

UDV MultiProtect

Руководство по эксплуатации

Содержание

1. Введение.....	8
2. Глоссарий.....	9
3. Справочная информация.....	15
3.1. Общие сведения.....	15
3.2. Разделение функций по администрированию.....	16
3.3. Логическая структура Комплекса и режимы функционирования.....	18
3.4. Общее описание UDV MultiProtect.....	20
3.4.1. Интерфейс Комплекса.....	20
3.4.2. Дополнительные функции Комплекса.....	60
3.5. Условия эксплуатации Комплекса.....	72
3.6. Описание источников событий.....	73
3.6.1. Описание служебных источников событий.....	73
3.6.2. Описание безагентного сбора событий Eventlog.....	77
3.7. Описание полей событий.....	79
3.8. Переменные Комплекса.....	82
3.8.1. Переменные Комплекса уровня Management.....	82
3.8.2. Переменные Комплекса уровня Sensor.....	91
3.8.3. Переменные службы обнаружения вторжений.....	94
3.8.4. Рекомендации по использованию переменных файлов manager.env и sensor.env.....	97
3.9. Основные переменные файла environment.json.....	98
3.10. Отображение времени в Комплексе.....	99
3.11. Перечень данных, собираемых Комплексом.....	100
3.12. Протоколы, обнаруживаемые Комплексом.....	108
3.13. Рекомендации по настройке сбора данных.....	152
3.14. Реестр сканеров Комплекса.....	153
3.15. Сетевые взаимодействия Комплексов.....	203
3.16. Синтаксис правил корреляции событий.....	206
3.16.1. Поддерживаемые типы событий.....	207
3.16.2. Фильтр событий.....	224
3.16.3. Временное окно.....	225
3.16.4. Группировка.....	227
3.16.5. Условие инцидента.....	228
3.16.6. Шаблоны обработки сложных событий.....	229
3.16.7. Сообщение инцидента.....	231

3.16.8. Приоритет и активность правил.....	232
3.17. События, попадающие в разделы мониторинга.....	233
3.18. Структура директорий Комплекса.....	313
4. Первичная настройка Комплекса.....	315
4.1. Подключение Комплекса.....	315
4.1.1. Подключение к веб-интерфейсу по протоколу HTTPS.....	315
4.1.2. Первоначальная настройка.....	318
4.2. Настройка локальных реквизитов и домашней сети.....	320
4.2.1. Изменение сведений о Комплексе и сенсорах.....	321
4.2.2. Настройка домашней сети.....	323
4.3. Настройка парольной политики.....	324
4.4. Импорт справочников из архива.....	326
4.5. Запуск обнаружения вторжений и синхронизация правил с сенсорами.....	329
4.6. Проверка работоспособности Комплекса.....	330
4.6.1. Проверка работоспособности системы передачи данных по иерархии.....	330
4.6.2. Проверка обнаружения активов из домашней сети.....	330
4.6.3. Проверка работоспособности системы обнаружения потоков данных.....	331
5. Работа с событиями.....	332
5.1. Поиск и просмотр событий в упрощенном режиме.....	334
5.2. Просмотр событий и создание запросов в экспертном режиме.....	341
5.3. Просмотр панели мониторинга «Статус защищенности».....	344
5.4. Настройка сбора событий.....	347
5.4.1. Экспорт и импорт правил нормализации событий.....	347
5.4.2. Экспорт и импорт источников событий.....	353
5.4.3. Включение и отключение служебных источников.....	355
5.4.4. Создание источника событий.....	356
5.4.5. Управление источниками событий.....	358
5.4.6. Выгрузка событий Комплекса в архив.....	359
5.4.7. Отправка событий во внешнюю систему по протоколу Syslog.....	360
6. Работа с инцидентами.....	362
6.1. Ручное создание инцидентов.....	363
6.2. Анализ инцидентов.....	365
6.3. Обработка инцидентов.....	366
6.4. Изменение параметров инцидентов.....	367
6.5. Удаление инцидентов.....	370
6.6. Групповые операции над инцидентами.....	372

6.7. Настройка инцидентов.....	373
6.7.1. Экспорт и импорт политики корреляции и статусов инцидентов.....	375
6.7.2. Управление службой корреляции событий.....	384
6.7.3. Управление схемой корреляции.....	385
6.7.4. Управление правилами корреляции событий.....	389
6.7.5. Анализ событий для генерации инцидентов.....	394
6.7.6. Настройка оповещений при появлении инцидентов.....	401
6.8. Выгрузка отчетов по инцидентам.....	409
7. Работа с активами.....	410
7.1. Экспорт и импорт активов и их групп.....	412
7.1.1. Экспорт активов.....	413
7.1.2. Экспорт групп активов.....	413
7.1.3. Импорт активов.....	413
7.1.4. Импорт групп активов.....	414
7.2. Управление активами.....	415
7.2.1. Кнопки управления активами.....	415
7.2.2. Фильтрация списка активов.....	417
7.3. Создание актива.....	420
7.4. Группировка активов.....	422
7.4.1. Создание группы активов.....	422
7.4.2. Добавление активов в группу.....	424
7.4.3. Управление группами активов.....	426
7.5. Редактирование активов.....	429
7.6. Удаление активов.....	436
7.7. Выгрузка отчетов по активам.....	439
7.8. Настройки активов.....	440
7.8.1. Настройка учетных данных активов.....	440
7.8.2. Настройка классификаторов.....	447
8. Активный сбор данных с активов.....	455
8.1. Просмотр сводки конфигураций.....	455
8.2. Настройка конфигураций активов.....	458
8.2.1. Содержание Python-скриптов.....	458
8.2.2. Цифровая подпись Python-скрипта.....	461
8.2.3. Экспорт и импорт задач сбора данных, сканеров и их групп.....	462
8.2.4. Настройка сканеров сбора данных.....	467
8.2.5. Добавление сетевых атрибутов активу с помощью сканера сбора данных по SNMP.....	481

8.2.6. Сбор данных с активов.....	483
8.2.7. Просмотр статуса сбора данных.....	493
8.2.8. Работа с архивом изменений конфигурации актива.....	497
8.3. Настройка активного сбора событий.....	504
8.4. Настройка сбора данных об операционной системе и установленном ПО.....	505
8.4.1. Запуск сбора данных об операционной системе и установленном ПО.....	506
8.5.	
9. Поиск уязвимостей и проверка соответствия требованиям информационной безопасности.....	508
9.1. Поиск уязвимостей ПО и ОС в базах CVE, CPE и БДУ ФСТЭК России.....	509
9.1.1. Проверка актуальности справочников поиска уязвимостей.....	510
9.1.2. Импорт справочников CVE и CPE и файла сопоставления ПО с CPE.....	512
9.1.3. Импорт справочника БДУ ФСТЭК России.....	514
9.1.4. Запуск поиска уязвимостей в базах CVE, CPE и БДУ ФСТЭК России.....	515
9.1.5. Выгрузка отчета по результатам сопоставления собранного ПО со справочником CPE.....	519
9.2. Проверки на уязвимости и соответствие требованиям информационной безопасности с помощью OVAL.....	520
9.2.1. Экспорт и импорт скриптов, настроек, групп определений OVAL.....	522
9.2.2. Настройка OVAL-проверки актива на соответствие требованиям информационной безопасности.....	531
9.2.3. Запуск OVAL-проверки актива на соответствие требованиям информационной безопасности....	541
9.2.4. Просмотр и выгрузка результатов проверки актива на соответствие требованиям информационной безопасности.....	543
9.2.5. Повторный запуск OVAL-проверки на соответствие требованиям ИБ.....	546
9.2.6. Удаление OVAL-проверок актива на соответствие требованиям информационной безопасности.....	547
10. Инспекция сети Комплекса.....	548
10.1. Просмотр карты сети.....	549
10.2. Настройка представлений на карте.....	553
10.3. Просмотр потоков данных.....	557
10.4. Управление потоками данных.....	559
10.4.1. Фильтрация списка потоков данных.....	559
10.4.2. Отчет по потокам данных.....	562
10.4.3. Изменение потоков данных.....	563
10.4.4. Фильтрация списка правил управления потоками данных.....	573
10.4.5. Экспорт и импорт правил управления потоками данных.....	575
10.5. Служба обнаружения вторжений.....	577
10.5.1. Создание правил обнаружения вторжений.....	579

10.5.2. Управление службой обнаружения вторжений.....	581
10.5.3. Экспорт и импорт правил службы обнаружения вторжения.....	586
10.5.4. Создание исключений для правил обнаружения вторжений.....	592
10.5.5. Удаление исключений для правил обнаружения вторжений.....	595
11. Управление Комплексом.....	597
11.1. Изменение сведений о Комплексе и сенсорах.....	597
11.2. Сканирование сети и определение интерфейсов активного сетевого оборудования.....	599
11.2.1. Интерпретация результатов пассивного сканирования сети.....	600
11.3. Настройка домашней сети.....	601
11.4. Управление пользователями.....	602
11.4.1. Управление учетными записями пользователей.....	608
11.4.2. Настройка парольной политики.....	616
11.4.3. Отключение ограничения на количество сессий пользователей.....	618
11.5. Экспорт отдельных справочников.....	619
11.6. Диагностика состояния системы Комплекса.....	621
11.7. Диагностика состояния сенсора.....	623
11.8. Удаление сенсора.....	624
12. Регламентные работы.....	625
12.1. Резервное копирование данных.....	625
12.1.1. Резервное копирование рабочей директории и данных Комплекса уровня Management.....	626
12.1.2. Резервное копирование Комплекса уровня Sensor.....	628
12.1.3. Выгрузка событий Комплекса в архив.....	629
12.1.4. Экспорт отдельных справочников.....	630
12.1.5. Экспорт нескольких справочников.....	632
12.2. Смена паролей.....	634
12.2.1. Смена пароля системной учетной записи администратора.....	634
12.2.2. Смена пароля учетной записи в веб-интерфейсе Комплекса.....	635
12.3. Обновление серверного сертификата.....	636
12.4. Удаление данных Комплекса.....	638
13. Нештатные ситуации и действия по их устранению.....	639
13.1. Диагностика сервисов и иерархии.....	639
13.2. Действия по восстановлению комплекса при сбойных ситуациях и ошибках в данных.....	640
13.2.1. Веб-интерфейс не загружается.....	640
13.2.2. Соединение с главной страницей веб-интерфейса осуществляется по протоколу HTTP вместо HTTPS.....	643
13.2.3. Время на Комплексе отличается от времени получения события.....	644

13.2.4. После запуска Комплекса при попытке загрузки веб-интерфейса открывается пустая страница.....	645
13.2.5. 502-я ошибка при загрузке страницы авторизации, 500-е ошибки сразу после авторизации.....	646
13.2.6. Не обнаруживаются новые потоки.....	649
13.2.7. Комплекс не обнаруживает активы в автоматическом режиме.....	652
13.2.8. Комплекс не обнаруживает активы без IP-адреса.....	654
13.2.9. Два актива с одинаковым IP-адресом.....	655
13.2.10. Не осуществляется сбор необходимых событий или конфигураций.....	657
13.2.11. При попытке сбора данных в результатах выводится предупреждение «Превышено время ожидания выполнения задачи сбора событий».....	659
13.2.12. Сбор конфигураций осуществляется, но результаты сбора не отображаются.....	661
13.2.13. Отсутствуют события, генерируемые Комплексом.....	662
13.2.14. Не принимаются Syslog-сообщения от активов.....	665
13.2.15. Не принимаются сообщения от служб корреляции и обнаружения вторжений.....	666
13.2.16. Не принимаются сообщения от службы корреляции.....	667
13.2.17. Не инициализируется стек udv-opensearch, udv-opensearch-dashboards, udv-logstash.....	668
13.2.18. Не создается индекс в экспертном режиме страницы «События».....	669
13.2.19. Не удастся отфильтровать записи на странице «События» по новым значениям полей после нормализации.....	670
13.2.20. Объекты мониторинга и визуализации импортируются с ошибкой.....	671
13.2.21. Не удастся импортировать сканер сбора данных в веб-интерфейсе.....	672
13.2.22. Не выполняется архивация событий при превышении размера или времени хранения индекса.....	674
13.2.23. Ошибки вида «<...>Cannot start service <...>. Bind for <ip_address>:<TCP/UDP_port> is ready allocated» при попытке запуска сервисов.....	675
13.2.24. Недоступен сервис корреляции событий.....	676
13.2.25. При бездействии в веб-интерфейсе сеанс завершается раньше, чем через 10 минут.....	677
13.2.26. Ошибки поиска уязвимостей в базах CVE, CPE и БДУ ФСТЭК России.....	679
13.2.27. Не устанавливается соединение с сенсором.....	683
13.3. Восстановление данных из резервных копий.....	686
13.3.1. Восстановление данных из резервных копий Комплекса уровня Management и Комплекса уровня Management+Sensor.....	686
13.3.2. Восстановление данных из резервных копий Комплекса уровня Sensor.....	690
13.4. Действия в случаях несанкционированного доступа к данным.....	692
13.4.1. Просмотр журнала действий пользователей Комплекса.....	692
13.4.2. Изменение статуса активности учетной записи пользователя Комплекса.....	693
13.5. Действия в других аварийных ситуациях.....	694
13.6. Диагностика сервиса сбора данных по протоколам SSH, Telnet, WinRM, winexe.....	695

1. Введение

В настоящем документе приведено Руководство по эксплуатации Комплекса UDV MultiProtect. В документе описаны область назначения, возможности Комплекса, процедуры подготовки к работе и мониторинга работоспособности Комплекса, выполняемые пользователями функции, задачи и процедуры Комплекса, а также действия в нештатных ситуациях.

2. Глоссарий

2.1. Автоматизированная система

Система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

2.2. Актив

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

2.3. Банк данных угроз безопасности информации ФСТЭК России

База данных уязвимостей, созданная Федеральной службой по техническому и экспортному контролю. Содержит сведения об основных угрозах безопасности информации и уязвимостях, в первую очередь, характерных для государственных информационных систем и автоматизированных систем управления производственными и технологическими процессами критически важных объектов.

2.4. Бесклассовая адресация

Метод IP-адресации, позволяющий гибко управлять пространством IP-адресов, не используя жёсткие рамки классовой адресации.

2.5. Виджет

Представление информации о событиях в виде, удобном для зрительного наблюдения и анализа.

2.6. Внешняя сеть

Специфический элемент на карте, который включает в себя потоки из внешней сети в локальную и из локальной во внешнюю.

2.7. Задача сбора данных

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

2.8. Индекс событий

Совокупность событий за сутки.

2.9. Информационная безопасность

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

ИБ

2.10. Информационная система

Система, которая организует хранение и манипулирование информацией о предметной области.

Аббревиатура: ИС

2.11. Информационный поток

Зарегистрированное взаимодействие между двумя узлами сети. Потоки данных регистрируются Комплексом автоматически на основе известных системе интерфейсов от активов.

2.12. Источник событий

Объект или сервис, от которого поступают события.

2.13. Карта сети

Модель, описывающая состав вычислительной сети предприятия: узлы и потоки между узлами на сетевом и канальном уровне.

2.14. Классификатор

Сгруппированный (по различным признакам) перечень наименованных объектов, где каждому из них присвоен уникальный код в соответствии с их общими признаками или различиями.

2.15. Комплекс

Программный комплекс UDV MultiProtect, предназначенный для мониторинга, контроля защищенности и анализа состояния ИБ для АСУ ТП, в т.ч. интернета вещей (IoT) и промышленного интернета вещей (IIoT). Комплекс позволяет выявлять несанкционированные изменения, уязвимости в компонентах и попытки их эксплуатации, регистрировать события, анализировать и расследовать инциденты информационной безопасности.

2.16. Конфигурация актива

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

2.17. Корреляция

Способность системы выявлять неочевидные закономерности в событиях и формировать инциденты на их основе.

2.18. Несанкционированный доступ

Доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами.



Внимание:

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

2.19. Нормализация событий

Приведение событий из разных источников к единому формату, принятому в Комплексе.

2.20. Операционная система

Комплекс взаимосвязанных программ, предназначенных для управления ресурсами компьютера и организации взаимодействия с пользователем.

ос

2.21. Панель мониторинга

Тип графического интерфейса, использующий интерактивные визуализации для обзора ключевых показателей.

2.22. Политика корреляции событий

Справочник, который содержит схему и правила корреляции.

2.23. Правила корреляции событий

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

2.24. Программно-техническое средство

Комплексное решение, состоящее из программных и аппаратных компонентов.

птс

2.25. Программное обеспечение

Программа или множество программ, используемых для управления компьютером.

по

2.26. Программный комплекс

Набор программных средств, работающих совместно для выполнения одной или нескольких сходных задач.

ПК

2.27. Регламентные работы

Комплекс профилактических работ и проверок, выполняемых на объектах автоматизированных систем в определенные (регламентированные) моменты времени периода эксплуатации и направленных на поддержание их надежности в течение межрегламентного срока.

2.28. Роль пользователя

Совокупность возможностей, которые получает пользователь Комплекса, входящий в определенное множество встроенных групп доступа, и оперирующий заданными наборами возможностей.

2.29. Сервис глубокой инспекции пакетов

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

2.30. Система обнаружения вторжений

Программное или аппаратное средство, предназначенное для выявления фактов неавторизованного доступа в компьютерную систему или сеть либо несанкционированного управления ими через Интернет.

СОВ

2.31. Сканер

Исполняемый скрипт сбора данных.

2.32. Скрипт

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

2.33. Справочник

Систематизированный список данных об одном или нескольких компонентах конкретного Комплекса.

2.34. Средство защиты информации

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

СрЗИ

2.35. Схема корреляции событий

Набор сущностей, используемый для представления и обработки событий, включает в себя представления различных типов событий, таких как окна данных, таблицы, контексты, переменные.

2.36. Технические условия

Документ, устанавливающий технические требования, которым должны соответствовать конкретное изделие, материал, вещество и пр. или их группа.

ТУ

2.37. Техническое обслуживание

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

ТО

2.38. Узел

Элемент сети предприятия, взаимодействующий с другими элементами сети.

2.39. Учетная запись

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

УЗ

2.40. Федеральная служба по техническому и экспортному контролю

Орган исполнительной власти, осуществляющий контроль за сертификацией и аттестацией автоматизированных систем с учетом требований информационной безопасности.

ФСТЭК

2.41. Фильтрация

Способ вывода нужных пользователю данных при помощи встроенных фильтров.

2.42. Common Platform Enumeration

Структурированная схема именования систем информационных технологий, программного обеспечения и пакетов.

CPE

2.43. Common Vulnerabilities and Exposures

База данных общеизвестных уязвимостей информационной безопасности.

CVE

2.44. Open Vulnerability and Assessment Language

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

OVAL

2.45. Syslog

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

2.46. UDV MultiProtect уровня Management

Компонент UDV MultiProtect с функциями управления сенсорами и анализа полученных с них данных.

Аббревиатура: Management

2.47. UDV MultiProtect уровня Sensor

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

Аббревиатура: Sensor

3. Справочная информация

3.1. Общие сведения

Решение UDV MultiProtect применяется для выявления несанкционированных изменений в информационных системах, регистрации событий информационной безопасности в ИС, выявления компонентов ИС, подверженных критическим уязвимостям, обнаружения попыток эксплуатации уязвимостей компонентов ИС до момента их устранения и автоматизированного контроля выполнения требований ИБ в ИС.

Текущая версия решения отображается в верхней левой части страницы рядом с логотипом.

UDV MultiProtect обеспечивает следующие функции и возможности:

- управление идентификаторами, в том числе создание, присвоение, изменение, уничтожение идентификаторов;
- сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения;
- мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них;
- генерирование временных меток и (или) синхронизация системного времени в автоматизированной системе управления;
- защиту информации о событиях безопасности;
- выявление, анализ и оперативное устранение вновь выявленных уязвимостей;
- контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации;
- контроль состава технических средств, программного обеспечения и средств защиты информации;
- защиту архивных файлов, параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки информации;
- обнаружение, идентификацию и регистрацию инцидентов;
- управление изменениями конфигурации автоматизированной системы управления и ее системы защиты;
- документирование информации (данных) об изменениях в конфигурации автоматизированной системы управления и ее системы защиты;
- идентификацию, проверку подлинности и контроль доступа субъектов в систему и к отдельным функциям Комплекса;
- возможность интеграции с внешними системами по протоколу Syslog и через API.

3.2. Разделение функций по администрированию

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

Табл. 1. Функциональные роли по администрированию Комплекса

НАИМЕНОВАНИЕ ФУНКЦИОНАЛЬНОЙ РОЛИ	КРАТКОЕ ОПИСАНИЕ ОСНОВНЫХ ФУНКЦИЙ
Инженер	Определение состава активов Добавление активов в каталог активов Определение легитимности изменений в составе активов Определение легитимности информационных потоков Определение легитимности изменения конфигурации активов Установка эталонной версии конфигурации активов Редактирование карты сети Привязывание интерфейсов к активам Формирование отчетов по результатам сканирования активов на уязвимости Формирование отчетов по результатам оценки выполнения требований по безопасной конфигурации активов Формирование отчетов по событиям и инцидентам ИБ Анализ событий и инцидентов ИБ Разработка задач сбора конфигураций с активов Запуск и контроль мероприятий по сбору конфигураций с активов
Администратор	Контроль функционирования компонентов ПТС Техническое обслуживание ПО Техническое обслуживание аппаратных средств Сопровождение и внедрение ПО Обновление СЗИ Изменение перечня информационных ресурсов, списков доступа и учетных записей пользователей Замена неисправного устройства

Табл. 1. Функциональные роли по администрированию Комплекса

НАИМЕНОВАНИЕ ФУНКЦИОНАЛЬНОЙ РОЛИ	КРАТКОЕ ОПИСАНИЕ ОСНОВНЫХ ФУНКЦИЙ
	Управление пользователями, в том числе присвоение ролей пользователям Управление парольной политикой Проверка реализации требований информационной безопасности Разработка правил корреляции событий ИБ Настройка сбора событий ИБ Настройка источников событий ИБ Настройка проверок актива на уязвимости и соответствие требованиям информационной безопасности Сканирование сети Управление иерархией
Просмотр веб-интерфейса	Просмотр всех разделов Комплекса
Просмотр панели мониторинга	Непрерывный просмотр страницы Статус защищенности

3.3. Логическая структура Комплекса и режимы функционирования

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

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

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

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

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

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

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

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

В Комплексе предусмотрено два режима функционирования:

1. Режим наблюдения (пассивный мониторинг), который подразумевает:

- одностороннее получение данных;
- прослушивание сетевого трафика и прием событий.

2. Режим «запрос-ответ» (активный мониторинг), который подразумевает:

- получение конфигурации и событий;
- взаимодействие с активами в режиме «запрос-ответ» с использованием штатных механизмов и протоколов;
- выявление уязвимостей и проверки на соответствие требованиям ИБ.

Табл. 2. Режимы функционирования Комплекса

ФУНКЦИИ	РЕЖИМ НАБЛЮДЕНИЯ	РЕЖИМ ОПРОСА
Сбор событий ИБ	х ✓	✓
Обнаружение атак	✓	✓

Табл. 2. Режимы функционирования Комплекса

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

3.4. Общее описание UDV MultiProtect

В этом разделе:

- Интерфейс Комплекса
- Дополнительные функции Комплекса

3.4.1. Интерфейс Комплекса

В разделе описаны детали работы с веб-интерфейсом Комплекса.

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

3.4.1.1. Страницы интерфейса

В подразделе описаны все страницы в интерфейсе решения.

3.4.1.1.1. Мониторинг

Пункт главного меню, включающий страницу **Статус защищенности**.

3.4.1.1.1.1. Статус защищенности

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

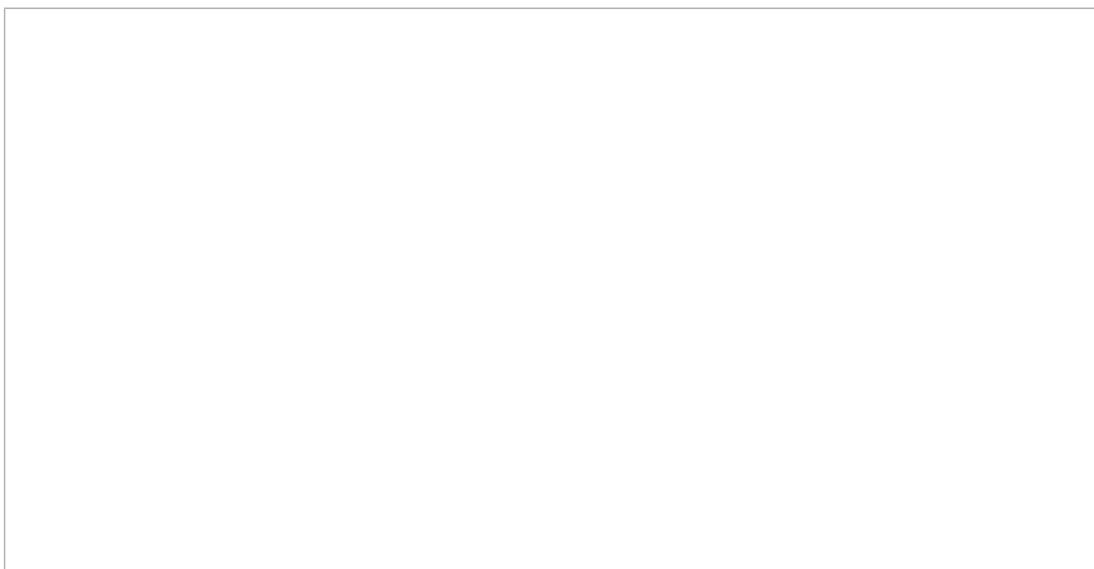


Рис. 1. Страница «Статус защищенности»

3.4.1.1.2. Инциденты

Пункт главного меню, содержащий информацию о всех выявленных и созданных инцидентах. На странице можно ознакомиться с подробностями инцидента: его текущим статусом, сформировавшими инцидент событиями, историей изменения инцидента, детализацией. В процессе расследования можно обновить статус и приоритет инцидента, подтвердить его или удалить. В результате будет сформировано событие с указанием выполненного действия, ответственного и его комментария.

☐	Дата регистрации...	Дата возникновения...	Номер	Наименование	Тип инцидента	Приоритет	Статус	Ответственный	Источник дан...
☐	04.03.2025, 14:40:56	04.03.2025, 14:40:37	349	123	Не определен	Критический	Новый	Михаил Монстров	ИР
☐	04.03.2025, 09:22:13		348	Обнаружен новый поток данных с у...	Аномальная сетев...	Высокий	Закрытый, Л...		ИР
☐	04.03.2025, 09:22:13		347	Обнаружен новый поток данных	Аномальная сетев...	Высокий	Новый		ИР
☐	04.03.2025, 09:22:13		346	Обнаружен новый поток данных	Аномальная сетев...	Высокий	Новый		ИР
☐	04.03.2025, 09:22:13		345	Обнаружен новый поток данных с у...	Аномальная сетев...	Высокий	Новый		ИР
☐	04.03.2025, 09:16:58		344	Обнаружен новый поток данных с у...	Аномальная сетев...	Высокий	Новый		ИР
☐	04.03.2025, 09:16:58		343	Обнаружен новый поток данных	Аномальная сетев...	Высокий	Новый		ИР
☐	04.03.2025, 09:16:38		342	Обнаружен новый поток данных	Аномальная сетев...	Высокий	Новый		ИР
☐	04.03.2025, 09:16:38		341	Обнаружен новый поток данных с у...	Аномальная сетев...	Высокий	Новый		ИР
☐	04.03.2025, 09:13:52		340	Обнаружен новый поток данных с у...	Аномальная сетев...	Высокий	Новый		ИР
☐	04.03.2025, 09:13:52		339	Обнаружен новый поток данных	Аномальная сетев...	Высокий	Новый		ИР
☐	04.03.2025, 09:13:03		338	Обнаружен новый поток данных с у...	Аномальная сетев...	Высокий	Новый		ИР
☐	04.03.2025, 09:13:02		337	Обнаружен новый поток данных	Аномальная сетев...	Высокий	Новый		ИР
☐	04.03.2025, 09:00:08		336	Обнаружен новый поток данных	Аномальная сетев...	Высокий	Новый		ИР
☐	04.03.2025, 09:00:07		335	Обнаружен новый поток данных с у...	Аномальная сетев...	Высокий	Новый		ИР
☐	04.03.2025, 08:50:49		334	Обнаружен новый акти...	Не определен	Критический	Новый		ИР
☐	04.03.2025, 08:48:01		333	Обнаружен новый поток данных с у...	Аномальная сетев...	Высокий	Новый		ИР
☐	04.03.2025, 08:48:01		332	Обнаружен новый поток данных	Аномальная сетев...	Высокий	Новый		ИР

Рис. 2. Страница «Инциденты»

3.4.1.1.3. События

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

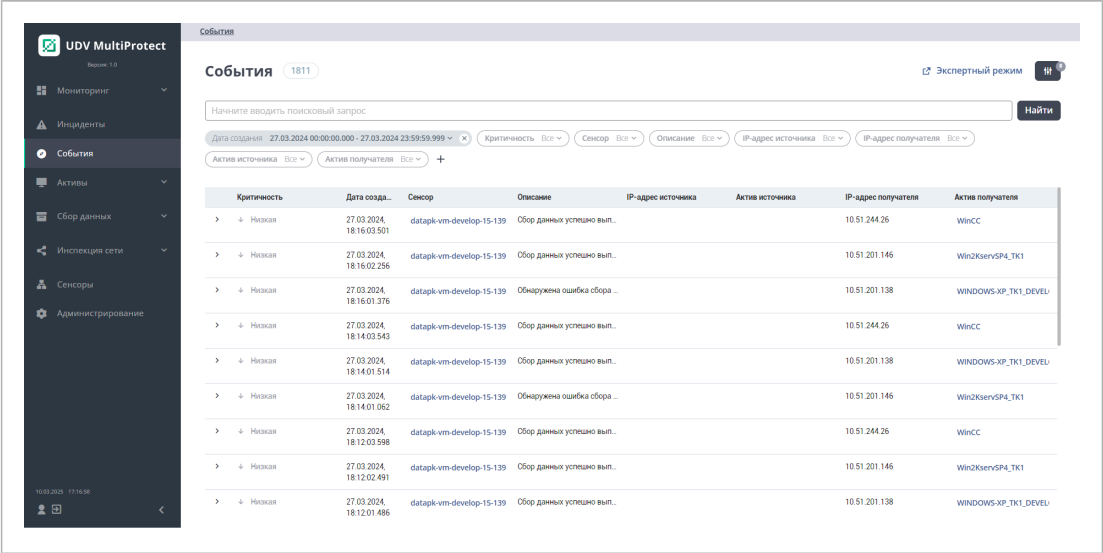


Рис. 3. Страница «События»

3.4.1.1.3.1. Экспертный режим

Страница для работы с событиями Комплекса в расширенном режиме.

Не является разделом основного интерфейса. Чтобы перейти в этот режим, на странице **События** нажмите **Экспертный режим**.

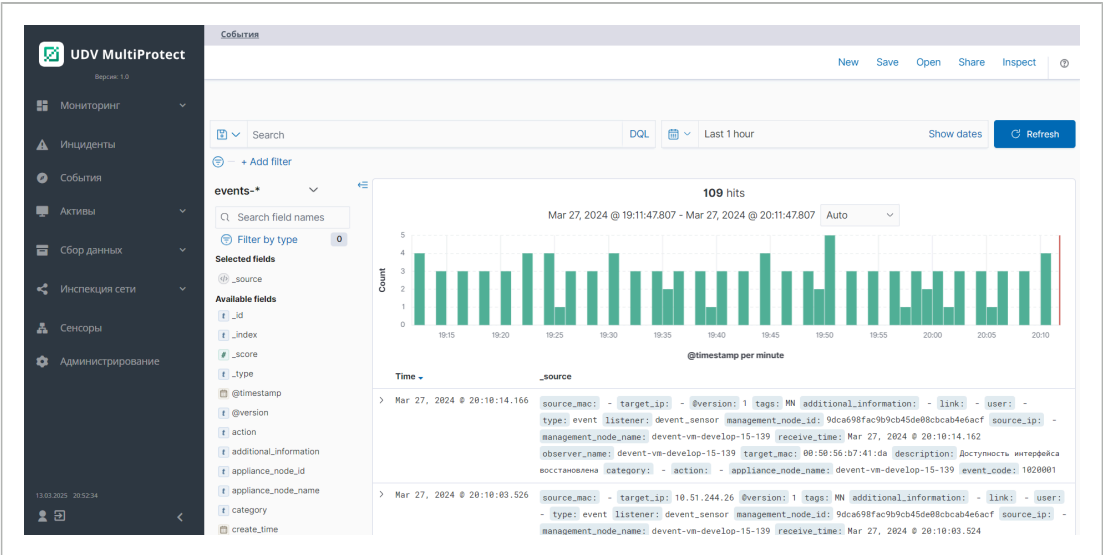


Рис. 4. Страница «Экспертный режим»

3.4.1.1.4. Активы

Пункт главного меню, включающий страницы [Активы → Технические средства](#), [Активы → Перечень ПО](#) и [Активы → Перечень ИС](#).

3.4.1.1.4.1. Активы → Технические средства

Подраздел, содержащий список всех найденных автоматически и добавленных пользователем активов. На странице присутствуют широкие возможности фильтрации и перехода к отдельным страницам различных аспектов активов (карточка актива, события, инциденты, учетные данные актива, конфигурации), кнопки экспорта, импорта, поиска уязвимостей, создания отчетов и удаления активов, столбцы статусов и статистики по сбору данных, отклонениям конфигураций, инцидентам, уязвимостям.

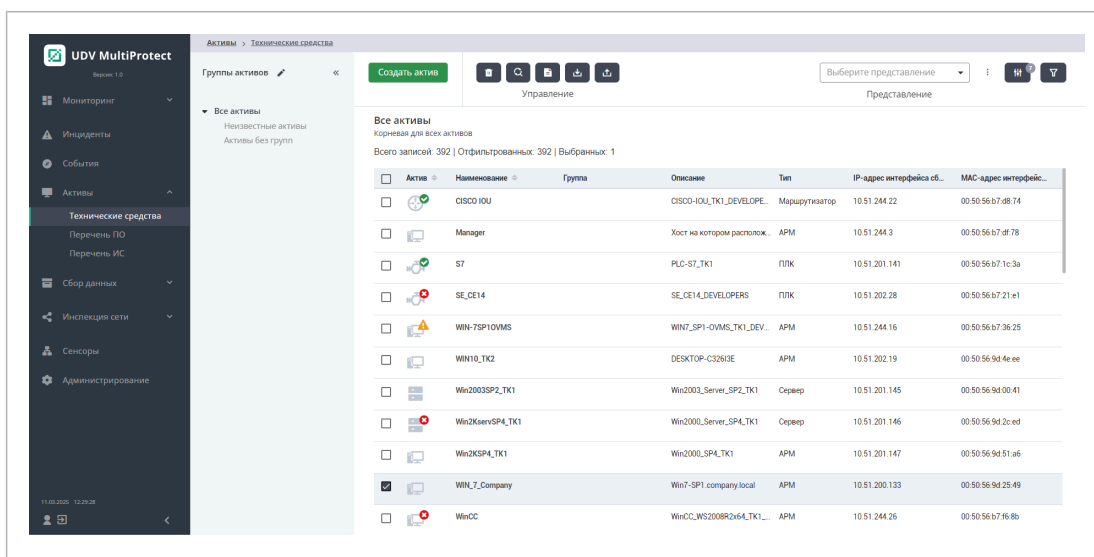


Рис. 5. Страница «Активы → Технические средства»

3.4.1.1.4.2. Активы → Перечень ПО

Подраздел, в котором можно просматривать и фильтровать список ПО, собранный сканерами, а также экспортировать отчет по результатам сопоставления ПО со справочником CVE.

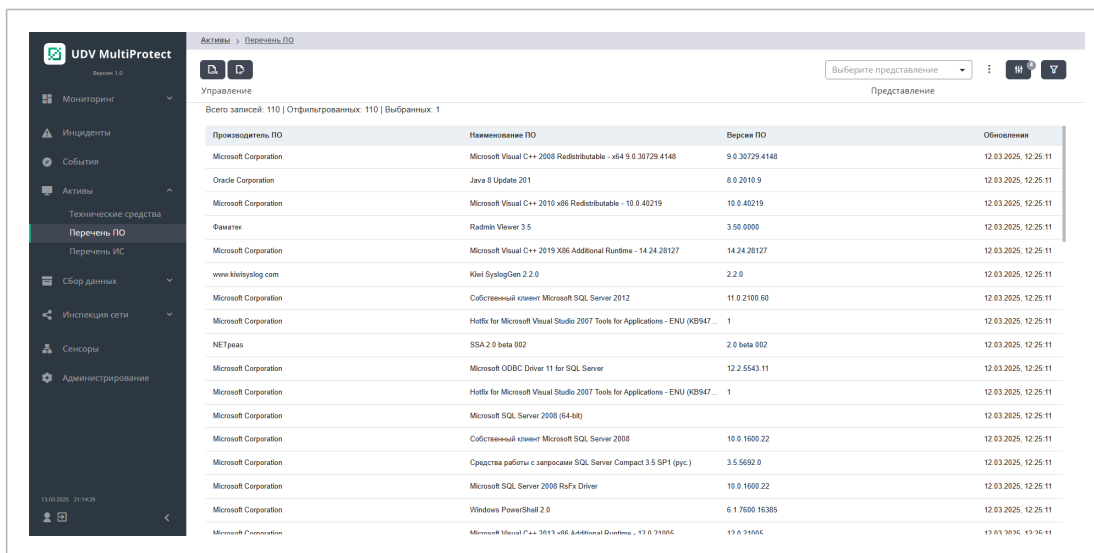


Рис. 6. Страница «Активы → Перечень ПО»

3.4.1.1.4.3. Активы → Перечень ИС

Подраздел, содержащий список всех ИС.

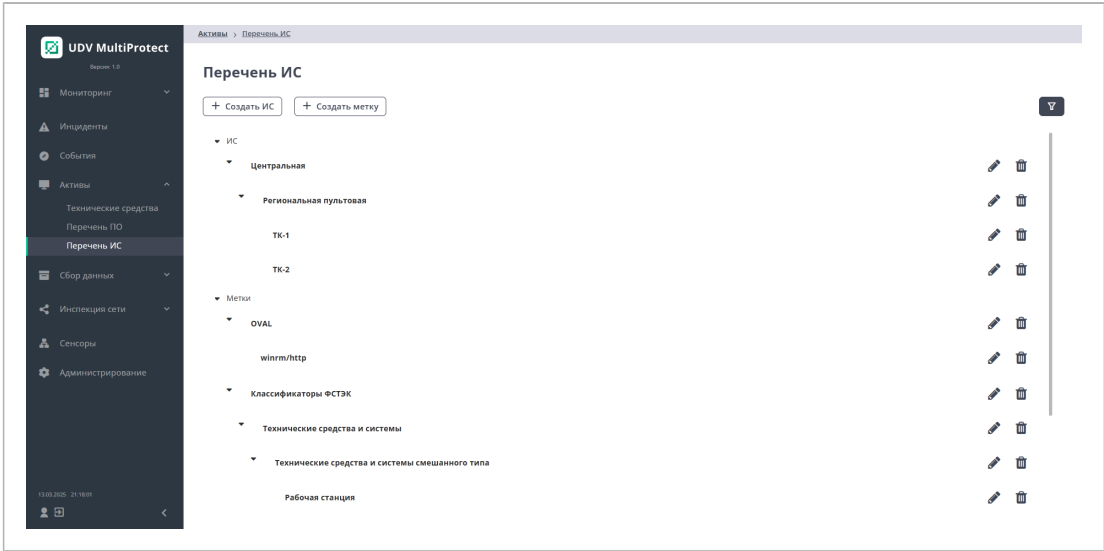


Рис. 7. Страница «Активы → Перечень ИС»

3.4.1.1.4.4. Карточка актива

Не является разделом основного интерфейса. Перейти в карточку можно со страниц **Активы**, **Потоки данных**, **Карта сети** при нажатии на значок или название актива. Доступен просмотр в отдельной вкладке. Содержание страницы различается в зависимости от актива, для которого открыта карточка.

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

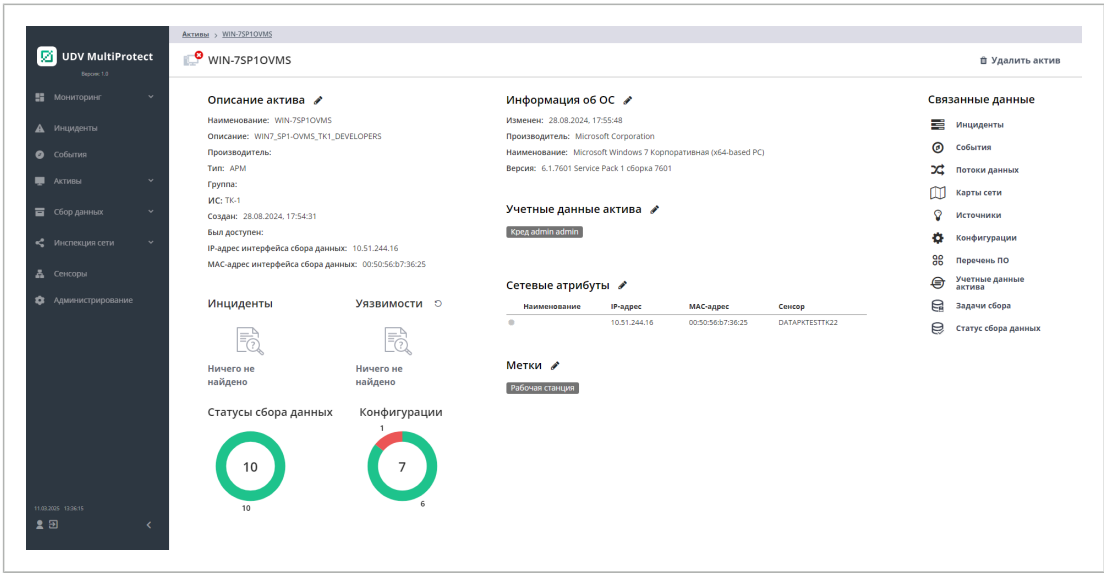


Рис. 8. Карточка актива

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

1. Описание актива. Содержит информацию о Комплексе, к которому относится актив, наименовании, описании, производителе, типе, группе, ИС, датах создания и появления, IP и MAC-адресах.
2. Виджеты для отображения состояния компонентов ИБ на активе:
 - a. Инциденты.
 - b. Уязвимости.
 - c. Статусы сбора данных.
 - d. Конфигурации.
3. Информация об операционной системе. Содержит дату и время последнего изменения указанных данных, производителя, наименование и версию Операционная система. Для актива с типом **Инженерное оборудование** содержит информацию о прошивке.
4. Учетные данные. Содержит список учетных данных, присвоенных активу.
5. Сетевые атрибуты. Содержит используемые IP и MAC-адреса, с которых происходит прослушивание трафика и сбора данных с актива, а также содержит информацию о сенсорах, чьим домашним сетям принадлежат IP-адреса сетевых атрибутов.
6. Метки. Содержит список присвоенных активу меток и кнопку  (**Редактировать**) для присвоения активу ранее созданных меток.
7. Связанные данные. Содержит ссылки на разделы, относящиеся к активу>.

3.4.1.1.5. Сбор данных

Пункт главного меню, включающий страницы **Задачи сбора**, **Статус сбора**, **Конфигурации** и **Результаты проверок**.

3.4.1.1.5.1. Задачи сбора

Подраздел, в котором можно создавать, редактировать, запускать и удалять задачи сбора данных.

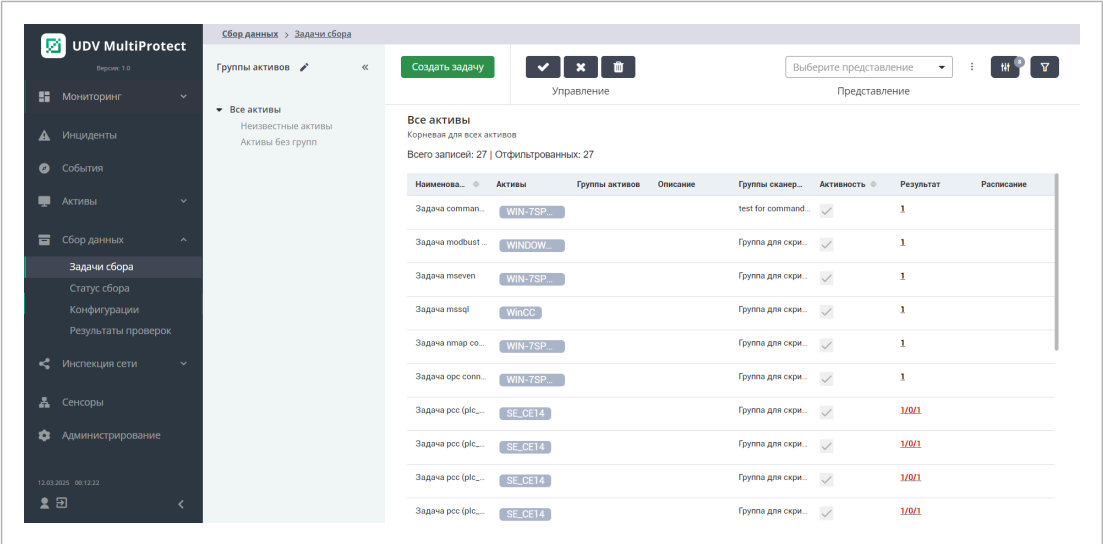


Рис. 9. Страница «Задачи сбора»

3.4.1.1.5.2. Статус сбора

Подраздел, в котором можно просматривать и удалять результаты, полученные при выполнении задач и сканеров.

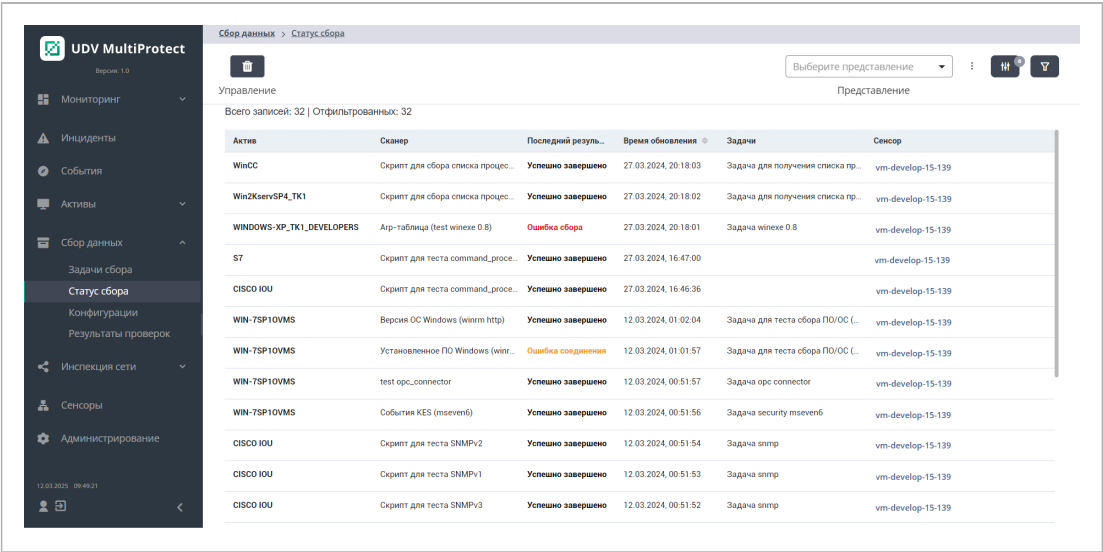


Рис. 10. Страница «Статус сбора»

3.4.1.1.5.3. Конфигурации

Подраздел, в котором можно просматривать последние собранные конфигурации со всех активов. Страница предоставляет широкие возможности по фильтрации собранных данных. При необходимости можно сформировать отчет.

Статус	Дата создания	Актив	Наименование
✓	28.10.2024, 14:26:03	WinCC	Скрипт для сбора списка процессов
✓	28.10.2024, 14:26:02	WinCCServerPL1	Скрипт для сбора списка процессов
✓	28.10.2024, 14:25:03	S7	test plc s7comm
✓	28.10.2024, 14:25:02	CISCO IOU	Скрипт для теста SNMPv2
✓	28.10.2024, 14:25:01	CISCO IOU	Скрипт для теста SNMPv1
✓	28.10.2024, 14:24:59	CISCO IOU	cisco-run-en-reg telnet
✓	28.10.2024, 14:24:58	CISCO IOU	test ssh
✓	28.10.2024, 14:24:53	WIN-7SP100MS	ports-smap
✓	28.10.2024, 14:24:50	WINDOWS-XP-TXT-DEVELOPERS	modbus_read_holding_reg
✓	28.10.2024, 14:24:47	WIN-7SP100MS	Atp-таблица (test winrm https rtm)
✓	28.10.2024, 14:24:46	WIN-7SP100MS	Atp-таблица (test winrm https basic)
✓	28.10.2024, 14:24:46	WIN-7SP100MS	Atp-таблица (test winrm http rtm)
✓	28.10.2024, 14:24:45	WIN-7SP100MS	Atp-таблица (test winrm http basic)
✓	28.10.2024, 14:24:45	WIN-7SP100MS	Скрипт для теста command_processor
✓	28.10.2024, 14:24:43	Windows 7 wsgp	Настройки безопасности тестов plc_allen_bradley
✓	28.10.2024, 14:24:43	Windows 7 wsgp	Настройки безопасности plc_allen_bradley

Рис. 11. Страница «Конфигурации»

3.4.1.1.5.3.1. Конфигурации актива

Не является разделом основного интерфейса. Перейти к конфигурациям актива можно двумя способами:

- со страницы **Конфигурации** по кнопке (**Просмотреть конфигурацию актива**) напротив выбранной конфигурации;
- из **карточки актива** по ссылке **Конфигурации** в разделе **Связанные данные**.

Содержание страницы различается в зависимости от актива, для которого открыта карточка. Основные блоки страницы конфигураций:

1. Меню со списком всех собранных когда-либо типов конфигураций в левой части страницы.
2. Управление конфигурациями в верхней части страницы:
 - выпадающий список со всеми собранными конфигурациями;
 - кнопка **Принять за эталонную**;
 - кнопка удаления конфигурации;
 - кнопка **Создать интерфейс**. Отображается для коммутаторов при сборе по протоколу SNMP.
3. Список собранных данных, доступных для просмотра и сравнению в виде:
 - таблицы;
 - строки под строкой;
 - двух экранов.

Если текущая конфигурация соответствует эталону, но в промежутке между эталонной и текущей обнаружены конфигурации, не соответствующие эталону, на страницу выводится предупреждение о том, что необходимо оценить легитимность таких изменений.

Конфигурация, не соответствующая эталону, отмечена значком 

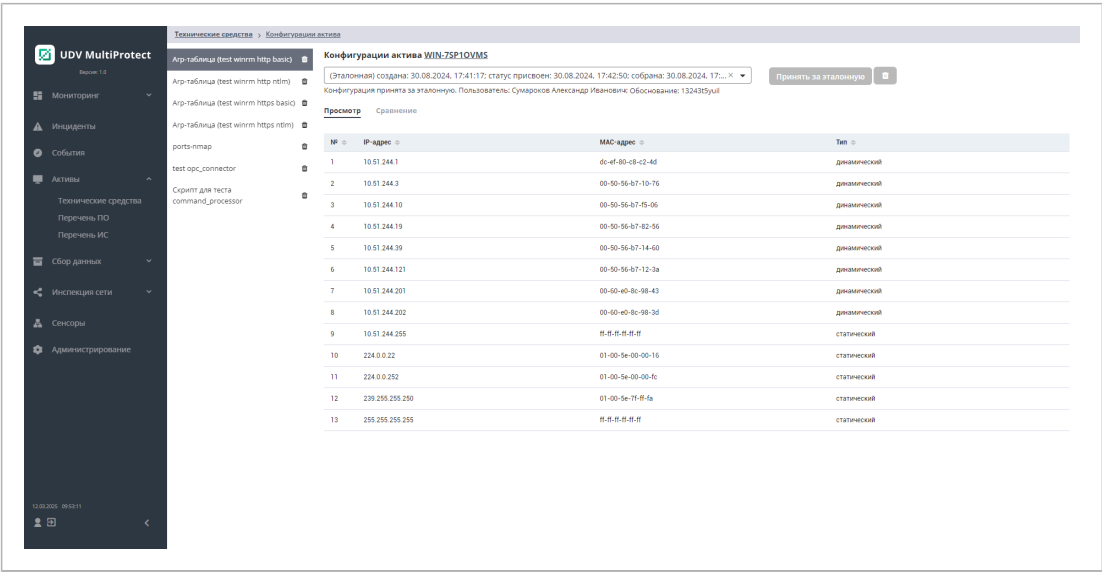


Рис. 12. Страница «Конфигурации актива»

3.4.1.1.5.4. Результаты проверок

Подраздел инспекции активов, где можно создавать, редактировать и удалять проверки на соответствие требованиям ИБ. После получения результата имеются возможности просмотреть и сохранить результат отдельной проверки, перезапустить проверку, сохранить отчет по результатам проверок на странице.

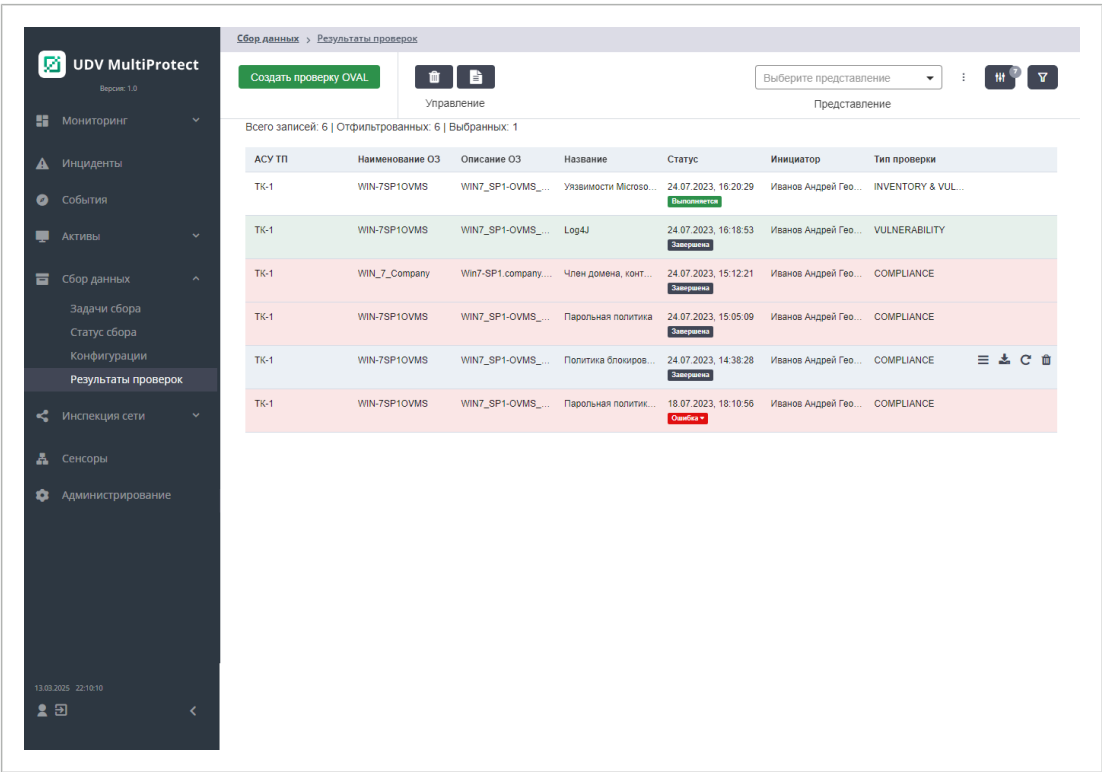


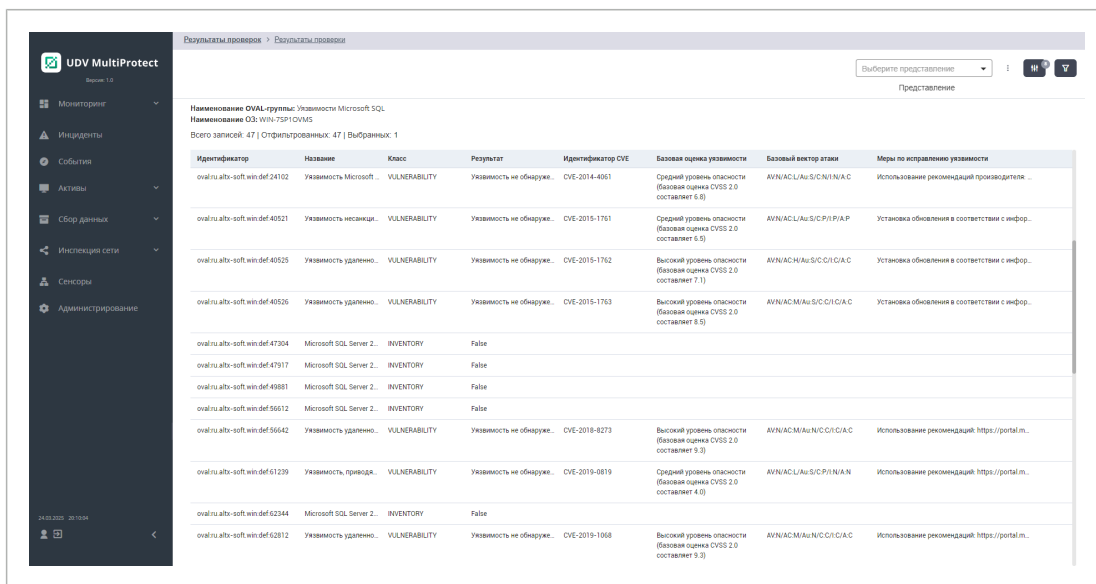
Рис. 13. Страница «Результаты проверок»

3.4.1.1.5.4.1. Результаты проверки

Не является разделом основного интерфейса. Перейти к подробным результатам проверки актива на соответствие требованиям ИБ можно со страницы по кнопке  (**Просмотреть результаты**) напротив успешно выполненной проверки.

Страница содержит таблицу с подробной информацией об отдельных критериях проверки соответствия, которые сформировали итоговый результат проверки. Содержание страницы различается в зависимости от актива и набора критериев проверки.

Для критериев наличия уязвимости (с классом **VULNERABILITY**) в колонке **Меры по исправлению уязвимостей** приводятся рекомендации по устранению как для обнаруженных, так и не обнаруженных уязвимостей.



Идентификатор	Название	Класс	Результат	Идентификатор CVE	Базовая оценка уязвимости	Базовый вектор атаки	Меры по исправлению уязвимости
oval/rn-altx-soft-win-def:24102	Уязвимость Microsoft...	VULNERABILITY	Уязвимость не обнаружена	CVE-2014-4061	Средний уровень опасности (Базовая оценка CVSS 2.0 составляет 6.8)	AVN/AC/L/Au/S/CN/1/N/A/C	Использование рекомендаций производителя...
oval/rn-altx-soft-win-def:40521	Уязвимость мессенджера...	VULNERABILITY	Уязвимость не обнаружена	CVE-2015-1761	Средний уровень опасности (Базовая оценка CVSS 2.0 составляет 6.5)	AVN/AC/L/Au/S/C/P/I/A/P	Установка обновления в соответствии с инфор...
oval/rn-altx-soft-win-def:40525	Уязвимость удаленно...	VULNERABILITY	Уязвимость не обнаружена	CVE-2015-1762	Высокий уровень опасности (Базовая оценка CVSS 2.0 составляет 7.1)	AVN/AC/H/Au/S/C/C/I/A/C	Установка обновления в соответствии с инфор...
oval/rn-altx-soft-win-def:40536	Уязвимость удаленно...	VULNERABILITY	Уязвимость не обнаружена	CVE-2015-1763	Высокий уровень опасности (Базовая оценка CVSS 2.0 составляет 6.5)	AVN/AC/M/Au/S/C/C/I/A/C	Установка обновления в соответствии с инфор...
oval/rn-altx-soft-win-def:47304	Microsoft SQL Server 2...	INVENTORY	False				
oval/rn-altx-soft-win-def:47917	Microsoft SQL Server 2...	INVENTORY	False				
oval/rn-altx-soft-win-def:49881	Microsoft SQL Server 2...	INVENTORY	False				
oval/rn-altx-soft-win-def:56612	Microsoft SQL Server 2...	INVENTORY	False				
oval/rn-altx-soft-win-def:56642	Уязвимость удаленно...	VULNERABILITY	Уязвимость не обнаружена	CVE-2018-8273	Высокий уровень опасности (Базовая оценка CVSS 2.0 составляет 9.3)	AVN/AC/M/Au/N/C/C/I/A/C	Использование рекомендаций: https://portal.m...
oval/rn-altx-soft-win-def:61239	Уязвимость привода...	VULNERABILITY	Уязвимость не обнаружена	CVE-2019-0819	Средний уровень опасности (Базовая оценка CVSS 2.0 составляет 4.9)	AVN/AC/L/Au/S/C/P/I/N/A/N	Использование рекомендаций: https://portal.m...
oval/rn-altx-soft-win-def:62344	Microsoft SQL Server 2...	INVENTORY	False				
oval/rn-altx-soft-win-def:62812	Уязвимость удаленно...	VULNERABILITY	Уязвимость не обнаружена	CVE-2019-1068	Высокий уровень опасности (Базовая оценка CVSS 2.0 составляет 9.3)	AVN/AC/M/Au/N/C/C/I/A/C	Использование рекомендаций: https://portal.m...

Рис. 14. Страница «Результаты проверки»

3.4.1.1.6.3. Правила потоков

Подраздел настроек потоков данных, где можно просматривать, создавать, редактировать правила автоматической обработки потоков данных, а также можно переходить к потокам, которые попали под правило.

Для просмотра подробной информации о правиле потоков нажать кнопку  или  (Просмотр правила) в строке с правилом.

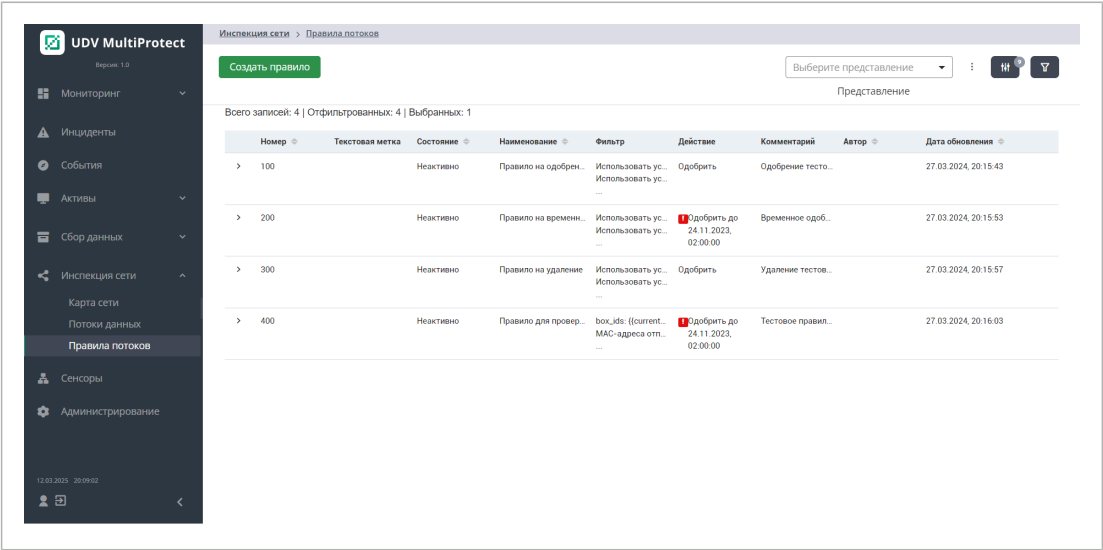


Рис. 17. Страница «Правила потоков»

3.4.1.1.7. Сенсоры

Пункт главного меню Комплекса, содержащий список всех подключенных сенсоров.

Для каждого сенсора можно задавать основные сведения, просматривать статусы и графики активности, запускать сканирование сети, настраивать домашние сети, включать службу обнаружения вторжений, удалять сенсор и его данные из Комплекса.

На странице отображается следующая информация о сенсорах:

- **Статус**
- **Наименование сенсора**
- **Описание сенсора**
- **Домашняя сеть**
- **Эксплуатирующая организация**
- **Место установки**
- **Был доступен** — время последней успешной проверки доступности сенсора.

Статус	Наименование	Описание	Домашняя сеть	Эксплуатирующая организация	Место установки	Был доступен
✓	ip-vm-staging-244-47	Автоматически добавленный сенсор	10.51.244.0/24 10.51.15.0/24 10.51.53.0/24	ООО «ИТ.Р»	Складово	13.03.2025, 22:10:45

Рис. 18. Страница «Сенсоры»

3.4.1.1.8. Администрирование

Раздел главного меню, который содержит страницы, связанные с настройкой различных аспектов работы Комплекса:

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

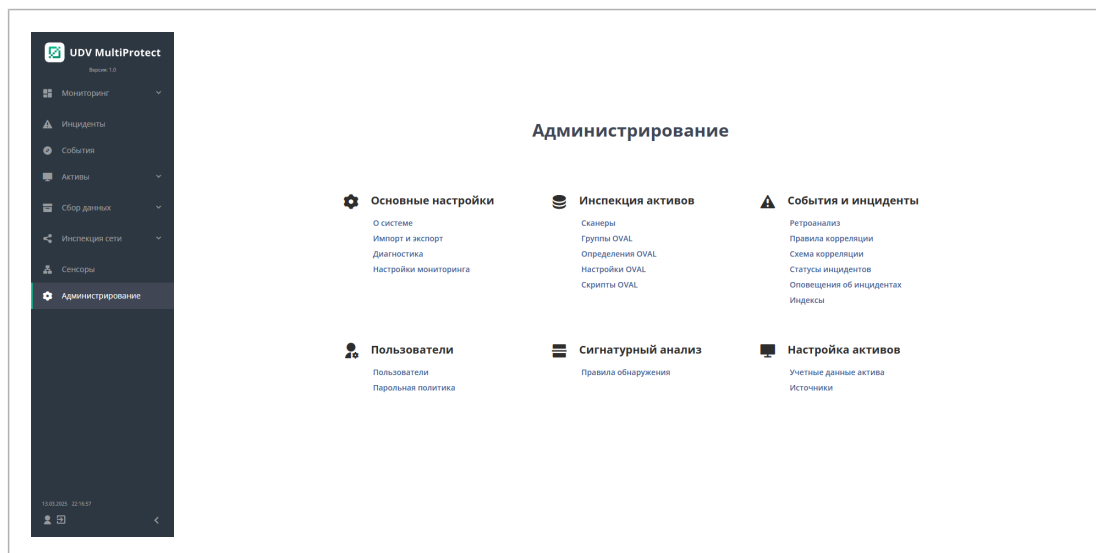


Рис. 19. Страница «Администрирование»

3.4.1.1.8.1. Основные настройки

3.4.1.1.8.1.1. О системе

Подраздел управления Комплексом, где можно задавать основные сведения о расположении Комплекса, эксплуатирующей организации, а также его описание. В правой части страницы указан производитель Комплекса и его версия.

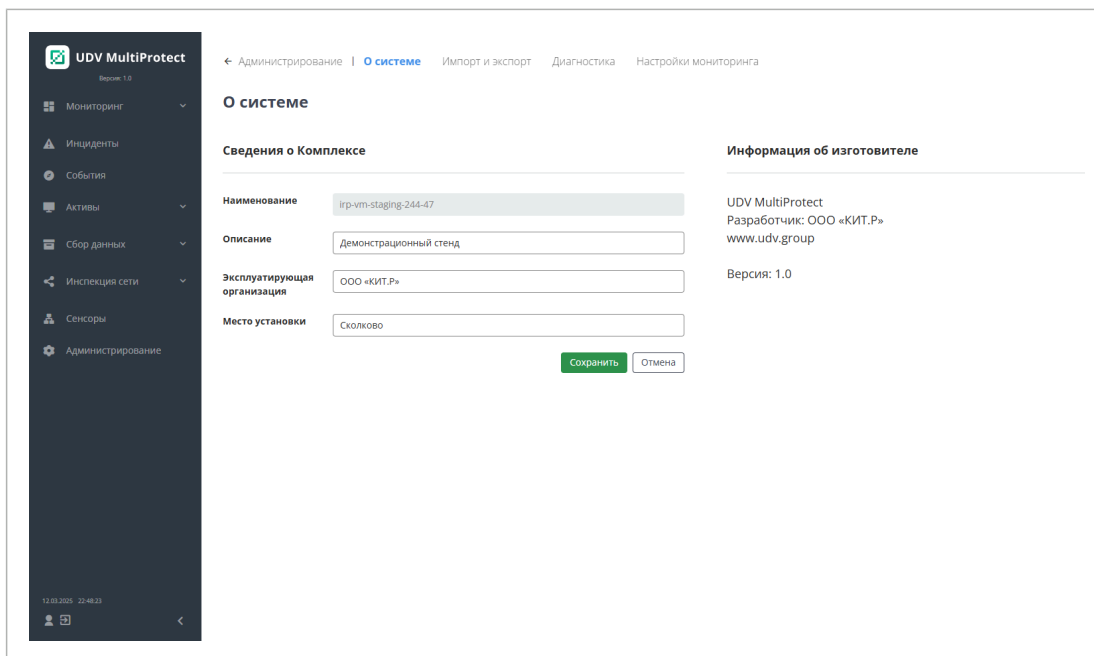


Рис. 20. Страница «О системе»

3.4.1.1.8.1.2. Импорт и экспорт

Страница, где можно экспортировать и импортировать справочники.



Подсказка:

Доступен импорт справочников размером до 145 МБ.

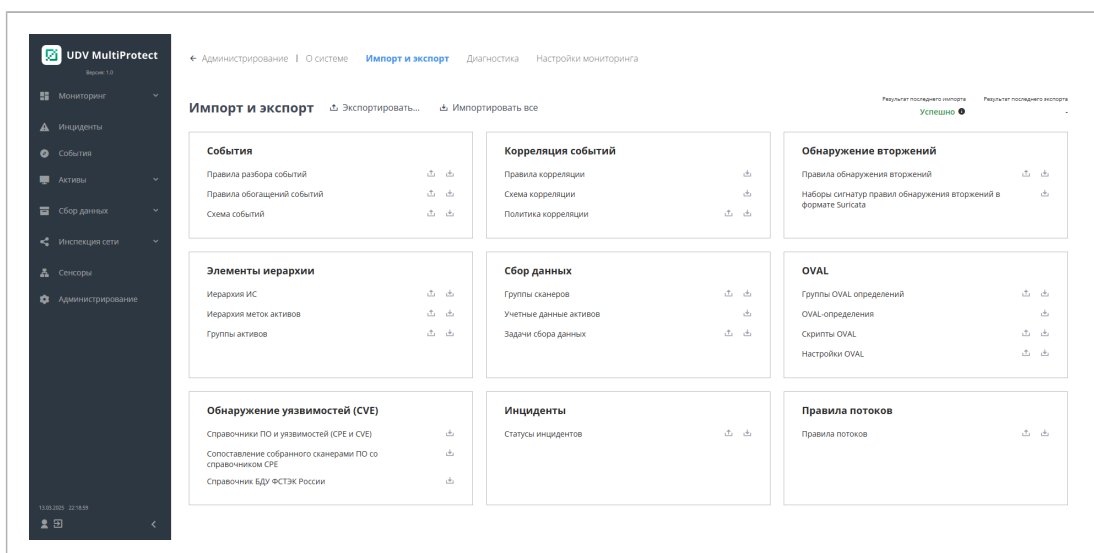


Рис. 21. Страница «Импорт и экспорт»

3.4.1.1.8.1.3. Диагностика

Подраздел управления Комплексом, где можно просматривать графики нагрузки на различные компоненты системы, на которой установлен текущий Комплекс. Для выбора доступны периоды 1 час, 24 часа и 7 дней.

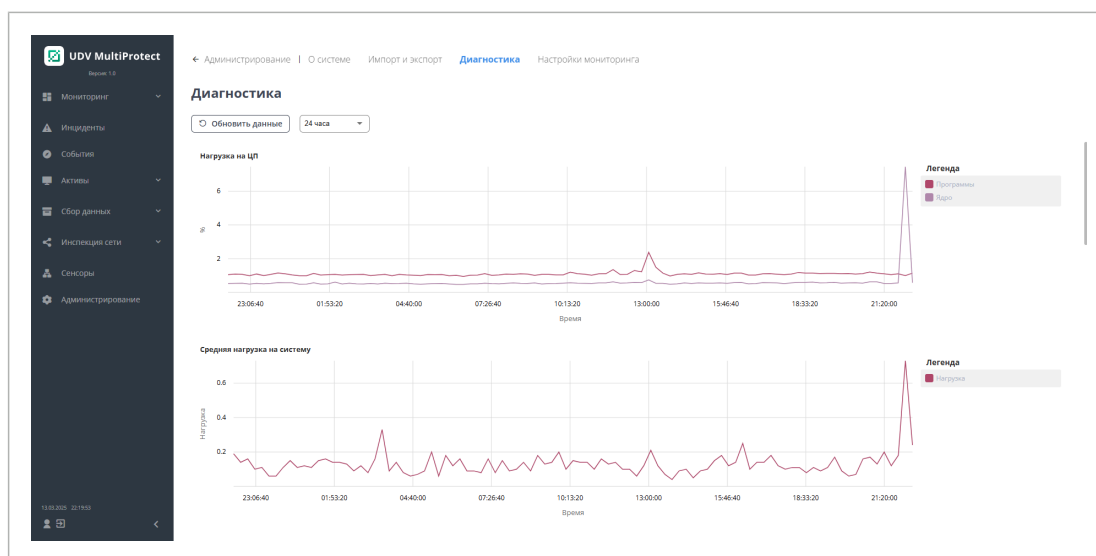


Рис. 22. Страница «Диагностика»

3.4.1.1.8.1.4. Настройки мониторинга

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

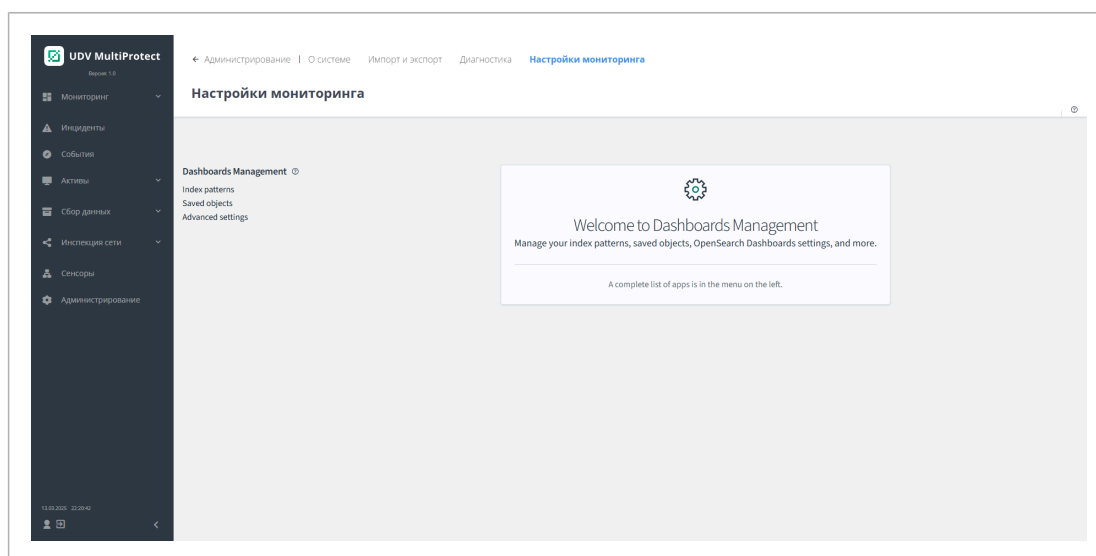


Рис. 23. Страница «Настройки мониторинга»

3.4.1.1.8.2. Инспекция активов

Пункт меню страницы **Администрирование**.

