для этого установите чекбоксы рядом с нужными объектами в списке и нажмите на области вне фильтра, чтобы применить изменения.

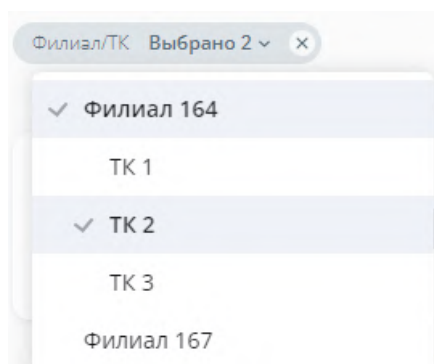



Рис. 4-7 Выбор филиалов и ТК, для которых будут отображаться данные на графиках

По умолчанию показаны графики для всех филиалов и входящих в них ТК. При выборе филиала входящие в него ТК не выбираются автоматически. Выбор ТК доступен независимо от того, выбран ли филиал, к которому он относится. Если у филиала 5 или больше вложенных ТК, становятся доступны кнопки:

- «Выделить все» — нажмите, чтобы выбрать все ТК, входящие в филиал.
- «Снять выделение» — нажмите, чтобы отменить выбор всех ТК, входящих в филиал.

Прим.:


Выбор объектов работает только для данных, полученных после обновления или установки UDV-ITM-VM версии 1.6 или выше. Данные, накопленные за время работы UDV-ITM-VM до обновления версии, отображаются только суммарно по всем серверам мониторинга и ТК.

 **Прим.:**

Графики **ОМ** по проблемности будут отображаться только для данных, полученных после обновления или установки UDV-ITM-VM версии 1.6 или выше. Данные, накопленные за время работы UDV-ITM-VM до обновления версии, на графиках не отображаются.


Перемещение графиков

Вы можете изменить местоположение графика на странице. Для этого:

1. Наведите курсор на иконку  в верхнем правом углу области с графиком.
2. Зажмите левую кнопку мыши и потяните область с графиком для перемещения.

Изменение размера графиков

Вы можете изменить размер любого из графиков. Для этого:

1. Наведите курсор на иконку  в нижнем левом углу области с графиком.
2. Зажмите левую кнопку мыши и потяните область с графиком для изменения размера.

Выбор отображаемых графиков

По умолчанию на странице *Панель информации* отображаются следующие графики:

- Количество объектов мониторинга по статусу;
- Количество объектов мониторинга по проблемности;
- Изменение количества объектов мониторинга;
- Количество нерешенных проблем по важности;
- Изменение количества проблем.

Вы можете изменить набор отображаемых графиков. Для этого:

1. Нажмите на кнопку «Виджеты» в правом верхнем углу.
2. В появившемся списке:
 - Установите чекбоксы рядом с виджетами, которые хотите отображать.
 - Снимите чекбоксы рядом с виджетами, которые хотите скрыть.

Виджеты



- Количество объектов мониторинга по статусу
- Количество объектов мониторинга по проблемности
- Изменение количества объектов мониторинга по статусу и проблемности i
- Количество нерешенных проблем по важности
- Изменение количества проблем i

Рис. 4-8 Пример выбора виджетов из списка

3. Нажмите на , чтобы закрыть панель со списком виджетов.

Прим.:

В текущей реализации настройки выбора отображаемых графиков сбрасываются при обновлении страницы и при переходе на другую страницу.

Количество объектов мониторинга по статусу

График, показывающий распределение ОМ по статусу на данный момент времени.

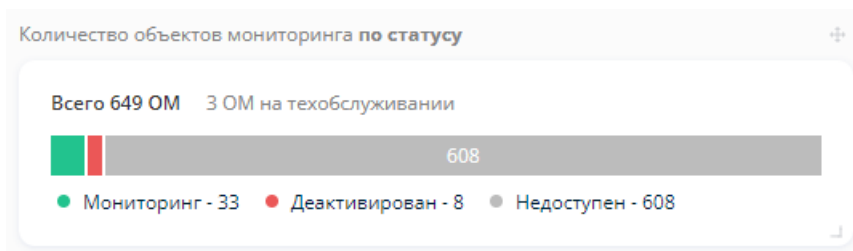


Рис. 4-9 График распределения ОМ по статусу

Над графиком указано общее количество ОМ и количество ОМ на техобслуживании. Области разного цвета обозначают количество ОМ в определенном статусе:

- зеленый цвет — ОМ в статусе «Мониторинг»;
- красный цвет — ОМ в статусе «Деактивирован»;
- серый цвет — ОМ в статусе «Недоступен».

Под графиком указано количество ОМ в каждом статусе.

Количество объектов мониторинга по проблемности

График, показывающий распределение ОМ по наличию у них проблем на данный момент времени.

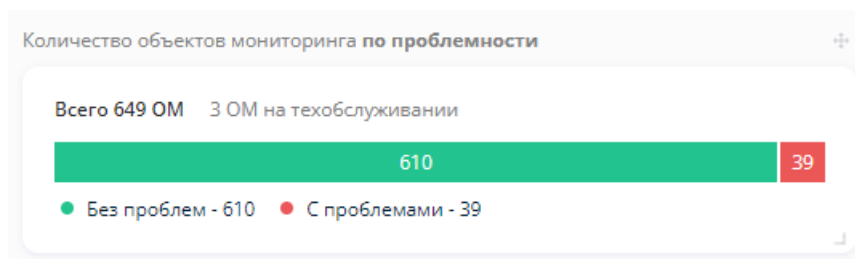


Рис. 4-10 График распределения ОМ по проблемности

Над графиком указано общее количество ОМ и количество ОМ на техобслуживании. Области разного цвета обозначают количество ОМ:

- зеленый цвет – ОМ без проблем;
- красный цвет – ОМ с проблемами.

Под графиком указано количество ОМ каждой проблемности.

Изменение количества объектов мониторинга

В разделе «Изменение количества объектов мониторинга» отображаются разные графики в зависимости от выбора значения над графиком.

- Если выбрать значение «По статусу», отображается график, показывающий изменение количества ОМ в разных статусах относительно указанного промежутка времени. Данные на графике отображаются с момента подключения сервера мониторинга.

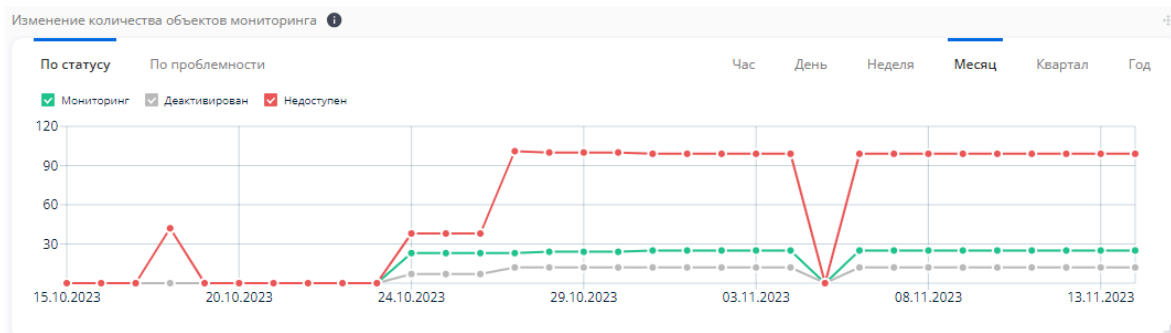


Рис. 4-11 График изменения количества объектов мониторинга относительно времени по статусу

Справа над графиком можно выбрать временной промежуток для отображения данных. При переходе на другую страницу или перезагрузке текущей страницы сохраняется последний выбранный пользователем временной промежуток. Пики графика показывают количество ОМ, зафиксированное в конце каждого временного промежутка.

Пример:

Для временного промежутка длиной 5 минут (с 11:30 до 11:35) будет зафиксировано то количество ОМ, которое актуально в 11:35.

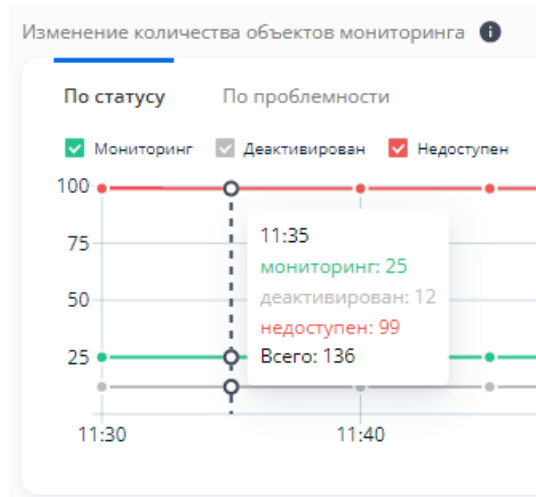


Рис. 4-12 Количество ОМ, зафиксированное в конце временного промежутка

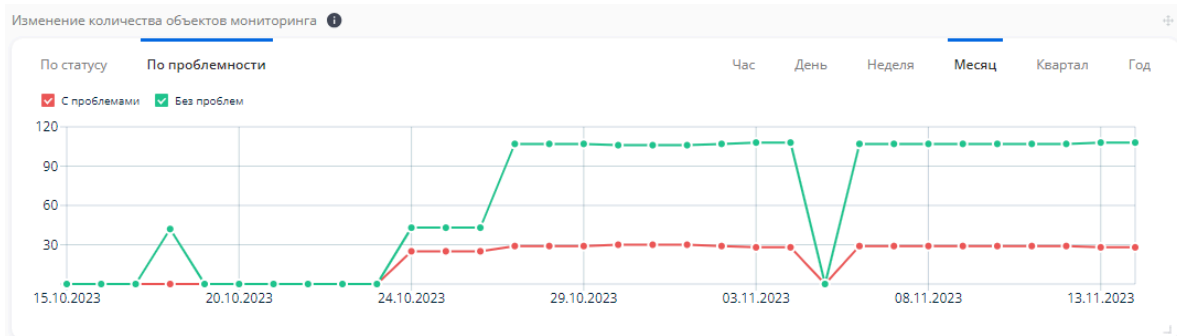
На графике на горизонтальной оси указано время, на вертикальной оси – количество ОМ.

При наведении курсора на точку графика отображается всплывающая подсказка со следующей информацией:

- дата или время для выбранной точки графика;
- статус и количество ОМ в этом статусе в указанный момент времени.

С помощью чекбоксов над графиком можно выбрать статусы ОМ для отображения. По умолчанию включено отображение ОМ во всех статусах. Для отключения отображения ОМ в определенном статусе отмените выбор чекбокса слева от названия этого статуса.

- Если выбрать значение «По проблемности», отображается график, показывающий изменение количества ОМ относительно указанного промежутка времени по проблемам. Данные на графике отображаются с момента подключения сервера мониторинга.



Справа над графиком можно выбрать временной промежуток для отображения данных. Пики графика показывают количество ОМ, зафиксированное в конце каждого временного промежутка.

Рис. 4-13 График изменения количества объектов мониторинга относительно времени по проблемам

Пример:

Для временного промежутка длиной 5 минут (с 16:00 до 16:05) будет зафиксировано то количество ОМ, которое актуально в 16:05.

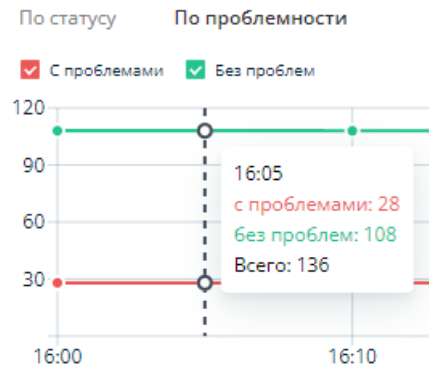


Рис. 4-14 Количество ОМ, зафиксированное в конце временного промежутка

На графике на горизонтальной оси указано время, на вертикальной оси – количество ОМ.

При наведении курсора на точку графика отображается всплывающая подсказка со следующей информацией:

- дата или время для выбранной точки графика;
- количество ОМ без проблем и с проблемами, а также суммарное количество ОМ в указанный момент времени.

С помощью чекбоксов над графиком можно выбрать проблемность ОМ для отображения. По умолчанию включено отображение ОМ любой проблемности. Для отключения отображения ОМ с наличием или отсутствием проблем отмените выбор соответствующего чекбокса.

Количество нерешенных проблем по важности

Круговая диаграмма, показывающая распределение нерешенных проблем по важности на данный момент времени.

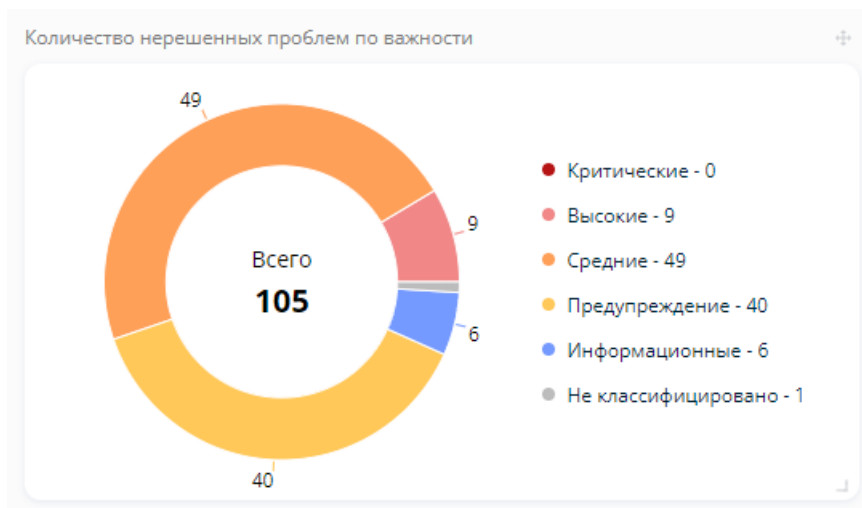


Рис. 4-15 Нерешенные проблемы по важности

В центре графика указано общее количество нерешенных проблем. Области разного цвета обозначают количество проблем определенной важности, при наведении курсора на каждую область появится всплывающая подсказка с названием уровня важности проблемы. Справа от диаграммы указано количество проблем каждого уровня важности.

Изменение количества проблем

График, показывающий количество нерешенных проблем относительно времени по важности. Данные на графике отображаются с момента подключения сервера мониторинга.

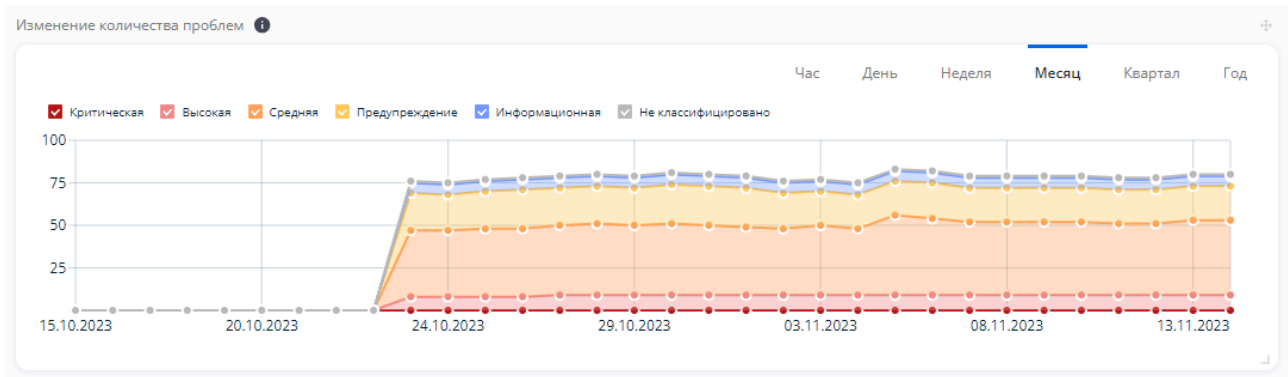


Рис. 4-16 График изменения количества проблем

Справа над графиком можно выбрать временной промежуток для отображения данных. При переходе на другую страницу или перезагрузке текущей страницы сохраняется последний выбранный пользователем временной промежуток.

На графике на горизонтальной оси указано время, на вертикальной оси — количество проблем. Данные графика отображаются суммарно: значения по вертикальной оси соответствуют сумме проблем разной степени важности. Чтобы узнать точное количество проблем определенного уровня важности, наведите курсор на точку графика для отображения всплывающей подсказки со следующей информацией:

- дата или время для выбранной точки графика;
- уровень важности проблемы и количество проблем этого уровня в указанный момент времени;
- общее количество проблем в указанный момент времени.

Пики графика показывают количество проблем, зафиксированное в конце каждого временного промежутка.

Пример:

Для временного промежутка длиной 1 час (с 10:21 до 11:21) будет зафиксировано то количество проблем, которое актуально в 11:21.

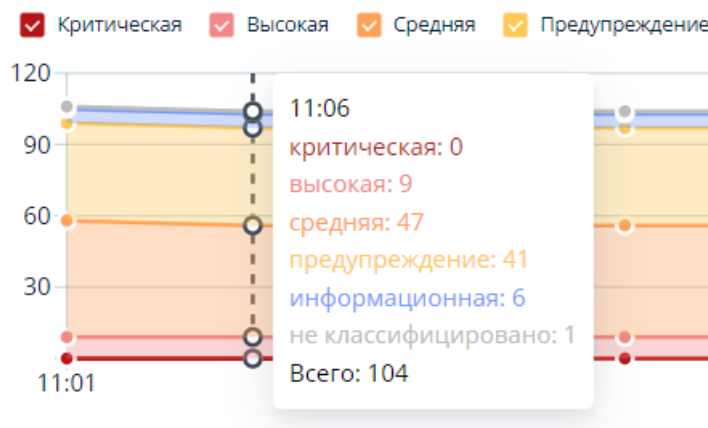


Рис. 4-17 Количество проблем, зафиксированное в конце временного промежутка

С помощью чекбоксов над графиком можно выбрать уровни важности проблем для отображения. По умолчанию включено отображение проблем всех уровней важности. Для отключения отображения проблем определенного уровня важности отмените выбор чекбокса слева от названия этого уровня важности.

Чтобы наблюдать за графиками длительное время без необходимости совершения действий для продления сессии, рекомендуется создать пользователя с ролью «Оператор мониторинга». Подробнее см. в разделах 5.1 Роли пользователей и доступные им интерфейсы (96) и 4.8.2.2 Создание учетной записи локального пользователя (68).

4.3. Серверы мониторинга


Раздел основного меню *Серверы мониторинга* содержит список подключенных серверов мониторинга.


Филиал	Сервер	Доступность	Сбор данных	IP-адрес	Версия ПО	Объектов	Проблем
Филиал Алексеевский	demo-rel-itm-vmk1	Активен	✓	10.51.16.167	ITM-K v.1.6.0.2	30	523
КС1	zabbix-proxy-docker			10.51.16.11		1	0
Филиал Петровский	eng-itm-vmk2	Активен	✓	10.51.16.164	ITM-K v.1.6.0.1	57	47326
Цех №1	test			addr		0	0
Цех №2	eng-itm-a1-new2			10.51.203.165		15	39996
ЭСН	fasd fasd est-proxy			10.51.16.168		0	0





Рис. 4-18 Список серверов мониторинга

Строка информации над списком серверов содержит следующие элементы:

1. Название «Серверы мониторинга».

2. Кнопка обновления  – при нажатии на кнопку осуществляется обновление данных на странице с сохранением настроенного пользователем представления. Через 1 минуту рядом с кнопкой появляется счетчик времени с момента обновления страницы. Время отображается только в минутах.
3. Блок общей информации о серверах. Серверов мониторинга:
 - a. активных – отображает количество активных подключенных серверов;
 - b. всего – отображает общее количество подключенных серверов.
4. Кнопка «Добавить сервер» – при нажатии на кнопку появляется окно добавления нового сервера мониторинга (см.п. 4.3.1 Подключение нового сервера мониторинга к ИТМ-VM (28)).
5. Кнопка «Настройка сбора данных» – при нажатии на кнопку появляется окно настройки периодичности получения данных от подключенных серверов мониторинга (см.п. 4.3.2 Настройка сбора данных (30)).
6. Строка поиска – предназначена для осуществления поиска по полям «Филиал», «Сервер», «IP-адрес», «Объектов», «Проблем» всех серверов мониторинга, в том числе не отображаемых на данной странице (если список серверов занимает несколько страниц).
7. Кнопка «Свернуть все»/«Развернуть все»:
 - Если количество записей в таблице меньше 20, то при открытии страницы все записи развернуты, кнопка находится в состоянии «Свернуть все» и позволяет свернуть все записи в таблице.
 - Если количество записей в таблице больше 20, то при открытии страницы все записи свернуты, кнопка в состоянии «Развернуть все» и позволяет развернуть все записи в таблице.