3.4.1.1.8.2.1. Сканеры

Подраздел настроек конфигураций, где можно создавать, редактировать, запускать и удалять сканеры сбора данных.

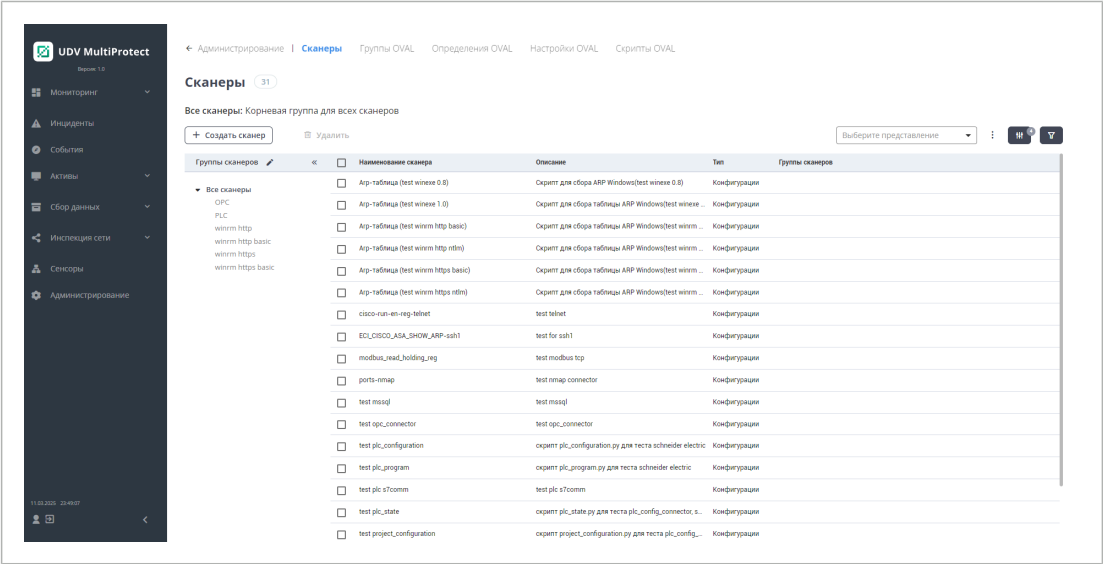


Рис. 24. Страница «Сканеры»

3.4.1.1.8.2.2. Группы OVAL

Подраздел настроек проверок и отчетов, где можно создавать, редактировать и удалять группы OVAL-определений.

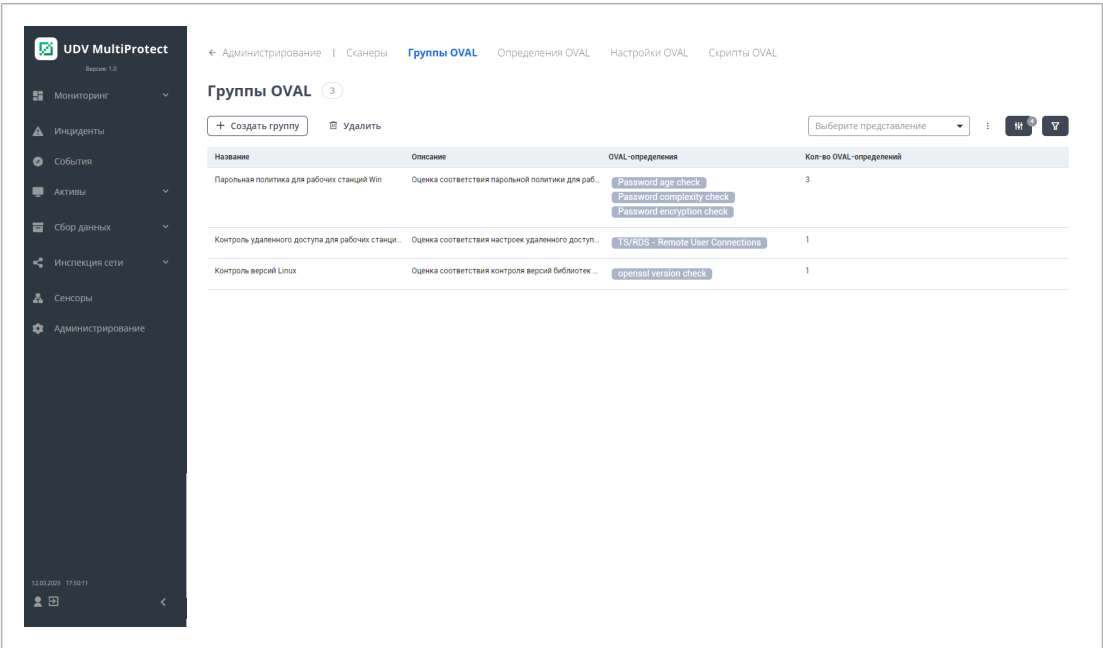


Рис. 25. Страница «Группы OVAL-определений»

3.4.1.1.8.2.3. Определения OVAL

Страница, где можно добавлять в группы, исключать из групп и удалять Open Vulnerability and Assessment Language-определения.

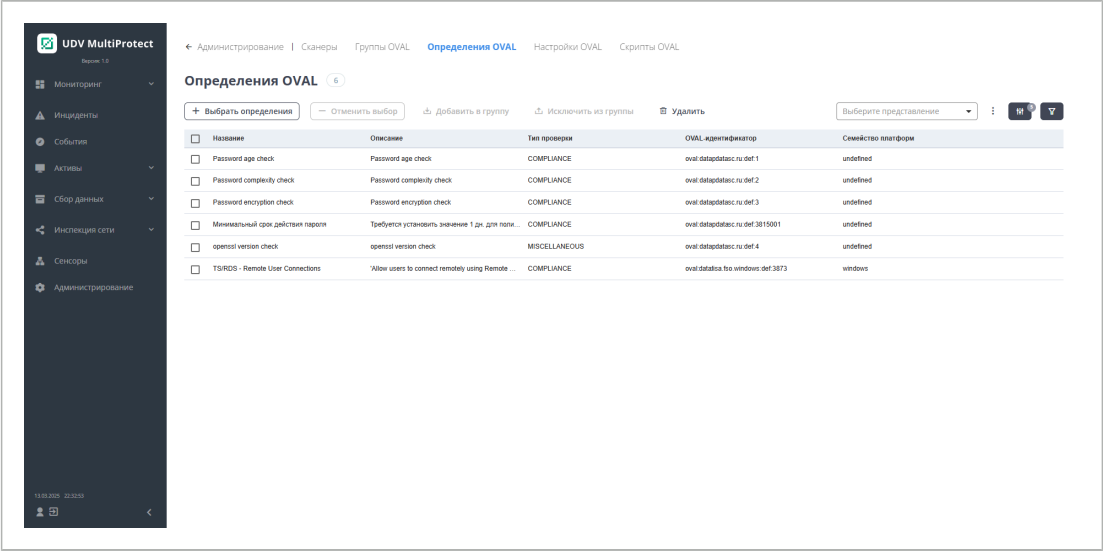


Рис. 26. Страница «Определения OVAL»

3.4.1.1.8.2.4. Настройки OVAL

Подраздел настроек проверок и отчетов, в котором можно создавать, редактировать и удалять настройки скриптов OVAL по отношению к активам и меткам.

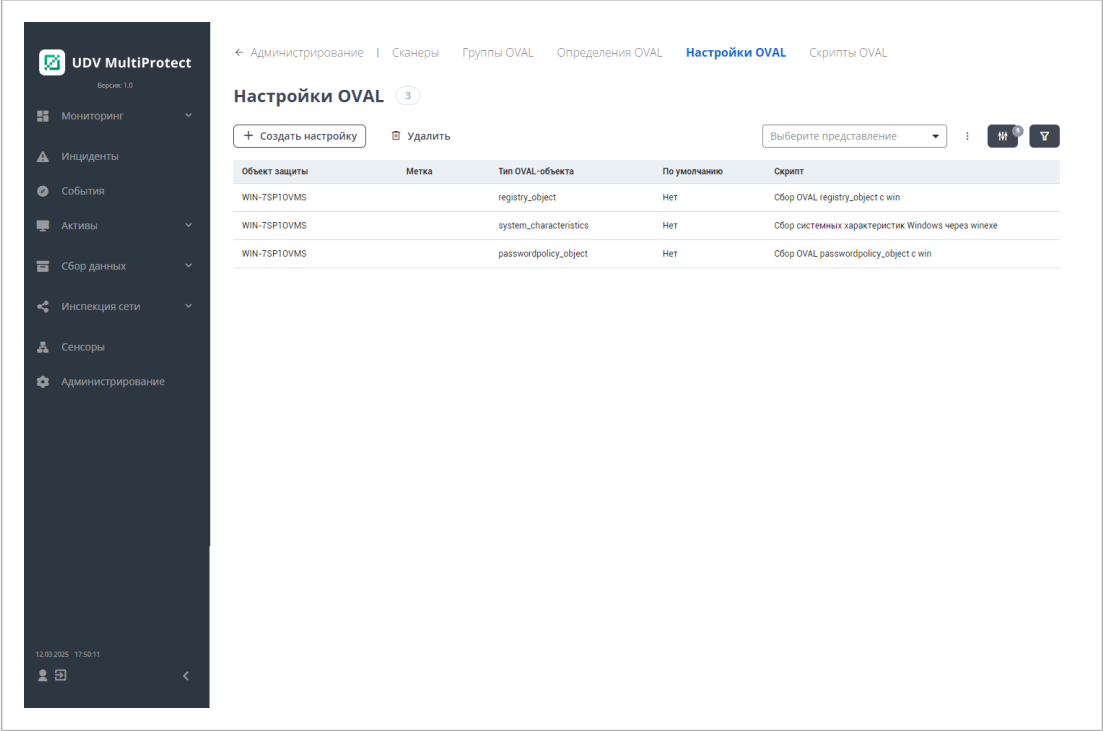


Рис. 27. Страница «Настройки OVAL»

3.4.1.1.8.2.5. Скрипты OVAL

Подраздел настроек проверок и отчетов, где можно создавать, редактировать и удалять скрипты сбора проверок на соответствие требованиям ИБ.

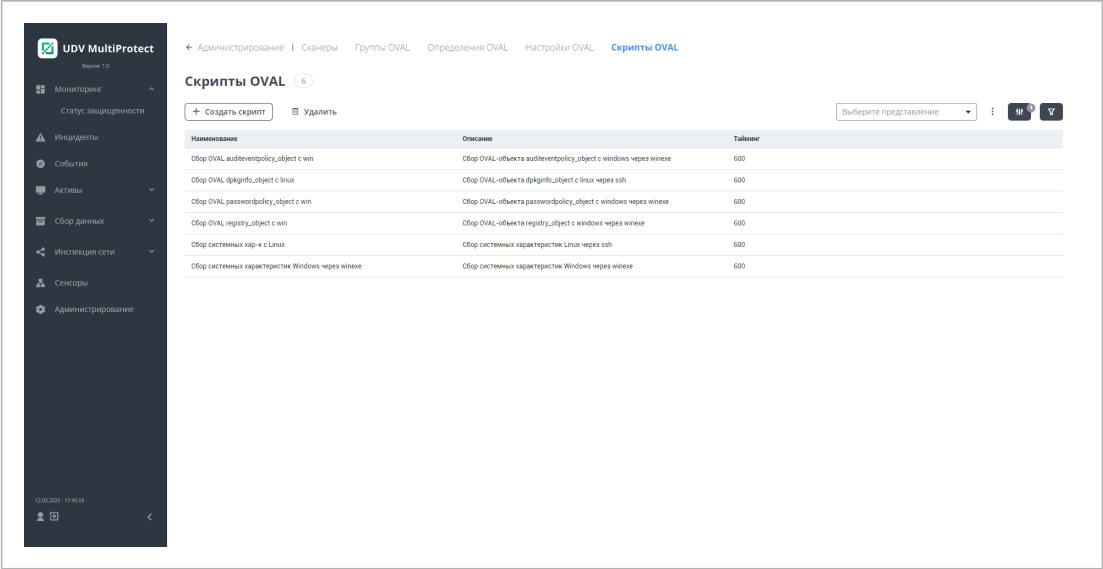


Рис. 28. Страница «Скрипты»

3.4.1.1.8.3. События и инциденты

Пункт главного меню, содержащий подразделы **События и инциденты** и **Ретроанализ**.

3.4.1.1.8.3.1. Ретроанализ

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

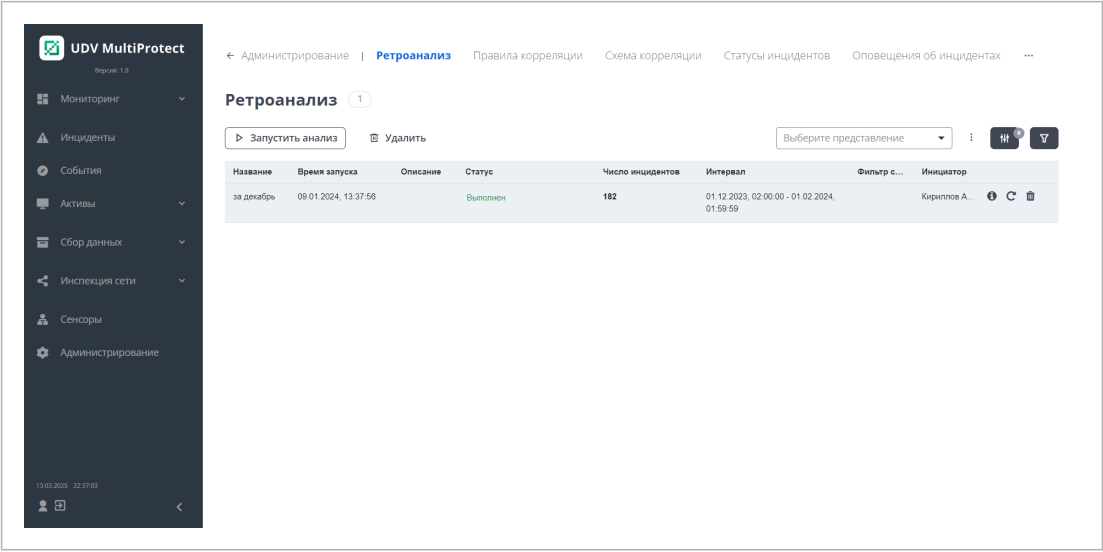


Рис. 29. Страница «Ретроанализ»

3.4.1.1.8.3.2. Правила корреляции

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

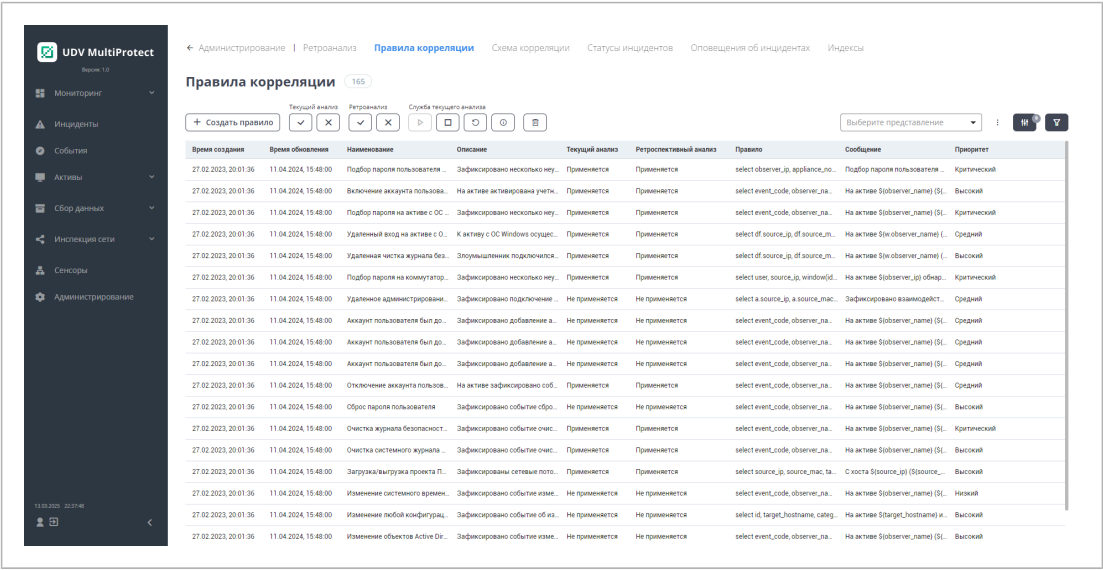


Рис. 30. Страница «Правила корреляции»

3.4.1.1.8.3.3. Схема корреляции

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

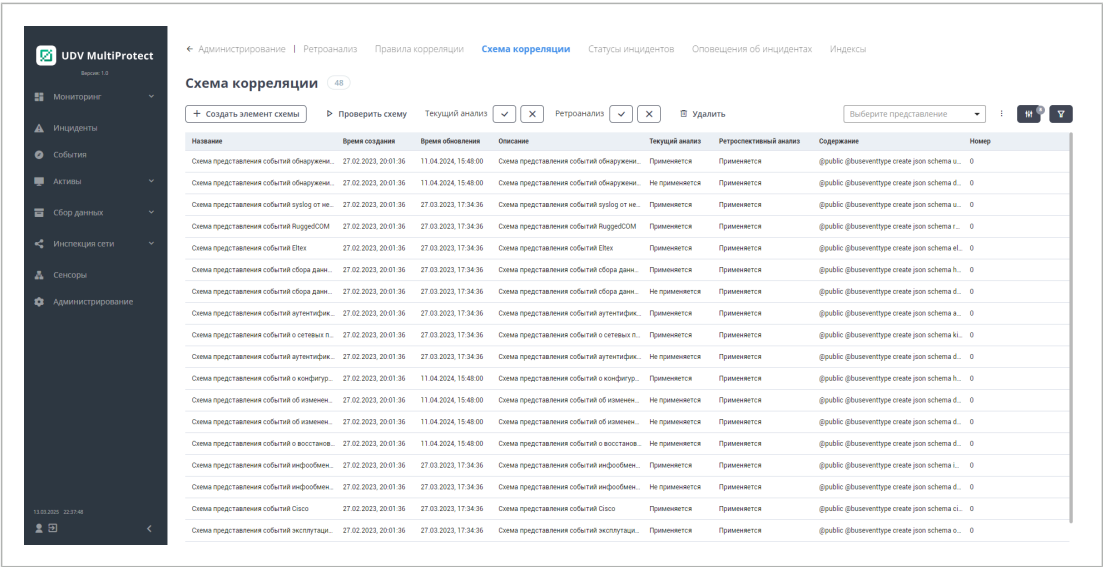


Рис. 31. Страница «Схема корреляции»

3.4.1.1.8.3.4. Статусы инцидентов

Подраздел настроек инцидентов, содержащий статусы, которые оператор может присвоить инцидентам.

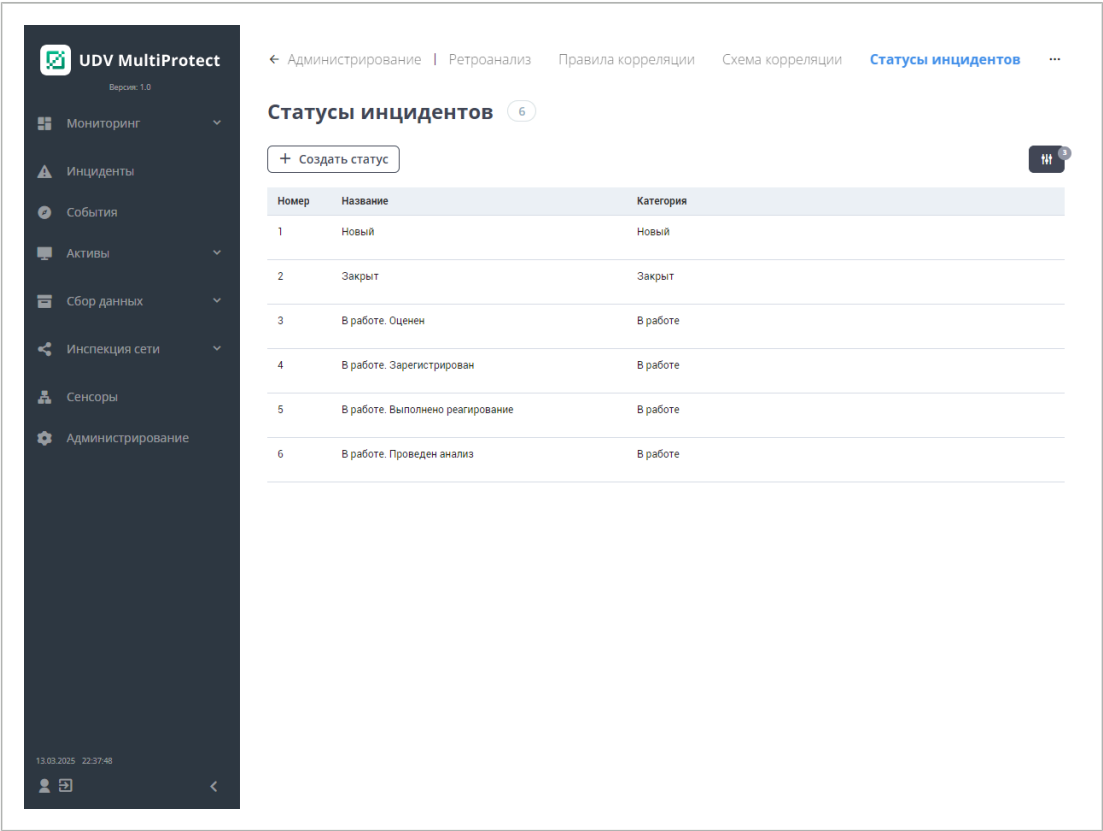


Рис. 32. Страница «Статусы инцидентов»

3.4.1.1.8.3.5. Оповещения об инцидентах

Подраздел настроек инцидентов, в котором можно создавать, редактировать, удалять оповещения об инцидентах.

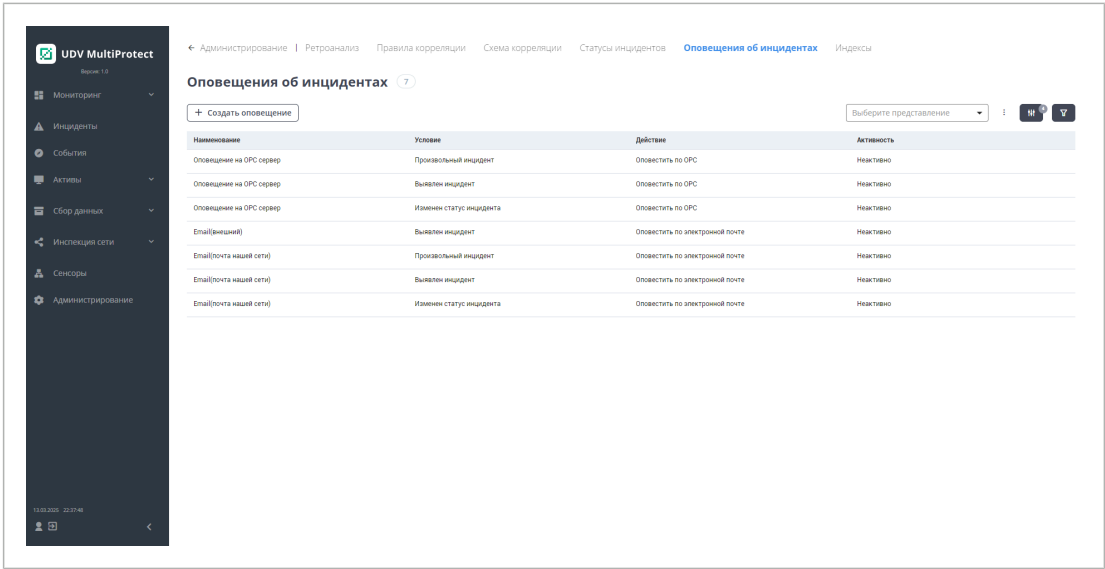


Рис. 33. Страница «Оповещения об инцидентах»

3.4.1.1.8.3.6. Индексы

Подраздел настроек мониторинга, в котором можно восстанавливать, архивировать и удалять индексы событий.

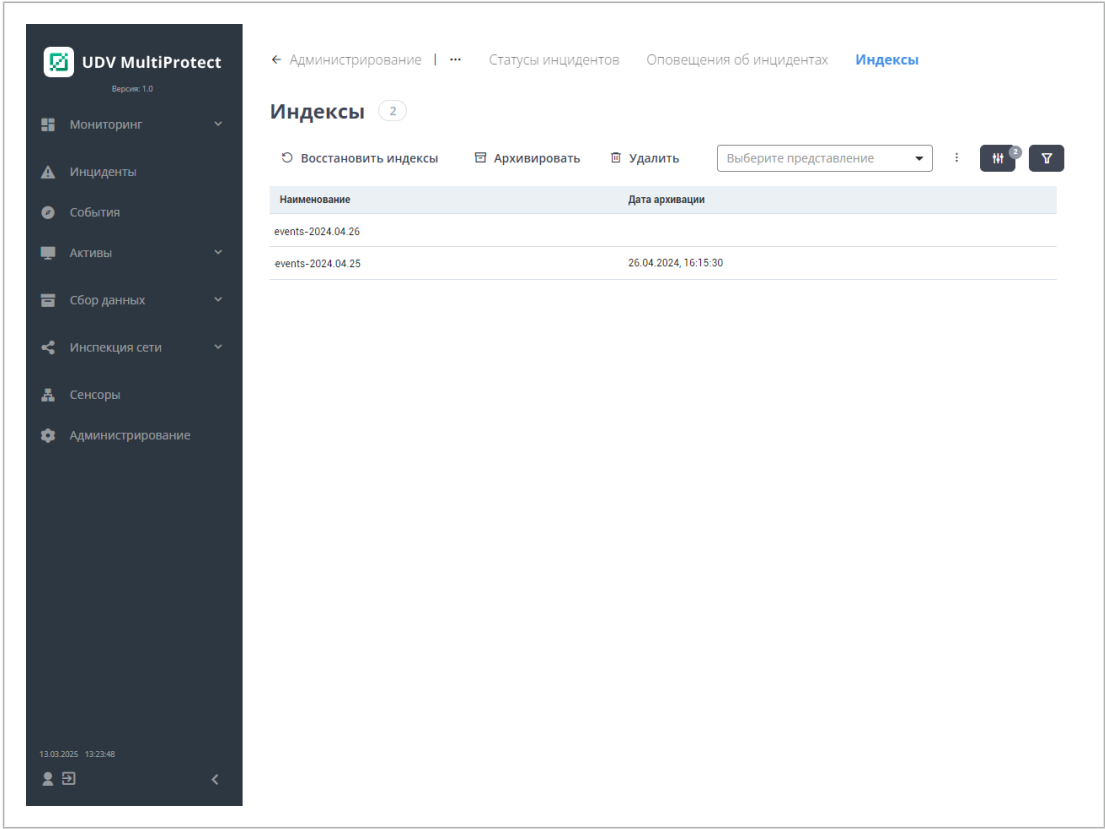


Рис. 34. Страница «Индексы»

3.4.1.1.8.4. Пользователи

Пункт меню подраздела Пользователи, содержащий страницу Парольная политика.

3.4.1.1.8.4.1. Пользователи

Подраздел управления Комплексом, где можно создавать, редактировать, блокировать и разблокировать, удалять пользователей.

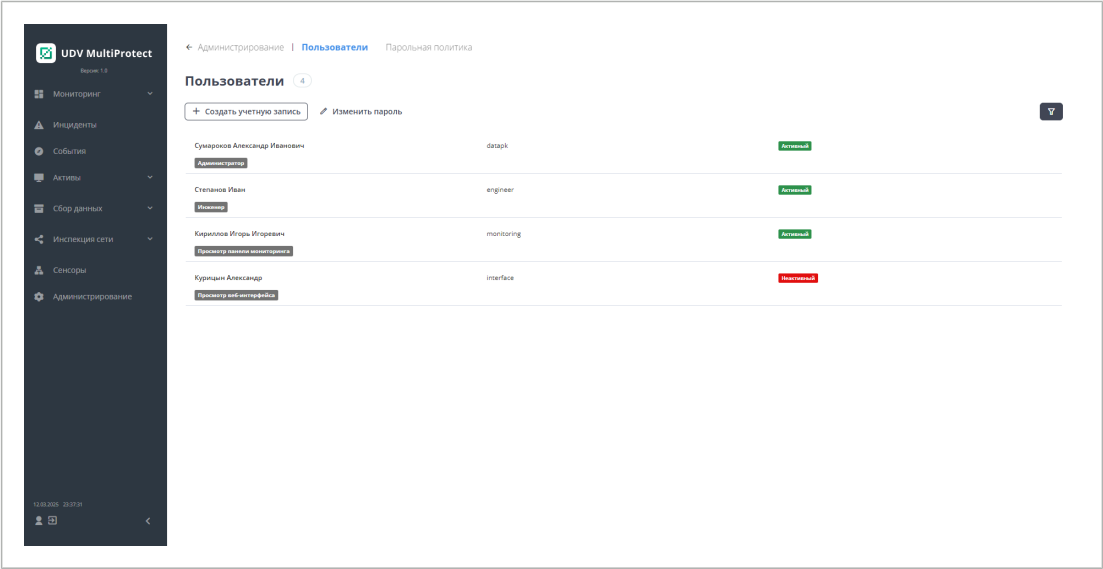


Рис. 35. Страница «Пользователи»

3.4.1.1.8.4.2. Парольная политика

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

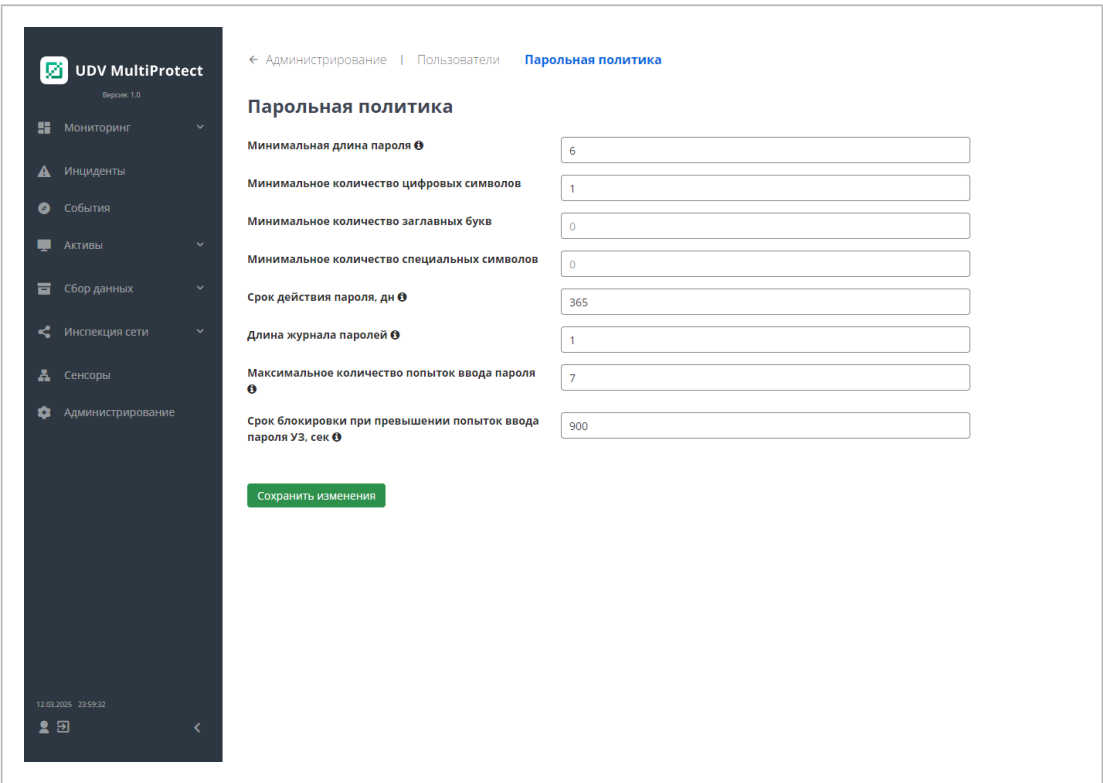


Рис. 36. Страница «Парольная политика»

3.4.1.1.8.5. Сигнатурный анализ

3.4.1.1.8.5.1. Правила обнаружения

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

- **Правила;**
- **Исключения.**

3.4.1.1.8.5.1.1. Правила

Подраздел инспекции сети, в котором можно управлять службой обнаружения вторжений, создавать, редактировать, активировать и деактивировать правила обнаружения вторжений.

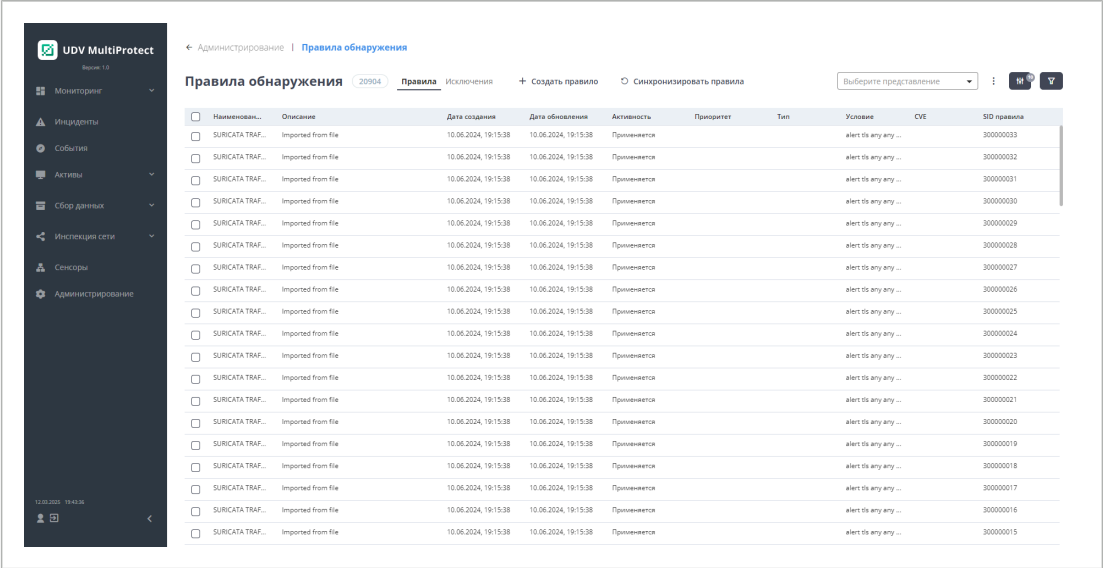


Рис. 37. Вкладка «Правила» на странице «Правила обнаружения»

3.4.1.1.8.5.1.2. Исключения

Подраздел инспекции сети, в котором можно создавать, редактировать и удалять исключения для правил обнаружения вторжений.

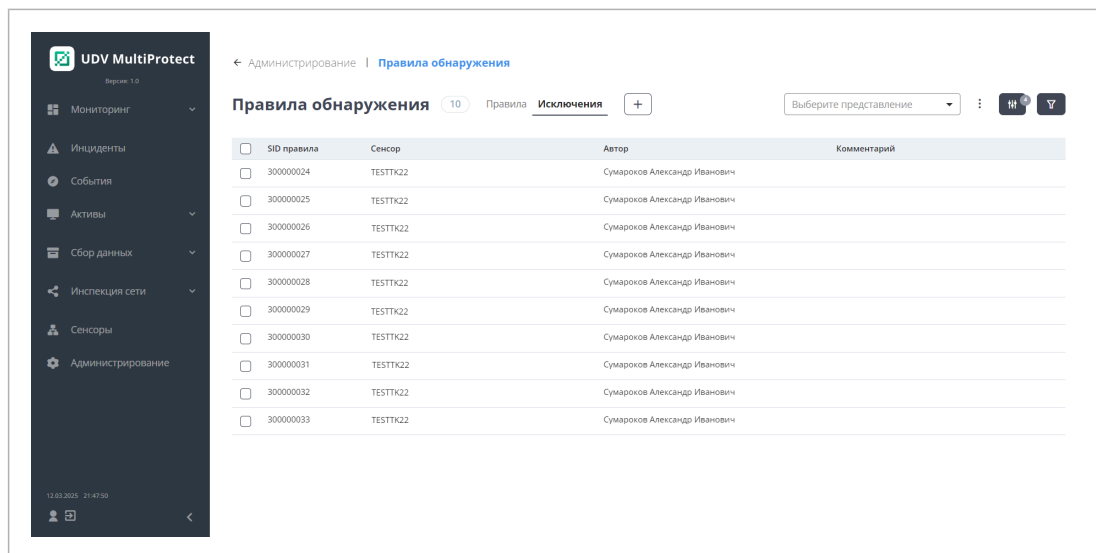


Рис. 38. Вкладка «Исключения» на странице «Правила обнаружения»

3.4.1.1.8.6. Настройка активов

Пункт меню раздела Администрирование, содержащий страницы Перечень ИС, Учетные данные актива и Источники.

3.4.1.1.8.6.1. Учетные данные актива

Подраздел настроек активов, где можно просмотреть, добавить, отредактировать учетные данные для сбора событий и конфигураций с активов. Пароль просмотреть нельзя.

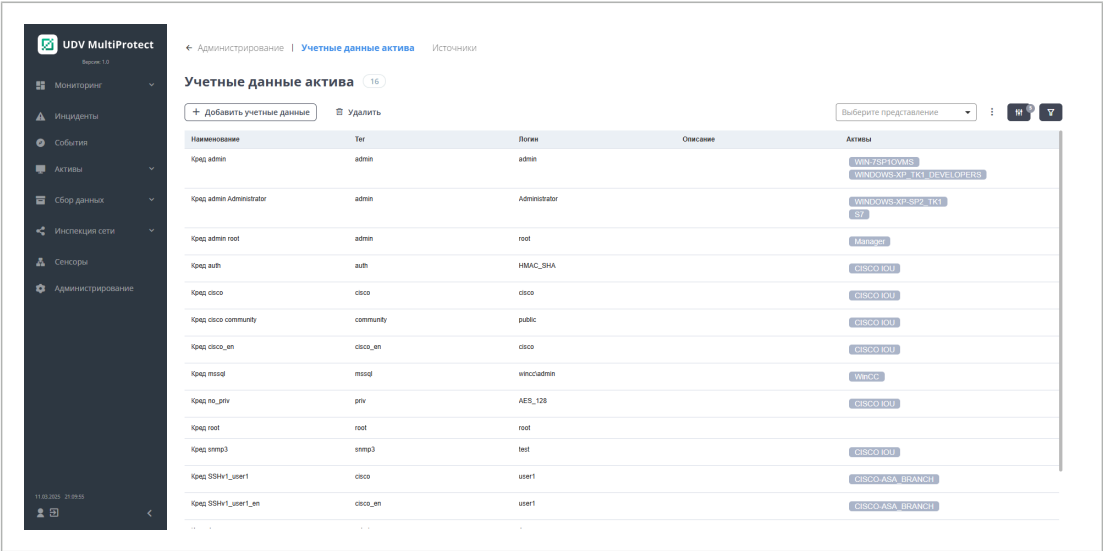


Рис. 39. Страница «Учетные данные актива»

3.4.1.1.8.6.2. Перечень ИС

Подраздел настроек активов, где можно создавать, редактировать и удалять классификаторы типов **Метки** и **АСУ ТП**.

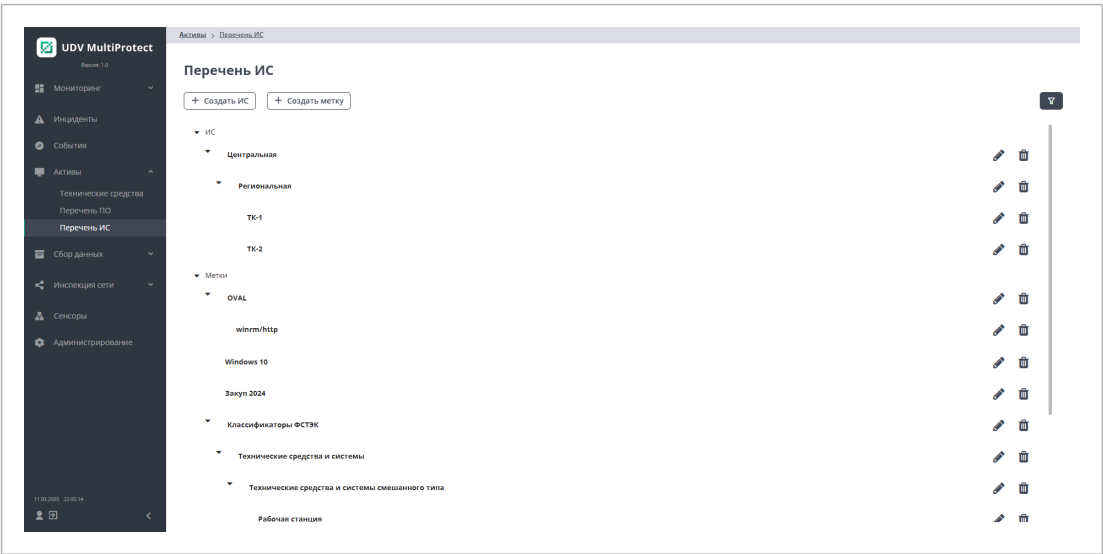


Рис. 40. Страница «Классификаторы»

3.4.1.1.8.6.3. Источники

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

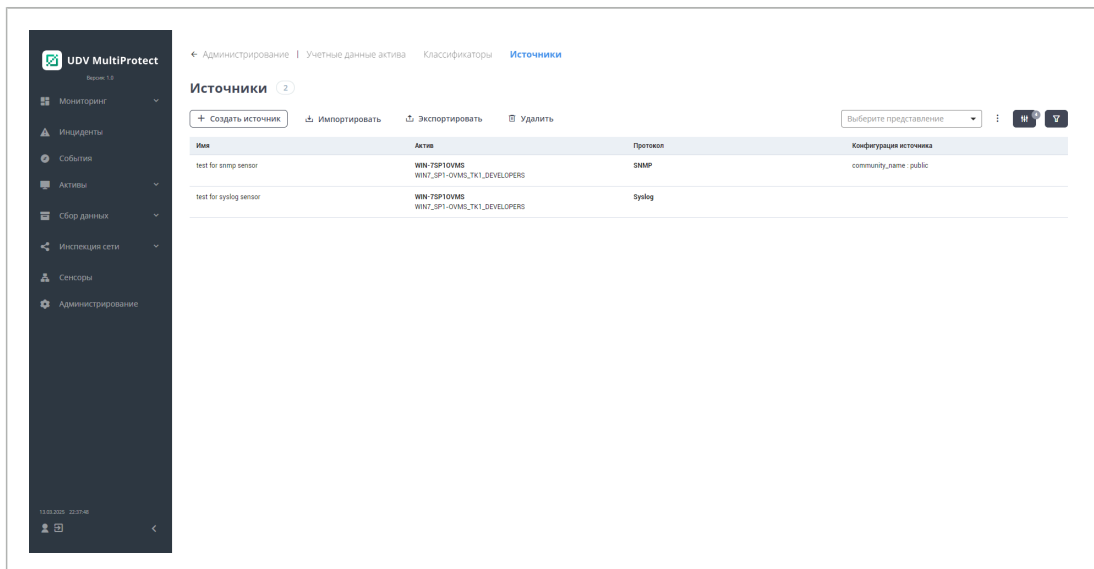


Рис. 41. Страница «Источники»

3.4.1.1.9. Страница «Страница не найдена»

Страница, которая автоматически открывается при переходе по ссылке на несуществующую страницу веб-интерфейса Комплекса. Страница также содержит ссылку для перехода на страницу **Статус защищенности**.



Рис. 42. Страница «Страница не найдена»

3.4.1.2. Цветовая индикация и виды уведомлений

В этом разделе вы можете ознакомиться со всеми видами цветовых индикаций и уведомлений, которые могут встретиться в веб-интерфейсе Комплекса:

- Цветовая индикация активов
- Статусы активов
- Статусы групповых операций
- Индикация потоков
- Индикация статусов операций
- Виды уведомлений
- Индикация результатов OVAL-проверок
- Статусы поиска уязвимостей

3.4.1.2.1. Цветовая индикация активов

В интерфейсе Комплекса на страницах **Инспекция сети** → **Карта сети** и **Активы** присутствует специфическая цветовая индикация активов. Ознакомиться с ней вы можете в таблице ниже.

Табл. 3. Индикация активов

ИНДИКАТОР	ОБОЗНАЧЕНИЕ	ОПИСАНИЕ
	Актив отмечен темно-синим	Трафик между устройством и прослушивающими интерфейсами Комплекса присутствует
	Актив отмечен серым	Отсутствует трафик между устройством и прослушивающими интерфейсами Комплекса
	Желтый знак вопроса в нижнем правом углу	Актив неизвестен
	Зеленая галочка в верхнем правом углу	На активе не обнаружено ошибок сбора данных и конфигураций, не соответствующих эталону

Табл. 3. Индикация активов

ИНДИКАТОР	ОБОЗНАЧЕНИЕ	ОПИСАНИЕ
	Желтый восклицательный знак в верхнем правом углу	На активе обнаружена одна или несколько следующих ошибок: неподтвержденное изменение конфигурации (последняя собранная конфигурация не равна эталонной); обнаружены затруднения при сборе данных некоторыми сканерами — выполнены успешно от 33 до 99% процессов сбора данных
	Красный крестик в верхнем правом углу	Обнаружены затруднения при сборе данных некоторыми сканерами — выполнены успешно от 0 до 33% процессов сбора данных
Индикация активов цветом и спецсимволами <u>не зависят</u> друг от друга		

3.4.1.2.2. Статусы активов

В таблице на странице **Активы** можно просматривать статусы выполненных операций активного сбора данных с активов и статистику по обнаруженным инцидентам и уязвимостям.

Столбцы таблицы можно выбрать и отобразить по кнопке  в правом верхнем углу страницы.

Описание статусов приведено в таблице ниже.

Табл. 4. Статусы активов на странице «Активы»

ОБОЗНАЧЕНИЕ	ОПИСАНИЕ	ИНДИКАТОРЫ
Конфигурации	Статус отклонения последней собранной с актива конфигурации от эталона. При наведении на статус отображается количество собранных конфигураций, сгруппированных по статусу их отклонения: - нет отклонений — количество конфигураций актива, соответствующих эталону в данный момент; - есть отклонения — количество конфигураций, не соответствующих эталону в данный момент; - были отклонения — количество конфигураций, которые соответствуют эталону в данный момент, но в их предыдущих версиях были отклонения.	 Красный — последняя конфигурация не соответствует эталону.  Оранжевый — последняя конфигурация соответствует эталону, но в ее предыдущих версиях были отклонения.  Зеленый — последняя конфигурация соответствует эталону.  Серый — сбор конфигураций не выполнялся.
Сбор данных	Процент успешно выполненных процессов сбора данных на активе. При наведении на статус отображается количество выполненных попыток сбора данных с активов по категориям: - количество процессов, выполненных успешно; - количество процессов, которые не удалось выполнить из-за ошибок соединения; - количество процессов, которые не удалось выполнить из-за ошибок сбора. Подробнее см. раздел Просмотр статуса сбора данных	 (красный) — 0-33% процессов сбора данных выполнены успешно.  (оранжевый) — 33-99% процессов сбора данных выполнены успешно.  (зеленый) — 100% процессов сбора данных выполнены успешно.  (серый) — сбор данных не выполнялся.

Табл. 4. Статусы активов на странице «Активы»

ОБОЗНАЧЕНИЕ	ОПИСАНИЕ	ИНДИКАТОРЫ
Инциденты	Наивысший приоритет среди обнаруженных инцидентов с категорией Новый на активе. При наведении на статус отображается количество обнаруженных инцидентов, сгруппированных по приоритету.	• Критический • Высокий • Средний • Низкий • пусто — инциденты с категорией Новый не обнаружены, либо поиск не выполнялся.
Уязвимости	Наивысший приоритет среди уязвимостей из базы CVE, обнаруженных на активе. При наведении на статус отображается количество обнаруженных уязвимостей, сгруппированных по приоритету. По нажатию на статус откроется окно просмотра уязвимостей выбранного актива.	• Критический • Высокий • Средний • Низкий • пусто — уязвимости не обнаружены, либо поиск не выполнялся.
Результаты сканирования	Статус процессов всех задач сбора данных актива. При наведении на статус отображается количество выполненных процессов сбора данных с активов по трем категориям: • назначено — общее количество процессов сбора данных, выполненных на активе; • количество процессов, которые не удалось выполнить из-за ошибок соединения; • количество процессов, которые не удалось выполнить из-за ошибок сбора.	• 167/1/156 (красный) — присутствуют ошибки сбора. Отображается количество всех результатов по категориям. • 97/43/0 (оранжевый) — присутствуют ошибки соединения, ошибок сбора нет. Отображается количество всех результатов по категориям. • 79 (черный) — успешный сбор всех конфигураций или событий. Отображается только количество назначенных процессов. • Пусто — сбор конфигураций или событий не выполнялся. Подробнее см. раздел Просмотр статуса сбора данных.

Табл. 4. Статусы активов на странице «Активы»

ОБОЗНАЧЕНИЕ	ОПИСАНИЕ	ИНДИКАТОРЫ
	При нажатии на статус открывается страница Задачи сбора с результатами сбора для выбранного актива.	

Статусы **Конфигурации**, **Сбор данных**, **Инциденты** и **Уязвимости** можно сортировать в порядке критичности. Порядок критичности по убыванию: темно-красный, красный, оранжевый, зеленый, серый/нет данных.



Внимание:

Статусы **Сбор данных** и **Конфигурации** формируют единый показатель актива **Статус проблемности**, по которому можно фильтровать список активов. Проблемность для каждого актива принимает одно из следующих значений:

- **Критический**: хотя бы один из статусов актива — **Сбор данных** или **Конфигурации** — имеет красный индикатор.
- **Важный**: хотя бы один из статусов актива — **Сбор данных** или **Конфигурации** — имеет оранжевый индикатор, но красные индикаторы отсутствуют.
- **ОК**: оба статуса имеют зеленый индикатор.
- **Нет данных**: сбор данных не выполнялся.

Подробнее см. раздел [Фильтрация списка активов](#).

3.4.1.2.3. Статусы групповых операций

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

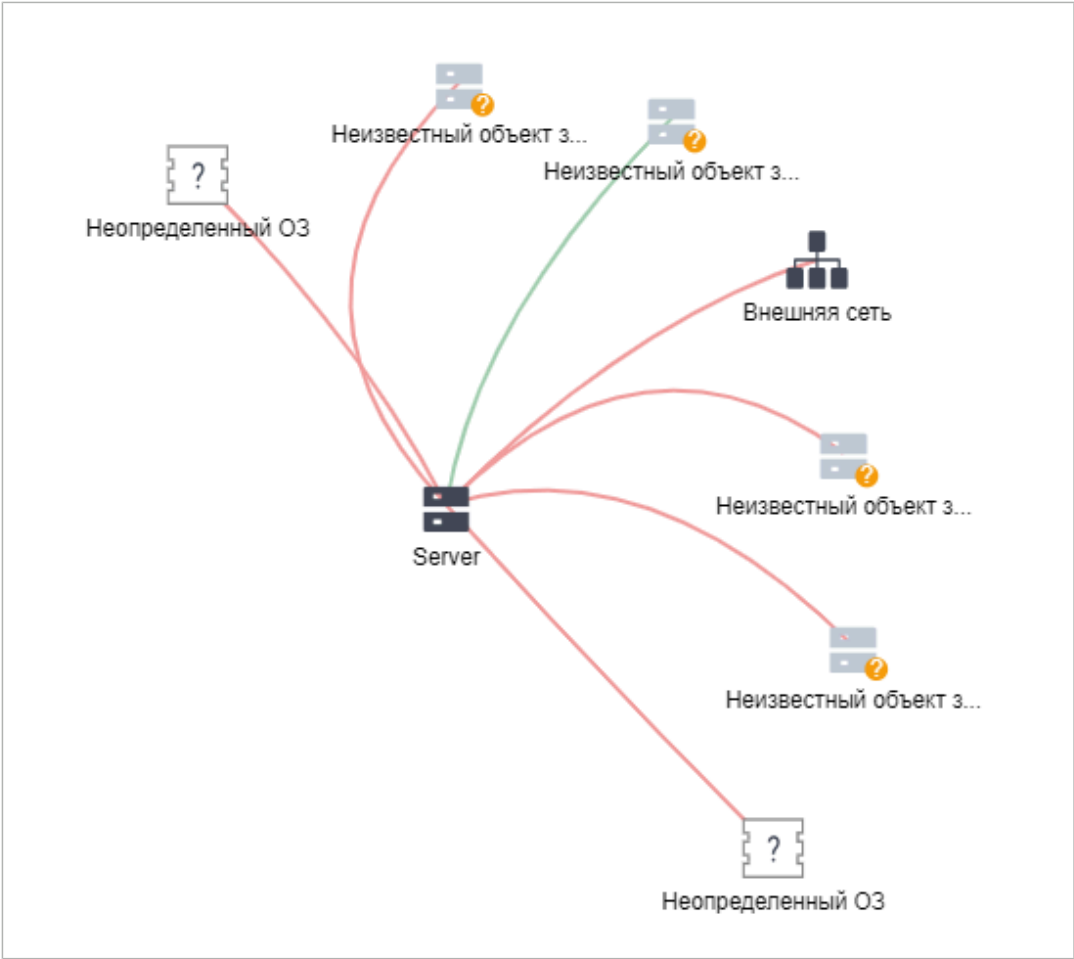
Табл. 5. Цветовая индикация групповых операций

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

3.4.1.2.4. Индикация потоков

Цветовая индикация потоков на странице **Карта сети** описана в таблице ниже.

Табл. 6. Цветовая индикация потоков на карте сети

ИНДИКАТОР	ОБОЗНАЧЕНИЕ	ОПИСАНИЕ
	Цвет потока красный	Потоки между активами не одобрены
	Цвет потока зеленый	Потоки между активами одобрены

3.4.1.2.5. Индикация статусов операций

В веб-интерфейсе присутствует индикация статусов выполнения длительных операций (например, группового удаления или изменения объектов). Ознакомиться с видами индикации статусов вы можете в таблице ниже.

Табл. 7. Индикаторы статусов операций в интерфейсе Комплекса

ИН-ДИКАТОР	ЦВЕТ	ОПИСАНИЕ	СТРАНИЦА ИНТЕРФЕЙСА
Ошибка обработки	Красный	Операция не была завершена вследствие ошибки. При нажатии на «▼» можно посмотреть детали	Карточка актива
Ошибка соединения	Оранжевый	Операция была инициирована пользователем, ожидает в очереди на выполнение	Карточка актива
Успешно завершено		Операция была запущена и выполняется в данный момент	Карточка актива
Предупреждение ▼	Оранжевый	Операция не была завершена вследствие превышения времени ожидания	Карточка актива
Активный	Зеленый	Пользователь активен (не заблокирован)	Пользователи
Неактивный	Красный	Пользователь неактивен (заблокирован)	Пользователи

3.4.1.2.6. Виды уведомлений

В результате действий в интерфейсе Комплекса пользователь может увидеть также всплывающие уведомления в правом верхнем углу. С их основными видами вы можете ознакомиться в таблице ниже.

Табл. 8. Виды уведомлений в интерфейсе Комплекса

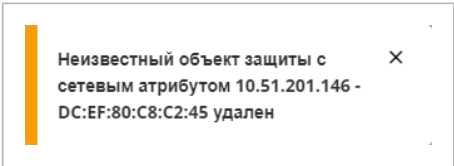
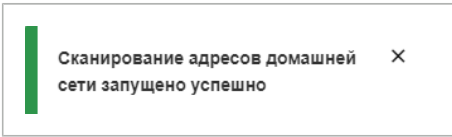
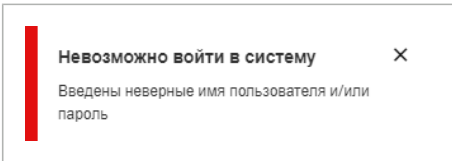
ПРИМЕР УВЕДОМЛЕНИЯ	ЦВЕТ	ОПИСАНИЕ
	Оранжевый	Предупреждения. Уведомляет пользователя о специфике работы выбранной операции и ее последствиях.

Табл. 8. Виды уведомлений в интерфейсе Комплекса

ПРИМЕР УВЕДОМЛЕНИЯ	ЦВЕТ	ОПИСАНИЕ
	Зеленый	Уведомляет пользователя об успешном начале потенциально длительной операции.
	Красный	Ошибки. Уведомляет пользователя о проблемах при выполнении операции.

3.4.1.2.7. Индикация результатов OVAL-проверок

Результаты OVAL-проверок актива на уязвимости или соответствие требованиям информационной безопасности имеют цветовую индикацию на странице веб-интерфейса.

Если проверка выполнена успешно и для актива не было обнаружено несоответствие по любому из критериев оценки соответствия (тип проверки: COMPLIANCE) либо ни одна из уязвимостей не была обнаружена (тип проверки: VULNERABILITY), в таблице результатов в строке **Статус** появится надпись *Завершена*, и строка таблицы будет выделена зеленым цветом.

TK-1	WIN-7SP1OVMS	WIN7_SP1-OVMS_TK1_DEVELOPERS	Уязвимости Microsoft SQL	24.07.2023, 16:21:50	Иванов Андрей Георгиевич (datapk)	INVENTORY & VULNERABILITY
Завершена						

Рис. 43. Результат успешной проверки на соответствие требованиям ИБ в случае выполнения всех критериев оценки

Если проверка выполнена, но для актива обнаружено несоответствие хотя бы по одному из критериев оценки (тип проверки: COMPLIANCE) либо была обнаружена хотя бы одна из уязвимостей (тип проверки: VULNERABILITY), в таблице результатов в строке **Статус** появится статус: **Завершена**, а строка таблицы будет выделена красным цветом.

TK-1	WIN_7_Company	Win7-SP1.company.local	Член домена, контроллер домена	24.07.2023, 15:12:21	Иванов Андрей Георгиевич (datapk)	COMPLIANCE
Завершена						

Рис. 44. Результат успешной проверки на соответствие требованиям ИБ в случае невыполнения критериев оценки

Если проверка не выполнена, в таблице результатов в столбце **Статус** появится статус: *Ошибка* с описанием ошибки.

TK-1	WIN-7SP1OVMS	WIN7_SP1-OVMS_TK1_DEVELOPERS	Парольная политика для работ...	18.07.2023, 18:10:56	Иванов Андрей Георгиевич (datapk)	COMPLIANCE
Ошибка ▲ Непредвиденная ошибка выполнения задачи проверки: [OVAL] Ошибка выполнения сбора объекта 'system_characteristics'						

Рис. 45. Результат неуспешной проверки на соответствие требованиям ИБ

Результаты проверок будут выделены желтым цветом, если в случае проверок типа COMPLIANCE и VULNERABILITY хотя бы один критерий имеет результат, отличный от true и false (например, в случае ошибки или невозможности получить данные с актива).

Результаты проверок типа INVENTORY (проверка наличия установленного ПО и версий ПО) и MISCELLANEOUS (иные виды проверок) не выделяются цветом.

3.4.1.2.8. Статусы поиска уязвимостей

В окне **Запустить поиск уязвимостей** на странице **Активы** можно просматривать статус поиска уязвимостей.

Описание статусов приведено в таблице ниже.

Табл. 9. Описание статусов поиска уязвимостей

ИНДИКАТОР	ОПИСАНИЕ
Не запущено	Поиск уязвимостей не был запущен пользователем
Выполняется	Поиск уязвимостей запущен и выполняется
Завершено	Поиск уязвимостей успешно завершился
Отменено	Поиск уязвимостей был отменен пользователем
Ошибка	Поиск уязвимостей завершен с ошибкой

Подробнее см. раздел [Запуск поиска уязвимостей в базах CVE, CPE и БДУ ФСТЭК России](#).

3.4.1.3. Сведения о версиях Комплекса

Версия Комплекса указывается в поставляемой документации на комплекс и отображается в веб-интерфейсе возле логотипа в верхней левой части страницы. Информация о версии также отображается на странице **Администрирование → О системе**.

3.4.2. Дополнительные функции Комплекса

В разделе описаны следующие дополнительные функциональные возможности Комплекса:

- Выгрузка отчетов
- Групповые операции
- Нормализация событий
- Фильтры

3.4.2.1. Выгрузка отчетов

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

СТРАНИЦА	СОДЕРЖАНИЕ ОТЧЕТА	ФОРМАТ ОТЧЕТА
Активы	Активы, выбранные чекбоксами	pdf, xlsx
	Уязвимости актива, для которого в последний раз выполнялся поиск	csv
Потоки данных	Все или отфильтрованные потоки данных	pdf, xlsx
Инциденты	Инциденты, выбранные чекбоксами	pdf, xlsx
Конфигурации	Все или отфильтрованные конфигурации	pdf, xlsx
	Результаты сопоставления собранного сканерами ПО и ОС со справочником CPE для актива, для которого в последний раз выполнялся поиск уязвимостей	csv
Результаты проверок	Все или отфильтрованные результаты проверок	pdf, xlsx

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



Внимание:

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

Для задачи создания отчета возможны следующие состояния:

- **Ожидание** — обычно кратковременный статус: происходит подготовка к созданию отчета. Может отображаться долго, если выбранных элементов много или есть другие задачи.
- **Выполняется** — отчет формируется в данный момент.
- **Ошибка** — во время формирования отчета произошла ошибка. При наведении на статус можно увидеть, какая именно ошибка вызвала статус.
- **Завершена** — отчет был успешно сформирован и его можно скачать.

3.4.2.2. Групповые операции

Для страниц оперативных данных и управления в интерфейсе Комплекса предусмотрен ряд групповых операций, которые имеют идентичный механизм работы.

Основные групповые операции

Основные групповые операции, общие для нескольких страниц интерфейса, вы можете увидеть в таблице ниже (Таблица 10. Основные групповые операции).

Табл. 10. Основные групповые операции

НАЗВАНИЕ	СТРАНИЦЫ ИНТЕРФЕЙСА
Удаление	Активы, Потоки данных, Инциденты, Индексы, Определения OVAL, Группы OVAL, Результаты проверок, Скрипты OVAL, Сканеры, Источники, Учетные данные актива, Настройки OVAL, Правила корреляции, Оповещения об инцидентах, Правила обнаружения, Статус сбора, Ретроанализ, Схема корреляции
Включение правил	Правила корреляции, Правила обнаружения
Отключение правил	Правила корреляции, Правила обнаружения



ОСТОРОЖНО:

Действие групповой операции применяется ко всем выбранным элементам страницы. Для страниц **Активы**, **Сканеры**, **Определения OVAL** выбор осуществляется при помощи установки чекбоксов. Выбор на остальных страницах осуществляется при помощи фильтров. Если фильтры и чекбоксы не установлены, операция будет применена ко всем элементам страницы.

Операции, доступные только при выборе одного или нескольких элементов

Если на странице, где элементы выбираются с помощью чекбоксов, ни одна строка не выбрана, часть операций будет недоступна. Подробности приведены в таблице ниже.

Табл. 11. Операции, доступные только при выборе одного или нескольких элементов.

СТРАНИЦА	КНОПКИ ОПЕРАЦИЙ, ДОСТУПНЫЕ ПРИ ВЫБОРЕ ХОТЯ БЫ ОДНОГО ЭЛЕМЕНТА
Активы	(Групповое удаление), (Запустить поиск уязвимостей), (Создать отчет)
Сканеры	Удалить
Определения OVAL	Отменить выбор, (Добавить в группу), (Исключить из группы)

Дополнительные групповые операции

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

Табл. 12. Дополнительные групповые операции

НАЗВАНИЕ	СТРАНИЦЫ ИНТЕРФЕЙСА
Изменить параметры инцидентов	Инциденты
Архивировать	Индексы
Добавить в группу OVAL-определения	Определения OVAL
Одобрить потоки	Потоки данных
Временно одобрить потоки	Потоки данных
Убрать одобрение с потоков	Потоки данных
Активировать	Задачи сбора
Деактивировать	Задачи сбора
Применить элементы схемы для текущего анализа	Схема корреляции
Не применять элементы схемы для текущего анализа	Схема корреляции
Применить элементы схемы для ретроспективного анализа	Схема корреляции
Не применять элементы схемы для ретроспективного анализа	Схема корреляции

Использование групповых операций

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

Для данного действия необходимо обоснование

✕

Введите текст обоснования

Подтвердить

Отменить

Рис. 46. Обоснование групповой операции

3.4.2.3. Нормализация событий

Выходным форматом сообщений Комплекса — внутренних или поступающих от источников событий — являются нормализованные события, которые отображаются на странице **События**.

Поля нормализованных событий и их значения используются в правилах корреляции событий, на основе которых Комплекс обнаруживает инциденты.

События приводятся к нормализованному виду по встроенным в Комплекс правилам нормализации с использованием следующих полей (часть полей может отсутствовать в зависимости от типа получаемых сообщений): @timestamp, @version, action, appliance_node_id, category, config_diff, config_type, create_time, description, event_code, event_type, observer_id, observer_name, id, justification, login, message, protocol, protocol_specific_data, receive_time, shell, source_ip, source_mac, status, target_ip, target_mac, type, user. Данные поля определены во встроенном шаблоне формата *.json, который хранится в директории /logstash/config/plugins/templates рабочей директории Комплекса.

Нормализация событий также осуществляется с помощью встроенных и пользовательских конфигурационных файлов Logstash. Файлы хранятся с расширением *.conf в директории /logstash/config/plugins/pipeline рабочей директории Комплекса.

Конфигурационные файлы нормализации делятся на три типа:

- **input** — генерируют события на основании сообщений из различных сервисов и определяют, к какому типу событий оно относится. Могут также содержать фильтры для начальной нормализации;
- **filter** — в зависимости от типа события выполняют основную нормализацию с помощью фильтров формата grok;
- **output** — в зависимости от типа нормализованных событий отправляют их в соответствующий сервис или в дополнительный output.

Рекомендуемый формат именования конфигурационных файлов нормализации: `${N}-${NAME}-${TYPE}.conf`, где:

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

Grok-фильтры имеют следующий формат: `%{ТИП_ДАННЫХ:значение_поля_события}`.

Пример

Пример grok-фильтра:

```
%{TIMESTAMP_ISO8601:date} %{WORD:method} %{IPV4:client} %{NUMBER:size} %{WORD:def} (?<Ver0s>.*)
```

Grok-фильтры могут применяться для разделения информации из встроенного поля по дополнительным пользовательским полям.

Пример

Пример конфигурационного файла с фильтром grok для сообщений из журнала SCADA:

```

filter {
  if [type] == "event" and [message] =~ "EventLog" {
    grok {
      # События SCADA
      #
      # Пример:
      # type="Info" message="TrainView session is ended" result="" source="User: admin"
      match => {"[message]" => "type=\"%{WORD:SCADA_type}\" message=\"%{GREEDYDATA:SCADA_message}\"
      result=\"%{GREEDYDATA:SCADA_result}\" source=\"%{GREEDYDATA:SCADA_source}\""}
      add_field => {"event_type" => "eventlog" }
      tag_on_failure => []
    }
  }
}

```

Сообщение из журнала SCADA, отправленное в Комплекс, сначала целиком записывается во встроенное поле `message`. Затем при помощи `grok`-фильтра содержимое этого поля нормализуется по следующим пользовательским полям: `SCADA_type`, `SCADA_message`, `SCADA_result`, `SCADA_source`.

3.4.2.4. Фильтры

Для поиска данных по критериям пользователь Комплекса может воспользоваться фильтрами.

The screenshot displays a web interface for filtering data flows. It includes several input fields and checkboxes:

- MAC-адреса отправителя**: A dropdown menu with the placeholder text "Введите MAC-адреса".
- Порты получателя**: A dropdown menu with the placeholder text "Введите порты или диапазоны".
- Использовать условие "AND"**: A checked checkbox.
- MAC-адреса получателя**: A dropdown menu with the placeholder text "Введите MAC-адреса".
- Изменил статус**: A text input field with the placeholder text "Введите имя пользователя".
- IP-адреса отправителя**: A dropdown menu with the placeholder text "Введите IP-адреса или диапазоны".
- Одобрённые/неодобрённые**: Two unchecked checkboxes labeled "Только одобренные" and "Только неодобренные".
- Сенсор**: A label for a sensor filter.

Below these filters is a large, dark, noisy area representing the data flow results.

Рис. 47. Пример фильтров на странице «Потоки данных»

Фильтры доступны на следующих страницах основного интерфейса:

- **Активы.**
- **Инспекция сети** → **Карта сети.**
- **Инспекция сети** → **Потоки данных.**
- **Инциденты.**
- **Администрирование** → **События и инциденты** → **Индексы**
- **Администрирование** → **Инспекция активов** → **Определения OVAL.**
- **Администрирование** → **Инспекция активов** → **Группы OVAL.**
- **Результаты проверок.**
- **Администрирование** → **Перечень ИС.**
- **Инспекция сети** → **Правила потоков.**
- **Администрирование** → **Инспекция активов** → **Скрипты OVAL.**
- **Администрирование** → **Сканеры.**

- [Администрирование](#) → [Настройка активов](#) → [Источники](#).
- [Администрирование](#) → [Настройка активов](#) → [Учетные данные актива](#).
- [Администрирование](#) → [Инспекция активов](#) → [Настройки OVAL](#).
- [Конфигурации](#).
- [Администрирование](#) → [События и инциденты](#) → [Правила корреляции](#).
- [Администрирование](#) → [События и инциденты](#) → [Оповещения об инцидентах](#).
- [Администрирование](#) → [Правила обнаружения](#).
- [Администрирование](#) → [Пользователи](#) → [Пользователи](#)

На каждой странице фильтры индивидуальны и зависят от содержания страницы.

Фильтры влияют только на отображение записей таблицы, количество и порядок столбцов таблицы можно изменить в окне «Настройка таблицы».

После настройки фильтров на страницах есть возможность сохранить примененный фильтр и другие параметры страницы, такие как расположение узлов на карте или колонок таблиц. Уже созданные представления можно изменить или удалить. Подробнее см. в разделе Управление представлениями.

3.4.2.5. Управление представлениями

Представление — элемент веб-интерфейса, предназначенный для сохранения текущего вида страницы. В большинстве случаев в представлении сохраняются примененные фильтры и выбранные для отображения колонки таблиц.

Например, на странице **Карта сети** сохраняются примененные фильтры, расположение узлов на карте, их вид (на сетке, по кругу), наличие сортировки по количеству потоков.

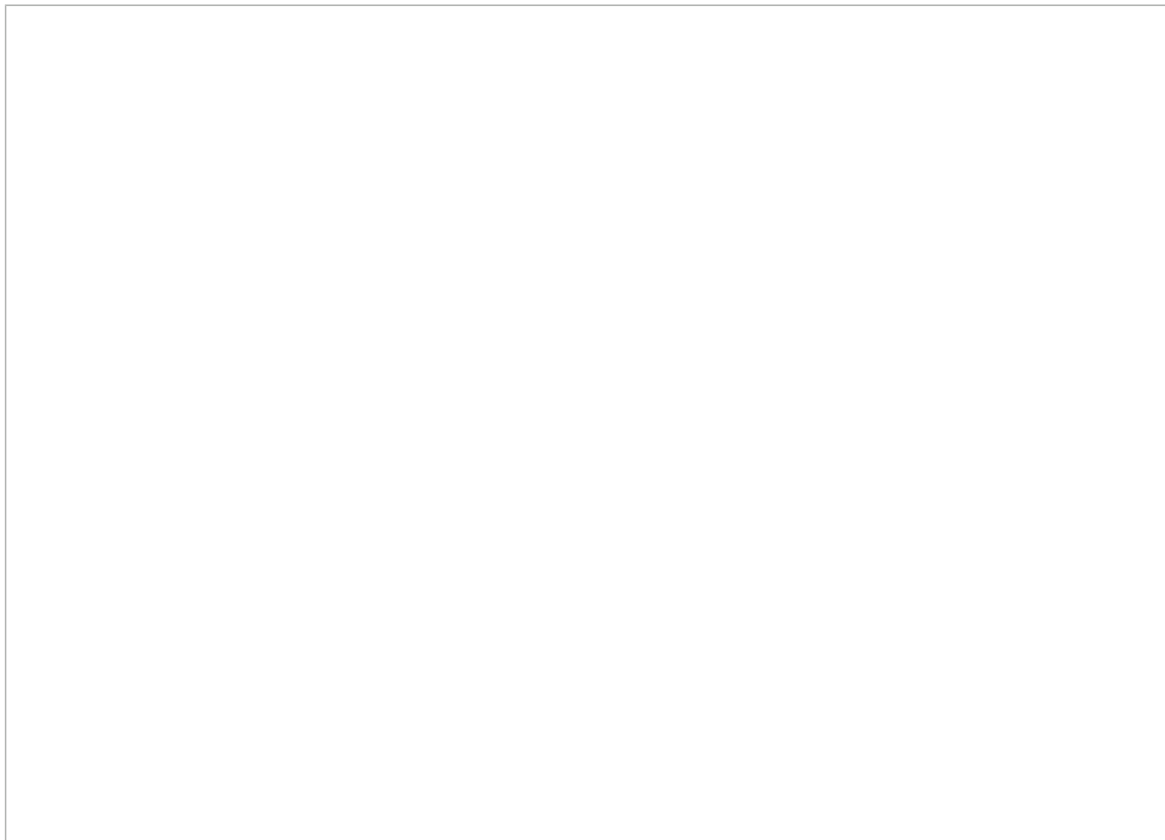


Рис. 48. Представления на странице «Карта сети»

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

3.4.2.5.1. Управление представлениями

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

1. Сохранение представления. Для сохранения:
 - а. Заполните все необходимые параметры фильтрации, выберите столбцы для отображения в представлении, либо отображение узлов на карте.
 - б. В верхней правой части страницы нажмите .
 - в. В выпадающем меню выберите опцию **Сохранить как**.
 - **Результат шага:** Откроется окно сохранения представления.
 - г. В окне сохранения представления:

- введите подходящее наименование;



Внимание:

Имя не должно совпадать с уже существующим.

- выберите, будет ли представление доступно для использования другими пользователями.

Сохранить представление «Все потоки за июль 2022»

Наименование *

☒ Сохранить только для меня
☐ Сохранить для всех пользователей

Рис. 49. Окно сохранения представления

д. Нажмите **Сохранить**.

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

2. Изменение представления. Для изменения:

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



Внимание:

Возле названия представления в верхней части панели фильтров появится оранжевый символ «*». Это означает, что есть несохраненные изменения представления.

в. Нажмите «» в верхней правой части страницы.

г. В появившемся меню выберите одну из следующих опций:

- **Сохранить** для сохранения изменений в выбранном представлении;
- **Сохранить как** для сохранения изменений в новом представлении;
- **Редактировать** для изменения названия и сохранения выбранного фильтра.

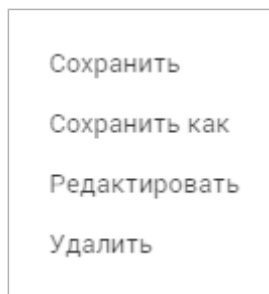


Рис. 50. Меню управления представлением

д. В окне сохранения представления введите имя представления.

Рис. 51. Предупреждение в окне сохранения представления

е. Нажмите **Сохранить**.

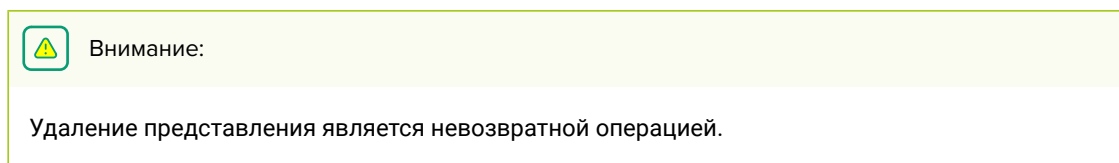
3. Удаление представления. Для удаления представления:

а. Нажмите «» в верхней правой части страницы.

б. В появившемся меню нажмите «Удалить».

► **Результат шага:** Откроется окно удаления представления.

в. В окне «Удалить представление» нажмите «Удалить».



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

3.5. Условия эксплуатации Комплекса

По условиям эксплуатации аппаратная часть для Комплекса предназначена для установки в стационарных, специальных и временных отапливаемых помещениях и укрытиях в условиях круглосуточной работы с перерывами на техническое обслуживание.

Нормальными климатическими условиями эксплуатации аппаратной части для Комплекса являются:

- температура окружающего воздуха – от –10 до +60 °С;
- относительная влажность воздуха – от 5 до 95%;
- атмосферное давление – от 630 до 800 мм рт.ст.

Способ подключения аппаратной части для Комплекса к оборудованию объекта информатизации определяется на этапе предпроектного обследования.

3.6. Описание источников событий

В этом разделе:

- Описание служебных источников событий
- Описание безагентного сбора событий Eventlog

3.6.1. Описание служебных источников событий

Служебные источники событий описаны в таблице ниже.

Табл. 13. Служебные источники событий Комплекса

НАЗВАНИЕ ИСТОЧНИКА (LISTENER)	ОПИСАНИЕ
Availability control	Изменение доступности активов, невозможность установки соединения с активом
Backup control	Статус процедуры резервного копирования
Configuration control	Изменение состояния эталонной конфигурации актива
Data flow control	Появление новых потоков, удаление отдельных потоков, одобрение и удаление групп потоков
Event control	Запуск или остановка системы регистрации событий
Host control	Создание, удаление и изменение активов, обнаружение неизвестных активов
Host data collecting	Статус выполнения задачи сбора данных с актива, состояние работы ее расписания
Incident control	Создание, удаление, изменение инцидентов
OVAL assessment control	Состояние выполнения, удаления результата проверок на соответствие требованиям ИБ
OVAL definitions control	Состояние задачи удаления проверок на соответствие требованиям ИБ
OVAL groups control	Состояние задачи на удаление группы или нескольких групп OVAL-определений
Script verification	Статус верификации Python-скриптов, используемых в сканерах сбора данных
User action control	Выполнение действий пользователями

Табл. 13. Служебные источники событий Комплекса

НАЗВАНИЕ ИСТОЧНИКА (LISTENER)	ОПИСАНИЕ
Switch Data Collecting Control	Статус активного сбора данных, смена задачи для активного сбора данных
System control	Статус компонентов Комплекса: оперативной памяти, дискового пространства, нагрузки на ЦП, средней нагрузки (Load average)
IDS control	Статус службы обнаружения вторжений
Esper control	Статус службы корреляции

Сбор событий с использованием служебных источников запускается автоматически после включения Комплекса.

Переменные для управления источниками событий

Администратор, имеющий доступ к консольному управлению, может настроить включение и отключение, а также критичность служебных событий. Для этого в файл `manager.env` добавляются соответствующие переменные, ознакомиться с которыми вы можете в таблице ниже (Таблица 14. Переменные для управления событиями Комплекса).

Переменные, наименование которых оканчивается на `_EVENTS`, могут иметь одно из следующих значений:

- `true` — для остановки работы служебного источника событий;
- `false` — для запуска работы служебного источника событий, если ранее он был отключен.

Переменные, наименование которых оканчивается на `_EVENTS_SEVERITY`, могут иметь одно из следующих значений:

- `critical` — для установки критичного приоритета событиям, сгенерированным сенсорами;
- `low` — для установки низкого приоритета событиям, сгенерированным сенсорами.

Табл. 14. Переменные для управления событиями Комплекса

ПЕРЕМЕННАЯ	ОПИСАНИЕ	ЗНАЧЕНИЕ ПЕРЕМЕННОЙ ПО УМОЛЧАНИЮ
<code>DISABLE_CONFIGURATION_CONTROL_EVENTS</code>	При значении переменной <code>true</code> события об изменении конфигурации не создаются	<code>false</code>
<code>DISABLE_DATA_FLOW_CONTROL_EVENTS</code>	При значении переменной <code>true</code> события о появлении новых потоков, удалении отдельных потоков, одобрении и удалении групп потоков не собираются	<code>false</code>

Табл. 14. Переменные для управления событиями Комплекса

ПЕРЕМЕННАЯ	ОПИСАНИЕ	ЗНАЧЕНИЕ ПЕРЕМЕННОЙ ПО УМОЛЧАНИЮ
DISABLE_HOST_DATA_COLLECTING_EVENTS	При значении переменной <code>true</code> события сбора данных не создаются	<code>false</code>
DISABLE_USER_ACTION_CONTROL_EVENTS	При значении переменной <code>true</code> события о действиях пользователей не создаются	<code>false</code>
DISABLE_HOST_CONTROL_EVENTS	При значении переменной <code>true</code> события о появлении новых, изменении и удалении узлов не создаются	<code>false</code>
DISABLE_AVAILABILITY_CONTROL_EVENTS	При значении переменной <code>true</code> события о доступности узлов не создаются	<code>false</code>
DISABLE_OVAL_ASSESSMENT_CONTROL_EVENTS	При значении переменной <code>true</code> события о проверках на соответствие требованиям ИБ не создаются	<code>false</code>
DISABLE_INCIDENT_CONTROL_EVENTS	При значении переменной <code>true</code> события об инцидентах не создаются	<code>false</code>
DISABLE_OVAL_DEFINITIONS_CONTROL_EVENTS	При значении переменной <code>true</code> события об удалении проверок на соответствие требованиям ИБ не создаются	<code>false</code>
DISABLE_OVAL_GROUPS_CONTROL_EVENTS	При значении переменной <code>true</code> события об удалении групп OVAL -определений не создаются	<code>false</code>
DATAPK_DISABLE_SWITCH_DATA_COLLECTING_CONTROL_EVENTS	При значении переменной <code>true</code> события о статусе активного сбора данных не собираются	<code>false</code>
DISABLE_BACKUP_CONTROL_EVENTS	При значении переменной <code>true</code> события о резервном копировании не создаются	<code>false</code>
DISABLE_SURICATA_CONTROL_EVENTS	При значении переменной <code>true</code> события службы обнаружения вторжений не собираются	<code>false</code>
CONFIGURATION_CONTROL_EVENTS_SEVERITY	Уровень критичности событий изменения конфигурации	<code>low</code>
DATA_FLOW_CONTROL_EVENTS_SEVERITY	Уровень критичности событий о появлении новых потоков, удалении отдельных потоков, одобрении и удалении групп потоков	<code>low</code>

Табл. 14. Переменные для управления событиями Комплекса

ПЕРЕМЕННАЯ	ОПИСАНИЕ	ЗНАЧЕНИЕ ПЕРЕМЕННОЙ ПО УМОЛЧАНИЮ
HOST_DATA_COLLECTING_EVENTS_SEVERITY	Уровень критичности событий сбора и ошибок сбора данных	low
USER_ACTION_CONTROL_EVENTS_SEVERITY	Уровень критичности событий по действиям пользователей	low
HOST_CONTROL_EVENTS_SEVERITY	Уровень критичности событий появления новых узлов	low
AVAILABILITY_CONTROL_EVENTS_SEVERITY	Уровень критичности событий доступности узлов	low
OVAL_ASSESSMENT_CONTROL_EVENTS_SEVERITY	Уровень критичности событий об объектах OVAL	low
INCIDENT_CONTROL_EVENTS_SEVERITY	Уровень критичности событий о создании, удалении, изменении инцидентов	low
OVAL_DEFINITIONS_CONTROL_EVENTS_SEVERITY	Уровень критичности событий удаления проверок на соответствие требованиям ИБ	low
OVAL_GROUPS_CONTROL_EVENTS_SEVERITY	Уровень критичности событий удаления групп OVAL -определений	low
DATAPK_SWITCH_DATA_COLLECTING_CONTROL_EVENTS_SEVERITY	Уровень критичности событий изменения статуса активного сбора данных	low
BACKUP_CONTROL_EVENTS_SEVERITY	Уровень критичности событий резервного копирования	low
IDS_CONTROL_EVENTS_SEVERITY	Уровень критичности событий службы обнаружения вторжений	low
ESPER_CONTROL_EVENTS_SEVERITY	Уровень критичности событий сервиса обработки событий	critical

3.6.2. Описание безагентного сбора событий Eventlog

Задачи сбора событий могут быть описаны в исполняемом файле, которые выполняются в среде, поддерживающей подмножество синтаксиса языка Python (RestrictedPython) – скрипте.

Пример Python-скрипта, используемого в сканере для сбора событий из журнала **security** Microsoft Windows с помощью учетной записи с тегом `admin`:

```
journal_name = 'Security'
offset = store.get('offset') if store else None
fetch_old_events = False # Нужно ли получать события с активов , созданные до первого запуска скрипта
try:
    credential = credentials['admin']
except KeyError as e:
    raise KeyError('Учетные данные для пользователя admin не найдены') # Получаем смещение, если необходимо
if not fetch_old_events and offset is None:
    protocol_args = {
        'interface': 'mseven',
        'host': host,
        'user': credential['user'],
        'password': credential['password'],
        'query': {
            'object': 'offset',
            'path': journal_name,
            'offset': 0
        },
        'timeout': 300,
        'ttl': 300,
    }
    offset = execute('msrpc', protocol_args, expiration)['newest_record_number'] # Получаем события
    protocol_args = {
        'interface': 'mseven',
        'host': host,
        'user': credential['user'],
        'password': credential['password'],
        'query': {
            'object': 'events',
            'path': journal_name,
            'offset': offset
        },
        'timeout': 300,
        'ttl': 300,
    }
    events = execute('msrpc', protocol_args, expiration)result = []
    for event in events:
        if event['EventId'] in
[4720, 4722, 4726, 4738, 4740, 4767, 4781, 4724, 4725, 4727, 4728, 4729, 4730, 4731, 4732,
```

```

4733, 4734, 4735, 4737, 4754, 4755, 4756, 4757, 4758, 4764, 4616, 1102, 4625, 4624]:
result.append({
    'receive_time': datetime.datetime.utcnow().isoformat(),
    'message': event['Message'],
    'host_id': host_id,
    'observer_id': observer_id,
    'protocol_specific_data': {
        'journal_name': journal_name,
        'computer_name': event['ComputerName'],
        'event_id': event['EventId'],
        'event_type': event['EventType'],
        'event_category': event['EventCategory'],
        'source_name': event['SourceName']
    }
}) offset = event['RecordNumber'] + 1
return {
    'data': result,
    'store': {'offset': offset}
}

```

Общий состав задачи сбора событий определяется в тексте Python-скрипта. В качестве настраиваемых параметров для описания задачи сбора событий могут быть выбраны:

- `computer_name` – идентификатор хоста;
- `event_category` – категория события;
- `event_id` – идентификатор события;
- `event_type` – тип события;
- `journal_name` – наименование журнала;
- `source_name` – название источника, создавшего событие.

Для возможности сбора событий с активов необходимо создать и настроить учетные записи на активах с правами, достаточными для удаленного доступа к необходимой информации. Учетную запись, настроенную в операционной системе актива, необходимо добавить в список учетных данных в веб-интерфейсе Комплекса. Порядок настройки учетных данных в Комплексе приведен в разделе Добавление учетных данных актива.

3.7. Описание полей событий

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

Табл. 15. Основные поля событий

ПОЛЕ	ОПИСАНИЕ	ПРИМЕРЫ ЗНАЧЕНИЯ ПОЛЯ
action	Краткое описание действия	detect, block, permit, audit_success, connection success, connection failure, auth success
additional_information	Дополнительная информация о действии или его результате	rpc_s_access_denied
appliance_node_id	ID Комплекса уровня Sensor, на котором было зафиксировано событие	b08deaf7edc5def382d2580870de5fbe
appliance_node_name	Наименование Комплекса уровня Sensor, на котором было зафиксировано событие	datapk-vm-tk2-test-244-36
category	Классификация события по результату или источнику	OK
create_time	Время регистрации события на источнике. Может не совпадать с часовым поясом Комплекса	11.05.2022 @ 18:42:33.789
description	Краткое описание события	Create incoming message
event_code	Идентификатор или классификатор типа события	1170004
event_type	Тип события	info_exchange
id	Уникальный идентификатор события	019b35f6-2b98-47de-a3d0-c37c554029a6
justification	Обоснование или комментарий к выполняемому действию	
link	Поле для внешних интеграторов	
listener	Наименование служебного источника событий	event_log_sensor
management_node_id	ID Комплекса уровня Management, на котором было зафиксировано событие	b08deaf7edc5def382d2580870de5fbe

Табл. 15. Основные поля событий

ПОЛЕ	ОПИСАНИЕ	ПРИМЕРЫ ЗНАЧЕНИЯ ПОЛЯ
management_node_name	Наименование Комплекса уровня Management, на котором было зафиксировано событие	datapk-vm-tk2-test-244-36
message	Исходное (оригинальное) событие	Выявлена ошибка подключения к активу 192.168.243.80 по MSRPC: rpc_s_access_denied
observer_id	ID регистратора события: актива, сенсора или Комплекса	9429058a-835a-4f9e-a666-ee5799b33db0
observer_ip	IP-адрес регистратора события: актива, сенсора или Комплекса	10.51.203.99
observer_name	Сетевое имя регистратора события: актива, сенсора или Комплекса	datapk-vm-tk2-test-244-36
priority	Приоритет инцидента	low
protocol	Протокол взаимодействия/API/ID канала инфообмена	ssh
receive_time	Время регистрации события на Комплексе	11.05.2022 @ 18:30:11.960
request_id	Идентификатор HTTP-запроса	GET /index.html HTTP/1.1
severity	Важность события	critical
source_hostname	Наименование отправителя (актива)	datapk-vm-tk2-test-244-36
source_id	Идентификатор отправителя (актива)	f37b0f20-c1f5-4401-9240-0cfccd9daa58
source_ip	IP-адрес отправителя (актива)	10.51.203.19
source_mac	datapk-vm-tk2-test-244-36	00:50:56:B7:2C:3C
source_port	Порт отправителя (актива)	5353
target_ip	IP-адрес получателя (актива)	10.51.203.9
target_mac	MAC-адрес получателя (актива)	00:50:56:B7:2C:3C
target_id	Идентификатор получателя (актива)	2098ebf1-7e32-4d8f-8b0e-3cfc92e9e921

Табл. 15. Основные поля событий

ПОЛЕ	ОПИСАНИЕ	ПРИМЕРЫ ЗНАЧЕНИЯ ПОЛЯ
target_ hostname	Наименование получателя (актива)	WIN-7
target_port	Порт получателя (актива)	80
user	Логин пользователя, инициировавшего событие	aivanov

3.8. Переменные Комплекса

Для Комплексов и их сервисов устанавливаются разные конфигурационные файлы с различным набором переменных.

Конфигурационные файлы с переменными и их расположение представлены в таблице ниже.

Табл. 16. Конфигурационные файлы с переменными и их расположение

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

3.8.1. Переменные Комплекса уровня Management

Обязательные переменные файла manager.env

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

Список обязательных переменных, содержащийся в файле manager.env, представлен в таблице ниже.

Табл. 17. Обязательные переменные файла manager.env

ПЕРЕМЕННАЯ	ОПИСАНИЕ	ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ (ЖИРНЫМ), ЛИБО ПРИМЕР
DB_USER	Пользователь базы данных.  ОСТОРОЖНО: Изменение значения переменной может привести к отсутствию доступа к базе данных.	postgres

Табл. 17. Обязательные переменные файла `manager.env`

ПЕРЕМЕННАЯ	ОПИСАНИЕ	ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ (ЖИРНЫМ), ЛИБО ПРИМЕР
<code>HOST_IP</code>	Интерфейс управления Комплекса. В качестве значения переменной задается IP-адрес одного из активных интерфейсов Комплекса	10.51.15.104
<code>DB_ENCRYPTION_KEY</code>	Ключ шифрования базы данных в сборщике данных (host data collector).	dJ2ZOZeU0nJh-Hwjfhq!OwF1x
<code>EVENT_INDICES_MAX_SIZE_GB</code>	Максимально допустимый объем оперативного архива. Суммарный объем с <code>EVENT_ARCHIVES_MAX_SIZE_GB</code> не должен составлять более 50-60% объема дискового пространства.  Внимание: На Комплексах базового уровня и (или) с HDD — не более 100 ГБ. На Комплексах среднего и верхнего уровней с SSD — не более 300 ГБ	10
<code>EVENT_INDICES_ACTION_SIZE_EXCEEDED</code>	Действие в случае переполнения оперативного архива событий. Возможны два варианта значений переменной: <code>rotate</code> — записывать события в глубокий архив и <code>break</code> — прервать регистрацию событий	rotate
<code>EVENT_INDICES_LIFETIME_DAYS</code>	Время хранения событий в оперативном архиве, задается в днях	30
<code>EVENT_ARCHIVES_LIFETIME_DAYS</code>	Время хранения событий в глубоком архиве, события старше указанного значения удаляются. Значение задается в днях	60
<code>EVENT_ARCHIVES_MAX_SIZE_GB</code>	Максимально допустимый объем глубокого архива. Суммарный объем с <code>EVENT_INDICES_MAX_SIZE_GB</code> должен составлять не более 50-60% объема дискового пространства	5

Дополнительные переменные файла `manager.env`

Переменные, которые не включены в автоматически генерируемый файл `manager.env` Комплекса уровня Management и добавляются при необходимости, указаны в таблице ниже.

Табл. 18. Дополнительные переменные файла `manager.env`

ПЕРЕМЕННАЯ	ОПИСАНИЕ	ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ (ЖИРНЫМ), ЛИБО ПРИМЕР
<code>API_SKIP_FIRST_INITIALIZATION</code>	Отключение первичной инициализации при первом запуске Комплекса при значении переменной <code>true</code>	false
<code>AUTOMATIC_HOST_CREATION_BY_MAC</code>	Включение фильтрации создания неизвестных объектов защиты без IP и MAC-адреса при значении переменной <code>true</code> . При значении переменной <code>false</code> неизвестные активы создаются с IP и MAC-адресом (IP+MAC)	false
<code>ASSETS_INACTIVITY_TIMEOUT</code>		600
<code>LIMIT_USER_SESSIONS</code>	При значении переменной <code>true</code> ограничивает до одной количество одновременных активных сессий в веб-интерфейсе Комплекса для каждой учетной записи. При значении переменной <code>false</code> ограничений на количество сессий нет	false
<code>LDAP_CONNECTION_STRING</code>	IP-адрес LDAP-сервера Active Directory для создания пользователей из службы каталогов	<code>ldaps://192.168.243.121</code>
<code>LDAP_TLS</code>	Использовать TLS-шифрование для Active Directory	false
<code>LOG_LEVEL</code>	Минимальная критичность системных событий, которые генерирует Комплекс уровня Management. Возможные значения:	INFO
<code>MAX_ROWS_PER_REPORT</code>	Максимальное количество строк, выгружаемых при формировании отчета. Если	1000

Табл. 18. Дополнительные переменные файла `manager.env`

ПЕРЕМЕННАЯ	ОПИСАНИЕ	ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ (ЖИРНЫМ), ЛИБО ПРИМЕР
	значение переменной более 1000, в отчет выгрузится только 1000 строк	
<code>DISABLE_CONFIGURATION_CONTROL_EVENTS</code>	При значении переменной <code>true</code> события об изменении конфигурации не создаются	false
<code>DISABLE_HOST_DATA_COLLECTING_EVENTS</code>	При значении переменной <code>true</code> события сбора данных не создаются	false
<code>DISABLE_USER_ACTION_CONTROL_EVENTS</code>	При значении переменной <code>true</code> события о действиях пользователей не создаются	false
<code>DISABLE_HOST_CONTROL_EVENTS</code>	При значении переменной <code>true</code> события о появлении новых, изменении и удалении узлов не создаются	false
<code>DISABLE_AVAILABILITY_CONTROL_EVENTS</code>	При значении переменной <code>true</code> события о доступности узлов не создаются	false
<code>DISABLE_OVAL_ASSESSMENT_CONTROL_EVENTS</code>	При значении переменной <code>true</code> события о проверках на соответствие требованиям ИБ не создаются	false
<code>DISABLE_INCIDENT_CONTROL_EVENTS</code>	При значении переменной <code>true</code> события об инцидентах не создаются	false
<code>DISABLE_OVAL_DEFINITIONS_CONTROL_EVENTS</code>	При значении переменной <code>true</code> события об удалении проверок на соответствие требованиям ИБ не создаются	false
<code>DISABLE_OVAL_GROUPS_CONTROL_EVENTS</code>	При значении переменной <code>true</code> события об удалении групп OVAL -определений не создаются	false
<code>DISABLE_BACKUP_CONTROL_EVENTS</code>	При значении переменной <code>true</code> события о резервном копировании не создаются	false
<code>CONFIGURATION_CONTROL_EVENTS_SEVERITY</code>	Уровень критичности событий изменения конфигурации	low

Табл. 18. Дополнительные переменные файла `manager.env`

ПЕРЕМЕННАЯ	ОПИСАНИЕ	ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ (ЖИРНЫМ), ЛИБО ПРИМЕР
<code>HOST_DATA_COLLECTING_EVENTS_SEVERITY</code>	Уровень критичности событий сбора и ошибок сбора данных	low
<code>USER_ACTION_CONTROL_EVENTS_SEVERITY</code>	Уровень критичности событий по действиям пользователей	low
<code>HOST_CONTROL_EVENTS_SEVERITY</code>	Уровень критичности событий появления новых узлов	low
<code>AVAILABILITY_CONTROL_EVENTS_SEVERITY</code>	Уровень критичности событий доступности узлов	low
<code>OVAL_ASSESSMENT_CONTROL_EVENTS_SEVERITY</code>	Уровень критичности событий об объектах OVAL	low
<code>INCIDENT_CONTROL_EVENTS_SEVERITY</code>	Уровень критичности событий о создании, удалении, изменении инцидентов	low
<code>OVAL_DEFINITIONS_CONTROL_EVENTS_SEVERITY</code>	Уровень критичности событий удаления проверок на соответствие требованиям ИБ	low
<code>OVAL_GROUPS_CONTROL_EVENTS_SEVERITY</code>	Уровень критичности событий удаления групп OVAL -определений	low
<code>BACKUP_CONTROL_EVENTS_SEVERITY</code>	Уровень критичности событий резервного копирования	low
<code>FSTEC_MAPPINGS_ENABLED</code>	При значении переменной <code>false</code> :	true
<code>OVAL_IMPORT_TIMEOUT_MINUTES</code>	Время, по истечении которого импорт OVAL-групп завершается с ошибкой. Значение задается в минутах	10
<code>NGINX_HTTPS_PORT</code>	Порт для подключения к Комплексу по протоколу HTTPS	443
<code>DISABLE_SURICATA_CONTROL_EVENTS</code>	При значении переменной <code>true</code> события службы обнаружения вторжений не собираются	false

Табл. 18. Дополнительные переменные файла `manager.env`

ПЕРЕМЕННАЯ	ОПИСАНИЕ	ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ (ЖИРНЫМ), ЛИБО ПРИМЕР
<code>DISABLE_DATA_FLOW_CONTROL_EVENTS</code>	При значении переменной <code>true</code> события о потоках данных не собираются	false
<code>DISABLE_HOME_NET_SCAN_CONTROL_EVENTS</code>	При значении переменной <code>true</code> события при сканировании домашней сети не собираются	false
<code>DISABLE_SCRIPT_VERIFICATION_EVENTS</code>	При значении переменной <code>true</code> события регистрации скриптов не собираются	false
<code>DISABLE_SYSTEM_CONTROL_EVENTS</code>	При значении переменной <code>true</code> системные события не собираются	false
<code>EVENT_CONTROL_EVENTS_SEVERITY</code>	Уровень критичности для событий, полученных от сервиса регистрации событий	critical
<code>HOME_NET_SCAN_CONTROL_EVENTS_SEVERITY</code>	Уровень критичности для событий, полученных при сканировании домашней сети	low
<code>SCRIPT_VERIFICATION_EVENTS_SEVERITY</code>	Уровень критичности событий верификации скриптов	low
<code>SYSTEM_CONTROL_EVENTS_SEVERITY</code>	Уровень критичности для системных событий	low
<code>DATA_FLOW_CONTROL_EVENTS_SEVERITY</code>	Уровень критичности событий о появлении новых потоков, удалении отдельных потоков, одобрении и удалении групп потоков	low
<code>EVENT_ARCHIVES_ACTION_SIZE_EXCEEDED</code>	Действие, выполняемое при превышении лимита на размер глубокого архива. Возможные значения переменной: • <code>nothing</code> • <code>break</code> • <code>rotate</code>	rotate

Табл. 18. Дополнительные переменные файла `manager.env`

ПЕРЕМЕННАЯ	ОПИСАНИЕ	ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ (ЖИРНЫМ), ЛИБО ПРИМЕР
<code>USER_SESSION_INACTIVITY_TIMEOUT</code>	Ограничение сессии при отсутствии активности пользователя. Значение переменной задается в секундах	600
<code>ENABLE_DNS_PINNING_PROTECTION</code>	Включение защиты от атаки Anti DNS Pinning. При значении переменной <code>true</code> веб-сервер будет отправлять 404 ошибку, если запрос пришел на адрес, не равный CN серверного сертификата	false

Переменные сервиса `udv-prometheus`

Переменные сервиса `udv-prometheus` устанавливаются в директории `/etc/sysconfig/udv-prometheus`

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

Табл. 19. Список переменных сервиса `udv-prometheus`

ПЕРЕМЕННАЯ	ОПИСАНИЕ	ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ (ЖИРНЫМ), ЛИБО ПРИМЕР
<code>MAX_DISK_SPACE_CONSUMED_PERCENTAGE</code>	Лимит заполнения ПЗУ (HDD, SSD) операционной системы Комплекса в процентах	80
<code>MAX_CPU_LOAD_CONSUMED_PERCENTAGE</code>	Лимит нагрузки на центральный процессор (CPU) операционной системы Комплекса в процентах	80
<code>MAX_LA</code>	Лимит средней нагрузки (Load average) операционной системы Комплекса в ядрах	8
<code>RMQ_LOW_AVAILABLE_DISK_SPACE_WATERMARK_BYTES</code>	Минимальный уровень свободного дискового пространства для брокера сообщений <code>rabbitmq</code> , при достижении которого в веб-интерфейсе появляется соответствующее событие 1180013, а при его нормализации появляется	500000000

Табл. 19. Список переменных сервиса `udv-prometheus`

ПЕРЕМЕННАЯ	ОПИСАНИЕ	ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ (ЖИРНЫМ), ЛИБО ПРИМЕР
	событие 1180014. Задается в байтах	
<code>RMQ_LOW_AVAILABLE_MEMORY_WATERMARK_BYTES</code>	Минимальный уровень свободной оперативной памяти для брокера сообщений <code>rabbitmq</code> , при достижении которого в веб-интерфейсе появляется соответствующее событие 1180011, а при его нормализации появляется событие 1180012. Задается в байтах	500000000

Переменные сервиса `udv-logstash`

Переменные сервиса `udv-logstash` устанавливаются в директории `/etc/sysconfig/udv-logstash`

Список переменных сервиса `udv-logstash` представлен в таблице ниже.

Табл. 20. Список переменных сервиса `udv-logstash`

ПЕРЕМЕННАЯ	ОПИСАНИЕ	ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ (ЖИРНЫМ), ЛИБО ПРИМЕР
<code>LOG_LEVEL</code>	Минимальная критичность системных событий, которые генерирует Комплекс уровня Management. Возможные значения:	INFO
<code>ESPER_PORT</code>	Порт сервиса корреляции событий	517
<code>LS_JAVA_OPTS</code>	Объем оперативной памяти, выделяемой под сервис <code>udv-logstash</code> . Задается в мегабайтах	- Dlog4j2.formatMsgNo- Lookups=true-Xmx1024m- Xms1024m

Переменные сервиса `udv-opensearch`

Переменные сервиса `udv-opensearch` устанавливаются в директории `/etc/sysconfig/udv-opensearch`

Список переменных сервиса `udv-opensearch` Комплекса уровня Management, представлен в таблице ниже.

Табл. 21. Список переменных сервиса `udv-opensearch`

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

Переменные сервиса `udv-esper`

Переменные сервиса `udv-esper` устанавливаются в директории `/etc/sysconfig/udv-esper`

Список переменных сервиса `udv-esper` Комплекса уровня Management, представлен в таблице ниже.

Табл. 22. Список переменных сервиса `udv-esper`

ПЕРЕМЕННАЯ	ОПИСАНИЕ	ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ (ЖИРНЫМ), ЛИБО ПРИМЕР
<code>ESPER_RMQ_MAX_QUEUE_SIZE</code>	Максимальная длина очереди событий Syslog и событий службы обнаружения вторжений. Задается в байтах	100000
<code>ESPER_JAVA_OPTS</code>	Объем оперативной памяти, выделяемой под сервис корреляции событий. Задается в мегабайтах	- <code>Djava.net.preferIPv4Stack=true-Dlog4j2.formatMsgNoLookups=true-Xmx1024m</code>

3.8.2. Переменные Комплекса уровня Sensor

Обязательные переменные файла `sensor.env`

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

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

Табл. 23. Обязательные переменные файла `sensor.env`

ПЕРЕМЕННАЯ	ОПИСАНИЕ	ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ (ЖИРНЫМ), ЛИБО ПРИМЕР
<code>MANAGER_NODE_ADDRESS</code>	IP-адрес для подключения к Комплексу уровня Management	127.0.0.1
<code>LISTENING_INTERFACES</code>	Наименования всех интерфейсов, с которых сенсор анализирует трафик. Можно указывать интерфейсы в любом режиме (не только прослушивания трафика). При использовании нескольких интерфейсов перечисляются через запятую без пробелов. Все интерфейсы должны быть в состоянии <i>up</i> , иначе сенсор не сможет корректно инициализироваться.	ens32,ens33,ens35
<code>LOG_LEVEL</code>	Минимальная критичность системных событий, которые генерирует Комплекс уровня Management. Возможные значения:	INFO

Дополнительные переменные файла `sensor.env`

Переменные, которые не включены в автоматически генерируемый файл `sensor.env` Комплекса уровня Sensor и добавляются при необходимости, указаны в таблице ниже.

Табл. 24. Дополнительные переменные файла `sensor.env`

ПЕРЕМЕННАЯ	ОПИСАНИЕ	ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ (ЖИРНЫМ), ЛИБО ПРИМЕР
<code>DISABLE_TCP_HIGH_PORT_DISCARDING</code>	Включает возможность при анализе потоков зафиксировать tcp-порты на значения ≥ 32768 при значении переменной <code>true</code> .	true

Табл. 24. Дополнительные переменные файла `sensor.env`

ПЕРЕМЕННАЯ	ОПИСАНИЕ	ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ (ЖИРНЫМ), ЛИБО ПРИМЕР
	При значении <code>false</code> фиксация портов больше или равных 32768 будет отключена, и при получении пакета с двумя такими портами в поток запишется значение * для обоих	
<code>GODPI_TCP_SKIP_SESSION_WITHOUT_HANDSHAKE</code>	При значении <code>true</code> включает возможность создания потоков по данным неполных TCP-сессий. Возникают в случае, когда Комплекс не может обнаружить пакеты установления TCP-соединения и поэтому не может достоверно определить, какой сетевой узел является отправителем, а какой — получателем	true
<code>TERMINAL_CONNECTOR_SSH_TIMEOUT</code>	Максимальное время ожидания выполнения задачи сбора данных по протоколу SSH. Задается в секундах	30
<code>COMMAND_PROCESSOR_WORKER_MAX_MEMORY_SIZE_MB</code>	Лимит памяти для обработки одного процесса сбора данных. При превышении лимита в результаты сбора выводится ошибка <i>Сбор данных был прерван в результате обнаружения большего объема данных, чем ожидалось</i> . Задается в мегабайтах	256
<code>MIBS_TO_COMPILE</code>	Список MIB-словарей для интерпретации сетевых данных	<code><mib1>, <mib2></code>
<code>GODPI_TCP_SESSION_TIMEOUT</code>	Временное значение, по истечении которого будут удаляться TCP-сессии. Задается в секундах	86400
<code>GODPI_TCP_SESSION_CLEANUP_INTERVAL</code>	Временное значение, по истечении которого будет выполняться очистка TCP-сессий. Задается в секундах	86400
<code>GODPI_METRICS_AND_DEBUG_PORT</code>	Порт для получения значений GODPI	6060

Табл. 24. Дополнительные переменные файла `sensor.env`

ПЕРЕМЕННАЯ	ОПИСАНИЕ	ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ (ЖИРНЫМ), ЛИБО ПРИМЕР
<code>COMMAND_PROCESSOR_SCRIPT_MODULES</code>	Список Python-модулей, доступных для сканеров сбора данных	re, string, unicodedata, hashlib, datetime, _strptime, textwrap, struct, dbfread, dateutil, dateutil.tz, parsel, random

3.8.3. Переменные службы обнаружения вторжений

Для службы обнаружения вторжений Комплекса устанавливается конфигурационный файл с набором переменных, расположенный в директории `/etc/sysconfig/suricata-wrapper`.

Значения переменных указываются следующим образом:

- одиночный IP-адрес или порт указываются в следующем формате: `20` или `192.168.0.0`;
- несколько IP-адресов указываются в следующем формате: `[192.168.0.0/16,10.0.0.0/8,172.16.0.0/12]`;
- несколько портов указываются в следующем формате: `[20,21]`.

Список переменных, содержащихся в данного конфигурационном файле, представлен в таблице ниже.

Табл. 25. Переменные службы обнаружения вторжений

ПЕРЕМЕННАЯ	ОПИСАНИЕ	ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ (ЖИРНЫМ), ЛИБО ПРИМЕР
<code>ADDRESS_VARIABLEA</code>	Переменные для добавления пользовательского IP-адреса или диапазона IP-адресов	<code>\$HOME_NET</code>
<code>ADDRESS_VARIABLEB</code>		
<code>ADDRESS_VARIABLEC</code>		
<code>ADDRESS_VARIABLED</code>		
<code>AIM_SERVERS</code>	Домашняя (контролируемая) сеть серверов AIM (AOL Instant Messenger)	<code>\$EXTERNAL_NET</code>
<code>DC_SERVERS</code>	Домашняя (контролируемая) сеть серверов DC (Domain Controllers)	<code>\$HOME_NET</code>
<code>DNP3_CLIENT</code>	Домашняя (контролируемая) сеть клиентов DNP3-протокола	<code>\$HOME_NET</code>
<code>DNP3_PORT</code>	Порты DNP3-протокола	<code>20000</code>
<code>DNP3_SERVER</code>	Домашняя (контролируемая) сеть серверов DNP3	<code>\$HOME_NET</code>
<code>DNS_SERVERS</code>	Домашняя (контролируемая) сеть серверов DNS	<code>\$HOME_NET</code>
<code>ENIP_CLIENT</code>	Домашняя (контролируемая) сеть клиентов ENIP-протокола	<code>\$HOME_NET</code>

Табл. 25. Переменные службы обнаружения вторжений

ПЕРЕМЕННАЯ	ОПИСАНИЕ	ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ (ЖИРНЫМ), ЛИБО ПРИМЕР
ENIP_SERVER	Домашняя (контролируемая) сеть серверов ENIP	\$HOME_NET
EXTERNAL_NET	IP-адреса, не входящих в домашнюю (контролируемую) сеть	!\$HOME_NET
FILE_DATA_PORTS	Порты, через которые выполняется передача файлов	[\$HTTP_PORTS,110,143]
FTP_PORTS	Порты, используемые для соединения по протоколу FTP	21
HOME_NET	IP-адреса домашней (контролируемой) сети	[192.168.0.0/16,10.0.0.0/8,172.16.0.0/12]
HTTP_PORTS	Порты, используемые для HTTP-трафика	80
HTTP_SERVERS	Домашняя (контролируемая) сеть HTTP-серверов	\$HOME_NET
MODBUS_CLIENT	Домашняя (контролируемая) сеть клиентов протокола Modbus	\$HOME_NET
MODBUS_PORTS	Порты протокола Modbus	502
MODBUS_SERVER	Домашняя (контролируемая) сеть серверов Modbus	\$HOME_NET
ORACLE_PORTS	Порты для подключения к серверам Oracle	1521
PORT_VARIABLEA	Переменные для добавления пользовательского порта, предназначенного для определенных протоколов	!80
PORT_VARIABLEB		
PORT_VARIABLEC		
PORT_VARIABLED		
SHELLCODE_PORTS	Порты, на которых выполняется мониторинг попыток выполнения shell-кодов	!80

Табл. 25. Переменные службы обнаружения вторжений

ПЕРЕМЕННАЯ	ОПИСАНИЕ	ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ (ЖИРНЫМ), ЛИБО ПРИМЕР
SMTP_SERVERS	Домашняя (контролируемая) сеть SMTP-серверов	\$HOME_NET
SQL_SERVERS	Домашняя (контролируемая) сеть серверов баз данных SQL	\$HOME_NET
SSH_PORTS	Домашняя (контролируемая) сеть SSH-серверов	22
TELNET_SERVERS	Домашняя (контролируемая) сеть Telnet-серверов	\$HOME_NET

3.8.4. Рекомендации по использованию переменных файлов `manager.env` и `sensor.env`

Не все доступные для использования переменные, которые могут быть в файле `manager.env` или `sensor.env`, сразу находятся в нем. Некоторые из них необходимо вводить самостоятельно или раскомментировать.

При использовании переменных объема и времени рекомендуется использовать форматы, предложенные производителем Комплекса. Значительные отклонения от значений по умолчанию могут повлечь некорректную работу, недоступность системы или ее частей.

Соблюдение предложенного формата переменных объема обязательно. Варианты написания `10GB` или `10 Gb` некорректны и неизбежно повлекут за собой ошибки, так как в первом варианте написания отсутствует пробел, во втором варианте написания использованы символы в нижнем регистре.

Примеры корректных вариантов:

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

Список остальных рекомендаций приведен в таблице ниже.

Табл. 26. Рекомендации по использованию переменных файлов `manager.env` и `sensor.env`

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

3.9. Основные переменные файла environment.json

Список переменных, содержащийся в файле `environment.json`, вы можете видеть в таблице (Таблица 27. Переменные файла `environment.json`).

Файл `environment.json` расположен в директории `/usr/share/udv/frontend`.

Табл. 27. Переменные файла `environment.json`

ПЕРЕМЕННАЯ	ОПИСАНИЕ	ЗНАЧЕНИЕ ПО УМОЛЧАНИЮ
mainPage	Ссылка на стартовую страницу.	нет значения
showMaps	Доступ к странице Карта сети.	true
showKibanaEvents	Доступ к страницам Индексы и События→Экспертный режим.	
showCorrelation	Доступ к странице Правила корреляции.  Внимание: При значении переменной false доступ к странице Администрирование → События и инциденты → Оповещения об инцидентах запрещен вне зависимости от значения переменной showAlerting.	
showIncidentStatuses	Доступ к странице Статусы инцидентов.	
showIncidents	Доступ к странице Инциденты.	
showDataFlows	Доступ к страницам Инспекция сети → Потоки данных и Администрирование → События и инциденты → Правила корреляции.	
showSuricata	Доступ к странице Правила обнаружения.	
showAlerting	Доступ к странице Администрирование → События и инциденты → Оповещения об инцидентах.	
esperRetroEnabled	Доступ к странице События и инциденты → Ретроанализ.	

3.10. Отображение времени в Комплексе

Дата и время в Комплексе хранятся во временной зоне UTC, а при отображении в интерфейсе адаптируются под часовой пояс клиента. Это позволяет пользователям просматривать события и другую информацию в своем часовом поясе.

На страницах **Мониторинг** и **События** время отображается в соответствии со временем на АРМ пользователя. В случае расхождения времени между АРМ клиента и операционной системой Комплекса могут обнаруживаться несоответствия, при которых события отображаются «в будущем» или «в прошлом». Такое расхождение не следует принимать за сбой работы системы регистрации событий.

Подобное поведение также наблюдается при получении событий от актива, на котором некорректно настроено время. При сортировке по полю `create_time` такое событие может отображаться «в прошлом» или «в будущем» относительно событий, полученных в то же время.

3.11. Перечень данных, собираемых Комплексом

Табл. 28. Перечень данных, собираемых Комплексом

ТИП АКТИВА	ДАННЫЕ	ПРОТОКОЛ
Windows	События Security	RPC (WMI/MSEVEN)
Windows	События System	RPC (WMI/MSEVEN)
Windows	События Application	RPC (WMI/MSEVEN)
Windows	События Kaspersky Event Log	RPC (WMI/MSEVEN)
Windows	Список процессов	RPC (WMI/MSEVEN)
Windows	Список установленных обновлений	RPC (WMI/MSEVEN)
Windows	Список пользователей (локальные)	RPC (WMI/MSEVEN)
Windows	Список пользователей (все)	RPC (WMI/MSEVEN)
Windows	Список устройств	RPC (WMI/MSEVEN)
Windows	Список групп пользователей	RPC (WMI/MSEVEN)
Windows	Автозагрузка	RPC (WMI/MSEVEN)
Windows	Список служб (автозапуск)	RPC (WMI/MSEVEN)
Windows	Список служб	RPC (WMI/MSEVEN)
Windows	Список установленных обновлений	WinRM
Windows	Содержимое файла Hosts	WinRM
Windows	Содержимое файла Hosts	WinRM over HTTPS
Windows	Содержимое файла Hosts	WinEXE
Windows	Общие папки	WinRM
Windows	Сетевые порты в режиме «LISTENING»	WinRM
Windows	Сетевые порты в режиме «LISTENING»	WinRM over HTTPS
Windows	Сетевые порты в режиме «LISTENING»	WinEXE

Табл. 28. Перечень данных, собираемых Комплексом

ТИП АКТИВА	ДАННЫЕ	ПРОТОКОЛ
Windows	Список процессов с указанием пользователя	WinRM
Windows	Список процессов с указанием пользователя	WinRM over HTTPS
Windows	Список процессов с указанием пользователя	WinEXE
Windows	Параметры сетевых интерфейсов	WinRM
Windows	Параметры сетевых интерфейсов	WinRM over HTTPS
Windows	Параметры сетевых интерфейсов	WinEXE
Windows	ARP-таблица	WinRM
Windows	ARP-таблица	WinRM over HTTPS
Windows	ARP-таблица	WinEXE
Windows	Таблица маршрутизации	WinRM
Windows	Таблица маршрутизации	WinRM over HTTPS
Windows	Таблица маршрутизации	WinEXE
Windows	Установленное ПО (по ключам реестра)	WinRM
Windows	Версия Windows (ver)	WinRM
Windows	Версия Windows (ver)	WinRM over HTTPS
Windows	Версия Windows (ver)	WinEXE
Windows	Версия Windows (winver)	WinRM
Windows	Версия Windows (winver)	WinRM over HTTPS
Windows	Версия Windows (winver)	WinEXE
Windows	Имя актива	WinRM
Windows	Имя актива	WinRM over HTTPS
Windows	Имя актива	WinEXE

Табл. 28. Перечень данных, собираемых Комплексом

ТИП АКТИВА	ДАННЫЕ	ПРОТОКОЛ
Windows	Политика безопасности	WinRM
Windows	Настройки парольной политики	WinRM
Windows	Правила МЭ	WinRM
Windows	Правила МЭ	WinRM over HTTPS
Windows	Правила МЭ	WinEXE
Windows	Состояние МЭ	WinRM
Windows	Состояние МЭ	WinRM over HTTPS
Windows	Состояние МЭ	WinEXE
Windows	Настройки аудита	WinRM
UNIX	ARP-таблица	SSH
UNIX	Таблица маршрутизации	SSH
UNIX	Имя сетевого узла	SSH
UNIX	Подключенные носители информации	SSH
UNIX	Список пользователей	SSH
UNIX	Список групп пользователей и их членов	SSH
UNIX	Список процессов	SSH
UNIX	Список установленного ПО	SSH
UNIX	Содержимое файла /etc/sudoers	SSH
UNIX	Используемые DNS-серверы	SSH
UNIX	Содержимое файла /etc/hosts	SSH
UNIX	Сетевые порты в режиме LISTENING	SSH
UNIX	Правила межсетевого экрана iptables	SSH

Табл. 28. Перечень данных, собираемых Комплексом

ТИП АКТИВА	ДАННЫЕ	ПРОТОКОЛ
UNIX	Объекты автозапуска	SSH
UNIX	Контроль целостности критичных файлов (/etc/network/interfaces и др.)	SSH
Debian	Список включенных служб	SSH
Debian	Список сервисов	SSH
Debian	Установленное ПО	SSH
Debian	Список устройств	SSH
Debian	Контрольные суммы файлов конфигурации	SSH
QNX	Параметры DNS	SSH
QNX	Список групп	SSH
QNX	Сетевые порты в режиме прослушивания	SSH
QNX	Список пользователей	SSH
QNX	Файл hosts	SSH
RHEL	ARP-таблица	SSH
RHEL	Список служб	SSH
RHEL	Планировщик задач	SSH
RHEL	Параметры DNS	SSH
RHEL	Файл hosts	SSH
RHEL	Правила iptables	SSH
RHEL	Список sudoers	SSH
RHEL	Список групп	SSH
RHEL	Имя актива	SSH
RHEL	Подключенные носители информации	SSH

Табл. 28. Перечень данных, собираемых Комплексом

ТИП АКТИВА	ДАННЫЕ	ПРОТОКОЛ
RHEL	Список пользователей	SSH
RHEL	Сетевые порты в режиме прослушивания	SSH
RHEL	Список процессов	SSH
RHEL	Таблица маршрутизации	SSH
RHEL	Установленное ПО	SSH
RHEL	Список устройств	SSH
ACO Cisco IOS	Текущая конфигурация	SSH
ACO Cisco IOS	Начальная конфигурация	SSH
ACO Cisco IOS	ARP-таблица	SSH
ACO Cisco IOS	Таблица MAC-адресов	SSH
ACO Cisco IOS	Версия ОС	SSH
ACO HP	Текущая конфигурация	SSH
ACO HP	Начальная конфигурация	SSH
ACO HP	Версия ОС	SSH
ACO Cisco ASA	ARP-таблица	SSH
ACO Cisco ASA	Таблица маршрутизации	SSH
ACO Cisco ASA	Текущая конфигурация	SSH
ACO Cisco ASA	Стартовая конфигурация	SSH
ACO Cisco ASA	Версия ОС	SSH
ACO Hirschmann	ARP-таблица	SSH
ACO Hirschmann	Таблица MAC-адресов	SSH
ACO Hirschmann	Текущая конфигурация	SSH

Табл. 28. Перечень данных, собираемых Комплексом

ТИП АКТИВА	ДАННЫЕ	ПРОТОКОЛ
ACO Hirschmann	Версия ОС	SSH
ACO Comware	ARP-таблица	SSH
ACO Comware	Текущая конфигурация	SSH
ACO Comware	Таблица маршрутизации	SSH
ACO Comware	Таблица MAC-адресов	SSH
ACO Comware	Стартовая конфигурация	SSH
ACO Comware	Версия ОС	SSH
ACO Huawei	ARP-таблица	SSH
ACO Huawei	Таблица маршрутизации	SSH
ACO Huawei	Таблица MAC-адресов	SSH
ACO Huawei	Текущая конфигурация	SSH
ACO Huawei	Серийный номер	SSH
ACO Huawei	Стартовая конфигурация	SSH
ACO Huawei	Версия ОС	SSH
ACO Huawei	Параметры интерфейсов	SNMP
АСО/шлюзы/кон- вертеры MOXA	Таблица MAC-адресов	SSH
АСО/шлюзы/кон- вертеры MOXA	Текущая конфигурация	SSH
АСО/шлюзы/кон- вертеры MOXA	Стартовая конфигурация	SSH
АСО/шлюзы/кон- вертеры MOXA	Версия ОС	SSH
АСО/шлюзы/кон- вертеры MOXA	Параметры интерфейсов	SSH

Табл. 28. Перечень данных, собираемых Комплексом

ТИП АКТИВА	ДАННЫЕ	ПРОТОКОЛ
MSSQL	Список логинов	MSSQL
MSSQL	Список пользователей	MSSQL
MSSQL	Права пользователей	MSSQL
MySQL	Список пользователей	MySQL
MySQL	Права пользователей	MySQL
ALLEN BRADLEY Control Logix	Сбор конфигураций . • Сведения о : вендор, тип , код продукта, версия, серийный номер, наименование или модель и его версия, режим работы ; • Программа(проект) : контрольная сумма проекта, чтение проекта ; • Значения тегов, список тегов.	Ethernet/IP
Siemens	Сбор конфигураций (код заказа, версия ОС, тип модуля, наименование модуля, серийный номер, состояние , контрольные суммы, размер, дата последней модификации программных блоков)	S7comm
SCHNEIDER ELECTRIC	Сбор конфигураций . • Сведения о проекте: дата компиляции проекта, время компиляции проекта, версия проекта, имя проекта; • Сведения о : наименование, идентификатор, семейство , тип , версия firmware, идентификатор hardware; • Состояние : контрольная сумма проекта , статус ; • Программа(проект) .	Modbus
Прочие активы с поддержкой SNMP	Параметры из раздела System – обобщенные данные о системе (имя, время работы с момента последней перезагрузки);	SNMP
Прочие активы с поддержкой SNMP	Параметры из раздела Interfaces – данные о сетевых интерфейсах (статус, количество, типы, размер пакетов);	SNMP

Табл. 28. Перечень данных, собираемых Комплексом

ТИП АКТИВА	ДАННЫЕ	ПРОТОКОЛ
Прочие активы с поддержкой SNMP	Параметры из раздела TCP – данные протокола TCP (количество соединений, получено и отправлено пакетов, количество ошибок);	SNMP
Прочие активы с поддержкой SNMP	Параметры из раздела ICMP – данные протокола обмена управляющими сообщениями ICMP (количество сообщений получено и отправлено, количество ошибок и их виды);	SNMP
Прочие активы с поддержкой SNMP	Параметры из раздела EGP – протокол обмена информацией о состоянии маршрутизации (получено и отправлено пакетов, количество ошибок);	SNMP
Прочие активы с поддержкой SNMP	Параметры из раздела UDP – данные протокола UDP (получено и отправлено датаграмм, количество ошибок);	SNMP
Прочие активы с поддержкой SNMP	Параметры из раздела SNMP – статистика работы одноименного протокола (количество входящих и исходящих пакетов, обработано запросов, ошибки);	SNMP
Прочие активы с поддержкой SNMP	Параметры из раздела IP – данные о функционировании этого протокола (количество пакетов получено и отправлено, количество ошибок и их разновидности)	SNMP
ОВЕН	Сбор конфигураций ОВЕН: • сведения о проекте; • сведения о : тип , его текущее состояние, настройки, наличие парольной защиты	PLC-Browser

3.12. Протоколы, обнаруживаемые Комплексом

Комплекс способен обнаруживать самые разные данные в трафике активов. Эти данные используют множество протоколов, ознакомиться с которыми вы можете в таблице ниже ([Таблица 29. Список протоколов, обнаруживаемых Комплексом](#)).

Табл. 29. Список протоколов, обнаруживаемых Комплексом

НАИМЕНОВАНИЕ	ОПИСАНИЕ
ARP (Address Resolution Protocol)	Address Resolution Protocol (ARP) — протокол в компьютерных сетях, предназначенный для определения соответствия между MAC-адресом (физическим адресом устройства) и IP-адресом (логическим адресом сетевого уровня) удаленного компьютера. Является протоколом канального уровня модели OSI
BACnet IP	BACnet — протокол, применяемый в системах автоматизации зданий и сетях управления. Использует протоколы стандартов ASHRAE, ANSI и ISO 16484-5
Bitcoin Protocol	Bitcoin — протокол, используемый для осуществления транзакций пользователей криптовалюты
Bitmessage Protocol	Bitmessage — криптографический мессенджер с открытым исходным кодом, использующий децентрализованную P2P сеть
BitTorrent	BitTorrent — одноранговый (P2P) протокол обмена файлами. Файлы по такому протоколу передаются частями, а каждый torrent-клиент, получая эти части, в то же время отдает их другим клиентам. Быстрое распространение программ P2P на рабочих компьютерах представляет новые проблемы безопасности для корпоративных сетей, поскольку сеть P2P может использоваться для облегчения выполнения различных сетевых атак
Bristol Standard Asynchronous Protocol	Bristol Standard Asynchronous/Synchronous Protocol (BSAP) — протокол промышленной автоматизации, разработанный компанией Bristol Babcock и предназначенный для подключения, управления и мониторинга семейства Bristol Babcock Network 3000 и ControlWave, удаленных терминалов и контроллеров потока производства компании Emerson
Bristol Standard Asynchronous Protocol Serial version	Версия для протоколов последовательной передачи данных
BSAP CHANGE LOCAL NODE ADDR command	Команда на изменение локального адреса
BSAP DIAGNOSTICS RESET command	Команда сброса диагностических данных

Табл. 29. Список протоколов, обнаруживаемых Комплексом

НАИМЕНОВАНИЕ	ОПИСАНИЕ
BSAP Download Command	Команда загрузки
BSAP Enhanced Security Code Validation (Secure Mode – GET KEY)	Валидация кода безопасности (запрос ключа)
BSAP Enhanced Security Code Validation (Secure Mode – LOGIN REQUEST)	Валидация кода безопасности (запрос авторизации)
BSAP RBE Activation/Deactivation request	Команда включения/выключения сигналов RBE
BSAP RBE Going Active satate	Перевод RBE в активное состояние
BSAP RBE Initialisation request	Команда инициализации RBE
BSAP READ DATE AND TIME command	Команда на чтение даты и времени
BSAP READ DATE command	Команда на чтение даты
BSAP READ LOGICAL BY ADDRESS command	Команда чтения логических данных по адресу
BSAP READ LOGICAL BY LIST CONTINUE command	Команда на продолжение считывания логических данных по списку
BSAP READ LOGICAL BY LIST START command	Команда на начало считывания логических данных по списку
BSAP READ LOGICAL BY NAME command	Команда чтения логических данных по имени
BSAP READ SIGNAL BY ADDRESS command	Команда чтения сигналов по адресу
BSAP READ SIGNAL BY LIST CONTINUE command	Команда на продолжение считывания сигналов по списку
BSAP READ SIGNAL BY LIST START command	Команда на начало считывания сигналов по списку
BSAP READ SIGNAL BY NAME command	Команда чтения сигналов по имени

Табл. 29. Список протоколов, обнаруживаемых Комплексом

НАИМЕНОВАНИЕ	ОПИСАНИЕ
BSAP READ TIME command	Команда на чтение времени
BSAP RESET SYSTEM command	Команда сброса системы
BSAP Standard Security Code Validation (Simple Mode)	Валидация кода безопасности (простой режим)
BSAP WRITE DATE AND TIME command	Команда на изменение даты и времени
BSAP WRITE DATE command	Команда на изменение даты
BSAP WRITE SIGNAL BY ADDRESS command	Команда записи сигналов по адресу
BSAP WRITE SIGNAL BY LIST CONTINUE command	Команда на продолжение записи списка сигналов
BSAP WRITE SIGNAL BY LIST START command	Команда на начало записи списка сигналов
BSAP WRITE SIGNAL BY NAME command	Команда записи сигналов по имени
BSAP WRITE TIME command	Команда на изменение времени
Browser	Browser — протокол службы Microsoft Computer Browser, которая обеспечивает функционирование списков Windows-доменов, рабочих групп и компьютеров в масштабе всей сети, а также списков других сетевых аппаратных устройств, совместимых с протоколом NetBIOS. Она позволяет пользователям легко просматривать и находить общие ресурсы на компьютерах в одной подсети (но недоступна в сегментах сети, разделенных маршрутизаторами)
CPMI (Check Point Management Interface)	Check Point Management Interface (CPMI) — протокол CheckPoint, используемый для связи между SmartConsole и сервером управления безопасностью, а также протокол для подключений из многодоменного графического интерфейса пользователя к MDS и CMA/домену
Cisco loopback detection	Cisco loopback detection (LBD) — протокол для функции коммутаторов Cisco, обеспечивающей защиту от петель путем передачи пакетов данного протокола из портов, где включена защита петель. Когда коммутатор отправляет пакет протокола LBD, а затем получает тот

Табл. 29. Список протоколов, обнаруживаемых Комплексом

НАИМЕНОВАНИЕ	ОПИСАНИЕ
	же пакет, он закрывает порт, получивший пакет. LBD работает независимо от протокола STP (Spanning Tree Protocol)
CoDeSys PLC protocol	Протокол взаимодействия программного обеспечения CoDeSys с Wago
CoDeSys protocol CREATE APPLICATION command	Команда "создать приложение" протокола взаимодействия программного обеспечения CoDeSys с Wago
CoDeSys protocol CREATE DEVICE APPLICATION command	Команда "создать приложение на устройстве" протокола взаимодействия программного обеспечения CoDeSys с Wago
CoDeSys protocol DELETE APPLICATION command	Команда "удалить приложение" протокола взаимодействия программного обеспечения CoDeSys с Wago
CoDeSys protocol DEVICE DOWNLOAD command	Команда "загрузка данных об устройстве" протокола взаимодействия программного обеспечения CoDeSys с Wago
CoDeSys protocol DOWNLOAD command	Команда "загрузка программы в " протокола взаимодействия программного обеспечения CoDeSys с Wago
CoDeSys protocol LOGIN command	Команда "авторизация пользователя" протокола взаимодействия программного обеспечения CoDeSys с Wago
CoDeSys protocol LOGOUT command	Команда "выход пользователя из системы" протокола взаимодействия программного обеспечения CoDeSys с Wago
CoDeSys protocol ONLINE CHANGE command	Команда "изменить программу в режиме online" протокола взаимодействия программного обеспечения CoDeSys с Wago
CoDeSys protocol READ command	Команда "чтение данных" протокола взаимодействия программного обеспечения CoDeSys с Wago
CoDeSys protocol RESET command	Команда "сброс " протокола взаимодействия программного обеспечения CoDeSys с Wago
CoDeSys protocol SINGLE CYCLE command	Команда "выполнить один цикл " протокола взаимодействия программного обеспечения CoDeSys с Wago
CoDeSys protocol START command	Команда "запуск " протокола взаимодействия программного обеспечения CoDeSys с Wago
CoDeSys protocol STOP command	Команда "останов " протокола взаимодействия программного обеспечения CoDeSys с Wago

Табл. 29. Список протоколов, обнаруживаемых Комплексом

НАИМЕНОВАНИЕ	ОПИСАНИЕ
CoDeSys protocol WRITE command	Команда "запись данных" протокола взаимодействия программного обеспечения CoDeSys с Wago
ConnectionLess Network Protocol	Connection Less Network Protocol (CLNP) — дейтаграммный протокол передачи данных, который реализует в OSI-сетях задачи Connectionless-mode Network Service (сетевое обслуживание без установления соединения), сопоставимые с UDP в стеке IP
ControlEdge Builder Controller Configuration protocol	ControlEdge Builder Controller Configuration protocol — протокол конфигурирования контроллеров Honeywell ControlEdge
ControlEdge Discovery protocol	ControlEdge Builder Discovery protocol — протокол обнаружения Honeywell ControlEdge PLC и Honeywell ControlEdge RTU
COTP (Connection-Oriented Transport Protocol)	Connection Oriented Transport Protocol (COTP) — транспортный протокол соединения ISO ProtocolFamily, используется ICCP (Inter-Control Center Communications Protocol) для установления сеансов и обмена параметрами соединения. В большинстве приложений этот протокол был заменен на TCP
Dameware Remote Control	Dameware Mini Remote Control — протокол для взаимодействия с агентом Dameware на удаленном рабочем столе
DeltaV PLC protocol	DeltaV — проприетарный протокол связи с контроллерами Emerson DeltaV
Delta DVP PLC Run command	Команда протокола Modbus для перевода DELTA DVP в состояние RUN
Delta DVP PLC Stop command	Команда протокола Modbus для перевода DELTA DVP в состояние STOP
Digital Imaging and Communications in Medicine	DICOM — протокол, предназначенный для передачи медицинской информации от медицинского оборудования в системы передачи и архивации DICOM изображений (PACS) и для связи между PACS.
DICOM_ABORT	Сообщение об аварийном завершении работы протокола DICOM. DICOM — протокол, предназначенный для передачи медицинской информации от медицинского оборудования в системы передачи и архивации DICOM изображений (PACS) и для связи между PACS.
DICOM ASSOCIATE connection accept	Разрешение на установку соединения по протоколу DICOM. DICOM — протокол, предназначенный для передачи медицинской информации

Табл. 29. Список протоколов, обнаруживаемых Комплексом

НАИМЕНОВАНИЕ	ОПИСАНИЕ
	от медицинского оборудования в системы передачи и архивации DICOM изображений (PACS) и для связи между PACS.
DICOM ASSOCIATE connetcion reject	Отказ установки соединения по протоколу DICOM. DICOM — протокол, предназначенный для передачи медицинской информации от медицинского оборудования в системы передачи и архивации DICOM изображений (PACS) и для связи между PACS.
DICOM ASSOCIATE connetcion request	Запрос на установку соединения по протоколу DICOM. DICOM — протокол, предназначенный для передачи медицинской информации от медицинского оборудования в системы передачи и архивации DICOM изображений (PACS) и для связи между PACS.
DICOM C-FIND command	Команда "поиск" DICOM-элементов или DICOM-файлов пациентов на выбранном DICOM-устройстве протокола DICOM. DICOM — протокол, предназначенный для передачи медицинской информации от медицинского оборудования в системы передачи и архивации DICOM изображений (PACS) и для связи между PACS.
DICOM C-MOVE command	Команда "копировать" (перенести) DICOM-элементы или DICOM-файлы пациентов с одного DICOM-устройства на другое протокола DICOM. DICOM — протокол, предназначенный для передачи медицинской информации от медицинского оборудования в системы передачи и архивации DICOM изображений (PACS) и для связи между PACS.
DICOM DATA transfer	Пакет передачи данных по протоколу DICOM. DICOM — протокол, предназначенный для передачи медицинской информации от медицинского оборудования в системы передачи и архивации DICOM изображений (PACS) и для связи между PACS.
DICOM RELEASE request	Запрос разрыва соединения протокола DICOM. DICOM — протокол, предназначенный для передачи медицинской информации от медицинского оборудования в системы передачи и архивации DICOM изображений (PACS) и для связи между PACS.
DICOM RELEASE response	Подтверждение разрыва соединения протокола DICOM. DICOM — протокол, предназначенный для передачи медицинской информации от медицинского оборудования в системы передачи и архивации DICOM изображений (PACS) и для связи между PACS.
DirectLogix ECOM protocol	DirectLogix — проприетарный протокол для взаимодействия с DirectLogix через модули ECOM, разработанный компанией AutomationDirect

Табл. 29. Список протоколов, обнаруживаемых Комплексом

НАИМЕНОВАНИЕ	ОПИСАНИЕ
Distributed Network Protocol 3	Протокол, используемый для связи между компонентами ИС
DNP3 Cold Restart command	Пакеты DNP3, содержащие код функции для команды холодного перезапуска. DNP3 — протокол, используемый для связи между компонентами ИС.
DNP3 Disable Unsolicited command	Пакеты DNP3, содержащие код функции для команды запретить нежелательные сообщения. DNP3 — протокол, используемый для связи между компонентами ИС.
DNP3 Enable Unsolicited command	Пакеты DNP3, содержащие код функции для разрешения нежелательных сообщений. DNP3 — протокол, используемый для связи между компонентами ИС.
DNP3 Initialize Application command	Пакеты DNP3, содержащие код функции для команды инициализации приложения. DNP3 — протокол, используемый для связи между компонентами ИС.
DNP3 Initialize Data command	Пакеты DNP3, содержащие код функции для команды инициализации данных. DNP3 — протокол, используемый для связи между компонентами ИС.
DNP3 Response Broadcast Message	Пакеты DNP3, содержащие флаг широковещательное сообщение. DNP3 — протокол, используемый для связи между компонентами ИС.
DNP3 Response Device Restart	Пакеты DNP3, содержащие флаг перезапуска устройства. DNP3 — протокол, используемый для связи между компонентами ИС.
DNP3 Response Device Trouble	Пакеты DNP3, содержащие флаг ошибки устройства. DNP3 — протокол, используемый для связи между компонентами ИС.
DNP3 Response Digital Outputs In Local	Пакеты DNP3, содержащие флаг "дискретные выходы управляются локально". DNP3 — протокол, используемый для связи между компонентами ИС.
DNP3 Response Event Buffer Overflow	Пакеты DNP3, содержащие флаг переполнения буфера событий. DNP3 — протокол, используемый для связи между компонентами ИС.
DNP3 Response Function Code Not Supported	Пакеты DNP3, содержащие флаг "функция не поддерживается". DNP3 — протокол, используемый для связи между компонентами ИС.
DNP3 Response Object Unknown	Пакеты DNP3, содержащие флаг "объект неизвестен". DNP3 — протокол, используемый для связи между компонентами ИС.

Табл. 29. Список протоколов, обнаруживаемых Комплексом

НАИМЕНОВАНИЕ	ОПИСАНИЕ
DNP3 Response Operation Already Executing	Пакеты DNP3, содержащие флаг "операция в процессе выполнения". DNP3 — протокол, используемый для связи между компонентами ИС.
DNP3 Response Parameter Error	Пакеты DNP3, содержащие флаг "ошибка параметра". DNP3 — протокол, используемый для связи между компонентами ИС.
DNP3 Response Time Synchronization Required	Пакеты DNP3, содержащие флаг "требуется синхронизация времени". DNP3 — протокол, используемый для связи между компонентами ИС.
DNP3 Response Configuration corrupt	Пакеты DNP3, содержащие флаг ошибки конфигурации. DNP3 — протокол, используемый для связи между компонентами ИС.
DNP3 Save Configuration command	Пакеты DNP3, содержащие код функции для команды сохранения конфигурации. DNP3 — протокол, используемый для связи между компонентами ИС.
DNP3 Start Application command	Пакеты DNP3, содержащие код функции для команды запуска приложения. DNP3 — протокол, используемый для связи между компонентами ИС.
DNP3 Stop Application command	Пакеты DNP3, содержащие код функции для команды остановки приложения. DNP3 — протокол, используемый для связи между компонентами ИС.
DNP3 Warm Restart command	Пакеты DNP3, команда горячего перезапуска. DNP3 — протокол, используемый для связи между компонентами ИС.
DNS (Domain Name System)	Domain Name System (DNS) — протокол компьютерной распределенной системы для получения информации о доменах. Система чаще всего используется для получения IP-адреса по имени хоста (компьютера или устройства), получения информации о маршрутизации почты, обслуживающих узлах для протоколов в домене. Является частью Zeroconf — пакета технологий, который помогает сетевым устройствам находить друг друга автоматически
Dynamic Host Configuration Protocol	Dynamic Host Configuration Protocol (DHCP) — протокол управления сетью, используемый в сетях TCP/IP, для динамического присваивания каждому устройству коммутируемой сети IP-адреса и других параметров сетевой конфигурации для возможности их связи с другими IP-сетями. DHCP-сервер выполняет назначение уникальных динамических IP-адресов и соответствующих масок подсети и шлюзов по умолчанию для запущенных компьютеров в конкретной серверной сети.