В таблице отображается список подключенных серверов мониторинга. Если к серверу мониторинга подключен хотя бы один сервер удаленного мониторинга, то в таблице в начале строки с этим сервером мониторинга отображается кнопка , а ниже отображаются дополнительные строки с подключенными серверами удаленного мониторинга.

- Чтобы скрыть строки с подключенными серверами удаленного мониторинга, нажмите на кнопку . При этом вид кнопки изменится на .
- Чтобы развернуть дополнительные строки с серверами удаленного мониторинга, нажмите на кнопку . При этом вид кнопки изменится на .

По умолчанию строки с подключенными серверами удаленного мониторинга развернуты.

В таблице отображаются следующие основные свойства серверов:

- Филиал. Значение этого свойства зависит от того, информация о каком сервере указана в строке:
 - для сервера мониторинга – наименование филиала, где размещен сервер;
 - для сервера удаленного мониторинга – наименование объекта из свойств сервера UDV-ITM-RM;
- Сервер – наименование сервера;




- Доступность – статус сервера мониторинга:
 - Активен – подключенный сервер мониторинга нормально функционирует. Статус присваивается, если при последнем обмене информацией с сервером мониторинга получены данные без ошибок.
 - Недоступен – при последнем обмене информацией с сервером мониторинга ответ от сервера мониторинга не получен. При наведении курсора на ячейку появится всплывающая подсказка с текстом ошибки.
 - Ошибка – при последнем обмене информацией с сервером мониторинга получена ошибка. При наведении курсора на ячейку появится всплывающая подсказка с текстом ошибки.
 - Отключен – обмен информацией с сервером мониторинга отключен администратором.


 **Прим.:**

Временное отключение сервера используется для технических целей, таких как проведение технического обслуживания, устранение неисправностей, настройка и т.п.

- Пустое значение – нет данных о статусе последней синхронизации сервера.

Для сервера удаленного мониторинга это свойство не заполняется.

- Сбор данных – результат синхронизаций этого сервера мониторинга. Возможные значения:
 -  – все типы синхронизаций успешны;
 -  – синхронизация хотя бы одного типа завершена с ошибкой или ни разу не выполнялась;
 -  – все типы синхронизаций завершены с ошибкой или не выполнялись.

 Подсказка:

При наведении курсора на ячейку столбца «Сбор данных» отображается всплывающая подсказка, где указан статус последней синхронизации и серверное время на момент ее окончания. Если какая-либо из задач синхронизации еще ни разу не завершилась, то на месте статуса и времени синхронизации ставится прочерк.

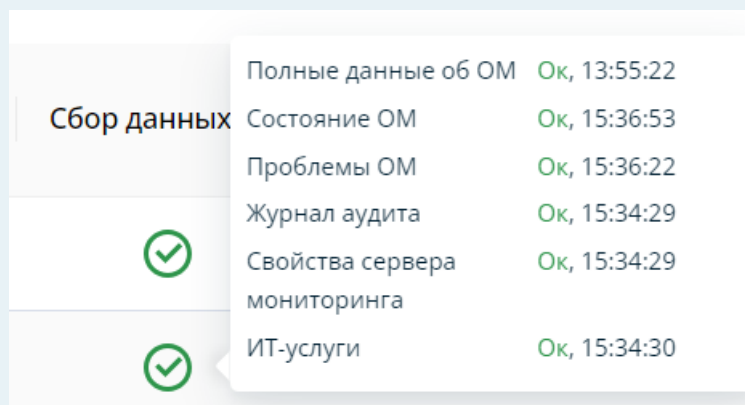


Рис. 4-19 Подсказка с задачами синхронизации



Для сервера удаленного мониторинга это свойство не заполняется.


- IP-адрес – IP-адрес сервера;
- Версия ПО – версия подключенного сервера мониторинга;

 Прим.:

При обновлении ПО сервера мониторинга, сервер ITM-VM версии 1.6.0 не обновляет версию ПО этого сервера мониторинга автоматически. Для обновления информации о версии ПО нужно отключить и заново подключить обновленный сервер мониторинга. Данные о проблемах при этом подгружаются заново.

Для сервера удаленного мониторинга это свойство не заполняется.

- Объектов – количество объектов мониторинга, подключенных к серверу;
- Проблем – количество проблем объектов мониторинга, подключенных к данному серверу;
- Кнопки действий:
 - Кнопка  – при нажатии на кнопку выполняется внеплановый сбор данных с сервера мониторинга. Если в момент нажатия на кнопку уже запущен процесс синхронизации, то выводится ошибка «В настоящий момент обновление данных уже выполняется»;
 - Кнопка  – при нажатии на кнопку открывается окно изменения свойств сервера мониторинга (см. п. 4.3.3 Просмотр информации о подключенном сервере мониторинга (32));

- Кнопка  – при нажатии на кнопку осуществляется переход в собственную панель управления сервером UDV-ITM-M в новой вкладке браузера.

Для сервера удаленного мониторинга кнопки отсутствуют.

Можно отсортировать записи таблицы по полям «Филиал», «Сервер», «Доступность», «Сбор данных».

По клику на строку записи таблицы открывается карточка соответствующего сервера мониторинга или сервера удаленного мониторинга с подробной информацией о нем (подробнее см. в разделах 4.3.3 Просмотр информации о подключенном сервере мониторинга (32) и 4.3.8 Просмотр свойств сервера удаленного мониторинга (38)).

Прим.:

Если версия подключенного сервера мониторинга будет обновлена, UDV-ITM-VM автоматически обновит версию этого сервера мониторинга во время ближайшей синхронизации. После этого сбор данных с подключенного сервера мониторинга продолжится. Для успешного обновления UDV-ITM-VM должен поддерживать новую версию подключенного сервера мониторинга. Список поддерживаемых версий см. в разделе 5.2 Совместимость компонентов решения для UDV-ITM-VM (96).

В этом разделе:

- 4.3.1 Подключение нового сервера мониторинга к ITM-VM (28)
- 4.3.2 Настройка сбора данных (30)
- 4.3.3 Просмотр информации о подключенном сервере мониторинга (32)
- 4.3.4 Изменение свойств подключенного сервера мониторинга (35)
- 4.3.5 Отключение автоматического сбора данных с сервера мониторинга (36)
- 4.3.6 Включение автоматического сбора данных с сервера мониторинга (37)
- 4.3.7 Удаление подключенного сервера мониторинга (37)
- 4.3.8 Просмотр свойств сервера удаленного мониторинга (38)
- 4.3.9 Изменение названия ТО сервера удаленного мониторинга (39)

4.3.1. Подключение нового сервера мониторинга к ITM-VM

В качестве сервера мониторинга можно подключить сервер UDV-ITM-M или сервер с установленным ПО Zabbix, перечень поддерживаемых версий см. в разделе 5.2 Совместимость компонентов решения для UDV-ITM-VM (96).

Для подключения сервера мониторинга:

1. Перейдите в раздел *Серверы мониторинга*.
2. Нажмите на кнопку «Добавить сервер».

Результат шага: Появится окно подключения сервера мониторинга.

3. Заполните следующие поля:

- a. IP-адрес – IP-адрес IPv4 сервера мониторинга;
- b. Порт – номер TCP порта для подключения к серверу, значение по умолчанию 443;
- c. Логин – логин учетной записи сервера UDV-ITM-M с правами доступа к API;
- d. Пароль – пароль учетной записи сервера UDV-ITM-M с правами доступа к API.

Подключение сервера мониторинга ✕

IP-адрес *

Порт *

Логин *

Пароль *

👁

ПодключитьОтменить

Рис. 4-20 Подключение сервера мониторинга. Авторизация

4. Нажмите на кнопку «Подключить» для авторизации на подключаемом сервере.

Результат шага: Появится окно «Добавление сервера мониторинга».

i Подсказка:

Возможные ошибки и способы их устранения:

- «Такой сервер уже подключен» – проверьте и при необходимости исправьте IP-адрес. Если IP-адрес верный, указанный сервер можно найти и настроить в списке серверов.
- «Ошибка подключения» – проверьте корректность IP-адреса и TCP порта.
- «Неверный логин или пароль» – проверьте правильность логина и пароля.
- «Данная версия ПО не поддерживается» – указанный сервер не может быть подключен, так как его программное обеспечение не поддерживается. Список совместимого ПО см. на странице 5.2 Совместимость компонентов решения для UDV-ITM-VM (96).

5. В окне «Добавление сервера мониторинга» заполните следующие поля:

- a. «Наименование сервера»:

- Если вы подключаете сервер UDV-ITM-M, то поле будет автоматически заполнено именем сервера и недоступно для редактирования.
 - Если вы подключаете сервер с ПО Zabbix, то это поле нужно заполнить, т.к. это требуется в том числе для событий, отправляемых в SIEM. Допускаются символы a-z, -, 0-9, - не может быть первым символом. Максимальная длина 253 символа.
- б. «Наименование филиала» – обязательное поле.
- с. «Описание» – заполните при необходимости.

Добавление сервера мониторинга ✕

Наименование сервера *

Версия ПО: ИТМ-К v1.4 или предыдущие версии

Наименование филиала *

IP-адрес: 10.51.16.10

Порт: 443

ДАТАРК:

Описание

Рис. 4-21 Добавление сервера мониторинга. Свойства

6. Нажмите на кнопку «Подключить» для сохранения информации о подключаемом сервере.

Результат шага:

Сервер будет подключен и будет запущен процесс полной синхронизации данных. Полный список параметров, которые будут получены с сервера мониторинга, можно увидеть, нажав на кнопку «Настройки сбора данных». В дальнейшем получение данных с сервера будет выполняться в соответствии с указанными параметрами.

4.3.2. Настройка сбора данных

Для настройки сбора данных:

1. Перейдите в раздел *Серверы мониторинга*.
2. Нажмите на кнопку «Настройка сбора данных».

Результат шага: Появится окно настройки сбора данных.

3. Измените необходимые вам параметры:

- Полных данных об объектах мониторинга – период получения полных данных, в том числе инвентарных данных об объектах мониторинга, подключенных к серверам мониторинга. Значение по умолчанию – 480 минут. Диапазон допустимых значений: 1 – 1440 минут.
- Данных о состоянии объектов мониторинга – период получения информации о состоянии (статусах) объектов мониторинга, подключенных к серверам мониторинга. Значение по умолчанию – 3 минуты. Диапазон допустимых значений: 1 – 60 минут.
- Данных о проблемах – период получения данных о проблемах объектов мониторинга, подключенных к серверам мониторинга. Значение по умолчанию – 1 минута. Диапазон допустимых значений: 1 – 60 минут.
- Журналов аудита – период синхронизации журналов аудита. Значение по умолчанию – 3 минуты. Диапазон допустимых значений: 1 – 60 минут.
- Свойств сервера мониторинга – период синхронизации системных параметров серверов UDV-ITM-M. Значение по умолчанию – 3 минуты. Диапазон допустимых значений: 1 – 60 минут.
- Данных о состоянии ИТ-услуг – период обновления данных о состоянии ИТ-услуг. Значение по умолчанию – 3 минуты. Диапазон допустимых значений: 1 – 60 минут.

Значения всех параметров указаны в минутах.

 **Внимание:**

Если ввести значение меньше указанного диапазона, оно автоматически будет заменено на минимальное допустимое значение. Значение больше указанного диапазона заменяется на максимальное допустимое.

Настройки сбора данных ✕

Параметры сбора данных применяются ко всем подключенным серверам мониторинга сразу после сохранения формы

Полных данных об объектах мониторинга, мин *

Данных о состоянии объектов мониторинга, мин *

Данных о проблемах, мин *

Журналов аудита, мин *

Свойств сервера мониторинга, мин * ?

Данных о состоянии ИТ-услуг, мин *

Рис. 4-22 Настройки сбора данных

4. Нажмите на кнопку «Сохранить».

4.3.3. Просмотр информации о подключенном сервере мониторинга

Окно просмотра информации о подключенном сервере появляется:

- при нажатии в любом месте строки конкретного сервера мониторинга на странице *Серверы мониторинга*;
- при нажатии на значение столбца «Филиал» на страницах *Объекты мониторинга* и *Проблемы*.

На страницах *Объекты мониторинга* и *Проблемы* все поля карточки выводятся в режиме просмотра без возможности изменения.

Свойства сервера мониторинга ✕

Наименование: eng-itm-vmk2

Версия ПО: ITM-K v.1.6.0.1

Наименование филиала: Филиал Петровский

Доступность: Активен

Сбор данных: Без ошибок ⓘ

Последняя синхронизация: 08.12.2023, 11:14:21

ID: 2

IP-адрес: 10.51.16.164

Порт: 443

DATAPK: sync-datapk-6

Описание: Сервер мониторинга в сегменте АСУ ТП


	Всего	Активно	Неактивно
Узлы сети	59	52	7
Шаблоны	48		
Элементы данных	3325	3159	166
Триггеры	1736	1687	49
ИТ-услуги	7		
Проблемы	8004		

[Перейти к серверу](#)
Изменить
Заккрыть

Рис. 4-23 Окно просмотра информации о подключенном сервере

В окне выводится информация о подключенном сервере:

- Наименование сервера;
- Версия ПО – версия подключенного сервера UDV-ITM-M или Zabbix;


 **Прим.:**

При обновлении ПО сервера мониторинга, сервер ITM-VM версии 1.6.0 не обновляет версию ПО этого сервера мониторинга автоматически. Для обновления информации о версии ПО нужно отключить и заново подключить обновленный сервер мониторинга. Данные о проблемах при этом подгрузятся заново.

- Наименование филиала;
- Доступность – актуальный статус сервера;
- Сбор данных – результат синхронизаций этого сервера. Возможные значения:
 - Без ошибок – все типы синхронизаций успешны;

- Нестабильно — синхронизация хотя бы одного типа завершена с ошибкой или ни разу не выполнялась;
- Отсутствует — все типы синхронизаций завершены с ошибкой или не выполнялись;

Подсказка:

При наведении курсора на иконку  отображается всплывающая подсказка, где указан статус последней синхронизации и серверное время на момент ее окончания. Если какая-либо из задач синхронизации еще ни разу не завершилась, то на месте статуса и времени синхронизации ставится прочерк.

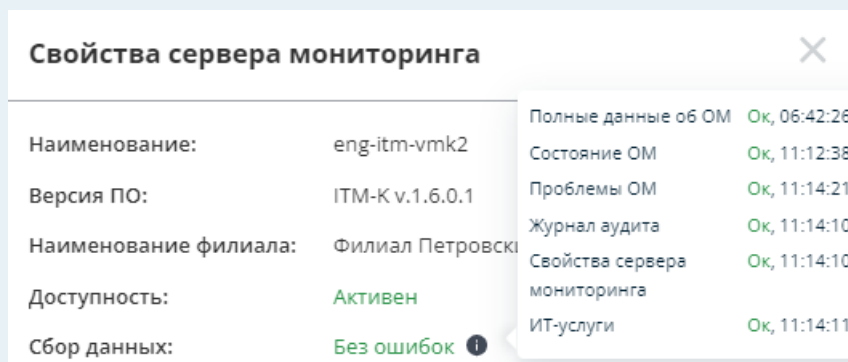


Рис. 4-24 Подсказка с задачами синхронизации

- Последняя синхронизация — дата и время последнего обновления информации о сервере;
- ID — идентификатор сервера UDV-ITM-M в базе данных сервера UDV-ITM-VM;
- IP-адрес;
- Порт;
- DATAPK — имя DATAPK, подключенного к серверу мониторинга;
- Описание;
- Таблица с параметрами конфигурации сервера мониторинга. В таблице отображаются основные параметры актуальной конфигурации сервера:
 - Узлы сети:
 - Всего — общее количество узлов сети;
 - Активно — все узлы сети, которые активны для мониторинга на сервере UDV-ITM-M или Zabbix, в том числе недоступные;
 - Неактивно — только те узлы сети, которые деактивированы администратором на сервере UDV-ITM-M или Zabbix.
 - Шаблоны — общее количество шаблонов в столбце «Всего».
 - Элементы данных:
 - Всего;
 - Активно;
 - Неактивно.
 - Триггеры:
 - Всего;
 - Активно;

- Неактивно.
- ИТ-услуги — общее количество ИТ-услуг в столбце «Всего».
- Проблемы — общее количество проблем (как решенных, так и нерешенных), которые хранятся в данный момент на сервере UDV-ITM-VM. Значение выводится в столбце «Всего» и соответствует количеству проблем этого филиала на странице *Проблемы*.


При переходе по ссылке «Перейти к серверу» открывается страница сервера мониторинга.

При нажатии на кнопку «Изменить» выполняется переход к окну изменения свойств сервера.

4.3.4. Изменение свойств подключенного сервера мониторинга

Для изменения свойств подключенного сервера мониторинга:

1. Перейдите в раздел *Серверы мониторинга*.

2. Нажмите на кнопку «Настройка»  в списке серверов или на кнопку «Изменить» в окне просмотра информации о подключенном сервере.

Прим.:

Подробнее про окно информации о сервере см. в разделе 4.3.3 Просмотр информации о подключенном сервере мониторинга (32).

Результат шага: Появится окно изменения свойств сервера мониторинга.

3. Измените свойства сервера:

Прим.:

Свойства полей соответствуют описанию на странице 4.3.1 Подключение нового сервера мониторинга к ITM-VM (28).

- Наименование филиала;
- IP-адрес;
- Порт;
- Логин;
- Пароль;
- Описание.

Изменение свойств сервера мониторинга ✕

Наименование: eng-itm-vmk2

Версия ПО: ITM-K v.1.6.0.1

Наименование филиала *

Филиал Петровский

Доступность: Активен

Сбор данных: Без ошибок ⓘ

ID: 2

IP-адрес * Порт *

10.51.16.164

443

Логин * Пароль

datapkitm

***** 👁

DATAPK: sync-datapk-6

Описание

Сервер мониторинга в сегменте АСУ ТП

⏪ 🗑 **Сохранить** Отменить

Рис. 4-25 Окно изменения свойств сервера мониторинга

Прим.:

полное описание свойств сервера см. в разделе [4.3.3 Просмотр информации о подключенном сервере мониторинга \(32\)](#).

4. Нажмите «Сохранить» для сохранения измененных значений.


⚠ Внимание:

Если поля в карточке не менялись, то кнопка недоступна для нажатия.


4.3.5. Отключение автоматического сбора данных с сервера мониторинга

Для отключения автоматического сбора данных с сервера мониторинга:

1. Перейдите на страницу *Серверы мониторинга*.

- Нажмите на кнопку «Настройка»  в списке серверов или на кнопку «Изменить» в окне просмотра информации о подключенном сервере.

Результат шага: Появится окно изменения свойств сервера мониторинга.

- Нажмите на кнопку  для приостановки автоматического сбора данных с сервера мониторинга.

Результат шага: Появится всплывающее окно «Отключение сервера».

- Нажмите «Отключить» для подтверждения действия.

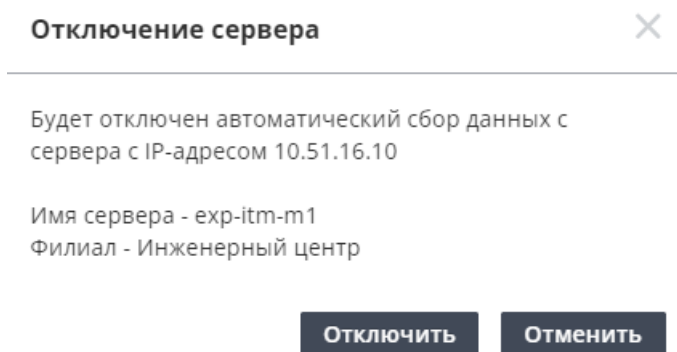



Рис. 4-26 Окно «Отключение сервера»


- Нажмите на кнопку «Сохранить» в окне изменения свойств сервера мониторинга.

4.3.6. Включение автоматического сбора данных с сервера мониторинга


Для включения автоматического сбора данных с сервера мониторинга:

- Перейдите на страницу *Серверы мониторинга*.
- Нажмите на кнопку «Настройка»  в списке серверов или на кнопку «Изменить» в окне просмотра информации о подключенном сервере.

Результат шага: Появится окно изменения свойств сервера мониторинга.

- Нажмите на кнопку  для возобновления автоматического сбора данных с сервера мониторинга.
- Нажмите на кнопку «Сохранить».

4.3.7. Удаление подключенного сервера мониторинга

- Перейдите в раздел *Серверы мониторинга*.
- Нажмите на кнопку «Настройка»  в списке серверов или на кнопку «Изменить» в окне просмотра информации о подключенном сервере.