Табл. 29. Список протоколов, обнаруживаемых Комплексом

НАИМЕНОВАНИЕ	ОПИСАНИЕ
Dynamic Host Configuration Protocol for IPv6	DHCPv6 — реализация протокола DHCP для IPv6
Emerson Data exchange protocol	Emerson Data exchange protocol — протокол обмена данными с устройствами Emerson
Encapsulated Remote Switch Packet Analysis	ERSPAN — технология компании Cisco, позволяющая отслеживать трафик между коммутаторами. Для копирования отслеживаемого сетевого трафика используется общая инкапсуляция маршрутов (Generic Routing Encapsulation, GRE)
Ethernet 802.3	Ethernet — технология пакетной передачи данных между устройствами для компьютерных и промышленных проводных локальных сетей
EthernetIP	EthernetIP — промышленный протокол Ethernet, обычно используемый для обмена данными между программируемыми контроллерами и системами человеко-машинного интерфейса. Разработан группой ODVA на основе коммуникационного протокола CIP (Common Interface Protocol)
EthernetIP Answer PLC reseted	Пакеты EthernetIP, содержащие ответ от на команду сброса
EthernetIP Answer PLC started	Пакеты EthernetIP, содержащие ответ от на команду запуска
EthernetIP Answer PLC stopped	Пакеты EthernetIP, содержащие ответ от на команду останова
EthernetIP CIP IO	EthernetIP — промышленный протокол Ethernet, обычно используемый для обмена данными между программируемыми контроллерами и системами человеко-машинного интерфейса. Разработан группой ODVA на основе коммуникационного протокола CIP (Common Interface Protocol).
EthernetIP CIP Request	Пакеты протокола EthernetIP, которые содержат запрос по протоколу CIP. EthernetIP — промышленный протокол Ethernet, обычно используемый для обмена данными между программируемыми контроллерами и системами человеко-машинного интерфейса. Разработан группой ODVA на основе коммуникационного протокола CIP (Common Interface Protocol).
EthernetIP CIP Response	Пакеты протокола EthernetIP, которые содержат ответ на запрос по протоколу CIP. EthernetIP — промышленный протокол Ethernet, обычно используемый для обмена данными между программируемыми контроллерами и системами человеко-машинного интерфейса. Раз-

Табл. 29. Список протоколов, обнаруживаемых Комплексом

НАИМЕНОВАНИЕ	ОПИСАНИЕ
	работан группой ODVA на основе коммуникационного протокола CIP (Common Interface Protocol).
EthernetIP Create Request	Пакеты протокола EthernetIP, которые содержат запрос на создание атрибута. EthernetIP — промышленный протокол Ethernet, обычно используемый для обмена данными между программируемыми контроллерами и системами человеко-машинного интерфейса. Разработан группой ODVA на основе коммуникационного протокола CIP (Common Interface Protocol).
EthernetIP Create Response	Пакеты протокола EthernetIP, которые содержат ответ на запрос создания атрибута. EthernetIP — промышленный протокол Ethernet, обычно используемый для обмена данными между программируемыми контроллерами и системами человеко-машинного интерфейса. Разработан группой ODVA на основе коммуникационного протокола CIP (Common Interface Protocol).
EthernetIP Delete Request	Пакеты протокола EthernetIP, которые содержат запрос удаления атрибута. EthernetIP — промышленный протокол Ethernet, обычно используемый для обмена данными между программируемыми контроллерами и системами человеко-машинного интерфейса. Разработан группой ODVA на основе коммуникационного протокола CIP (Common Interface Protocol).
EthernetIP Delete Response	Пакеты протокола EthernetIP, которые содержат ответ на запрос удаления атрибута. EthernetIP — промышленный протокол Ethernet, обычно используемый для обмена данными между программируемыми контроллерами и системами человеко-машинного интерфейса. Разработан группой ODVA на основе коммуникационного протокола CIP (Common Interface Protocol).
EthernetIP Download	Пакеты EthernetIP, содержащие код функции для загрузки программы в
EthernetIP Forward Close Connection Request	Пакеты протокола EthernetIP, которые содержат запрос команды "Forward Close". EthernetIP — промышленный протокол Ethernet, обычно используемый для обмена данными между программируемыми контроллерами и системами человеко-машинного интерфейса. Разработан группой ODVA на основе коммуникационного протокола CIP (Common Interface Protocol).
EthernetIP Forward Close Connection Response	Пакеты протокола EthernetIP, которые содержат ответ на запрос команды "Forward Close". EthernetIP — промышленный протокол Ethernet, обычно используемый для обмена данными между програм-

Табл. 29. Список протоколов, обнаруживаемых Комплексом

НАИМЕНОВАНИЕ	ОПИСАНИЕ
	мируемыми контроллерами и системами человеко-машинного интерфейса. Разработан группой ODVA на основе коммуникационного протокола CIP (Common Interface Protocol).
EthernetIP Forward Open Connection Request	Пакеты протокола EthernetIP, которые содержат запрос команды "Forward Open". EthernetIP — промышленный протокол Ethernet, обычно используемый для обмена данными между программируемыми контроллерами и системами человеко-машинного интерфейса. Разработан группой ODVA на основе коммуникационного протокола CIP (Common Interface Protocol).
EthernetIP Forward Open Connection Response	Пакеты протокола EthernetIP, которые содержат ответ на запрос команды "Forward Open". EthernetIP — промышленный протокол Ethernet, обычно используемый для обмена данными между программируемыми контроллерами и системами человеко-машинного интерфейса. Разработан группой ODVA на основе коммуникационного протокола CIP (Common Interface Protocol).
EthernetIP Get Attribute All Request	Пакеты протокола EthernetIP, которые содержат запрос всех атрибутов. EthernetIP — промышленный протокол Ethernet, обычно используемый для обмена данными между программируемыми контроллерами и системами человеко-машинного интерфейса. Разработан группой ODVA на основе коммуникационного протокола CIP (Common Interface Protocol).
EthernetIP Get Attribute All Response	Пакеты протокола EthernetIP, которые содержат ответ на запрос всех атрибутов. EthernetIP — промышленный протокол Ethernet, обычно используемый для обмена данными между программируемыми контроллерами и системами человеко-машинного интерфейса. Разработан группой ODVA на основе коммуникационного протокола CIP (Common Interface Protocol).
EthernetIP Get Attribute List Request	Пакеты протокола EthernetIP, которые содержат запрос списка атрибутов. EthernetIP — промышленный протокол Ethernet, обычно используемый для обмена данными между программируемыми контроллерами и системами человеко-машинного интерфейса. Разработан группой ODVA на основе коммуникационного протокола CIP (Common Interface Protocol).
EthernetIP Get Attribute List Response	Пакеты протокола EthernetIP, которые содержат ответ на запрос списка атрибутов. EthernetIP — промышленный протокол Ethernet, обычно используемый для обмена данными между программируемыми контроллерами и системами человеко-машинного ин-

Табл. 29. Список протоколов, обнаруживаемых Комплексом

НАИМЕНОВАНИЕ	ОПИСАНИЕ
	терфейса. Разработан группой ODVA на основе коммуникационного протокола CIP (Common Interface Protocol).
EthernetIP Get Attribute Single Request	Пакеты протокола EthernetIP, которые содержат запрос одного из атрибутов. EthernetIP – промышленный протокол Ethernet, обычно используемый для обмена данными между программируемыми контроллерами и системами человеко-машинного интерфейса. Разработан группой ODVA на основе коммуникационного протокола CIP (Common Interface Protocol).
EthernetIP Get Attribute Single Response	Пакеты протокола EthernetIP, которые содержат ответ на запрос одного атрибута. EthernetIP – промышленный протокол Ethernet, обычно используемый для обмена данными между программируемыми контроллерами и системами человеко-машинного интерфейса. Разработан группой ODVA на основе коммуникационного протокола CIP (Common Interface Protocol).
EthernetIP Get Instance Attribute List Request	Пакеты протокола EthernetIP, которые содержат запрос списка атрибутов экземпляра. EthernetIP – промышленный протокол Ethernet, обычно используемый для обмена данными между программируемыми контроллерами и системами человеко-машинного интерфейса. Разработан группой ODVA на основе коммуникационного протокола CIP (Common Interface Protocol).
EthernetIP Get Instance Attribute List Response	Пакеты протокола EthernetIP, которые содержат ответ на запрос списка атрибутов экземпляра. EthernetIP – промышленный протокол Ethernet, обычно используемый для обмена данными между программируемыми контроллерами и системами человеко-машинного интерфейса. Разработан группой ODVA на основе коммуникационного протокола CIP (Common Interface Protocol).
EthernetIP HMI Read Tag Request	Пакеты протокола EthernetIP, которые содержат запрос из HMI/SCADA на чтение тегов. EthernetIP – промышленный протокол Ethernet, обычно используемый для обмена данными между программируемыми контроллерами и системами человеко-машинного интерфейса. Разработан группой ODVA на основе коммуникационного протокола CIP (Common Interface Protocol).
EthernetIP List Identity request/response command	Пакеты протокола EthernetIP, которые содержат команду запроса списка идентификаторов устройства. EthernetIP – промышленный протокол Ethernet, обычно используемый для обмена данными между программируемыми контроллерами и системами человеко-ма-

Табл. 29. Список протоколов, обнаруживаемых Комплексом

НАИМЕНОВАНИЕ	ОПИСАНИЕ
	шинного интерфейса. Разработан группой ODVA на основе коммуникационного протокола CIP (Common Interface Protocol).
EthernetIP List Interface request/response command	Пакеты протокола EthernetIP, которые содержат команду запроса списка интерфейсов устройства. EthernetIP — промышленный протокол Ethernet, обычно используемый для обмена данными между программируемыми контроллерами и системами человеко-машинного интерфейса. Разработан группой ODVA на основе коммуникационного протокола CIP (Common Interface Protocol).
EthernetIP List Services request/response command	Пакеты протокола EthernetIP, которые содержат команду запроса списка сервисов устройства. EthernetIP — промышленный протокол Ethernet, обычно используемый для обмена данными между программируемыми контроллерами и системами человеко-машинного интерфейса. Разработан группой ODVA на основе коммуникационного протокола CIP (Common Interface Protocol).
EthernetIP Multiple Service Request	Пакеты протокола EthernetIP, которые содержат список запросов команд. EthernetIP — промышленный протокол Ethernet, обычно используемый для обмена данными между программируемыми контроллерами и системами человеко-машинного интерфейса. Разработан группой ODVA на основе коммуникационного протокола CIP (Common Interface Protocol).
EthernetIP Multiple Service Response	>Пакеты протокола EthernetIP, которые содержат список ответов на запросы команд. EthernetIP — промышленный протокол Ethernet, обычно используемый для обмена данными между программируемыми контроллерами и системами человеко-машинного интерфейса. Разработан группой ODVA на основе коммуникационного протокола CIP (Common Interface Protocol).
EthernetIP Read Fragment Request	Пакеты протокола EthernetIP, которые содержат запрос чтения фрагмента данных. EthernetIP — промышленный протокол Ethernet, обычно используемый для обмена данными между программируемыми контроллерами и системами человеко-машинного интерфейса. Разработан группой ODVA на основе коммуникационного протокола CIP (Common Interface Protocol).
EthernetIP Read Modify Write Service Request	Пакеты протокола EthernetIP, которые содержат запрос чтения, изменения или записи фрагмента данных. EthernetIP — промышленный протокол Ethernet, обычно используемый для обмена данными между программируемыми контроллерами и системами человеко-ма-

Табл. 29. Список протоколов, обнаруживаемых Комплексом

НАИМЕНОВАНИЕ	ОПИСАНИЕ
	шинного интерфейса. Разработан группой ODVA на основе коммуникационного протокола CIP (Common Interface Protocol).
EthernetIP Read Modify Write Service Response	Пакеты протокола EthernetIP, которые содержат ответ на запрос чтения/изменения/записи фрагмента данных. EthernetIP — промышленный протокол Ethernet, обычно используемый для обмена данными между программируемыми контроллерами и системами человеко-машинного интерфейса. Разработан группой ODVA на основе коммуникационного протокола CIP (Common Interface Protocol).
EthernetIP Read Modify Write Tag Service Request	Пакеты протокола EthernetIP, которые содержат запрос чтения, изменения или записи фрагмента тега. EthernetIP — промышленный протокол Ethernet, обычно используемый для обмена данными между программируемыми контроллерами и системами человеко-машинного интерфейса. Разработан группой ODVA на основе коммуникационного протокола CIP (Common Interface Protocol).
EthernetIP Read Request	Пакеты протокола EthernetIP, которые содержат запрос чтения данных. EthernetIP — промышленный протокол Ethernet, обычно используемый для обмена данными между программируемыми контроллерами и системами человеко-машинного интерфейса. Разработан группой ODVA на основе коммуникационного протокола CIP (Common Interface Protocol).
EthernetIP Read Response	Пакеты протокола EthernetIP, которые содержат ответ на запрос чтения данных. EthernetIP — промышленный протокол Ethernet, обычно используемый для обмена данными между программируемыми контроллерами и системами человеко-машинного интерфейса. Разработан группой ODVA на основе коммуникационного протокола CIP (Common Interface Protocol).
EthernetIP Read Tag Fragment Request	Пакеты протокола EthernetIP, которые содержат запрос чтения фрагмента тега. EthernetIP — промышленный протокол Ethernet, обычно используемый для обмена данными между программируемыми контроллерами и системами человеко-машинного интерфейса. Разработан группой ODVA на основе коммуникационного протокола CIP (Common Interface Protocol).
EthernetIP Read Tag Fragment Response	Пакеты протокола EthernetIP, которые содержат ответ на запрос чтения фрагмента данных. EthernetIP — промышленный протокол Ethernet, обычно используемый для обмена данными между программируемыми контроллерами и системами человеко-машинного ин-

Табл. 29. Список протоколов, обнаруживаемых Комплексом

НАИМЕНОВАНИЕ	ОПИСАНИЕ
	терфейса. Разработан группой ODVA на основе коммуникационного протокола CIP (Common Interface Protocol).
EthernetIP Read Tag Request	Пакеты протокола EthernetIP, которые содержат запрос чтения тегов. EthernetIP – промышленный протокол Ethernet, обычно используемый для обмена данными между программируемыми контроллерами и системами человеко-машинного интерфейса. Разработан группой ODVA на основе коммуникационного протокола CIP (Common Interface Protocol).
EthernetIP Register Session request/ response command	Пакеты протокола EthernetIP, которые содержат команду запроса регистрации сессии. EthernetIP – промышленный протокол Ethernet, обычно используемый для обмена данными между программируемыми контроллерами и системами человеко-машинного интерфейса. Разработан группой ODVA на основе коммуникационного протокола CIP (Common Interface Protocol).
EthernetIP Reset command	Пакеты EthernetIP, содержащие код функции для сброса. EthernetIP – промышленный протокол передачи данных, используемый для взаимодействия с компании Rockwell Automation.
EthernetIP RSlogix5000 Online Change Request	Пакеты протокола EthernetIP, которые содержат запрос на изменение программы в процессе работы. EthernetIP – промышленный протокол Ethernet, обычно используемый для обмена данными между программируемыми контроллерами и системами человеко-машинного интерфейса. Разработан группой ODVA на основе коммуникационного протокола CIP (Common Interface Protocol).
EthernetIP RSlogix5000 Service Request	Пакеты протокола EthernetIP, которые содержат сервисные запросы ПО RSlogix5000. EthernetIP – промышленный протокол Ethernet, обычно используемый для обмена данными между программируемыми контроллерами и системами человеко-машинного интерфейса. Разработан группой ODVA на основе коммуникационного протокола CIP (Common Interface Protocol).
EthernetIP RSlogix5000 Service Response	Пакеты протокола EthernetIP, которые содержат ответ на сервисные запросы ПО RSlogix5000. EthernetIP – промышленный протокол Ethernet, обычно используемый для обмена данными между программируемыми контроллерами и системами человеко-машинного интерфейса. Разработан группой ODVA на основе коммуникационного протокола CIP (Common Interface Protocol).
EthernetIP Set Attribute All Request	Пакеты протокола EthernetIP, которые содержат запрос установления значений всех атрибутов. EthernetIP – промышленный протокол

Табл. 29. Список протоколов, обнаруживаемых Комплексом

НАИМЕНОВАНИЕ	ОПИСАНИЕ
	Ethernet, обычно используемый для обмена данными между программируемыми контроллерами и системами человеко-машинного интерфейса. Разработан группой ODVA на основе коммуникационного протокола CIP (Common Interface Protocol).
EthernetIP Set Attribute All Response	Пакеты протокола EthernetIP, которые содержат ответ на запрос установления значений всех атрибутов. EthernetIP — промышленный протокол Ethernet, обычно используемый для обмена данными между программируемыми контроллерами и системами человеко-машинного интерфейса. Разработан группой ODVA на основе коммуникационного протокола CIP (Common Interface Protocol).
EthernetIP Set Attribute List Request	Пакеты протокола EthernetIP, которые содержат запрос установления значений списка атрибутов. EthernetIP — промышленный протокол Ethernet, обычно используемый для обмена данными между программируемыми контроллерами и системами человеко-машинного интерфейса. Разработан группой ODVA на основе коммуникационного протокола CIP (Common Interface Protocol).
EthernetIP Set Attribute List Response	Пакеты протокола EthernetIP, которые содержат ответ на запрос установления значений списка атрибутов. EthernetIP — промышленный протокол Ethernet, обычно используемый для обмена данными между программируемыми контроллерами и системами человеко-машинного интерфейса. Разработан группой ODVA на основе коммуникационного протокола CIP (Common Interface Protocol).
EthernetIP Set Attribute Single Request	Пакеты протокола EthernetIP, которые содержат запрос установления значений одного атрибута. EthernetIP — промышленный протокол Ethernet, обычно используемый для обмена данными между программируемыми контроллерами и системами человеко-машинного интерфейса. Разработан группой ODVA на основе коммуникационного протокола CIP (Common Interface Protocol).
EthernetIP Set Attribute Single Response	Пакеты протокола EthernetIP, которые содержат ответ на запрос установления значений одного атрибута. EthernetIP — промышленный протокол Ethernet, обычно используемый для обмена данными между программируемыми контроллерами и системами человеко-машинного интерфейса. Разработан группой ODVA на основе коммуникационного протокола CIP (Common Interface Protocol).
EthernetIP Set Password	Пакеты EthernetIP, содержащие код операции для установки или изменения пароля. EthernetIP — промышленный протокол передачи

Табл. 29. Список протоколов, обнаруживаемых Комплексом

НАИМЕНОВАНИЕ	ОПИСАНИЕ
	данных, используемый для взаимодействия с компании Rockwell Automation.
EthernetIP Start command	Пакеты EthernetIP, содержащие код функции для запуска . EthernetIP – промышленный протокол передачи данных, используемый для взаимодействия с компании Rockwell Automation.
EthernetIP Stop command	Пакеты EthernetIP, содержащие код функции для останова . EthernetIP – промышленный протокол передачи данных, используемый для взаимодействия с компании Rockwell Automation.
EthernetIP T3 connected msg	Пакеты протокола EthernetIP, формата SendUnitData. EthernetIP – промышленный протокол Ethernet, обычно используемый для обмена данными между программируемыми контроллерами и системами человеко-машинного интерфейса. Разработан группой ODVA на основе коммуникационного протокола CIP (Common Interface Protocol).
EthernetIP unconnected msg	Пакеты протокола EthernetIP, формата SendRRData. EthernetIP – промышленный протокол Ethernet, обычно используемый для обмена данными между программируемыми контроллерами и системами человеко-машинного интерфейса. Разработан группой ODVA на основе коммуникационного протокола CIP (Common Interface Protocol).
EthernetIP Unregister Session request/ response command	Пакеты протокола EthernetIP, которые содержат команду запроса окончания сессии. EthernetIP – промышленный протокол Ethernet, обычно используемый для обмена данными между программируемыми контроллерами и системами человеко-машинного интерфейса. Разработан группой ODVA на основе коммуникационного протокола CIP (Common Interface Protocol).
EthernetIP Unsecure PLC	Пакеты протокола EthernetIP, содержащие код операции для снятия защиты с . EthernetIP – промышленный протокол передачи данных, используемый для взаимодействия с компании Rockwell Automation.
EthernetIP Upload	Пакеты EthernetIP, содержащие код функции для выгрузки программы из
EthernetIP Write Fragment Request	Пакеты протокола EthernetIP, которые содержат запрос записи фрагмента данных. EthernetIP – промышленный протокол Ethernet, обычно используемый для обмена данными между программируемыми контроллерами и системами человеко-машинного интерфейса. Разработан группой ODVA на основе коммуникационного протокола CIP (Common Interface Protocol).

Табл. 29. Список протоколов, обнаруживаемых Комплексом

НАИМЕНОВАНИЕ	ОПИСАНИЕ
EthernetIP Write Request	Пакеты протокола EthernetIP, которые содержат запрос записи данных. EthernetIP — промышленный протокол Ethernet, обычно используемый для обмена данными между программируемыми контроллерами и системами человеко-машинного интерфейса. Разработан группой ODVA на основе коммуникационного протокола CIP (Common Interface Protocol).
EthernetIP Write Response	Пакеты протокола EthernetIP, которые содержат ответ на запрос записи данных. EthernetIP — промышленный протокол Ethernet, обычно используемый для обмена данными между программируемыми контроллерами и системами человеко-машинного интерфейса. Разработан группой ODVA на основе коммуникационного протокола CIP (Common Interface Protocol).
EthernetIP Write Tag Fragment Request	Пакеты протокола EthernetIP, которые содержат запрос записи фрагмента тега. EthernetIP — промышленный протокол Ethernet, обычно используемый для обмена данными между программируемыми контроллерами и системами человеко-машинного интерфейса. Разработан группой ODVA на основе коммуникационного протокола CIP (Common Interface Protocol).
EthernetIP Write Tag Fragment Response	Пакеты протокола EthernetIP, которые содержат ответ на запрос записи фрагмента данных. EthernetIP — промышленный протокол Ethernet, обычно используемый для обмена данными между программируемыми контроллерами и системами человеко-машинного интерфейса. Разработан группой ODVA на основе коммуникационного протокола CIP (Common Interface Protocol).
EthernetIP Write Tag Request	Пакеты протокола EthernetIP, которые содержат запрос записи значения тега. EthernetIP — промышленный протокол Ethernet, обычно используемый для обмена данными между программируемыми контроллерами и системами человеко-машинного интерфейса. Разработан группой ODVA на основе коммуникационного протокола CIP (Common Interface Protocol).
FTP (File Transfer Protocol) — Control connection	File Transfer Protocol (FTP) — стандартный протокол передачи файлов по сети. Формально FTP подразумевает подключение к определенной папке, которая находится на сервере
General Electric Global Data	Ethernet Global Data (EGD) — протокол, предназначенный для передачи данных между GE Fanuc и другими компонентами автоматизированных систем: приводами, HMI, SCADA, иными. EGD позволяет источнику данных (серверу) предоставить доступ потре-

Табл. 29. Список протоколов, обнаруживаемых Комплексом

НАИМЕНОВАНИЕ	ОПИСАНИЕ
	бителям (клиентам) к областям его памяти с заданным периодом времени
Generic Routing Encapsulation	GRE (Generic Routing Encapsulation — общая инкапсуляция маршрутов) — протокол туннелирования сетевых пакетов, разработанный компанией Cisco Systems. Его основное назначение — инкапсуляция пакетов сетевого уровня сетевой модели OSI в IP-пакеты
GE-SRTP (General Electric Service Request Transport Protocol)	General Electric Service Request Transport Protocol (GE-SRTP) — протокол, разработанный компанией GE Fanuc и предназначенный для обмена данными между GE Fanuc. Применяется через Ethernet. Протокол GE-SRTP поддерживается практически всем оборудованием автоматизации, произведенным компанией GE и оснащенным портами Ethernet. Чтение и запись в системную память любого количества удаленных устройств, поддерживающих протокол SRTP, может осуществляться любым клиентом SRTP.
GE-SRTP change PLC CPU Privilege Level command	Пакеты протокола GE-SRTP, которые содержат код операции для изменения уровня привилегий ЦПУ. GE-SRTP — протокол для обмена данными между GE Fanuc.
GE-SRTP download to PLC command	Пакеты протокола GE-SRTP, которые содержат код операции для загрузки программы в. GE-SRTP — протокол для обмена данными между GE Fanuc.
GE-SRTP logon command	Пакеты протокола GE-SRTP, которые содержат код операции для авторизации пользователей. GE-SRTP — протокол для обмена данными между GE Fanuc.
GE-SRTP read program memory command	Пакеты протокола GE-SRTP, которые содержат код операции для чтения программной памяти. GE-SRTP — протокол для обмена данными между GE Fanuc.
GE-SRTP set control ID (CPU ID) command	Пакеты протокола GE-SRTP, которые содержат код операции для назначения контрольного идентификатора (Идентификатора ЦПУ). GE-SRTP — протокол для обмена данными между GE Fanuc.
GE-SRTP set PLC (run vs stop) command	Пакеты протокола GE-SRTP, которые содержат код операции для настройки (запуск или остановка). GE-SRTP — протокол для обмена данными между GE Fanuc.
GE-SRTP upload from PLC command	Пакеты протокола GE-SRTP, которые содержат код операции для выгрузки программ из. GE-SRTP — протокол для обмена данными между GE Fanuc.

Табл. 29. Список протоколов, обнаруживаемых Комплексом

НАИМЕНОВАНИЕ	ОПИСАНИЕ
GE-SRTP write program memory command	Пакеты протокола GE-SRTP, которые содержат код операции записи памяти программ. GE-SRTP – протокол для обмена данными между GE Fanuc.
Graylog	Graylog – протокол для взаимодействия с ПО компании Graylog, предназначенного для централизованного сбора, хранения и анализа данных о различных событиях в журналах на серверах локальной сети
Haiwell PLC connect	Haiwell PLC connect – протокол подключения среды разработки к ПЛК Haiwell
Haiwell PLC diagnostics	Haiwell PLC diagnostics – протокол сбора данных с ПЛК Haiwell
Haiwell PLC password change	Haiwell PLC password change – протокол смены пароля ПЛК Haiwell
Haiwell PLC project clear	Haiwell PLC project clear – протокол удаление текущей программы из ПЛК Haiwell
Haiwell PLC project download	Haiwell PLC project download (PC to PLC) – протокол загрузки проекта на ПЛК Haiwell
Haiwell PLC project upload	Haiwell PLC project upload (PLC to PC) – протокол выгрузки проекта из ПЛК Haiwell
Haiwell PLC set parameters	Haiwell PLC set parameters – протокол изменения параметров ПЛК Haiwell
Honeywell C300 Data Exchange protocol	Honeywell C300 Data Exchange – протокол для обмена информацией в контроллерах Honeywell C300
Honeywell C300 Information protocol	Honeywell C300 Information – протокол для передачи сведений о контроллерах Honeywell C300
HTTP (Hyper Text Transfer Protocol)	Hypertext Transfer Protocol (HTTP) – протокол прикладного уровня передачи данных для передачи гипертекстовых документов, таких как HTML. В первую очередь он используется для связи между веб-браузерами и веб-серверами, но также может использоваться и для других целей. Протокол работает на основе классической клиент-серверной модели, когда клиент открывает соединение для создания запроса, а затем ждет ответа. Клиенты и серверы взаимодействуют, обмениваясь одиночными сообщениями

Табл. 29. Список протоколов, обнаруживаемых Комплексом

НАИМЕНОВАНИЕ	ОПИСАНИЕ
Huawei loopback detection	Протокол 2 уровня, используемый в коммутаторах Huawei для обнаружения петель в сети
ICMP (Internet Control Message Protocol)	Internet Control Message Protocol (ICMP) — межсетевой протокол управляющих сообщений. Используется сетевыми устройствами для отправки запросов или сообщений об ошибках и других исключительных ситуациях, возникших при передаче данных. Обычно применяется для диагностики проблем со связностью в сети (помогает определить, может ли достичь пакет адреса назначения в установленные временные рамки).
ICMP debug	Пакеты группы Debug протокола ICMP, которые содержат в поле тип одно из значений: • 0 (echo reply); • 8 (echo); • 13 (timestamp); • 14 (timestamp reply). Стандартные пакеты, которые постоянно используются для отладки сети. Internet Control Message Protocol (ICMP) — межсетевой протокол управляющих сообщений. Используется сетевыми устройствами для отправки запросов или сообщений об ошибках и других исключительных ситуациях, возникших при передаче данных. Обычно применяется для диагностики проблем со связностью в сети (помогает определить, может ли достичь пакет адреса назначения в установленные временные рамки).
ICMP extra	Пакеты группы Extra протокола ICMP, не относящиеся к группам host_error, route_error, net_error, debug или suspicious. Internet Control Message Protocol (ICMP) — межсетевой протокол управляющих сообщений. Используется сетевыми устройствами для отправки запросов или сообщений об ошибках и других исключительных ситуациях, возникших при передаче данных. Обычно применяется для диагностики проблем со связностью в сети (помогает определить, может ли достичь пакет адреса назначения в установленные временные рамки).
ICMP host error	Пакеты группы Host-error протокола ICMP с типом 3 (адресат недоступен), которые содержат одно из следующих сообщений: • 2 (протокол недостижим); • 3 (порт недостижим).

Табл. 29. Список протоколов, обнаруживаемых Комплексом

НАИМЕНОВАНИЕ	ОПИСАНИЕ
	Данные пакеты предупреждают о возможной проблеме на хосте-получателе
ICMP net error	Net-error – пакеты ICMP с типом 4 (Сдерживание источника, отключение источника при переполнении очереди) или 12 (Неверный параметр, проблема с параметрами дейтаграммы: ошибка в IP-заголовке или отсутствует необходимая опция), предупреждающие о проблеме в сети
ICMP route error	Route_error – пакеты ICMP с типом 3 (Адресат недоступен), содержащие одно из сообщений: 0 («Сеть недостижима»), 1 («Узел недостижим»), 4 («Необходима фрагментация, но установлен флаг DF ее запрета»), или 5 («Неверный маршрут от источника»), либо пакеты ICMP с типом 11 (Время жизни дейтаграммы истекло), содержащие одно из сообщений: 0 («Время жизни пакета (TTL) истекло при транспортировке») или 1 («Время жизни пакета истекло при сборке фрагментов»). Данные пакеты предупреждают о возможной проблеме маршрутизации в сети
ICMP suspicious	Suspicious – пакеты ICMP с типом 5 (Перенаправление), 15 (Информационный запрос – устаревший тип) или 16 (Информационный ответ – устаревший тип). Появление такого пакета ICMP с высокой вероятностью является признаком компьютерной атаки
ICMPv6 (Internet Control Message Protocol version 6)	ICMPv6 – реализация протокола ICMP для IPv6
ICPDAS MiniOS7 Utility protocol	ICPDAS protocol – протокол, предназначенный для связи с ICPDAS, работающими на операционной системе MiniOS7.
ICPDAS bios1 command	Команда обновления операционной системы MiniOS7 (второй шаг, запись файла в FLASH память). ICPDAS protocol – протокол, предназначенный для связи с ICPDAS, работающими на операционной системе MiniOS7.
ICPDAS research command	Команда поиска ICPDAS в сети. ICPDAS protocol – протокол, предназначенный для связи с ICPDAS, работающими на операционной системе MiniOS7.
ICPDAS reset command	Команда перезагрузки системы MiniOS7. ICPDAS protocol – протокол, предназначенный для связи с ICPDAS, работающими на операционной системе MiniOS7.

Табл. 29. Список протоколов, обнаруживаемых Комплексом

НАИМЕНОВАНИЕ	ОПИСАНИЕ
ICPDAS upload command	Команда обновления операционной системы MiniOS7 (первый шаг, загрузка файла в SRAM). ICPDAS protocol — протокол, предназначенный для связи с ICPDAS, работающими на операционной системе MiniOS7.
IEC 60870-5-104	IEC 60870-5-104 — протокол стандарта IEC 60870-5 для оборудования и систем телеуправления, который обеспечивает профиль связи для отправки базовых сообщений телеуправления между системами в электротехнике и автоматизации энергосистем
IEC 60870-5-104 insert command	Команда insert
IEC 60870-5-104 insert off command	Команда insert off
IEC 60870-5-104 put command	Команда put
IEC 60870-5-104 put reverse command	Команда put reverse
IEC104 change value command	Команда change value
IEC104 insert command	Команда insert
IEC104 insert off command	Команда insert off
IEC104 put command	Команда put
IEC104 put reverse command	Команда put reverse
IEC 61850/GOOSE	GOOSE (Generic Object-Oriented Substation Event) — протокол стандарта МЭК 61850, предназначенный для обмена дискретными данными между терминалами релейной защиты и автоматики (РЗА) посредством передачи данных в цифровом виде по Ethernet
IEC 61850/MMS	MMS (Manufacturing Message Specification) — протокол передачи данных по технологии «клиент-сервер» стандарта МЭК 61850, предназначенный для передачи данных от терминалов релейной защиты и автоматики (РЗА) в SCADA систему для дальнейшей визуализации
IEC 61850/MMS Confirmed Response PDU	Пакеты протокола IEC61850 MMS, которые содержат ответ на запрос в формате "Confirmed RequestPDU". IEC 61850 (стандарт для сетей передачи данных и систем подстанций) — стандарт, который определяет протокол MMS как клиент-серверный тип передачи данных. Этот протокол используется для информационного обмена между интеллектуальными электронными устройствами (IED) и более высокоуровневыми устройствами (н-р SCADA) по Ethernet. Протокол MMS

Табл. 29. Список протоколов, обнаруживаемых Комплексом

НАИМЕНОВАНИЕ	ОПИСАНИЕ
	определяется по TCP/IP и предоставляет доступ к серверу, где клиент может читать и записывать данные, считывать конфигурации и обмениваться файлами.
IEC 61850/MMS Confirmed ResponsePDU read command	Пакеты протокола IEC61850 MMS, которые содержат ответ на запрос чтения данных. IEC 61850 (стандарт для сетей передачи данных и систем подстанций) — стандарт, который определяет протокол MMS как клиент-серверный тип передачи данных. Этот протокол используется для информационного обмена между интеллектуальными электронными устройствами (IED) и более высокоуровневыми устройствами (н-р SCADA) по Ethernet. Протокол MMS определяется по TCP/IP и предоставляет доступ к серверу, где клиент может читать и записывать данные, считывать конфигурации и обмениваться файлами.
IEC 61850/MMS Confirmed ResponsePDU write command	Пакеты протокола IEC61850 MMS, которые содержат ответ на запрос записи данных. IEC 61850 (стандарт для сетей передачи данных и систем подстанций) — стандарт, который определяет протокол MMS как клиент-серверный тип передачи данных. Этот протокол используется для информационного обмена между интеллектуальными электронными устройствами (IED) и более высокоуровневыми устройствами (н-р SCADA) по Ethernet. Протокол MMS определяется по TCP/IP и предоставляет доступ к серверу, где клиент может читать и записывать данные, считывать конфигурации и обмениваться файлами.
IEC 61850/MMS Confirmed Request delete Program Invocation command	Пакеты протокола IEC61850 MMS, которые содержат запрос на удаление программы. IEC 61850 (стандарт для сетей передачи данных и систем подстанций) — стандарт, который определяет протокол MMS как клиент-серверный тип передачи данных. Этот протокол используется для информационного обмена между интеллектуальными электронными устройствами (IED) и более высокоуровневыми устройствами (н-р SCADA) по Ethernet. Протокол MMS определяется по TCP/IP и предоставляет доступ к серверу, где клиент может читать и записывать данные, считывать конфигурации и обмениваться файлами.
IEC 61850/MMS Confirmed Request Download command	Пакеты протокола IEC61850 MMS, которые содержат запрос передачи контента домена, включая любые подчиненные объекты, посредством загрузки данных MMS-пользователю. IEC 61850 (стандарт для сетей передачи данных и систем подстанций) — стандарт, который определяет протокол MMS как клиент-серверный тип передачи данных. Этот протокол используется для информационного обмена между интеллектуальными электронными устройствами (IED) и более высокоуровневыми устройствами (н-р SCADA) по Ethernet. Протокол MMS определяется по TCP/IP и предоставляет доступ к

Табл. 29. Список протоколов, обнаруживаемых Комплексом

НАИМЕНОВАНИЕ	ОПИСАНИЕ
	серверу, где клиент может читать и записывать данные, считывать конфигурации и обмениваться файлами.
IEC 61850/MMS Confirmed Request GetNameList command	Пакеты протокола IEC61850 MMS, которые содержат запрос списка имен. IEC 61850 (стандарт для сетей передачи данных и систем подстанций) — стандарт, который определяет протокол MMS как клиент-серверный тип передачи данных. Этот протокол используется для информационного обмена между интеллектуальными электронными устройствами (IED) и более высокоуровневыми устройствами (н-р SCADA) по Ethernet. Протокол MMS определяется по TCP/IP и предоставляет доступ к серверу, где клиент может читать и записывать данные, считывать конфигурации и обмениваться файлами.
IEC 61850/MMS Confirmed Request GetNamedVariableListAttributes command	Пакеты протокола IEC61850 MMS, которые содержат запрос чтения списка атрибутов. IEC 61850 (стандарт для сетей передачи данных и систем подстанций) — стандарт, который определяет протокол MMS как клиент-серверный тип передачи данных. Этот протокол используется для информационного обмена между интеллектуальными электронными устройствами (IED) и более высокоуровневыми устройствами (н-р SCADA) по Ethernet. Протокол MMS определяется по TCP/IP и предоставляет доступ к серверу, где клиент может читать и записывать данные, считывать конфигурации и обмениваться файлами.
IEC 61850/MMS Confirmed Request Identify command	Пакеты протокола IEC61850 MMS, которые содержат запрос идентификатора устройства. IEC 61850 (стандарт для сетей передачи данных и систем подстанций) — стандарт, который определяет протокол MMS как клиент-серверный тип передачи данных. Этот протокол используется для информационного обмена между интеллектуальными электронными устройствами (IED) и более высокоуровневыми устройствами (н-р SCADA) по Ethernet. Протокол MMS определяется по TCP/IP и предоставляет доступ к серверу, где клиент может читать и записывать данные, считывать конфигурации и обмениваться файлами.
IEC 61850/MMS Confirmed Request Kill command	Пакеты протокола IEC61850 MMS, которые содержат команду уничтожения. IEC 61850 (стандарт для сетей передачи данных и систем подстанций) — стандарт, который определяет протокол MMS как клиент-серверный тип передачи данных. Этот протокол используется для информационного обмена между интеллектуальными электронными устройствами (IED) и более высокоуровневыми устройствами (н-р SCADA) по Ethernet. Протокол MMS определяется по TCP/IP и предоставляет доступ к серверу, где клиент может читать и записывать данные, считывать конфигурации и обмениваться файлами.

Табл. 29. Список протоколов, обнаруживаемых Комплексом

НАИМЕНОВАНИЕ	ОПИСАНИЕ
IEC 61850/MMS Confirmed Request PDU	Пакеты протокола IEC 61850 MMS, которые содержат запрос в формате "Confirmed RequestPDU". IEC 61850 (стандарт для сетей передачи данных и систем подстанций) — стандарт, который определяет протокол MMS как клиент-серверный тип передачи данных. Этот протокол используется для информационного обмена между интеллектуальными электронными устройствами (IED) и более высокоуровневыми устройствами (н-р SCADA) по Ethernet. Протокол MMS определяется по TCP/IP и предоставляет доступ к серверу, где клиент может читать и записывать данные, считывать конфигурации и обмениваться файлами.
IEC 61850/MMS Confirmed Request read command	Пакеты протокола IEC61850 MMS, которые содержат запрос чтения данных. IEC 61850 (стандарт для сетей передачи данных и систем подстанций) — стандарт, который определяет протокол MMS как клиент-серверный тип передачи данных. Этот протокол используется для информационного обмена между интеллектуальными электронными устройствами (IED) и более высокоуровневыми устройствами (н-р SCADA) по Ethernet. Протокол MMS определяется по TCP/IP и предоставляет доступ к серверу, где клиент может читать и записывать данные, считывать конфигурации и обмениваться файлами.
IEC 61850/MMS Confirmed Request Rename command	Пакеты протокола IEC61850 MMS, которые содержат запрос изменения имени. IEC 61850 (стандарт для сетей передачи данных и систем подстанций) — стандарт, который определяет протокол MMS как клиент-серверный тип передачи данных. Этот протокол используется для информационного обмена между интеллектуальными электронными устройствами (IED) и более высокоуровневыми устройствами (н-р SCADA) по Ethernet. Протокол MMS определяется по TCP/IP и предоставляет доступ к серверу, где клиент может читать и записывать данные, считывать конфигурации и обмениваться файлами.
IEC 61850/MMS Confirmed Request Reset command	Пакеты протокола IEC61850 MMS, которые содержат команду сброса. IEC 61850 (стандарт для сетей передачи данных и систем подстанций) — стандарт, который определяет протокол MMS как клиент-серверный тип передачи данных. Этот протокол используется для информационного обмена между интеллектуальными электронными устройствами (IED) и более высокоуровневыми устройствами (н-р SCADA) по Ethernet. Протокол MMS определяется по TCP/IP и предоставляет доступ к серверу, где клиент может читать и записывать данные, считывать конфигурации и обмениваться файлами.
IEC 61850/MMS Confirmed Request Resume command	Пакеты протокола IEC61850 MMS, которые содержат команду возобновления работы. IEC 61850 (стандарт для сетей передачи данных

Табл. 29. Список протоколов, обнаруживаемых Комплексом

НАИМЕНОВАНИЕ	ОПИСАНИЕ
	и систем подстанций) — стандарт, который определяет протокол MMS как клиент-серверный тип передачи данных. Этот протокол используется для информационного обмена между интеллектуальными электронными устройствами (IED) и более высокоуровневыми устройствами (н-р SCADA) по Ethernet. Протокол MMS определяется по TCP/IP и предоставляет доступ к серверу, где клиент может читать и записывать данные, считывать конфигурации и обмениваться файлами.
IEC 61850/MMS Confirmed Request Start command	Пакеты протокола IEC61850 MMS, которые содержат команду запуска. IEC 61850 (стандарт для сетей передачи данных и систем подстанций) — стандарт, который определяет протокол MMS как клиент-серверный тип передачи данных. Этот протокол используется для информационного обмена между интеллектуальными электронными устройствами (IED) и более высокоуровневыми устройствами (н-р SCADA) по Ethernet. Протокол MMS определяется по TCP/IP и предоставляет доступ к серверу, где клиент может читать и записывать данные, считывать конфигурации и обмениваться файлами.
IEC 61850/MMS Confirmed Request Stop command	Пакеты протокола IEC61850 MMS, которые содержат команду останова. IEC 61850 (стандарт для сетей передачи данных и систем подстанций) — стандарт, который определяет протокол MMS как клиент-серверный тип передачи данных. Этот протокол используется для информационного обмена между интеллектуальными электронными устройствами (IED) и более высокоуровневыми устройствами (н-р SCADA) по Ethernet. Протокол MMS определяется по TCP/IP и предоставляет доступ к серверу, где клиент может читать и записывать данные, считывать конфигурации и обмениваться файлами.
IEC 61850/MMS Confirmed Request status command	Пакеты протокола IEC 61850 MMS, которые содержат запрос статуса устройства. IEC 61850 (стандарт для сетей передачи данных и систем подстанций) — стандарт, который определяет протокол MMS как клиент-серверный тип передачи данных. Этот протокол используется для информационного обмена между интеллектуальными электронными устройствами (IED) и более высокоуровневыми устройствами (н-р SCADA) по Ethernet. Протокол MMS определяется по TCP/IP и предоставляет доступ к серверу, где клиент может читать и записывать данные, считывать конфигурации и обмениваться файлами.
IEC 61850/MMS Confirmed Request Upload command	Пакеты протокола IEC61850 MMS, которые содержат запрос передачи контента домена, включая любые подчиненные объекты, посредством загрузки данных от удаленного пользователя. IEC 61850 (стандарт для сетей передачи данных и систем подстанций) — стандарт, который определяет протокол MMS как клиент-серверный тип передачи данных. Этот протокол используется для информа-

Табл. 29. Список протоколов, обнаруживаемых Комплексом

НАИМЕНОВАНИЕ	ОПИСАНИЕ
	ционного обмена между интеллектуальными электронными устройствами (IED) и более высокоуровневыми устройствами (н-р SCADA) по Ethernet. Протокол MMS определяется по TCP/IP и предоставляет доступ к серверу, где клиент может читать и записывать данные, считывать конфигурации и обмениваться файлами.
IEC 61850/MMS Confirmed Request Write command	Пакеты протокола IEC61850 MMS, которые содержат запрос записи данных. IEC 61850 (стандарт для сетей передачи данных и систем подстанций) — стандарт, который определяет протокол MMS как клиент-серверный тип передачи данных. Этот протокол используется для информационного обмена между интеллектуальными электронными устройствами (IED) и более высокоуровневыми устройствами (н-р SCADA) по Ethernet. Протокол MMS определяется по TCP/IP и предоставляет доступ к серверу, где клиент может читать и записывать данные, считывать конфигурации и обмениваться файлами.
IEEE 802.2 Logical Link Control	IEEE 802.2 Logical Link Control (LLC) — протокол управления логическим каналом. По стандарту IEEE 802 — это верхний подуровень канального уровня модели OSI, который осуществляет управление передачей данных и обеспечивает проверку и правильность передачи информации по соединению
IEEE 802.2 Logical Link Control SNAP	IEEE 802.2 Logical Link Control Subnetwork Access Protocol (SNAP) — протокол доступа к подсети, который используется для инкапсуляции дейтаграмм IP и запросов ARP в сетях IEEE 802. Дейтаграммы IP передаются в сетях IEEE 802 инкапсулированными в 802.2 LLC и канальный уровень SNAP, а также в физические уровни 802.3, 802.4 и 802.5
IGMP	Internet Group Management Protocol (IGMP) — протокол сетевого уровня для управления групповой передачей данных в сетях, основанных на протоколе IP. IGMP используется маршрутизаторами и IP-узлами для организации сетевых устройств в группы. Используется только при взаимодействии связанных друг с другом маршрутизатора и хоста, который выступает или желает выступить в роли получателя трафика группового вещания
IMAP	IMAP — протокол прикладного уровня для доступа к электронной почте
Internet Group Management Protocol	Internet Group Management Protocol (IGMP) — протокол сетевого уровня для управления групповой передачей данных в сетях, основанных на протоколе IP. IGMP используется маршрутизаторами и IP-узлами для организации сетевых устройств в группы. Используется только при взаимодействии связанных друг с другом маршрутизатора и хоста,

Табл. 29. Список протоколов, обнаруживаемых Комплексом

НАИМЕНОВАНИЕ	ОПИСАНИЕ
	который выступает или желает выступать в роли получателя трафика группового вещания
Internet Message Access Protocol	IMAP протокол прикладного уровня для доступа к электронной почте
Internet Relay Chat Protocol	IRC — протокол прикладного уровня для обмена сообщениями в режиме реального времени
IP (Internet Protocol)	Internet Protocol (IP) — маршрутизируемый протокол сетевого уровня (по сетевой модели OSI) стека TCP/IP. Это протокол или набор правил для маршрутизации и адресации пакетов данных, чтобы они могли перемещаться по сети и достигать правильного пункта назначения. IP объединяет сегменты сети в единую сеть, обеспечивая доставку пакетов данных между любыми узлами сети через произвольное число промежуточных узлов (маршрутизаторов)
IPv4 (Internet Protocol version 4)	Internet Protocol version 4 (IPv4) — в протоколе IP этой версии каждому узлу сети ставится в соответствие IP-адрес длиной 4 октета (4 байта). При этом компьютеры в подсетях объединяются общими начальными битами адреса. Количество этих бит, общее для данной подсети, называется маской подсети
IPv6 (Internet Protocol version 6)	Internet Protocol version 6 (IPv6) — новая версия интернет-протокола (IP), призванная решить проблемы предыдущей версии (IPv4) при ее использовании в Интернете (исчерпание IPv4 адресов) и обеспечить дополнительные возможности (поддержку огромных пакетов — джамбограмм, многоадресное вещание и др.)
IPX (Internetwork Packet Exchange)	IPX (Internetwork Packet Exchange) — протокол сетевого уровня модели OSI в стеке протоколов IPX/SPX, предназначенный для передачи дейтаграмм (без установления соединения) от одного процесса к другому
IRC	IRC — протокол прикладного уровня для обмена сообщениями в режиме реального времени
ISO 8327-1 OSI Session Protocol	ISO 8327 — базовый протокол сеансового уровня, ориентированный на соединение. Протокол устанавливает, управляет и завершает соединение между локальными и удаленными приложениями. Также управляет безопасностью соединения, использует приостановку/возобновление для синхронизации аудио и видео
ISO 8823 OSI Presentation	ISO 8823 — протокол уровня представления данных, ориентированный на соединение. Применяется для кодирования и декодирования данных. Поддерживает синтаксис однократной передачи данных и

Табл. 29. Список протоколов, обнаруживаемых Комплексом

НАИМЕНОВАНИЕ	ОПИСАНИЕ
	базовые правила кодирования (BER). Другие синтаксисы передачи данных будут отклонены при попытке соединения
JavaScript Object Notation Remote Procedure Call	JSON-RPC — протокол удаленного вызова процедур, использующий JSON для кодирования сообщений
JSON-RPC	JSON-RPC — протокол удаленного вызова процедур, использующий JSON для кодирования сообщений
Kaspersky Security Center	Протокол, используемый Kaspersky Security Center для управления клиентскими устройствами и подчиненными Серверами администрирования. Легитимный протокол
Lightweight Directory Access Protocol (LDAP)	Lightweight Directory Access Protocol (LDAP) — протокол прикладного уровня для доступа к службе каталогов X.500, разработанный сообществом IETF. Позволяет производить операции аутентификации, поиска и сравнения, а также операции добавления, изменения или удаления записей службы
Link Layer Discovery Protocol (LLDP)	Link Layer Discovery Protocol (LLDP) — протокол канального уровня, который позволяет сетевым устройствам анонсировать в сеть информацию о себе и о своих возможностях, а также собирать эту информацию о соседних устройствах. Это стандартный протокол, который описан в стандарте IEEE 802.1AB
Link-local Multicast Name Resolution (LLMNR)	Link-Local Multicast Name Resolution (LLMNR) — протокол легковесной службы имен LLMNR, использующей группу абонентов (multicast group) для поиска и преобразования базовых имен в пределах одной подсети для IPv4, IPv6 или обоих видов адресов сразу без обращения к серверам. Аналог NetBIOS Name Service. Используется в сетях, где применение DNS-сервера либо неудобно, либо невозможно
MC Protocol for Mitsubishi PLC binary	MC Protocol — открытый протокол, предназначенный для связи с устройствами MELSOFT компании MITSUBISHI ELECTRIC
MDLC	Message Data Link Controller или Motorola Data Link Communication (MDLC) — протокол, базирующийся на 7-уровневой модели OSI, опубликованной Международной организацией по стандартизации, адаптированный компанией Motorola для систем SCADA и передачи данных по радиоканалу
MDLC RTU to RTU	MDLC RTU to RTU — вариант протокола MDLC для передачи базы данных, локального состояния и измерений от одного RTU сети другому

Табл. 29. Список протоколов, обнаруживаемых Комплексом

НАИМЕНОВАНИЕ	ОПИСАНИЕ
MDLC RTU to SCADA	MDLC RTU to SCADA — вариант протокола MDLC для передачи базы данных, локального состояния и измерений от одного RTU сети к SCADA путем эмуляции SCADA-протоколов.
Media Redundancy Protocol	MRP — это стандартный протокол, используемый в кольцевых топологиях, позволяет избежать отказов точек, обеспечивая время восстановления 10 мс или меньше
MELSOFT connection for Mitsubishi PLC	MELSOFT connection — проприетарный протокол, предназначенный для связи между устройствами и программным обеспечением MELSOFT компании MITSUBISHI ELECTRIC
Message Queue Telemetry Transport	MQTT — упрощенный сетевой протокол, ориентированный на обмен сообщениями между устройствами по принципу издатель-подписчик
Microsoft Windows Browser Protocol	Browser — протокол службы Microsoft Computer Browser, которая обеспечивает функционирование списков Windows-доменов, рабочих групп и компьютеров в масштабе всей сети, а также списков других сетевых аппаратных устройств, совместимых с протоколом NetBIOS. Она позволяет пользователям легко просматривать и находить общие ресурсы на компьютерах в одной подсети (но недоступна в сегментах сети, разделенных маршрутизаторами)
Mitsubishi FX2N PLC protocol	Mitsubishi FX2N — проприетарный протокол для связи с FX2N MITSUBISHI ELECTRIC
Mitsubishi PLC REMOTE Latch Clear command	Команда удаленной очистки памяти MITSUBISHI ELECTRIC
Mitsubishi PLC REMOTE Logon command	Команда авторизации пользователя MITSUBISHI ELECTRIC
Mitsubishi PLC REMOTE PAUSE command	Команда удаленного перевода MITSUBISHI ELECTRIC в состояние PAUSE
Mitsubishi PLC REMOTE RESET command	Команда удаленного сброса MITSUBISHI ELECTRIC
Mitsubishi PLC REMOTE RUN command	Команда удаленного перевода MITSUBISHI ELECTRIC в состояние RUN
Mitsubishi PLC REMOTE STOP command	Команда удаленного перевода MITSUBISHI ELECTRIC в состояние STOP

Табл. 29. Список протоколов, обнаруживаемых Комплексом

НАИМЕНОВАНИЕ	ОПИСАНИЕ
MMS	MMS (Manufacturing Message Specification) — протокол передачи данных по технологии «клиент-сервер» стандарта МЭК 61850, предназначенный для передачи данных от терминалов релейной защиты и автоматики (РЗА) в SCADA-систему для дальнейшей визуализации
Modbus	Modbus — открытый коммуникационный протокол, часто встречающийся в сетях SCADA и применяемый в промышленности для организации связи между электронными устройствами на основе архитектуры «ведущий — ведомый» («master-slave»). Необходимо оценивать легитимность указанного потока
Modbus RTU over TCP	Протокол Modbus RTU через TCP/IP. Обычно используется серверами последовательных интерфейсов, где может быть расположен клиент Modbus Ethernet, связывающийся с несколькими ведомыми устройствами Modbus RTU-RS485 через сервер. Последовательный сервер удаляет секцию Ethernet и пересылает сообщение Modbus RTU на последовательный порт
Modbus/TCP operational	TCP-протокол Modbus
Modbus/TCP programming	Пакеты Modbus TCP, содержащие зарезервированные коды функций
Modbus/TCP Response Error	Ответы Modbus TCP, содержащие ошибки выполнения Modbus-запросов
Motorola Data Link Communication (MDLC)	Message Data Link Controller/Motorola Data Link Communication (MDLC) — протокол, базирующийся на 7-уровневой модели OSI, опубликованной Международной организацией по стандартизации, адаптированный компанией Motorola для систем SCADA и передачи данных по радиоканалу
Motorola MDLC RTU to RTU	MDLC RTU to RTU — вариант протокола MDLC для передачи базы данных, локального состояния и измерений от одного RTU сети другому
Motorola MDLC RTU to SCADA	MDLC RTU to SCADA — вариант протокола MDLC для передачи базы данных, локального состояния и измерений от одного RTU сети к SCADA путем эмуляции SCADA-протоколов
Moxa MXconfig Broadcast Search	Мокса MXconfig Broadcast Search — широковещательный поиск устройств Мокса из ПО MXconfig

Табл. 29. Список протоколов, обнаруживаемых Комплексом

НАИМЕНОВАНИЕ	ОПИСАНИЕ
MQTT	MQTT — упрощенный сетевой протокол, ориентированный на обмен сообщениями между устройствами по принципу «издатель-подписчик»
MRP	MRP — протокол, используемый в кольцевых топологиях; позволяет избежать отказов точек, обеспечивая время восстановления 10 мс или меньше
Multicast DNS	Multicast DNS (mDNS) — многоадресная (multicast) версия протокола DNS (запросы рассылаются всем устройствам широковещательного домена). Domain Name System (DNS) — протокол компьютерной распределенной системы для получения информации о доменах. Система чаще всего используется для получения IP-адреса по имени хоста (компьютера или устройства), получения информации о маршрутизации почты, обслуживающих узлах для протоколов в домене. Является частью Zeroconf — пакета технологий, который помогает сетевым устройствам находить друг друга автоматически
MySQL Protocol	MySQL — протокол для взаимодействия с СУБД MySQL
Network Basic Input/Output System (NetBIOS)	Network Basic Input/Output System (NetBIOS) — протокол сетевого уровня для обнаружения компьютеров в сети, построенной на базе TCP/IP. Особенностью является возможность его работы поверх разных протоколов (NetBEUI, IPX, стек протоколов TCP/IP)
Netbios Datagram Service	NetBIOS Datagram Services (NETBIOS-DGM) — протокол службы рассылки дейтаграмм NetBIOS (для связи без установления соединения). Этот сервис обеспечивает: персональный запрос к одной станции, широковещательный запрос ко всем станциям, запрос к станциям с одним групповым именем
NetBIOS over IPX	NetBIOS over IPX — протокол NetBIOS, использующий протокол IPX в качестве транспорта
NetBIOS over LLC	NetBIOS over LLC — протокол NetBIOS, использующий протокол LLC в качестве транспорта
NetBios Session Service	NetBIOS-SSN — протокол службы сеанса NetBIOS (для связи с установлением соединения). Служба позволяет двум компьютерам устанавливать соединение, позволяет сообщениям охватывать несколько пакетов и обеспечивает обнаружение и восстановление ошибок
Network Dynamic Data Exchange	Network Dynamic Data Exchange (NetDDE) — протокол механизма Network DDE, предназначенный для динамического взаимодействия

Табл. 29. Список протоколов, обнаруживаемых Комплексом

НАИМЕНОВАНИЕ	ОПИСАНИЕ
	приложений в операционных системах Microsoft Windows и OS/2, выполняющихся на разных компьютерах в сети
Network File System	NFS — протокол, используемый для получения сетевого доступа к файлам сети
Network File System v2	В NFSv2 отсутствуют данные о внутреннем состоянии внутри протокола
Network File System v2 or v3 on rpc	Определяются как NFSv2, так и NFSv3 с использованием протокола удаленного вызова процедур (RPC)
Network File System v3	В NFSv3 добавлена поддержка дескрипторов файлов переменного размера до 64 байт, снято ограничение на 8192 байта в RPC-вызовах чтения и записи, реализована поддержка файлов больших размеров, добавлена поддержка асинхронных вызовов операций записи, к процедурам READ и WRITE добавлены вызовы ACCESS, MKNOD, REaddirPLUS, FSINFO, FSSTAT, PATHCONF и COMMIT
Network File System v4	NFSv4 отличается улучшенными по сравнению с предыдущей версией параметрами производительности и безопасности
Network Time protocol	Network Time Protocol (NTP) — протокол для синхронизации времени внутренних системных часов компьютера. В NTP время передается от одной системы к другой с использованием сетевого протокола UDP
NXLog	NXLog — протокол для взаимодействия с ПО NXLog, предназначенного для централизованного сбора, хранения и анализа данных о различных событиях в журналах на серверах локальной сети
OLE for Process Control Data Access OR DCOM	Distributed Component Object Model (DCOM) — протокол стандарта OPC DA, описывающий набор функций обмена данными в реальном времени между серверами и различными промышленными устройствами (, PCU, ЧМИ, ЧПУ и др.). OPC — это семейство программных технологий, предоставляющих единый интерфейс для управления объектами автоматизации и технологическими процессами
OMRON FINS Protocol	OMRON FINS — открытый протокол компании OMRON для взаимодействия с контроллерами разработки компании Omron
OPC Unified Architecture	Унифицированная архитектура OPC — это спецификация OPC, определяющая передачу данных в промышленных сетях и взаимодействие устройств в них

Табл. 29. Список протоколов, обнаруживаемых Комплексом

НАИМЕНОВАНИЕ	ОПИСАНИЕ
OWEN_PLC_Protocol	Протокол обмена данными между Овен и ПО CoDeSys
OWEN PLC Browser command	Запрос данных при помощи утилиты -Браузер протокола обмена данными между Овен и ПО CoDeSys
OWEN PLC Browser Delete password command	Команда «Удалить пароль», отправленная при помощи утилиты -Браузер протокола обмена данными между Овен и ПО CoDeSys
OWEN PLC Browser Set password command	Команда «Установить пароль», отправленная при помощи утилиты -Браузер протокола обмена данными между Овен и ПО CoDeSys
OWEN PLC Browser Start program command	Команда «Запуск программы », отправленная при помощи утилиты -Браузер протокола обмена данными между Овен и ПО CoDeSys
OWEN PLC Browser Stop program command	Команда «Остановка программы », отправленная при помощи утилиты -Браузер протокола обмена данными между Овен и ПО CoDeSys
OWEN PLC Cold Read command	Команда «Чтение данных из » протокола обмена данными между Овен и ПО CoDeSys
OWEN PLC Cold Reset command	Команда «Сброс (холодный) » протокола обмена данными между Овен и ПО CoDeSys
OWEN PLC Cold Write command	Команда «Запись данных в » протокола обмена данными между Овен и ПО CoDeSys
OWEN PLC Download command	Команда «Загрузка программы в » протокола обмена данными между Овен и ПО CoDeSys
OWEN PLC Download full command	Команда «Полная загрузка программы в » протокола обмена данными между Овен и ПО CoDeSys
OWEN PLC Factory Reset command	Команда «Сброс (заводской) » протокола обмена данными между Овен и ПО CoDeSys
OWEN PLC One Shot command	Команда «Выполнить один цикл» протокола обмена данными между Овен и ПО CoDeSys
OWEN PLC Read File from PLC command	Команда «Читать файл из » протокола обмена данными между Овен и ПО CoDeSys
OWEN PLC Reset command	Команда «Сброс » протокола обмена данными между Овен и ПО CoDeSys

Табл. 29. Список протоколов, обнаруживаемых Комплексом

НАИМЕНОВАНИЕ	ОПИСАНИЕ
OWEN PLC Start command	Команда «Старт » протокола обмена данными между Овен и ПО CoDeSys
OWEN PLC Stop command	Команда «Стоп » протокола обмена данными между Овен и ПО CoDeSys
OWEN PLC Write File to PLC command	Команда «Записать файл в » протокола обмена данными между Овен и ПО CoDeSys
Post Office Protocol Version 3	POP3 — стандартный интернет-протокол прикладного уровня, используемый клиентами электронной почты для получения почты с удаленного сервера по TCP-соединению
PostgreSQL	PGSQL — протокол для взаимодействия с СУБД PostgreSQL
Precision Time Protocol (PTP)	Precision Time Protocol (PTP) — протокол синхронизации времени по сети Ethernet для устройств, требующих высокой точности временной синхронизации.
Precision Time Protocol Event Messages	Пакеты категории «события» протокола PTP, используемые для расчета задержки соединения на основе меток времени
Precision Time Protocol General Messages	Пакеты категории «общие» протокола PTP, используемые для установления иерархии «клиент-сервер» и не требующие меток времени. Precision Time Protocol (PTP) — протокол синхронизации времени по сети Ethernet для устройств, требующих высокой точности временной синхронизации.
Precision Time Protocol over Ethernet	Протокол PTP версии 2 и выше, использующий в качестве транспортного протокол Ethernet. Precision Time Protocol (PTP) — протокол синхронизации времени по сети Ethernet для устройств, требующих высокой точности временной синхронизации.
Precision Time Protocol version 1	Версия 1 протокола PTP, использующий в качестве транспортного протокол UDP
Precision Time Protocol version 2	Версия 2 протокола PTP, использующий в качестве транспортного протокол UDP. Precision Time Protocol (PTP) — протокол синхронизации времени по сети Ethernet для устройств, требующих высокой точности временной синхронизации.
PROFINET	PROFINET — стандарт промышленных сетей в области автоматизации — один из двух открытых стандартных протоколов автоматизации

Табл. 29. Список протоколов, обнаруживаемых Комплексом

НАИМЕНОВАНИЕ	ОПИСАНИЕ
	Ethernet от Profibus International. Обмен данными ввода/вывода реализован поверх Ethernet
Profinet IO	PROFINET IO — один из двух открытых стандартных протоколов автоматизации Ethernet от Profibus International. PROFINET IO в первую очередь предназначен для обмена данными в , а PROFINET CBA — для распределенных систем автоматизации. PROFINET IO использует циклическую передачу данных для обмена данными через Ethernet
Profinet IO Real Time	Profinet IO Real Time — один из двух открытых стандартных протоколов автоматизации Ethernet от Profibus International. Обмен данными ввода/вывода реализован поверх Ethernet
PRP/HSR	PRP/HSR — протоколы резервирования стандарта МЭК 62439-3. PRP (Parallel Redundancy Protocol) — протокол параллельного резервирования. При использовании PRP строятся две независимые сети. Каждый пакет данных дублируется и одновременно передается по обеим сетям. Если до получателя доходят оба пакета, то пакет, который пришел позже, отбрасывается. Это позволяет обеспечить бесшовную передачу данных даже при полном отказе одной из сетей. HSR (High-availability Seamless Redundancy) — протокол резервирования кольцевого соединения. HSR используют в кольцевых топологиях. Каждый передаваемый кадр дублируется и передается в обоих направлениях кольца HSR. Если до получателя доходят оба пакета, то пакет, который пришел позже, отбрасывается. Это позволяет обеспечить бесшовную передачу данных при одиночном обрыве линии связи
Radmin	Radmin — протокол на базе архитектуры «клиент-сервер», используемый программой Radmin. Это программа удаленного администрирования ПК для платформы Windows, которая позволяет работать на нескольких удаленных компьютерах с помощью графического интерфейса, передавать файлы и использовать режим голосового или текстового общения с пользователем удаленного компьютера
RARP (Reverse Address Resolution Protocol)	Reverse Address Resolution Protocol (ARP) — протокол, выполняющий обратное отображение адресов. Преобразует физический (MAC) адрес в IP-адрес
Regul protocol	Regul — протокол для взаимодействия с ПЛК Regul
Regul authentication	Пакеты протокола Regul, содержащие команду аутентификации на ПЛК Regul. Regul — протокол для взаимодействия с ПЛК Regul

Табл. 29. Список протоколов, обнаруживаемых Комплексом

НАИМЕНОВАНИЕ	ОПИСАНИЕ
Regul load application	Пакеты протокола Regul, содержащие команду загрузки приложения на ПЛК Regul. Regul – протокол для взаимодействия с ПЛК Regul
Regul start application	Пакеты протокола Regul, содержащие команду запуска приложения на ПЛК Regul. Regul – протокол для взаимодействия с ПЛК Regul
Regul stop application	Пакеты протокола Regul, содержащие команду остановки приложения на ПЛК Regul. Regul – протокол для взаимодействия с ПЛК Regul
Remote Call Procedure	Remote Procedure Call (RPC) – спецификация для механизма удаленного вызова процедур, разработанная для Distributed Computing Environment (DCE). Является ключевой технологией, используемой при построении распределенных приложений. RPC позволяет приложению выполнять процедуры на другой машине в сети. При этом механизм RPC скрывает от разработчика детали сетевого взаимодействия при удаленных вызовах и может использоваться в сетях, построенных с использованием различных архитектур
Remote Call Procedure	Пакеты протокола DCE RPC версии 3 и ниже
Remote Call Procedure V4	Пакеты протокола DCE RPC версии 4
Remote Desktop Protocol	Remote Desktop Protocol (RDP) – проприетарный протокол Microsoft, который используется для подключения к другому компьютеру через сетевое соединение. Клиент RDP предоставляет графический интерфейс после успешного подключения. Серверы RDP, необходимые для подключения от клиента, встроены в ОС Windows
Reverse Address Resolution Protocol	Reverse Address Resolution Protocol – протокол, выполняющий обратное отображение адресов. Преобразует физический (MAC) адрес в IP-адрес
RTSP (Real Time Streaming Protocol)	RTSP – протокол управления сетью, разработанный для использования в развлекательных и коммуникационных системах для управления серверами потоковых данных
S7 Communication	S7 Communication – проприетарный протокол Siemens для взаимодействия с семейства Siemens S7-300/400.
S7 Communication Monitoring	Пакеты S7, содержащие код функции для мониторинга состояния (Monitor)

Табл. 29. Список протоколов, обнаруживаемых Комплексом

НАИМЕНОВАНИЕ	ОПИСАНИЕ
S7 PLC Start Command	Пакеты S7, содержащие код функции для запуска (PLC_START). S7 Communication — проприетарный протокол Siemens для взаимодействия с семейства Siemens S7-300/400.
S7 PLC Stop Command	Пакеты S7, содержащие код функции для остановки (PLC_STOP). S7 Communication — проприетарный протокол Siemens для взаимодействия с семейства Siemens S7-300/400.
S7 Plus Communication	S7 Communication Plus — проприетарный протокол Siemens для взаимодействия с семейства Siemens S7-1200/1500
S7 Plus Communication keep alive	Пакеты keep_alive протокола S7comm Plus
S7 Plus Communication Monitor Program	Пакеты S7 Plus, содержащие код функции для мониторинга состояния (Monitor)
S7 Plus Communication new Hardware configuration Download to PLC	Пакеты S7 Plus, содержащие код функции для загрузки новой конфигурации оборудования в (Hardware_to_PLC)
S7 Plus Communication Program Download to PLC	Пакеты S7 Plus, содержащие код функции для загрузки приложения в (Upload)
S7 Plus Communication Program Upload from PLC	Пакеты S7 Plus, содержащие код функции для загрузки приложения из (Download)
S7 Plus Communication Start Command	Пакеты S7 Plus, содержащие код функции для запуска (PLC_START)
S7 Plus Communication Stop Command	Пакеты S7 Plus, содержащие код функции для остановки (PLC_STOP)
S7 Plus Communication version 1	Версия 1 протокола S7comm Plus
S7 Plus Communication version 2	Версия 2 протокола S7comm Plus
S7 Plus Communication version 3	Версия 3 протокола S7comm Plus
S7 Project Download Command	Пакеты S7, содержащие код функции для загрузки приложения в (Download)
S7 Project Upload Command	Пакеты S7, содержащие код функции для выгрузки приложения из (Upload)

Табл. 29. Список протоколов, обнаруживаемых Комплексом

НАИМЕНОВАНИЕ	ОПИСАНИЕ
SCADA SONATA	Протокол системы SCADA «Соната» - проприетарный протокол верхнего уровня, применяемый для передачи событий между компонентами АСУ ТП. Каждый переданный пакет подтверждается принимающей стороной
Secure Shell (SSH)	Secure Shell (SSH) — сетевой протокол прикладного уровня, позволяющий производить удаленное управление операционной системой и туннелирование TCP-соединений (в том числе для передачи файлов). Схож по функциональности с протоколами Telnet и rlogin, но, в отличие от них, шифрует весь трафик, включая и передаваемые пароли. SSH допускает выбор различных алгоритмов шифрования
Simple Service Discovery Protocol	Simple Service Discovery Protocol (SSDP) — сетевой протокол, основанный на наборе протоколов Интернета, служащий для объявления и обнаружения сетевых сервисов без использования специальных механизмов статической конфигурации или действий со стороны серверов, таких как DHCP или DNS. SSDP является основой протокола обнаружения Universal plug-and-play (UPnP) и предназначен для использования в домашних сетях и в малом бизнесе
Simple Service Discovery Protocol Reply	Ответ на запрос SSDP
Sirius IS Proprietary protocol	Sirius_IS — проприетарный протокол для взаимодействия систем Сириус-ИС, предназначенных для контроля и управления технологическими объектами в реальном времени
SMB	Server Message Block (SMB) — сетевой протокол прикладного уровня для удаленного доступа к файлам, принтерам, COM-портам и другим сетевым ресурсам, а также для межпроцессного взаимодействия. Используется в операционных системах Microsoft Windows
SMTP (Simple Mail Transfer Protocol)	SMTP — сетевой протокол, предназначенный для передачи электронной почты в сетях TCP/IP
SNMP (Simple Network Management Protocol)	Simple Network Management Protocol (SNMP) — стандартный интернет-протокол для управления устройствами в IP-сетях на основе архитектур TCP/UDP. К таким устройствам относятся маршрутизаторы, коммутаторы, серверы, рабочие станции, принтеры, модемные стойки и другие. Протокол обычно используется в системах сетевого управления для контроля подключенных к сети устройств на предмет условий, которые требуют внимания администратора

Табл. 29. Список протоколов, обнаруживаемых Комплексом

НАИМЕНОВАНИЕ	ОПИСАНИЕ
SOCKS5	SOCKS5 — протокол, позволяющий пересылать пакеты от клиента к серверу через прокси-сервер
Spanning Tree Protocol	Spanning Tree Protocol (STP) — протокол канального уровня, предназначенный для устранения петель в топологии произвольной сети Ethernet, в которой есть один или более сетевых мостов, связанных избыточными соединениями
SSL	Secure Sockets Layer (SSL) или Transport Layer Security (TLS) — сетевой протокол, обеспечивающий шифрованную связь по сети. Используемые версии: SSL 1.0, SSL 3.0, TLS 1.0, TLS 1.1 и TLS 1.2. Цель TLS — обеспечить конфиденциальность и целостность данных между двумя взаимодействующими сторонами. Симметричная криптография, асимметричная криптография и аутентификация по ключу используются для предотвращения перехвата и изменения данных третьими сторонами
SysLog BSD	System Log (Syslog) — протокол для отправки и регистрации сообщений на Syslog-сервере о происходящих в системе событиях, использующийся в компьютерных сетях, работающих по протоколу IP. Syslog не может использоваться для опроса устройств для сбора информации
Tabular Data Stream	TDS (Tabular Data Stream) — протокол, используемый для передачи данных между сервером базы данных и клиентом и обеспечивающий согласование аутентификации и шифрования канала. Используется для взаимодействия с СУБД MSSQL
TCP (Transmission Control Protocol)	Transmission Control Protocol (TCP) — основной протокол стека TCP/IP и один из основных протоколов передачи данных интернета, используемый для обеспечения надежной доставки данных на транспортном уровне модели OSI. Механизм TCP предоставляет поток данных с предварительной установкой соединения, осуществляет повторный запрос данных в случае потери данных и устраняет дублирование при получении двух копий одного пакета, гарантируя тем самым, в отличие от UDP, целостность передаваемых данных и уведомление отправителя о результатах передачи
TCP Dynamic	TCP-соединение с одновременным использованием динамических портов источника и получателя (с номерами портов, превышающих 32767)

Табл. 29. Список протоколов, обнаруживаемых Комплексом

НАИМЕНОВАНИЕ	ОПИСАНИЕ
TeamViewer	TeamViewer — протокол для удаленного контроля компьютеров, обмена файлами между управляющей и управляемой машинами, видеосвязи и веб-конференций
Telnet	Telnet — протокол прикладного уровня для удаленного управления, используемый для реализации двунаправленного текстового терминального интерфейса по сети (при помощи транспорта TCP). Используется для удаленного администрирования различными сетевыми устройствами и программными серверами
TPKT	TPKT — пакеты протокольного блока данных транспортного уровня. Транспортная служба ISO поверх TCP. TCP и ISO относятся к двум конкурирующим наборам сетевых протоколов. TPKT обеспечивает перевод между этими двумя группами: он переносит пакет OSI в полезной нагрузке своего собственного пакета, а затем передает полученную структуру в TCP, после чего пакет обрабатывается как пакет TCP / IP
Transparent Network Substrate	TNS — протокол для взаимодействия с СУБД Oracle
Trivial File Transfer Protocol	TFTP — простой протокол передачи файлов. Используется для загрузки бездисковых рабочих станций, загрузки обновлений и конфигураций в «умные» сетевые устройства, записи статистики с мини-АТС (CDR) и аппаратных маршрутизаторов/межсетевых экранов
UDP (User Datagram protocol)	User Datagram Protocol (UDP) — протокол связи, который используется в Интернете для передачи данных, чувствительных ко времени, в виде дейтаграмм. Он ускоряет обмен данными, т.к. не требует предварительного сообщения для установки специальных каналов передачи или путей данных, позволяя передавать данные до того, как принимающая сторона согласится на обмен
Unified Messaging Application Services (UMAS)	Unified Messaging Application Services (UMAS) — проприетарный протокол, используемый для настройки и мониторинга производства компании Schneider Electric
UMAS PLC monitor command	Пакеты UMAS, содержащие коды функции для мониторинга состояния (Monitor)
UMAS PLC start command	Пакеты UMAS, содержащие код функции для запуска (PLC_Start)
UMAS PLC stop command	Пакеты UMAS, содержащие код функции для остановки (PLC_Stop)

Табл. 29. Список протоколов, обнаруживаемых Комплексом

НАИМЕНОВАНИЕ	ОПИСАНИЕ
UMAS transfer project from PLC command	Пакеты UMAS, содержащие код функции для загрузки приложения из (transfer_project_from_PLC)
UMAS transfer project to PLC command	Пакеты UMAS, содержащие код функции для загрузки приложения в (transfer_project_to_PLC)
Virtual LAN (802.3ac)	Tag VLAN в кадре Ethernet, предназначенный для передачи информации о принадлежности к VLAN. Virtual LAN — топологическая (виртуальная) локальная сеть (Virtual Local Area Networks, VLAN) в сети IEEE 802.3 Ethernet. Представляет собой группу хостов с общим набором требований, которые взаимодействуют так, как если бы они были подключены к ширококестельному домену, независимо от их физического местонахождения
Virtual Network Computing	VNC (Virtual Network Computing) — система, использующая протокол RFB (Remote Framebuffer) для удаленного доступа к графическому рабочему столу компьютера
VNET/IP Protocol Yokogawa	Vnet/IP — протокол сети Vnet/IP, работающий в реальном времени и применяемый в распределенных системах управления. Сеть разработана компанией Yokogawa. Vnet/IP базируется на 1 Гбит Ethernet и реализует транспортные протоколы, оптимизированные для автоматизации технологических процессов поверх UDP протокола
Wago PLC protocol	Сервисный проприетарный протокол Wago
Web Services Dynamic Discovery	Web Services Dynamic Discovery (WS-Discovery) — протокол связи на основе UDP, используемый для автоматического обнаружения веб-служб внутри сетей. Он используется принтерами, камерами и другими типами устройств, в том числе различными функциями Windows, начиная с Windows Vista
WinCC Client-Server Proprietary protocol	WinCC Client-Server Proprietary protocol — проприетарный протокол, разработанный компанией Siemens для взаимодействия HMI систем WinCC на основе архитектуры «клиент — сервер»
Windows Remote Management	Windows Remote Management (WinRM) — протокол службы удаленного управления для операционных систем Windows. Служба WinRM — серверная часть приложения удаленного управления, к которому возможно удаленное подключение с помощью клиента Windows Remote Shell (WinRS)
Wonderware SuiteLink	Wonderware InTouch SuiteLink — промышленный протокол, разработанный компанией Wonderware для взаимодействия HMI систем

Табл. 29. Список протоколов, обнаруживаемых Комплексом

НАИМЕНОВАНИЕ	ОПИСАНИЕ
	InTouch на основе архитектуры «клиент – сервер». В основе протокола SuiteLink лежит протокол TCP/IP
X Window System core protocol version 11	X Window System core protocol является базовым протоколом системы X Window, которая представляет собой сетевую оконную систему для растровых дисплеев, используемую для создания графических пользовательских интерфейсов в Unix, Unix-подобных и других операционных системах
Zabbix Agent	Протокол обмена данными Zabbix-сервера для связи с Zabbix-агентом, основанный на формате JSON. Легитимный протокол
Zabbix Trapper	Протокол коммуникации на основе JSON, который Zabbix-сервер использует для получения данных от утилиты Zabbix sender в случае с траппер элементами данных. Легитимный протокол

3.13. Рекомендации по настройке сбора данных

Для корректного сбора данных необходимо придерживаться следующих общих принципов:

- Настройка сбора данных — только в режиме технического обслуживания.
- Расписания в задачах сбора данных различных компонентов не должны пересекаться. Во избежание ошибок, в один момент времени следует собирать данные только одной задачей.
- Устанавливать количество запросов сбора данных с активов не более четырех раз в сутки.
- Устанавливать интервал между задачами сбора данных не менее 10–20 минут.
- Формировать задачи согласно операционной системе активов.
- Использовать один протокол сбора данных в одной задаче.
- Не рекомендуется использовать группы, количество сканеров в которых превышает 30. Подробнее о группах сканеров см. в разделе [Группировка сканеров сбора данных](#).
- Сбор данных по протоколу ms-even4 возможен только для Windows XP, Windows Server 2003 и Windows Server 2000.

3.14. Реестр сканеров Комплекса

В таблицах ниже представлен список предоставляемых разработчиком Комплекса Python-скриптов, входящих в состав сканеров сбора данных, и их описание. Доступен сбор данных следующих категорий:

- Таблица 30. Python-скрипты для сбора данных об ОС и ПО
- Таблица 31. Python-скрипты для сбора данных ПО Acronis
- Таблица 32. Python-скрипты для сбора данных ПЛК Allen Bradley
- Таблица 33. Python-скрипты для сбора данных сетевого оборудования Checkpoint
- Таблица 34. Python-скрипты для сбора данных межсетевых экранов Cisco ASA
- Таблица 35. Python-скрипты для сбора данных с сетевого оборудования Cisco
- Таблица 36. Python-скрипты для сбора данных сетевого оборудования Eltex
- Таблица 37. Python-скрипты для сбора данных SCADA Honeywell
- Таблица 38. Python-скрипты для сбора данных с сетевого оборудования Huawei VRP
- Таблица 39. Python-скрипты для сбора данных сетевого оборудования HP
- Таблица 40. Python-скрипты для сбора данных SCADA InTouch
- Таблица 41. Python-скрипты для сбора данных сетевого оборудования Mgate
- Таблица 42. Python-скрипты для сбора трафика баз данных MSSQL и MySQL
- Таблица 43. Python-скрипты для сбора данных сетевого оборудования NIS
- Таблица 44. Python-скрипты для сбора данных утилиты nmap
- Таблица 45. Python-скрипты для сбора данных с ОС QNX
- Таблица 46. Python-скрипты для сбора данных Redkit
- Таблица 47. Python-скрипты для сбора данных ПЛК Siemens
- Таблица 48. Python-скрипты для сбора данных ПЛК Schneider Electric
- Таблица 49. Python-скрипты для сбора данных по протоколу SNMP
- Таблица 50. Python-скрипты для сбора данных ОС Solaris
- Таблица 51. Python-скрипты для сбора данных ОС Unix
- Таблица 52. Python-скрипты для сбора данных ОС Windows
- Таблица 53. Python-скрипты для сбора данных ОС Windows CC
- Таблица 54. Python-скрипты для инвентаризации объектов Windows



Внимание:

Сбор данных по протоколу ms-even4 возможен только для Windows XP, Windows Server 2003 и Windows Server 2000.

Табл. 30. Python-скрипты для сбора данных об ОС и ПО

НАИМЕНОВАНИЕ	ОПИСАНИЕ	ТЕГ
Версия ОС Unix (ssh)	Сканер для сбора информации о версии ОС Unix по протоколу SSH	admin
Версия ОС Windows (winexe 0.8)	Сканер для сбора информации о версии ОС по протоколу winexe 0.8	admin

Табл. 30. Python-скрипты для сбора данных об ОС и ПО

НАИМЕНОВАНИЕ	ОПИСАНИЕ	ТЕГ
Версия ОС Windows (winexe 1.0)	Сканер для сбора информации о версии ОС по протоколу	admin
Версия ОС Windows (winrm http)	Сканер для сбора информации о версии ОС Windows по протоколу winrm http	admin
Версия ОС Windows (winrm https)	Сканер для сбора информации о версии ОС Windows по протоколу winrm https	admin
Версия ОС Cisco (enable) (ssh)	Сканер для сбора информации о версии ОС Cisco (enable) по протоколу SSH	admin
Версия ОС Cisco (ssh)	Сканер для сбора информации о версии ОС Cisco по протоколу SSH	admin
Версия ОС DevLink	Сканер для сбора информации о версии ОС DevLink	admin
Версия ОС Eltex	Сканер для сбора информации о версии ОС Eltex	admin
Версия ОС ПЛК Allen Bradley	Сканер для сбора информации о версии ОС ПЛК Allen Bradley	admin
Версия ОС ПЛК Schneider	Сканер для сбора информации о версии ОС ПЛК Schneider Electric	admin
Версия ОС ПЛК Siemens	Сканер для сбора информации о версии ОС ПЛК Siemens	admin
Версия ОС ПЛК Regul	Сканер для сбора информации о версии ОС ПЛК Regul	admin
Версия ОС D-Link	Сканер для сбора информации о версии ОС D-Link	admin
Версия ОС Moxa	Сканер для сбора информации о версии ОС Moxa	admin
Версия ОС Huawei	Сканер для сбора информации о версии ОС Huawei	admin
Установленное ПО Centos (ssh) (os soft)	Сканер для сбора информации об установленном ПО Centos по протоколу SSH	admin
Установленное ПО Debian (ssh) (os soft)	Сканер для сбора информации об установленном ПО Debian по протоколу SSH	admin
Установленное ПО Windows (winexe 0.8)	Сканер для сбора информации об установленном ПО Windows по протоколу winexe 0.8	admin
Установленное ПО Windows (winexe 1.0)	Сканер для сбора информации об установленном ПО Windows по протоколу winexe 1.0	admin

Табл. 30. Python-скрипты для сбора данных об ОС и ПО

НАИМЕНОВАНИЕ	ОПИСАНИЕ	ТЕГ
Установленное ПО Windows (winrm http)	Сканер для сбора информации об установленном ПО Windows по протоколу winrm http	admin
Установленное ПО Windows (winrm https)	Сканер для сбора информации об установленном ПО Windows по протоколу winrm https	admin
Установленное ПО Windows (wmi)	Сканер для сбора информации об установленном ПО Windows по протоколу wmi	admin

Табл. 31. Python-скрипты для сбора данных ПО Acronis

НАИМЕНОВАНИЕ	ОПИСАНИЕ	ТЕГ
Acronis список активных задач	Сканер для сбора списка активных задач Acronis по протоколу winexe	admin
Acronis список задач	Сканер для сбора списка задач Acronis по протоколу winexe	admin
Acronis список планов	Сканер для сбора списка планов Acronis по протоколу winexe	admin

Табл. 32. Python-скрипты для сбора данных ПЛК Allen Bradley

НАИМЕНОВАНИЕ	ОПИСАНИЕ
Значения тегов ПЛК Allen Bradley	Сканер для сбора значений тегов ПЛК Allen Bradley
Конфигурации ПЛК Allen Bradley (Ethernet_IP)	Сканер для сбора конфигурации ПЛК Allen Bradley по протоколу Ethernet IP
Конфигурация ПЛК Allen Bradley	Сканер для сбора конфигурации ПЛК Allen Bradley
Модули ПЛК Allen Bradley	Сканер для сбора модулей ПЛК Allen Bradley
Наименование ПЛК Allen Bradley	Сканер для сбора наименования ПЛК Allen Bradley
Программа ПЛК Allen Bradley	Сканер для сбора программы ПЛК Allen Bradley
Состояние ПЛК Allen Bradley	Сканер для сбора состояния ПЛК Allen Bradley
Список тегов ПЛК Allen Bradley	Сканер для сбора списка тегов ПЛК Allen Bradley

Табл. 33. Python-скрипты для сбора данных сетевого оборудования Checkpoint

НАИМЕНОВАНИЕ	ОПИСАНИЕ	ТЕГ
Checkpoint изменение правил	Сканер для сбора изменений правил Checkpoint	checkpoint, checkpoint_expert
Checkpoint изменить объекты	Сканер для сбора измененных объектов Checkpoint	checkpoint, checkpoint_expert
Checkpoint по- лучить ARP-таблицу	Сканер для сбора ARP-таблицы Checkpoint	checkpoint
Checkpoint получить конфигурацию	Сканер для сбора конфигурации Checkpoint	checkpoint
Checkpoint получить уста- новленную политику	Сканер для получения установленной политики Checkpoint	checkpoint

Табл. 34. Python-скрипты для сбора данных межсетевых экранов Cisco ASA

НАИМЕНОВАНИЕ	ОПИСАНИЕ	ТЕГ
ECI_CISCO_ASA_- SHOW_ARP (ssh1-en)	Сканер для сбора ARP-таблицы Cisco Asa по протоколу SSH (enable)	cisco, cisco_- en
ECI_CISCO_ASA_- SHOW_ARP (ssh2-en)	Сканер для сбора ARP-таблицы Cisco Asa по протоколу SSH (enable)	cisco, cisco_- en
ECI_CISCO_ASA_SHOW_- IPROUTE (ssh1-en)	Сканер для сбора таблицы маршрутизации Cisco Asa по протоколу SSH (enable)	cisco, cisco_- en
ECI_CISCO_ASA_SHOW_- IPROUTE (ssh2-en)	Сканер для сбора таблицы маршрутизации Cisco Asa по протоколу SSH (enable)	cisco, cisco_- en
ECI_CISCO_ASA_SHOW_- RUNNING_CONFIG (ssh1-en)	Сканер для сбора текущей конфигурации Cisco Asa по протоколу SSH (enable)	cisco, cisco_- en
ECI_CISCO_ASA_SHOW_- RUNNING_CONFIG (ssh2-en)	Сканер для сбора текущей конфигурации Cisco Asa по протоколу SSH (enable)	cisco, cisco_- en

Табл. 34. Python-скрипты для сбора данных межсетевых экранов Cisco ASA

НАИМЕНОВАНИЕ	ОПИСАНИЕ	ТЕГ
ECI_CISCO_ASA_SHOW_- STARTUP_CONFIG (ssh1-en)	Сканер для сбора начальной конфигурации Cisco Asa по протоколу SSH (enable)	cisco, cisco_- en
ECI_CISCO_ASA_SHOW_- STARTUP_CONFIG (ssh2-en)	Сканер для сбора начальной конфигурации Cisco Asa по протоколу SSH (enable)	cisco, cisco_- en
ECI_CISCO_ASA_- SHOW_VERSION (ssh1)	Сканер для сбора версии Cisco Asa по протоколу SSH	cisco
ECI_CISCO_ASA_- SHOW_VERSION (ssh2)	Сканер для сбора версии Cisco Asa по протоколу SSH	cisco

Табл. 35. Python-скрипты для сбора данных с сетевого оборудования Cisco

НАИМЕНОВАНИЕ	ОПИСАНИЕ	ТЕГ
ECI_CISCO_IOS_- SHOW_ARP (ssh)	Сканер для сбора ARP-таблицы Cisco по протоколу SSH	cisco
ECI_CISCO_IOS_- SHOW_ARP (telnet)	Сканер для сбора ARP-таблицы Cisco по протоколу telnet	cisco
ECI_CISCO_IOS_SHOW_- ARP-telnet-nologin	Сканер для сбора ARP-таблицы Cisco по протоколу telnet (nologin)	cisco
ECI_CISCO_IOS_- SHOW_IPROUTE (ssh)	Сканер для сбора таблицы маршрутизации Cisco по протоколу SSH	cisco
ECI_CISCO_IOS_SHOW_- IPROUTE (ssh-en)	Сканер для сбора таблицы маршрутизации Cisco по протоколу SSH (enable)	cisco, cisco_- en
ECI_CISCO_IOS_- SHOW_IPROUTE (telnet)	Сканер для сбора таблицы маршрутизации Cisco по протоколу telnet	cisco
ECI_CISCO_IOS_SHOW_- IPROUTE (telnet_en)	Сканер для сбора таблицы маршрутизации Cisco по протоколу telnet (enable)	cisco, cisco_- en
ECI_CISCO_IOS_SHOW_- IPROUTE-telnet-nologin	Сканер для сбора таблицы маршрутизации Cisco по протоколу telnet (nologin)	cisco

Табл. 35. Python-скрипты для сбора данных с сетевого оборудования Cisco

НАИМЕНОВАНИЕ	ОПИСАНИЕ	ТЕГ
ECI_CISCO_IOS_SHOW_- MAC_ADDRESS_TABLE (ssh)	Сканер для сбора таблицы mac-адресов Cisco по протоколу SSH	cisco
ECI_CISCO_IOS_SHOW_- MAC_ADDRESS_- TABLE (ssh) alternative	Сканер для сбора таблицы mac-адресов Cisco по протоколу SSH	cisco
ECI_CISCO_IOS_SHOW_MAC_- ADDRESS_TABLE (ssh-en)	Сканер для сбора таблицы mac-адресов Cisco по протоколу SSH (enable)	cisco, cisco_- en
ECI_CISCO_IOS_SHOW_MAC_- ADDRESS_TABLE (telnet)	Сканер для сбора таблицы mac-адресов Cisco по протоколу telnet	cisco
ECI_CISCO_IOS_SHOW_MAC_- ADDRESS_TABLE (telnet-en)	Сканер для сбора таблицы mac-адресов Cisco по протоколу telnet (enable)	cisco, cisco_- en
ECI_CISCO_IOS_SHOW_MAC_- ADDRESS_TABLE-telnet-nologin	Сканер для сбора таблицы mac-адресов Cisco по протоколу telnet (nologin)	cisco
ECI_CISCO_IOS_SHOW_- RUNNING_CONFIG (ssh)	Сканер для сбора текущей конфигурации Cisco по протоколу SSH	cisco
ECI_CISCO_IOS_SHOW_- RUNNING_CONFIG (ssh-en)	Сканер для сбора текущей конфигурации Cisco по протоколу SSH (enable)	cisco, cisco_- en
ECI_CISCO_IOS_SHOW_- RUNNING_CONFIG (telnet)	Сканер для сбора текущей конфигурации Cisco по протоколу telnet	cisco
ECI_CISCO_IOS_SHOW_- RUNNING_CONFIG (telnet-en)	Сканер для сбора текущей конфигурации Cisco по протоколу telnet (enable)	cisco, cisco_- en
ECI_CISCO_IOS_- SHOW_RUNNING_- CONFIG-telnet-en-nologin	Сканер для сбора текущей конфигурации Cisco по протоколу telnet (nologin)	cisco
ECI_CISCO_IOS_SHOW_- STARTUP_CONFIG (ssh)	Сканер для сбора начальной конфигурации Cisco по протоколу SSH	cisco

Табл. 35. Python-скрипты для сбора данных с сетевого оборудования Cisco

НАИМЕНОВАНИЕ	ОПИСАНИЕ	ТЕГ
ECI_CISCO_IOS_SHOW_- STARTUP_CONFIG (ssh-en)	Сканер для сбора начальной конфигурации Cisco по протоколу SSH (enable)	cisco, cisco_- en
ECI_CISCO_IOS_SHOW_- STARTUP_CONFIG (telnet)	Сканер для сбора начальной конфигурации Cisco по протоколу telnet	cisco
ECI_CISCO_IOS_SHOW_- STARTUP_CONFIG (telnet-en)	Сканер для сбора начальной конфигурации Cisco по протоколу telnet (enable)	cisco, cisco_- en
ECI_CISCO_IOS_- SHOW_STARTUP_- CONFIG-telnet-en-nologin	Сканер для сбора начальной конфигурации Cisco по протоколу telnet (nologin)	cisco
ECI_CISCO_IOS_- SHOW_VERSION (ssh)	Сканер для сбора версии Cisco по протоколу SSH	cisco
ECI_CISCO_IOS_SHOW_- VERSION (ssh-en)	Сканер для сбора версии Cisco по протоколу SSH (enable)	cisco, cisco_- en
ECI_CISCO_IOS_SHOW_- VERSION (telnet)	Сканер для сбора версии Cisco по протоколу telnet	cisco
ECI_CISCO_IOS_SHOW_- VERSION (telnet-en)	Сканер для сбора версии Cisco по протоколу telnet (enable)	cisco, cisco_- en
ECI_CISCO_IOS_SHOW_- VERSION-telnet-nologin	Сканер для сбора версии Cisco по протоколу telnet (nologin)	cisco
ECI_CISCO_IOS_- SH_INV (ssh-en)	Сканер для инвентаризации Cisco по протоколу SSH (enable)	cisco
ECI_CISCO_IOS_- SH_INV (telnet-en)	Сканер для инвентаризации Cisco по протоколу telnet (enable)	cisco

Табл. 36. Python-скрипты для сбора данных сетевого оборудования Eltex

НАИМЕНОВАНИЕ	ОПИСАНИЕ	ТЕГ
ECI_ELTEX_ESR_SHOW_ARP	Сканер для сбора ARP-таблицы Eltex по протоколу SSH	eltex

Табл. 36. Python-скрипты для сбора данных сетевого оборудования Eltex

НАИМЕНОВАНИЕ	ОПИСАНИЕ	ТЕГ
ECI_ELTEX_ESR-SHOW_IP_ROUTE	Сканер для сбора таблицы маршрутизации Eltex по протоколу SSH	eltex
ECI_ELTEX_ESR_SHOW_RUNNING_CONFIG	Сканер для сбора текущей конфигурации Eltex по протоколу SSH	eltex
ECI_ELTEX_ESR-SHOW_VERSION	Сканер для сбора версии Eltex по протоколу SSH	eltex
ECI_ELTEX_MES_SHOW_ARP	Сканер для сбора ARP-таблицы Eltex по протоколу SSH	eltex
ECI_ELTEX_MES-SHOW_IPROUTE	Сканер для сбора таблицы маршрутизации Eltex по протоколу SSH	eltex
ECI_ELTEX_MES_SHOW_MAC_ADDRESS_TABLE	Сканер для сбора таблицы mac-адресов Eltex по протоколу SSH	eltex
ECI_ELTEX_MES_SHOW_RUNNING_CONFIG	Сканер для сбора текущей конфигурации Eltex по протоколу SSH	eltex
ECI_ELTEX_MES_SHOW_STARTUP_CONFIG	Сканер для сбора начальной конфигурации Eltex по протоколу SSH	eltex
ECI_ELTEX_MES-SHOW_VERSION	Сканер для сбора версии Eltex по протоколу SSH	eltex

Табл. 37. Python-скрипты для сбора данных SCADA Honeywell

НАИМЕНОВАНИЕ	ОПИСАНИЕ	ТЕГ
Шаблон безопасности Win Server 2008 для SCADA Honeywell (winrm http)	Сканер для сбора списка шаблонов безопасности Win Server 2008 для SCADA Honeywell по протоколу winrm http	admin
Шаблон безопасности Win Server 2008 для SCADA Honeywell (winrm https)	Сканер для сбора списка шаблонов безопасности Win Server 2008 для SCADA Honeywell по протоколу winrm https	admin
Шаблон безопасности Win10 для SCADA Honeywell (winrm http)	Сканер для сбора списка шаблонов безопасности Win10 для SCADA Honeywell по протоколу winrm http	admin

Табл. 37. Python-скрипты для сбора данных SCADA Honeywell

НАИМЕНОВАНИЕ	ОПИСАНИЕ	ТЕГ
Шаблон безопасности Win10 для SCADA Honeywell (winrm https)	Сканер для сбора списка шаблонов безопасности Win10 для SCADA Honeywell по протоколу winrm https	admin
Шаблон безопасности Win7 для SCADA Honeywell (winrm http)	Сканер для сбора списка шаблонов безопасности Win7 для SCADA Honeywell по протоколу winrm http	admin
Шаблон безопасности Win7 для SCADA Honeywell (winrm https)	Сканер для сбора списка шаблонов безопасности Win7 для SCADA Honeywell по протоколу winrm https	admin

Табл. 38. Python-скрипты для сбора данных с сетевого оборудования Huawei VRP

НАИМЕНОВАНИЕ	ОПИСАНИЕ	ТЕГ
ECI_HUAWEI_VRP_SHOW_STARTUP_CONFIG (ssh, noen)	Начальная конфигурация (ssh, без enable)	huawei
ECI_HUAWEI_VRP_SHOW_MAC_ADDRESS_TABLE (ssh,noen)	Таблица mac-адресов Huawei VRP (ssh, без enable)	huawei
ECI_HUAWEI_VRP_SHOW_ARP (ssh, noen)	ARP таблица Huawei VRP (ssh, без enable)	huawei
ECI_HUAWEI_VRP_SHOW_RUNNING_CONFIG (ssh, noen)	Текущая конфигурация Huawei VRP (ssh, без enable)	huawei
ECI_HUAWEI_VRP_SHOW_VERSION (ssh, noen)	Версия ОС Huawei VRP (ssh, без enable)	huawei

Табл. 39. Python-скрипты для сбора данных сетевого оборудования HP

НАИМЕНОВАНИЕ	ОПИСАНИЕ	ТЕГ
HP2424 IP (telnet)	Сканер для сбора таблицы IP-адресов HP2424 по протоколу telnet	hp
HP2424 IP (telnet, nologin)	Сканер для сбора таблицы IP-адресов HP2424 по протоколу telnet (no login)	hp
HP2424 конфигурация (telnet)	Сканер для сбора конфигурации HP2424 по протоколу telnet	hp

Табл. 39. Python-скрипты для сбора данных сетевого оборудования HP

НАИМЕНОВАНИЕ	ОПИСАНИЕ	ТЕГ
HP2424 конфигурация (telnet, nologin)	Сканер для сбора конфигурации HP2424 по протоколу telnet (no login)	hp
HP2424 модули (telnet)	Сканер для сбора модулей HP2424 по протоколу telnet	hp
HP2424 модули (telnet, nologin)	Сканер для сбора модулей HP2424 по протоколу telnet (no login)	hp
HP2424 сведения о системе (telnet)	Сканер для сбора сведения о системе HP2424 по протоколу telnet	hp
HP2424 сведения о системе (telnet, nologin)	Сканер для сбора сведения о системе HP2424 по протоколу telnet (no login)	hp
Начальная конфигурация HP (ssh)	Сканер для сбора начальной конфигурации HP по протоколу SSH	hp
Конфигурация HP A5500 (ssh)	Сканер для сбора конфигурации HP A5500 по протоколу SSH	hp
Начальная конфигурация HP (telnet)	Сканер для сбора начальной конфигурации HP по протоколу telnet	hp
Текущая конфигурация HP (ssh)	Сканер для сбора текущей конфигурации HP по протоколу SSH	hp
Текущая конфигурация HP (telnet)	Сканер для сбора текущей конфигурации HP по протоколу telnet	hp

Табл. 40. Python-скрипты для сбора данных SCADA InTouch

НАИМЕНОВАНИЕ	ОПИСАНИЕ	ТЕГ
Проверка параметров операционной системы (winrm http)	Сканер для проверки параметров операционной системы по протоколу winrm http	admin
Проверка параметров операционной системы (winrm https)	Сканер для проверки параметров операционной системы по протоколу winrm https	admin
Проверка прав пользователя (winrm http)	Сканер для проверки прав пользователя по протоколу winrm http	admin
Проверка прав пользователя (winrm https)	Сканер для проверки прав пользователя по протоколу winrm https	admin

Табл. 41. Python-скрипты для сбора данных сетевого оборудования Mgate

НАИМЕНОВАНИЕ	ОПИСАНИЕ	ТЕГ
ECI_MOXA_MGATE_SHOW_RUNNING_CONFIG (telnet)	Сканер для сбора списка запущенных конфигураций по протоколу telnet	моха
ECI_MOXA_MGATE_SHOW_RUNNING_CONFIG (telnet-noauth)	Сканер для сбора списка запущенных конфигураций по протоколу telnet (noauth)	None
ECI_MOXA_MGATE_SHOW_RUNNING_CONFIG-telnet-noauth-full	Сканер для сбора списка запущенных конфигураций по протоколу telnet (noauth-full)	None

Табл. 42. Python-скрипты для сбора трафика баз данных MSSQL и MySQL

НАИМЕНОВАНИЕ	ОПИСАНИЕ	ТЕГ
MSSQL_Логин и права	Сканер для сбора списка логинов и их прав на MSSQL по протоколу sql	sa
MSSQL_Логин и права (noport)	Сканер для сбора списка логинов и их прав на MSSQL по протоколу sql (no port)	sa, instance
MSSQL_Логин и права (без паролей)	Сканер для сбора списка логинов и их прав на MSSQL по протоколу sql (no pass)	sa
MSSQL_Права пользователей на БД	Сканер для сбора списка прав пользователей на БД MSSQL по протоколу sql	sa
MSSQL_Права пользователей на БД (noport)	Сканер для сбора списка прав пользователей на БД MSSQL по протоколу sql (no port)	sa, instance
MySQL пользователи	Сканер для сбора списка пользователей на БД MySQL	sa
MySQL права пользователей	Сканер для сбора списка прав пользователей на БД MySQL	sa
MySQL сбор событий входа и выхода пользователя	Сканер для сбора списка событий входа и выхода пользователей на БД MySQL	datapk
MySQL сбор событий запуска и остановки	Сканер для сбора списка событий запуска и остановки на БД MySQL	admin
MySQL_Права пользователей	Сканер для сбора списка прав пользователей на MySQL по протоколу sql	datapk

Табл. 42. Python-скрипты для сбора трафика баз данных MSSQL и MySQL

НАИМЕНОВАНИЕ	ОПИСАНИЕ	ТЕГ
MySQL_Права пользователей_Columns	Сканер для сбора списка прав пользователей на столбцы MySQL по протоколу sql	datapk
MySQL_Права пользователей_DB	Сканер для сбора списка прав пользователей на БД MySQL по протоколу sql	datapk
MySQL_Права пользователей_Tables	Сканер для сбора списка прав пользователей на таблицы MySQL по протоколу sql	datapk
MySQL_События входа-выхода	Сканер для сбора событий входа-выхода MySQL по протоколу sql	datapk

Табл. 43. Python-скрипты для сбора данных сетевого оборудования NIS

НАИМЕНОВАНИЕ	ОПИСАНИЕ	ТЕГ
ECI_NIS_SHOW_ARP-ssh	Сканер для сбора ARP-таблицы NIS по протоколу SSH	nis
ECI_NIS_SHOW_IPROUTE-ssh	Сканер для сбора таблицы маршрутизации NIS по протоколу SSH	nis
ECI_NIS_SHOW_MAC_-ADDRESS_TABLE-ssh	Сканер для сбора таблицы mac-адресов NIS по протоколу SSH	nis
ECI_NIS_SHOW_RUNNING_-CONFIG-ssh-noen	Сканер для сбора текущей конфигурации NIS по протоколу SSH	nis
ECI_NIS_SHOW_VERSION-ssh	Сканер для сбора версии Nis по протоколу SSH	nis
NIS 3500-2216 интерфейсы (telnet)	Сканер для сбора интерфейсов NIS 3500-2216 по протоколу Telnet	nis
NIS 3500-2216 информация об IP (telnet)	Сканер для сбора информации об IP NIS 3500-2216 по протоколу Telnet	nis
NIS 3500-2216 общая информация (telnet)	Сканер для сбора общей информации NIS 3500-2216 по протоколу Telnet	nis
NIS_SHOW_ARP(telnet)	Сканер для сбора ARP-таблицы Nis по протоколу telnet	nis
NIS_SHOW_IPROUTE(telnet)	Сканер для сбора таблицы маршрутизации Nis по протоколу telnet	nis
NIS_SHOW_MAC_-ADDRESS_TABLE(telnet)	Сканер для сбора таблицы mac-адресов Nis по протоколу telnet	nis

Табл. 43. Python-скрипты для сбора данных сетевого оборудования NIS

НАИМЕНОВАНИЕ	ОПИСАНИЕ	ТЕГ
NIS_SHOW_RUNNING_CONFIG(telnet)	Сканер для сбора текущей конфигурации NIS по протоколу telnet	nis

Табл. 44. Python-скрипты для сбора данных утилиты nmap

НАИМЕНОВАНИЕ	ОПИСАНИЕ
Открытые порты (nmap)	Сканер для сбора списка открытых портов nmap
Расширенное сканирование (nmap)	Сканер для расширенного сканирования nmap

Табл. 45. Python-скрипты для сбора данных с ОС QNX

НАИМЕНОВАНИЕ	ОПИСАНИЕ	ТЕГ
ARP таблица QNX 6.5 (ssh)	Сканер для сбора ARP-таблицы с QNX 6.5	admin
ARP-таблица QNX (telnet)	Сканер для сбора ARP-таблицы QNX по протоколу telnet	admin
Зарегистрированные пользователи QNX (lastlog)	Сканер для сбора зарегистрированных пользователей QNX по протоколу telnet (lastlog)	admin
Зарегистрированные пользователи QNX (telnet)	Сканер для сбора зарегистрированных пользователей QNX по протоколу telnet	admin
Зарегистрированные пользователи QNX 6.5 (ssh)	Сканер для сбора списка вошедших в систему пользователей по протоколу SSH	admin
Имя сетевого узла QNX (telnet)	Сканер для сбора имени сетевого узла QNX по протоколу telnet	admin
Имя сетевого узла QNX 6.5 (ssh)	Сканер для сбора имени сетевого узла по протоколу SSH	admin
Информация об ОС QNX 6.5 (ssh)	Сканер для сбора информации об ОС по протоколу SSH	admin
Используемые DNS-сервера QNX (telnet)	Сканер для сбора используемых DNS-серверов QNX по протоколу telnet	admin
Используемые DNS-сервера QNX 6.5 (ssh)	Сканер для сбора содержимого файла resolv.conf по протоколу SSH	admin

Табл. 45. Python-скрипты для сбора данных с ОС QNX

НАИМЕНОВАНИЕ	ОПИСАНИЕ	ТЕГ
Конфигурационные строки QNX 6.5 (getconf -a) (ssh)	Сканер для сбора настроек безопасности QNX по протоколу SSH	admin
Объекты cron QNX 6.5 (ssh)	Сканер для сбора объектов crontab по протоколу SSH	admin
Объекты cron QNX4 (telnet)	Сканер для сбора объектов cron QNX4 по протоколу telnet	admin
Сетевая статистика QNX (telnet)	Сканер для сбора сетевой статистики QNX по протоколу telnet	admin
Сетевая статистика QNX 6.5 (ssh)	Сканер для сбора сетевой статистики по протоколу SSH	admin
Сетевые интерфейсы QNX (telnet)	Сканер для сбора сетевых интерфейсов QNX по протоколу telnet	admin
Сетевые интерфейсы QNX 6.5 (ssh)	Сканер для сбора списка сетевых интерфейсов QNX по протоколу SSH	admin
Сетевые порты в режиме Listening QNX (telnet)	Сканер для сбора сетевых портов в режиме Listening QNX по протоколу telnet	admin
Сетевые порты в режиме listening QNX 6.5 (ssh)	Сканер для сбора списка портов в режиме LISTEN по протоколу SSH	admin
Список групп QNX (telnet)	Сканер для сбора списка групп QNX по протоколу telnet	admin
Список групп QNX 6.5 (ssh)	Сканер для сбора списка групп QNX	admin
Список подключенных устройств QNX4 (telnet)	Сканер для сбора списка подключенных устройств QNX4 по протоколу telnet	admin
Список пользователей QNX (telnet)	Сканер для сбора списка пользователей QNX по протоколу telnet	admin
Список пользователей QNX 6.5 (ssh)	Сканер для сбора списка пользователей по протоколу SSH	admin
Список процессов QNX 6.5 (ssh)	Сканер для сбора списка процессов по протоколу SSH с QNX	admin
Список процессов QNX4 (telnet)	Сканер для сбора списка процессов QNX4 по протоколу telnet	admin

Табл. 45. Python-скрипты для сбора данных с ОС QNX

НАИМЕНОВАНИЕ	ОПИСАНИЕ	ТЕГ
Таблица маршрутизации QNX (telnet)	Сканер для сбора таблицы маршрутизации QNX4 по протоколу telnet	admin
Таблица маршрутизации QNX 6.5 (ssh)	Сканер для сбора таблицы маршрутизации по протоколу SSH	admin
Установленные утилиты QNX 6.5 (ssh)	Сканер для сбора списка установленных утилит по протоколу SSH	admin
Установленные утилиты QNX4 (telnet)	Сканер для сбора списка установленных утилит QNX4 по протоколу telnet	admin
Файл hosts QNX (telnet)	Сканер для сбора файла hosts QNX по протоколу telnet	admin
Файл hosts QNX 6.5 (ssh)	Сканер для сбора содержимого файла hosts QNX	admin

Табл. 46. Python-скрипты для сбора данных Redkit

НАИМЕНОВАНИЕ	ОПИСАНИЕ	ТЕГ
Время изменения таблиц сигналов Redkit	Сканер для сбора времени изменения таблиц сигналов Redkit	datapk
Контроль неизменности проекта Redkit	Сканер для контроля неизменности проекта Redkit	datapk
Контрольная сумма каталогов Redkit (winrm https)	Сканер для сбора списка контрольных сумм каталогов Redkit по протоколу winrm https	admin
Контрольная сумма каталогов Redkit конфигурации (winrm https)	Сканер для сбора списка контрольных сумм каталогов конфигурации Redkit по протоколу winrm https	admin
Контрольная сумма каталогов Redkit кэши (winrm https)	Сканер для сбора списка кэша контрольных сумм каталогов Redkit по протоколу winrm https	admin
Контрольная сумма проекта Redkit	Сканер для сбора списка контрольных сумм проекта Redkit	datapk
Перечень пользователей Redkit	Сканер для сбора списка пользователей проекта Redkit	datapk
Права пользователей в Redkit	Сканер для сбора списка прав пользователей Redkit	datapk

Табл. 47. Python-скрипты для сбора данных ПЛК Siemens

НАИМЕНОВАНИЕ	ОПИСАНИЕ
Конфигурация ПЛК (snap 7)	Сканер для сбора конфигурации ПЛК Siemens по протоколу SNAP 7
Конфигурация ПЛК (snap 7) (1.18+)	Сканер для сбора конфигурации ПЛК Siemens по протоколу SNAP 7
Конфигурация ПЛК (snap 7) (1.18+) (extended)	Сканер для сбора конфигурации ПЛК Siemens по протоколу SNAP 7 (extended)
Конфигурация ПЛК (snap 7) (No CPU)	Сканер для сбора конфигурации ПЛК Siemens по протоколу SNAP 7
Конфигурация ПЛК Siemens S7-300_400	Сканер для сбора конфигурации ПЛК Siemens по протоколу S7-300_400
Просмотр слотов ПЛК (snap7)	Сканер для просмотра слотов ПЛК Siemens по протоколу SNAP7
Расширенная конфигурация ПЛК Siemens S7-300_400	Сканер для сбора расширенной конфигурации ПЛК Siemens по протоколу S7-300_400

Табл. 48. Python-скрипты для сбора данных ПЛК Schneider Electric

НАИМЕНОВАНИЕ	ОПИСАНИЕ
Schenieder M340 Ethernet settings	Сканер для сбора настроек сети Ethernet ПЛК Schneider Electric M340
Schenieder M580 Ethernet settings NOR0200_NGD0100	Сканер для сбора настроек сети Ethernet ПЛК Schneider Electric M580 с сетевых интерфейсов NOR0200 и NGD0100
Schenieder M580 Ethernet settings встроенный модуль	Сканер для сбора настроек сети Ethernet ПЛК Schneider Electric M580 со встроенного модуля
Schenieder Momentum Ethernet settings	Сканер для сбора настроек сети Momentum Ethernet ПЛК Schneider Electric
Schenieder password_control	Сканер для сбора изменений пароля ПЛК Schneider Electric
Schenieder Premium Ethernet settings	Сканер для сбора настроек сети Premium Ethernet ПЛК Schneider Electric
Schenieder Quantum Ethernet settings	Сканер для сбора настроек сети Quantum Ethernet ПЛК Schneider Electric

Табл. 48. Python-скрипты для сбора данных ПЛК Schneider Electric

НАИМЕНОВАНИЕ	ОПИСАНИЕ
Schenieder Quantum io_head settings	Сканер для сбора настроек сети Quantum с использованием головного модуля Remote IO ПЛК Schneider Electric
Конфигурация ПЛК Schneider	Сканер для сбора конфигурации ПЛК Schneider Electric
Конфигурация проекта ПЛК Schneider	Сканер для сбора конфигурации проекта ПЛК Schneider Electric
Программа ПЛК Schneider	Сканер для сбора программы ПЛК Schneider Electric
Состояние ПЛК Schneider	Сканер для сбора состояния ПЛК Schneider Electric

Табл. 49. Python-скрипты для сбора данных по протоколу SNMP

НАИМЕНОВАНИЕ	ОПИСАНИЕ	ТЕГ
SNMP 2с. Раздел IP	Сканер для сбора параметров IP по протоколу SNMP2с	community
SNMP 2с. Раздел egr	Сканер для сбора параметров EGP по протоколу SNMP2с	community
SNMP 2с. Раздел icmp	Сканер для сбора параметров ICMP по протоколу SNMP2с	community
SNMP 2с. Раздел interfaces	Сканер для сбора списка интерфейсов по протоколу SNMP2с	community
SNMP 2с. Раздел snmp	Сканер для сбора параметров SNMP по протоколу SNMP2с	community
SNMP 2с. Раздел system	Сканер для сбора параметров System по протоколу SNMP2с	community
SNMP 2с. Раздел system (noformat)	Сканер для сбора параметров System по протоколу SNMP2с (noformat)	community
SNMP 2с. Раздел tcp	Сканер для сбора параметров TCP по протоколу SNMP2с	community
SNMP 2с. Раздел udp	Сканер для сбора параметров UDP по протоколу SNMP2с	community
SNMP 3. Раздел IP	Сканер для сбора параметров IP по протоколу SNMP3	snmp3, auth, priv
SNMP 3. Раздел egr	Сканер для сбора параметров EGP по протоколу SNMP3	snmp3, auth, priv
SNMP 3. Раздел icmp	Сканер для сбора параметров ICMP по протоколу SNMP3	snmp3, auth, priv

Табл. 49. Python-скрипты для сбора данных по протоколу SNMP

НАИМЕНОВАНИЕ	ОПИСАНИЕ	ТЕГ
SNMP 3. Раздел interfaces	Сканер для сбора списка интерфейсов по протоколу SNMP3	snmp3, auth, priv
SNMP 3. Раздел snmp	Сканер для сбора параметров SNMP по протоколу SNMP3	snmp3, auth, priv
SNMP 3. Раздел system	Сканер для сбора параметров System по протоколу SNMP3	snmp3, auth, priv
SNMP 3. Раздел system (noformat)	Сканер для сбора параметров System по протоколу SNMP3 (noformat)	snmp3, auth, priv
SNMP 3. Раздел tcp	Сканер для сбора параметров TCP по протоколу SNMP3	snmp3, auth, priv
SNMP 3. Раздел udp	Сканер для сбора параметров UDP по протоколу SNMP3	snmp3, auth, priv

Табл. 50. Python-скрипты для сбора данных ОС Solaris

НАИМЕНОВАНИЕ	ОПИСАНИЕ	ТЕГ
ARP-таблица Solaris (ssh)	Сканер для сбора ARP-таблицы Solaris по протоколу SSH	admin
Группы пользователей Solaris (ssh)	Сканер для сбора групп пользователей Solaris по протоколу SSH	admin
Запланированные задачи cron Solaris (ssh, su)	Сканер для сбора запланированных задач cron Solaris по протоколу SSH (sudo)	admin
Имя сетевого узла Solaris (ssh)	Сканер для сбора имени сетевого узла Solaris по протоколу SSH	admin
Объекты автозапуска Solaris (ssh)	Сканер для сбора объектов автозапуска Solaris по протоколу SSH	admin
Пользователи Solaris (ssh)	Сканер для сбора списка пользователей Solaris по протоколу SSH	admin
Сетевые порты в режиме LISTENING Solaris (ssh)	Сканер для сбора сетевых портов в режиме LISTENING Solaris по протоколу SSH	admin
Список процессов Solaris (ssh)	Сканер для сбора списка процессов Solaris по протоколу SSH	admin

Табл. 50. Python-скрипты для сбора данных ОС Solaris

НАИМЕНОВАНИЕ	ОПИСАНИЕ	ТЕГ
Таблица маршрутизации Solaris (ssh)	Сканер для сбора таблицы маршрутизации Solaris по протоколу SSH	admin
Установленное ПО Solaris (ssh)	Сканер для сбора списка установленного ПО Solaris по протоколу SSH	admin

Табл. 51. Python-скрипты для сбора данных ОС Unix

НАИМЕНОВАНИЕ	ОПИСАНИЕ	ТЕГ
ARP-таблица (ssh, sudo)	Скрипт для сбора ARP-таблицы Unix по протоколу SSH (sudo)	admin
ARP-таблица SuSE (ssh)	Сканер для сбора ARP-таблицы SuSE по протоколу SSH	admin
ARP-таблица Unix (ssh)	Сканер для сбора ARP-таблицы Unix по протоколу SSH	admin
DNS-сервера Unix (ssh)	Сканер для сбора DNS-серверов Unix по протоколу SSH	admin
Запланированные задачи cron Unix (ssh)	Сканер для сбора запланированных задач cron Unix по протоколу SSH	admin
Запланированные задачи cron Unix (ssh, sudo)	Сканер для сбора запланированных задач cron Unix по протоколу SSH (sudo)	admin
Имя сетевого узла Unix (ssh)	Сканер для сбора имени сетевого узла Unix по протоколу SSH	admin
Контрольные суммы DATAPK (ssh)	Сканер для сбора контрольных сумм DATAPK по протоколу SSH	admin
Объекты автозапуска SuSE (ssh)	Сканер для сбора объектов автозапуска SuSE по протоколу SSH	admin
Объекты автозапуска Unix (ssh)	Сканер для сбора объектов автозапуска Unix по протоколу SSH	admin
Подключенные носители информации SuSE (ssh)	Сканер для сбора подключенных носителей информации SuSE по протоколу SSH	admin
Подключенные носители информации Unix (ssh)	Сканер для сбора подключенных носителей информации Unix по протоколу SSH	admin
Подключенные устройства Unix (ssh)	Сканер для сбора подключенных устройств Unix по протоколу SSH	admin

Табл. 51. Python-скрипты для сбора данных ОС Unix

НАИМЕНОВАНИЕ	ОПИСАНИЕ	ТЕГ
Правила Iptables SuSE (ssh, sudo)	Сканер для сбора правил Iptables SuSE по протоколу SSH (sudo)	admin
Правила Iptables Unix (ssh)	Сканер для сбора правил Iptables Unix по протоколу SSH	admin
Правила Iptables Unix (ssh, sudo)	Сканер для сбора правил Iptables Unix по протоколу SSH (sudo)	admin
Правила SuSEfirewall2 (ssh)	Сканер для сбора правил SuSEfirewall2 по протоколу SSH	admin
Сетевые порты в режиме LISTENING Unix (ssh)	Сканер для сбора сетевых портов в режиме LISTENING Unix по протоколу SSH	admin
Содержимое файла sudoers Unix (ssh)	Сканер для сбора содержимого файла sudoers Unix по протоколу SSH	admin
Содержимое файла sudoers Unix (ssh, sudo)	Сканер для сбора содержимого файла sudoers Unix по протоколу SSH (sudo)	admin
Состояние сервисов DATAPK (ssh)	Сканер для сбора состояния сервисов DATAPK по протоколу SSH	admin
Список групп Unix (ssh)	Сканер для сбора списка групп Unix по протоколу SSH	admin
Список пользователей Unix (ssh)	Сканер для сбора списка пользователей Unix по протоколу SSH	admin
Список процессов Unix (ssh)	Сканер для сбора списка процессов Unix по протоколу SSH	admin
Список процессов Unix (ssh) nodiff	Сканер для сбора списка процессов Unix по протоколу SSH	admin
Список процессов Unix (ssh) без PID	Сканер для сбора списка процессов Unix без PID по протоколу SSH	admin
Таблица маршрутизации SuSE (ssh)	Сканер для сбора таблицы маршрутизации SuSE по протоколу SSH	admin
Таблица маршрутизации Unix (ssh)	Сканер для сбора таблицы маршрутизации Unix по протоколу SSH	admin
Файл Shadow Unix (ssh)	Сканер для сбора файла shadow Unix по протоколу SSH	admin
Файл Shadow Unix (ssh, sudo)	Сканер для сбора файла shadow Unix по протоколу SSH (sudo)	admin

Табл. 51. Python-скрипты для сбора данных ОС Unix

НАИМЕНОВАНИЕ	ОПИСАНИЕ	ТЕГ
Файл hosts Unix (ssh)	Сканер для сбора файла hosts Unix по протоколу SSH	admin

Табл. 52. Python-скрипты для сбора данных ОС Windows

НАИМЕНОВАНИЕ	ОПИСАНИЕ	ТЕГ
ARP-таблица (basic) (winrm http)	Сканер для сбора таблицы ARP Windows по протоколу winrm http	admin
ARP-таблица (basic) (winrm https)	Сканер для сбора таблицы ARP Windows по протоколу winrm https	admin
ARP-таблица (winexe 0.8)	Сканер для сбора таблицы ARP Windows по протоколу winexe 0.8	admin
ARP-таблица (winexe 1.0)	Сканер для сбора таблицы ARP Windows по протоколу winexe 1.0	admin
ARP-таблица (winrm http)	Сканер для сбора таблицы ARP Windows по протоколу winrm http	admin
ARP-таблица (winrm https)	Сканер для сбора таблицы ARP Windows по протоколу winrm https	admin
Версия KES (basic) (winrm http)	Сбор версии Kaspersky Endpoint Security по протоколу winrm http	admin
Версия KES (basic) (winrm https)	Сбор версии Kaspersky Endpoint Security по протоколу winrm https	admin
Версия KES (winexe 0.8)	Сбор версии Kaspersky Endpoint Security по протоколу winexe 0.8	admin
Версия KES (winexe 1.0)	Сбор версии Kaspersky Endpoint Security по протоколу winexe 1.0	admin
Версия KES (winrm http)	Сбор версии Kaspersky Endpoint Security по протоколу winrm http	admin
Версия KES (winrm https)	Сбор версии Kaspersky Endpoint Security по протоколу winrm https	admin
Версия WinNT (basic) (winrm http)	Сканер для сбора версии Windows NT по протоколу winrm http	admin
Версия WinNT (basic) (winrm https)	Сканер для сбора версии Windows NT по протоколу winrm https	admin
Версия WinNT (winexe 0.8)	Сканер для сбора версии Windows NT по протоколу winexe 0.8	admin
Версия WinNT (winexe 1.0)	Сканер для сбора версии Windows NT по протоколу winexe 1.0	admin

Табл. 52. Python-скрипты для сбора данных ОС Windows

НАИМЕНОВАНИЕ	ОПИСАНИЕ	ТЕГ
Версия WinNT (winrm http)	Сканер для сбора версии Windows NT по протоколу winrm http	admin
Версия WinNT (winrm https)	Сканер для сбора версии Windows NT по протоколу winrm https	admin
Версия Windows (basic) (winrm http)	Сканер для сбора версии Windows по протоколу winrm http	admin
Версия Windows (basic) (winrm https)	Сканер для сбора версии Windows по протоколу winrm https	admin
Версия Windows (winexe 0.8)	Сканер для сбора версии Windows по протоколу winexe 0.8	admin
Версия Windows (winexe 1.0)	Сканер для сбора версии Windows по протоколу winexe 1.0	admin
Версия Windows (winrm http)	Сканер для сбора версии Windows по протоколу winrm http	admin
Версия Windows (winrm https)	Сканер для сбора версии Windows по протоколу winrm https	admin
Группы и их члены (wmi)	Сбор списка групп и членов групп Windows по протоколу wmi	admin
Группы и их члены powershell (basic) (winrm http)	Сбор списка групп и членов групп Windows по протоколу winrm http	admin
Группы и их члены powershell (basic) (winrm https)	Сбор списка групп и членов групп Windows по протоколу winrm https	admin
Группы и их члены powershell (winrm http)	Сбор списка групп и членов групп Windows по протоколу winrm http	admin
Группы и их члены powershell (winrm https)	Сбор списка групп и членов групп Windows по протоколу winrm https	admin
Доверенные сертификаты (basic) (winrm http)	Сканер для сбора списка доверенных сертификатов на машине по протоколу winrm http	admin
Доверенные сертификаты (basic) (winrm https)	Сканер для сбора списка доверенных сертификатов на машине по протоколу winrm https	admin
Доверенные сертификаты (winexe 0.8)	Сканер для сбора списка доверенных сертификатов на машине по протоколу winexe 0.8	admin
Доверенные сертификаты (winexe 1.0)	Сканер для сбора списка доверенных сертификатов на машине по протоколу winexe 1.0	admin

Табл. 52. Python-скрипты для сбора данных ОС Windows

НАИМЕНОВАНИЕ	ОПИСАНИЕ	ТЕГ
Доверенные сертификаты (winrm http)	Сканер для сбора списка доверенных сертификатов на машине по протоколу winrm http	admin
Доверенные сертификаты (winrm https)	Сканер для сбора списка доверенных сертификатов на машине по протоколу winrm https	admin
Долгие/бесконечные пароли (basic) (winrm http)	Сканер для сбора паролей, до смены которых осталось больше 120 дней по протоколу winrm http	admin
Долгие/бесконечные пароли (basic) (winrm https)	Сканер для сбора паролей, до смены которых осталось больше 120 дней по протоколу winrm https	admin
Долгие/бесконечные пароли (winexe 0.8)	Сканер для сбора паролей, до смены которых осталось больше 120 дней по протоколу winexe 0.8	admin
Долгие/бесконечные пароли (winexe 1.0)	Сканер для сбора паролей, до смены которых осталось больше 120 дней по протоколу winexe 1.0	admin
Долгие/бесконечные пароли (winrm http)	Сканер для сбора паролей, до смены которых осталось больше 120 дней по протоколу winrm http	admin
Долгие/бесконечные пароли (winrm https)	Сканер для сбора паролей, до смены которых осталось больше 120 дней по протоколу winrm https	admin
Значимые события Security (mseven) cp866	Сбор значимых событий журнала Security по протоколу mseven	admin
Значимые события System (mseven) cp866	Сбор значимых событий журнала System по протоколу mseven	admin
Контрольные суммы файлов (basic) (winrm http)	Сканер для вычисления контрольных сумм файлов (ОС после XP) по протоколу winrm http	admin
Контрольные суммы файлов (basic) (winrm https)	Сканер для вычисления контрольных сумм файлов (ОС после XP) по протоколу winrm https	admin
Контрольные суммы файлов (winexe 0.8)	Сканер для вычисления контрольных сумм файлов (ОС после XP) по протоколу winexe 0.8	admin
Контрольные суммы файлов (winexe 1.0)	Сканер для вычисления контрольных сумм файлов (ОС после XP) по протоколу winexe 1.0	admin
Контрольные суммы файлов (winrm http)	Сканер для вычисления контрольных сумм файлов (ОС после XP) по протоколу winrm http	admin

Табл. 52. Python-скрипты для сбора данных ОС Windows

НАИМЕНОВАНИЕ	ОПИСАНИЕ	ТЕГ
Контрольные суммы файлов (winrm https)	Сканер для вычисления контрольных сумм файлов (ОС после XP) по протоколу winrm https	admin
Конфигурация KES (basic) (winrm http)	Сбор конфигурации Kaspersky Endpoint Security по протоколу winrm http	admin
Конфигурация KES (basic) (winrm https)	Сбор конфигурации Kaspersky Endpoint Security по протоколу winrm https	admin
Конфигурация KES (winexe 0.8)	Сбор конфигурации Kaspersky Endpoint Security по протоколу winexe 0.8	admin
Конфигурация KES (winexe 1.0)	Сбор конфигурации Kaspersky Endpoint Security по протоколу winexe 1.0	admin
Конфигурация KES (winrm http)	Сбор конфигурации Kaspersky Endpoint Security по протоколу winrm http	admin
Конфигурация KES (winrm https)	Сбор конфигурации Kaspersky Endpoint Security по протоколу winrm https	admin
Локальная политика безопасности (basic) (winrm http)	Сканер для сбора локальной политики безопасности по протоколу winrm http	admin
Локальная политика безопасности (basic) (winrm https)	Сканер для сбора локальной политики безопасности по протоколу winrm https	admin
Локальная политика безопасности (winexe 0.8)	Сканер для сбора локальной политики безопасности по протоколу winexe 0.8	admin
Локальная политика безопасности (winexe 1.0)	Сканер для сбора локальной политики безопасности по протоколу winexe 1.0	admin
Локальная политика безопасности (winrm http)	Сканер для сбора локальной политики безопасности по протоколу winrm http	admin
Локальная политика безопасности (winrm https)	Сканер для сбора локальной политики безопасности по протоколу winrm https	admin
Наименование актива (basic) (winrm http)	Сканер для сбора имени хоста по протоколу winrm http	admin

Табл. 52. Python-скрипты для сбора данных ОС Windows

НАИМЕНОВАНИЕ	ОПИСАНИЕ	ТЕГ
Наименование актива (basic) (winrm https)	Сканер для сбора имени хоста по протоколу winrm https	admin
Наименование актива (winexe 0.8)	Сканер для сбора имени хоста по протоколу winexe 0.8	admin
Наименование актива (winexe 1.0)	Сканер для сбора имени хоста по протоколу winexe 1.0	admin
Наименование актива (winrm http)	Сканер для сбора имени хоста по протоколу winrm http	admin
Наименование актива (winrm https)	Сканер для сбора имени хоста по протоколу winrm https	admin
Неактивные аккаунты (basic) (winrm http)	Сканер для сбора списка пользователей, неактивных 30 и более дней по протоколу winrm http	admin
Неактивные аккаунты (basic) (winrm https)	Сканер для сбора списка пользователей, неактивных 30 и более дней по протоколу winrm https	admin
Неактивные аккаунты (winexe 0.8)	Сканер для сбора списка пользователей, неактивных 30 и более дней по протоколу winexe 0.8	admin
Неактивные аккаунты (winexe 1.0)	Сканер для сбора списка пользователей, неактивных 30 и более дней по протоколу winexe 1.0	admin
Неактивные аккаунты (winrm http)	Сканер для сбора списка пользователей, неактивных 30 и более дней по протоколу winrm http	admin
Неактивные аккаунты (winrm https)	Сканер для сбора списка пользователей, неактивных 30 и более дней по протоколу winrm https	admin
Общие файловые ресурсы (basic) (winrm http)	Сканер для сбора общих файловых ресурсов через net share по протоколу winrm http	admin
Общие файловые ресурсы (basic) (winrm https)	Сканер для сбора общих файловых ресурсов через net share по протоколу winrm https	admin
Общие файловые ресурсы без системных (basic) (winrm http)	Сканер для сбора общих файловых ресурсов через net share по протоколу winrm http	admin

Табл. 52. Python-скрипты для сбора данных ОС Windows

НАИМЕНОВАНИЕ	ОПИСАНИЕ	ТЕГ
Общие файловые ресурсы без системных (basic) (winrm https)	Сканер для сбора общих файловых ресурсов через net share по протоколу winrm https	admin
Общие файловые ресурсы (winexe 0.8)	Сканер для сбора общих файловых ресурсов через net share по протоколу winexe 0.8	admin
Общие файловые ресурсы (winexe 1.0)	Сканер для сбора общих файловых ресурсов через net share по протоколу winexe 1.0	admin
Общие файловые ресурсы (winrm http)	Сканер для сбора общих файловых ресурсов через net share по протоколу winrm http	admin
Общие файловые ресурсы (winrm https)	Сканер для сбора общих файловых ресурсов через net share по протоколу winrm https	admin
Общие файловые ресурсы без системных (winrm https)	Сканер для сбора общих файловых ресурсов через net share по протоколу winrm https	admin
Общие файловые ресурсы без системных (winexe 0.8)	Сканер для сбора общих файловых ресурсов через net share по протоколу winexe 0.8	admin
Общие файловые ресурсы без системных (winexe 1.0)	Сканер для сбора общих файловых ресурсов через net share по протоколу winexe 1.0	admin
Общие файловые ресурсы без системных (winrm http)	Сканер для сбора общих файловых ресурсов через net share по протоколу winrm http	admin
Объекты автозапуска (basic) (winrm http)	Сканер для сбора объектов автозапуска по протоколу winrm http	admin
Объекты автозапуска (basic) (winrm https)	Сканер для сбора объектов автозапуска по протоколу winrm https	admin
Объекты автозапуска (winexe 0.8)	Сканер для сбора объектов автозапуска по протоколу winexe 0.8	admin
Объекты автозапуска (winexe 1.0)	Сканер для сбора объектов автозапуска по протоколу winexe 1.0	admin
Объекты автозапуска (winrm http)	Сканер для сбора объектов автозапуска по протоколу winrm http	admin

Табл. 52. Python-скрипты для сбора данных ОС Windows

НАИМЕНОВАНИЕ	ОПИСАНИЕ	ТЕГ
Объекты авто-запуска (winrm https)	Сканер для сбора объектов автозапуска по протоколу winrm https	admin
Объекты автозапуска (wmi)	Сканер для сбора объектов автозапуска по wmi	admin
Объекты автозапуска powershell (basic) (winrm http)	Сканер для сбора объектов автозапуска по протоколу winrm http	admin
Объекты автозапуска powershell (basic) (winrm https)	Сканер для сбора объектов автозапуска по протоколу winrm https	admin
Объекты автозапуска powershell (winrm http)	Сканер для сбора объектов автозапуска по протоколу winrm http	admin
Объекты автозапуска powershell (winrm https)	Сканер для сбора объектов автозапуска по протоколу winrm https	admin
Параметры сетевых интерфейсов (basic) (winrm http)	Сканер для сбора параметров ipconfig /all (кодировка 866) по протоколу winrm http	admin
Параметры сетевых интерфейсов (basic) (winrm https)	Сканер для сбора параметров ipconfig /all (кодировка 866) по протоколу winrm https	admin
Параметры сетевых интерфейсов (winexe 0.8)	Сканер для сбора параметров ipconfig /all (кодировка 866) по протоколу winexe 0.8	admin
Параметры сетевых интерфейсов (winexe 1.0)	Сканер для сбора параметров ipconfig /all (кодировка 866) по протоколу winexe 1.0	admin
Параметры сетевых интерфейсов (winrm http)	Сканер для сбора параметров ipconfig /all (кодировка 866) по протоколу winrm http	admin
Параметры сетевых интерфейсов (winrm https)	Сканер для сбора параметров ipconfig /all (кодировка 866) по протоколу winrm https	admin
Параметры сетевых интерфейсов XP (basic) (winrm http)	Сканер для сбора параметров Windows XP ipconfig /all (кодировка 1251) по протоколу winrm http	admin
Параметры сетевых интерфейсов XP (basic) (winrm https)	Сканер для сбора параметров Windows XP ipconfig /all (кодировка 1251) по протоколу winrm https	admin
Параметры сетевых интерфейсов XP (winexe 0.8)	Сканер для сбора параметров Windows XP ipconfig /all (кодировка 1251) по протоколу winexe 0.8	admin

Табл. 52. Python-скрипты для сбора данных ОС Windows

НАИМЕНОВАНИЕ	ОПИСАНИЕ	ТЕГ
Параметры сетевых интерфейсов XP (winexe 1.0)	Сканер для сбора параметров Windows XP <code>ipconfig /all</code> (кодировка 1251) по протоколу winexe 1.0	admin
Параметры сетевых интерфейсов XP (winrm http)	Сканер для сбора параметров Windows XP <code>ipconfig /all</code> (кодировка 1251) по протоколу winrm http	admin
Параметры сетевых интерфейсов XP (winrm https)	Сканер для сбора параметров Windows XP <code>ipconfig /all</code> (кодировка 1251) по протоколу winrm https	admin
Планировщик задач (basic) (winrm http)	Сканер для сбора планировщика задач Windows по протоколу winrm http	admin
Планировщик задач (basic) (winrm https)	Сканер для сбора планировщика задач Windows по протоколу winrm https	admin
Планировщик задач (winexe 0.8)	Сканер для сбора планировщика задач Windows по протоколу winexe 0.8	admin
Планировщик задач (winexe 1.0)	Сканер для сбора планировщика задач Windows по протоколу winexe 1.0	admin
Планировщик задач (winrm http)	Сканер для сбора планировщика задач Windows по протоколу winrm http	admin
Планировщик задач (winrm https)	Сканер для сбора планировщика задач Windows по протоколу winrm https	admin
Права на файлы и папки до XP (basic) (winrm http)	Сканер для сбора прав на файлы и папки <code>saccls</code> (ОС до XP включительно) по протоколу winrm http	admin
Права на файлы и папки до XP (basic) (winrm https)	Сканер для сбора прав на файлы и папки <code>saccls</code> (ОС до XP включительно) по протоколу winrm https	admin
Права на файлы и папки после XP (basic) (winrm http)	Сканер для сбора прав на файлы и папки <code>icacls</code> (ОС после XP) по протоколу winrm http	admin
Права на файлы и папки после XP (basic) (winrm https)	Сканер для сбора прав на файлы и папки <code>icacls</code> (ОС после XP) по протоколу winrm https	admin
Права на файлы и папки до XP (winexe 0.8)	Сканер для сбора прав на файлы и папки <code>saccls</code> (ОС до XP включительно) по протоколу winexe 0.8	admin
Права на файлы и папки до XP (winexe 1.0)	Сканер для сбора прав на файлы и папки <code>saccls</code> (ОС до XP включительно) по протоколу winexe 1.0	admin

Табл. 52. Python-скрипты для сбора данных ОС Windows

НАИМЕНОВАНИЕ	ОПИСАНИЕ	ТЕГ
Права на файлы и папки до XP (winrm http)	Сканер для сбора прав на файлы и папки sacls (ОС до XP включительно) по протоколу winrm http	admin
Права на файлы и папки до XP (winrm https)	Сканер для сбора прав на файлы и папки sacls (ОС до XP включительно) по протоколу winrm https	admin
Права на файлы и папки после XP (winexe 0.8)	Сканер для сбора прав на файлы и папки icacls (ОС после XP) по протоколу winexe 0.8	admin
Права на файлы и папки после XP (winexe 1.0)	Сканер для сбора прав на файлы и папки icacls (ОС после XP) по протоколу winexe 1.0	admin
Права на файлы и папки после XP (winrm http)	Сканер для сбора прав на файлы и папки icacls (ОС после XP) по протоколу winrm http	admin
Права на файлы и папки после XP (winrm https)	Сканер для сбора прав на файлы и папки icacls (ОС после XP) по протоколу winrm https	admin
Правила МЭ (basic) (winrm http)	Сканер для сбора правил межсетевого экрана для ОС после Windows XP по протоколу winrm http	admin
Правила МЭ (basic) (winrm https)	Сканер для сбора правил межсетевого экрана для ОС после Windows XP по протоколу winrm https	admin
Правила МЭ (winexe 0.8)	Сканер для сбора правил межсетевого экрана для ОС после Windows XP по протоколу winexe 0.8	admin
Правила МЭ (winexe 1.0)	Сканер для сбора правил межсетевого экрана для ОС после Windows XP по протоколу winexe 1.0	admin
Правила МЭ (winrm http)	Сканер для сбора правил межсетевого экрана для ОС после Windows XP по протоколу winrm http	admin
Правила МЭ (winrm https)	Сканер для сбора правил межсетевого экрана для ОС после Windows XP по протоколу winrm https	admin
Правила МЭ PS (winrm http)	Сканер для сбора правил межсетевого экрана для ОС после Windows XP по протоколу winrm http	admin
Правила МЭ PS (winrm https)	Сканер для сбора правил межсетевого экрана для ОС после Windows XP по протоколу winrm https	admin
Правила МЭ XP (basic) (winrm http)	Сканер для сбора правил межсетевого экрана для ОС Windows XP по протоколу winrm http	admin

Табл. 52. Python-скрипты для сбора данных ОС Windows

НАИМЕНОВАНИЕ	ОПИСАНИЕ	ТЕГ
Правила МЭ XP (basic) (winrm https)	Сканер для сбора правил межсетевого экрана для ОС Windows XP по протоколу winrm https	admin
Правила МЭ XP (winexe 0.8)	Сканер для сбора правил межсетевого экрана для ОС Windows XP по протоколу winexe 0.8	admin
Правила МЭ XP (winexe 1.0)	Сканер для сбора правил межсетевого экрана для ОС Windows XP по протоколу winexe 1.0	admin
Правила МЭ XP (winrm http)	Сканер для сбора правил межсетевого экрана для ОС Windows XP по протоколу winrm http	admin
Правила МЭ XP (winrm https)	Сканер для сбора правил межсетевого экрана для ОС Windows XP по протоколу winrm https	admin
Проверка обновлений KES (basic) (winrm http)	Сканер для сбора времени запуска обновлений KES по протоколу winrm http	admin
Проверка обновлений KES (basic) (winrm https)	Сканер для сбора времени запуска обновлений KES по протоколу winrm https	admin
Проверка обновлений KES (winexe 0.8)	Сканер для сбора времени запуска обновлений KES по протоколу winexe 0.8	admin
Проверка обновлений KES (winexe 1.0)	Сканер для сбора времени запуска обновлений KES по протоколу winexe 1.0	admin
Проверка обновлений KES (winrm http)	Сканер для сбора времени запуска обновлений KES по протоколу winrm http	admin
Проверка обновлений KES (winrm https)	Сканер для сбора времени запуска обновлений KES по протоколу winrm https	admin
Расширенная политика аудита (basic) (winrm http)	Сканер для сбора расширенной политики аудита по протоколу winrm http	admin
Расширенная политика аудита (basic) (winrm https)	Сканер для сбора расширенной политики аудита по протоколу winrm https	admin
Расширенная политика аудита (winexe 0.8)	Сканер для сбора расширенной политики аудита по протоколу winexe 0.8	admin
Расширенная политика аудита (winexe 1.0)	Сканер для сбора расширенной политики аудита по протоколу winexe 1.0	admin

Табл. 52. Python-скрипты для сбора данных ОС Windows

НАИМЕНОВАНИЕ	ОПИСАНИЕ	ТЕГ
Расширенная политика аудита (winrm http)	Сканер для сбора расширенной политики аудита по протоколу winrm http	admin
Расширенная политика аудита (winrm https)	Сканер для сбора расширенной политики аудита по протоколу winrm https	admin
Сетевые порты в режиме Listening (basic) (winrm http)	Сканер для сбора открытых портов Windows по протоколу winrm http	admin
Сетевые порты в режиме Listening (basic) (winrm https)	Сканер для сбора открытых портов Windows по протоколу winrm https	admin
Сетевые порты в режиме Listening (winexe 0.8)	Сканер для сбора открытых портов Windows по протоколу winexe 0.8	admin
Сетевые порты в режиме Listening (winexe 1.0)	Сканер для сбора открытых портов Windows по протоколу winexe 1.0	admin
Сетевые порты в режиме Listening (winrm http)	Сканер для сбора открытых портов Windows по протоколу winrm http	admin
Сетевые порты в режиме Listening (winrm https)	Сканер для сбора открытых портов Windows по протоколу winrm https	admin
Сканер для сбора компонентов Windows (winrm http)	Сбор компонентов Windows по протоколу winrm http	admin
Сканер для сбора компонентов Windows (winrm https)	Сбор компонентов Windows по протоколу winrm https	admin
Службы с автоматическим типом запуска (basic) (winrm https)	Сканер для сбора списка служб с автоматическим типом запуска по протоколу winrm https	admin
Службы с автоматическим типом запуска (winrm https)	Сканер для сбора списка служб с автоматическим типом запуска по протоколу winrm https	admin
Службы с автоматическим типом запуска (basic) (winrm http)	Сканер для сбора списка служб с автоматическим типом запуска по протоколу winrm http	admin
Службы с автоматическим типом запуска (winexe 0.8)	Сканер для сбора списка служб с автоматическим типом запуска по протоколу winexe 0.8	admin

Табл. 52. Python-скрипты для сбора данных ОС Windows

НАИМЕНОВАНИЕ	ОПИСАНИЕ	ТЕГ
Службы с автоматическим типом запуска (winexe 1.0)	Сканер для сбора списка служб с автоматическим типом запуска по протоколу winexe 1.0	admin
Службы с автоматическим типом запуска (winrm http)	Сканер для сбора списка служб с автоматическим типом запуска по протоколу winrm http	admin
Службы с автоматическим типом запуска (wmi)	Сканер для сбора списка служб с автоматическим типом запуска по протоколу wmi	admin
Службы с автоматическим типом запуска Powershell (basic) (winrm http)	Сканер для сбора списка служб с автоматическим типом запуска по протоколу winrm http	admin
Службы с автоматическим типом запуска Powershell (basic) (winrm https)	Сканер для сбора списка служб с автоматическим типом запуска по протоколу winrm https	admin
Службы с автоматическим типом запуска Powershell (winrm http)	Сканер для сбора списка служб с автоматическим типом запуска по протоколу winrm http	admin
Службы с автоматическим типом запуска Powershell (winrm https)	Сканер для сбора списка служб с автоматическим типом запуска по протоколу winrm https	admin
События Windows (Application)	Сбор журнала событий Application по протоколу mseven	admin
События Windows (Application) - XP и старше	Сбор журнала событий Application по протоколу mseven	admin
События Windows (KES) winrm http	Сбор журнала событий KES по протоколу winrm http	admin
События Windows (KES) winrm https	Сбор журнала событий KES по протоколу winrm https	admin
События Windows (KSC) winrm http	Сбор журнала событий KSC по протоколу winrm http	admin
События Windows (KSC) winrm https	Сбор журнала событий KSC по протоколу winrm https	admin
События Windows (Kaspersky)	Сбор журнала событий Kaspersky по протоколу mseven	admin

Табл. 52. Python-скрипты для сбора данных ОС Windows

НАИМЕНОВАНИЕ	ОПИСАНИЕ	ТЕГ
События Windows (Kaspersky) - XP и старше	Сбор журнала событий KES по протоколу mseven	admin
События Windows (Security)	Сбор журнала событий Security по протоколу mseven	admin
События Windows (Security) - XP и старше	Сбор журнала событий Security по протоколу mseven	admin
События Windows (System)	Сбор журнала событий System по протоколу mseven	admin
События Windows (System) - XP и старше	Сбор журнала событий System по протоколу mseven	admin
События Windows (application) winrm http	Сбор журнала событий Application по протоколу winrm http	admin
События Windows (application) winrm https	Сбор журнала событий Application по протоколу winrm https	admin
События Windows (basic) (KES) winrm http	Сбор журнала событий KES по протоколу winrm http	admin
События Windows (basic) (KES) winrm https	Сбор журнала событий KES по протоколу winrm https	admin
События Windows (basic) (KSC) winrm http	Сбор журнала событий KSC по протоколу winrm http	admin
События Windows (basic) (KSC) winrm https	Сбор журнала событий KSC по протоколу winrm https	admin
События Windows (basic) (application) winrm http	Сбор журнала событий Application по протоколу winrm http	admin
События Windows (basic) (application) winrm https	Сбор журнала событий Application по протоколу winrm https	admin
События Windows (basic) (printservice/admin) winrm http	Сбор журнала событий Printservice/Admin по протоколу winrm http	admin
События Windows (basic) (printservice/admin) winrm https	Сбор журнала событий Printservice/Admin по протоколу winrm https	admin

Табл. 52. Python-скрипты для сбора данных ОС Windows

НАИМЕНОВАНИЕ	ОПИСАНИЕ	ТЕГ
События Windows (basic) (printsrv/operational) winrm http	Сбор журнала событий Printservice/Operational по протоколу winrm http	admin
События Windows (basic) (printsrv/operational) winrm https	Сбор журнала событий Printservice/Operational по протоколу winrm https	admin
События Windows (basic) (security) winrm http	Сбор журнала событий Security по протоколу winrm http	admin
События Windows (basic) (security) winrm https	Сбор журнала событий Security по протоколу winrm https	admin
События Windows (basic) (system) winrm http	Сбор журнала событий System по протоколу winrm http	admin
События Windows (basic) (system) winrm https	Сбор журнала событий System по протоколу winrm https	admin
События Windows (printservice/admin) winrm http	Сбор журнала событий Printservice/Admin по протоколу winrm http	admin
События Windows (printservice/admin) winrm https	Сбор журнала событий Printservice/Admin по протоколу winrm https	admin
События Windows (printsrv/operational) winrm http	Сбор журнала событий Printservice/Operational по протоколу winrm http	admin
События Windows (printsrv/operational) winrm https	Сбор журнала событий Printservice/Operational по протоколу winrm https	admin
События Windows (security) winrm http	Сбор журнала событий Security по протоколу winrm http	admin
События Windows (security) winrm https	Сбор журнала событий Security по протоколу winrm https	admin
События Windows (system) winrm http	Сбор журнала событий System по протоколу winrm http	admin
События Windows (system) winrm https	Сбор журнала событий System по протоколу winrm https	admin

Табл. 52. Python-скрипты для сбора данных ОС Windows

НАИМЕНОВАНИЕ	ОПИСАНИЕ	ТЕГ
События Windows Application (mseven6)	Сбор журнала событий Application по протоколу mseven6	admin
События Windows KES (mseven6)	Сбор журнала событий KES по протоколу mseven6	admin
События Windows KSC (mseven6)	Сбор журнала событий KSC по протоколу mseven6	admin
События Windows Print-Service_Admin (mseven6)	Сбор журнала событий PrintService_Admin по протоколу mseven6	admin
События Windows Print-Service_Operational (mseven6)	Сбор журнала событий PrintService_Operational по протоколу mseven6	admin
События Windows Security (mseven6)	Сбор журнала событий Security по протоколу mseven6	admin
События Windows System (mseven6)	Сбор журнала событий System по протоколу mseven6	admin
Состояние МЭ (basic) (winrm http)	Сканер для сбора статуса межсетевого экрана по протоколу winrm http	admin
Состояние МЭ (basic) (winrm https)	Сканер для сбора статуса межсетевого экрана по протоколу winrm https	admin
Состояние МЭ (winexe 0.8)	Сканер для сбора статуса межсетевого экрана по протоколу winexe 0.8	admin
Состояние МЭ (winexe 1.0)	Сканер для сбора статуса межсетевого экрана по протоколу winexe 1.0	admin
Состояние МЭ (winrm http)	Сканер для сбора статуса межсетевого экрана по протоколу winrm http	admin
Состояние МЭ (winrm https)	Сканер для сбора статуса межсетевого экрана по протоколу winrm https	admin
Состояние МЭ XP (basic) (winrm http)	Сканер для сбора статуса межсетевого экрана по протоколу winrm http	admin
Состояние МЭ XP (basic) (winrm https)	Сканер для сбора статуса межсетевого экрана по протоколу winrm https	admin

Табл. 52. Python-скрипты для сбора данных ОС Windows

НАИМЕНОВАНИЕ	ОПИСАНИЕ	ТЕГ
Состояние МЭ XP (winexe 0.8)	Сканер для сбора статуса межсетевого экрана по протоколу winexe 0.8	admin
Состояние МЭ XP (winexe 1.0)	Сканер для сбора статуса межсетевого экрана по протоколу winexe 1.0	admin
Состояние МЭ XP (winrm http)	Сканер для сбора статуса межсетевого экрана по протоколу winrm http	admin
Состояние МЭ XP (winrm https)	Сканер для сбора статуса межсетевого экрана по протоколу winrm https	admin
Список групп (basic) (winrm http)	Сбор списка групп Windows по протоколу winrm http	admin
Список групп (basic) (winrm https)	Сбор списка групп Windows по протоколу winrm https	admin
Список групп (winexe 0.8)	Сбор списка групп Windows по протоколу winexe 0.8	admin
Список групп (winexe 1.0)	Сбор списка групп Windows по протоколу winexe 1.0	admin
Список групп (winrm http)	Сбор списка групп Windows по протоколу winrm http	admin
Список групп (winrm https)	Сбор списка групп Windows по протоколу winrm https	admin
Список групп (wmi)	Сбор списка групп Windows по протоколу wmi	admin
Список групп win2000 (wmi)	Сканер для сбора списка групп Windows 2000 по протоколу wmi	admin
Список групп powershell (basic) (winrm http)	Сбор списка групп Windows по протоколу winrm https	admin
Список групп powershell (basic) (winrm https)	Сбор списка групп Windows по протоколу winrm https	admin
Список групп powershell (winrm http)	Сбор списка групп Windows по протоколу winrm http	admin
Список групп powershell (winrm https)	Сбор списка групп Windows по протоколу winrm https	admin
Список локальных групп (basic) (winrm http)	Сбор списка локальных групп Windows по протоколу winrm http	admin

Табл. 52. Python-скрипты для сбора данных ОС Windows

НАИМЕНОВАНИЕ	ОПИСАНИЕ	ТЕГ
Список локальных групп (basic) (winrm https)	Сбор списка локальных групп Windows по протоколу winrm https	admin
Список локальных групп (winexe 0.8)	Сбор списка локальных групп Windows по протоколу winexe 0.8	admin
Список локальных групп (winexe 1.0)	Сбор списка локальных групп Windows по протоколу winexe 1.0	admin
Список локальных групп (winrm http)	Сбор списка локальных групп Windows по протоколу winrm http	admin
Список локальных групп (winrm https)	Сбор списка локальных групп Windows по протоколу winrm https	admin
Список локальных групп (wmi)	Сбор списка локальных групп Windows по протоколу wmi	admin
Список локальных групп powershell (basic) (winrm http)	Сбор списка локальных групп Windows по протоколу winrm http	admin
Список локальных групп powershell (basic) (winrm https)	Сбор списка локальных групп Windows по протоколу winrm https	admin
Список локальных групп powershell (winrm http)	Сбор списка локальных групп Windows по протоколу winrm http	admin
Список локальных групп powershell (winrm https)	Сбор списка локальных групп Windows по протоколу winrm https	admin
Список локальных пользователей (basic) (winrm http)	Сбор списка локальных пользователей Windows по протоколу winrm http	admin
Список локальных пользователей (basic) (winrm https)	Сбор списка локальных пользователей Windows по протоколу winrm https	admin
Список локальных пользователей (winexe 0.8)	Сбор списка локальных пользователей Windows по протоколу winexe 0.8	admin
Список локальных пользователей (winexe 1.0)	Сбор списка локальных пользователей Windows по протоколу winexe 1.0	admin
Список локальных пользователей (winrm http)	Сбор списка локальных пользователей Windows по протоколу winrm http	admin

Табл. 52. Python-скрипты для сбора данных ОС Windows

НАИМЕНОВАНИЕ	ОПИСАНИЕ	ТЕГ
Список локальных пользователей Win10 (winrm http)	Сбор списка локальных пользователей Windows (Win10 only) по протоколу winrm http	admin
Список локальных пользователей (winrm https)	Сбор списка локальных пользователей Windows по протоколу winrm https	admin
Список локальных пользователей Win10 (winrm https)	Сбор списка локальных пользователей Windows (Win10 only) по протоколу winrm https	admin
Список локальных пользователей (wmi)	Сбор списка локальных пользователей Windows по протоколу wmi	admin
Список локальных пользователей powershell (basic) (winrm http)	Сбор списка локальных пользователей Windows по протоколу winrm http	admin
Список локальных пользователей powershell (basic) (winrm https)	Сбор списка локальных пользователей Windows по протоколу winrm https	admin
Список локальных пользователей powershell (winrm http)	Сбор списка локальных пользователей Windows по протоколу winrm http	admin
Список локальных пользователей powershell (winrm https)	Сбор списка локальных пользователей Windows по протоколу winrm https	admin
Список пользователей (basic) (winrm http)	Сбор списка пользователей Windows по протоколу winrm http	admin
Список пользователей (basic) (winrm https)	Сбор списка пользователей Windows по протоколу winrm https	admin
Список пользователей (winexe 0.8)	Сбор списка пользователей Windows по протоколу winexe 0.8	admin
Список пользователей (winexe 1.0)	Сбор списка пользователей Windows по протоколу winexe 1.0	admin
Список пользователей (winrm http)	Сбор списка пользователей Windows по протоколу winrm http	admin

Табл. 52. Python-скрипты для сбора данных ОС Windows

НАИМЕНОВАНИЕ	ОПИСАНИЕ	ТЕГ
Список пользователей (winrm https)	Сбор списка пользователей Windows по протоколу winrm https	admin
Список пользователей (wmi)	Сбор списка пользователей Windows по протоколу wmi	admin
Список пользователей win2000 (wmi)	Сканер для сбора списка пользователей Windows 2000 по протоколу wmi	admin
Список пользователей powershell (basic) (winrm http)	Сбор списка пользователей Windows по протоколу winrm http	admin
Список пользователей powershell (basic) (winrm https)	Сбор списка пользователей Windows по протоколу winrm https	admin
Список пользователей powershell (winrm http)	Сканер для сбора списка пользователей Windows по протоколу winrm http	admin
Список пользователей powershell (winrm https)	Сбор списка пользователей Windows по протоколу winrm https	admin
Список пользователей и их группы (basic) (winrm http)	Сбор списка пользователей и их групп по протоколу winrm http	admin
Список пользователей и их группы (basic) (winrm https)	Сбор списка пользователей и их групп по протоколу winrm https	admin
Список пользователей и их группы (winrm http)	Сбор списка пользователей и их групп по протоколу winrm http	admin
Список пользователей и их группы (winrm https)	Сбор списка пользователей и их групп по протоколу winrm https	admin
Список пользователей и их группы (wmi)	Сбор списка пользователей и их групп по протоколу wmi	admin
Список пользователей и их группы win2000 (wmi)	Сканер для сбора списка пользователей и их групп Windows 2000 по протоколу wmi	admin
Список пользователей и их группы PS (basic) (winrm http)	Сбор списка пользователей и их групп по протоколу winrm http	admin
Список пользователей и их группы PS (basic) (winrm https)	Сбор списка пользователей и их групп по протоколу winrm https	admin

Табл. 52. Python-скрипты для сбора данных ОС Windows

НАИМЕНОВАНИЕ	ОПИСАНИЕ	ТЕГ
Список пользователей и их группы PS (winrm http)	Сбор списка пользователей и их групп по протоколу winrm http	admin
Список пользователей и их группы PS (winrm https)	Сбор списка пользователей и их групп по протоколу winrm https	admin
Список процессов (basic) (winrm http)	Список процессов Windows по протоколу winrm http	admin
Список процессов (basic) (winrm https)	Список процессов Windows по протоколу winrm https	admin
Список процессов (winexe 0.8)	Список процессов Windows по протоколу winexe 0.8	admin
Список процессов (nodiff) (winexe 0.8)	Список процессов Windows по протоколу winexe 0.8	admin
Список процессов (winexe 1.0)	Список процессов Windows по протоколу winexe 1.0	admin
Список процессов (nodiff) (winexe 1.0)	Список процессов Windows по протоколу winexe 1.0	admin
Список процессов (winrm http)	Список процессов Windows по протоколу winrm http	admin
Список процессов (nodiff) (winrm http)	Список процессов Windows по протоколу winrm http	admin
Список процессов (winrm https)	Список процессов Windows по протоколу winrm https	admin
Список процессов (nodiff) (winrm https)	Список процессов Windows по протоколу winrm https	admin
Список процессов (wmi)	Список процессов Windows по протоколу wmi	admin
Список процессов (nodiff) (wmi)	Список процессов Windows по протоколу wmi	admin
Список процессов без PID (wmi)	Список процессов Windows без PID по протоколу wmi	admin
Список процессов без PID (nodiff) (wmi)	Список процессов Windows без PID по протоколу wmi	admin