Результат шага: Появится окно изменения свойств сервера мониторинга.

3. Нажмите на кнопку «Удалить»  для удаления сервера мониторинга.

Результат шага: Появится модальное окно «Удаление сервера».

4. Нажмите «Удалить» для подтверждения действия.

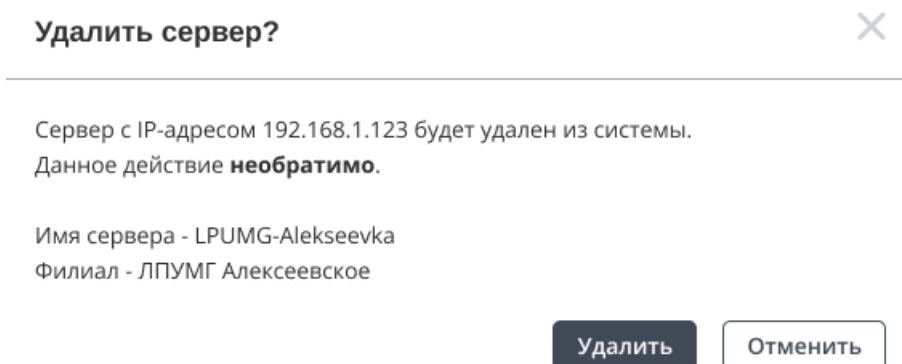


Рис. 4-27 Окно «Удаление сервера»

Результат шага: При удалении сервера мониторинга из системы удаляются связанные с ним ОМ и проблемы этих ОМ.

4.3.8. Просмотр свойств сервера удаленного мониторинга

Окно просмотра информации о сервере удаленного мониторинга появляется:

- при нажатии в любом месте строки конкретного сервера удаленного мониторинга на странице *Серверы мониторинга*;
- при нажатии на значение столбца «ТК» на страницах *Объекты мониторинга* и *Проблемы*.

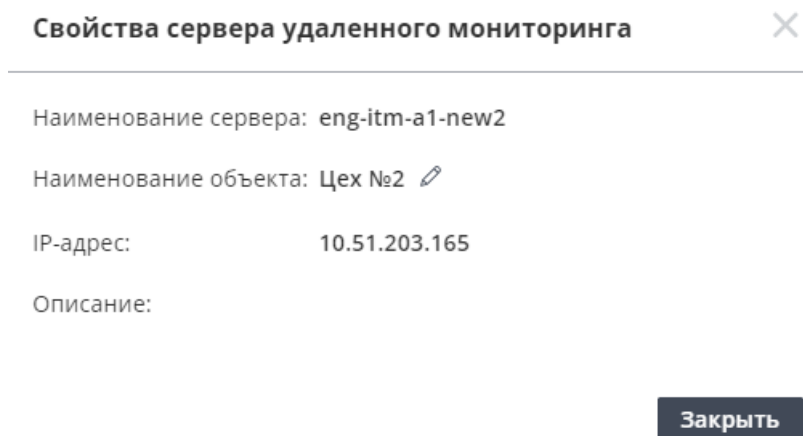


Рис. 4-28 Свойства сервера удаленного мониторинга


Окно содержит следующие свойства:

- Наименование сервера — имя сервера удаленного мониторинга UDV-ITM-RM;

- Наименование объекта – имя ТК, где находятся ОМ сервера удаленного мониторинга;
- IP-адрес – IP-адрес сервера удаленного мониторинга;
- DNS-имя – DNS-имя сервера удаленного мониторинга;
- Описание – описание сервера удаленного мониторинга.

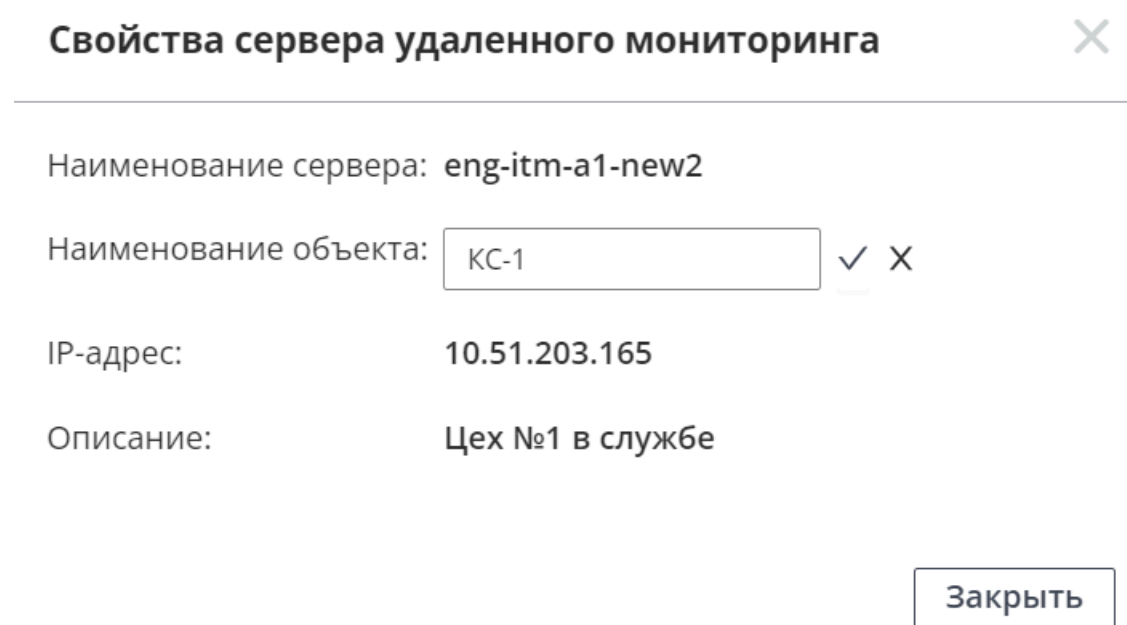
4.3.9. Изменение названия ТО сервера удаленного мониторинга

Для изменения названия ТК сервера удаленного мониторинга:

1. Откройте окно «Свойства сервера агентов» одним из способов:
 - Нажмите в любом месте строки конкретного сервера удаленного мониторинга на странице *Серверы мониторинга*.
 - Нажмите на значение столбца «ТК» на странице *Объекты мониторинга* или *Проблемы*.
2. В окне свойств сервера удаленного мониторинга нажмите на кнопку  рядом с полем «Наименование объекта».

Результат шага: Поле станет доступно для редактирования.

3. Измените название ТК.



Свойства сервера удаленного мониторинга ✕

Наименование сервера: eng-itm-a1-new2

Наименование объекта: ✓ ✕

IP-адрес: 10.51.203.165

Описание: Цех №1 в службе

Закреть

Рис. 4-29 Изменение названия объекта сервера удаленного мониторинга

4. Нажмите на кнопку ✓ для сохранения изменений.

 **Прим.:**

Для отмены изменений нажмите на кнопку ✕.

5. Нажмите на кнопку «Закреть».

4.4. Объекты мониторинга

Раздел *Объекты мониторинга* отображает информацию обо всех объектах мониторинга на уровне предприятия с возможностью фильтрации по серверам уровня филиалов и серверам уровня технологический комплексов.

В этом разделе:

- 4.4.1 Список объектов мониторинга (40)
- 4.4.2 Просмотр информации об объекте мониторинга (43)

4.4.1. Список объектов мониторинга

Список выводится при нажатии в боковом меню на раздел *Объекты мониторинга*.

Наименование	Мониторинг	Филиал	ТК	Проблемы	АСУ ТП	IP-адрес	ОС	ТО	Тип ОМ	Обновлен	Ссылки
АРМ инженера		Филиал Алексеевс...		1		192.168.243.160				07.12.2023, 15:47:02	
ИБП цеха 1		Филиал Петровский		2	Цех 1	10.30.133.11			Smart-UP...	07.12.2023, 15:47:02	
Ноутбук дизайнера		Филиал Петровский				10.30.133.11			Smart-UP...	07.12.2023, 15:47:02	
Ноутбук инженера АСУ		Филиал Петровский		2		10.30.133.11			Smart-UP...	07.12.2023, 15:47:02	
Ноутбук инженера ДАТАРК		Филиал Петровский		1		10.41.56.41				07.12.2023, 15:47:02	
Ноутбук инженера ITM		Филиал Петровский				10.41.56.14				07.12.2023, 15:47:02	
Телефон инженера		Филиал Петровский		1		192.168.7.18				07.12.2023, 15:47:02	
Коммутатор цеха № 2		Филиал Петровский	Цех №2			10.51.203.37	Linux version 3...			07.12.2023, 15:47:02	

Рис. 4-30 Список объектов мониторинга

Над списком ОМ выводится название «Объекты мониторинга».

Рядом с названием отображаются:

- Счетчик объектов мониторинга. Если никакие фильтры не применены, счетчик показывает общее количество ОМ. Если применены какие-либо фильтры, счетчик показывает количество отфильтрованных ОМ/общее количество ОМ.
- Кнопка обновления данных на странице . Через 1 минуту рядом с кнопкой появляется счетчик времени с момента обновления страницы. Время отображается только в минутах.

Список объектов мониторинга можно отфильтровать или отсортировать.

Внимание:

При обновлении страницы в браузере или переходе на другую страницу выбранные фильтры и сортировка будут сброшены. При обновлении страницы с помощью кнопки («Обновить данные») фильтры и сортировка не сбрасываются.

Фильтры

Ниже строки с названием находится фильтр «Филиал/ТК», который позволяет отобразить все ОМ выбранных филиалов или ТК. При нажатии на поле фильтра появляется выпадающий список с имеющимися филиалами и ТК.

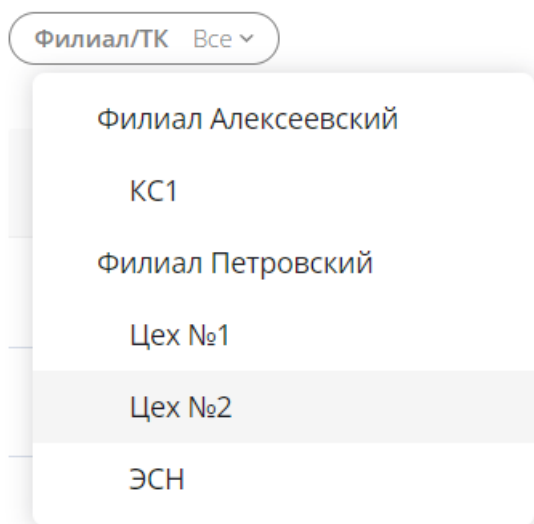




Рис. 4-31 Фильтр «Филиал/ТК»

При выборе филиала входящие в него ТК не выбираются автоматически. Выбор ТК доступен независимо от того, выбран ли филиал, к которому он относится. Если у филиала 5 или больше вложенных ТК, становятся доступны кнопки:

- «Выделить все» – нажмите, чтобы выбрать все ТК, входящие в филиал.
- «Снять выделение» – нажмите, чтобы отменить выбор всех ТК, входящих в филиал.

В списках фильтров можно выбрать одно или несколько значений.

- Чтобы закрыть список и применить фильтр, после выбора всех нужных значений кликните вне области фильтра.
- Чтобы отменить выбор конкретного значения, еще раз кликните по этому значению в выпадающем списке.
- Чтобы сбросить примененный фильтр целиком, нажмите на кнопку  в области фильтра.
- Чтобы сбросить сразу все выбранные фильтры, нажмите на кнопку  справа от фильтра.

Сортировка

По умолчанию ОМ отсортированы по возрастанию по следующим столбцам:

- Филиал;
- ТК (внутри филиала);
- Наименование (внутри ТК/филиала).

Можно отсортировать ОМ вручную по наименованию или филиалу.

Свойства объектов мониторинга

Для просмотра полного списка ОМ используется вертикальная прокрутка списка справа.

В списке отображаются следующие свойства объектов мониторинга:




- Наименование (отображаемое имя ОМ).
- Мониторинг – индикатор статуса объекта мониторинга. Возможные значения:
 -  Активирован – активирован и доступен по одному из каналов мониторинга. Статус «Активирован» не отображается при использовании мониторинга по протоколу WMI.
 -  Недоступен – объект мониторинга недоступен ни по одному из каналов мониторинга
 -  Деактивирован – объект мониторинга деактивирован администратором сервера мониторинга.
- Филиал – наименование сервера мониторинга, к которому подключен ОМ. При нажатии на значение этого столбца открывается окно «Свойства сервера мониторинга». Подробнее см. в разделе 4.3.3 Просмотр информации о подключенном сервере мониторинга (32).
- ТК – наименование сервера удаленного мониторинга, к которому подключен ОМ. При нажатии на значение этого столбца открывается окно «Свойства сервера агента». Подробнее см. в разделе 4.3.8 Просмотр свойств сервера удаленного мониторинга (38).
- Проблемы – количество проблем ОМ. При нажатии на количество проблем появится всплывающее окно со списком проблем.



Рис. 4-32 Окно со списком проблем ОМ

Проблемы в списке отсортированы по уровню критичности, сверху расположены наиболее важные. В списке отображается не более 5 проблем.

Внизу окна находится ссылка «Открыть полный список проблем». При нажатии на ссылку в новой вкладке откроется страница *Проблемы* с фильтрацией по выбранному ОМ и состоянию («Требуется решения»). Отфильтрованные проблемы также будут отсортированы по важности по убыванию.

Чтобы закрыть окно со списком проблем, нажмите на кнопку ✕.

- АСУ ТП – соответствует значению тега asu_tp. Поле не заполняется, если тег отсутствует.
- IP-адрес – IP-адрес интерфейса ОМ, по которому осуществляется мониторинг.
- ОС – операционная система ОМ.
- ТО – техническое обслуживание ОМ.

Если ОМ находится в состоянии технического обслуживания:

- поле содержит дату начала технического обслуживания ОМ;
- все значения строки этого ОМ серого цвета.



Если ОМ не находится в состоянии технического обслуживания:

- поле не заполняется;
- все значения строки этого ОМ черного цвета.

- Тип ОМ — тип объекта мониторинга, указанный в инвентарных данных ОМ.

 **Прим.:**

поле Тип ОМ соответствует типу ОЗ в DATAPK.

- Обновлен — дата и время последнего успешного обновления статуса ОМ или полных данных об ОМ.
- Ссылки — если на сервере мониторинга UDV-ITM-M или Zabbix в разделе инвентарных данных заполнено хотя бы одно из полей «URL A», «URL B», «URL C», то в этом разделе отобразится кнопка  . При нажатии на кнопку  откроется окно со списком ссылок.

URL A
https://10.51.16.164/

Рис. 4-33 Окно, содержащее ссылку из поля «URL A»

При нажатии на ссылку указанный веб-сайт откроется в новой вкладке браузера.

4.4.2. Просмотр информации об объекте мониторинга

Окно просмотра информации об объекте мониторинга появляется:

- при нажатии в любом месте строки конкретного ОМ на странице *Объекты мониторинга*, кроме значений в столбцах «Филиал», «ТК», «Проблемы» и кнопки в столбце «Ссылки»;
- при нажатии на значение в столбце «Объект» на странице *Проблемы*.

Все поля окна выводятся в режиме просмотра без возможности изменения.

ITM-K-Филиал №2 (164)
✕

ID: 65

Наименование: ITM-K-Филиал №2 (164)

Сетевое имя OM: eng-itm-vmk2

Статус: Активен

Обновление статуса: 08.12.2023, 14:39:52

Филиал: Филиал Петровский

Технологический комплекс:

Система:

Тип OM:

Операционная система: Linux version 4.19.79-1

Способ мониторинга: AGENT

Описание:

Обновление свойств OM: 08.12.2023, 06:42:26

Внешние ссылки

URL A <https://10.51.16.164/>

Сетевые интерфейсы

IP-адрес	DNS-имя
172.17.0.1	host.docker.internal

Закреть

Рис. 4-34 Окно просмотра информации об объекте мониторинга

Заголовок окна содержит имя объекта мониторинга.

Окно содержит следующие поля:

- ID – идентификатор объекта мониторинга;
- Наименование – видимое имя объекта мониторинга;
- Сетевое имя OM – сетевое имя объекта мониторинга, соответствует имени узла сети в UDV-ITM-M;
- Статус – актуальный статус объекта мониторинга. Соответствует статусу в столбце «Мониторинг» в списке OM. Доступные значения:
 - Активирован;
 - Недоступен;
 - Деактивирован.

Если OM находится на техническом обслуживании, информация о дате и времени начала технического обслуживания будет указана рядом со статусом OM.

- Обновление статуса – дата и время последнего обновления статуса объекта мониторинга. По умолчанию обновление статуса OM происходит каждые 3 минуты;
- Филиал – название филиала, где находится объект мониторинга;
- Технологический комплекс – название ТК, где находится объект мониторинга;

- Система – наименование защищаемой АСУ ТП;

 **Прим.:**

В UDV-ITM-M значение этого поля записано в теге asu_tp.

- Тип ОМ – тип объекта мониторинга, указанный в инвентарных данных ОМ;

 **Прим.:**


поле Тип ОМ соответствует типу ОЗ в DATAPK.


- Операционная система – операционная система объекта мониторинга, указанная в карточке инвентарных данных ОМ в UDV-ITM-M;
- Способ мониторинга – описывает, каким образом осуществляется мониторинг. Возможные значения:
 - Агент – получение данных с объектов мониторинга с применением агентов;
 - SNMP – получение данных с объектов мониторинга по протоколу SNMP;
 - JMX – получение данных с объектов мониторинга с использованием технологии JMX;
 - IPMI – получение данных с объектов мониторинга с использованием технологии IPMI.
- Описание – текстовое описание объекта мониторинга, внесенное на сервере UDV-ITM-M;
- Обновление свойств ОМ – дата и время последнего полного обновления информации об объекте мониторинга. По умолчанию обновление свойств ОМ происходит каждые 480 минут;
- Внешние ссылки – содержит ссылки, добавленные в качестве значения полей «URL А», «URL В», «URL С» в инвентарных данных на сервере мониторинга UDV-ITM-M или Zabbix. В окне отображаются только те поля, которые содержат ссылки. Если на сервере мониторинга не заполнено ни одно из полей «URL А», «URL В», «URL С», то раздел «Внешние ссылки» не будет отображаться.
- Сетевые интерфейсы – содержит список всех интерфейсов, которые есть у объекта мониторинга. Для каждого интерфейса указан IP-адрес или DNS-имя.

4.5. Мониторинг ИТ-услуг

Страница *ИТ-услуги* содержит список ИТ-услуг, мониторинг которых осуществляет подключенный сервер UDV-ITM-M или zabbix. В качестве ИТ-услуг для мониторинга могут подключаться различные системно-значимые ИТ-сервисы, каналы связи, сервисы ИБ и т.д.

Над списком ИТ-услуг расположены следующие элементы:

- Название «Мониторинг ИТ-услуг» и кнопка обновления страницы . Через 1 минуту рядом с кнопкой появляется счетчик времени с момента обновления страницы. Время отображается только в минутах.
- Переключатель «Показать отключенные». Позволяет скрыть из списка отключенные услуги, которые вам не нужно контролировать, либо отобразить все услуги, чтобы проверить актуальность списка контролируемых услуг для последующего включения. По умолчанию





переключатель выключен, при этом отключенные с помощью кнопки  услуги не отображаются в списке. При включении переключателя отключенные услуги отображаются в списке серым цветом.

- Кнопка «Свернуть все»/«Развернуть все»:
 - «Развернуть все» — отображается по умолчанию, при нажатии на кнопку будут развернуты все вложенные группы услуг и услуги и кнопка сменится на «Свернуть все».
 - «Свернуть все» — отображается, если развернута хотя бы одна строка филиала. При нажатии на кнопку все услуги и группы услуг будут свернуты до уровня филиалов и кнопка сменится на «Развернуть все».

 **Прим.:**



Кнопка «Свернуть все»/«Развернуть все» применяется ко всем записям, а не только к записям на текущей странице.


Список ИТ-услуг содержит следующую информацию:

- Услуга — столбец содержит список услуг, сгруппированный по филиалам и группам.
 - Филиал — наименование филиала, к которому относится сервер мониторинга, с которого получен список услуг. Филиал может содержать группы услуг и услуги. Филиал не отображается в таблице, если не содержит вложенных записей групп услуг или услуг. Список групп услуг и услуг, принадлежащих филиалу, можно свернуть и развернуть с помощью кнопок  и . Настроенное состояние свернутости сохраняется для браузера. По умолчанию строки свернуты.
 - Группа услуг — услуги 1-го уровня вложенности на сервере мониторинга. Группа услуг не отображается в таблице, если не содержит дочерних услуг. Список дочерних услуг можно свернуть и развернуть с помощью кнопок  и .
 - Услуга — услуги 2-го уровня вложенности на сервере мониторинга.