Табл. 52. Python-скрипты для сбора данных ОС Windows

НАИМЕНОВАНИЕ	ОПИСАНИЕ	ТЕГ
Список устройств (basic) (winrm http)	Сбор списка устройств Windows по протоколу winrm http	admin
Список устройств (basic) (winrm https)	Сбор списка устройств Windows по протоколу winrm https	admin
Список устройств (winexe 0.8)	Сбор списка устройств Windows по протоколу winexe 0.8	admin
Список устройств (winexe 1.0)	Сбор списка устройств Windows по протоколу winexe 1.0	admin
Список устройств (winrm http)	Сбор списка устройств Windows по протоколу winrm http	admin
Список устройств (winrm https)	Сбор списка устройств Windows по протоколу winrm https	admin
Список устройств (wmi)	Сбор списка устройств Windows по протоколу wmi	admin
Список устройств powershell (basic) (winrm http)	Сбор списка устройств Windows по протоколу winrm http	admin
Список устройств powershell (basic) (winrm https)	Сбор списка устройств Windows по протоколу winrm https	admin
Список устройств powershell (winrm http)	Сбор списка устройств Windows по протоколу winrm http	admin
Список устройств powershell (winrm https)	Сбор списка устройств Windows по протоколу winrm https	admin
Статус системы DEP (basic) (winrm http)	Сканер для сбора статуса DEP (Data execution prevention) системы Windows по протоколу winrm http	admin
Статус системы DEP (basic) (winrm https)	Сканер для сбора статуса DEP (Data execution prevention) системы Windows по протоколу winrm https	admin
Статус системы DEP (winexe 0.8)	Сканер для сбора статуса DEP (Data execution prevention) системы Windows по протоколу winexe 0.8	admin
Статус системы DEP (winexe 1.0)	Сканер для сбора статуса DEP (Data execution prevention) системы Windows по протоколу winexe 1.0	admin
Статус системы DEP (winrm http)	Сканер для сбора статуса DEP (Data execution prevention) системы Windows по протоколу winrm http	admin

Табл. 52. Python-скрипты для сбора данных ОС Windows

НАИМЕНОВАНИЕ	ОПИСАНИЕ	ТЕГ
Статус системы DEP (winrm https)	Сканер для сбора статуса DEP (Data execution prevention) системы Windows по протоколу winrm https	admin
Таблица маршрутизации (basic) (winrm http)	Сканер для сбора таблицы маршрутизации Windows по протоколу winrm http	admin
Таблица маршрутизации (basic) (winrm https)	Сканер для сбора таблицы маршрутизации Windows по протоколу winrm https	admin
Таблица маршрутизации (winexe 0.8)	Сканер для сбора таблицы маршрутизации Windows по протоколу winexe 0.8	admin
Таблица маршрутизации (winexe 1.0)	Сканер для сбора таблицы маршрутизации Windows по протоколу winexe 1.0	admin
Таблица маршрутизации (winrm http)	Сканер для сбора таблицы маршрутизации Windows по протоколу winrm http	admin
Таблица маршрутизации (winrm https)	Сканер для сбора таблицы маршрутизации Windows по протоколу winrm https	admin
Установленное ПО (basic) (winrm http)	Сканер для сбора установленного ПО x64 Windows по протоколу winrm http	admin
Установленное ПО (basic) (winrm https)	Сканер для сбора установленного ПО x64 Windows по протоколу winrm https	admin
Установленное ПО (winexe 0.8)	Сканер для сбора установленного ПО x64 Windows по протоколу winexe 0.8	admin
Установленное ПО (winexe 1.0)	Сканер для сбора установленного ПО x64 Windows по протоколу winexe 1.0	admin
Установленное ПО (winrm http)	Сканер для сбора установленного ПО x64 Windows по протоколу winrm http	admin
Установленное ПО (winrm https)	Сканер для сбора установленного ПО x64 Windows по протоколу winrm https	admin
Установленное ПО Windows Installer (basic) (winrm http)	Сканер для сбора установленного ПО x64 Windows Installer по протоколу winrm http	admin
Установленное ПО Windows Installer (basic) (winrm https)	Сканер для сбора установленного ПО x64 Windows Installer по протоколу winrm https	admin

Табл. 52. Python-скрипты для сбора данных ОС Windows

НАИМЕНОВАНИЕ	ОПИСАНИЕ	ТЕГ
Установленное ПО Windows Installer (winrm http)	Сканер для сбора установленного ПО x64 Windows Installer по протоколу winrm http	admin
Установленное ПО Windows Installer (winrm https)	Сканер для сбора установленного ПО x64 Windows Installer по протоколу winrm https	admin
Установленное ПО Windows Installer (wmi)	Сканер для сбора установленного ПО x64 Windows Installer по протоколу wmi	admin
Установленное ПО Windows Installer powershell (basic) (winrm http)	Сканер для сбора установленного ПО x64 Windows Installer по протоколу winrm http	admin
Установленное ПО Windows Installer powershell (basic) (winrm https)	Сканер для сбора установленного ПО x64 Windows Installer по протоколу winrm https	admin
Установленное ПО Windows Installer powershell (winrm http)	Сканер для сбора установленного ПО x64 Windows Installer по протоколу winrm http	admin
Установленное ПО Windows Installer powershell (winrm https)	Сканер для сбора установленного ПО x64 Windows Installer по протоколу winrm https	admin
Установленное ПО x32 (basic) (winrm http)	Сканер для сбора установленного ПО x32 Windows по протоколу winrm http	admin
Установленное ПО x32 (basic) (winrm https)	Сканер для сбора установленного ПО x32 Windows по протоколу winrm https	admin
Установленное ПО x32 (winexe 0.8)	Сканер для сбора установленного ПО x32 Windows по протоколу winexe 0.8	admin
Установленное ПО x32 (winexe 1.0)	Сканер для сбора установленного ПО x32 Windows по протоколу winexe 1.0	admin
Установленное ПО x32 (winrm http)	Сканер для сбора установленного ПО x32 Windows по протоколу winrm http	admin
Установленное ПО x32 (winrm https)	Сканер для сбора установленного ПО x32 Windows по протоколу winrm https	admin
Установленные обновления Windows (basic) (winrm http)	Сканер для сбора установленных обновлений Windows по протоколу winrm http	admin

Табл. 52. Python-скрипты для сбора данных ОС Windows

НАИМЕНОВАНИЕ	ОПИСАНИЕ	ТЕГ
Установленные обновления Windows (basic) (winrm https)	Сканер для сбора установленных обновлений Windows по протоколу winrm https	admin
Установленные обновления Windows (winexe 0.8)	Сканер для сбора установленных обновлений Windows по протоколу winexe 0.8	admin
Установленные обновления Windows (winexe 1.0)	Сканер для сбора установленных обновлений Windows по протоколу winexe 1.0	admin
Установленные обновления Windows (winrm http)	Сканер для сбора установленных обновлений Windows по протоколу winrm http	admin
Установленные обновления Windows (winrm https)	Сканер для сбора установленных обновлений Windows по протоколу winrm https	admin
Установленные обновления Windows (wmi)	Сканер для сбора установленных обновлений Windows по протоколу wmi	admin
Файл hosts (basic) (winrm http)	Сканер для сбора файла hosts Windows по протоколу winrm http	admin
Файл hosts (basic) (winrm https)	Сканер для сбора файла hosts Windows по протоколу winrm https	admin
Файл hosts (winexe 0.8)	Сканер для сбора файла hosts Windows по протоколу winexe 0.8	admin
Файл hosts (winexe 1.0)	Сканер для сбора файла hosts Windows по протоколу winexe 1.0	admin
Файл hosts (winrm http)	Сканер для сбора файла hosts Windows по протоколу winrm http	admin
Файл hosts (winrm https)	Сканер для сбора файла hosts Windows по протоколу winrm https	admin
Читатели журнала событий (basic) (winrm http)	Сканер для сбора списка пользователей, имеющих доступ к журналам Windows по протоколу winrm http	admin
Читатели журнала событий (basic) (winrm https)	Сканер для сбора списка пользователей, имеющих доступ к журналам Windows по протоколу winrm https	admin
Читатели журнала событий (winexe 0.8)	Сканер для сбора списка пользователей, имеющих доступ к журналам Windows по протоколу winexe 0.8	admin
Читатели журнала событий (winexe 1.0)	Сканер для сбора списка пользователей, имеющих доступ к журналам Windows по протоколу winexe 1.0	admin

Табл. 52. Python-скрипты для сбора данных ОС Windows

НАИМЕНОВАНИЕ	ОПИСАНИЕ	ТЕГ
Читатели журнала событий (winrm http)	Сканер для сбора списка пользователей, имеющих доступ к журналам Windows по протоколу winrm http	admin
Читатели журнала событий (winrm https)	Сканер для сбора списка пользователей, имеющих доступ к журналам Windows по протоколу winrm https	admin

Табл. 53. Python-скрипты для сбора данных ОС Windows CC

НАИМЕНОВАНИЕ	ОПИСАНИЕ	ТЕГ
WinCC6 Группы (SQL, noport)	Сканер для сбора списка групп WINCC 6 по протоколу MS SQL (no port)	dbadmin, instance
WinCC6 Конфигурация (SQL, noport)	Сканер для сбора конфигурации WINCC 6 по протоколу MS SQL (no port)	dbadmin, instance
WinCC6 Пользователи (SQL, noport)	Сканер для сбора списка пользователей WINCC 6 по протоколу MS SQL (no port)	dbadmin, instance
WinCC6 Права групп (SQL, noport)	Сканер для сбора прав групп WINCC 6 по протоколу MS SQL (no port)	dbadmin, instance
WinCC6 Права пользователей (SQL, noport)	Сканер для сбора прав пользователей WINCC 6 по протоколу MS SQL (no port)	dbadmin, instance
WinCC7-авторизация (SQL)	Сканер для сбора списка авторизаций WINCC 7 по протоколу MS SQL	dbadmin
WinCC7-авторизация (SQL, noport)	Сканер для сбора списка авторизаций WINCC 7 по протоколу MS SQL (no port)	dbadmin, instance
WinCC7-группы (SQL)	Сканер для сбора списка групп WINCC 7 по протоколу MS SQL	dbadmin
WinCC7-группы (SQL, noport)	Сканер для сбора списка групп WINCC 7 по протоколу MS SQL (no port)	dbadmin, instance
WinCC7-запуск/останов (winexe)	Сканер для сбора списка событий запуска и останова WINCC 7 по протоколу winexe	admin
WinCC7-запуск/останов (winrm/http)	Сканер для сбора списка событий запуска и останова WINCC 7 по протоколу winrm/http	admin
WinCC7-запуск/останов (winrm/https)	Сканер для сбора списка событий запуска и останова WINCC 7 по протоколу winrm/https	admin

Табл. 53. Python-скрипты для сбора данных ОС Windows CC

НАИМЕНОВАНИЕ	ОПИСАНИЕ	ТЕГ
WinCC7-конфигурация (SQL)	Сканер для сбора списка конфигураций WINCC 7 по протоколу MS SQL	dbadmin
WinCC7-конфигурация (SQL, noport)	Сканер для сбора списка конфигураций WINCC 7 по протоколу MS SQL (noport)	dbadmin, instance
WinCC7-пользователи (SQL)	Сканер для сбора списка пользователей WINCC 7 по протоколу MS SQL	dbadmin
WinCC7-пользователи (SQL, noport)	Сканер для сбора списка пользователей WINCC 7 по протоколу MS SQL (noport)	dbadmin, instance
WinCC7-права групп (SQL)	Сканер для сбора списка прав групп WINCC 7 по протоколу MS SQL	dbadmin
WinCC7-права групп (SQL, noport)	Сканер для сбора списка прав групп WINCC 7 по протоколу MS SQL (noport)	dbadmin, instance
WinCC7-права пользователей (SQL)	Сканер для сбора списка прав пользователей WINCC 7 по протоколу MS SQL	dbadmin
WinCC7-права пользователей (SQL, noport)	Сканер для сбора списка прав пользователей WINCC 7 по протоколу MS SQL (noport)	dbadmin, instance
Проверка настроек проекта визуализации, реализованного на ПО Siemens WinCC (winrm http)	Сканер для проверки настроек проекта визуализации WinCC, реализованного на ПО Siemens по протоколу winrm http	admin
Проверка настроек проекта визуализации, реализованного на ПО Siemens WinCC (winrm https)	Сканер для проверки настроек проекта визуализации WinCC, реализованного на ПО Siemens по протоколу winrm https	admin

Табл. 54. Python-скрипты для инвентаризации объектов Windows

НАИМЕНОВАНИЕ	ОПИСАНИЕ	ТЕГ
ECI_WIN_DEVICES (winrm http)	Сканер для сбора списка устройств Windows по протоколу winrm http	admin
ECI_WIN_DEVICES (winrm https)	Сканер для сбора списка устройств Windows по протоколу winrm https	admin

Табл. 54. Python-скрипты для инвентаризации объектов Windows

НАИМЕНОВАНИЕ	ОПИСАНИЕ	ТЕГ
ECI_WIN_DEVICES (wmi)	Сканер для сбора списка устройств Windows по протоколу wmi	admin
ECI_WIN_DEVICES_- CDROM (winexe 0.8)	Сканер для сбора списка CD-ROM'ов Windows по протоколу winexe 0.8	admin
ECI_WIN_DEVICES_- CDROM (winrm http)	Сканер для сбора списка CD-ROM'ов Windows по протоколу winrm http	admin
ECI_WIN_DEVICES_- CDROM (winrm https)	Сканер для сбора списка CD-ROM'ов Windows по протоколу winrm https	admin
ECI_WIN_DEVICES_- CDROM (wmi)	Сканер для сбора списка CD-ROM'ов Windows по протоколу wmi	admin
ECI_WIN_DEVICES_- CPU (winexe 0.8)	Сканер для сбора списка процессоров Windows по протоколу winexe 0.8	admin
ECI_WIN_DEVICES_- CPU (winrm http)	Сканер для сбора списка процессоров Windows по протоколу winrm http	admin
ECI_WIN_DEVICES_- CPU (winrm https)	Сканер для сбора списка процессоров Windows по протоколу winrm https	admin
ECI_WIN_DEVICES_CPU (wmi)	Сканер для сбора списка процессоров Windows по протоколу wmi	admin
ECI_WIN_DEVICES_- HDD (winexe 0.8)	Сканер для сбора списка физических дисков Windows по протоколу winexe 0.8	admin
ECI_WIN_DEVICES_- HDD (winrm http)	Сканер для сбора списка физических дисков Windows по протоколу winrm http	admin
ECI_WIN_DEVICES_- HDD (winrm https)	Сканер для сбора списка физических дисков Windows по протоколу winrm https	admin
ECI_WIN_DEVICES_HDD (wmi)	Сканер для сбора списка физических дисков Windows по протоколу wmi	admin
ECI_WIN_DEVICES_- LAN (winexe 0.8)	Сканер для сбора списка сетевых адаптеров Windows по протоколу winexe 0.8	admin
ECI_WIN_DEVICES_- LAN (winrm http)	Сканер для сбора списка сетевых адаптеров Windows по протоколу winrm http	admin

Табл. 54. Python-скрипты для инвентаризации объектов Windows

НАИМЕНОВАНИЕ	ОПИСАНИЕ	ТЕГ
ECI_WIN_DEVICES_- LAN (winrm https)	Сканер для сбора списка сетевых адаптеров Windows по протоколу winrm https	admin
ECI_WIN_DEVICES_LAN (wmi)	Сканер для сбора списка сетевых адаптеров Windows по протоколу wmi	admin
ECI_WIN_DEVICES_- MB (winexe 0.8)	Сканер для сбора списка материнских плат Windows по протоколу winexe 0.8	admin
ECI_WIN_DEVICES_- MB (winrm http)	Сканер для сбора списка материнских плат Windows по протоколу winrm http	admin
ECI_WIN_DEVICES_- MB (winrm https)	Сканер для сбора списка материнских плат Windows по протоколу winrm https	admin
ECI_WIN_DEVICES_MB (wmi)	Сканер для сбора списка материнских плат Windows по протоколу wmi	admin
ECI_WIN_DEVICES_- RAM (winexe 0.8)	Сканер для сбора списка физической памяти Windows по протоколу winexe 0.8	admin
ECI_WIN_DEVICES_- RAM (winrm http)	Сканер для сбора списка физической памяти Windows по протоколу winrm http	admin
ECI_WIN_DEVICES_- RAM (winrm https)	Сканер для сбора списка физической памяти Windows по протоколу winrm https	admin
ECI_WIN_DEVICES_RAM (wmi)	Сканер для сбора списка физической памяти Windows по протоколу wmi	admin
ECI_WIN_DEVICES_- VIDEO (winexe 0.8)	Сканер для сбора списка видеоадаптеров Windows по протоколу winexe 0.8	admin
ECI_WIN_DEVICES_- VIDEO (winrm http)	Сканер для сбора списка видеоадаптеров Windows по протоколу winrm http	admin
ECI_WIN_DEVICES_- VIDEO (winrm https)	Сканер для сбора списка видеоадаптеров Windows по протоколу winrm https	admin
ECI_WIN_DEVICES_VIDEO (wmi)	Сканер для сбора списка видеоадаптеров Windows по протоколу wmi	admin
ECI_WIN_DEVICES_- VOLUME (winexe 0.8)	Сканер для сбора списка логических дисков Windows по протоколу winexe 0.8	admin

Табл. 54. Python-скрипты для инвентаризации объектов Windows

НАИМЕНОВАНИЕ	ОПИСАНИЕ	ТЕГ
ECI_WIN_DEVICES_- VOLUME (winrm http)	Сканер для сбора списка логических дисков Windows по протоколу winrm http	admin
ECI_WIN_DEVICES_- VOLUME (winrm https)	Сканер для сбора списка логических дисков Windows по протоколу winrm https	admin
ECI_WIN_DEVICES_- VOLUME (wmi)	Сканер для сбора списка логических дисков Windows по протоколу wmi	admin
ECI_WIN_INVENTORY (winexe 0.8)	Сканер для сбора информации о системе Windows по протоколу winexe 0.8	admin
ECI_WIN_INVENTORY (winrm http)	Сканер для сбора информации о системе Windows по протоколу winrm http	admin
ECI_WIN_INVENTORY (winrm https)	Сканер для сбора информации о системе Windows по протоколу winrm https	admin
ECI_WIN_PROGRAMS PS (winrm http)	Сканер для сбора списка установленного ПО Windows по протоколу winrm http (PS)	admin
ECI_WIN_PROGRAMS PS (winrm https)	Сканер для сбора списка установленного ПО Windows по протоколу winrm https (PS)	admin
ECI_WIN_PROGRAMS WI (winrm http)	Сканер для сбора списка установленного ПО Windows по протоколу winrm http (WI)	admin
ECI_WIN_PROGRAMS WI (winrm https)	Сканер для сбора списка установленного ПО Windows по протоколу winrm https (WI)	admin
ECI_WIN_PROGRAMS WI (wmi)	Сканер для сбора списка установленного ПО Windows по протоколу wmi (WI)	admin
ECI_WIN_PROGRAMS WI PS (winrm http)	Сканер для сбора списка установленного ПО Windows по протоколу winrm http (WI+PS)	admin
ECI_WIN_PROGRAMS WI PS (winrm https)	Сканер для сбора списка установленного ПО Windows по протоколу winrm https (WI+PS)	admin
ECI_WIN_USERS (local, winrm http)	Сканер для сбора списка пользователей Windows по протоколу winrm http	admin
ECI_WIN_USERS (local, winrm http, PS)	Сканер для сбора списка пользователей Windows по протоколу winrm http (PS)	admin

Табл. 54. Python-скрипты для инвентаризации объектов Windows

НАИМЕНОВАНИЕ	ОПИСАНИЕ	ТЕГ
ECI_WIN_USERS (local, winrm https)	Сканер для сбора списка пользователей Windows по протоколу winrm https	admin
ECI_WIN_USERS (local, winrm https, PS)	Сканер для сбора списка пользователей Windows по протоколу winrm https (PS)	admin
ECI_WIN_USERS (local, wmi)	Сканер для сбора списка пользователей Windows по протоколу wmi	admin

3.15. Сетевые взаимодействия Комплексов

В таблице представлены сетевые взаимодействия Комплексов.

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

Табл. 55. Сетевые взаимодействия Комплексов

ИСТОЧНИК ТРАФИКА	ПОРТ НАЗНАЧЕНИЯ (ДЛЯ ВНЕШНИХ АКТИВОВ И СИСТЕМ ПРИВЕДЕНА ПОРТЫ ПО УМОЛЧАНИЮ)	УЗЕЛ НАЗНАЧЕНИЯ	НАЗНАЧЕНИЕ ТРАФИКА
UDV MP уровня Sensor	TCP 135 (MSRPC) TCP 139 TCP 445 (Winexe) TCP 1024-5000 (MSRPC в Windows XP) TCP 49152-65535 (MSRPC в Windows Vista и новее) TCP 5985 TCP 5986 (WinRM) TCP 3306 (MySQL) TCP 1433 (MSSQL)	Активы на базе ОС Windows, СУБД	Взаимодействие с активом (режим опроса)
	TCP 22 (SSH) TCP 23 (Telnet)	Активы на базе ОС Unix, АСО	
	UDP 161 (SNMP) TCP 102 (S7) TCP 502 (Modbus) TCP 44818 (EthernetIP)		
Активы, поддерживающие передачу событий через стандарт	UDP 514 (Syslog 3164) UDP 515 (Syslog 5424) TCP 514 (Syslog 3164 TCP) TCP 515 (Syslog 5424 TCP) UDP 162 (SNMP-trap)	UDV MP уровня Sensor	Пассивный сбор событий от активов

Табл. 55. Сетевые взаимодействия Комплексов

ИСТОЧНИК ТРАФИКА	ПОРТ НАЗНАЧЕНИЯ (ДЛЯ ВНЕШНИХ АКТИВОВ И СИСТЕМ ПРИВЕДЕННЫ ПОРТЫ ПО УМОЛЧАНИЮ)	УЗЕЛ НАЗНАЧЕНИЯ	НАЗНАЧЕНИЕ ТРАФИКА
syslog/SNMP-trap			
UDV MP уровня Sensor	TCP 16379 (redis) – синхронизация настроек TCP 19091 (prometheus) – метрики TCP 15673 (rabbitmq) – получение данных UDP 123 (если Management выступает в роли NTP-сервера для Sensor)	UDV MP уровня Management	Взаимодействие уровня Sensor с уровнем Management. Иницирует соединения всегда сенсор, поэтому его действительный IP-адрес допускается скрывать по технологии NAT (SNAT). Если межсетевой экран стоит уже после SNAT, доступы к уровню Management нужно открывать с использованием виртуального адреса сенсора
UDV MP уровня Sensor (опционально) UDV MP уровня Management	UDP 123 (NTP)	NTP-серверы	Синхронизация времени
UDV MP уровня Management	UDP 514 TCP 514 TCP 25 (SMTP)	Смежная система	Отправка событий и почтовых уведомлений в смежные системы

Табл. 55. Сетевые взаимодействия Комплексов

ИСТОЧНИК ТРАФИКА	ПОРТ НАЗНАЧЕНИЯ (ДЛЯ ВНЕШНИХ АКТИВОВ И СИСТЕМ ПРИВЕДЕННЫ ПОРТЫ ПО УМОЛЧАНИЮ)	УЗЕЛ НАЗНАЧЕНИЯ	НАЗНАЧЕНИЕ ТРАФИКА
	TCP 465 (SMTPS)		
UDV MP уровня Management	TCP 389 (LDAP) или TCP 636 (LDAPS)	LDAP-сервер	Для возможности авторизации поль- зователей UDV MP через службу ка- талогов
APM админи- стративного персонала	TCP 443 (HTTPS) TCP 22 (SSH)	UDV MP уровня Management	Администри- рование UDV MP. SSH — для сер- висного обслу- живания в тер- минале опера- ционной системы
	TCP 22 (SSH)	UDV MP уровня Sensor	Администри- рование UDV MP (сервисное обслу- живание)

3.16. Синтаксис правил корреляции событий

Синтаксис языка EPL схож с SQL-запросами, и его можно описать следующим образом:

Select → поля → из → тип события → фильтр (опционально).

В правилах используются поля нормализованных событий — подробнее см. раздел «Нормализация событий».

Синтаксис на языке EPL на основе популярной конструкции представлен ниже:

```
SELECT [необходимые поля] FROM [тип события]([фильтр событий]).win:time([отслеживаемое время]) GROUP BY [поле для группировки событий] HAVING COUNT([поле по которому ведется счет]) = [порог для появления инцидента]
```

Описание используемых команд и функций приведено в таблице (Таблица 56. Команды, используемые в примере синтаксиса EPL).

Табл. 56. Команды, используемые в примере синтаксиса EPL

КОМАНДА	ПЕРЕВОД НАЗВАНИЯ	ОПИСАНИЕ
SELECT	Выбрать	Выбор некоторых полей для вывода информации в сообщении об инциденте, а также используются агрегирующие функции, примененные к данным полям, и метки. После оператора идут требуемые поля.
FROM	Из	Указание источника – откуда выбирать вышеуказанные поля.
GROUP BY	Группировать по	Группировка событий по определенному полю, указанному после команды. Так, например, можно разделить события по хостам или по обнаруживающему средству, чтобы исключить ложные срабатывания правила.
HAVING	Содержит	Команда для работы с групповыми записями, которая вводит критерий отбора событий, указанный после команды.
COUNT()	Количество	Подсчитывает количество вхождений событий с указанным внутри нее полем.  Внимание: Для корректной работы порога количества условно обнаруженных событий требуется также указать временное окно, иначе счетчик будет увеличиваться перманентно и пересечет порог единожды.
.win:time()	Время	Условие определяет временной промежуток, обозреваемый от обнаруженного по условию события.

В составлении данных запросов необходимо использовать только те поля, которые соответствуют классу события. Описание полей для разных классов приведено далее.

3.16.1. Поддерживаемые типы событий

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

- События генерируемые Комплексом:
 - резервное копирование данных (backup_control);
 - поток данных (datapk_data_flow);
 - действие пользователя (user_action_detected);
 - аутентификация (appliance_authentication);
 - нарушение эталонного состояния конфигурации актива (datapk_host_config_changed);
 - изменение эталонного состояния конфигурации Актив (datapk_reference_config_changed);
 - восстановление эталонного состояния конфигурации Актив (datapk_host_config_restored);
 - обнаружение неизвестного актива (datapk_unknown_host_detected);
 - обнаружение действия пользователя с актива (host_user_action_detected);
 - изменение статуса доступности актива (availability_control);
 - события о настройке, запуске и остановке сбора данных (host_connection);
 - результаты проверок на соответствие требованиям ИБ (oval_control);
 - верификация импортированного Python-скрипта (script_verification_event);
 - контроль событий Комплекса (event_control);
 - события контроля инцидентов (incident_control);
 - события службы обнаружения вторжений (suricata_control);
 - события сканирования домашней сети (home_net_scan_control)
- События KICS4Net (kics4net_event);
 - Поток KICS4Net(kics4net_data_flow);
- События Linux (linux_event);
- События Cisco (cisco_event);
- События RuggedCOM (ruggedcom_event);
- События Eltex (eltex_event);
- События FortiGate (fortigate_event);
- События Hirschmann (hirschmann_event);
- События Enterasys (enterasys_event);
- События Windows (windows_event);
- События, полученные по SNMP (snmp_event);
- События, полученные по Syslog (unknown_syslog_event).

3.16.1.1. Ключевые поля для выборки

Следующие поля являются обязательными при создании правила корреляции, так как данная информация необходима для создания инцидента.

Табл. 57. Обязательные поля

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

3.16.1.2. События Комплекса

Общие поля для событий Комплекса

Общие поля для событий Комплекса приведены в таблице ниже.

Табл. 58. Общие поля для событий Комплекса

ПОЛЕ	ОПИСАНИЕ
observer_name	Сетевое имя регистратора события: актива, сенсора или Комплекса
observer_ip	IP-адрес регистратора события: актива, сенсора или Комплекса
event_code	Идентификатор события
event_type	Тип события

Резервное копирование данных (backup_control)

Поля для событий резервного копирования приведены в таблице ниже.

Табл. 59. Поля для событий резервного копирования

ПОЛЕ	ОПИСАНИЕ
additional_information	Обоснование действия (комментарий) и изменившееся значение
description	Описание выполненного действия
justification	Обоснование выполненного действия
user	Пользователь Комплекса, который выполнил действие
target_hostname	Сетевое имя Комплекса
target_id	Идентификатор Комплекса

Поток данных (datapk_data_flow)

Поля для событий потоков данных приведены в таблице ниже.

Табл. 60. Поля для событий потоков данных

ПОЛЕ	ОПИСАНИЕ
action	Произведенное действие. Возможны следующие варианты: detect или delete
additional_information	Дополнительные данные при автоматическом одобрении (состояние, комментарий, наименование правила)
description	Описание события
protocol	Сетевой протокол передачи данных.  Внимание: Сетевой протокол указывается строчными буквами.
source_ip	IP-адрес источника потока данных
source_mac	MAC-адрес источника потока данных.  Внимание: MAC-адрес источника указывается заглавными буквами.
source_port	Порт источника потока данных
target_ip	IP-адрес получателя потока данных
target_mac	MAC-адрес получателя потока данных.  Внимание: MAC-адрес получателя указывается заглавными буквами.
target_port	Порт получателя потока данных
user	Имя пользователя, выполнившего удаление или создавшего правило одобрения

Действие пользователя (user_action_detected)

Поля для событий действий пользователя приведены в таблице ниже.

Табл. 61. Поля для событий о действиях пользователя

ПОЛЕ	ОПИСАНИЕ
additional_information	Обоснование действия (комментарий) и изменившееся значение
category	Результат (статус выполненного действия) например: OK, cert_error, access_denied
description	Описание выполненного действия
user	Пользователь Комплекса, который выполнил действие
target_hostname	Сетевое имя Комплекса
target_id	Идентификатор Комплекса

Аутентификация (appliance_authentication)

Поля для событий аутентификации в Комплексе приведены в таблице ниже.

Табл. 62. Поля для событий об аутентификации

ПОЛЕ	ОПИСАНИЕ
action	Произведенное действие. Возможны следующие варианты: login или exit
category	Категория события аутентификации Возможны следующие варианты: success, failure или token_expired
description	Описание события
source_ip	IP-адрес с которого совершена попытка аутентификации
user	Имя пользователя, который выполнял попытку аутентификации

Действия с эталонным состоянием конфигурации актива (host_config)

Возможны следующие изменения эталонного состояния конфигурации:

- datapk_host_config_changed — *Нарушено эталонное состояние конфигурации;*
- datapk_reference_config_changed — *Изменено эталонное состояние конфигурации;*
- datapk_host_config_restored — *Восстановлено эталонное состояние конфигурации.*

Поля для событий изменения эталонного состояния конфигурации активов приведены в таблице ниже.

Табл. 63. Поля для событий о состоянии конфигурации актива

ПОЛЕ	ОПИСАНИЕ
additional_information	Список изменений в конфигурации, либо обоснование изменения эталонной конфигурации
category	Категория конфигурации (совпадает с названием сканера сбора конфигурации)
description	Описывает событие изменения конфигурации актива
target_hostname	Сетевое имя актива, на котором обнаружено нарушение эталонного состояния конфигурации
user	Имя пользователя, который изменил эталонную конфигурацию

Обнаружение неизвестного актива (datapk_unknown_host_detected)

Поля для событий обнаружения неизвестных активов приведены в таблице ниже.

Табл. 64. Поля для событий обнаружения неизвестного актива

ПОЛЕ	ОПИСАНИЕ
description	Описание события
target_ip	IP-адрес обнаруженного актива
target_mac	MAC-адрес обнаруженного актива  Внимание: MAC-адрес обнаруженного актива указывается заглавными буквами.

Обнаружение действия пользователя с активом (host_user_action_detected)

Поля для событий о действиях пользователей с активами приведены в таблице ниже.

Табл. 65. Поля для событий о действиях пользователя с активом

ПОЛЕ	ОПИСАНИЕ
action	Произведенное действие (варианты: create, change, change_interface или delete)
additional_information	Дополнительные данные об активе

Табл. 65. Поля для событий о действиях пользователя с активом

ПОЛЕ	ОПИСАНИЕ
target_ip	IP-адрес актива, с которым производят манипуляции
target_hostname	Сетевое имя актива, с которым производят манипуляции
target_mac	MAC-адрес актива, с которым производят манипуляции  Внимание: MAC-адрес актива указывается заглавными буквами.

Изменение статуса доступности актива (availability_control)

Поля для событий о статусе доступности активов приведены в таблице ниже.

Табл. 66. Поля для событий статуса доступности актива

ПОЛЕ	ОПИСАНИЕ
description	Описание доступности интерфейса
target_ip	IP-адрес актива, у которого происходит изменение статуса доступности
target_hostname	Сетевое имя актива, у которого происходит изменение статуса доступности
target_mac	MAC-адрес актива, у которого происходит изменение статуса доступности  Внимание: MAC-адрес указывается заглавными буквами.

События о настройке, запуске и остановке сбора данных (host_connection)

Поля для событий о команде запуска и остановки сбора данных приведены в таблице ниже.

Табл. 67. Поля для событий о подключениях к активу

ПОЛЕ	ОПИСАНИЕ
additional_information	Дополнительные данные (что изменено, ошибки запуска)

Табл. 67. Поля для событий о подключениях к активу

ПОЛЕ	ОПИСАНИЕ
description	Описание и перечень активов, для которых изменяется состояние сбора данных
observer_id	Идентификатор сенсора, выполнившего сбор данных
observer_name	Сетевое имя сенсора, выполнившего сбор данных
source_hostname	Сетевое имя сенсора, выполнившего сбор данных
source_id	Идентификатор сенсора, выполнившего сбор данных
target_hostname	Сетевое имя Комплекса, получающего команду
target_id	Идентификатор актива, с которого осуществлялся сбор данных
target_ip	IP-адрес актива, с которого осуществлялся сбор данных
user	Имя пользователя, который производит действия с задачами

Результат проверок на соответствие требованиям ИБ (oval_event)

Поля для событий о проверках OVAL приведены в таблице ниже.

Табл. 68. Поля для событий о результатах проверок на соответствие требованиям ИБ

ПОЛЕ	ОПИСАНИЕ
action	Статус действия проверки. Возможны следующие варианты: oval_check_success или oval_check_error
additional_information	Статус завершенного действия (например, «Проверка завершена») или вывод ошибки
category	Название группы OVAL-определений
description	Описание проверки на соответствие требованиям ИБ
target_ip	IP-адрес проверяемого актива
target_hostname	Сетевое имя проверяемого актива
target_mac	MAC-адрес проверяемого актива

Табл. 68. Поля для событий о результатах проверок на соответствие требованиям ИБ

ПОЛЕ	ОПИСАНИЕ
	 Внимание: MAC-адрес указывается заглавными буквами.
user	Имя пользователя, который производит проверку на соответствие требованиям ИБ

Верификация импортированного Python-скрипта (script_verification_event)

Поля для событий верификации скриптов приведены в таблице ниже.

Табл. 69. Поля для событий верификации Python-скриптов

ПОЛЕ	ОПИСАНИЕ
additional_information	Вывод ошибки
category	Название сканера, который содержит проверяемый Python-скрипт
description	Описание события Комплекса
request_id	Идентификатор запроса
user	Имя пользователя, который производит манипуляции со сканером
target_hostname	Сетевое имя регистратора события: актива, сенсора или Комплекса
target_id	ID регистратора события: актива, сенсора или Комплекса

Контроль событий Комплекса (event_control)

Поля для контроля событий Комплекса приведены в таблице ниже.

Табл. 70. Поля для контроля событий Комплекса

ПОЛЕ	ОПИСАНИЕ
description	Описание события Комплекса
protocol	Идентификатор источника
source_hostname	Сетевое имя актива
source_ip	IP-адрес актива

Табл. 70. Поля для контроля событий Комплекса

ПОЛЕ	ОПИСАНИЕ
target_hostname	Сетевое имя объекта, над которым выполнялось действие: актива, сенсора или Комплекса
target_id	ID объекта, над которым выполнялось действие: актива, сенсора или Комплекса

События контроля инцидентов (incident_control_event)

Поля для контроля инцидентов приведены в таблице ниже.

Табл. 71. Поля для событий контроля инцидентов

ПОЛЕ	ОПИСАНИЕ
additional_information	Служебные поля инцидента (например, наименование правила корреляции)
description	Описание выполненного действия
justification	Обоснование выполненного действия
incident_id	Идентификатор созданного или измененного инцидента
link	Все id событий, на основе которых сформирован инцидент
target_ip	Все IP-адреса из событий, на основе которых сформирован инцидент  Внимание: Отображаются, только если это явно указано в правилах корреляции.
target_id	Идентификатор регистратора события: актива, сенсора или Комплекса
target_hostname	Сетевое имя регистратора события: актива, сенсора или Комплекса
user	Имя пользователя, который выполнил действие
priority	Текущий приоритет созданного или измененного инцидента

События службы обнаружения вторжений (suricata_event)

Поля для событий службы обнаружения вторжений приведены в таблице ниже.

Табл. 72. Поля для событий службы обнаружения вторжений

ПОЛЕ	ОПИСАНИЕ
action	Действие службы обнаружения вторжений.  Подсказка: Берется из поля action правила службы обнаружения вторжений.
category	Категория события службы обнаружения вторжений.  Подсказка: Берется из поля event_type правила службы обнаружения вторжений.
description	Описание правила срабатывания сигнатуры (IDS)
event_code	Значение поля signature_id правила службы обнаружения вторжений
protocol	Протокол срабатывания правила службы обнаружения вторжений.  Подсказка: Берется из поля app_proto правила службы обнаружения вторжений.
source_ip	IP-адрес отправителя сетевых пакетов
source_port	Порт, по которому отправлены сетевые пакеты
target_ip	IP-адрес получателя сетевых пакетов
target_port	Порт, на который отправлены сетевые пакеты

3.16.1.3. События KICS4Net

Потоки KICS4Net(kics4net_data_flow)

Поля для событий потоков KICS4Net приведены в таблице ниже..

Табл. 73. Поля для событий потоков KICS4Net

ПОЛЕ	ОПИСАНИЕ
category	Наименование точки мониторинга.

Табл. 73. Поля для событий потоков KICS4Net

ПОЛЕ	ОПИСАНИЕ
description	Описание потока.
event_code	Идентификатор типа события в KICS4Net.
observer_name	Сетевое имя регистратора события: актива (сервера KICS4Net), сенсора или Комплекса.
observer_id	IP-адрес регистратора события: актива (сервера KICS4Net), сенсора или Комплекса.
protocol	Название протокола.
source_ip	IP-адрес источника потока данных.
source_mac	MAC-адрес источника потока данных.  Внимание: MAC-адрес указывается заглавными буквами.
source_port	Порт источника потока данных.
target_ip	IP-адрес получателя потока данных.
target_mac	MAC-адрес источника потока данных.  Внимание: MAC-адрес указывается заглавными буквами.
target_port	Порт получателя потока данных.

События KICS4Net (kics4net_event)

Поля для событий KICS4Net приведены в таблице ниже.

Табл. 74. Поля для событий KICS4Net

ПОЛЕ	ОПИСАНИЕ
additional_information	Название сработавшего правила или значение noTrafficDuration.
category	Наименование точки мониторинга.

Табл. 74. Поля для событий KICS4Net

ПОЛЕ	ОПИСАНИЕ
description	Описание потока.
event_code	Идентификатор типа события в KICS4Net.
hostname	Сетевое имя сервера KICS4Net.
ip	IP-адрес KICS4Net.
protocol	Название протокола.
source_ip	IP-адрес источника потока данных.
source_mac	MAC-адрес источника.  Внимание: MAC-адрес указывается заглавными буквами.
source_port	Порт источника потока данных.
target_ip	IP-адрес получателя потока данных.
target_mac	MAC-адрес получателя.  Внимание: MAC-адрес указывается заглавными буквами.
target_port	Порт получателя потока данных.

3.16.1.4. События Linux

Доступные для событий Linux поля приведены в таблице ниже.

Табл. 75. Поля для событий Linux

ПОЛЕ	ОПИСАНИЕ
event_code	Уникальный идентификатор события. Представляет собой facility+severity из protocol_specific_data.
category	Название журнала или процесса Linux.

Табл. 75. Поля для событий Linux

ПОЛЕ	ОПИСАНИЕ
ip	IP-адрес актива.
Дополнительные поля	
description	Описание события.
protocol	Протокол, использованный в событии Linux.
source_ip	IP-адрес источника события при воздействии на Linux.
source_port	Порт источника события при воздействии на Linux.
user	Пользователь, инициировавший событие.

3.16.1.5. События Cisco

Доступные для событий Cisco поля приведены в таблице ниже.

Табл. 76. Поля для событий Cisco

ПОЛЕ	ОПИСАНИЕ
action	Произведенное действие. Содержит значение из facility_mnemonic (кроме ASA).
additional_information	Развернутое значение facility (из словаря), либо название политики для firepower.
category	Категория важности события. Содержит читаемое значение severity (из словаря).
description	Описание события.
event_code	Уникальный идентификатор события. Составляется из Facility-Severity-Mnemonic.
ip	IP-адрес актива.
target_ip	IP-адрес получателя (IP-адрес Cisco или IP-адрес для SNMP).
target_port	Порт получателя или подключения.
Дополнительные поля	

Табл. 76. Поля для событий Cisco

ПОЛЕ	ОПИСАНИЕ
protocol	Протокол событий ACL и протокол доступа событий, связанных с пользователями.
source_ip	IP-адрес источника события (при воздействии на Cisco).
source_port	Порт источника события.
hostname	Сетевое имя актива, с которого пришло событие (если включена отправка hostname на Cisco).
user	Пользователь, инициировавший событие.

3.16.1.6. События RuggedCOM

Доступные для событий RuggedCOM поля приведены в таблице ниже.

Табл. 77. Поля для событий RuggedCOM

ПОЛЕ	ОПИСАНИЕ
event_code	Уникальный идентификатор события. Составляется из facility+severity из protocol_specific_data.
ip	IP-адрес актива.
Дополнительные поля	
user	Пользователь, инициировавший событие.

3.16.1.7. События Eltex

Доступные для событий поля приведены в таблице ниже.

Табл. 78. Поля для событий Eltex

ПОЛЕ	ОПИСАНИЕ
action	Тип выполняемого действия.
category	Группа логирования.
description	Описание события.
event_code	Идентификатор типа события, состоит из category-action.

Табл. 78. Поля для событий Eltex

ПОЛЕ	ОПИСАНИЕ
ip	IP-адрес актива.
protocol	Протокол подключения (только в событиях подключения).
source_ip	IP-адрес источника действия.
target_ip	IP-адрес коммутатора.
user	Имя пользователя, если есть в событии.
Дополнительные поля	
additional_information	Выполненная команда.  Внимание: Только для событий с фиксацией команд.

3.16.1.8. События FortiGate

Доступные для событий FortiGate поля приведены в таблице ниже.

Табл. 79. Поля для событий FortiGate

ПОЛЕ	ОПИСАНИЕ
action	Значение поля action события.
additional_information	Поле msg или название vpn-тоннеля.
category	Тип события.
description	Описание события.
event_code	Значение поля logid.
observer_name	Сетевое имя регистратора события: актива (МЭ fortigate), сенсора или Комплекса.
observer_ip	IP-адрес регистратора события: актива (МЭ fortigate), сенсора или Комплекса.
protocol	Наименование протокола из события.

Табл. 79. Поля для событий FortiGate

ПОЛЕ	ОПИСАНИЕ
source_ip	Значение поля srcip или locip.
source_port	Значение поля srcport или locport.
target_ip	Значение поля dstip или remip.
target_port	Значение поля dstport или remport.
user	Значение поля user.

3.16.1.9. События Hirschmann

Доступные для событий Hirschmann поля приведены в таблице ниже.

Табл. 80. Поля для событий Hirschmann

ПОЛЕ	ОПИСАНИЕ
category	Категория (например: TRAPMGR, HM_HPL_FDB, DOT1S, UNKN).
description	Описание события.
event_code	Уникальный идентификатор события. Состоит из Facility+severity из protocol_specific_data.
ip	IP-адрес актива.

3.16.1.10. События Enterasys

Доступные для событий Enterasys поля приведены в таблице ниже.

Табл. 81. Поля для событий Enterasys

ПОЛЕ	ОПИСАНИЕ
description	Описание события.
event_code	Уникальный идентификатор событий. Состоит из Facility +severity из protocol_specific_data.
ip	IP-адрес актива.
protocol	Протокол подключения (только в событиях подключения).
source_ip	IP-адрес источника событий.

Табл. 81. Поля для событий Enterasys

ПОЛЕ	ОПИСАНИЕ
user	Имя пользователя в событии.

3.16.1.11. События Windows

Доступные для событий Windows поля приведены в таблице ниже.

Табл. 82. Поля для событий Windows

ПОЛЕ	ОПИСАНИЕ
action	Произведенное действие или категория события.
category	Название журнала событий.
description	Описание события.
event_code	Идентификатор события в журнале событий.
observer_name	Имя регистратора события: актива, сенсора или Комплекса.
observer_ip	IP-адрес регистратора события: актива, сенсора или Комплекса.
user	Пользователь, инициировавший событие.
Дополнительные поля	
additional_information	Описание события из внутренней библиотеки Комплекса в соответствии с данными от Microsoft.
source_ip	IP-адрес источника события.
user	Пользователь. Используется поле targetUserName из события.

3.16.1.12. События SNMP

Доступные для событий SNMP поля приведены в таблице ниже.

Табл. 83. Поля для событий SNMP

ПОЛЕ	ОПИСАНИЕ
action	Имя переменной SNMP (snmpTrapOID).
category	Ключевое слово, которое определяет имя объединения для взаимодействия (community_name).

Табл. 83. Поля для событий SNMP

ПОЛЕ	ОПИСАНИЕ
ip	IP-адрес отправителя сообщения.
target_ip	IP-адрес актива, с которого пришло событие.

3.16.1.13. События syslog

Доступные для событий syslog поля приведены в таблице ниже.

Табл. 84. Поля для событий syslog

ПОЛЕ	ОПИСАНИЕ
event_code	Уникальный идентификатор события. Используется facility+severity из protocol_specific_data.
ip	IP-адрес актива.

3.16.2. Фильтр событий

В правилах корреляции заложена возможность установки двух параметров – условий инцидента и фильтра событий.

В данном пункте рассматривается фильтр событий. Его возможно задать после указания типа события. Указанное условие размещается в круглых скобках и должно использовать поля того типа события, которое было задано за скобками.

Пример

Например,

```
windows_event(event_code ="4625" OR event_code ="529")
```

В данном случае происходит условная фильтрация событий ресурса (типа windows_event) по идентификаторам самого ресурса.

Данное условие возможно составить, используя поля поддерживаемых типов, логические операторы и требуемые значения полей, указанные в двойных кавычках.

3.16.3. Временное окно

Для выявления инцидента, основанного на цепочке событий в течение временного диапазона, рекомендуется использовать конструкцию:

```
[тип события]([фильтр событий]).win:time([отслеживаемое время])
```

Пример

Например,

```
windows_event(event_code="4625" OR event_code="529").win:time(180 sec)
```

Поэлементно данное выражение означает следующее:

- точка «.» после описания типа событий и фильтров подразумевает использование какого-либо свойства;
- «win:» - в данном случае пространство имен обозначает «data window» или окно данных;
- «time()» - функция, принимающая значение временного диапазона окна данных, по умолчанию принимает значение в секундах.

Функция time может принимать явно указанные значения:

- дни (days или day);
- часы (hours или hour);
- минуты (min);
- секунды (sec);
- миллисекунды (msec).

Работа функции представлена на рисунке.

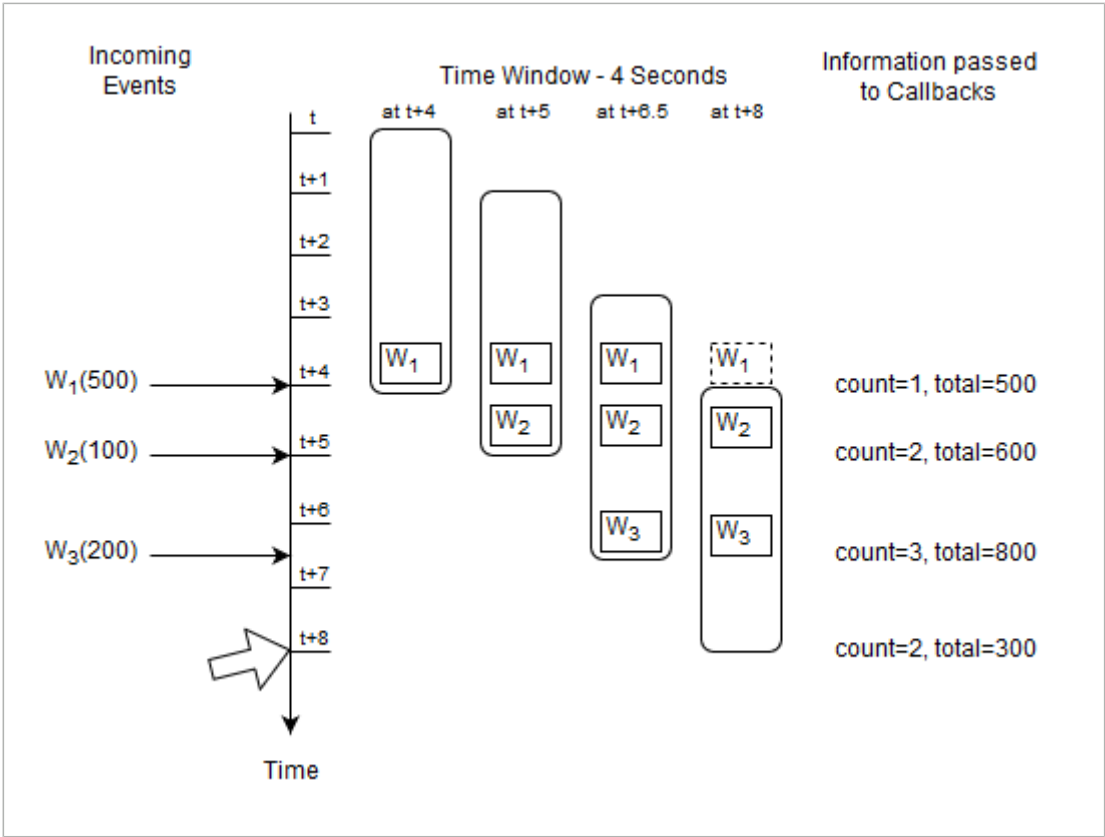


Рис. 52. Работа функции `time()`

На данном рисунке отображены приходящие события (Incoming Events) в виде символов «`Wn`», где `n` – номер события. По временному отрезку движется окно данных с диапазоном в 4 секунды и ведет счет полученных событий. Так, на восьмой секунде отбрасывается первое пришедшее событие, и число событий становится на единицу меньше.

3.16.4. Группировка

В связи с тем, что события бывают от разных объектов, применяют механизм группировки событий для разделения их по активам, исключая ложные срабатывания механизма корреляции.

Так, при использовании команды: `GROUP BY observer_name` несколько одинаковых событий от разных активов не будут образовывать цепочку атаки и приводить к инциденту ИБ.

Особенность данного режима заключается в дальнейшем описании условия возникновения инцидента (при его наличии). Вместо «WHERE», который применяется для описания единичных событий, используется «HAVING». Отсюда, при использовании примера, указанного выше, конструкция принимает вид:

```
GROUP BY observer_name HAVING ...
```

Группировать можно только по тем полям, которые принадлежат выбранному типу событий.

3.16.5. Условие инцидента

Действия, описанные в данной части конструкции правила, вариативные. В качестве примера была отображена функция «COUNT()» и логический оператор «=».

Пример

Например, используя данное условие, возможно вести подсчет событий, пока их количество не превысит заданное:

```
COUNT(event_code) = 3
```

Вместо данной функции можно использовать различные агрегаторы:

- Сумма значений (sum);
- Среднее значение (avg);
- Максимальное значение (max);
- Минимальное значение (min);
- Медианное значение (median);
- Стандартное отклонение значений (stddev);
- Среднее отклонение значений (avedev).

При необходимости глубокого изучения возникновения ошибок, проверки состояния службы и валидации правил в модуле корреляции возможно использовать данные log-записей сервиса `udv-esper`, используя команду, описанную в начале подраздела.

3.16.6. Шаблоны обработки сложных событий

В этом разделе:

- Команда **PATTERN**
- Оператор **EVERY**

С помощью правил корреляции можно создавать модели поведения злоумышленников. Для реализации этого существует такой инструмент, как шаблоны обработки сложных событий.

Пример

Пример использования шаблона:

```
SELECT df.user, df.source_ip, df.target_ip FROM PATTERN@SuppressOverlappingMatches
[EVERY df=cisco_event(df.description="Login Success" OR df.action
"LOGIN_SUCCESS") AND EVERY c=datapk_data_flow(c.action="detect" AND c.protocol="ssh" AND
df.source_ip=c.source_ip)].win:time(180 sec) =
```

Далее рассмотрим применение самого шаблона **PATTERN** и используемый оператор **EVERY**.

3.16.6.1. Команда **PATTERN**

Ключевым словом **PATTERN** для модуля обозначают начало шаблона, описание которого происходит в квадратных скобках далее.

Отсюда, синтаксис для составления шаблона следующий:

```
PATTERN [[первое событие] → [второе событие] AND ...]
```



Подсказка:

Оператор между событиями может быть любой из поддерживаемых языком EPL.

В качестве дополнений шаблонов могут использоваться аннотации. Полный список аннотаций представлен в справочной информации Esper.

Аннотации в шаблонах указываются сразу после ключевого слова **PATTERN** и отличаются знаком «@» в начале обозначения.

Пример

В данном случае рассмотрен пример аннотации «@SuppressOverlappingMatches», означающий подавление совпадений с одним и тем же событием.

Допустим, у нас есть последовательность событий «A₁ A₂ B₁» и правило, которое просматривает каждое совпадение событий A → B (оператор для данного правила рассмотрен ниже). Следовательно, в данном случае мы получим два срабатывания на один инцидент, что в определенной ситуации (например, большого потока событий в один момент времени) сделает оповещения неинформативными. Если же применить аннотацию «@SuppressOverlappingMatches», то в случае последовательности «A₁ A₂ B₁» произойдет одно срабатывание на инцидент ИБ.

3.16.6.2. Оператор EVERY

Рассмотренное в разделе Команда PATTERN правило «каждое совпадение событий $A \rightarrow B$ » представляется возможным благодаря оператору EVERY.

Пример

Для примера возьмем поток событий: « $A_1 B_1 C_1 B_2 A_2 D_1 A_3 B_3 E_1 A_4 F_1 B_4$ », где буква обозначает событие, а индекс — номер события данного типа.

При написании следующей конструкции:

```
EVERY ( A → B )
```

совпадения будут в следующих комбинациях:

```
{A1 , B1 }; {A2 , B3 }; {A4 , B4 }
```

При конструкции:

```
EVERY A → B
```

будут комбинации:

```
{A1 , B1 }; {A2 , B3 }; {A3 , B3 }; {A4 , B4 }
```

Следующая конструкция:

```
A → EVERY B
```

выберет данные комбинации:

```
{A1 , B1 }; {A1 , B2 }; {A1 , B3 }; {A1 , B4 }
```

И при заключительном варианте:

```
EVERY A → EVERY B
```

результат будет следующим:

```
{A1 , B1 }; {A1 , B2 }; {A1 , B3 }; {A2 , B3 }; {A3 , B3 }; {A1 , B4 };  
{A2 , B4 }; {A3 , B4 }; {A4 , B4 }
```

3.16.7. Сообщение инцидента

При создании правила корреляции требуется обозначить текст, отображаемый оператору в случае возникновения инцидента. Чтобы сообщение было более информативным, рекомендуется индивидуализировать его посредством внесения переменных.

Переменными в сообщении могут являться только те поля, которые были «выбраны» командой `SELECT`.

Пример

Например, при указании данного правила:

```
SELECT event_code, observer_name, user, ip FROM windows_event(event_code = "4625" OR event_code = "529").win:time(180 sec) GROUP BY observer_name HAVING COUNT(event_code) = 3
```

возможно использование следующего сообщения оператору:

```
На активе ${observer_name} (${observer_ip}) обнаружен подбор пароля к учетной записи пользователя  
${user}
```

В случае наименования хоста — «GasStation», IP-адреса — 192.168.0.100, атакуемого пользователя «Администратор», по прошествии трех неудачных попыток ввода пароля оператор ИБ получит сообщение об инциденте следующего вида:

```
На активе GasStation ( 192.168.0.100) обнаружен подбор пароля к учетной записи пользователя  
Администратор
```

Для образования информативных сообщений необходимо воспользоваться следующим синтаксисом написания переменных:

```
${ [наименование выводимого поля] }
```

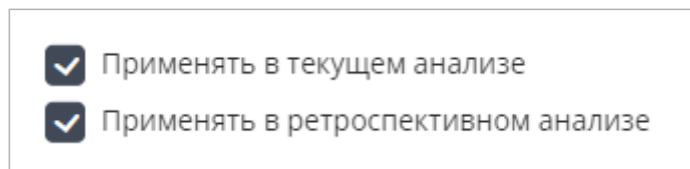
3.16.8. Приоритет и активность правил

Заключительным этапом в создании правила является определение критичности выявляемого инцидента и указание статуса работы правила (активно или неактивно).

Критичность выявляемого инцидента задается в поле «Приоритет» и имеет следующую градацию:

- Низкий
- Средний
- Высокий
- Критический

Статус правила задается чекбоксами («☒») «Применять в текущем анализе» и «Применять в ретроспективном анализе».



The image shows a rectangular box containing two lines of text, each preceded by a checked checkbox icon. The first line reads "Применять в текущем анализе" and the second line reads "Применять в ретроспективном анализе".

Рис. 53. Активные статусы правила корреляции

3.17. События, попадающие в разделы мониторинга

Так как разделы мониторинга предназначены для первичного анализа, не все события попадают в них. Виды и примеры событий, которые попадают в разделы мониторинга, приведены в таблице ([Таблица 85. Основные события Комплекса](#)).



Подсказка:

Виды служебных источников (поле `listener`) см. в разделе [Описание служебных источников событий](#).

Помимо событий от сервисов Комплекса и API могут быть получены события от службы обнаружения вторжений. Поле `event_type` в таких событиях имеет значение «ids_event», а идентификаторы событий отличаются от стандартных.

Табл. 85. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИСТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВАТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫПОЛНЕНИЕ ФУНКЦИИ
1020001	Поток в фоновом режиме помечает доступные интерфейсы	Доступность интерфейса восстановлена	{{ip} – {mac}}: Доступность интерфейса восстановлена (Актив: {netbios_name})	Availability Control	нет (внутренняя пассивная функция Комплекса)	нет
1020002	Поток в фоновом режиме помечает недоступные интерфейсы	Интерфейс недоступен	{{ip} – {mac}}: Интерфейс недоступен (Актив: {netbios_name})	Availability Control	нет (внутренняя пассивная функция Комплекса)	нет
1030001	Запущенную операцию резервного копирования завершить не удалось	Не удалось завершить создание резервной копии в результате ошибки	Обоснование: {justification}; Пользователь: {username}; Ошибка: {exception}	Backup Control	/backup/create POST	Администратор
1030002	Запущенная операция создания резервной копии завершена успешно	Резервная копия	Обоснование: {justification}; Пользователь: {username}	Backup Control	/backup/create POST	Администратор

Табл. 85. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИС- ТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВА- ТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫ- ПОЛНЕНИЕ ФУНКЦИИ
		создана успешно				
1030003	Пользователь запустил со- здание резервной копии	Запущено создание ре- зервной копии	Обоснование: {justification}; Пользо- ватель: {username}	Backup Control	/backup/create POST	Админи- стратор
1050001	Конфигурация собрана впервые и принята за эталон	Изменено эталонное состояние конфи- гурации	Актив: {host_netbios_- name}; Наименование сканера: {scanner_name}	Configuration Control	нет (внутренняя пассивная функция Комплекса)	нет
1050002	Состояние конфигурации не соответствует эталонному	Нарушено эталонное состояние конфи- гурации	Актив: {host_netbios_- name}; Наименование сканера: {scanner_name}; Изменения: {changes}	Configuration Control	Внутренняя проверка очередного (не первого) результата сбора конфигурации после вы- полнения запроса: /config_collection_tasks POST	нет

Табл. 85. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИС- ТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВА- ТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫ- ПОЛНЕНИЕ ФУНКЦИИ
1050004	Пользователь удалил конфигурацию	Удалена конфигурация	Актив: {host_netbios_name}; Наименование сканера: {scanner_name}; Пользователь: {user_login}; Обоснование: {justification}; Собрана: {collected_at}	Configuration Control	/collected_configs/[config_id]/delete POST	Администратор
1050005	Пользователь изменил эталонную конфигурацию	Изменено эталонное состояние конфигурации	Актив: {host_netbios_name}; Наименование сканера: {scanner_name}; Пользователь: {user_login}; Обоснование: {justification}	Configuration Control	/collected_configs/[config_id]/standard POST	Администратор Инженер
1050006	Пользователь удалил все конфигурации сканера	Удалены конфигурации	Актив: {host_netbios_name}; Наименование сканера: {scanner_name}; Пользователь: {user_	Configuration Control	/collected_configs/delete POST	Администратор

Табл. 85. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИС- ТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВА- ТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫ- ПОЛНЕНИЕ ФУНКЦИИ
			login}; Обоснование: {justification}			
1060001	Обнаружен поток данных, не соответствующий ни одному из правил	Обнаружен поток данных	Обнаружен и автоматически одобрен правилом № {rule_number} поток данных; Обнаружен поток данных; {src_ip} [{src_mac}] sport: {sport} host_id: {src_host_id} -> {dst_ip} [{dst_mac}] dport: {dport} host_id: {dst_host_id}({last_protocol_name})	Data Flow Control	нет (внутренняя пассивная функция Комплекса)	нет
1060002	Пользователь отменил изменение статусов потоков	Изменен статус группы потоков данных	Пользователь: {status_changer}; Задача изменения статусов группы потоков данных отменена пользователем; Количество потоков: {data_flows_	Data Flow Control	/data_flows/bulk/background/deletion_task/abort POST	Администратор Инженер

Табл. 85. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИС- ТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВА- ТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫ- ПОЛНЕНИЕ ФУНКЦИИ
			count}; Примененный фильтр: {filter_info}			
1060003	Пользователь изменил статусы потоков	Изменен статус группы потоков данных	Пользователь: {status_ changer}; Количество потоков: {data_flows_ count}; Примененный фильтр: {filter_info}	Data Flow Control	/data_flows/bulk/background/ status_change POST	Админи- стратор Инженер
1060004	Пользователь отменил удаление потоков	Удалена группа потоков данных	Пользователь: {initiator}; Удаление группы потоков данных прервано поль- зователем; Количество потоков: {data_flows_ count}; Примененный фильтр: {filter_info}	Data Flow Control	/data_flows/bulk/background/ deletion_task/abort POST	Админи- стратор Инженер
1060005	Удаление потоков успешно завершилась	Удалена группа потоков данных	Пользователь: {initiator}; Количество потоков: {data_flows_count}; При-	Data Flow Control	/data_flows/bulk/background/deletion POST	Админи- стратор Инженер

Табл. 85. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИС- ТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВА- ТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫ- ПОЛНЕНИЕ ФУНКЦИИ
			мененный фильтр: {filter_info}			
1060007	Пользователь изменил статус нескольких потоков	Изменен статус группы потоков данных	Пользователь: {username}; Количество потоков: {data_flows_count}; Примененный фильтр: {filter_info}	Data Flow Control	/data_flows/bulk/background/status_change POST	Администратор Инженер
1060008	Пользователь изменил статус потока данных	Изменен статус потока данных	Пользователь: {username}; Поток данных: {data_flow_str_repr}; Старое состояние: [{data_flow_old_state}]; Новое состояние: [{data_flow_new_state}]	Data Flow Control	/data_flows/[data_flow_id]/status PUT	Администратор Инженер
1060009	Пользователь удалил поток данных	Удален поток данных	Пользователь: {initiator}; Поток данных {data_flow_repr} был удален	Data Flow Control	/data_flows/[data_flow_id]/delete POST	Администратор Инженер

Табл. 85. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИСТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВАТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫПОЛНЕНИЕ ФУНКЦИИ
1060010	Пользователь изменил комментарий к потоку	Указан комментарий потока данных	Пользователь: {username}; Поток данных {data_flow_str_repr}; Старое состояние [{data_flow_old_state}]; Новое состояние: [{data_flow_new_state}]; Комментарий: {comment}	Data Flow Control	/data_flows/[data_flow_id]/comment PUT	Администратор
1060011	Пользователь изменил домашнюю сеть, в старой оставались потоки	Удалены все потоки данных текущего Комплекса, содержащие IP-адреса	Причина: потоки данных принадлежали старой домашней сети	Data Flow Control	/host_interfaces/home_net PATCH	Администратор
1060012	Потоки данных, не относящиеся к домашней сети, удалены	Удалены все потоки данных вне	Диапазон домашней сети: {ranges}; Причина: потоки	Data Flow Control	нет (внутренняя пассивная функция Комплекса)	нет

Табл. 85. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИС- ТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВА- ТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫ- ПОЛНЕНИЕ ФУНКЦИИ
		домашней сети	данных принадлежали старой домашней сети			
1060013	Удален актив, который со- держался в потоках	Удалены потоки данных в ре- зультате удаления актива	Количество потоков: {data_flows_count}; Актив: {host_id}	Data Flow Control	нет (внутренняя пассивная функция Комплекса)	нет
1060014	Поток попал под правило и был одобрен	Обнаружен и автома- тически одобрен правилom № {rule_ number} поток данных	Обнаружен и автома- тически одобрен правилom № {rule_number} поток данных; Обнаружен поток данных; {src_ip} [{src_ mac}] sport: {sport} host_ id: {src_host_id} -> {dst_ ip} [{dst_mac}] dport: {dport} host_id: {dst_ id}	Data Flow Control	нет (внутренняя пассивная функция Комплекса)	нет

Табл. 85. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИС- ТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВА- ТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫ- ПОЛНЕНИЕ ФУНКЦИИ
			host_id){last_ protocol_name}}			
1070001	Сообщение о запуске регистрации событий	Запущен сервис регистрации событий		System Event	нет (внутренняя пассивная функция Комплекса)	нет
1070002	Сообщение об остановке регистрации событий	Остановлен сервис регистрации событий		System Event	нет (внутренняя пассивная функция Комплекса)	нет
1070003	После остановки получения событий журнал был очищен	Сервис регистрации событий запущен после очистки зарезервированного дис-		System Event	нет (внутренняя пассивная функция Комплекса)	нет

Табл. 85. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИС- ТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВА- ТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫ- ПОЛНЕНИЕ ФУНКЦИИ
		кового про- странства				
1070004	Достигнуто предельное значение размера журнала событий	Сервис регистрации событий остановлен в результате переполнения зарезервированного дискового пространства		System Event	нет (внутренняя пассивная функция Комплекса)	нет
1070005	Выявлено отклонение от указанного минимального количества событий от источника	С источника получено меньше событий, чем указано	Источник: {source_name}; Актив: {host_name} ({host_id}); За {delay} секунд было получено {received} событий, ожи-	System Event	нет (внутренняя пассивная функция Комплекса)	нет

Табл. 85. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИС- ТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВА- ТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫ- ПОЛНЕНИЕ ФУНКЦИИ
		в его пара- метрах	далось {threshold} событий.			
1070006	Новых событий не обнару- жилось в результате вы- полнения задачи	Задача сбора событий успешно вы- полнена, новых событий не обнаружено	Актив: {host_name} ({host_id}); Наименование сканера: {scanner_name}	System Event	нет (внутренняя пассивная функция Комплекса)	нет
1080001	Пользователь создает актив	Создан новый актив	id: {id}; Имя: {netbios_- name}; Описание: {description}; Тип: {host_- type}; ipv4-ipv6-mac: {interfaces_list}	Host Control	/hosts POST	Админи- стратор Инженер
1080002	Пользователь удаляет актив	Удален актив	Обоснование: {justification}; Поль- зователь: {user} id:	Host Control	/hosts/[host_id]/delete POST	Админи- стратор

Табл. 85. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИС- ТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВА- ТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫ- ПОЛНЕНИЕ ФУНКЦИИ
			{id}; Имя: {netbios_name}; Описание: {description}; Тип: {host_type}; ipv4-mac: {interfaces_list}			
1080003	Пользователь редактирует актив	Изменен актив	ID актива: {old_id}; Старые значения: [id: {old_id}; Имя: {old_- netbios_name}; Описание: {old_description}; Тип: {old_host_type}; ipv4-ipv6- mac: {old_interfaces_- list}]; Новые значения: [id: {new_id}; Имя: {new_- netbios_name}; Описание: {new_description}; Тип: {new_host_type}; ipv4-ipv6- mac: {new_interfaces_- list}]; Пользователь: {user}	Host Control	/hosts/[host_id] PATCH	Админи- стратор Инженер

Табл. 85. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИС- ТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВА- ТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫ- ПОЛНЕНИЕ ФУНКЦИИ
1080004	Пользователь изменил домашнюю сеть	Актив был удален в результате изменения адресов домашней сети	id: {id}; Имя: {netbios_name}; Описание: {description}; Тип: {host_type}; ipv4-ipv6-мас: {interfaces_list}	Host Control	/sensors-backend/home_nets PUT	Администратор
1080005	Пользователь изменил домашнюю сеть	Интерфейс был удален в результате изменения адресов домашней сети	ID: {id}; ID актива: {host_id}; Имя: {name}; Интерфейс сбора данных: {default}; ipv4: {ip_v4_address}; mac: {mac_address}	Host Control	/sensors-backend/home_nets PUT	Администратор
1080006	Пользователь удалил несколько активов	Удалены активы	Количество активов: {filtered_count}; Примененный фильтр: [АСУ ТП: {asu_tp}; Типы активов: {host_types}; Метки: {host_labels}; IP-	Host Control	/hosts/bulk/delete POST	Администратор

Табл. 85. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИС- ТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВА- ТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫ- ПОЛНЕНИЕ ФУНКЦИИ
			адреса: {ip_filters}; Активы: {hosts}; Про- изводители: {vendors}; Группы активов: {host_ groups}; Активы без групп: {outside_tree}}; пользо- ватель: {user}; Обос- нование: {justification}			
1080007	Пользователь удалил сетевые атрибуты актива	Отвязан ин-терфейс	[ID: {id}; ID актива: {host_ id}; Имя: {name}; Ин- терфейс сбора данных: {default}; ipv4: {ip_v4_ address}; mac: {mac_ address}} Пользователь: {user}	Host Control	/host_interfaces/[host_interface_id] PATCH	Админи- стратор Инженер
1080008	Пользователь присвоил сетевые атрибуты активу	Привязан интерфейс	[ID: {id}; ID актива: {host_ id}; Имя: {name}; Ин- терфейс сбора данных: {default}; ipv4: {ip_v4_ address}; mac: {mac_ address}} Пользователь: {user}	Host Control	/host_interfaces/[host_interface_id] PATCH	Админи- стратор Инженер

Табл. 85. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИС- ТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВА- ТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫ- ПОЛНЕНИЕ ФУНКЦИИ
			address}; mac: {mac_ address}} Пользователь: {user}			
1080009	Пользователь не изменил данные в карточке актива, но нажал Сохранить	Вместе с сенсором удалены сетевые атрибуты актива	Сенсор: {sensor_name} ({sensor_id}); Актив: {host_name} ({host_id}); Сетевые атрибуты: {ip_v4_address}, {mac_address}	Host Control	/hosts/[host_id] PATCH	Администратор Инженер
1080010	Сетевые атрибуты присвоены активу	Интерфейс привязан к активу	Интерфейс <{ip}, {mac}> был привязан к активу <{netbios_name}, {host_id}>	Host Control	нет (внутренняя пассивная функция Комплекса)	нет
1080011	Комплекс сканирует домашнюю сеть	Обнаружен неизвестный актив	id: {host_id}; ip-mac: [{ip} - {mac}]	Host Control	нет (внутренняя пассивная функция Комплекса)	нет

Табл. 85. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИС- ТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВА- ТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫ- ПОЛНЕНИЕ ФУНКЦИИ
1080013	Отправлены пустые данные для изменения актива	Вместе с сенсором удален актив	Сенсор: {sensor_name} ({sensor_id}); Актив: {netbios_name} ({id}); Сетевые атрибуты: {ip}, {mac}	Host Control	нет (внутренняя пассивная функция Комплекса)	нет
1080015	Пользователь удалил несколько групп активов	Изменены группы активов	Пользователь: {user}; Число удаленных групп активов: {removed_host_groups_quantity}; Число созданных групп активов: {created_host_groups_quantity}; Число измененных групп активов: {changed_host_groups_quantity}; Число неизмененных групп активов: {unchanged_host_groups_quantity}	Host Control	<code>/host_groups/replace</code> <code>PUT</code>	Администратор

Табл. 85. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИС- ТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВА- ТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫ- ПОЛНЕНИЕ ФУНКЦИИ
1080016	Один и тот же IP-адрес присвоен более, чем одному активу	Обнаружено дубли- рование IP- адреса	IP-адрес: {duplicated_ip}; Актив 1: {target_name} ({target_id}, {target_ip}, {target_mac}); Актив 2: {source_name} ({source_ id}, {source_ip}, {source_ mac}); Сенсор: {observer_ id} ({observer_name}).	Host Control	нет (внутренняя пассивная функция Комплекса)	нет
1080017	Одно и то же на- именование присвоено нескольким активам	Обнаружены активы с совпа- дающим сетевым именем	Обнаружены активы с совпадающим сетевым именем: {target_name} ({target_id}, {target_ ip}, {target_mac}, сенсор: {target_sensor_name}) и {source_name} ({source_ id}, {source_ip}, {source_ mac}, сенсор: {source_ sensor_name}).	Host Control	нет (внутренняя пассивная функция Комплекса)	нет

Табл. 85. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИСТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВАТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫПОЛНЕНИЕ ФУНКЦИИ
1080018	Пользователь создал сетевые атрибуты актива	Созданы сетевые атрибуты актива	ID актива: {host_id}; {interface_str}	Host Control	/host_interfaces POST	Администратор Инженер
1080019	Пользователь удалил сетевые атрибуты актива	Удалены сетевые атрибуты актива	ID актива: {host_id}; {interface_str}	Host Control	/host_interfaces/{interface_id} DELETE	
1080020	Пользователь изменил сетевые атрибуты актива	Изменены сетевые атрибуты актива	ID актива: {host_id}; interface_id; Старые значения: [{old_values}]; Новые значения: [{new_values}]	Host Control	/host_interfaces/{interface_id} PATCH	
1080022	Пользователь присвоил учетные данные активу	Присвоены учетные данные активу	Актив: {host_netbios_name}; Учетные данные: {cred_name}; Пользователь: {user_login}	Host Control	/host_data_collector/ host_credential_relations/bulk/ replace	Администратор Инженер