 **Прим.:**

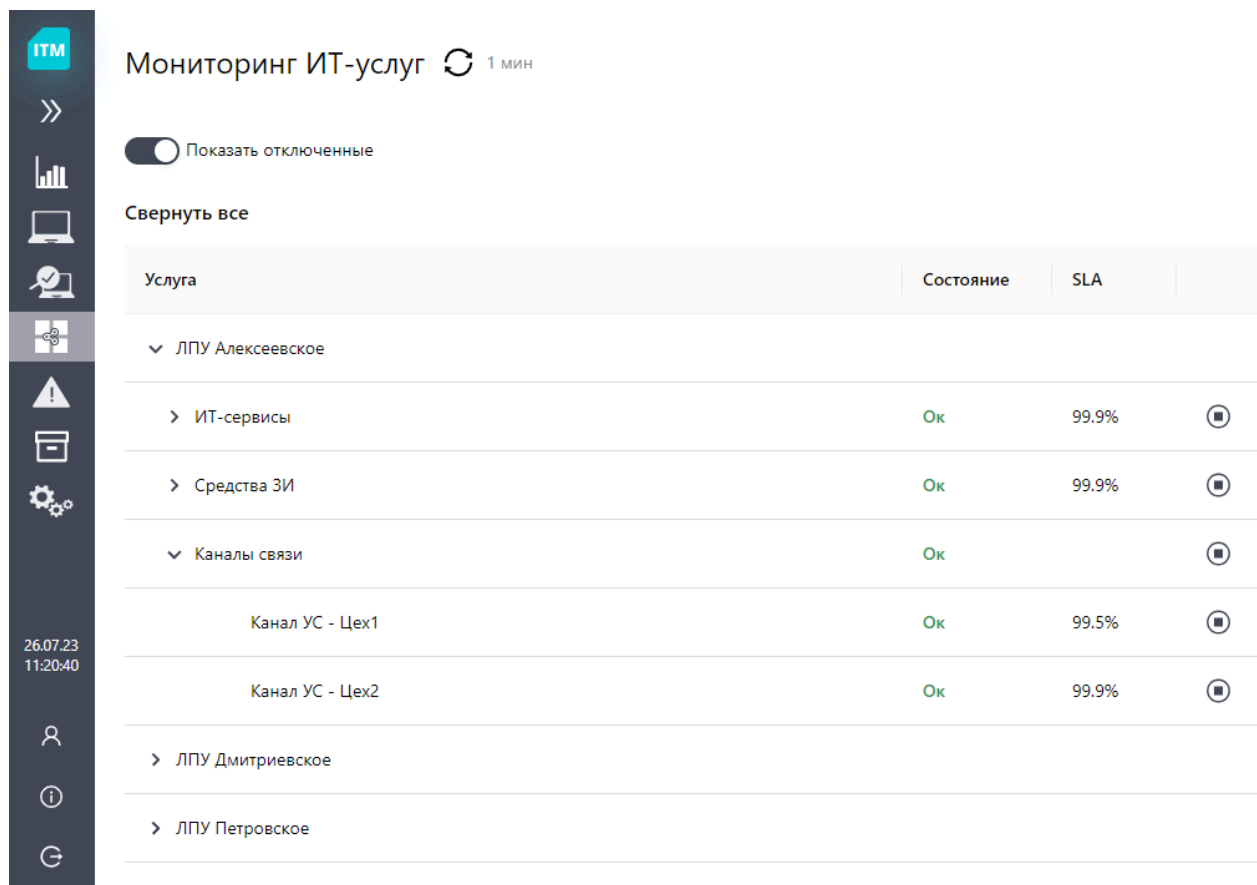
Услуги с вложенностью больше 2-го уровня в списке не отображаются.


- Состояние — статус услуги. Доступны значения «ОК» и «Проблема».
- SLA — установленный уровень качества, который считается приемлемым для данной услуги. Если фактический уровень SLA для услуги ниже этого значения, услуга перейдет в состояние «Проблема».
- Кнопка отключения услуги  — позволяет скрыть или выделить другим цветом услугу:
 - Если переключатель «Показать отключенные» включен, отключенная услуга отображается в списке серым цветом, кнопка меняется на кнопку включения .
 - Если переключатель «Показать отключенные» выключен, отключенная услуга не отображается в списке.

При нажатии на кнопку включения  услуга снова отображается в обычном режиме, состояние и свойства услуги обновляются при ближайшей синхронизации и дальше по графику синхронизатора.

 **Прим.:**






Включение и отключение услуг доступно только пользователям с ролью «Администратор».



Мониторинг ИТ-услуг  1 мин

Показать отключенные

Свернуть все

Услуга	Состояние	SLA	
<ul style="list-style-type: none"> ЛПУ Алексеевское <ul style="list-style-type: none"> ИТ-сервисы Ок 99.9%  Средства ЗИ Ок 99.9%  Каналы связи Ок  <ul style="list-style-type: none"> Канал УС - Цех1 Ок 99.5%  Канал УС - Цех2 Ок 99.9%  ЛПУ Дмитриевское ЛПУ Петровское 			

26.07.23 11:20:40

Рис. 4-35 Страница «ИТ-услуги»



При нажатии на имя услуги открывается карточка с подробной информацией о ней (подробнее см. в разделе 4.5.1 Просмотр информации об ИТ-услуге (47)).

Для просмотра большого списка ИТ-услуг используется вертикальная прокрутка списка справа.

4.5.1. Просмотр информации об ИТ-услуге

Для просмотра подробной информации об ИТ-услуге нажмите на ее имя в списке. В результате откроется карточка услуги, которая содержит следующую информацию:

- Название.
- Группа услуг — услуга 1-го уровня вложенности на сервере мониторинга, для которой выбранная услуга является дочерней. Не отображается, если выбранная услуга сама находится на 1 уровне.
- Филиал — филиал, к которому относится выбранная услуга.

- **Контроль** – переключатель включения и выключения контроля услуги на уровне UDV-ITM-VM. Действие переключателя соответствует работе кнопок  («Включить») и  («Отключить») в списке услуг.
 - Во включенном состоянии услуга работает и отображается как обычно.
 - В выключенном состоянии:
 - услуга отображается в списке, только если включен переключатель «Показать отключенные»;
 - услуга показана в списке серым цветом.
- **Состояние** – статус услуги. Доступны значения «ОК» и «Проблема».
- **Контролируемые параметры** – информация о вложенных услугах и их триггерах в виде таблицы. В таблице отображается следующая информация:
 - Контролируемые параметры – наименование вложенной услуги (обязательно) и наименование триггера (при наличии);
 - Состояние – статус вложенной услуги. Доступны значения «ОК» и «Проблема». Узнать подробнее, как формируется состояние, можно в Руководстве по эксплуатации UDV-ITM-M в разделе .
- **Обновлено** – дата и время последнего успешного сбора данных об услуге с сервера мониторинга.

ИТ-Услуга
✕


Название: Сервис e-mail
Группа услуг: Сервисы
Филиал: Fil 164
Контроль:
Состояние: Ок

Контролируемые параметры	Состояние
Журнал событий - "Eventlog" (Журнал событий) не запущен (тип зап...	Ок
Доступность - Агент недоступен (в течение {\$AGENT.TIMEOUT})	Ок

Обновлено: 20.11.2023 12:26:06

Закреть

Рис. 4-36 Карточка «ИТ-услуга»

Для закрытия карточки ИТ-услуги нажмите на кнопку «Закреть» в нижнем правом углу или на кнопку  в верхнем правом углу.

Про изменение параметров услуги можно узнать в разделе Руководства по эксплуатации UDV-ITM-M .

4.6. Проблемы объектов мониторинга

Раздел *Проблемы* отображает информацию обо всех проблемах объектов мониторинга со всех серверов уровней филиалов UDV-ITM-M и Zabbix и серверов уровня технологических комплексов UDV-ITM-RM. Сервер UDV-ITM-VM получает от серверов мониторинга UDV-ITM-M и Zabbix данные обо всех проблемах ОМ периодически по расписанию.

В этом разделе:

- 4.6.1 Список проблем объектов мониторинга (49)
- 4.6.2 Просмотр карточки проблемы (53)

4.6.1. Список проблем объектов мониторинга

Список проблем выводится при нажатии в боковом меню на раздел *Проблемы*. Для просмотра полного списка проблем используются вертикальная прокрутка списка справа.


Время	Важность	Состояние	Филиал	TK	Объект	Проблема	Длительность	Подтверждено
08.12.2023, 14:51:14	Средняя	⚠	Филиал Петровс...		ИБП APC-14Demo	Тест. Напряжение на входе мень...	24 м 3 с	Нет
08.12.2023, 14:27:20	Средняя	✅	Филиал Петровс...	Цех №2	DATAPKTESTTK22	Средняя нагрузка слишком высок...	13 с	Нет
08.12.2023, 13:53:14	Средняя	⚠	Филиал Петровс...		ИБП APC-14Demo	Тест. Напряжение на входе боль...	1 ч 22 м 3 с	Нет
08.12.2023, 13:45:21	Средняя	⚠	Филиал Петровс...		ИБП Ш123-3 APC --test--	Тест. Напряжение на входе боль...	1 ч 29 м 56 с	Нет
08.12.2023, 13:25:14	Средняя	✅	Филиал Петровс...		ИБП APC-14Demo	Тест. Напряжение на входе боль...	20 м	Нет
08.12.2023, 12:53:21	Средняя	✅	Филиал Петровс...		ИБП Ш123-3 APC --test--	Тест. Напряжение на входе боль...	16 м	Нет
08.12.2023, 11:53:21	Средняя	✅	Филиал Петровс...		ИБП Ш123-3 APC --test--	Тест. Напряжение на входе боль...	30 м	Нет
08.12.2023, 11:45:14	Средняя	✅	Филиал Петровс...		ИБП APC-14Demo	Тест. Напряжение на входе боль...	24 м 1 с	Нет

Рис. 4-37 Список проблем объектов мониторинга

Над списком выводится строка общей информации и фильтры.

Общая информация

Строка общей информации содержит:

- Счетчик проблем. Если никакие фильтры не применены, счетчик показывает общее количество проблем. Если применены какие-либо фильтры, счетчик показывает количество отфильтрованных проблем/общее количество проблем.
- Кнопку обновления страницы  — при нажатии на кнопку происходит обновление информации о проблемах. При обновлении выбранные фильтры не сбрасываются.
- Количество минут, прошедшее с момента последнего обновления информации о проблемах.

Прим.:

этот параметр появляется через 1 минуту после последнего обновления страницы.

Фильтры

На странице есть следующие фильтры:

- «Филиал/ТК» – позволяет отобразить все ОМ выбранных филиалов или ТК.

При нажатии на поле фильтра появляется выпадающий список с имеющимися филиалами и ТК.

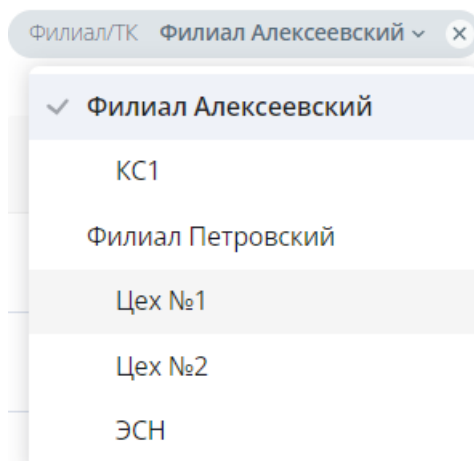


Рис. 4-38 Фильтр «Филиал/ТК»

- «Объект» – позволяет отобразить проблемы определенных объектов мониторинга.

При нажатии на поле фильтра появляется выпадающий список с доступными ОМ.

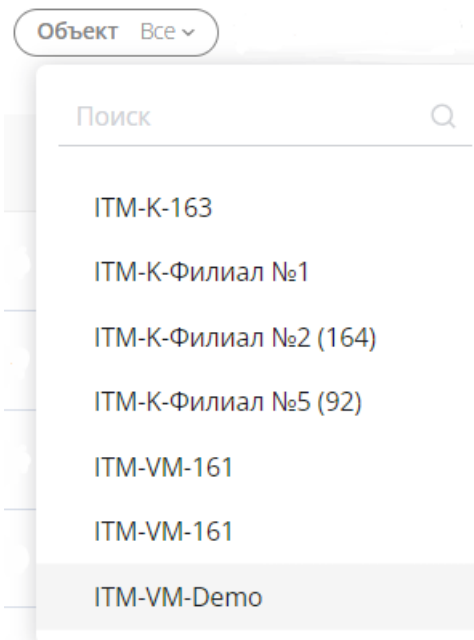


Рис. 4-39 Фильтр «Объект»

По умолчанию в этом списке отображаются все ОМ. Если проблемы уже отфильтрованы по филиалу, то в списке будут отображаться только ОМ выбранных филиалов и подключенных к ним ТК.

Над списком находится строка поиска. Для поиска конкретного объекта начните вводить его название в строку поиска и нажмите на нужный вариант из найденных соответствий. Поиск объектов в списке имеет следующие особенности:

- не зависит от регистра;

- осуществляется по любой части слова;
 - результат обновляется после каждого ввода символа.
- «Важность» — позволяет отобразить проблемы с определенным уровнем важности. При нажатии на поле фильтра появляется выпадающий список с уровнями важности.

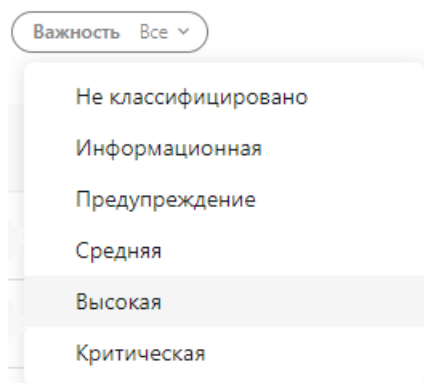


Рис. 4-40 Фильтр «Важность»

- «Состояние» — позволяет отобразить проблемы в определенном состоянии. При нажатии на поле фильтра появляется выпадающий список с состояниями проблемы.

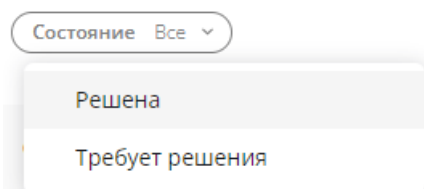





Рис. 4-41 Фильтр «Состояние»

В списках фильтров можно выбрать одно или несколько значений. Чтобы закрыть список и применить фильтр, после выбора всех нужных значений кликните вне области фильтра. Чтобы отменить выбор конкретного значения, еще раз кликните по этому значению в выпадающем списке. Чтобы сбросить примененный фильтр целиком, нажмите на кнопку  в области фильтра. Чтобы сбросить сразу все

выбранные фильтры, нажмите на кнопку  справа от фильтров.

Внимание:

При обновлении страницы в браузере или переходе на другую страницу выбранные фильтры будут сброшены. При обновлении страницы с помощью кнопки  («Обновить данные») фильтры не сбрасываются.


Сортировка

Проблемы в списке можно отсортировать по времени, важности и длительности. По умолчанию проблемы отсортированы по времени (сверху самые новые). Одновременно можно отсортировать проблемы только по одному столбцу.

Сортировка проблем с одинаковой важностью или длительностью работает следующим образом:

- Если выполнена сортировка по важности/длительности по убыванию, то проблемы с одинаковой важностью/длительностью будут дополнительно отсортированы по времени по убыванию.
- Если выполнена сортировка по важности/длительности по возрастанию, то проблемы с одинаковой важностью/длительностью будут дополнительно отсортированы по времени по возрастанию.

⚠ Внимание:

При обновлении страницы в браузере или переходе на другую страницу выбранная сортировка будет сброшена. При обновлении страницы с помощью кнопки  («Обновить данные») сортировка не сбрасывается.

Свойства проблем ОМ

В списке отображаются следующие свойства проблем ОМ:

- Время — дата и время фиксации проблемы сервером мониторинга.
- Важность — уровень критичности проблемы:

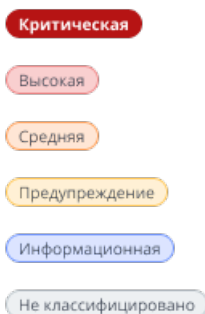




Рис. 4-42 Уровни важности проблем

- Состояние:

	Требуется решения
	Проблема решена

- Филиал — наименование филиала. При нажатии на значение этого столбца появится окно свойств сервера мониторинга. Подробнее см. в разделе 4.3.3 Просмотр информации о подключенном сервере мониторинга (32).
- ТК — наименование ТК. При нажатии на значение этого столбца появится окно свойств сервера удаленного мониторинга. Подробнее см. в разделе 4.3.8 Просмотр свойств сервера удаленного мониторинга (38).
- Объект — имя узла сети. При нажатии на значение этого столбца появится окно с информацией об объекте мониторинга. Подробнее см. в разделе 4.4.2 Просмотр информации об объекте мониторинга (43).
- Проблема — наименование проблемы.

- Длительность – время с момента обнаружения проблемы.
- Подтверждено – признак подтверждения проблемы пользователем сервера мониторинга.

4.6.2. Просмотр карточки проблемы

Карточка проблемы появляется при нажатии в любом месте строки конкретной проблемы, кроме значений в столбцах «Филиал», «ТК» и «Объект». Карточка содержит список событий проблемы.

Все поля окна выводятся в режиме просмотра без возможности изменения.

Карточка проблемы
✕

Высокая загрузка памяти (>90% за 5 мин)

Время	Время восстановления	Состояние	Длительность	Подтверждено
15.11.2023 23:11	16.11.2023 00:22	Решено	1 ч 11 м	Нет
14.11.2023 14:41	14.11.2023 15:19	Решено	38 м	Нет
14.11.2023 02:55	14.11.2023 05:30	Решено	2 ч 35 м	Нет
14.11.2023 02:35	14.11.2023 02:48	Решено	13 м	Нет
13.11.2023 08:58	13.11.2023 09:34	Решено	36 м	Нет
12.11.2023 22:36	13.11.2023 01:40	Решено	3 ч 4 м	Нет
12.11.2023 19:33	12.11.2023 20:08	Решено	35 м	Нет
12.11.2023 11:20	12.11.2023 16:12	Решено	4 ч 52 м	Нет
12.11.2023 11:13	12.11.2023 11:14	Решено	1 м	Нет
12.11.2023 07:13	12.11.2023 09:30	Решено	2 ч 17 м	Нет

Показаны 10 событий. Полный список событий доступен для детального просмотра на сервере мониторинга

[🔗 Подробнее о проблеме](#)
Заккрыть

Рис. 4-43 Карточка проблемы

В окне выводится следующая информация:

- Текстовое описание проблемы.
- Таблица со списком событий по данной проблеме. Таблица содержит колонки:
 - Время – время возникновения проблемы в формате ДД.ММ.ГГГГ ЧЧ:ММ;
 - Время восстановления – время, когда проблема была решена, в формате ДД.ММ.ГГГГ ЧЧ:ММ;
 - Состояние – состояние проблемы. Доступные значения:
 - Проблема;
 - Решено.
 - Длительность – длительность проблемы в формате ХХ д ХХ ч ХХ м;
 - Подтверждено – была ли проблема подтверждена. Доступные значения:
 - Да;
 - Нет.

Для подтверждения проблемы необходимо перейти на сервер мониторинга UDV-ITM-M на страницу «Проблемы». Рекомендуется отмечать как подтвержденные те проблемы, которые уже просмотрены и проанализированы. Также пользователь может оставить комментарий к подтвержденной проблеме. Например, написать о том, что работает над проблемой или предложить варианты решения.

Прим.:

В таблице отображается не более 10 событий. Если событий более 10, внизу окна выводится надпись «Показаны 10 событий. Полный список доступен на сервере мониторинга». На сервер мониторинга можно перейти по ссылке «Подробнее о проблеме».

- Ссылка на страницу с деталями события проблемы на сервере мониторинга.

4.7. Администрирование


Раздел доступен только пользователям с ролью «Администратор».

В этом разделе:

- 4.7.1 Журнал событий (54)

4.7.1. Журнал событий

Страница *Администрирование* → *Журнал событий* содержит список событий и информацию о них.

Над списком событий выводится название «Журнал событий» и кнопка обновления данных на странице . Через 1 минуту рядом с кнопкой появляется счетчик времени с момента обновления страницы. Время отображается только в минутах.