Табл. 85. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИС- ТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВА- ТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫ- ПОЛНЕНИЕ ФУНКЦИИ
					POST	
1080023	Пользователь отменил присвоение учетных данных активу	Отменено присвоение учетных данных активу	Актив: {host_netbios_name}; Учетные данные: {cred_name}; Пользователь: {user_login}	Host Control	/host_data_collector/ host_credential_relations/bulk/ replace POST	
1080024	Пользователь удалил учетные данные актива	Удалены учетные данные активов	Наименование УД: {cred_name}; активы, которым были присвоены УД: {host_netbios_names}; Пользователь: {user}; Обоснование: {justification}	Host Control	host_data_collector/credentials/ [credentials_id]/delete POST	
1080025	Пользователь удалил несколько учетных данных активов	Удалено {count} учетных данных активов	Наименование УД: {cred_names}; Пользователь: {user}; Обоснование: {justification}	Host Control	host_data_collector/credentials POST	

Табл. 85. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИС- ТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВА- ТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫ- ПОЛНЕНИЕ ФУНКЦИИ
1080026	Пользователь добавил учетные данные активов	Добавлены учетные данные активов	Наименование УД: {cred_ name}; Пользователь: {user}	Host Control	host_data_collector/credentials/bulk/ delete?name=[cred_name] POST	
1080027	Пользователь изменил учетные данные активов	Изменены учетные данные активов	Наименование УД: {cred_ name}; Пользователь: {user}	Host Control	host_data_collector/credentials/ [cred_id] PATCH	
1090023	Пользователь удаляет скрипт OVAL	Удален скрипт OVAL	Пользователь: {user}; Обос- нование: {justification}; Название: {script_name}; Описание: {script_ description}	Host Data Collecting	/host_data_collector/oval/scripts/ [script_id]/delete POST	Админи- стратор
1090024	Пользователь удаляет несколько скриптов OVAL	Удалены скрипты OVAL	Пользователь: {user}; Обос- нование: {justification}; Удалено: {deleted_count}	Host Data Collecting	/host_data_collector/oval/scripts/ bulk/delete POST	

Табл. 85. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИСТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВАТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫПОЛНЕНИЕ ФУНКЦИИ
1090201	Пользователь импортирует группы сканеров	Импортированы группы сканеров	Пользователь: {user}; Импортировано {count} из {file_count} групп; Выбранное действие для добавленных ранее элементов: {action_for_missing_elements}	Host Data Collecting	/exporter/import/catalogs/file?catalog=scanner_groups PUT	Администратор
1090202	Пользователь экспортирует группы сканеров	Экспортированы группы сканеров	Пользователь: {user}	Host Data Collecting	/exporter/export/catalogs/file?catalog=scanner_groups POST	Администратор Инженер
1090203	Пользователь создает сканер	Создан сканер	Пользователь: {user}; Тип: {scanner_type}; Наименование: {scanner_name}; Группы сканеров: {scanner_group_name}	Host Data Collecting	/host_data_collector/scanners POST	Администратор

Табл. 85. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИС- ТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВА- ТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫ- ПОЛНЕНИЕ ФУНКЦИИ
1090206	Пользователь запускает сканер	Запущен сканер на активе	Пользователь: {user}; Тип: {scanner_type}; Наименование: {scanner_name}; Актив: {host_name} ({host_id});	Host Data Collecting	/host_data_collector/scanners/execute POST	Администратор Инженер
1090208	Пользователь редактирует сканер	Изменен сканер	Пользователь: {user}; Предыдущее состояние: [Наименование: {old_scanner_name}; Описание: {old_scanner_description}; Тип {old_scanner_type}; Группа {old_scanner_group_name}]; Новое состояние: [Наименование: {new_scanner_name}; Описание: {new_scanner_description}; Тип {new_scanner_type}; Группа	Host Data Collecting	/host_data_collector/scanners/[scanner_id] PATCH	Администратор

Табл. 85. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИС- ТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВА- ТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫ- ПОЛНЕНИЕ ФУНКЦИИ
			{new_scanner_group_ - name}};			
1090209	Пользователь удаляет несколько групп сканеров	Удалены группы сканеров	Пользователь: {user}; Коли- чество: {deleted_count}	Host Data Collecting	/host_data_collector/scanner_groups/ bulk/delete POST	
1090210	Пользователь удаляет группу сканеров	Удалена группа сканеров	Пользователь: {user}; На- именование: {scanner_ - group_name}	Host Data Collecting	/host_data_collector/scanner_groups/ [id]/delete POST	
1090211	Пользователь удаляет несколько сканеров сбора данных	Удалены сканеры	Пользователь: {user}; Обос- нование: {justification}; Количество: {deleted_ - count}	Host Data Collecting	/scanners/bulk/delete POST	
1090212	Пользователь удаляет сканер сбора данных	Удален сканер	Пользователь: {user}; Обос- нование: {justification}; Наименование: {scanner_ -	Host Data Collecting	/scanners/[scanner_id]/delete POST	

Табл. 85. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИС- ТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВА- ТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫ- ПОЛНЕНИЕ ФУНКЦИИ
			name}; Описание: {scanner_description}; Тип: {scanner_type}			
1090213	Пользователь удаляет сканер, который используется при сборе данных	Удален сканер во время выполнения сбора данных	Пользователь: {user}; Обоснование: {justification}; Результаты сбора не будут сохранены; Задачи, где использовался сканер: {task_name}; Наименование: {scanner_name}; Описание: {scanner_description}; Тип: {scanner_type}	Host Data Collecting	/scanners/[scanner_id]/delete POST	
1090214	В результате выполнения сканера получен некорректный ответ	Обнаружена ошибка соединения при выполнении сканера	Актив: {host_netbios_name} ({host_id}); Сканер: {scanner_name}; Задачи: {task_names}; Ошибка: {error}	Host Data Collecting	/config_collection_tasks POST или /commands/create_event_task	Администратор Инженер

Табл. 85. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИС- ТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВА- ТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫ- ПОЛНЕНИЕ ФУНКЦИИ
		сбора данных			POST	
1090215	Сбор данных завершился ошибкой	Обнаружена ошибка сбора при выполнении сканера сбора данных	Актив: {host_netbios_name} ({host_id}); Сканер: {scanner_name}; Задачи: {task_names}; Ошибка: {error}	Host Data Collecting	нет (внутренняя пассивная функция Комплекса)	нет
1090301	Пользователь импортирует задачи сбора данных	Импортированы задачи сбора данных	Пользователь: {user}; Импортировано {count} из {file_count} групп; Выбранное действие для добавленных ранее элементов: {action_for_missing_elements}	Host Data Collecting	/exporter/import/catalogs/file?catalog=collection_tasks PUT	Администратор Инженер

Табл. 85. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИС- ТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВА- ТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫ- ПОЛНЕНИЕ ФУНКЦИИ
1090302	Пользователь экспортирует задачи сбора данных	Экспорти- рованы задачи сбора данных	Пользователь: {user}	Host Data Collecting	/exporter/export/catalogs/file? catalog=collection_tasks POST	
1090303	Пользователь создает задачу сбора данных	Создана задача сбора данных	Пользователь: {user}; На- именование: {task_name}; Активность: {activity}; Время запуска расписания: {start_date}; Тип запуска: {type}	Host Data Collecting	/host_data_collector/collection/tasks POST	
1090304	Пользователь меняет ак- тивность нескольких задач сбора данных	Изменена активность задач сбора данных	Пользователь: {user}; Обос- нование: {justification}; Статус активности: {activity}; Наименование: {tasks_name}; Количество: {updated_count}	Host Data Collecting	/host_data_collector/collection/ tasks/bulk/activity POST	

Табл. 85. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИС- ТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВА- ТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫ- ПОЛНЕНИЕ ФУНКЦИИ
1090305	Пользователь редактирует задачу сбора данных	Изменена задача сбора данных	Пользователь: {user}; Предыдущее состояние: [Наименование: {old_name}; Описание: {old_description}; Период запуска {old_cron}; Время старта {old_start_date}; Время завершения {old_end_date}; Активность {old_active}; Список групп сканеров {old_scanner_groups_ids}; Список групп активов {old_host_groups_ids}; Список активов {old_host_ids}]; Новое состояние: [Наименование: {new_name}; Описание: {new_description}; Период запуска {new_cron}; Время	Host Data Collecting	/host_data_collector/collection/tasks/{task_id} PATCH	

Табл. 85. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИС- ТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВА- ТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫ- ПОЛНЕНИЕ ФУНКЦИИ
			старта {new_start_date}; Время завершения {new_end_date}; Активность {new_active}; Список групп сканеров {new_scanner_groups_ids}; Список групп активов {new_host_groups_ids}; Список активов {new_host_ids}]			
1090308	Пользователь удаляет несколько задач сбора данных	Удалены задачи сбора данных	Пользователь: {user}; Обоснование: {justification}; Количество: {count} задач	Host Data Collecting	/host_data_collector/collection/tasks/bulk/delete DELETE	
1090309	Пользователь удаляет задачу сбора данных	Удалена задача сбора данных	Пользователь: {user}; Обоснование: {justification}; Наименование: {task_name}; Группы сканеров: {scanner_groups}; Активы: {host_names}; Группы	Host Data Collecting	/host_data_collector/collection/tasks/[task_id] DELETE	

Табл. 85. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИСТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВАТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫПОЛНЕНИЕ ФУНКЦИИ
			активов: {host_group_names}			
1090310	Получен результат сбора данных	Сбор данных успешно выполнен	Тип: {scanner_type}; Актив: {host_netbios_name}; Сканер: {scanner_name}	Host Data Collecting	/config_collection_tasks POST или /commands/create_event_task POST	
1090313	Пользователь удаляет несколько результатов сбора данных	Удалены статусы сбора данных	Пользователь: {user}; Обоснование: {justification}; Количество удаленных результатов: {deleted_count}	Host Data Collecting	/host_data_collector/collection/logs/bulk/delete DELETE	Администратор
1090314	Пользователь удаляет статус сбора данных	Удален статус сбора данных	Пользователь: {user}; Обоснование: {justification}; Сканер: {scanner_name}; Актив: {host_name}; Задачи:	Host Data Collecting	/host_data_collector/collection/logs/delete POST	

Табл. 85. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИСТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВАТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫПОЛНЕНИЕ ФУНКЦИИ
			{task_names}; Результат: {result_type}; Дата получения: {updated_at}			
1100001	Пользователь удаляет статус инцидентов	Удален пользовательский инцидент	Обоснование: {justification}; Пользователь: {user}; Название: {name}; Категория: {category}	Incident Control	/incident_statuses/[status_id]/delete DELETE	Администратор
1100003	Пользователь создает статус инцидента	Создан пользовательский статус инцидента	Обоснование: {justification}; Пользователь: {user}; Новый статус: [Название: {name}; Категория: {category}]	Incident Control	/incident_manager/statuses POST	
1100004	Пользователь редактирует статус инцидента	Изменен пользовательский статус инцидента	Обоснование: {justification}; Пользователь: {user}; Предыдущий статус: [Название: {name}; Категория: {category}]	Incident Control	/incident_manager/statuses/[status_id] PATCH	

Табл. 85. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИС- ТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВА- ТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫ- ПОЛНЕНИЕ ФУНКЦИИ
			{category}}; Новый статус: [Название: {new_name}; Ка- тегория: {new_category})			
1100005	Пользователь редактирует параметры инцидента	Изменен ин- цидент	Комментарий: {action_ comment}; Пользователь: {user}; Предыдущий статус: {status}; Название: {name}; Описание: Изменен ин- цидент; Приоритет: {priority}; Комментарий: {comment}; Подтвержден: {is_confirmed}; Новый статус: {new_status}; На- звание: {new_name}; Описание: {new_ description}; Приоритет: {new_priority}; Ком- ментарий: {new_comment};	Incident Control	/incident/[incident_id] PATCH	Админи- стратор Инженер

Табл. 85. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИС- ТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВА- ТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫ- ПОЛНЕНИЕ ФУНКЦИИ
			Подтвержден: {new_is_ confirmed}			
1100006	Пользователь удаляет инцидент	Удален инцидент	Обоснование: {justification}; Пользователь: {user}; Название: {name}; Описание: Удален инцидент; Приоритет: {priority}; Статус: {status}; Комментарий: {comment}; Подтвержден: {is_confirmed}	Incident Control	/incident/[incident_id] DELETE	
1100007	Пользователь удаляет несколько инцидентов	Удалена группа инцидентов	Обоснование: {justification}; Пользователь: {user}; Количество удаленных инцидентов: {deleted_incident_count}; Примененный фильтр: {filter_info}	Incident Control	/incidents/bulk/delete DELETE	

Табл. 85. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИСТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВАТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫПОЛНЕНИЕ ФУНКЦИИ
1100008	Пользователь отменяет групповое удаление инцидентов	Удаление инцидентов прервано пользователем	Обоснование: {justification}; Пользователь: {user}; Количество удаленных инцидентов: {deleted_incident_count}; Примененный фильтр: {filter_info}	Incident Control	/incidents/bulk/stop_deletion POST	Администратор Инженер
1100009	Пользователь меняет параметры нескольких инцидентов	Изменена группа инцидентов	Комментарий: {action_comment}; Пользователь: {user}; Количество измененных инцидентов: {incident_count}; Примененный фильтр: {filter_info}	Incident Control	/incidents/bulk/update POST	Администратор Инженер
1100010	Пользователь отменяет групповое изменение параметров инцидентов	Задача обновления инцидентов была отменена	Комментарий: {action_comment}; Пользователь: {user}; Количество измененных инцидентов: {incident_count}	Incident Control	/incidents/bulk/stop_update POST	Администратор Инженер

Табл. 85. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИС- ТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВА- ТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫ- ПОЛНЕНИЕ ФУНКЦИИ
		менена пользо- вателем	{incident_count}; Приме- ненный фильтр: {filter_ info}			
1100011	Срабатывает правило кор- реляции	Обнаружен инцидент	Описание: {incident_ description}; Правило: {rule_name}; Активы: {host_ids}; Приоритет: {priority}; Тип инцидента: {incident_type}; иденти- фикатор проверки: {retro_ entry_id}	Incident Control	нет (внутренняя пассивная функция Комплекса)	нет
1110001	Пользователь прерывает выполнение проверки на со- ответствие требованиям ИБ	Выполнение проверки прервано	Название проверки: {assessment_title}; На- звание актива: {host_ netbios_name}; ID актива: {assessment_host_id}; Пользователь: {assessment_created_by}; Результат: {assessment_ }	Oval Assessment Control	/oval_scanner/oval/assessments/ [assessment_id]/cancel POST	Админи- стратор

Табл. 85. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИС- ТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВА- ТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫ- ПОЛНЕНИЕ ФУНКЦИИ
			status_value}; Описание: Выполнение проверки прервано; Время запуска проверки: {assessment_ created_at}; Время окончания проверки: {assessment_updated_at}; IP актива: {host_ interface_ip_v4_address}; MAC актива: {host_ interface_mac_address}			
1110002	Проверка на соответствие требованиям ИБ не за- вершена в результате пре- вышения времени ожидания	Превышено время ожидания выполнения задачи проверки	Название проверки: {assessment_title}; На- звание актива: {host_ netbios_name}; ID актива: {assessment_host_id}; Пользователь: {assessment_created_by}; Результат: {assessment_ status_value}	Oval Assessment Control	/oval_scanner/oval/assessments POST	Админи- стратор Инженер

Табл. 85. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИС- ТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВА- ТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫ- ПОЛНЕНИЕ ФУНКЦИИ
			status_value}; Описание: Превышено время ожидания выполнения задачи проверки; Время запуска проверки: {assessment_created_at}; Время окончания проверки: {assessment_updated_at}; IP актива: {host_- interface_ip_v4_address}; MAC актива: {host_- interface_mac_address}; Ошибка: {timeout_error}			
1110003	Проверка на соответствие требованиям ИБ удалена до ее завершения	Задача проверки была удалена в процессе выполнения	Название проверки: {assessment_title}; На- звание актива: {host_- netbios_name}; ID актива: {assessment_host_id}; Пользователь:	Oval Assessment Control	/oval_scanner/oval/assessments/ [assestment_id]/delete POST	Админи- стратор

Табл. 85. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИС- ТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВА- ТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫ- ПОЛНЕНИЕ ФУНКЦИИ
			{assessment_created_by}; Результат: {assessment_- status_value}; Описание: Задача проверки была удалена в процессе вы- полнения; Время запуска проверки: {assessment_- created_at}; Время окончания проверки: {assessment_updated_at}; IP актива: {host_- interface_ip_v4_address}; MAC актива: {host_- interface_mac_address}			
1110004	При выполнении проверки на соответствие требованиям ИБ получена ошибка	Ошибка выполнения задачи проверки	Название проверки: {assessment_title}; На- звание актива: {host_- netbios_name}; ID актива: {assessment_host_id};	Oval Assessment Control	/oval_scanner/oval/assessments POST	Админи- стратор Инженер

Табл. 85. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИС- ТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВА- ТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫ- ПОЛНЕНИЕ ФУНКЦИИ
			Пользователь: {assessment_created_by}; Результат: {assessment_status_value}; Описание: Ошибка выполнения задачи проверки; Время запуска проверки: {assessment_created_at}; Время окончания проверки: {assessment_updated_at}; IP актива: {host_interface_ip_v4_address}; MAC актива: {host_interface_mac_address}; Ошибка: {error}			
1110005	При выполнении проверки на соответствие требованиям ИБ произошла ошибка	Непредвиденная ошибка выполнения	Название проверки: {assessment_title}; На- звание актива: {host_netbios_name}; ID актива:	Oval Assessment Control		

Табл. 85. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИС- ТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВА- ТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫ- ПОЛНЕНИЕ ФУНКЦИИ
		задачи проверки	{assessment_host_id}; Пользователь: {assessment_created_by}; Результат: {assessment_- status_value}; Описание: Непредвиденная ошибка выполнения задачи проверки; Время запуска проверки: {assessment_- created_at}; Время окончания проверки: {assessment_updated_at}; IP актива: {host_- interface_ip_v4_address}; MAC актива: {host_- interface_mac_address}; Ошибка: {error}			

Табл. 85. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИС- ТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВА- ТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫ- ПОЛНЕНИЕ ФУНКЦИИ
1110006	В результате проверки на соответствие требованиям ИБ обнаружены несоответствия и уязвимости	Выполнение проверки завершено успешно	Название проверки: {assessment_title}; Название актива: {host_netbios_name}; ID актива: {assessment_host_id}; Пользователь: {assessment_created_by}; Результат: {assessment_status_value}; Описание: Выполнение проверки завершено успешно; Время запуска проверки: {assessment_created_at}; Время окончания проверки: {assessment_updated_at}; IP актива: {host_interface_ip_v4_address}; MAC актива: {host_interface_mac_address}; {self.assessment_	Oval Assessment Control		

Табл. 85. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИС- ТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВА- ТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫ- ПОЛНЕНИЕ ФУНКЦИИ
			status_value}; Количество OVAL-определений: {oval_definitions_count}; Количество выполненных проверок: {performed_checks_count}; Состояние соответствия: есть несоответствия/есть уязвимости; Количество выявленных несоответствий: {compliance_false_count}; Количество выявленных уязвимостей: {vulnerabilities_true_count}			
1110007	В результате проверки на соответствие требованиям ИБ обнаружены несоответствия	Выполнение проверки завершено успешно	Название проверки: {assessment_title}; Название актива: {host_netbios_name}; ID актива:	Oval Assessment Control		

Табл. 85. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИС- ТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВА- ТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫ- ПОЛНЕНИЕ ФУНКЦИИ
			{assessment_host_id}; Пользователь: {assessment_created_by}; Результат: {assessment_- status_value}; Описание: Выполнение проверки за- вершено успешно; Время запуска проверки: {assessment_created_at}; Время окончания проверки: {assessment_updated_at}; IP актива: {host_- interface_ip_v4_address}; MAC актива: {host_- interface_mac_address}; {self.assessment_- status_value};Количество OVAL-определений: {oval_- definitions_count}; Ко- личество выполненных			

Табл. 85. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИС- ТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВА- ТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫ- ПОЛНЕНИЕ ФУНКЦИИ
			проверок: {performed_ - checks_count}; Состояние соответствия: есть несоот- ветствия/уязвимостей нет; Количество выявленных несоответствий: {compliance_false_count}; Количество выявленных уязвимостей: {vulnerabilities_true_ - count}			
1110008	В результате проверки на соответствие требованиям ИБ обнаружены уязвимости	Выполнение проверки завершено успешно	Название проверки: {assessment_title}; На- звание актива: {host_ - netbios_name}; ID актива: {assessment_host_id}; Пользователь: {assessment_created_by}; Результат: {assessment_ -	Oval Assessment Control		

Табл. 85. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИС- ТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВА- ТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫ- ПОЛНЕНИЕ ФУНКЦИИ
			status_value}; Описание: Выполнение проверки за- вершено успешно; Время запуска проверки: {assessment_created_at}; Время окончания проверки: {assessment_updated_at}; IP актива: {host_- interface_ip_v4_address}; MAC актива: {host_- interface_mac_address}; {self.assessment_- status_value};Количество OVAL-определений: {oval_- definitions_count}; Ко- личество выполненных проверок: {performed_- checks_count}; Состояние соответствия: соответ- ствуют/есть уязвимости; Ко-			

Табл. 85. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИС- ТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВА- ТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫ- ПОЛНЕНИЕ ФУНКЦИИ
			личество выявленных несоответствий: {compliance_false_count}; Количество выявленных уязвимостей: {vulnerabilities_true_count}			
1110009	В результате проверки на соответствие требованиям ИБ уязвимости и несоответствия не обнаружены	Выполнение проверки завершено успешно	Название проверки: {assessment_title}; Название актива: {host_netbios_name}; ID актива: {assessment_host_id}; Пользователь: {assessment_created_by}; Результат: {assessment_status_value}; Описание: Выполнение проверки завершено успешно; Время запуска проверки: {assessment_created_at};	Oval Assessment Control		

Табл. 85. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИС- ТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВА- ТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫ- ПОЛНЕНИЕ ФУНКЦИИ
			Время окончания проверки: {assessment_updated_at}; IP актива: {host_interface_ip_v4_address}; MAC актива: {host_interface_mac_address}; {self.assessment_status_value};Количество OVAL-определений: {oval_definitions_count}; Ко- личество выполненных проверок: {performed_checks_count}; Состояние соответствия: соответ- ствуют/уязвимостей нет; Ко- личество выявленных несо- ответствий: {compliance_false_count}; Количество выявленных уязвимостей:			

Табл. 85. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИС- ТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВА- ТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫ- ПОЛНЕНИЕ ФУНКЦИИ
			{vulnerabilities_true_count}			
1110010	В результате проверки на соответствие требованиям ИБ получена ошибка	Ошибка получения результатов задачи проверки	Название проверки: {assessment_title}; Название актива: {host_netbios_name}; ID актива: {assessment_host_id}; Пользователь: {assessment_created_by}; Результат: {assessment_status_value}; Описание: Ошибка получения результатов задачи проверки; Время запуска проверки: {assessment_created_at}; Время окончания проверки: {assessment_updated_at}; IP актива: {host_interface_ip_v4_address};	Oval Assessment Control		

Табл. 85. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИС- ТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВА- ТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫ- ПОЛНЕНИЕ ФУНКЦИИ
			MAC актива: {host_ interface_mac_address}; Ошибка: {error}			
1110011	Пользователь удаляет несколько проверок на соот- ветствие требованиям ИБ	Удалены проверки OVAL	Обоснование: {justification}; Поль- зователь: {user_login}; Фильтр: [Активы: {filter_ hosts}; Инициатор: {filter_created_by}; Статус: {filter_status}; Дата обновления от: {filter_updated_at_from}; Дата обновления до: {filter_updated_at_to}; Название: {filter_title}}; Количество удаленных проверок: {deleted_count}	Oval Assessment Control	/host_data_collector/oval/ assessments/bulk/delete DELETE	Админи- стратор Инженер

Табл. 85. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИС- ТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВА- ТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫ- ПОЛНЕНИЕ ФУНКЦИИ
1110012	Пользователь удаляет проверку на соответствие требованиям ИБ	Удалена проверка	Пользователь: {user_login}; Обоснование: {justification}; Проверка: [Название: {assessment_title}; Наименование актива: {host_netbios_name}; Инициатор: {assessment_created_by}; Статус: {assessment_status}]	Oval Assessment Control	/host_data_collector/oval/assessments/[assessment_id]/delete DELETE	
1120001	Пользователь удаляет OVAL-определение	Удалено OVAL-определение	Пользователь: {user_login}; Обоснование: {justification}; OVAL-определение: [Название: {definition_title}; Описание: {definition_description}; Тип: {definition_type}; OVAL-	Oval Definitions Control	oval_scanner/oval/definitions/delete POST	

Табл. 85. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИС- ТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВА- ТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫ- ПОЛНЕНИЕ ФУНКЦИИ
			идентификатор: {definition_oval_id}]			
1120002	Пользователь удаляет несколько OVAL-определений	Удалены OVAL-определения	Пользователь: {user_login}; Обоснование: {justification}; Фильтр: [Название: {definition_title}; Описание: {definition_description}; Тип проверки: {definition_type}; OVAL-идентификатор: {definition_oval_id}; Семейство платформ: {definition_affected_families}; Платформы: {definition_affected_platforms}; Продукты: {definition_affected_products}]; Количество	Oval Definitions Control	/oval_scanner/definitions/bulk/delete POST	

Табл. 85. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИС- ТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВА- ТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫ- ПОЛНЕНИЕ ФУНКЦИИ
			удаленных определений: {deleted_count}}			
1120003	Пользователь предпри- нимает неудачную попытку удалить несколько OVAL- определений	Не удалось выполнить групповое удаление OVAL опре- делений	Ошибка {error_message}; Пользователь: {user_ login}; Обоснование: {justification}; Фильтр: [Название: {definition_ title}; Описание: {definition_description}; Тип проверки: {definition_type}; OVAL- идентификатор: {definition_oval_id}; Се- мейство платформ: {definition_affected_ families}; Платформы: {definition_affected_ platforms}; Продукты:	Oval Definitions Control	/oval_scanner/definitions/bulk/delete POST	Админи- стратор Инженер Про- смотрщик

Табл. 85. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИС- ТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВА- ТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫ- ПОЛНЕНИЕ ФУНКЦИИ
			{definition_affected_products}}			
1130001	Пользователь удаляет несколько групп OVAL-определений	Удалены группы OVAL-определений	Пользователь: {user_login}; Обоснование: {justification}; Фильтр: [Название или описание содержит: {filter_search}]; Количество удаленных групп: {deleted_count}	Oval Groups Control	/oval_scanner/oval/groups/bulk/delete POST	Администратор
1130002	Пользователь удаляет группу OVAL-определений	Удалена группа OVAL-определений	Пользователь: {user_login}; Обоснование: {justification}; Группа OVAL определений: [Название: {oval_group_title}; Описание: {oval_group_description};]	Oval Groups Control	/oval_scanner/oval/groups/[group_id]/delete POST	Администратор

Табл. 85. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИС- ТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВА- ТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫ- ПОЛНЕНИЕ ФУНКЦИИ
1150001	При попытке сохранения сканера обнаружена ошибка в синтаксисе скрипта	Ошибка верификации сканера	Ошибка: {error}	Script Verification	/host_data_collector/scanners POST	Администратор
1150002	Пользователь, которому не назначена соответствующая роль, предпринимает неудачную попытку импорта сканеров сбора данных	Попытка импорта сканеров пользователем без соответствующих ролей	Ошибка: {error}; Пользователь: {user}	Script Verification	/host_data_collector/scanner_groups POST	Администратор
1150003	Пользователь, которому не назначена соответствующая роль, предпринимает неудачную попытку создания сканера сбора данных	Попытка создания сканера пользователем без соответ-	Ошибка: {error}; Пользователь: {user}	Script Verification	/host_data_collector/scanners POST	Администратор

Табл. 85. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИС- ТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВА- ТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫ- ПОЛНЕНИЕ ФУНКЦИИ
		ствующих ролей				
1150004	Пользователь, которому не назначена соответствующая роль, предпринимает неудачную попытку изменения сканера сбора данных	Попытка внесения изменений в сканер пользователем без соответствующих ролей	Ошибка: {error}; Пользователь: {user}	Script Verification		
1150005	Пользователь, которому не назначена соответствующая роль, предпринимает неудачную попытку создания скрипта OVAL	Попытка создания скрипта OVAL пользователем без соответствующих ролей	Ошибка: {error}; Пользователь: {user}	Script Verification	/oval_scanner/oval/scripts POST	Администратор

Табл. 85. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИС- ТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВА- ТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫ- ПОЛНЕНИЕ ФУНКЦИИ
1150006	Пользователь, которому не назначена соответствующая роль, предпринимает неудачную попытку изменения скрипта OVAL	Попытка внесения изменений в скрипт OVAL пользователем без соответствующих ролей	Ошибка: {error}; Пользователь: {user}	Script Verification	/oval_scanner/oval/scripts/[script_id] PATCH	Администратор
1150007	Пользователь, которому не назначена соответствующая роль, предпринимает неудачную попытку импорта скриптов OVAL	Попытка импорта скриптов OVAL пользователем без соответствующих ролей	Ошибка: {error}; Пользователь: {user}	Script Verification	/host_data_collector/oval/scripts/import POST	

Табл. 85. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИС- ТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВА- ТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫ- ПОЛНЕНИЕ ФУНКЦИИ
1160001	Пользователь удалил одно правило обнаружения вторжений	Удалено правило обнаружения вторжений	Пользователь: {user_login}; Обоснование: {justification}; ID правила: {rule_id}	Suricata Control		
1160002	Пользователь удалил несколько правил обнаружения вторжений	Удалены правила обнаружения вторжений	Пользователь: {user_login}; Обоснование: {justification}; ID правил: {rule_ids}; Всего удалено правил: {len_rule_ids}	Suricata Control		
1160006	Пользователь деактивировал несколько правил обнаружения вторжений	Деактивированы правила обнаружения вторжений	Пользователь: {user}; Правила (ID правила - Сенсор): {rule_sid_ids}; Обоснование: {justification}; Всего деактивировано правил: {len_rule_ids}	Suricata Control		

Табл. 85. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИС- ТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВА- ТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫ- ПОЛНЕНИЕ ФУНКЦИИ
1160007	Пользователь активировал одно правило обнаружения вторжений	Активировано правило обнаружения вторжений	Пользователь: {user}; ID правила: {rule_id}; Сенсор: {node_hostname}	Suricata Control		
1160008	Пользователь активировал несколько правил обнаружения вторжений	Активированы правила обнаружения вторжений	Пользователь: {user}; Правил (ID правила - Сенсор): {rule_sid_ids}; Обоснование: {justification}; Всего активировано правил: {len_rule_ids}	Suricata Control		
1170001	Пользователь авторизовался	Успешный вход в Комплекс	Пользователь: {user}; IP адрес: {user_ip}	User Action Control	/users/auth_token GET	Все роли
1170002	Авторизоваться не удалось	Неудачная попытка	Пользователь: {user_name}; IP адрес: {client_ip}	User Action Control	/users/auth_token	Генерируется при

Табл. 85. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИС- ТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВА- ТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫ- ПОЛНЕНИЕ ФУНКЦИИ
		входа в Комплекс			GET	выполнении действия неавторизо- ванным пользо- вателем
1170003	Пользователь выполняет какие-либо действия без со- ответствующих ролей	Ошибка аутенти- фикации	Ошибка: {error}; IP адрес: {user_ip}	User Action Control	/users/auth_token GET	Все роли
1170006	Пользователь нажал кнопку «Выход»	Успешный выход из Комплекса	Пользователь: {user} IP адрес: {user_ip}	User Action Control	/users/auth_token GET	Все роли
1170007	Пользователь изменил пароль и другие данные учетной записи (своей или чужой)	Изменены данные и пароль учетной записи поль- зователя	Ответственный: {login_ initiator}; Пользователь, чьи данные были из- менены: {login_edited}; Старые значения: [Со- стояние: {old_state}, Роль:	User Action Control	/users/[uuid:user_id] PATCH	Админи- стратор

Табл. 85. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИС- ТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВА- ТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫ- ПОЛНЕНИЕ ФУНКЦИИ
			{old_role}, Логин: {old_login}, Имя: {old_name}, Отчество: {old_patronymic_name}, Фамилия: {old_surname}], Новые значения: [Состояние: {new_state}, Роль: {new_role}, Логин: {new_login}, Имя: {new_name}, Отчество: {new_patronymic_name}, Фамилия: {new_surname}]			
1170011	Попытка сохранения учетной записи с логином, уже существующим в Комплексе	Не удалось изменить данные учетной записи пользователя: пользователь с	Пользователь: {login}	User Action Control	/users/[uuid:user_id] PATCH	Администратор

Табл. 85. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИС- ТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВА- ТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫ- ПОЛНЕНИЕ ФУНКЦИИ
		таким логином уже существует				
1170012	Попытка изменения статуса активности собственной учетной записи	Не удалось изменить данные учетной записи пользователя: деактивация текущего пользователя невозможна	Пользователь: {login}	User Action Control	/users/[uuid:user_id] PATCH	Администратор
1170013	Попытка изменения учетной записи без присвоения ей ролей	Не удалось изменить данные учетной записи поль-	Пользователь: {login}	User Action Control	/users/[uuid:user_id] PATCH	Администратор

Табл. 85. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИС- ТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВА- ТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫ- ПОЛНЕНИЕ ФУНКЦИИ
		зователя: от- сутствует роль				
1170014	Попытка изменения учетной записи с паролем, который не соответствует парольной политике	Не удалось изменить данные учетной записи пользователя: пароль не соответствует парольной политике	Пользователь: {login}	User Action Control	/users/[uuid:user_id] PATCH	Администратор
1170015	Попытка изменения учетной записи без задания пароля	Не удалось изменить данные учетной записи пользователя	Пользователь: {login}	User Action Control	/users/[uuid:user_id] PATCH	Администратор

Табл. 85. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИС- ТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВА- ТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫ- ПОЛНЕНИЕ ФУНКЦИИ
		зователя: от- сутствует пароль				
1170016	Пользователь меняет пароль своей учетной записи	Изменен пароль учетной записи	Учетная запись: {target_ user_login}; Пользователь: {source_user_login}	User Action Control	/users/current_user/password PATCH	Все роли
1170017	Попытка изменения пароля	Не удалось изменить пароль учетной записи	Учетная запись: {target_ user_login}; Пользователь: {source_user_login}	User Action Control	/users/current_user/password PATCH	Все роли
1170018	Пользователь редактирует данные учетной записи, оставляя пароль прежним	Изменены данные учетной записи поль- зователя.	Ответственный: {login_ initiator}; Пользователь, чьи данные были из- менены: {login_edited}; Старые значения: [Со- стояние: {old_state}, Роль:	User Action Control	/users/[uuid:user_id] PATCH	Админи- стратор

Табл. 85. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИСТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВАТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫПОЛНЕНИЕ ФУНКЦИИ
		Пароль не изменен	{old_role}, Логин: {old_login}, Имя: {old_name}, Отчество: {old_patronymic_name}, Фамилия: {old_surname}], Новые значения: [Состояние: {new_state}, Роль: {new_role}, Логин: {new_login}, Имя: {new_name}, Отчество: {new_patronymic_name}, Фамилия: {new_surname}]			
1170019	Пользователь удаляет правило обнаружения вторжений	Удалено правило обнаружения вторжений	Пользователь: {user_login}; Обоснование: {justification}; ID правила: {rule_id}	User Action Control	/suricata_wrapper/rules/[rule_id]/delete DELETE	Администратор
1170020	Пользователь удаляет несколько правил обнаружения вторжений	Удалены правила об-	Пользователь: {user_login}; Обоснование: {justification}; Примеры	User Action Control	/suricata_wrapper/rules/bulk/delete DELETE	

Табл. 85. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИС- ТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВА- ТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫ- ПОЛНЕНИЕ ФУНКЦИИ
		наружения вторжений	ID правил: {rule_ids}; Всего удалено правил: {len_ rule_ids}			
1170021	Неудачная попытка удаления правила обна- ружения вторжений	Не удалось удалить правило об- наружения вторжений	Пользователь: {user_ login}; ID правила: {rule_ id}; Ошибка: {error_ message}	User Action Control	/suricata_wrapper/rules/[rule_id]/ delete DELETE	
1170022	Неудачная попытка удаления нескольких правил обнаружения вторжений	Не удалось удалить правила об- наружения вторжений	Пользователь: {user_ login}; Ошибка: {error_ message}	User Action Control	/suricata_wrapper/rules/bulk/delete DELETE	
1170026	Пользователь отредак- тировал парольную по- литику	Изменена парольная политика	Старые значения: [{old_ policy_fields}]; Новые значения [{new_policy_ fields}]	User Action Control	/	Админи- стратор

Табл. 85. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИС- ТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВА- ТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫ- ПОЛНЕНИЕ ФУНКЦИИ
1170027	Пользователь создал учетную запись пользователя Комплекса	Пользователь создан	{self.additional_info}	User Action Control	/users POST	
1170028	Пользователь удалил учетную запись пользователя Комплекса	Пользователь удален	{self.additional_info}	User Action Control	/users/[user_id] DELETE	
1170029	Пользователь выполнил вход в веб-интерфейс Комплекса с нового устройства, не выполнив выход с предыдущего, при условии, что переменная LIMIT_USER_SESSIONS имеет значение true	Обнаружено одновременное использование веб-интерфейса Комплекса более, чем на одном устройстве пользователем	Пользователь: {user}; IP-адрес первого устройства: {old_ip}; IP-адрес второго устройства: {new_ip}	User Action Control		

Табл. 85. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИС- ТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВА- ТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫ- ПОЛНЕНИЕ ФУНКЦИИ
		{user_ - login}				
1170030	Произошла ошибка при авторизации пользователя	Ошибка авторизации	Пользователь: {user_ - login}; Действие: {action_name}; Объект: {object_name}	User Action Control		
1180001	Оперативная память на ОС Комплекса заполнена на значение, превышающее заданное в переменной DATAPK_MAX_RAM_PERCENTAGE_CONSUMED	Обнаружено превышение потребления оперативной памяти (RAM)	Комплекс: {hostname_ - label}; Превышен порог в {max_ram_consumed_ - percentage}%	System Control	нет (внутренняя пассивная функция Комплекса)	нет
1180002	Потребление оперативной памяти снижено до значений, не превышающих заданных в пере-	Потребление оперативной памяти	Комплекс: {hostname_ - label}	System Control	нет (внутренняя пассивная функция Комплекса)	нет

Табл. 85. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИС- ТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВА- ТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫ- ПОЛНЕНИЕ ФУНКЦИИ
	менной <code>DATAPK_MAX_RAM_- PERCENTAGE_CONSUMED</code>	(RAM) нор- мализовано				
1180003	Заполненность диска на ОС Комплекса превысило значение, заданное в пере- менной <code>MAX_DISK_SPACE_- CONSUMED_PERCENTAGE</code>	Обнаружено пере- полнение дискового про- странства (HDD/SSD) на Ком- плексе	Комплекс: <code>{hostname_- label}</code> ; Превышен порог в <code>{max_disk_space_- consumed_percentage}%</code>	System Control	нет (внутренняя пассивная функция Комплекса)	нет
1180004	Дисковое пространство освобождено до значений, не превышающих заданных в переменной <code>MAX_DISK_- SPACE_CONSUMED_- PERCENTAGE</code>	Пере- полнение дискового про- странства (HDD, SSD) на Ком-	Комплекс: <code>{hostname_- label}</code>	System Control	нет (внутренняя пассивная функция Комплекса)	нет

Табл. 85. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИС- ТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВА- ТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫ- ПОЛНЕНИЕ ФУНКЦИИ
		плексе устранено				
1180005	Нагрузка на центральный процессор ОС Комплекса превысила значение, заданное в переменной MAX_CPU_LOAD_CONSUMED_PERCENTAGE	Обнаружено превышение нагрузки на центральный процессор (CPU)	Комплекс: {hostname_label}; Превышен порог в {max_cpu_load_consumed_percentage}%	System Control	нет (внутренняя пассивная функция Комплекса)	нет
1180006	Нагрузка на центральный процессор снижена до значений, не превышающих заданных в переменной MAX_CPU_LOAD_CONSUMED_PERCENTAGE	Нагрузка на центральный процессор (CPU) нормализована	Комплекс: {hostname_label}	System Control	нет (внутренняя пассивная функция Комплекса)	нет
1180007	Средняя нагрузка на ОС Комплекса превысила	Обнаружено превышение средней на-	Комплекс: {hostname_label}; Значение превышает {max_la}	System Control	нет (внутренняя пассивная функция Комплекса)	нет

Табл. 85. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИС- ТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВА- ТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫ- ПОЛНЕНИЕ ФУНКЦИИ
	значение, заданное в переменной DATAPK_MAX_LA	грузки (Load average)				
1180008	Средняя нагрузка снижена до значений, не превышающих заданных в переменной DATAPK_MAX_LA	Средняя нагрузка (Load average) нормализована	Комплекс: {hostname_label}	System Control	нет (внутренняя пассивная функция Комплекса)	нет
1180009	Пользователь меняет NTP-серверы	NTP-серверы изменены	Старое значение: {old_value}; Новое значение: {new_value}	datapk sensor	нет (внутренняя пассивная функция Комплекса)	учетная запись администратора ОС
1180010	Пользователь меняет временную зону Комплекса	Временная зона (TZ) Комплекса была изменена. Старое значение: ; Новое	Старое значение: {old_value}; Новое значение: {new_value}	datapk sensor	нет (внутренняя пассивная функция Комплекса)	учетная запись администратора ОС

Табл. 85. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИС- ТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВА- ТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫ- ПОЛНЕНИЕ ФУНКЦИИ
		значение: {new_value}				
1180011	Брокер сообщений потребляет больше оперативной памяти, чем указано в переменной <code>RMQ_LOW_AVAILABLE_MEMORY_WATERMARK_BYTES</code>	Обнаружено превышение потребления выделенной для брокера сообщений оперативной памяти (RAM)	Комплекс: {hostname_label}; Лимит RAM: {low_available_memory_watermark_mb} Мбайт	System Control	нет (внутренняя пассивная функция Комплекса)	нет
1180012	Потребление оперативной памяти брокером нормализовано до значений, не превышающих указанных в переменной <code>RMQ_LOW_AVAILABLE_MEMORY_WATERMARK_BYTES</code>	Потребление выделенной для брокера сообщений оперативной	Комплекс: {hostname_label}; Лимит RAM: {low_available_memory_watermark_mb} Мбайт	System Control	нет (внутренняя пассивная функция Комплекса)	нет

Табл. 85. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИС- ТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВА- ТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫ- ПОЛНЕНИЕ ФУНКЦИИ
		памяти (RAM) нор- мализовано				
1180013	Брокер сообщений по- требляет больше дискового пространства, чем указано в переменной <code>RMQ_LOW_</code> <code>AVAILABLE_DISK_SPACE_</code> <code>WATERMARK_BYTES</code>	Обнаружено пере- полнение выде- ленного для брокера со- общений дискового про- странства (HDD/SSD) на Ком- плексе	Комплекс: <code>{hostname_-</code> <code>label}</code> ; Лимит HDD/ SSD: <code>{low_available_-</code> <code>disk_space_watermark_mb}</code> Мбайт	System Control	нет (внутренняя пассивная функция Комплекса)	нет
1180014	Дисковое пространство освобождено до значений, не превышающих заданных	Пере- полнение выде-	Комплекс: <code>{hostname_-</code> <code>label}</code> ; Лимит HDD/ SSD: <code>{low_available_-</code>	System Control	нет (внутренняя пассивная функция Комплекса)	нет

Табл. 85. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИС- ТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВА- ТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫ- ПОЛНЕНИЕ ФУНКЦИИ
	в переменной <code>RMQ_LOW_AVAILABLE_DISK_SPACE_WATERMARK_BYTES</code>	ленного для брокера сообщений дискового пространства (HDD, SSD) устранено	<code>disk_space_watermark_mb</code> Мбайт			
1180015	Запрос к сенсору остался без ответа	Не удается установить соединение с сенсором	Сенсор: <code>{node_name}</code> (<code>{node_id}</code>); Источник данных: <code>{exporter_name}</code> ; Был доступен <code>{max_delay:.3f}</code> минут назад;	System Control	нет (внутренняя пассивная функция Комплекса)	нет
1180016	Соединение с сенсором восстановлено	Соединение с сенсором восстановлено	Сенсор: <code>{node_name}</code> (<code>{node_id}</code>);	System Control	нет (внутренняя пассивная функция Комплекса)	нет

Табл. 85. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИС- ТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВА- ТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫ- ПОЛНЕНИЕ ФУНКЦИИ
1180017	Комплексу не удается установить соединение с сервисом получения данных на сенсоре	Не удается установить соединение с сенсором. Получение данных недоступно	Сенсор: {node_name}({node_id}; Был доступен {max_delay.3f} минут назад;	System Control	нет (внутренняя пассивная функция Комплекса)	нет
1180018	Комплекс установил соединение с сервисом получения данных на сенсоре	Соединение и возможность получения данных с сенсора восстановлены	Сенсор: {node_name}({node_id};	System Control	нет (внутренняя пассивная функция Комплекса)	нет
1180019	Комплексу не удается установить соединение с сервисом отправки данных на сенсоре	Недоступен сервис отправки	Сенсор: {node_name}({node_id}; Был доступен {max_delay:.3f} минут назад;	System Control	нет (внутренняя пассивная функция Комплекса)	нет

Табл. 85. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИС- ТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВА- ТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫ- ПОЛНЕНИЕ ФУНКЦИИ
		данных с сенсора				
1180020	Комплекс установил со- единение с сервисом от- правки данных на сенсоре	Доступность сервиса от- правки данных вос- становлена	Сенсор: {node_ name}({node_id};	System Control	нет (внутренняя пассивная функция Комплекса)	нет
1180021	Комплексу не удается установить соединение с сервисом синхронизации настроек на сенсоре	Не удается установить соединение с сенсором. Синхро- низация на- строек недо- ступна.	Сенсор: {node_ name}({node_id}; Был до- ступен {max_delay:.3f} минут назад;	System Control	нет (внутренняя пассивная функция Комплекса)	нет
1180022	Комплексу установил со- единение с сервисом син-	Соединение и воз- можность	Сенсор: {node_ name}({node_id};	System Control	нет (внутренняя пассивная функция Комплекса)	нет

Табл. 85. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИС- ТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВА- ТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫ- ПОЛНЕНИЕ ФУНКЦИИ
	хронизации настроек на сенсоре	синхро- низации на- строек сенсора вос- становлены				
1180023	Сервис синхронизации настроек на сенсоре не отвечает	Недоступен сервис синхронизации настроек	Сенсор: {node_name}({node_id}; Был доступен {max_delay:.3f} минут назад;	System Control	нет (внутренняя пассивная функция Комплекса)	нет
1180024	Работоспособность сервиса синхронизации настроек на сенсоре восстановлена	Доступность сервиса синхронизации настроек восстановлена	Сенсор: {node_name}({node_id};	System Control	нет (внутренняя пассивная функция Комплекса)	нет
1180025	Соединение между Комплексом и сенсором было прервано некоторое время.	Достигнут установленный	Сенсор: {node_name}({node_id};	System Control	нет (внутренняя пассивная функция Комплекса)	нет

Табл. 85. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИС- ТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВА- ТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫ- ПОЛНЕНИЕ ФУНКЦИИ
	Часть накопленных за этот период данных для отправки будет удалена	лимит для отправки данных. Старейшие данные будут удалены.				
1180026	Соединение между Комплексом и сенсором было восстановлено. Данные отправляются в обычном режиме	Отправка данных нормализована	Сенсор: {node_name}({node_id};	System Control	нет (внутренняя пассивная функция Комплекса)	нет
1180027	Пользователь удаляет сенсор	Удален сенсор	Наименование сенсора: {node_name}; Идентификатор сенсора: {node_id}; Пользователь: {user}; Обоснование: {justification}	System Control	нет (внутренняя пассивная функция Комплекса)	нет

Табл. 85. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИС- ТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВА- ТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫ- ПОЛНЕНИЕ ФУНКЦИИ
1180028	Сенсор отклоняет со- общения от источника	Сенсор от- клонил входящее сообщение от ис- точника: не удалось об- работать текст со- общения	Сенсор: {node_ name}({node_id});	System Control		
1180029	На сенсоре восстановлен прием сообщений от ис- точника	Прием сенсором входящих сообщений от ис- точника вос- становлен	Сенсор: {node_ name}({node_id});	System Control		

Табл. 85. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИС- ТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВА- ТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫ- ПОЛНЕНИЕ ФУНКЦИИ
1180030	Пользователь изменил NTP-серверы на сенсоре	NTP-серверы изменены на сенсоре	Сенсор: {node_id}; Старое значение: {old_value}; Новое значение: {new_value}			
1180031	Пользователь изменил временную зону сенсора	Временная зона (TZ) сенсора была изменена	Сенсор: {node_id}; Старое значение: {old_value}; Новое значение: {new_value}			
1220001	Пользователь запускает сканирование сети	Запущено сканирование сети	Диапазон сканирования: {first_ip} - {last_ip}; Пользователь: {user}	home_net	/scan POST	Администратор
1220002	Сеть была успешно просканирована	Сканирование сети	Диапазон сканирования: {first_ip} - {last_ip}	home_net	нет (внутренняя пассивная функция Комплекса)	нет

Табл. 85. Основные события Комплекса

ID	ДЕЙСТВИЕ	ОПИСАНИЕ	ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ	ИС- ТОЧНИК	МЕТОД ПОЛУЧЕНИЯ СОБЫТИЙ	ПОЛЬЗОВА- ТЕЛЬСКАЯ РОЛЬ, КОТОРОЙ ДОСТУПНО ВЫ- ПОЛНЕНИЕ ФУНКЦИИ
		успешно за- вершено				
1220003	Не удалось завершить ска- нирование сети	Обнаружена ошибка при попытке скани- рования сети	Ошибка: {error}	home_net	нет (внутренняя пассивная функция Комплекса)	нет

3.18. Структура директорий Комплекса

Список общих директорий и файлов настроек, а также их описание представлены в таблице ниже (Таблица 86. Общие директории и файлы настроек).

Табл. 86. Общие директории и файлы настроек

ДИРЕКТОРИЯ (ФАЙЛ)	НАЗНАЧЕНИЕ
<code>/usr/share/udv</code>	Основная директория Комплекса
<code>/usr/share/udv/scripts-certs</code>	Директория для хранения сертификата для верификации сканеров сбора данных
<code>/usr/share/udv/scripts-certs/datapk_script.crt</code>	Сертификат для верификации сканеров сбора данных
<code>/usr/share/udv/certs/ca.crt</code>	Корневой сертификат

Список директорий и основных файлов Комплекса уровня Management, а также их описание представлены в таблице ниже (Таблица 87. Директории и основные файлы настроек Комплекса уровня Management).

Табл. 87. Директории и основные файлы настроек Комплекса уровня Management

ДИРЕКТОРИЯ (ФАЙЛ)	НАЗНАЧЕНИЕ
<code>/usr/share/udv/datapk/manager.env</code>	Основные настройки Комплекса
<code>/var/cache/udv/nginx/certs</code>	Серверные сертификаты
<code>/usr/share/udv/nginx</code>	Шаблоны nginx
<code>/usr/share/udv/frontend</code>	Настройки меню (интерфейса)
<code>/etc/logstash</code>	Правила нормализации
<code>/var/backups</code>	Директория для хранения резервных копий. Содержит tar-архивы с резервными копиями (dtpk-backup-version-timestamp.tar)
<code>/var/backups/elasticsearch</code>	Директория для хранения резервных копий событий
<code>/var/backups/elasticsearch/indices</code>	Архивированные индексы событий

Табл. 87. Директории и основные файлы настроек Комплекса уровня Management

ДИРЕКТОРИЯ (ФАЙЛ)	НАЗНАЧЕНИЕ
<code>/var/backups/ elasticsearch/uploads</code>	Индексы событий для импорта
<code>/usr/share/udv/ vulnerability-backend</code>	Директория для хранения импортированного справочника ПО и уязвимостей (CPE и CVE), импортированной базы сопоставления собранного сканерами ПО со справочником CPE и отчета с последними результатами поиска уязвимостей
<code>/var/opt/udv, cache/udv</code> <code>/var/</code>	Служебные директории Комплекса

Список директорий и основных файлов Комплекса уровня Sensor, а также их описание представлены в таблице ниже (Таблица 88. Директории и основные файлы настроек Комплекса уровня Sensor).

Табл. 88. Директории и основные файлы настроек Комплекса уровня Sensor

ДИРЕКТОРИЯ (ФАЙЛ)	НАЗНАЧЕНИЕ
<code>/usr/share/udv/ datapk/sensor.env</code>	Основные настройки Комплекса
<code>/usr/share/udv/snmp- connector/snmp_mibs</code>	Словари SNMP

4. Первичная настройка Комплекса

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

Рекомендуется производить первичную настройку в предложенном порядке.

4.1. Подключение Комплекса

В этом разделе:

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

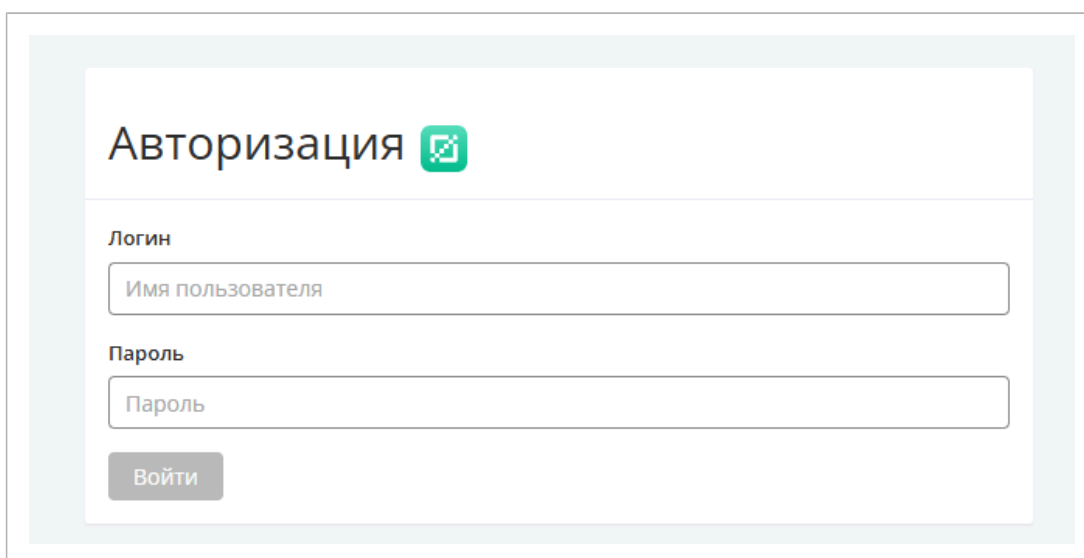
Порядок включения аппаратной платформы установленного Комплекса для выполнения первичной настройки:

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

4.1.1. Подключение к веб-интерфейсу по протоколу HTTPS

Для подключения к веб-интерфейсу Комплекса по протоколу HTTPS:

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



Авторизация 

Логин

Имя пользователя

Пароль

Пароль

Войти

Рис. 54. Окно входа в веб-интерфейс Комплекса

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

а. Нажмите кнопку **Дополнительные**.

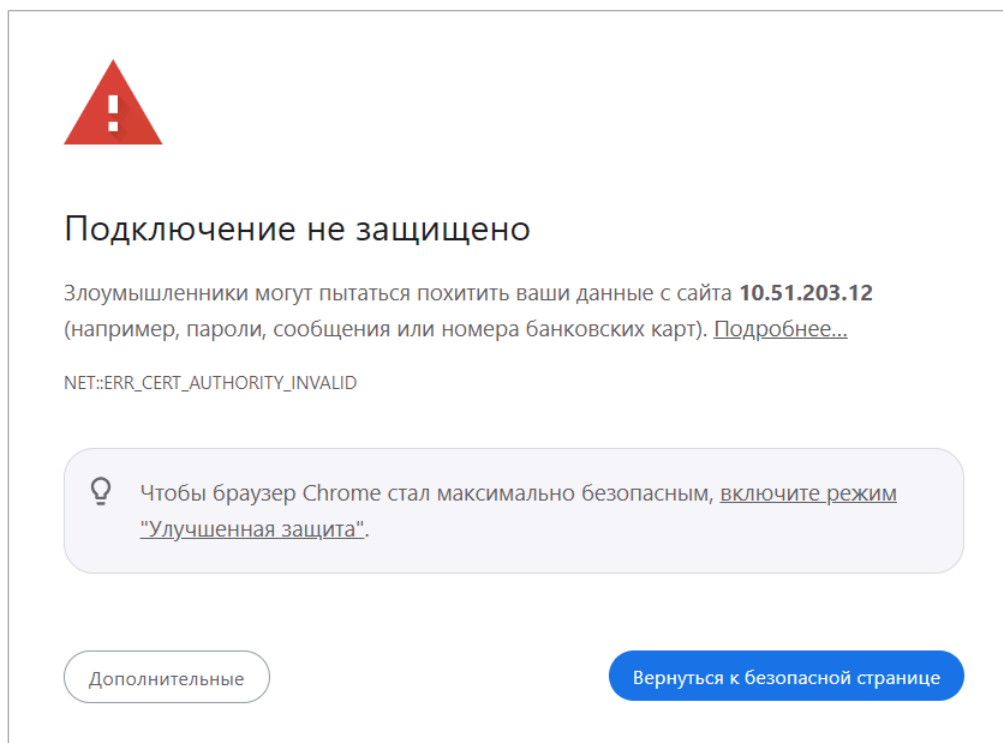


Рис. 55. Окно предупреждения о незащищенном подключении

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

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

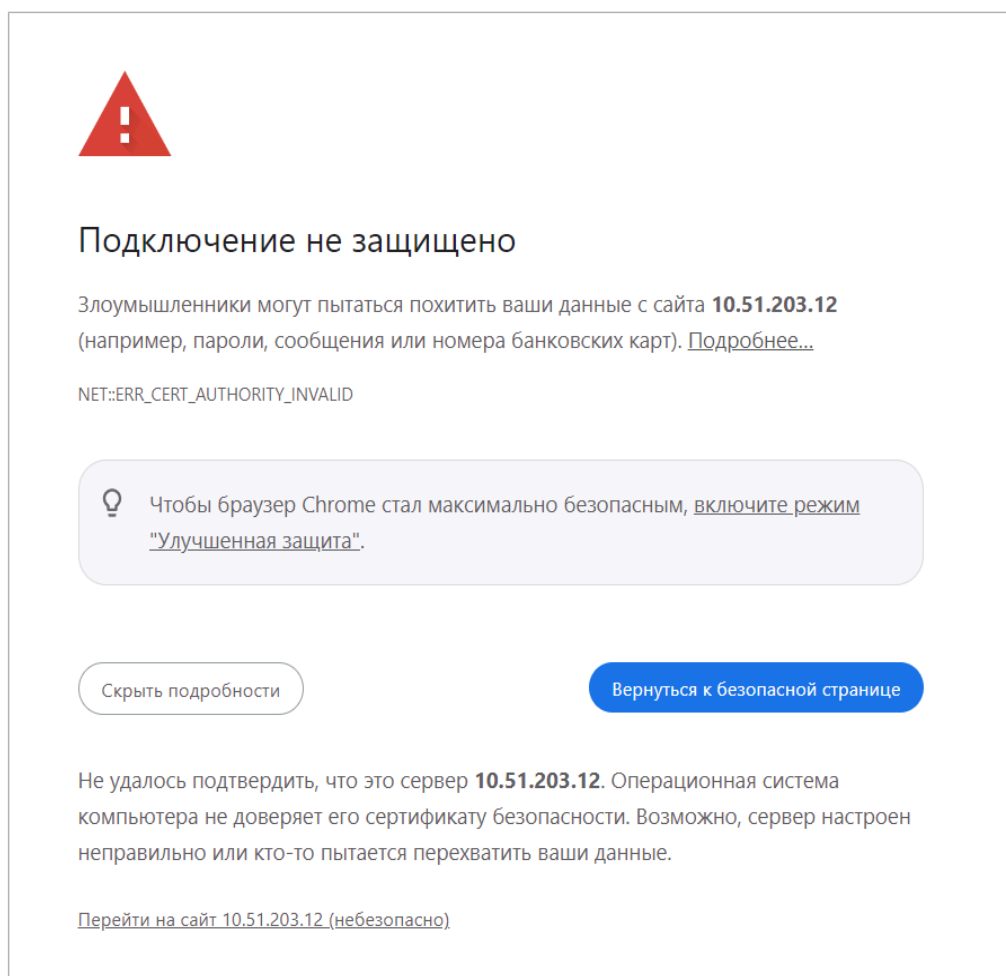


Рис. 56. Подключение к ПК UDV DATAPK по HTTPS

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

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

Внимание:

Максимальное количество неудачных попыток ввода пароля по умолчанию равно 3.

По умолчанию при превышении неудачных попыток ввода пароля учетная запись блокируется на 900 секунд (15 минут).

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

Внимание:

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

4.1.2. Первоначальная настройка

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



Подсказка:

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

Для настройки:

1. Ознакомьтесь с условиями лицензионного соглашения. В случае согласия с условиями лицензионного соглашения установите чекбокс **Принимаю условия лицензионного соглашения** и нажмите кнопку **Далее**.
 - **Результат шага:** откроется окно **Настройка учетной записи**.
2. Настройте предустановленную учетную запись администратора Комплекса. Для этого:
 - а. В окне **Настройка учетной записи** введите следующие параметры:
 - введите новый логин в поле **Логин**;
 - пароль учетной записи и его подтверждение в полях **Новый пароль** и **Подтверждение нового пароля**;



Внимание:

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

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

Рис. 57. Окно «Настройка учетной записи»

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

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

- Импортируйте справочники. Для этого:

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



Подсказка:

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

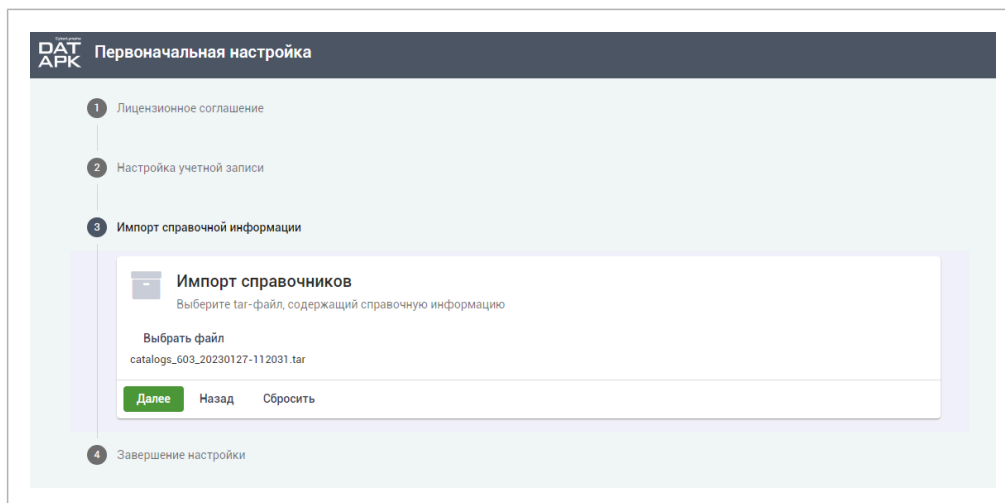


Рис. 58. Окно «Импорт справочников»

в. Нажмите **Далее**.

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

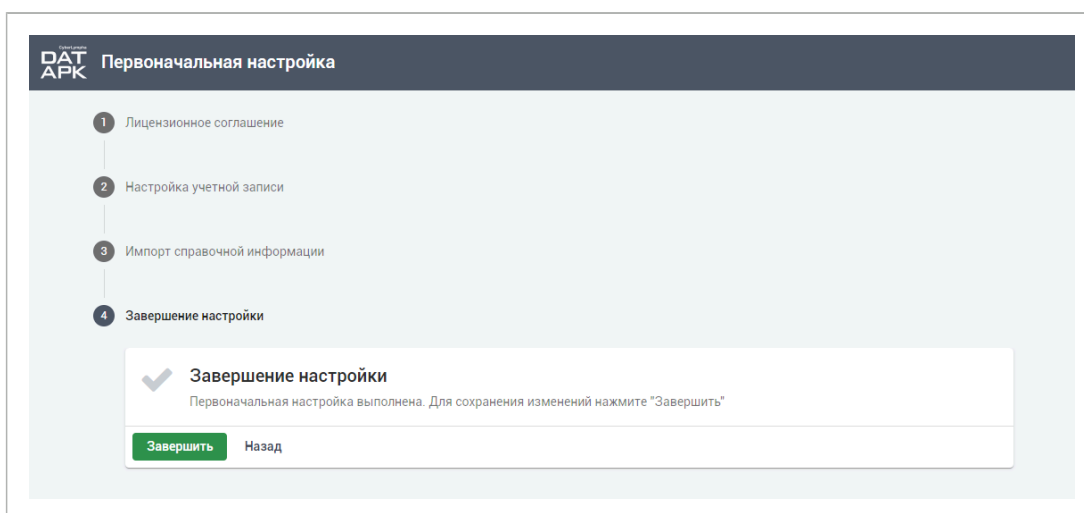


Рис. 59. Окно «Завершение настройки»

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

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

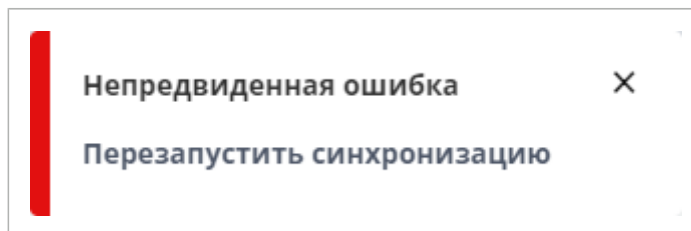


Рис. 60. Ошибка синхронизации сенсоров с Комплексом

4.2. Настройка локальных реквизитов и домашней сети

В этом разделе:

- Изменение сведений о Комплексе и сенсорах
- Настройка домашней сети

4.2.1. Изменение сведений о Комплексе и сенсорах

4.2.1.1. Изменение сведений о текущем Комплексе

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

The screenshot shows the 'О системе' (About System) page in the UDV MultiProtect interface. The page has a dark sidebar on the left with a menu containing: Мониторинг, Инциденты, События, Активы, Сбор данных, Инспекция сети, Сенсоры, and Администрирование. The main content area is titled 'О системе' and has a breadcrumb trail: ← Администрирование | О системе | Импорт и экспорт | Диагностика | Настройки мониторинга. Below the title is a section 'Сведения о Комплексе' with four input fields: 'Наименование' (lrp-vm-staging-244-47), 'Описание' (Демонстрационный стенд), 'Эксплуатирующая организация' (ООО «КИТ.Р»), and 'Место установки' (Сколково). To the right of these fields is a section 'Информация об изготовителе' containing: UDV MultiProtect, Разработчик: ООО «КИТ.Р», www.udv.group, and Версия: 1.0. At the bottom right of the form are two buttons: 'Сохранить' (Save) and 'Отмена' (Cancel). The bottom of the sidebar shows the date and time: 12.03.2025 22:48:23.

Рис. 61. Страница «О системе»

3. Нажмите **Сохранить**.

4.2.1.2. Изменение сведений о сенсорах, подключенных к Комплексу

1. Перейдите на страницу **Сенсоры**.
2. Выберите сенсор из списка.
 - **Результат шага:** Откроется боковая панель настроек выбранного сенсора.
3. В открывшейся панели нажмите кнопку  (**Редактировать**) напротив наименования сенсора.

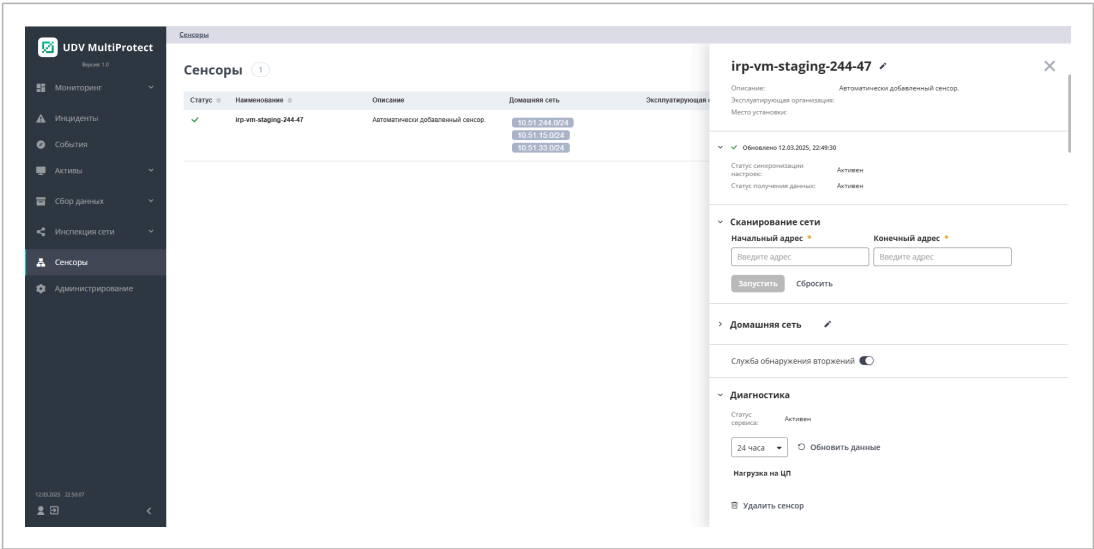


Рис. 62. Страница «Сенсоры»

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

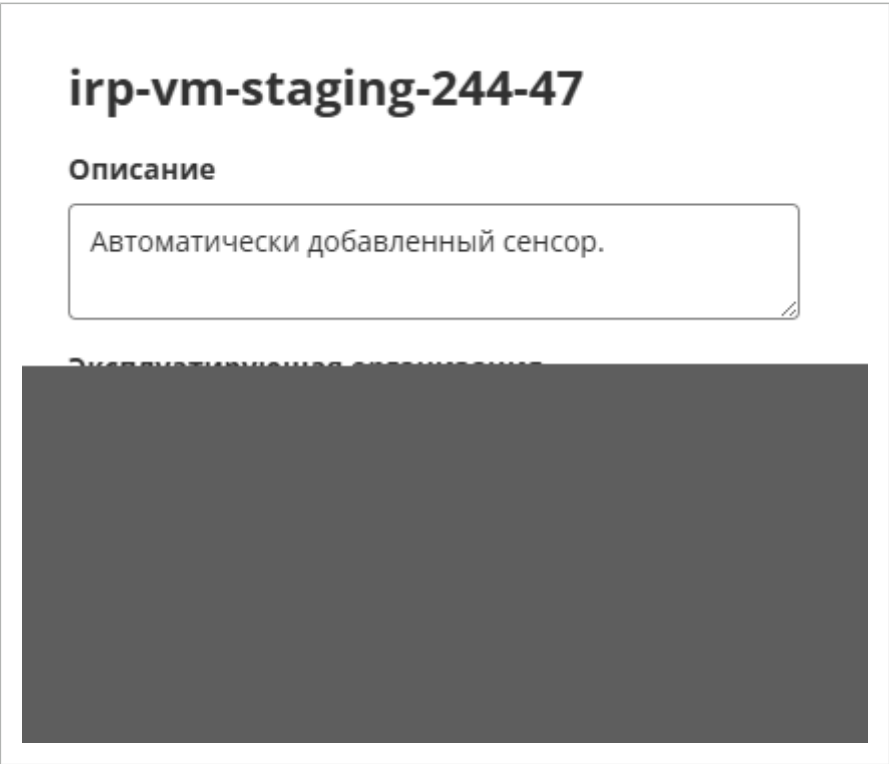


Рис. 63. Блок редактирования информации о сенсоре

5. Нажмите **Сохранить**.

4.2.2. Настройка домашней сети

Настройка домашней сети необходима для отображения на странице **Активы** активов, IP-адреса которых входят в домашнюю сеть. До выполнения настройки домашней сети, в зависимости от настроек Комплекса, в списке активов отображаются все активы, найденные только по MAC-адресу, независимо от наличия у них IP-адреса, либо только активы, у которых не определен IP-адрес (подробнее см. раздел Сканирование сети и определение интерфейсов активного сетевого оборудования).

Для настройки домашней сети Комплекса:

1. Перейдите на страницу **Сенсоры**.
2. Выберите сенсор из списка.
 - **Результат шага:** Откроется боковая панель настроек выбранного сенсора.
3. В открывшейся панели в блоке **Домашняя сеть** нажмите кнопку  (**Редактировать сеть**).
4. Нажмите кнопку **+ Добавить сеть** и введите IP-адрес и маску подсети управляющего контура в качестве домашней подсети. Если требуется удалить добавленную ранее подсеть из списка, нажмите кнопку (**Удалить сеть**).
5. Нажмите **Применить**.
 - **Результат шага:** Появится окно с предупреждением: **При смене домашней сети активы и потоки, не входящие в новую сеть, будут удалены.**
6. Нажмите **Подтвердить** для подтверждения всех изменений и запуска обновления списка активов в соответствии с указанными домашними сетями.
7. Выполните шаги 2–6 для всех подключенных сенсоров, для которых нужно настроить домашнюю сеть.
 - **Результат шага:**
 - В список активов на странице **Активы** будут добавлены обнаруженные активы, IP-адреса которых входят в настроенные домашние сети.
 - Каждому сетевому атрибуту обнаруженного актива будет присвоен сенсор, в чью домашнюю сеть входит IP-адрес атрибута. Присвоенный сенсор будет отображаться в поле **Сенсор** блока **Сетевые атрибуты** в карточке актива.

4.3. Настройка парольной политики

Для настройки единой парольной политики для всех пользователей:

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

Рис. 64. Страница «Парольная политика»

2. Настройте следующие параметры парольной политики:

- общее минимальное количество символов, которое должен содержать пароль;

 **Внимание:**

Доступен ввод значений в диапазоне от 6 до 14. Суммарное количество цифровых символов, заглавных букв и спецсимволов не должно превышать это значение.

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

 **Внимание:**

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

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



Внимание:

Доступен ввод значений в диапазоне от 1 до 24.

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



Внимание:

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

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



Внимание:

Чтобы отключить автоматическую блокировку, введите значение 0.

3. Нажмите **Сохранить изменения**.

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

4.4. Импорт справочников из архива

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



Внимание:

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

Справочники, доступные для импорта из архива на странице **Импорт и экспорт**, представлены в таблице ниже (Таблица 89. Справочники, которые можно импортировать).