В списке отображаются следующие типы событий:

- События, связанные с серверами мониторинга.
- События о проблемах с подключенных серверов мониторинга. Этот тип включает в себя события о создании, изменении критичности или закрытии проблемы.
- События, связанные с сервером UDV-ITM-VM. Этот тип включает в себя события об изменении общих сведений о UDV-ITM-VM и события об изменении периода сбора данных.
- События об учетных записях сервера UDV-ITM-VM. Этот тип включает в себя события о создании, изменении, удалении, блокировке и разблокировке пользователя.

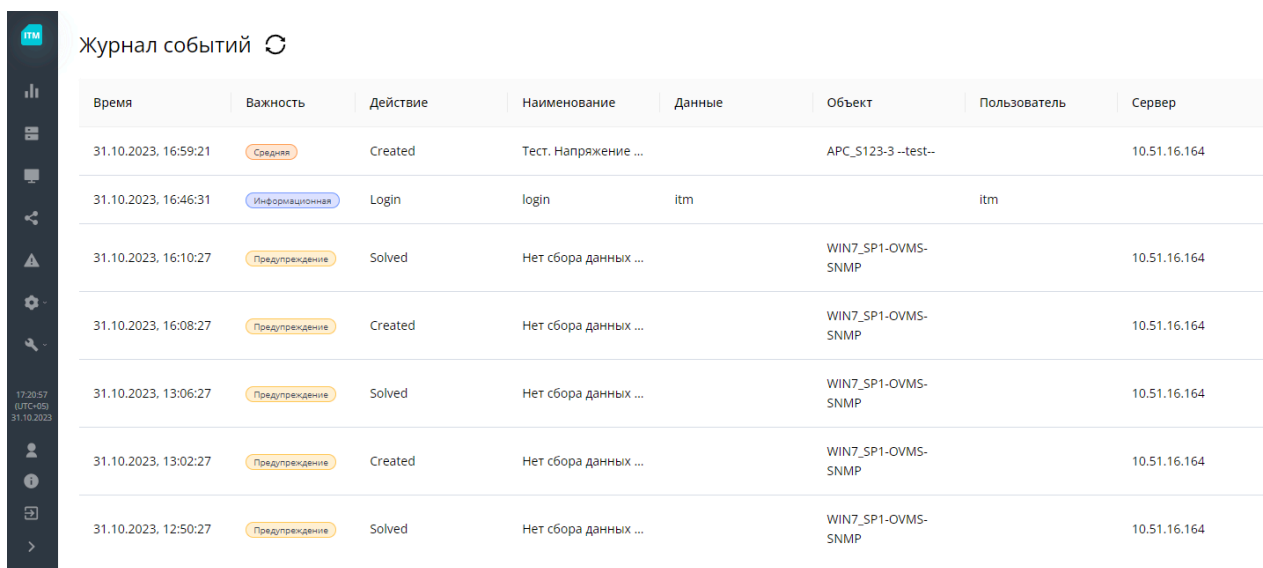
В списке отображаются следующие свойства событий:

- Время — дата и время создания события (используется часовой пояс сервера источника события).
- Важность — уровень критичности события:

-  Критическая ;

- Высокая ;
- Средняя ;
- Предупреждение ;
- Информационная ;
- Не классифицировано ;

- Действие — действие пользователя или событие проблемы.
- Наименование — наименование события, объекта доступа или триггера.
- Данные — дополнительное описание.
- Объект — имя объекта мониторинга, с которым связана проблема. Это поле заполняется только для событий о проблемах.
- Пользователь — пользователь, совершивший действие. Это поле заполняется только для действий пользователя.
- Сервер — IP-адрес сервера источника события.



Время	Важность	Действие	Наименование	Данные	Объект	Пользователь	Сервер
31.10.2023, 16:59:21	Средняя	Created	Тест. Напряжение ...		APC_S123-3 --test--		10.51.16.164
31.10.2023, 16:46:31	Информационная	Login	login	itm		itm	
31.10.2023, 16:10:27	Предупреждение	Solved	Нет сбора данных ...		WIN7_SP1-OVMS-SNMP		10.51.16.164
31.10.2023, 16:08:27	Предупреждение	Created	Нет сбора данных ...		WIN7_SP1-OVMS-SNMP		10.51.16.164
31.10.2023, 13:06:27	Предупреждение	Solved	Нет сбора данных ...		WIN7_SP1-OVMS-SNMP		10.51.16.164
31.10.2023, 13:02:27	Предупреждение	Created	Нет сбора данных ...		WIN7_SP1-OVMS-SNMP		10.51.16.164
31.10.2023, 12:50:27	Предупреждение	Solved	Нет сбора данных ...		WIN7_SP1-OVMS-SNMP		10.51.16.164

Рис. 4-44 Список событий

Для просмотра полного списка событий используются вертикальная прокрутка списка справа.

По умолчанию события отсортированы по времени: самые новые события отображаются в верху списка.

4.8. Настройки

В этом разделе:

- 4.8.1 Основные настройки (56)
 - 4.8.1.1 Изменение основных свойств сервера (60)
 - 4.8.1.2 Настройка Email-оповещений (62)
 - 4.8.1.3 Очистка настроек Email-оповещений (63)

- 4.8.2 Пользователи (65)
 - 4.8.2.5 Изменение пароля пользователя (76)
 - 4.8.2.2 Создание учетной записи локального пользователя (68)
 - 4.8.2.3 Создание учетной записи пользователя LDAP (69)
 - 4.8.2.1 Просмотр свойств учетной записи пользователя (67)
 - 4.8.2.4 Управление учетной записью пользователя (73)
- 4.8.3 LDAP (78)
 - 4.8.3.1 Подключение к LDAP или LDAPS (79)
 - 4.8.3.2 Настройка атрибутов пользователей LDAP или LDAPS (82)
 - 4.8.3.3 Очистка настроек LDAP (86)
- 4.8.4 Правила оповещений (87)
 - 4.8.4.1 Создание правила оповещений (89)
 - 4.8.4.2 Управление правилами оповещений (92)

4.8.1. Основные настройки

При переходе в раздел основного меню *Настройки* → *Основные* открывается страница, которая содержит сведения о сервере, параметры пользовательской сессии, настройки e-mail оповещений, параметры хранения журнала событий и параметры интеграции с SIEM.

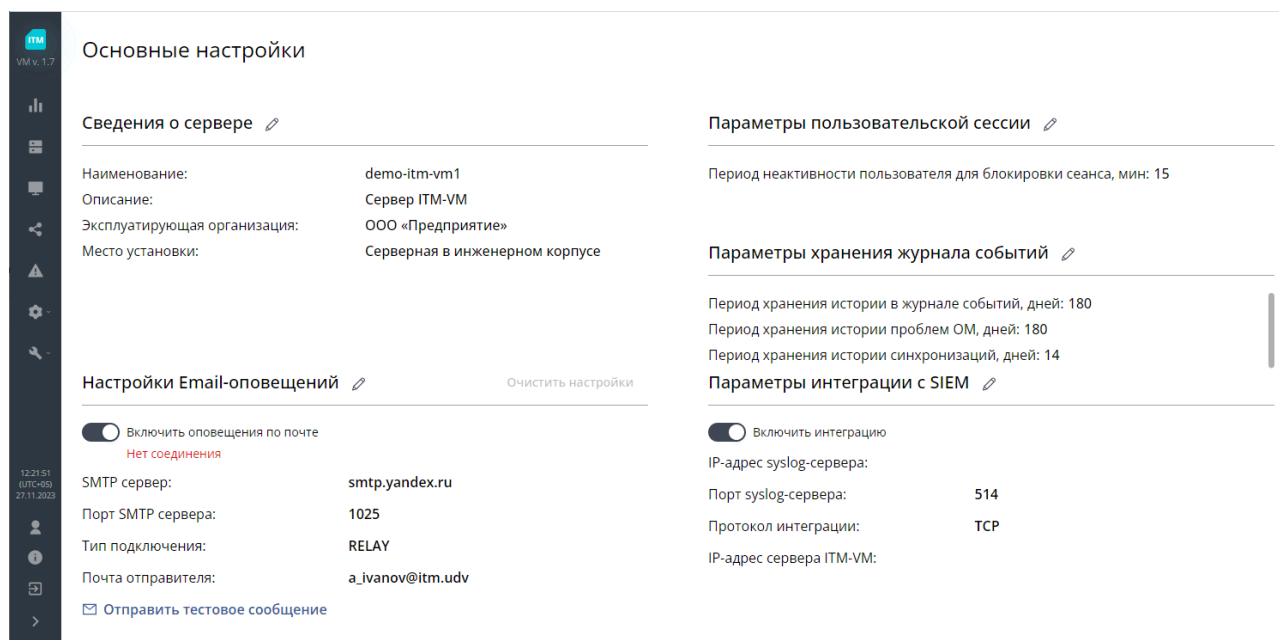


Рис. 4-45 Основные настройки

Сведения о сервере

В разделе «Сведения о сервере» выводятся следующие свойства:

- Наименование — наименование сервера, не редактируемое поле;
- Описание — описание сервера, не обязательное поле;
- Эксплуатирующая организация — наименование эксплуатирующей организации, редактируемое поле, не обязательное;

- Место установки – адрес или описание места установки сервера, редактируемое поле, не обязательное.

Параметры пользовательской сессии

В разделе «Параметры пользовательской сессии» в поле «Период неактивности пользователя для блокировки сеанса, мин» указан период неактивности пользователя, после окончания которого сеанс будет заблокирован. Значение параметра по умолчанию – 15 минут.

За X секунд до истечения времени сессии появляется оповещение о скором завершении сеанса. $X=10\%$ от значения параметра в поле «Период неактивности пользователя для блокировки сеанса, мин».

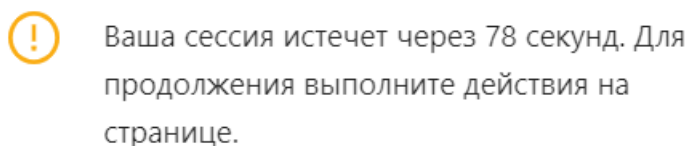


Рис. 4-46 Оповещение о скором завершении сеанса

Например, если в поле «Период неактивности пользователя для блокировки сеанса, мин» указан период 10 минут, то оповещение появится за 1 минуту до истечения времени сессии.

Для продолжения сессии необходимо в любой момент до истечения времени сессии выполнить на странице одно из действий:

- скроллинг колесом;
- нажатие на кнопки навигации клавиатуры;
- клики или движения мыши;
- смена активности вкладки;
- выполнение пользователем запроса на странице.



После выполнения действия отсчет времени до блокировки сеанса начнется заново.

Если пользователь останется неактивным, то текущий сеанс завершится и откроется страница авторизации.

Настройки Email-оповещений

В разделе «Настройки Email-оповещений» выводятся следующие элементы:

- Кнопка «Очистить настройки».
- Переключатель «Включить оповещения по почте». По умолчанию находится в положении «Выключено». Событие о включении или выключении переключателя отправляется в SIEM.
 - В положении «Выключено»:
 - Оповещения не работают.
 - Если настройка ни разу не выполнялась, все поля настроек пустые.
 - Если настройка выполнялась хотя бы один раз, поля настроек содержат последние сохраненные значения.

- Редактирование параметров невозможно, кнопка  неактивна.
- Кнопка «Отправить тестовое сообщение» неактивна.
- Кнопка «Очистить настройки» активна.
- Заголовки и значения полей серого цвета.
- В положение «Включено»:
 - Оповещения работают.
 - Кнопка  активна, при нажатии доступно редактирование полей настроек.
 - Кнопка «Отправить тестовое сообщение» активна, при нажатии отправляется тестовое письмо.
 - Кнопка «Очистить настройки» неактивна.
 - Заголовки и значения полей черного цвета.
- Индикатор состояния подключения к SMTP-серверу. Доступные значения:
 - Подключение активно;
 - Нет соединения.

Если режим оповещений по почте включен, то текущее состояние подключения к SMTP-серверу проверяется и отображается при каждом открытии страницы.

При отключении режима оповещений по почте и при переходе в режим редактирования настроек Email-оповещений индикатор состояния подключения не отображается.
- SMTP сервер – DNS-адрес SMTP-сервера.
- Порт SMTP сервера – номер порта SMTP-сервера.
- Тип подключения – протокол передачи данных. Доступные значения:
 - RELAY;
 - SMTPS;
 - STARTTLS.
- Почта отправителя – Email отправителя. Поле отображается при выборе типа подключения RELAY.
- Логин – логин пользователя для подключения к SMTP-серверу. Поле отображается при выборе типов подключения SMTPS и STARTTLS.
- Пароль – пароль пользователя. Поле отображается при выборе типов подключения SMTPS и STARTTLS.
- Кнопка «Отправить тестовое сообщение». При нажатии на кнопку появляется всплывающее окно для отправки тестового письма.

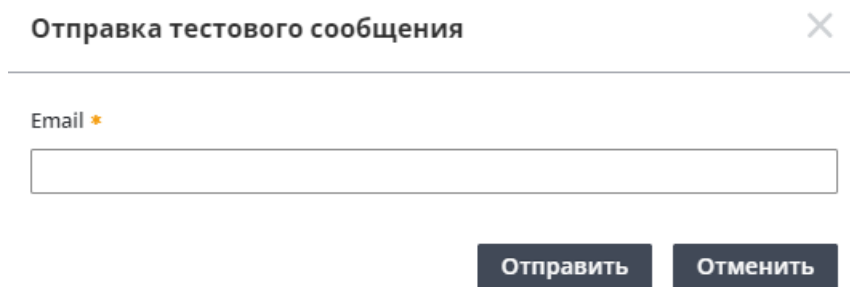


Рис. 4-47 Отправка тестового сообщения

Для отправки сообщения введите адрес электронной почты получателя в поле «Email» и нажмите на кнопку «Отправить». В результате на указанный адрес придет письмо в формате:

Тема письма: Тестовое сообщение с сервера [Наименование сервера ITM-VM]
 Содержание письма: Тестовое письмо системы оповещений сервера [Наименование сервера ITM-VM] отправлено в [Время отправки письма в формате ЧЧ:ММ ДД.ММ.ГГГГ]

Параметры хранения журнала событий

В разделе «Параметры хранения журнала событий» доступна настройка следующих параметров:

- Период хранения истории в журнале событий, дней — количество дней, в течение которого записи о событиях аудита хранятся в журнале. Значение параметра по умолчанию — 180 дней.
- Период хранения истории проблем ОМ, дней — количество дней, в течение которого хранится история возникновения проблем ОМ, полученных из серверов мониторинга. Значение параметра по умолчанию — 180 дней.
- Период хранения истории синхронизаций, дней — количество дней, в течение которого хранится история синхронизации данных с серверами мониторинга. Значение параметра по умолчанию — 14 дней.

Все поля раздела являются обязательными. Диапазон допустимых значений для каждого из полей — от 1 до 1095.

Параметры интеграции с SIEM

В разделе «Параметры интеграции с SIEM» доступна настройка следующих параметров:

- IP-адрес syslog-сервера.
- Порт syslog-сервера. Диапазон допустимых значений — 1-65535. Значение параметра по умолчанию — 514.
- Протокол интеграции. Доступные значения — TCP или UDP. Значение параметра по умолчанию — TCP.
- IP-адрес сервера ITM-VM — IP-адрес сервера ITM-VM, от имени которого отправляются данные на syslog-сервер.


В этом разделе:

- 4.8.1.1 Изменение основных свойств сервера (60)
- 4.8.1.2 Настройка Email-оповещений (62)
- 4.8.1.3 Очистка настроек Email-оповещений (63)
- 4.8.1.4 Настройка интеграции с SIEM (64)

4.8.1.1. Изменение основных свойств сервера

Для изменения основных настроек сервера:

1. Перейдите на страницу *Настройки* → *Основные*.
2. Для изменения сведений о сервере:

- a. Нажмите на кнопку  рядом с заголовком «Сведения о сервере».

Результат шага: поля станут доступны для редактирования.

- b. Измените сведения о сервере.

Сведения о сервере

Наименование: itm-vm-test


Описание

Эксплуатирующая организация

Место установки

Рис. 4-48 Редактирование сведений о сервере

- c. Нажмите на кнопку «Сохранить».

3.  **Внимание:**


Изменение периода неактивности пользователя для блокировки сеанса приведет к закрытию сессий всех пользователей, авторизованных в системе.

Для изменения периода неактивности пользователя, после окончания которого сеанс будет заблокирован:

- a. Нажмите на кнопку  рядом с заголовком «Параметры пользовательской сессии».

Результат шага: поле «Период неактивности пользователя для блокировки сеанса, мин» станет доступно для редактирования.

- b. Измените период неактивности пользователя.

 **Прим.:**

Доступен ввод значений от 2 до 60 минут.

Параметры пользовательской сессии

Период неактивности пользователя для блокировки сеанса, мин: * ?

Сохранить

Отменить

Рис. 4-49 Редактирование периода неактивности пользователя для блокировки сеанса

- c. Нажмите на кнопку «Сохранить».

Результат шага: откроется окно подтверждения результата.

- d. В открывшемся окне нажмите на кнопку «Изменить».

Изменить период?



Изменение периода неактивности пользователя для блокировки сеанса приведет к закрытию сессий всех пользователей, авторизованных в системе.

Изменить

Отменить


Рис. 4-50 Окно подтверждения

4. Для изменения параметров хранения журнала событий:

- a. Нажмите на кнопку  рядом с заголовком «Параметры хранения журнала событий».

Результат шага: поля раздела станут доступны для редактирования.

в. Измените нужный период.

 **Прим.:**
Доступен ввод значений от 1 до 1095 дней.

Параметры хранения журнала событий

Период хранения истории в журнале событий, дней: * ?

Период хранения истории проблем ОМ, дней: * ?

Период хранения истории синхронизаций, дней: * ?

Сохранить

Отменить

Рис. 4-51 Редактирование параметров хранения журнала событий


с. Нажмите на кнопку «Сохранить».

4.8.1.2. Настройка Email-оповещений

Для настройки Email-оповещений:

1. Перейдите на страницу *Настройки* → *Основные*.
2. Установите переключатель «Включить оповещения по почте» в положение «Включено».

Результат шага: кнопка  станет активна.

3. Нажмите на кнопку  рядом с заголовком «Настройки Email-оповещений».

Результат шага: поля станут доступны для редактирования.

4. Измените параметры оповещений.

Настройки Email-оповещений

[Очистить настройки](#)

SMTP сервер *

Порт SMTP сервера *

Тип подключения *

- RELAY
- SMTPS
- STARTTLS

Почта отправителя *

Рис. 4-52 Редактирование настроек оповещений

Прим.:

Описания всех параметров см. в разделе «Настройки Email-оповещений» на странице [4.8.1 Основные настройки \(56\)](#).

5. Нажмите на кнопку «Сохранить».

4.8.1.3. Очистка настроек Email-оповещений

В UDV-ITM-VM можно очистить параметры подключения к SMTP-серверу. Это может понадобиться для очистки параметров тестового контура, перемещения сервера в другой сегмент и т.п. Для очистки настроек:

1. Перейдите на страницу *Настройки* → *Основные*.
2. Установите переключатель «Включить оповещения по почте» в разделе «Настройки Email-оповещений» в положение «Выключено».

Результат шага: кнопка «Очистить настройки» станет активна.

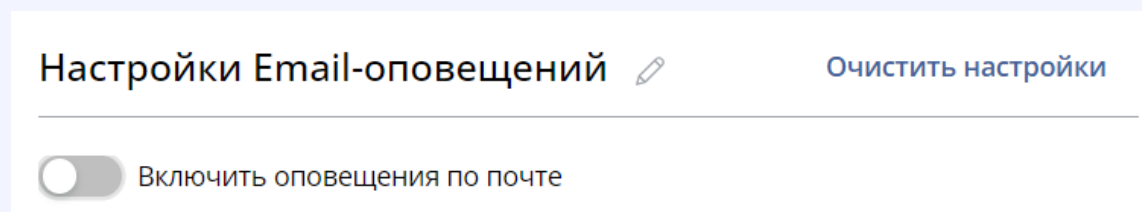


Рис. 4-53 Кнопка «Очистить настройки» при выключенном переключателе оповещений

3. Нажмите на кнопку «Очистить настройки».

Результат шага: появится окно подтверждения.

4. В открывшемся окне нажмите на кнопку «Подтвердить».

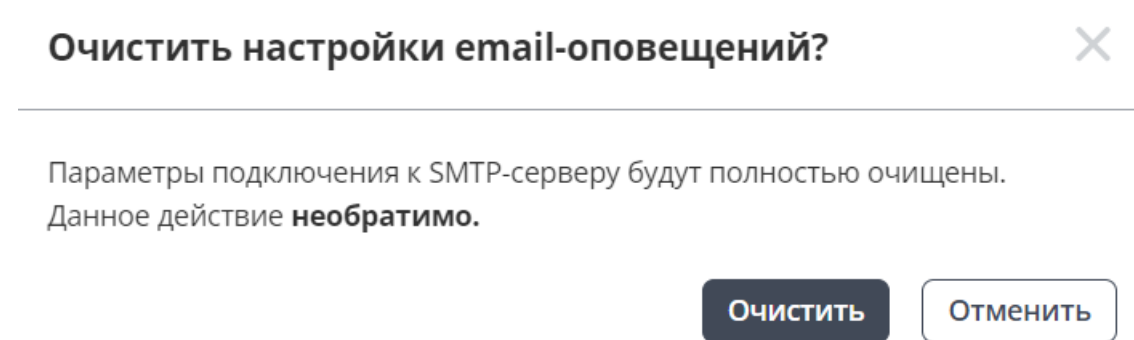


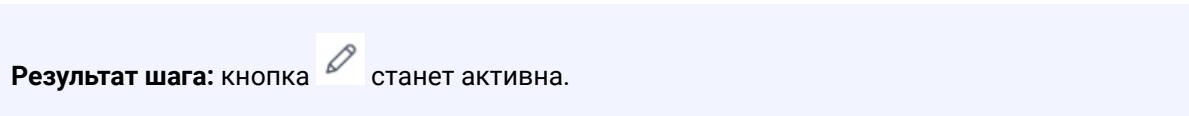
Рис. 4-54 Окно подтверждения очистки настроек

Результат шага: после подтверждения параметры подключения к SMTP-серверу очистятся.


4.8.1.4. Настройка интеграции с SIEM

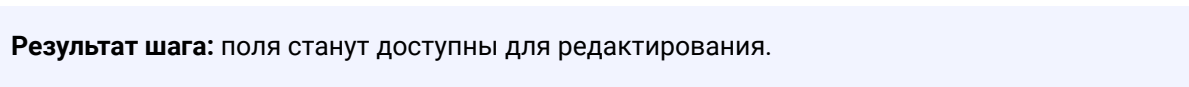
Для настройки интеграции сервера UDV-ITM-VM с SIEM:

1. Перейдите на страницу *Настройки* → *Основные*.
2. Установите переключатель «Включить интеграцию» в положение «Включено».



Результат шага: кнопка  станет активна.

3. Нажмите на кнопку  рядом с заголовком «Параметры интеграции с SIEM».



Результат шага: поля станут доступны для редактирования.

4. Измените параметры интеграции с SIEM.

Параметры интеграции с SIEM

IP-адрес syslog-сервера *

Порт syslog-сервера *

Протокол интеграции

IP-адрес сервера ITM-VM *

Сохранить **Отменить**

Рис. 4-55 Редактирование параметров интеграции с SIEM

Прим.:

Описание всех параметров см. в разделе «Параметры интеграции с SIEM» на странице 4.8.1 Основные настройки (56).

5. Нажмите на кнопку «Сохранить».

4.8.2. Пользователи

При нажатии на пункт *Настройки* → *Пользователи* в основном меню выводится список пользователей сервера UDV-ITM-VM.

Пользователи

[Добавить пользователя](#)

ID	Пользователь	Тип УЗ	Подразделение	Логин	Роль	Email	Статус
1	Иванов Петр Петрович	Локальная	Отдел ИБ	itm	Администратор	ivanov@example.ru	Активен
2	Истомина Ирина Андреевна	Локальная		info	Оператор мониторинга		Активен
3	Петров Петр Петрович	Локальная	Отдел ИТ	petrov	Пользователь	petrov@company.ru	Активен
4	Терентьев Максим Семенович	LDAP		terentiev.m	Пользователь	terentiev.maksim@company.ru	Активен
5	Устинова Лариса Владимировна	Локальная		ustinova	Техническая		Активен

Рис. 4-56 Список пользователей

В случае большого списка появляется вертикальная прокрутка справа.


Строка поиска предназначена для осуществления поиска по всем полям всех пользователей.

В таблице пользователей выводятся следующие поля:

- ID – уникальный идентификатор пользователя в базе данных сервера UDV-ITM-VM;
- Пользователь – ФИО пользователя;
- Тип УЗ – тип учетной записи пользователя. Возможные значения:
 - Локальная – создание локальной учетной записи пользователя UDV-ITM-VM;
 - LDAP – подключение учетной записи из каталога LDAP.
- Подразделение;
- Логин;
- Роль:
 - Пользователь – пользователь системы, которому доступны основные функции:
 - работа с графиками;
 - просмотр списков и карточек объектов мониторинга, серверов мониторинга, ИТ-услуг, событий, пользователей;
 - создание, изменение, включение, выключение и удаление собственных правил оповещений;
 - просмотр параметров своей учетной записи, изменение своего пароля.
 - Администратор – пользователь системы, которому доступны те же основные функции, что и пользователю, а также функции управления и администрирования:
 - добавление серверов мониторинга;
 - настройка сбора данных;
 - просмотр журнала событий;
 - настройки сервера, параметров пользовательской сессии, email-оповещений, хранения журнала событий, интеграции с SIEM;
 - добавление, изменение и удаление пользователей системы;
 - настройки подключения LDAP;
 - изменение и удаление правил оповещений, созданных другими пользователями.
 - Техническая – учетная запись для предоставления доступа к данным для смежных систем;
 - Оператор мониторинга – пользователь системы, обладающий правами только на просмотр и работу с графиками на странице *Панель информации*.

 **Прим.:**

Подробнее см. в разделе 5.1 Роли пользователей и доступные им интерфейсы (96).

- Email – электронный адрес пользователя;
- Статус – статус учетной записи пользователя:
 1. Активен – учетная запись пользователя активна, пользователь может пользоваться функциями сервера UDV-ITM-VM;
 2. Заблокирован – учетная запись пользователя заблокирована администратором.
- Кнопка «Изменить»  – при нажатии открывается окно изменения свойств учетной записи пользователя.

Изменение свойств пользователя ✕

Логин
ivanov_p

ФИО
Иванов Петр Александрович

Роль пользователя *
Пользователь ▾

Email
ivanov_p@example.ru

Подразделение
Отдел ИБ

ID
4


Статус
Активен  Заблокировать пользователя

Рис. 4-57 Изменение свойств учетной записи пользователя

По умолчанию записи в таблице пользователей отсортированы вначале по статусу (первыми указаны активные пользователи, далее заблокированные), потом по ФИО пользователя.

Записи в таблице пользователей можно отсортировать по столбцам «ID», «Пользователь», «Тип УЗ», «Подразделение», «Логин», «Роль» и «Статус».

4.8.2.1. Просмотр свойств учетной записи пользователя

При клике на учетную запись в списке пользователей появляется окно просмотра свойств учетной записи пользователя. В окне выводятся все свойства учетной записи пользователя в режиме «на чтение».

Свойства пользователя		✕
Тип учетной записи:	Локальная	
Логин:	itm	
Фамилия Имя Отчество:	Иванов Петр Петрович	
Роль:	Администратор	
Email:	ivanov@example.ru	
Подразделение:	Отдел ИБ	
ID:	1	
Статус:	Активен	

Рис. 4-58 Свойства учетной записи

4.8.2.2. Создание учетной записи локального пользователя

Для создания учетной записи пользователя:


1. Перейдите на страницу *Настройки* → *Пользователи*.
2. Нажмите на кнопку «Добавить пользователя» над списком пользователей.
3. В открывшемся окне выберите вариант «Создать локального пользователя».
4. Заполните следующие поля:
 - «Логин»;
 - «Пароль»;

Подсказка:

При создании пароля к учетной записи необходимо следовать требованиям парольной политики:

- длина — не менее 12 символов;
- символы — буквы в нижнем и верхнем регистрах, цифры и специальные символы;
- минимальное количество цифр — 2.

Прим.:

Введенные символы маскируются. Чтобы просмотреть пароль, нажмите на кнопку  в поле с паролем;

- «Подтверждение пароля»;
- «Роль пользователя».

Прим.:

Подробнее см. в разделе 5.1 Роли пользователей и доступные им интерфейсы (96).


5. При необходимости заполните поля:

- «ФИО»;
- «Email»;
- «Подразделение».

Добавление пользователя ✕

Создать локального пользователя
 Создать пользователя из LDAP


Логин *

Пароль * 

Подтверждение пароля *

ФИО

Роль пользователя *

Пользователь 

Email


Подразделение

Рис. 4-59 Добавление локального пользователя

6. Нажмите на кнопку «Сохранить».

При вводе данных и нажатии на кнопку «Сохранить» выполняется проверка корректности значений в полях формы и, в случае ошибок, выводятся ошибки рядом с каждым полем.

4.8.2.3. Создание учетной записи пользователя LDAP

 **Прим.:**

Пользователь сможет входить в веб-интерфейс UDV-ITM-VM с учетной записью LDAP только после выполнения настроек, описанных в разделах 4.8.3.1 Подключение к LDAP или LDAPS (79) и 4.8.3.2 Настройка атрибутов пользователей LDAP или LDAPS (82).

Для создания учетной записи пользователя LDAP:

1. Перейдите на страницу *Настройки* → *Пользователи*.
2. Нажмите на кнопку «Добавить пользователя» над списком пользователей.
3. В открывшемся окне выберите вариант «Создать пользователя из LDAP».

 **Прим.:**

Этот вариант активен, только если включен режим интеграции с LDAP.

Результат шага: В окне «Добавление пользователя» отобразятся поля формы создания пользователя из LDAP.

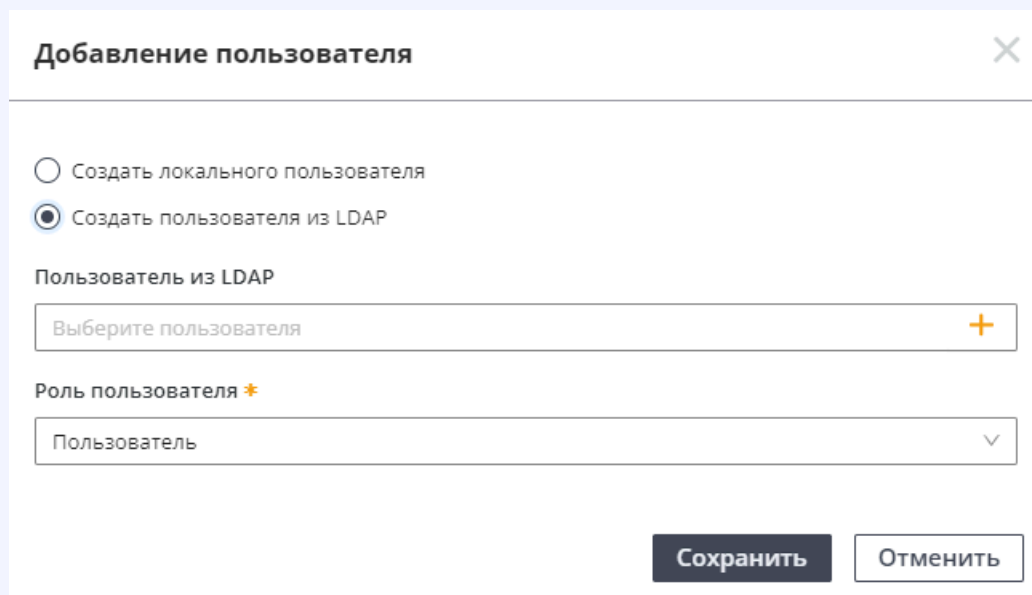



Рис. 4-60 Добавление пользователя из LDAP

4. Выберите пользователя из LDAP. Для этого:

- а. Нажмите на кнопку  в поле «Пользователь из LDAP».

Результат шага: Откроется окно «Выбор пользователя LDAP».

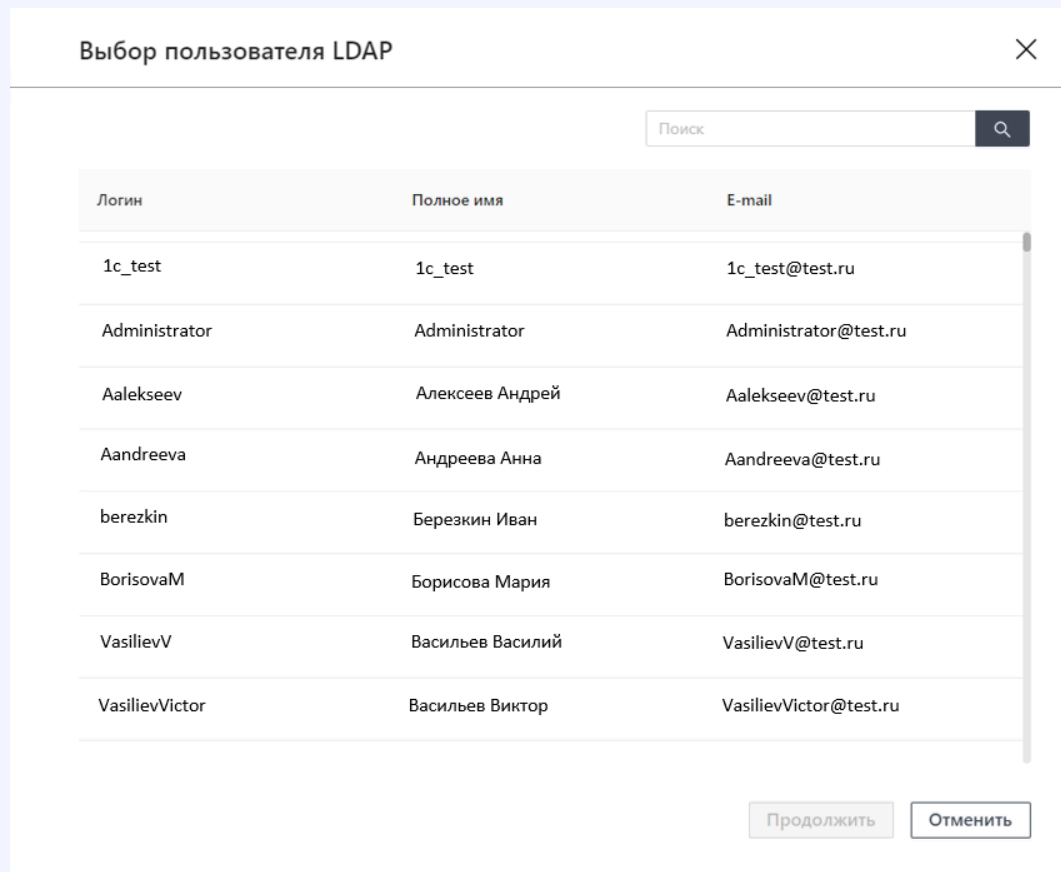


Рис. 4-61 Окно «Выбор пользователя LDAP»

- b. Выберите пользователя LDAP из списка. Для этого кликните в любой части выбранной строки.

 Подсказка:

Вы можете воспользоваться поиском по первым символам логина, полного имени или e-mail или прокруткой списка. Записи в списке отсортированы по столбцу «Полное имя» по алфавиту.

Результат шага: Выбранная запись будет выделена цветом.

- c. Нажмите на кнопку «Продолжить».

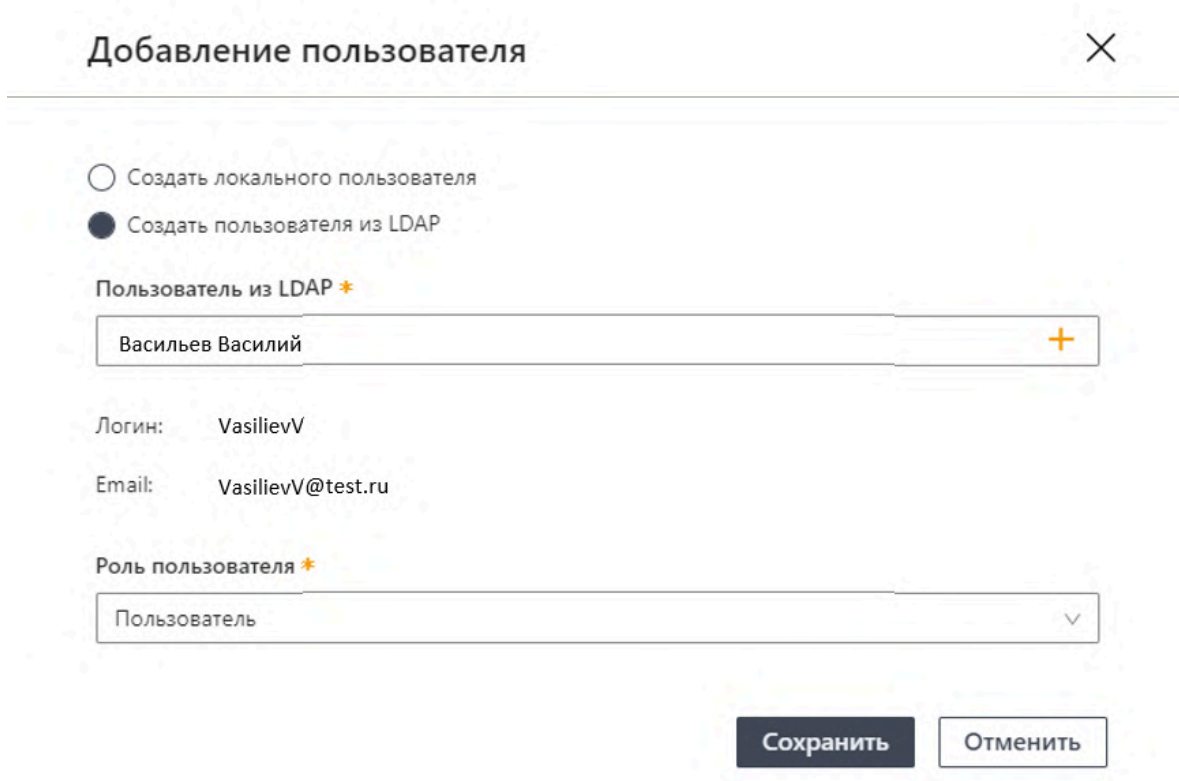
Результат шага: Окно «Выбор пользователя LDAP» закрывается, информация в окне «Добавление пользователя» обновится:

- поле «Пользователь из LDAP» будет заполнено значением ФИО выбранного пользователя;
- появятся поля:
 - «Логин» – не редактируемое поле, содержит значение логина выбранного пользователя из каталога LDAP;
 - «Email» – не редактируемое поле, содержит значение email выбранного пользователя из каталога LDAP.

5. Выберите роль пользователя. По умолчанию установлена роль «Пользователь».

 **Прим.:**

Подробнее см. в разделе 5.1 Роли пользователей и доступные им интерфейсы (96).



Добавление пользователя X

Создать локального пользователя

Создать пользователя из LDAP

Пользователь из LDAP *

Васильев Василий +

Логин: VasilievV

Email: VasilievV@test.ru

Роль пользователя *

Пользователь v

Сохранить Отменить

Рис. 4-62 Добавление пользователя из LDAP

6. Нажмите на кнопку «Сохранить».



При вводе данных и нажатии на кнопку «Сохранить» выполняется проверка корректности значений в полях формы и, в случае ошибок, выводятся ошибки рядом с каждым полем.

4.8.2.4. Управление учетной записью пользователя

Управление учетными записями пользователей может осуществляться на странице *Настройки* → *Пользователи*. Возможности для управления учетной записью пользователя:

1. Изменение учетной записи. Доступно только пользователям с ролью «Администратор». Для изменения:

а. Выполните одно из действий:

- Для изменения своей учетной записи нажмите на кнопку  («Перейти в профиль пользователя») в нижнем левом углу главного меню.
- Для изменения учетной записи другого пользователя нажмите на кнопку «Изменить» в окне просмотра свойств для этого пользователя или на кнопку  в строке с учетной записью.

Результат шага: Появится окно «Изменение свойств пользователя».

б. Измените необходимые вам значения полей.

При этом осуществляется проверка значений в полях формы и, в случае ошибок, выводится информация об ошибках рядом с каждым полем.

Изменение свойств пользователя ✕

Логин
ivanov_p


ФИО
Иванов Петр Александрович

Роль пользователя *
Пользователь ▾

Email
ivanov_p@example.ru

Подразделение
Отдел ИБ

ID
4

Статус
Активен  Заблокировать пользователя

Сохранить **Удалить** **Отменить**

Рис. 4-63 Изменение свойств учетной записи пользователя

Изменение свойств пользователя ✕

Логин:	ivanov
Фамилия Имя Отчество:	Иванов Иван
Email:	ivanov@ussc.ru
ID:	5

Роль пользователя ✱

Пользователь ▼

Статус

Активен
 Заблокировать пользователя

Сохранить
Удалить
Отменить

Рис. 4-64 Изменение свойств учетной записи пользователя LDAP

с. Нажмите на кнопку «Сохранить».

2. Блокировка пользователя. Для блокировки:

a. Нажмите на кнопку «Изменить» в окне просмотра свойств или на кнопку в строке с учетной записью.

Результат шага: Появится окно «Изменение свойств пользователя».

b. Нажмите на кнопку «Заблокировать пользователя» ;

Результат шага: Статус учетной записи сменится на «Заблокирован». Открытые сессии заблокированного пользователя будут удалены. При попытке авторизации появится сообщение об ошибке «Пользователь заблокирован».


3. Разблокировка пользователя. Для разблокировки:

a. Нажмите на кнопку «Изменить» в окне просмотра свойств или на кнопку в строке с учетной записью.

b. Нажмите на кнопку «Разблокировать пользователя» ;

Результат шага: Статус учетной записи сменится на «Активен». Станет доступна авторизация с использованием этой учетной записи.

4. Удаление пользователя. Для удаления:

- a. Нажмите на кнопку «Изменить» в окне просмотра свойств или на кнопку  в строке с учетной записью.

Результат шага: Появится окно «Изменение свойств пользователя».

- b. Нажмите на кнопку «Удалить».

После нажатия на кнопку выводится окно подтверждения удаления учетной записи.

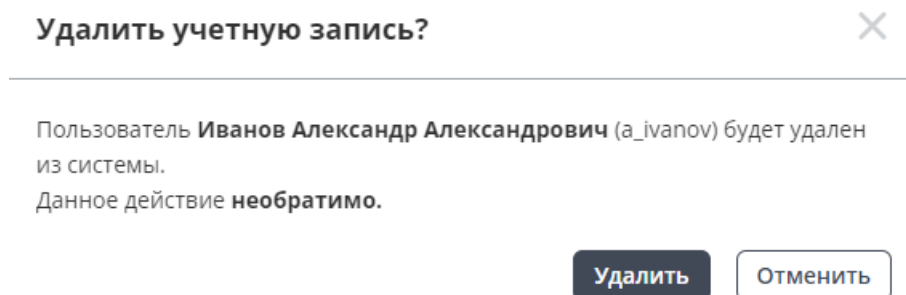


Рис. 4-65 Окно подтверждения удаления учетной записи


- c. Нажмите на кнопку «Удалить» в окне подтверждения.

Результат шага: Учетная запись будет удалена, при этом открытые сессии пользователя будут завершены.

4.8.2.5. Изменение пароля пользователя

Пользователям с ролью «Администратор» доступно изменение паролей всех учетных записей, с ролью «Пользователь» – только изменение пароля своей учетной записи. Для изменения пароля:

1. Выполните одно из действий:

- a. Для изменения своего пароля нажмите на кнопку «Перейти в профиль пользователя»  в нижнем левом углу главного меню.
- b. Для изменения пароля другого пользователя нажмите на имя этого пользователя в списке на странице *Настройки → Пользователи*.

Результат шага: Откроется окно «Свойства пользователя».

2. Нажмите на кнопку «Изменить пароль».

Свойства пользователя		✕
Тип учетной записи:	Локальная	
Логин:	itm	
Фамилия Имя Отчество:	Иванов Петр Петрович	
Роль:	Администратор	
Email:	ivanov@example.ru	
Подразделение:	Отдел ИБ	
ID:	1	
Статус:	Активен	

[Изменить пароль](#) [Изменить](#) [Закреть](#)

Рис. 4-66 Окно «Свойства пользователя»

Результат шага: Откроется окно «Изменение пароля пользователя».

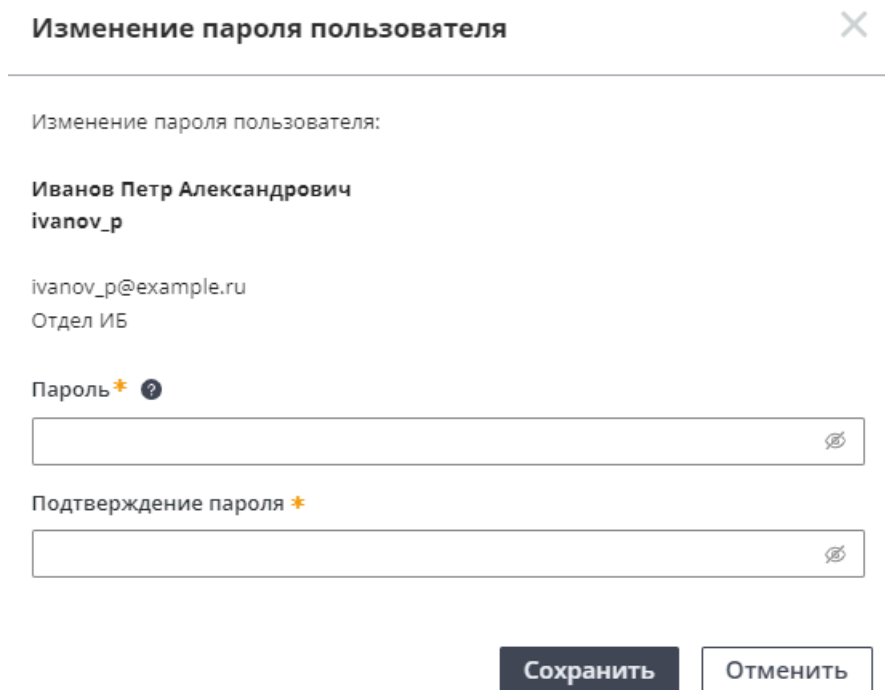
3. В открывшемся окне введите новый пароль и подтвердите его.

 **Подсказка:**

При создании пароля к учетной записи необходимо следовать требованиям парольной политики:

- длина — не менее 12 символов;
- символы — буквы в нижнем и верхнем регистрах, цифры и специальные символы;
- минимальное количество цифр — 2.

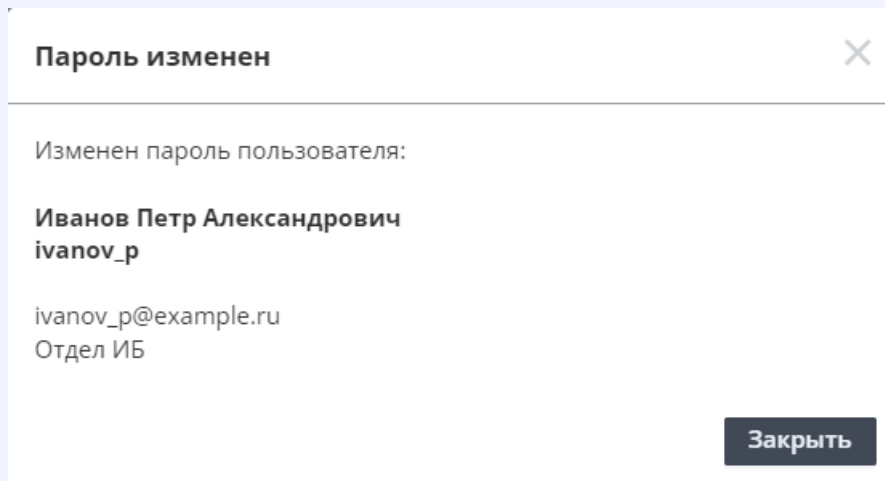
4. Нажмите на кнопку «Сохранить».



The dialog box is titled "Изменение пароля пользователя" (Change user password) and has a close button (X) in the top right corner. Below the title, it says "Изменение пароля пользователя:". The user's name "Иванов Петр Александрович" and login "ivanov_p" are displayed. Below that, the email "ivanov_p@example.ru" and department "Отдел ИБ" are shown. There are two password input fields: "Пароль" (Password) with a star and a help icon, and "Подтверждение пароля" (Confirm password) with a star. Both fields have a copy icon on the right. At the bottom, there are two buttons: "Сохранить" (Save) and "Отменить" (Cancel).

Рис. 4-67 Окно «Изменение пароля пользователя»

Результат шага: Появится окно «Пароль изменен».



The dialog box is titled "Пароль изменен" (Password changed) and has a close button (X) in the top right corner. Below the title, it says "Изменен пароль пользователя:". The user's name "Иванов Петр Александрович" and login "ivanov_p" are displayed. Below that, the email "ivanov_p@example.ru" and department "Отдел ИБ" are shown. At the bottom right, there is a "Закреть" (Close) button.

Рис. 4-68 Окно «Пароль изменен»

5. Нажмите на кнопку «Закреть» в окнах «Пароль изменен» и «Изменение пароля пользователя».

Результат шага: Пароль учетной записи изменится. Сессия, в которой был изменен пароль, останется активной, остальные открытые сессии пользователя с измененным паролем завершатся.

4.8.3. LDAP

Страница *Настройки* → *LDAP* предназначена для настройки подключения к каталогу LDAP и для предоставления пользователям возможности авторизации с использованием корпоративной учетной записи LDAP.

При выключенном LDAP возможна авторизация только с помощью локальных учетных записей, созданных администратором в разделе «Пользователи».

При включенном режиме LDAP администратор может добавить пользователей из корпоративного каталога LDAP (подробнее см. в разделе 4.8.2.3 Создание учетной записи пользователя LDAP (69)) и настроить подключение. После этого пользователям будет доступна авторизация с использованием корпоративной учетной записи.

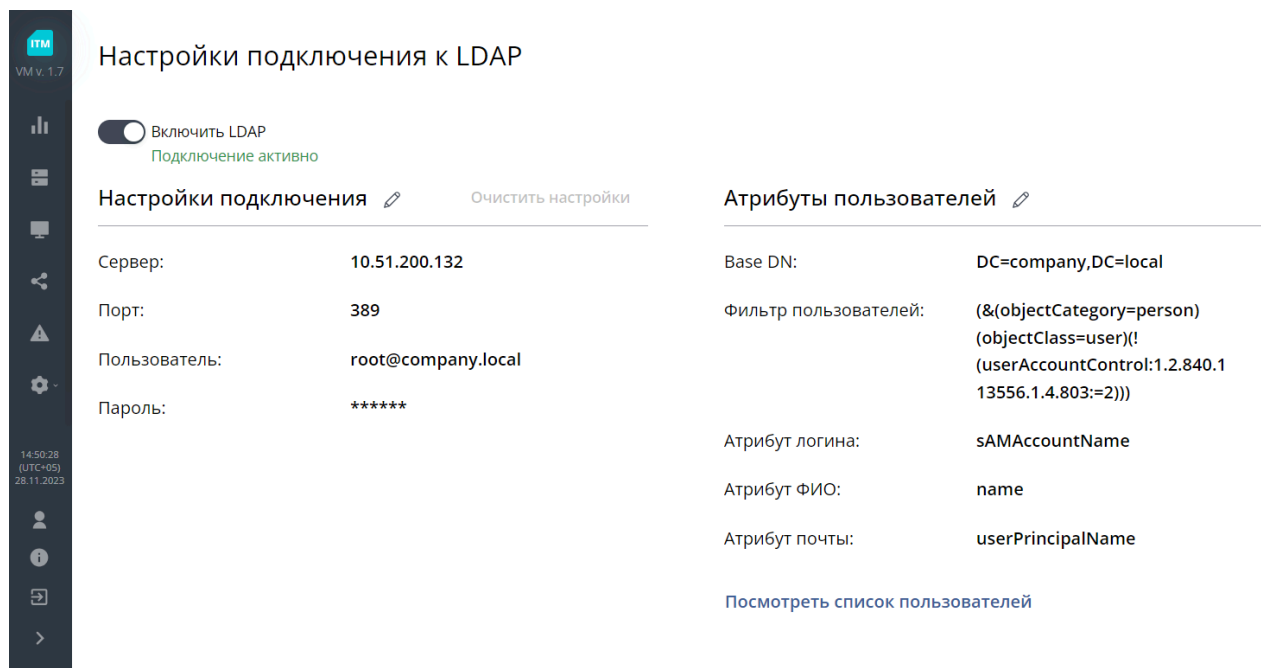


Рис. 4-69 Настройки подключения к LDAP

Рекомендуемая версия ОС для сервера, где находится каталог LDAP – Windows Server 2008 и выше. Для подключения UDV-ITM-VM к LDAP-каталогу и входа в веб-интерфейс UDV-ITM-VM необходимо, чтобы учетная запись LDAP имела права на подключение к домену и чтение списка доменных пользователей. В большинстве случаев достаточно членства в группе Domain Users (Пользователи домена).

Прим.:

Права пользователя могут отличаться в зависимости от настроек домена.

В этом разделе:


- 4.8.3.1 Подключение к LDAP или LDAPS (79)
- 4.8.3.2 Настройка атрибутов пользователей LDAP или LDAPS (82)
- 4.8.3.3 Очистка настроек LDAP (86)

4.8.3.1. Подключение к LDAP или LDAPS

Для настройки подключения к LDAP или LDAPS:

1. Перейдите на страницу *Настройки* → *LDAP*.


2. Установите переключатель «Включить LDAP» в верхней части страницы в положение «Включено».
3. Настройте подключение к LDAP или LDAPS (LDAP over SSL). Для этого:

- a. Нажмите на кнопку  рядом с заголовком «Настройки подключения».

Результат шага: поля станут доступны для редактирования.

- b. Отредактируйте поля с параметрами подключения:

- Сервер — введите DNS-имя или IP-адрес сервера LDAP;
- Порт — введите значение 389 для настройки LDAP или 636 для настройки LDAPS;
- Пользователь — введите логин пользователя для подключения к LDAP-каталогу;

 **Подсказка:**

Рекомендуется создать отдельный аккаунт LDAP (пользователя LDAP), чтобы подключаться к LDAP-серверу с минимальными привилегиями в LDAP, вместо использования реальных аккаунтов пользователей. Такой подход более безопасный и не потребует изменения пароля, если пользователь изменит свой пароль на LDAP-сервере.

- Пароль — введите пароль пользователя для подключения к LDAP-каталогу.

Настройки подключения к LDAP

Включить LDAP
Подключение активно

Настройки подключения

[Очистить настройки](#)

Сервер * ?

Порт * ?

Пользователь * ?

Пароль * ?

Использовать SSL

Рис. 4-70 Редактирование настроек подключения для LDAPS

- с. Измените положение переключателя «Использовать SSL»:
- включите протокол SSL для настройки LDAPS;
 - отключите протокол SSL для настройки LDAP.
- d. Нажмите на кнопку «Подключить».
- e. Возможные ошибки: «Невозможно подключиться к серверу LDAP», «Не правильный логин или пароль». В случае ошибок необходимо убедиться в корректности введенных данных для подключения.
- f. После успешного подключения к серверу LDAP, система автоматически получит список пользователей каталога LDAP и определит используемую схему атрибутов пользователей. Убедитесь в корректности атрибутов пользователей следующим образом:
- i. Нажмите на кнопку «Посмотреть список пользователей».
- Результат шага: откроется окно со списком пользователей LDAP.

Список пользователей LDAP ✕

Логин	Полное имя	E-mail
agent	agent	agent@example.ru
a_alekseev	Alex Alekseev	a_alekseev@example.ru
1c_admin	1C administrator	1c_admin@example.ru
Administrator	Administrator	Administrator@example.ru
a_ivanova	Anna Ivanova	a_ivanova@example.ru
b_petrov	Boris Petrov	b_petrov@example.r

Рис. 4-71 Список пользователей LDAP

- ii. Найдите строку, где значение в поле «Атрибут логина» соответствует логину известной вам учетной записи (например, учетной записи, используемой для подключения к каталогу).
- iii. Убедитесь, что значения атрибутов «Полное имя» и «E-mail» соответствуют данной учетной записи.
- iv. Если значения атрибутов в таблице корректные, то интеграция с сервером LDAP осуществлена успешно, нажмите на кнопку «Заккрыть».
- v. Если значения атрибутов в таблице некорректные, то интеграция с сервером LDAP осуществлена не успешно и требуется настройка схемы атрибутов пользователей. Настройка схемы может быть выполнена в соответствии с 4.8.3.2 Настройка атрибутов пользователей LDAP или LDAPS (82).

4.8.3.2. Настройка атрибутов пользователей LDAP или LDAPS


В разделе «Атрибуты пользователей» необходимо указать базу поиска. Другие атрибуты будут автоматически заполнены корректными значениями после редактирования и сохранения настроек подключения к LDAP или LDAPS, но при необходимости их можно изменить.

Прим.:

Редактирование атрибутов пользователей LDAP или LDAPS доступно, только когда указаны настройки подключения LDAP или LDAPS.

Для изменения атрибутов пользователей LDAP или LDAPS:

1. Перейдите на страницу *Настройки* → *LDAP*.

2. Нажмите на кнопку  рядом с заголовком «Атрибуты пользователей».

Результат шага: атрибуты станут доступны для редактирования.

3. В выпадающем списке BaseDN выберите базу поиска — объект каталога, в котором производится поиск учетных записей пользователей. База поиска указывается в формате `CN=имя_объекта,DC=класс_объекта_домена`.

Пример: База поиска `CN=TestObject,DC=example,DC=ru` означает, что поиск будет произведен в объекте с именем `TestObject` в домене `example.ru`.

4. При необходимости отредактируйте другие атрибуты пользователей:

- а. Фильтр пользователей — критерий, по которому выбирается объект из базы поиска. Фильтр влияет на то, какие записи попадут в список пользователей. Примеры доступных фильтров:

- вывод списка всех включенных пользователей текущего домена. Используется как значение по умолчанию в поле «Фильтр пользователей»:

```
(&(objectCategory=person)(objectClass=user)(!(userAccountControl:1.2.840.113556.1.4.803:=2)))
```

- вывод списка пользователей конкретного подразделения и конкретной группы:

```
(&(objectCategory=person)(memberOf=cn=TestGroup,ou=TestOU,dc=company,dc=local))
```

Где:

- `OU` — подразделение;
 - `DC` — домен-контроллер;
 - `TestGroup` — наименование группы;
 - `TestOU` — наименование подразделения;
 - `company` — наименование поддомена, где находится подразделение `TestOU`;
 - `local` — наименование домена, где находится поддомен `company`.
- вывод списка пользователей из разных подразделений и групп:

```
(&(objectCategory=person)(|(memberOf=cn=TestGroup,ou=TestOU,dc=company,dc=local)(memberOf=cn=TestGroup2,ou=TestOU2,dc=company,dc=local)))
```

Где:

- `OU` — подразделение;
- `DC` — домен-контроллер;
- `TestGroup` и `TestGroup2` — наименование Группы1 и Группы2;
- `TestOU` и `TestOU2` — наименование Подразделения1 и Подразделения2;
- `company` — наименование поддомена, где находятся подразделения `TestOU` и `TestOU2`;
- `local` — наименование домена, где находится поддомен `company`.

- вывод списка групп, имя которых начинается с «Test»:


```
(&(objectCategory=group)(cn=Test*))
```

- вывод списка пользователей, которые находятся в подразделении с несколькими уровнями вложенности:

```
&(objectCategory=person)
(memberOf=cn=test_inside,ou=Inside_deep,ou=Inside,ou=TestOU,dc=company,dc=local)
```

Где:

- `OU` – подразделение;
- `DC` – домен-контроллер;
- `test_inside` – наименование группы;
- `Inside_deep`, `Inside`, `TestOU` – каталоги, которые составляют путь к подразделению, где находится группа `test_inside`;

 **Прим.:**

В фильтре каталоги указываются в обратном порядке, начиная с `Inside_deep`. Путь, который они составляют – `TestOU/Inside/Inside_deep`.

- `company` – наименование поддомена, где находится подразделение `TestOU/Inside/Inside_deep`;
- `local` – наименование домена, где находится поддомен `company`.

b. Атрибут логина – поле, где хранится логин пользователя;

c. Атрибут ФИО – поле, где хранится ФИО пользователя;

d. Атрибут почты – поле, где хранится адрес электронной почты пользователя;

 **Внимание:**

Параметры полей «Атрибут логина», «Атрибут ФИО», «Атрибут почты» определяются автоматически. Изменение этих значений может потребоваться только в случае, если схема атрибутов пользователей в каталоге подключенного сервера LDAP отличается от стандартной, что проявляется в некорректных значениях в столбцах «Логин», «Полное имя» и «E-mail» списка пользователей.

Атрибуты пользователей

Base DN *

DC=company,DC=local

Фильтр пользователей *

```
(&(objectCategory=person)
(objectClass=user)(!
(userAccountControl:1.2.840.11355
6.1.4.803:=2)))
```

Атрибут логина *

sAMAccountName

Атрибут ФИО *

name

Атрибут почты *

userPrincipalName

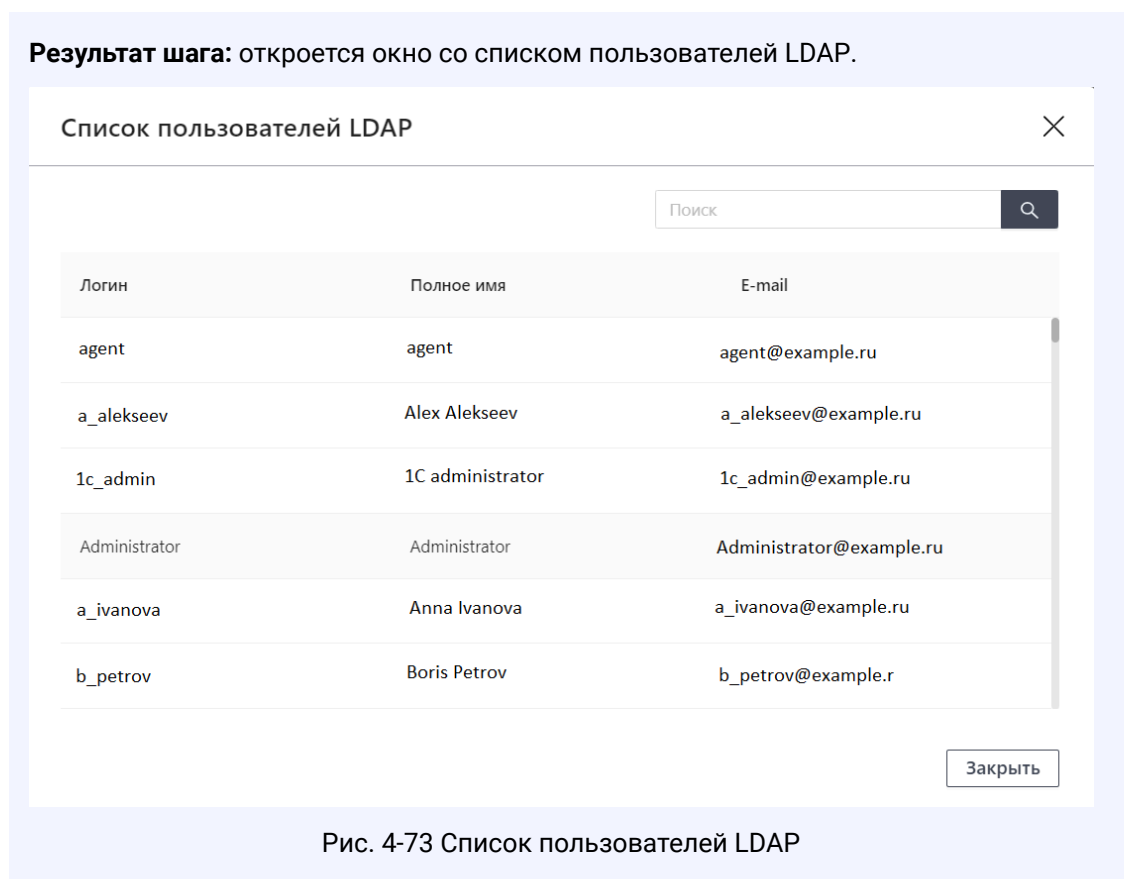
Сохранить


Отменить

[Посмотреть список пользователей](#)

Рис. 4-72 Редактирование атрибутов пользователей

5. Нажмите на кнопку «Сохранить» для применения изменений.
6. Просмотрите список пользователей LDAP, чтобы убедиться в корректности интеграционной схемы атрибутов пользователей и ее соответствии схеме атрибутов пользователей в каталоге подключенного сервера LDAP. Для этого:
 - a. Нажмите на кнопку «Посмотреть список пользователей».



- b. Просмотрите список пользователей. Для каждого пользователя указаны логин, полное имя и e-mail.
- c. Для поиска конкретной записи введите начальные символы или полное название одного из параметров в строку поиска и нажмите на кнопку «».

Результат шага: в окне появятся записи, соответствующие критерию поиска.

- d. Нажмите на кнопку «Закреть».

После завершения настроек добавьте учетную запись LDAP для входа в веб-интерфейс UDV-ITM-VM. Подробнее см. в разделе 4.8.2.3 Создание учетной записи пользователя LDAP (69).

4.8.3.3. Очистка настроек LDAP

В UDV-ITM-VM можно очистить параметры подключения к LDAP. Это может понадобиться для очистки параметров тестового контура, перемещения сервера в другой сегмент и т.п. Для очистки настроек:

1. Перейдите на страницу *Настройки* → *LDAP*.
2. Установите переключатель «Включить LDAP» в верхней части страницы в положение «Выключено».

Результат шага: кнопка «Очистить настройки» станет активна.

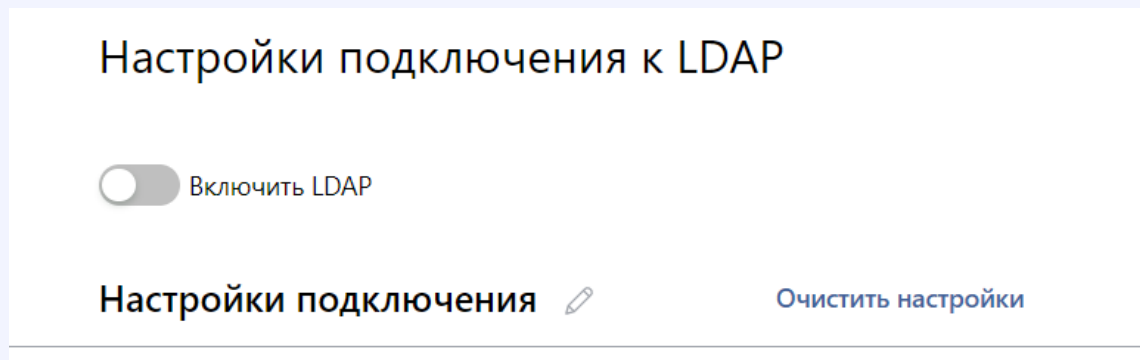


Рис. 4-74 Кнопка «Очистить настройки» при выключенном переключателе LDAP.

3. Нажмите на кнопку «Очистить настройки».

Результат шага: появится окно подтверждения.

4. В открывшемся окне нажмите на кнопку «Подтвердить».

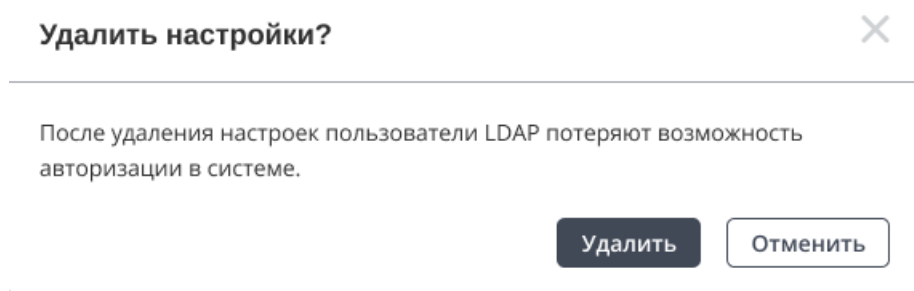




Рис. 4-75 Окно подтверждения очистки настроек

Результат шага: после подтверждения параметры подключения LDAP полностью очистятся.

4.8.4. Правила оповещений


В разделе основного меню *Настройки* → *Правила оповещений* можно создавать, просматривать и редактировать правила оповещений о проблемах. Правила оповещений позволяют пользователям получать уведомления о появлении или изменении критичности проблем на указанную электронную почту. Ограничения на количество правил оповещений нет.

Рядом с заголовком страницы отображается иконка  или , которая показывает состояние работоспособности канала Email-оповещений. Состояние канала оповещения проверяется при открытии страницы, для этого:

1. Проверяется факт настройки Email-сервера.
2. Проверяется наличие ответа на обращение к Email-серверу.

Возможные состояния канала оповещения:

-  — подключение к Email-серверу настроено и функционирует;

-  – подключение к Email-серверу не настроено или Email-сервер не отвечает.

Строка информации над списком правил оповещений содержит следующие элементы:


1. Название «Правила оповещений»;
2. Информация об общем количестве правил оповещений в формате:

Правила оповещений: [общее количество добавленных правил] всего [количество правил в статусе «Активно»] активно




3. Строка поиска – предназначена для поиска правил в списке по полям «ID», «Наименование» и «Получатели»;
4. Кнопка «Добавить правило» – при нажатии на кнопку появляется окно добавления нового правила оповещений. Подробнее см. в разделе 4.8.4.1 Создание правила оповещений (89).

Таблица со списком правил оповещений содержит следующие столбцы:

- ID – идентификатор правила, нужен для сортировки, сопоставления записей в логах при поиске неисправностей и т.п.;

 **Прим.:**

Последовательность идентификаторов может содержать пропуски, так как идентификаторы удаленных или несохраненных из-за ошибок правил повторно не используются.

- Наименование;
- Статус – актуальный статус правила оповещений, «Активно» или «Неактивно»;
- Расписание – время отправки оповещений. Доступны следующие варианты:
 - Немедленно – для режима отправки оповещений сразу;
 - Ежедневно в ЧЧ:ММ – для режима отправки оповещений по расписанию.
- Получатели – список адресов электронной почты получателей оповещений;
- Столбец с кнопками действий, которые можно совершить с правилом:
 -  – редактировать правило;
 -  – выключить правило;
 -  – удалить правило.

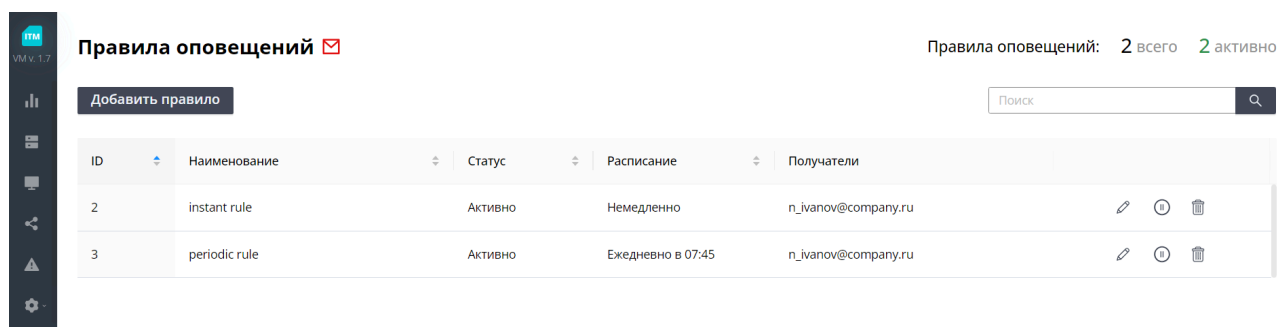


Рис. 4-76 Список правил оповещений

Таблицу можно отсортировать по полям «ID», «Наименование», «Статус», «Расписание». По умолчанию записи отсортированы по возрастанию значений поля «ID».

Количество отображаемых на странице правил оповещений можно изменить, кликнув по выпадающему списку в правом нижнем углу. Доступные значения — 10, 20 и 50. Значение по умолчанию — 20.

В этом разделе:

- 4.8.4.1 Создание правила оповещений (89)
- 4.8.4.2 Управление правилами оповещений (92)

4.8.4.1. Создание правила оповещений

Для создания правила оповещений:

1. Перейдите на страницу *Настройки* → *Правила оповещений*.
2. Нажмите на кнопку «Добавить правило» в верхнем левом углу страницы.

Результат шага: Откроется окно «Создание правила оповещений».

3. В открывшемся окне заполните поле «Наименование».

Прим.:

Наименование правила обнаружения должно быть уникальным.

4. Выберите тип правила оповещений:
 - Отправить сразу — оповещение отправляется сразу при обнаружении или изменении критичности проблемы;
 - Отправлять списком один раз в сутки — отправляется список проблем за сутки в заданное время. При выборе этого варианта укажите серверное время отправки сообщения в формате чч:мм. По умолчанию указано время 07:45.
5. При необходимости в выпадающем списке «Объекты» выберите филиалы или входящие в них ТК, для ОМ которых будут формироваться оповещения.

 **Прим.:**

По умолчанию оповещения формируются для **ОМ** всех филиалов и входящих в них **ТК**.

При выборе филиала входящие в него ТК не выбираются автоматически. Выбор ТК доступен независимо от того, выбран ли филиал, к которому он относится. Если у филиала 5 или больше вложенных ТК, становятся доступны кнопки:

- «Выделить все» – нажмите, чтобы выбрать все ТК, входящие в филиал.
- «Снять выделение» – нажмите, чтобы отменить выбор всех ТК, входящих в филиал.

6. В выпадающем списке «Важность» выберите уровень важности проблем. Оповещения будут отправляться для проблем с выбранным и более высокими уровнями важности. Доступны следующие значения:

- Критическая – значение по умолчанию;
- Высокая;
- Средняя;
- Предупреждение;
- Информационная;
- Не классифицировано.

7. Введите один или несколько адресов электронной почты получателей оповещений в поле «Email получателей».

8. При необходимости введите описание правила.

Создание правила оповещений ✕

Наименование *

Тип правила оповещения *

Отправить сразу **i**

Отправлять списком один раз в сутки **i**

Объекты **i**

Важность * **i**

Email получателей *

Описание

Рис. 4-77 Окно создания правила оповещений

9. Нажмите на кнопку «Сохранить».

Результат шага:

При срабатывании правила оповещения будут приходить в следующем формате:

Тема письма: ITM [Критичность] [Наименование оповещения] [Имя ОМ]

[Была создана новая проблема:] или [У проблемы обновлена критичность:] или [Отчет о проблемах функционирования объектов мониторинга за сутки к [чч:мм (UTC) дд.мм.гггг]:]

Всего событий – [Количество проблем], нерешенных – [Количество нерешенных проблем]

№	Время появления	Критичность	Филиал, ТО	Объект	Проблема	Состояние
[Номер]	[Серверное время в формате гггг-мм-дд чч-мм-сс (UTC)]	[Уровень критичности проблемы]	[Наименование филиала] или [Наименование филиала и ТО]	[Наименование объекта]	[Наименование проблемы]	«Требуется решение» или «Решена [дата и время в формате гггг-мм-дд чч-мм-сс (UTC)]»

Наименование сервера ITM-VM – [Наименование сервера ITM-VM]

Оповещение – [ID оповещения], [Наименование оповещения]

4.8.4.2. Управление правилами оповещений

Управление правилами оповещений осуществляется на странице *Настройки → Правила оповещений*.

Доступны следующие возможности:

1. Просмотр правила оповещений. Для просмотра:


- а. Нажмите на строку с правилом в списке.

Результат шага: Откроется всплывающее окно просмотра свойств правила оповещений.

Правило оповещений ✕

Наименование:	Критические проблемы филиала 164
Периодичность:	Немедленно
Объекты:	Fil 164
Важность:	Критическая
E-mail получателей:	a_ivanov@company.ru
ID правила:	4
Статус:	Активно
Описание:	

Рис. 4-78 Окно «Правило оповещений»

- b. Нажмите на кнопку «Закреть» для завершения просмотра.
2. Редактирование правила оповещений. Для редактирования:
 - a. Нажмите на кнопку «Изменить» в окне просмотра свойств правила оповещений или на кнопку  в строке с правилом.

Результат шага: Откроется всплывающее окно «Изменение правила оповещений».

Изменение правила оповещений ✕

Наименование *

Тип правила оповещения *

Отправить сразу ⓘ

Отправлять списком один раз в сутки ⓘ

Объекты ⓘ

Важность * ⓘ

Email получателей *


Описание

ID

Сохранить

Рис. 4-79 Окно «Изменение правила оповещений»


b. Измените необходимые вам свойства.

 **Прим.:**

Если рядом с одним из филиалов в поле «Объект» отображается надпись «сервер удален», этот филиал был удален из списка подключенных серверов мониторинга (подробнее см. в разделе 4.3.7 Удаление подключенного сервера мониторинга (37)). Такой филиал можно удалить из списка объектов, но нельзя добавить туда. Удаление филиала из списка подключенных серверов мониторинга не влияет на статус правила.


c. Нажмите на кнопку «Сохранить».

3. Включение правила оповещений. Для включения:

- а. Нажмите на кнопку .

Результат шага: Статус правила сменится на «Активно», оповещения будут отправляться в соответствии с настройками правила.

4. Выключение правила оповещений. Для выключения:

- а. Нажмите на кнопку .

Результат шага: Статус правила сменится на «Неактивно», оповещения перестанут отправляться.

5. Удаление правила оповещений. Для удаления:

- а. Нажмите на кнопку  в строке с правилом.

Результат шага: Появится всплывающее окно «Удаление правила оповещения».

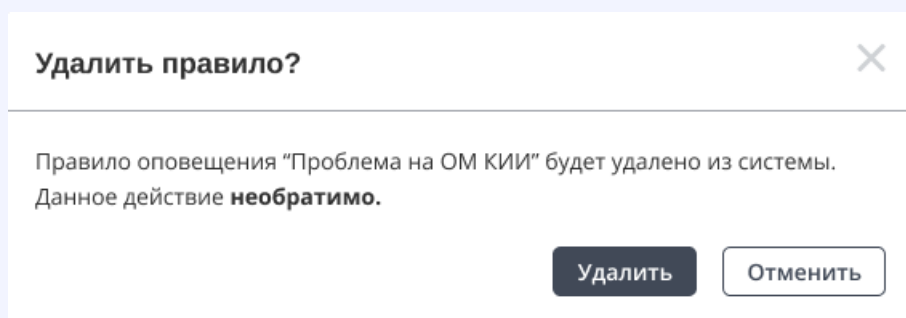







Рис. 4-80 Окно «Удаление правила оповещения»

- б. Нажмите на кнопку «Удалить».

5. Справочная информация

5.1. Роли пользователей и доступные им интерфейсы

Табл. 5-1

Роль	Список доступных для роли интерфейсов	Список доступных страниц
Пользователь	Интерфейс авторизации	
	Интерфейс управления	<ul style="list-style-type: none"> • <i>Панель информации</i> – доступны просмотр и работа с графиками. • <i>Серверы мониторинга</i> – только просмотр списка и карточки сервера. • <i>Объекты мониторинга</i> – просмотр списков и карточек. • <i>ИТ-услуги</i> – просмотр списка и карточек ИТ-услуг. • <i>Проблемы</i> – просмотр списка и карточки со списком событий. • <i>Настройки</i> → <i>Правила оповещений</i> – просмотр списка и карточек правил; создание, изменение, включение, выключение и удаление собственных правил оповещений. • Окно «Свойства пользователя» при нажатии на кнопку  в нижнем левом углу – просмотр параметров своей учетной записи, изменение пароля. • Окно «О системе» при нажатии на кнопку  в нижнем левом углу – просмотр информации
Администратор	Интерфейс авторизации	
	Интерфейс управления	Все разделы со всем функционалом в полном объеме
Техническая	Техническая учетная запись предназначена для доступа смежных систем к данным по API. Не рекомендуется использовать техническую учетную запись для доступа в веб-интерфейс, так как корректная работа при этом не гарантируется.	
Оператор мониторинга	Интерфейс авторизации	
	Интерфейс управления	<ul style="list-style-type: none"> • <i>Панель информации</i> – доступны просмотр и работа с графиками. • Окно «Свойства пользователя» при нажатии на кнопку  в нижнем левом углу – просмотр параметров своей учетной записи. • Окно «О системе» при нажатии на кнопку  в нижнем левом углу – просмотр информации. <div style="border: 1px solid #add8e6; padding: 5px; margin-top: 10px;"> <p> Прим.: Для этой роли время пользовательской сессии не ограничено</p> </div>

5.2. Совместимость компонентов решения для UDV-ITM-VM

В таблице указаны поддерживаемые версии компонентов решения для UDV-ITM-VM v. 1.7.0.

Табл. 5-2 Совместимость компонентов решения для UDV-ITM-VM

Компонент решения	Версия ПО	Примечание
Подключаемые серверы мониторинга	<ul style="list-style-type: none"> • UDV-ITM-M v. 1.6*; 1.5; 1.4; 1.3 • Zabbix v. 5.2; 5.0; 4.0 	При подключении Zabbix v. 4.0 отсутствует сбор данных журналов аудита.
Операционная система	<ul style="list-style-type: none"> • РЕД ОС v. 7.3*; 7.2 • CentOS v. 8.4 • Astra Linux Special Edition (Смоленск) v. 1.6 	
СУБД	<ul style="list-style-type: none"> • Jatoba v. 4.5*; 1.14 	

Табл. 5-2 Совместимость компонентов решения для UDV-ITM-VM

Компонент решения	Версия ПО	Примечание
	• PostgreSQL v. 14	
Виртуализация	Docker v. 20	

Где * – рекомендованная версия, обеспечивающая весь доступный функционал и стабильность работы.