Табл. 89. Справочники, которые можно импортировать

НАЗВАНИЕ СПРАВОЧНИКА	РАЗДЕЛ
События	
Правила разбора событий	Импорт правил разбора событий
Правила обогащения событий	Импорт правил обогащения событий
Схема событий	Импорт схемы событий
Элементы иерархии	
Иерархия ИС	Импорт справочников с классификаторами ИС
Иерархия меток активов	Импорт меток
Группы активов	
Обнаружение уязвимостей (CVE)	
Справочники ПО и уязвимостей (CPE и CVE)	Импорт справочников CVE и CPE и файла сопоставления ПО с CPE
Сопоставление собранного сканерами ПО со справочником CPE	
Справочник БДУ ФСТЭК	Импорт справочника БДУ ФСТЭК России
Корреляция событий	
Правила корреляции	Импорт правил корреляции
Схема корреляции	Импорт схемы корреляции

Табл. 89. Справочники, которые можно импортировать

НАЗВАНИЕ СПРАВОЧНИКА	РАЗДЕЛ
Политика корреляции	Импорт политики корреляции
Сбор данных	
Группы сканеров	Импорт сканеров и их групп
Учетные данные активов	Импорт учетных данных активов
Задачи сбора данных	Импорт задач сбора данных
Инциденты	
Статусы инцидентов	Импорт статусов инцидентов
Обнаружение вторжений	
Правила обнаружения вторжений	Импорт правил обнаружения вторжений в формате *.json
Наборы сигнатур правил обнаружения вторжений в формате Suricata	Импорт правил обнаружения вторжений в формате *.rules
OVAL	
Группы OVAL-определений вместе с OVAL-определениями	Импорт групп OVAL-определений
Скрипты OVAL	Импорт скриптов OVAL
Настройки OVAL	Импорт настроек OVAL
Правила потоков	
Правила потоков	Импорт правил управления потоками данных
Источники событий	Импорт источников событий

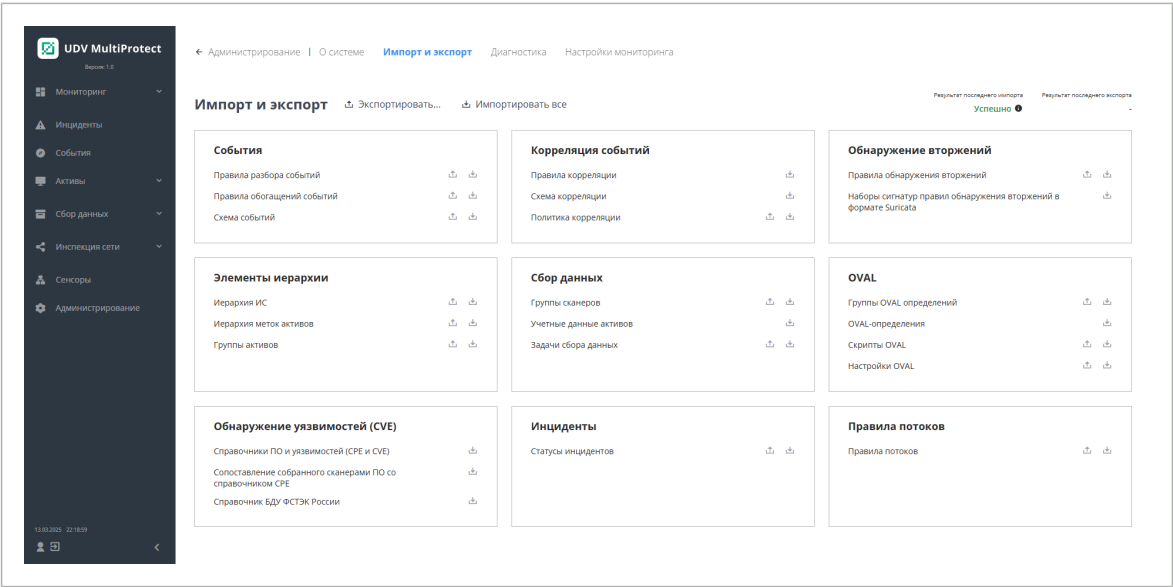


Рис. 65. Страница «Импорт и экспорт»

4.5. Запуск обнаружения вторжений и синхронизация правил с сенсорами

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

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

1. Перейдите на страницу **Сенсоры**.
2. Нажмите на строку с сенсором, для которого нужно проверить статус службы обнаружения вторжений.
 - **Результат шага:** Откроется боковая панель настроек выбранного сенсора.
3. В открывшейся справа карточке включите или выключите службу обнаружения вторжений сенсора с помощью переключателя: если переключатель в состоянии  — служба включена.
4. Перейдите на страницу **Администрирование** → **Правила обнаружения**.
5. Нажмите кнопку **Синхронизация правил**.
 - **Результат шага:** Правила будут обновлены на сенсорах, подключенных к текущему Комплексу, и активные правила начнут автоматически применяться для обнаружения вторжений на сенсорах, на которых включен этот сервис.

4.6. Проверка работоспособности Комплекса

Чтобы убедиться в работоспособности Комплекса после подключения к нему сенсоров:

1. Проверьте работоспособность системы передачи данных от сенсоров к Комплексу. Подробнее см. в разделе [Проверка работоспособности системы передачи данных по иерархии](#).
2. Проверьте обнаружение активов при прослушивании трафика после настройки домашней сети на сенсорах. Подробнее см. в разделе [Проверка обнаружения активов из домашней сети](#).
3. Проверьте работоспособность системы обнаружения потоков данных. Подробнее см. в разделе [Проверка работоспособности системы обнаружения потоков данных](#).

4.6.1. Проверка работоспособности системы передачи данных по иерархии

Для проверки работоспособности системы передачи данных по иерархии:

1. Перейдите на страницу **Сенсоры**.
2. Выберите сенсор.
 - **Результат шага:** Справа откроется карточка с описанием и настройками выбранного сенсора.
3. Просмотрите статусы синхронизации настроек и получения данных с сенсора.

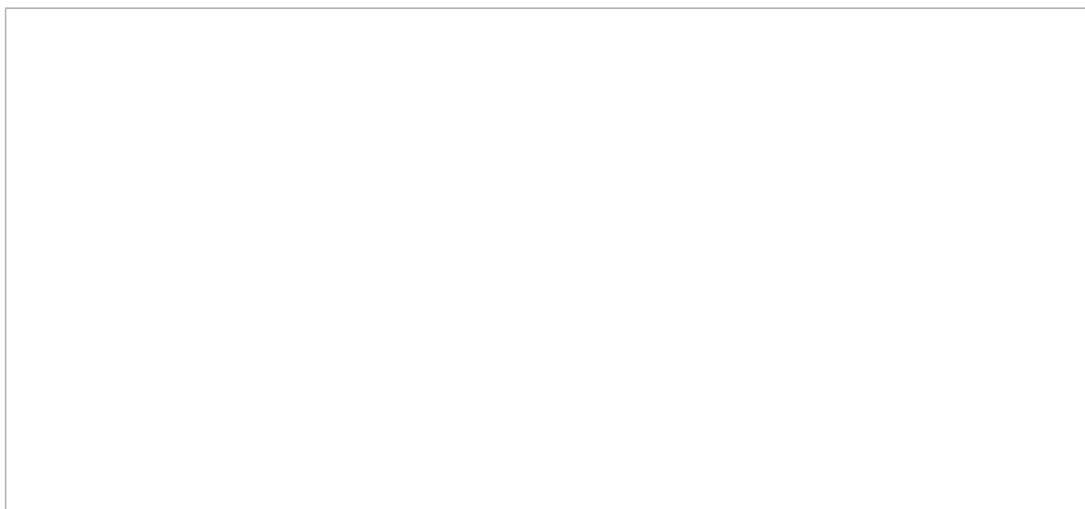


Рис. 66. Статусы исправной синхронизации настроек и получения данных с сенсора

4.6.2. Проверка обнаружения активов из домашней сети

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

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

4.6.3. Проверка работоспособности системы обнаружения потоков данных

Для проверки работоспособности системы обнаружения потоков данных:

1. Перейдите на страницу **Инспекция сети** → **Потоки данных**.

Инспекция сети > Потоки данных									
Действия		Управление		Выберите представление					
Всего записей: 852 Отфильтрованных: 852									
Дата обнаружения	Статус	Последний расп.	IP-адрес	Пор.	IP-адрес	Пор.	Отправитель	Получатель	
> 27.03.2024, 19:23:50	Не одобрен	air					Неизвестный актив	Актив не определен	
> 27.03.2024, 19:23:50	Не одобрен	gapr					Неизвестный актив	Актив не определен	
> 27.03.2024, 18:58:56	Не одобрен	tcp	10.41.56.41	61712	10.51.15.139	8443	Внешняя сеть	Неизвестный актив	
> 27.03.2024, 18:58:54	Не одобрен	ssl	10.41.56.41	61694	10.51.15.139	8443	Внешняя сеть	Неизвестный актив	
> 27.03.2024, 18:58:54	Не одобрен	http	10.41.56.41	61688	10.51.15.139	80	Внешняя сеть	Неизвестный актив	
> 27.03.2024, 18:56:28	Не одобрен	air					Неизвестный актив	Актив не определен	
> 27.03.2024, 18:56:28	Не одобрен	gapr					Неизвестный актив	Актив не определен	
> 27.03.2024, 18:52:37	Не одобрен	air					Неизвестный актив	Актив не определен	
> 27.03.2024, 18:52:36	Не одобрен	gapr					Неизвестный актив	Актив не определен	
> 27.03.2024, 18:38:49	Не одобрен	air					Неизвестный актив	Актив не определен	
> 27.03.2024, 18:38:48	Не одобрен	gapr					Неизвестный актив	Актив не определен	
> 27.03.2024, 18:20:19	Не одобрен	icmp_route_error	10.51.15.139		10.199.1.151		Неизвестный актив	Внешняя сеть	
> 27.03.2024, 18:15:43	Не одобрен	air					Неизвестный актив	Актив не определен	
> 27.03.2024, 18:15:43	Не одобрен	gapr					Неизвестный актив	Актив не определен	

Рис. 67. Страница «Потоки данных»

2. Убедитесь в отображении потоков данных активов, полученных с сенсоров.

5. Работа с событиями

Просмотр и визуализация событий

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

Все события отображаются на странице **События** и в экспертном режиме в порядке их обнаружения от последних к более ранним. Событие можно развернуть и посмотреть подробности в виде таблицы.

Критичность	Дата созда...	Сенсор	Описание	IP-адрес источника	Актив источника	IP-адрес получателя	Актив получателя
> + Низкая	27.03.2024, 18:16:03.501	datapk-vm-develop-15-139	Сбор данных успешно вып...			10.51.244.26	WinCC
> + Низкая	27.03.2024, 18:16:02.256	datapk-vm-develop-15-139	Сбор данных успешно вып...			10.51.201.146	Win2KservSP4_TK1
> + Низкая	27.03.2024, 18:16:01.376	datapk-vm-develop-15-139	Обнаружена ошибка сбора ...			10.51.201.138	WINDOWS-XP_TK1_DEVEL
> + Низкая	27.03.2024, 18:14:03.543	datapk-vm-develop-15-139	Сбор данных успешно вып...			10.51.244.26	WinCC
> + Низкая	27.03.2024, 18:14:01.514	datapk-vm-develop-15-139	Сбор данных успешно вып...			10.51.201.138	WINDOWS-XP_TK1_DEVEL
> + Низкая	27.03.2024, 18:14:01.062	datapk-vm-develop-15-139	Обнаружена ошибка сбора ...			10.51.201.146	Win2KservSP4_TK1
> + Низкая	27.03.2024, 18:12:03.598	datapk-vm-develop-15-139	Сбор данных успешно вып...			10.51.244.26	WinCC
> + Низкая	27.03.2024, 18:12:02.491	datapk-vm-develop-15-139	Сбор данных успешно вып...			10.51.201.146	Win2KservSP4_TK1
> + Низкая	27.03.2024, 18:12:01.486	datapk-vm-develop-15-139	Сбор данных успешно вып...			10.51.201.138	WINDOWS-XP_TK1_DEVEL

Рис. 68. Список событий на странице «События»

Пользователь может перейти на страницу сенсора из события — для этого нужно нажать на название сенсора. В новой вкладке браузера откроется страница **Сенсоры**.

Также можно перейти на страницу потока данных из события. При нажатии кнопки **Подробнее о потоках**, расположенной в строке информации о событии, в новой вкладке браузера откроется страница **Потоки данных** со следующими предварительно установленными фильтрами:

- MAC-адрес отправителя;
- MAC-адрес получателя;
- IP-адрес отправителя;
- IP-адрес получателя;
- Порт отправителя;
- Порт получателя;
- Последние протоколы.



Внимание:

Кнопка **Подробнее о потоках** доступна в строке информации о событии только при условии одобрения потока с последним распознанным протоколом.

Поиск и просмотр событий

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

Чтобы выполнить поиск, воспользуйтесь одним из способов или их комбинацией:

1. Используйте строку поиска.
2. Используйте фильтры, расположенные под строкой поиска.

В каждом событии расположены поля, для которых генерируются уникальные данные. Подробнее о полях событий см. в разделе Описание полей событий.

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

Генерация событий

Решение позволяет выявлять критичные события ИБ, называемые инцидентами. Подробнее см. в разделе [Работа с инцидентами](#).

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

Все типы событий, необходимых для обеспечения информационной безопасности ИС, могут быть зарегистрированы решением, если корректно настроена их отправка с активов.

Сбор событий с активов выполняется при помощи протоколов TCP/UDP и SNMP. Прием реализуется механизмами syslog (стандарты RFC 3164 и RFC 5424), SNMP-trap и Eventlog. Предусмотрена возможность интеграции с внешними системами для отправки событий из решения по протоколу Syslog .

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



Внимание:

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

Хранение событий

События, которые доступны к просмотру через веб-интерфейс, хранятся в оперативном архиве — индексе. По умолчанию при превышении размера или времени хранения в индексе события переходят в глубокий архив. При достижении лимита объема или времени хранения в глубоком архиве события удаляются безвозвратно. Такой процесс называется ротацией событий.

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

5.1. Поиск и просмотр событий в упрощенном режиме

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

5.1.1. Просмотр событий

Чтобы посмотреть информацию о событии:

1. Нажмите кнопку .
- **Результат шага:** Откроется подробная информация о событии.

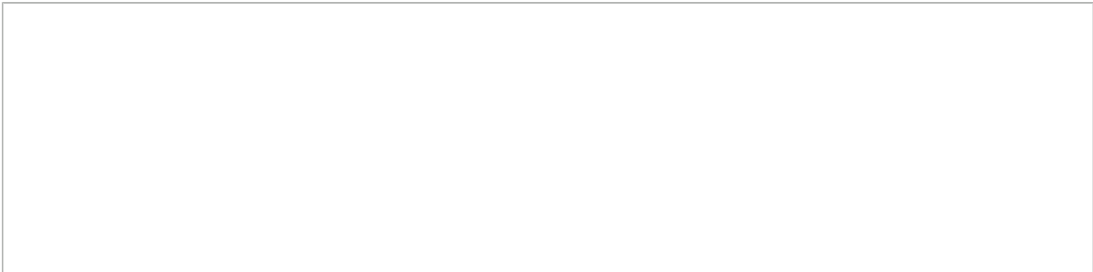


Рис. 69. Подробная информация о событии

2. Для перехода к активам, связанным с событием, нажмите  **Перейти к активам**.

 **Внимание:**

Кнопка  **Перейти к активам** доступна, если к моменту регистрации события Комплекс уже зарегистрировал активы, чьи сетевые атрибуты и идентификаторы присутствуют в событии в полях **Источник** и **Получатель**.

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

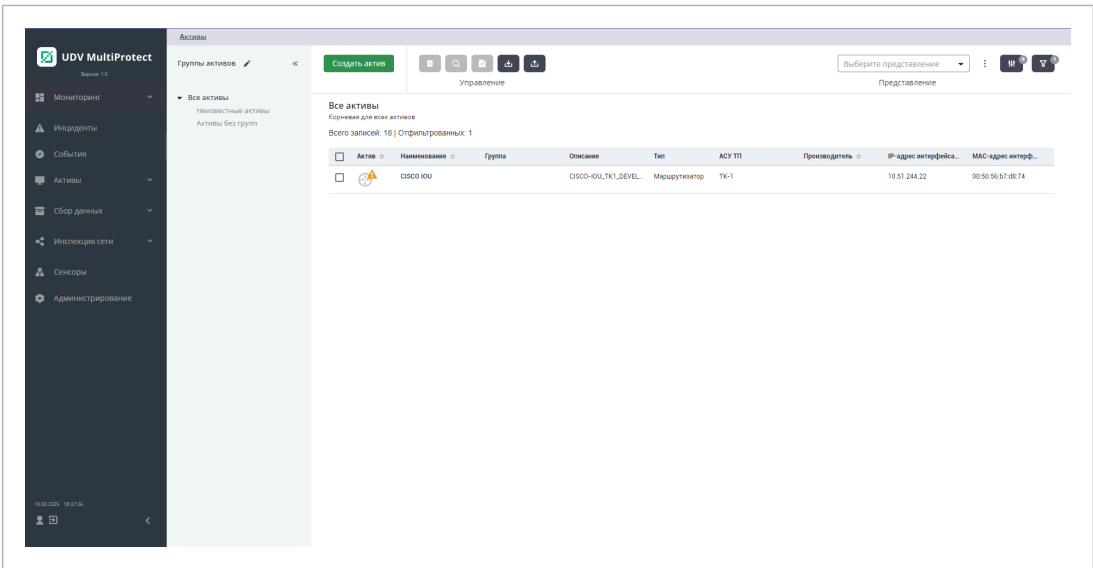


Рис. 70. Активы, связанные с событием

5.1.2. Поиск событий с помощью строки поиска

Чтобы осуществить поиск с помощью строки поиска:

1. Установите курсор в строку поиска.

► **Результат шага:** Отобразится раскрывающийся список с наименованиями доступных полей событий.

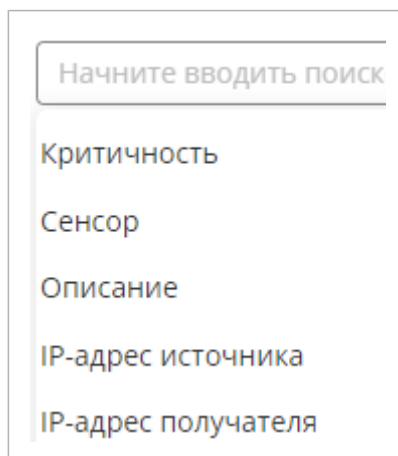


Рис. 71. Список доступных полей событий

2. Выберите поле события из списка или начните вводить поле вручную.

💡
Подсказка:

При вводе поискового запроса в строке поиска будут появляться подсказки с доступными полями, операторами и значениями полей.

3. Выберите оператор поля события из списка.

Доступные операторы для числовых данных:

- ☐ = — равно;
- ☐ != — не равно;
- ☐ > — больше;
- ☐ < — меньше;
- ☐ >= — больше или равно;
- ☐ <= — меньше или равно;

Доступные операторы для текстовых данных:

- ☐ = — равно;
- ☐ != — не равно;
- ☐ ~ — содержит;
- ☐ !~ — не содержит;
- ☐ ^ — начинается с;
- ☐ !^ — не начинается с.

4. Введите значение поля.



Подсказка:

Допускается создавать сложные поисковые запросы, объединяя несколько запросов «поле–оператор–значение» с помощью логических операторов **и/или**. Данные операторы также появляются в строке поиска в виде подсказок.

5. Нажмите **Найти**.

► **Результат шага:** Результаты поиска появятся на странице.

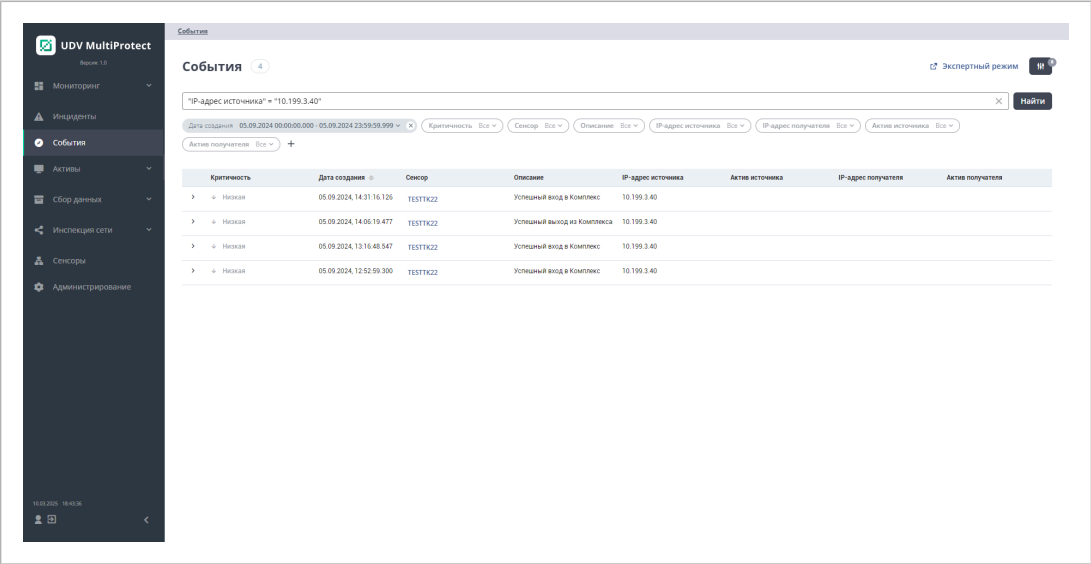


Рис. 72. Отображение результатов поиска

5.1.3. Поиск событий с помощью фильтров

Фильтры — это набор инструментов на странице **События** для фильтрации событий по заданным параметрам. Фильтрация выполняется после ввода значения в фильтр, за исключением следующих фильтров:

- фильтр **Критичность**, в котором по умолчанию заданы значения **Низкая** или **Критическая**;
- фильтр **Тип**, в котором заданы значения типов событий;
- фильтр **Протокол**, в котором заданы значения протоколов, обнаруживаемых решением.

Фильтры расположены под строкой поиска.



Подсказка:

Для более точного поиска событий можно использовать одновременно несколько фильтров и строку поиска.

Для поиска события с помощью фильтра:

1. Выберите необходимый фильтр.

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

Рис. 73. Поле ввода значения в фильтр

2. Введите значение.
3. Нажмите .
- **Результат шага:** Результаты поиска появятся на странице.
4. При необходимости повторите шаги 1–3 с другими фильтрами для более точного поиска событий.
5. Для очистки результатов поиска по одному из фильтров нажмите  справа от выбранного фильтра.
- **Результат шага:** Результаты поиска будут автоматически обновлены на странице.

5.1.4. Поиск событий с помощью фильтра «Дата создания»

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

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

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

Рис. 74. Календарь выбора временного периода регистрации событий

2. Выберите начальную дату.
- **Результат шага:** Автоматически отобразятся события за выбранную дату.

3. При необходимости выберите конечную дату.

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

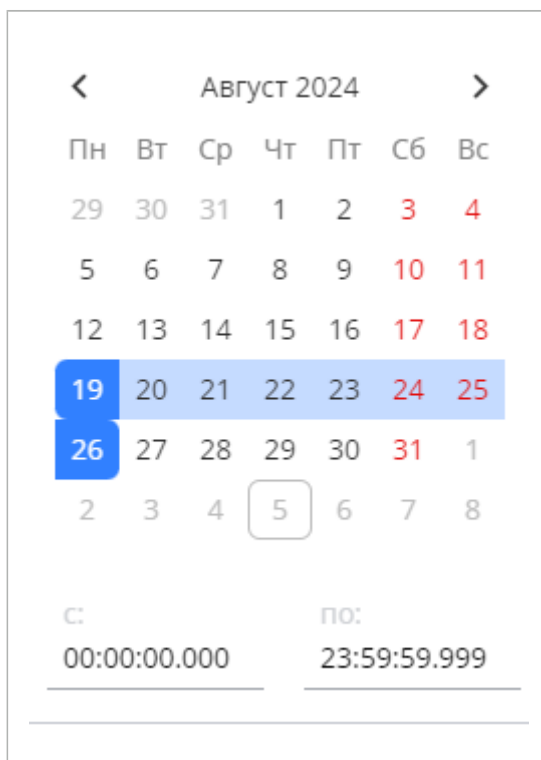


Рис. 75. Выбранные даты в календаре

4. При необходимости введите время в поля **с:** и **по:**. Используйте формат ЧЧ:ММ:СС.ССС.



Внимание:

Если начальная и конечная даты отличаются, в поле **с:** нужно указывать время для начальной даты, а в поле **по:** — для конечной.

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

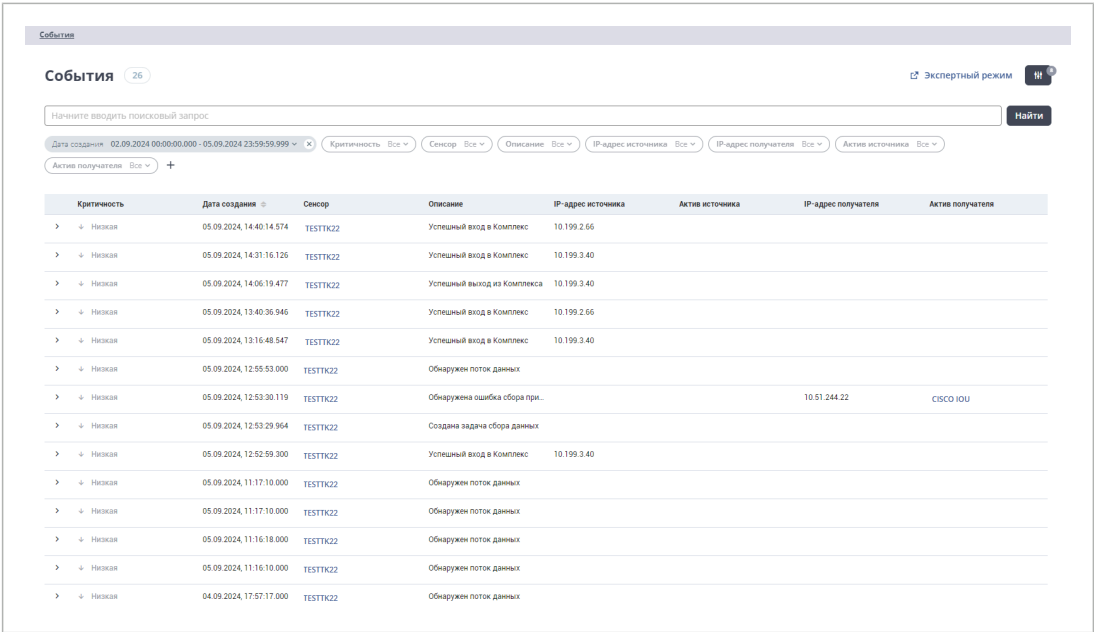


Рис. 76. Отображение событий за установленный временной период

5. Для очистки результатов поиска по выбранному временному периоду нажмите кнопку  справа от фильтра **Дата создания**.

► **Результат шага:** На странице автоматически отобразятся события за текущую дату.

5.1.5. Добавление фильтров

Для добавления фильтров на страницу **События**:

1. Нажмите кнопку , расположенную под строкой поиска.

► **Результат шага:** Отобразится раскрывающийся список с доступными фильтрами. Фильтры, уже выбранные для отображения на странице, окрашиваются в серый цвет и отмечаются значком  слева от названия.

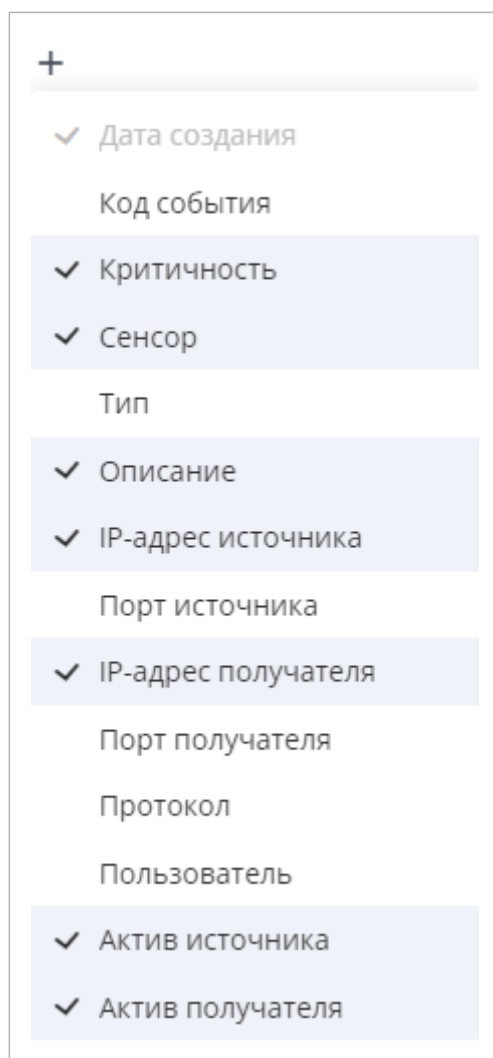


Рис. 77. Список доступных фильтров

- В раскрывающемся списке выберите необходимые фильтры.

► **Результат шага:** Фильтры отобразятся на панели.

5.1.6. Удаление фильтров

Для удаления фильтров со страницы **События**:

- Нажмите кнопку , расположенную под строкой поиска.
- В выпадающем списке отмените выбор необходимых фильтров.

► **Результат шага:** Фильтры перестанут отображаться на панели.

5.2. Просмотр событий и создание запросов в экспертном режиме

Перед созданием запросов убедитесь, что создан шаблон индекса согласно инструкции [Создание шаблона индекса](#).

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

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

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

Для создания нового запроса:

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

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

Рис. 78. Результат выбора столбцов «description» и «listener»

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

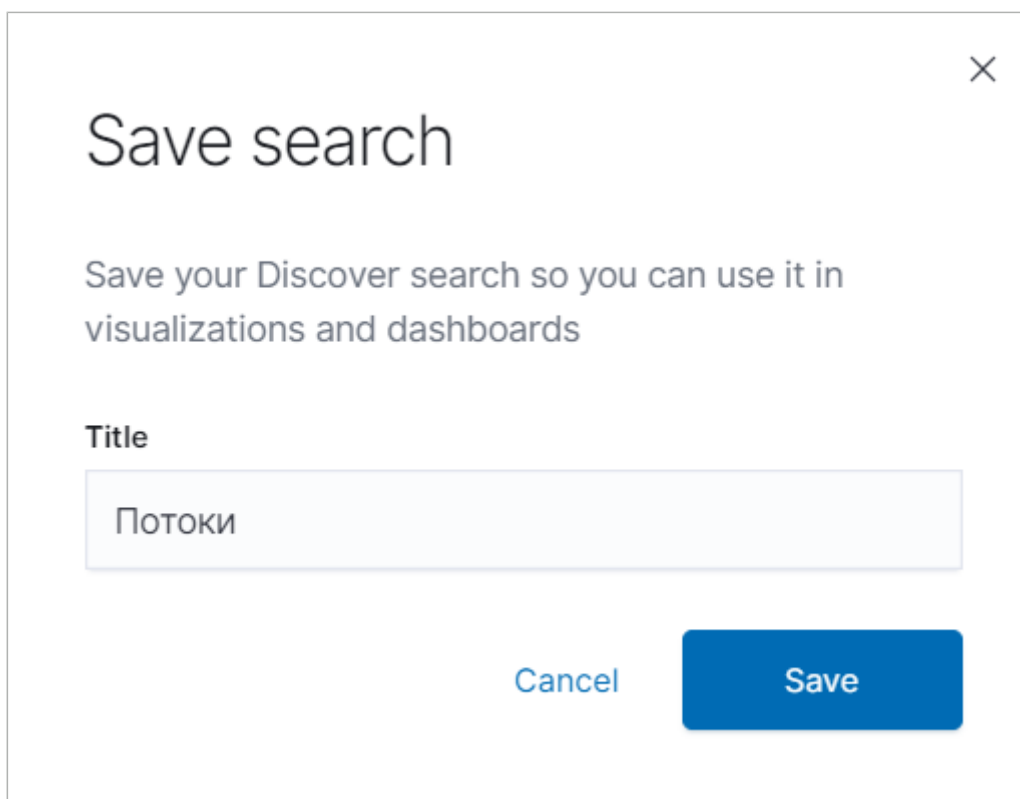


Рис. 79. Окно сохранения поиска

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

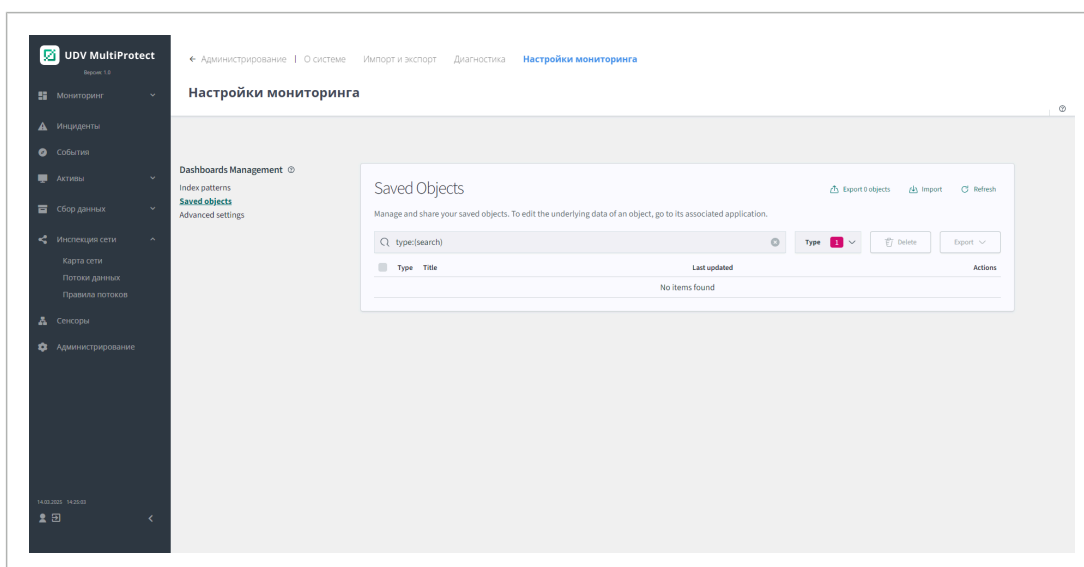


Рис. 80. Выбор типа «search» в разделе «Saved objects» страницы «Настройки мониторинга»

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

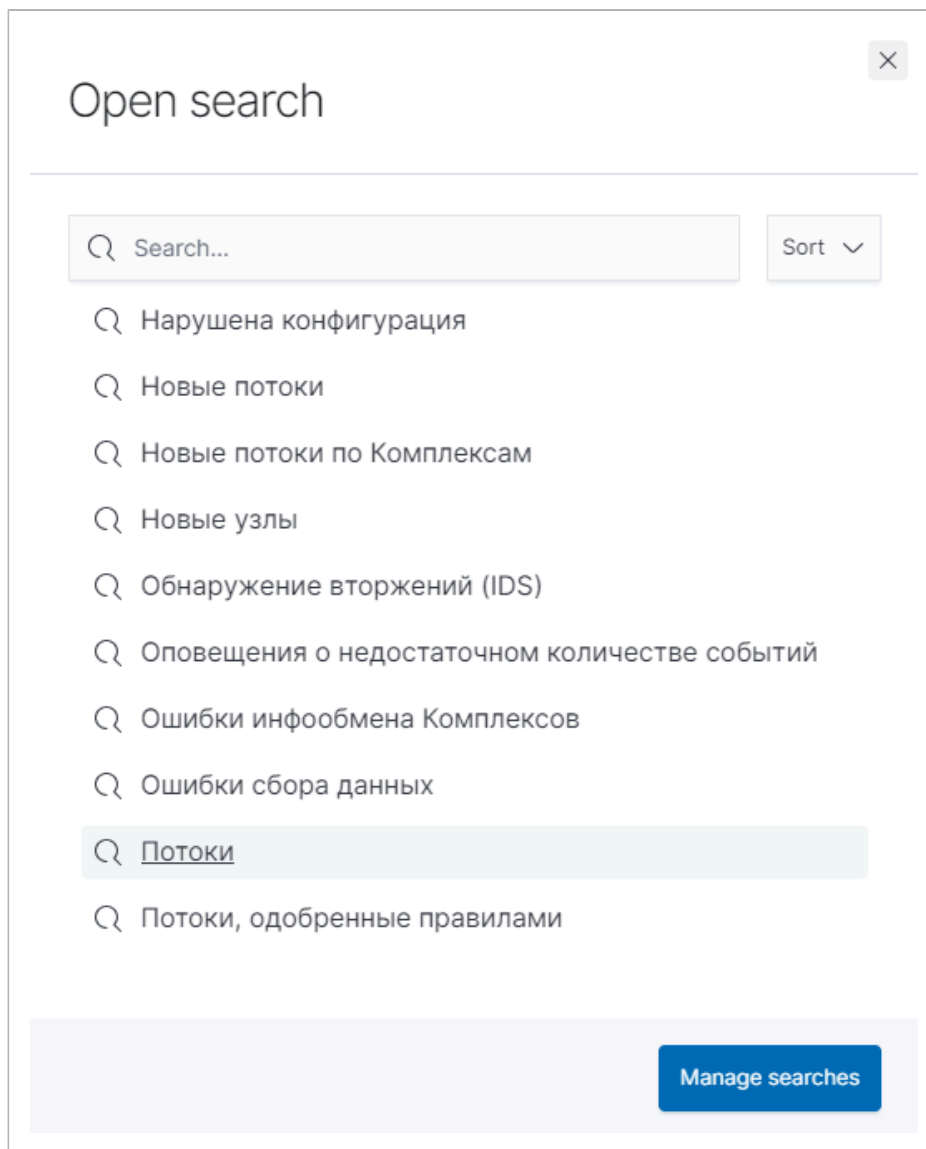


Рис. 81. Окно выбора поискового запроса

5.3. Просмотр панели мониторинга «Статус защищенности»

Общая информация

На странице можно отслеживать статистику и изменения ключевых оперативных данных в режиме реального времени.

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

Данные на странице обновляются автоматически раз в пять минут. Чтобы обновить их вручную, нажмите **Обновить** в правом верхнем углу.

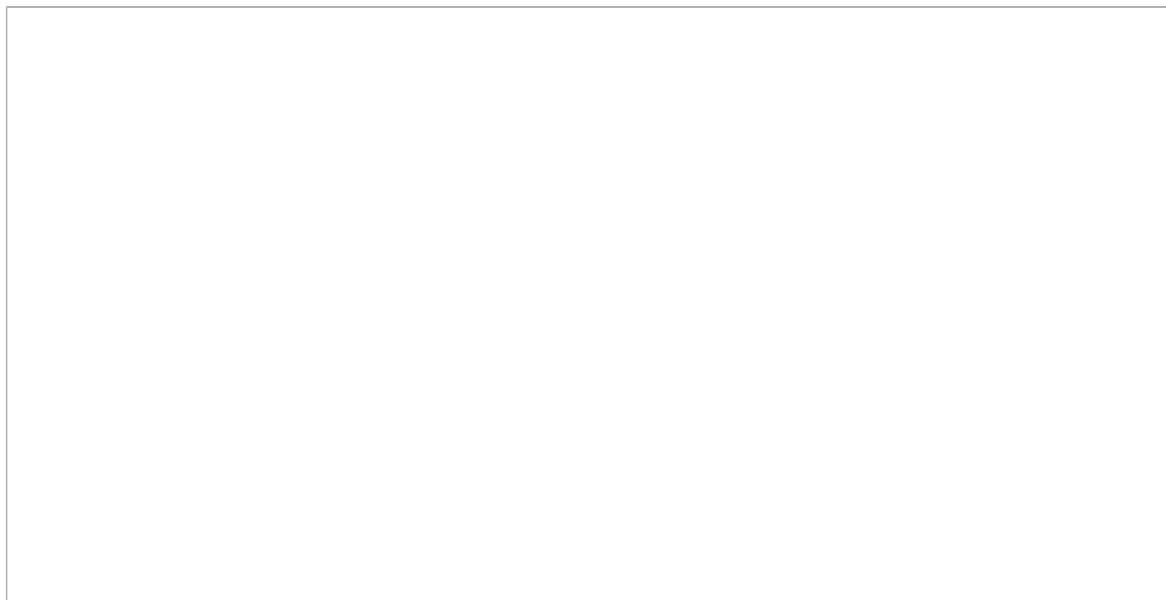


Рис. 82. Страница «Статус защищенности»

Сенсоры

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

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

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



Подсказка:

Подробнее о возможных причинах недоступности сенсоров и способах восстановления доступа см. в разделе [Не устанавливается соединение с сенсором](#).

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

Виджеты

На странице доступны следующие виджеты:

- **Активы.**

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



Внимание:

В виджете **Активы** учитываются только активы с интерфейсами. Список активов на странице **Активы** включает в себя активы с интерфейсами и без интерфейсов.

- **Неизвестные активы** — список обнаруженных неизвестных активов. Для каждого неизвестного актива фиксируется IP-адрес, наименование производителя и дата обнаружения.
- **Обнаруженные инциденты** — количество инцидентов, обнаруженных в выбранный период времени до текущего момента.
- **Обнаруженные потоки** — количество инцидентов, обнаруженных в выбранный период времени до текущего момента. В этом графике не учитываются потоки, которые автоматически одобрены правилами одобрения потоков.
- **Обнаруженные вторжения** — количество вторжений, обнаруженных в выбранный период времени до текущего момента.

Над графиками **Обнаруженные инциденты**, **Обнаруженные потоки** и **Обнаруженные вторжения** отображается примерное количество обнаруженных объектов за период, которое рассчитывается с учетом аппроксимации и исторических данных обнаружения относительно фактических значений на страницах **Инциденты** и **События**. Погрешность отображаемых данных на графиках — $\pm 1\%$.

Существует возможность установить один из следующих интервалов обнаружения:

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

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

Ссылки в виджетах на смежные страницы

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

В виджетах присутствуют следующие ссылки:

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



Внимание:

Пользователям с ролью **Просмотр панели мониторинга** недоступен просмотр данных при переходе по ссылкам.

5.4. Настройка сбора событий

В этом разделе:

- Экспорт и импорт правил нормализации событий
- Экспорт и импорт источников событий
- Включение и отключение служебных источников
- Создание источника событий
- Управление источниками событий
- Выгрузка событий Комплекса в архив
- Отправка событий во внешнюю систему по протоколу Syslog

5.4.1. Экспорт и импорт правил нормализации событий

В этом разделе:

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

5.4.1.1. Экспорт правил разбора событий

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

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

5.4.1.2. Экспорт правил обогащения событий

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

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

5.4.1.3. Экспорт схемы событий

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

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

5.4.1.4. Импорт правил разбора событий

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

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

5.4.1.5. Импорт правил обогащения событий

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

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

5.4.1.6. Импорт схемы событий

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

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

5.4.2. Экспорт и импорт источников событий

В этом разделе:

- Экспорт источников событий
- Импорт источников событий

5.4.2.1. Экспорт источников событий

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

1. Перейдите на страницу **Администрирование** → **Основные настройки** → **Импорт и экспорт**.
2. На панели **Сбор данных** в строке **Источники событий** нажмите кнопку  (**Экспортировать**).
 - **Результат шага:** Будет загружен файл `sources[дата_и_время].json`.

5.4.2.2. Импорт источников событий

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

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

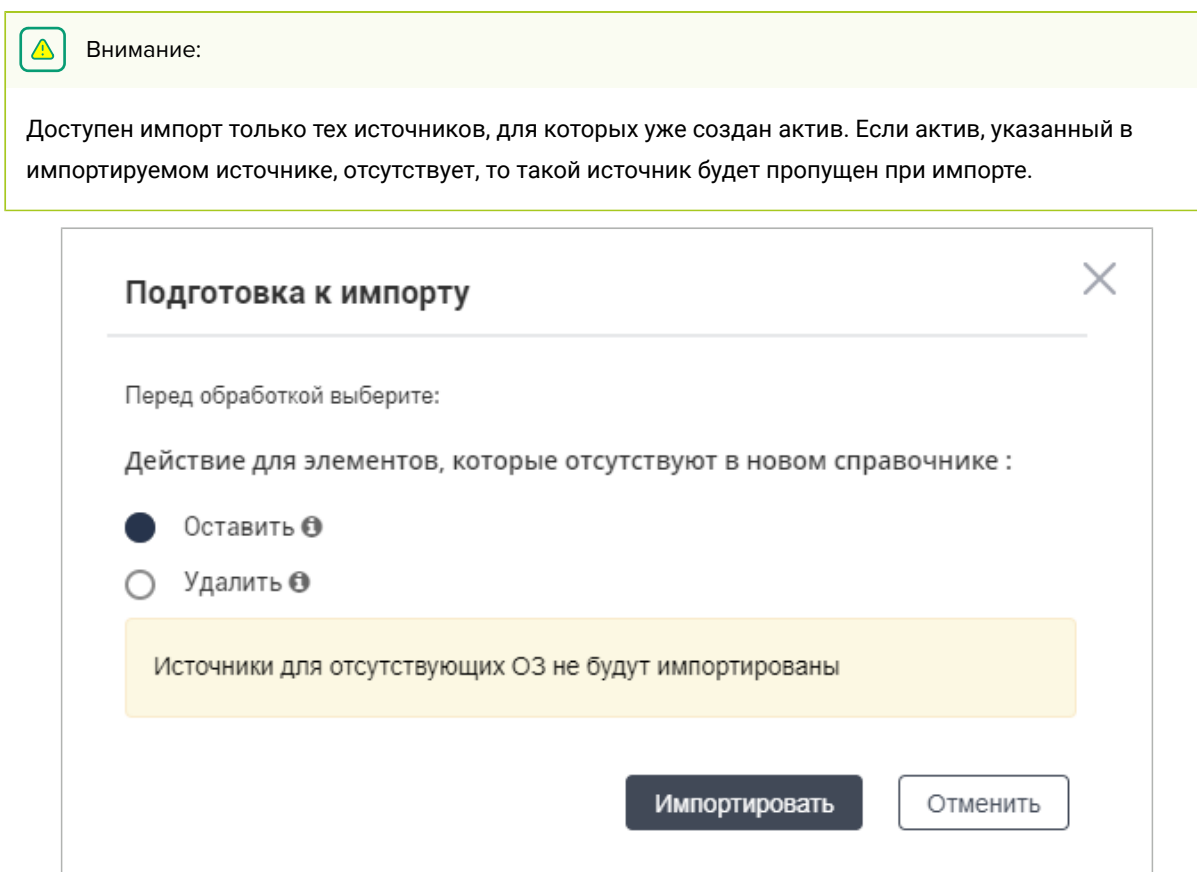


Рис. 83. Окно «Подготовка к импорту» при импорте источников событий активов

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

5.4.3. Включение и отключение служебных источников

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

Для управления запуском служебных источников:

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

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

3. Остановите работу сервисов Комплекса с помощью команды:

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

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

```
mcedit sensor.env
```

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



Подсказка:

Подробное описание сенсоров и возможных переменных см. в разделе «[Описание служебных источников событий](#)».

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

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

9. Дождитесь запуска работы всех сервисов.

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

5.4.4. Создание источника событий

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

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

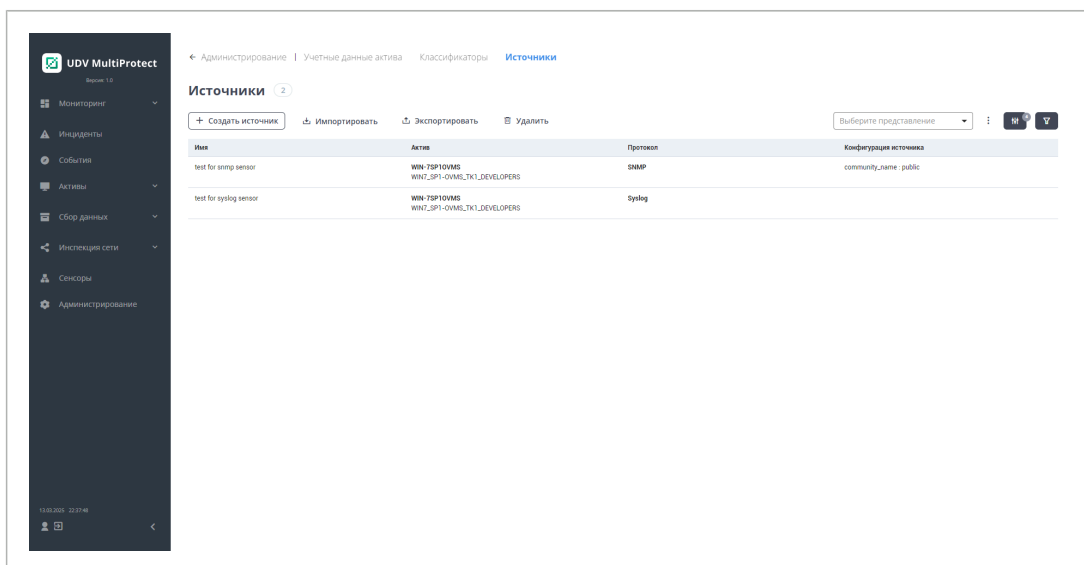


Рис. 84. Страница «Источники»

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

Создание источника

Наименование *

cisco-syslog

Описание

Объект защиты *

CISCO IOU

Степень критичности

low

Контроль активности источника ?

☒ Включить

Минимальное количество событий за период *

1

Период, сек *

300

Протокол *

Syslog

Создать

Отменить

Рис. 85. Окно «Создание источника» при создании источника syslog_rfc3164_sensor

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

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

5.4.5. Управление источниками событий

Для управления источниками событий присутствуют следующие возможности:

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

5.4.6. Выгрузка событий Комплекса в архив

Комплекс сохраняет архивы индексов событий в операционную систему в директорию `indices`. Директория `indices` расположена по умолчанию в `/var/backups/elasticsearch`, либо в другой директории, указанной в переменной `DATAPK_ELASTICSEARCH_BACKUP_DIR` конфигурационного файла `manager.env`.

5.4.6.1. Выгрузка индекса событий в архив

Чтобы сохранить отдельный индекс с событиями в архив:

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

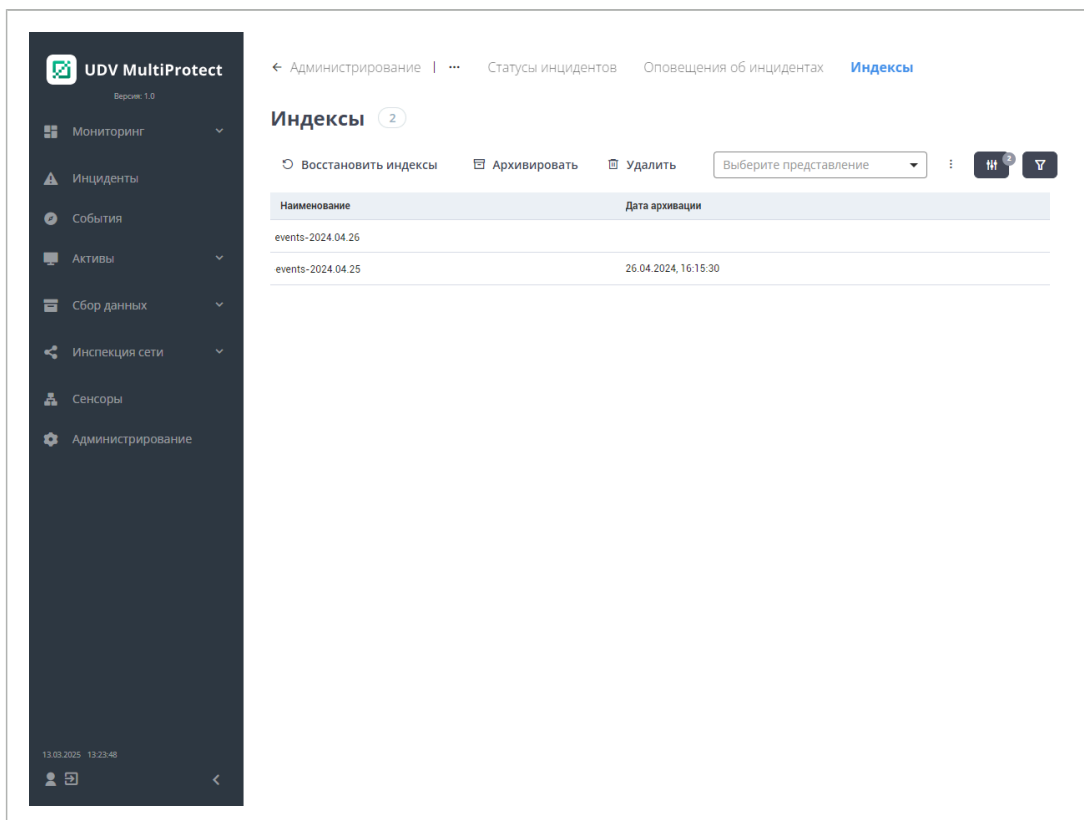


Рис. 86. Страница «Индексы»

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

5.4.6.2. Выгрузка нескольких индексов событий в архив

Чтобы сохранить отфильтрованные индексы с событиями в архивы:

1. Перейдите на страницу **Администрирование** → **События и инциденты** → **Индексы**.
2. Воспользуйтесь фильтрами для получения списка индексов, подлежащих архивированию.
3. Нажмите кнопку  (**Архивировать**) в верхней части страницы.
 - **Результат шага:** Для каждого отфильтрованного индекса отдельный архив `datapk_events_[тип_индекса]_[дата_индекса]` будет загружен в директорию `indices` (путь по умолчанию `/var/backups/elasticsearch/indices`).

5.4.7. Отправка событий во внешнюю систему по протоколу Syslog

Для отправки событий во внешнюю систему, например SIEM:

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

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

2. Если конфигурационный файл `95-siem-output.conf` отсутствует в директории `/etc/logstash/pipeline`, скопируйте его в текущую директорию одним из способов:

- скопируйте его из дистрибутива Комплекса;
- создайте новый файл вручную, выполнив команду:

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



ОСТОРОЖНО:

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

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

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

5. При необходимости измените в файле `95-siem-output.conf` следующие параметры:
 - в поле `host` измените IP-адрес внешнего сервера, на который будет выполняться отправка событий;
 - в поле `port` измените номер порта, если на внешнем сервере настроен другой порт для получения событий по Syslog UDP.
6. Сохраните изменения в файле, нажав клавишу **F2**, и закройте файл, нажав клавишу **F10**.
7. Поместите созданный файл в `/etc/logstash/pipeline` командой:

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

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

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

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

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

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

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

11. Откройте веб-интерфейс Комплекса и убедитесь, что события генерируются.

12. Убедитесь, что сетевой трафик отправляется на внешний Syslog-сервер. Для этого перейдите в режим командной строки Комплекса и введите команду:

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

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

Рис. 87. Пример отправки сетевого трафика на внешний Syslog-сервер

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

5.4.7.1. Остановка отправки событий во внешнюю систему по протоколу Syslog

Для остановки отправки событий во внешнюю систему по протоколу Syslog:

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

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

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

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

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

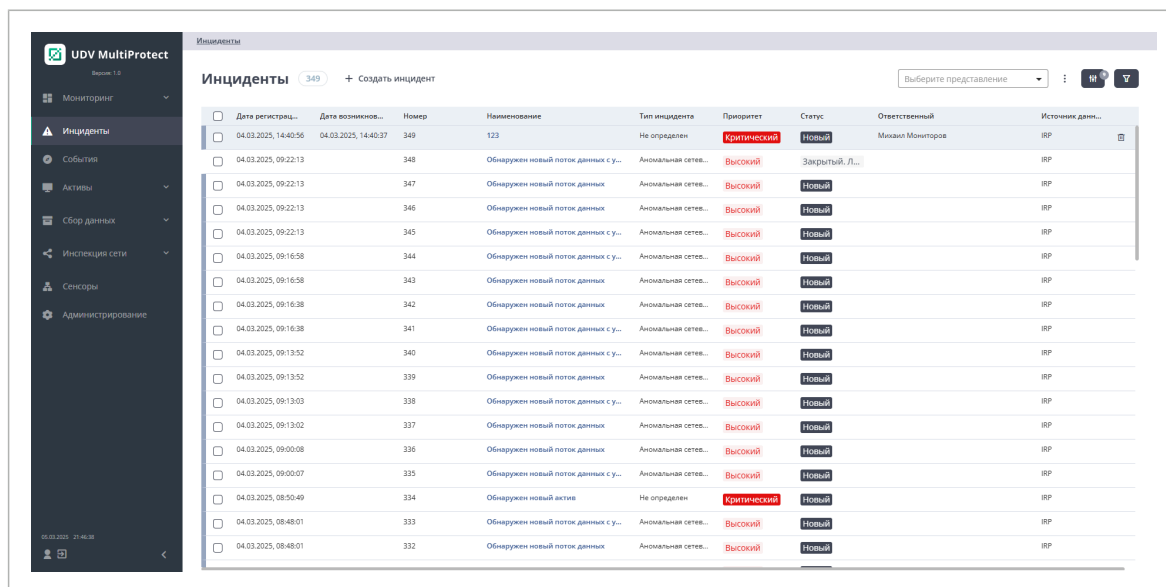
```
journalctl -u udv-logstash.service
```

6. Работа с инцидентами

Система автоматически генерирует инциденты из поступающих событий на основе правил корреляции. Также инциденты можно создавать вручную.

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

Список инцидентов доступен в веб-интерфейсе на соответствующей странице.



Дата регистрации...	Дата возникновения...	Номер	Наименование	Тип инцидента	Приоритет	Статус	Ответственный	Источник дан...
04.03.2025, 14:40:56	04.03.2025, 14:40:37	349	123	Не определен	Критический	Новый	Михаил Монитор	IRP
04.03.2025, 09:22:13		348	Обнаружен новый поток данных с у...	Аномальная сетев...	Высокий	Закрытый, л...		IRP
04.03.2025, 09:22:13		347	Обнаружен новый поток данных	Аномальная сетев...	Высокий	Новый		IRP
04.03.2025, 09:22:13		346	Обнаружен новый поток данных	Аномальная сетев...	Высокий	Новый		IRP
04.03.2025, 09:22:13		345	Обнаружен новый поток данных с у...	Аномальная сетев...	Высокий	Новый		IRP
04.03.2025, 09:16:58		344	Обнаружен новый поток данных с у...	Аномальная сетев...	Высокий	Новый		IRP
04.03.2025, 09:16:58		343	Обнаружен новый поток данных	Аномальная сетев...	Высокий	Новый		IRP
04.03.2025, 09:16:38		342	Обнаружен новый поток данных	Аномальная сетев...	Высокий	Новый		IRP
04.03.2025, 09:16:38		341	Обнаружен новый поток данных с у...	Аномальная сетев...	Высокий	Новый		IRP
04.03.2025, 09:13:52		340	Обнаружен новый поток данных с у...	Аномальная сетев...	Высокий	Новый		IRP
04.03.2025, 09:13:52		339	Обнаружен новый поток данных	Аномальная сетев...	Высокий	Новый		IRP
04.03.2025, 09:13:03		338	Обнаружен новый поток данных с у...	Аномальная сетев...	Высокий	Новый		IRP
04.03.2025, 09:13:02		337	Обнаружен новый поток данных	Аномальная сетев...	Высокий	Новый		IRP
04.03.2025, 09:00:08		336	Обнаружен новый поток данных	Аномальная сетев...	Высокий	Новый		IRP
04.03.2025, 09:00:07		335	Обнаружен новый поток данных с у...	Аномальная сетев...	Высокий	Новый		IRP
04.03.2025, 08:50:49		334	Обнаружен новый актив	Не определен	Критический	Новый		IRP
04.03.2025, 08:48:01		333	Обнаружен новый поток данных с у...	Аномальная сетев...	Высокий	Новый		IRP
04.03.2025, 08:48:01		332	Обнаружен новый поток данных	Аномальная сетев...	Высокий	Новый		IRP

Рис. 88. Страница «Инциденты»

Поиск инцидентов

Для фильтрации инцидентов нажмите кнопку  в правом верхнем углу. Для инцидентов доступны следующие фильтры:

- дата и время регистрации;
- дата и время возникновения;
- источник данных — **Вручную** или из доступных смежных систем;
- статус — **Новый, В работе, Закрытый. Устранен и Закрытый. Ложное срабатывание;**
- приоритет — **Критический, Высокий, Средний, Низкий;**
- пораженные компоненты;
- ответственный.

Статусы инцидентов

Инциденты в системе обрабатываются в соответствии с моделью статусов (состояний):

1. **Новый** — начальный статус инцидентов, который присваивается им по умолчанию. На данном этапе пользователи могут просматривать первичные данные об инцидентах, брать их в работу самостоятельно или назначать других ответственных.
2. **В работе** — статус, при котором выполняется обработка инцидентов. Пользователи могут запускать плейбуки для обогащения данных и локализации инцидентов, выполнять рекомендованные системой

мероприятия (задачи), закрывать инциденты или переводить их в ложные срабатывания, а также заполнять заключения и указывать дальнейшие рекомендации.

3. **Закрытый. Устранен** — конечное состояние решенных инцидентов. Пользователи могут просматривать карточки инцидентов, но не могут их редактировать и запускать плейбуки.
4. **Закрытый. Ложное срабатывание** — конечное состояние инцидентов, признанных ложными. Возможности пользователей совпадают с предыдущим пунктом.

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

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

6.1. Ручное создание инцидентов

Пользователи могут создавать инциденты вручную. Для этого:

1. Откройте страницу **Инциденты**.
2. Нажмите **Создать инцидент**.
 - **Результат шага:** Откроется окно для заполнения информации об инциденте.

Создание нового инцидента

Дата и время возникновения *

06.03.2025

✕

📅

12:39:37

Наименование *

Тестовый инцидент

Тип инцидента *

Нарушение работы сети

✕ ▾

Приоритет *

Средний

✕ ▾

Оповестивший *

Сидоров А. Е.

Ответственный *

Константин Волков

✕ ▾

Описание

Введите описание инцидента

Создать

Отменить

Рис. 89. Создание нового инцидента

3. Укажите информацию об инциденте: дату и время возникновения, наименование, тип и приоритет, имена оповестившего и ответственного. Дополнительную информацию об инциденте можно добавить в поле «Описание».
4. Нажмите **Создать**.
 - **Результат шага:** После этого откроется карточка, в которой можно будет просмотреть дополнительную информацию об инциденте и начать его обработку.

6.2. Анализ инцидентов

Подробности о выявленных и созданных вручную инцидентах можно просматривать в карточках.

Чтобы просмотреть карточку инцидента, нажмите на его наименование в таблице на странице **Инциденты**.

Инциденты > 332: Обнаружен новый поток данных с учетом правил автоматического одобрения

Инцидент 332: Обнаружен новый поток данных с учетом правил автоматического одобрения

Общая информация Реагирование Заключение

Описание

Между активами ip: 10.199.0.76, mac: 30:c5:0f:c8:09:fd и ip: 10.51.244.47, mac: 00:50:56:b7:14:72 обнаружено взаимодействие по протоколу ssl, которое не попадает под правила автоматического одобрения

Пораженные компоненты

Название актива	IPv4	Тип
APM финансового директора	10.51.244.47	APM

Атакующие компоненты

IP v4	FQDN	Email	Хеш-сумма
10.199.0.76	Ivanov.Aleksey	Ivanov@udv.group	521432a5b9df5630e1a9102bb7dd196d

Методики MITRE ATT&CK

Тактика	Код техники	Описание техники
Управление и контроль	T1001	Запутывание данных
Управление и контроль	T1008	Использование запасных каналов
Управление и контроль	T1090	Использование прокси
Управление и контроль	T1132	Кодирование данных для усложнения обнаружения
Закрепление	T1205	Использование сигнального трафика
Управление и контроль	T1571	Использование нестандартных портов

Характеристики

Статус В работе

Приоритет Высокий

Категория Сетевая атака

Тип Аномальная сетевая активность

Дата возникновения —

Дата регистрации 12.03.2025, 12:40:00

Дата взятия в работу 14.03.2025, 17:22:39

Дата закрытия —

Ответственный Константин Волков

Оповещений 123

Источник —

Реагирование

SLA реакции 3162 мин 39 сек

Закрыть до 12.03.2025, 15:40:00

Рис. 90. Карточка инцидента. Общая информация

Вкладка содержит следующие пункты:

- Описание.** В поле кратко объясняется, что произошло. Если инцидент сгенерирован системой на основе правил корреляции, текст будет составлен автоматически. Если инцидент добавляется вручную, описание может составить пользователь.
- Пораженные компоненты.** В таблице приводится список пораженных активов с указанием их названий и типов, а также IPv4-адресов. Вы можете открыть дополнительные сведения об указанных активах, нажав на нужную строку.
- Атакующие компоненты.** В таблице приводится список компонентов, участвовавших в атаке, с указанием их IPv4-адресов, FQDN, адресами электронных почт и хеш-суммами. Вы можете открыть дополнительные сведения об указанных активах, нажав на нужную строку.
- Методики MITRE ATT&CK.** В таблице указываются тактики, а также коды и описания техник, которые автоматически привязываются к инциденту в соответствии с его типом.
- Методики ТТУ ФСТЭК.** В таблице указываются тактики, а также коды и описания техник, которые автоматически привязываются к инциденту в соответствии с его типом.
- Связанные события.** В таблице указываются названия и даты возникновения событий, связанных с открытым инцидентом. Вы можете открыть дополнительные сведения о связанных событиях, нажав на нужную строку.

В боковой панели карточки всегда отображаются основные характеристики открытого инцидента — статус, категория, приоритет и др.

6.3. Обработка инцидентов

Инциденты обрабатываются специалистами ИБ после ознакомления с общей информацией в карточке.

Для обработки инцидента:

1. Откройте страницу **Инциденты**.
2. Нажмите на наименование нужного инцидента, чтобы открыть его карточку.
3. Чтобы начать обработку, нажмите **В работу** в верхней части карточки.
4. Чтобы получить дополнительные сведения об инциденте, нажмите **Запустить обогащение**.
5. Чтобы посмотреть полученные в результате обогащения данные, нажмите на строку с нужным компонентом. Если обогащение прошло успешно, в открывшейся вкладке будет доступна секция **Обогащение** с соответствующей информацией.
6. Выберите вкладку **Реагирование**. На ней представлен список плейбуков, которые назначаются автоматически в соответствии с типом инцидента. Запустите нужные плейбуки.
7. Завершив обработку и реагирование, нажмите **Закрыть инцидент**.
 - **Результат шага:** Откроется окно **Закрытие инцидента**.

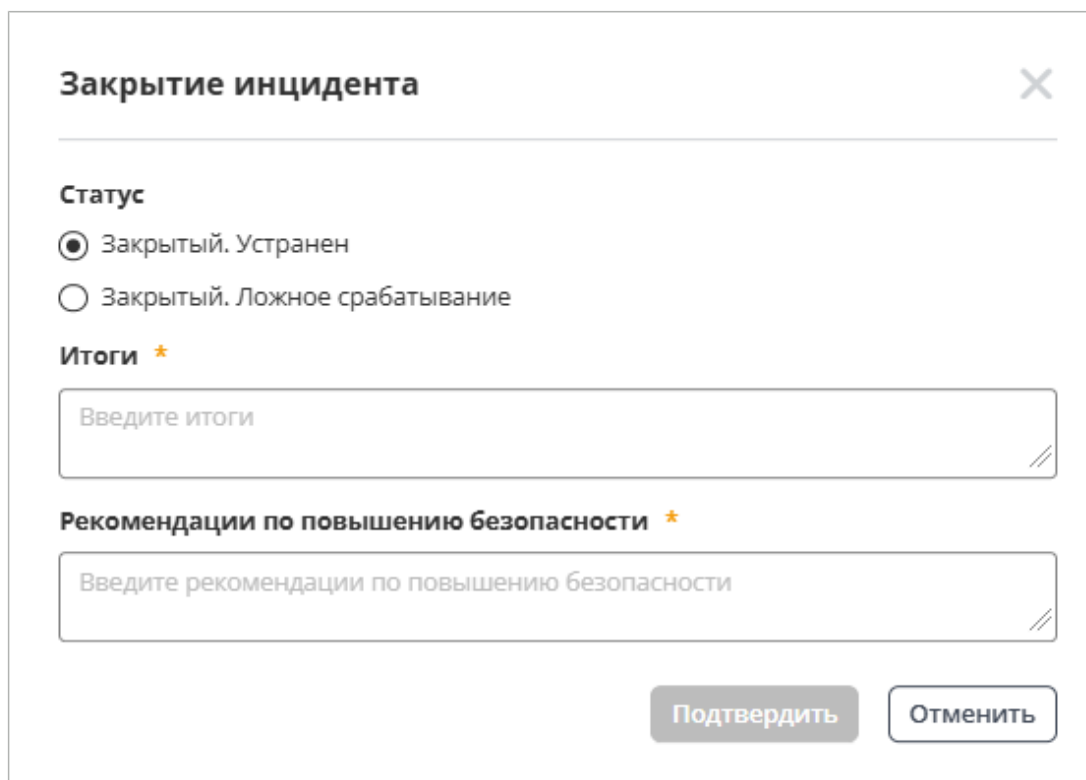


Рис. 91. Закрытие инцидента

8. Выберите статус инцидента:
 - **Закрытый. Устранен**, если инцидент оказался легитимным и все операции для его устранения выполнены;
 - **Закрытый. Ложное срабатывание**, если инцидент оказался нелегитимным и для его устранения не понадобилось дополнительных действий.
9. Укажите итоги разбора инцидента. Например, если инцидент оказался легитимным, кратко опишите, в чем он заключался и что было сделано для его устранения.
10. Укажите рекомендации по повышению безопасности.
11. Нажмите **Подтвердить**.

6.4. Изменение параметров инцидентов

В веб-интерфейсе Комплекса можно изменить приоритет и статус как одного, так и нескольких инцидентов.

6.4.1. Изменение параметров инцидента

Для редактирования одного инцидента:

1. Перейдите на страницу **Инциденты**.
2. Нажмите на название инцидента в таблице инцидентов.
 - **Результат шага:** Откроется карточка инцидента.
3. В боковой панели **Характеристики** нажмите .
- **Результат шага:** Откроется окно **Редактирование характеристик инцидента**.
4. Заполните следующие поля:
 - а. **Приоритет** — степень важности и срочности работы над инцидентом.
 - б. **Тип** — тип инцидента.
 - в. **Ответственный** — пользователь из списка, который будет отвечать за расследование инцидента.
 - г. **Оповестивший** — имя пользователя, который оповестил о возникновении инцидента.



Прим.:

Поля **Статус**, **Дата возникновения** и **Дата закрытия** нельзя редактировать вручную. Они заполняются автоматически при смене статусов инцидента во время расследования.

Редактирование характеристик инцидента

Статус *

В работе

Приоритет *

Критический

Тип *

Подозрительное повышение привилегий

Дата возникновения *

Дата закрытия

Ответственный *

Николай Кузнецов

Оповестивший *

Тестов А. Г.

Сохранить

Отменить

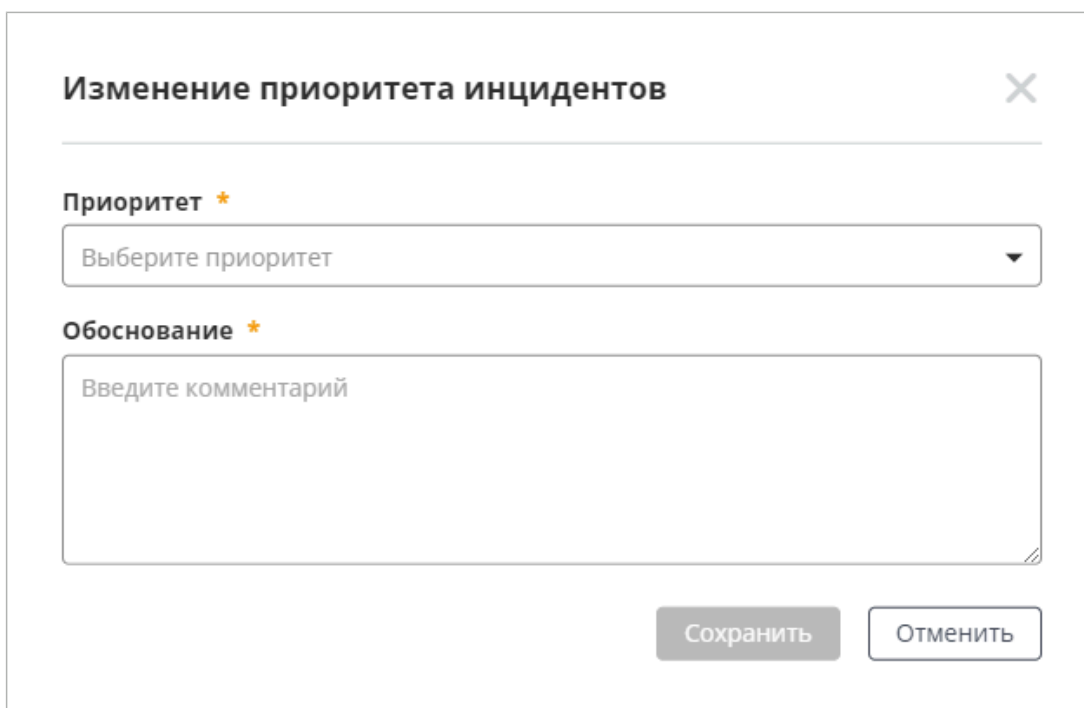
Рис. 92. Окно «Редактирование характеристик инцидента»

5. Нажмите **Сохранить**.

6.4.2. Изменение параметров нескольких инцидентов

Пользователи могут изменить приоритет нескольких инцидентов одновременно. Для этого:

1. Перейдите на страницу **Инциденты**.
2. Установите чекбокс возле необходимых инцидентов.
3. В открывшемся внизу меню нажмите **Приоритет**.
 - **Результат шага:** Откроется окно **Изменение приоритета инцидентов**.



Изменение приоритета инцидентов ✕

Приоритет *

Выберите приоритет ▼

Обоснование *

Введите комментарий

Сохранить Отменить

Рис. 93. Окно «Изменение приоритета инцидентов»

4. Заполните следующие обязательные поля:

- **Приоритет;**
- **Обоснование.**

5. Нажмите **Сохранить**.

 Прим.:
Пользователь, который меняет параметры, будет автоматически назначен ответственным за выбранные инциденты.

► **Результат шага:** Будет зафиксировано событие об изменении группы инцидентов. На странице **Инциденты** появится уведомление об обновлении инцидентов с датой и временем обновления.

6.5. Удаление инцидентов

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

6.5.1. Удаление инцидента

Для удаления одного инцидента:

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

 **Внимание:**

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

Для удаления инцидента необходимо обоснование×

Вы действительно хотите удалить инцидент?

Введите текст обоснования

Подтвердить

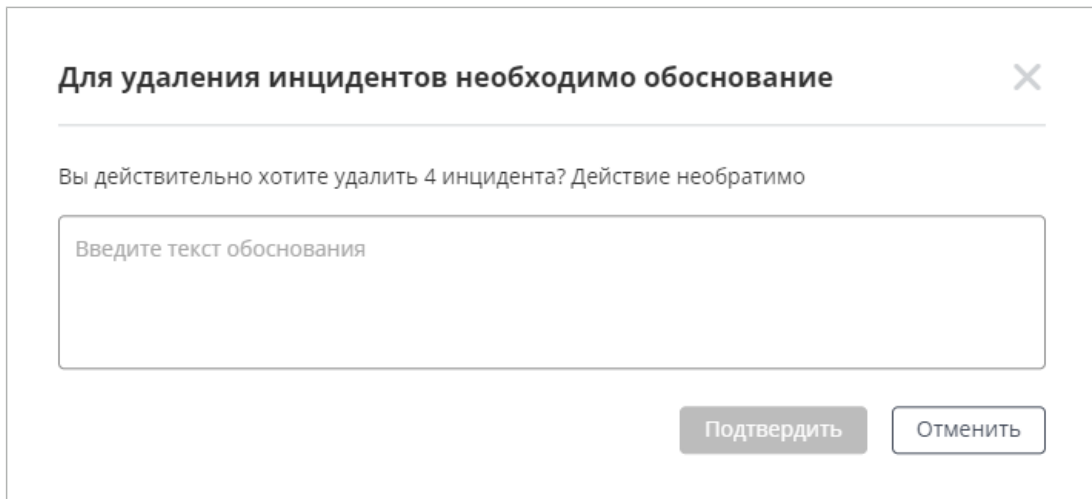
Отменить

Рис. 94. Окно обоснования удаления инцидента

6.5.2. Удаление нескольких инцидентов

Для удаления нескольких инцидентов:

1. Перейдите на страницу **Инциденты**.
2. Установите чекбоксы возле инцидентов, которые нужно удалить.
3. В открывшемся внизу меню нажмите **Удалить**.
4. Во всплывающем окне введите обоснование действия и нажмите **Подтвердить**.



The dialog box has a title bar with the text "Для удаления инцидентов необходимо обоснование" and a close button (X) in the top right corner. Below the title bar, the text "Вы действительно хотите удалить 4 инцидента? Действие необратимо" is displayed. A large text input field with the placeholder "Введите текст обоснования" is positioned below the text. At the bottom right, there are two buttons: "Подтвердить" (Confirm) and "Отменить" (Cancel).

Рис. 95. Окно обоснования удаления нескольких инцидентов

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

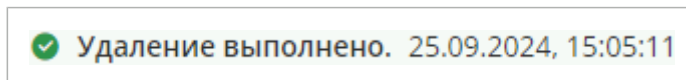


Рис. 96. Уведомление об удалении инцидентов

6.6. Групповые операции над инцидентами

Комплекс позволяет выполнять следующие групповые операции над инцидентами:

- устанавливать приоритет (подробнее см. раздел [Изменение параметров инцидентов](#));
- создавать отчет (подробнее см. раздел [Выгрузка отчетов](#));
- удалять инциденты (подробнее см. раздел [Удаление инцидентов](#)).

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

Групповые операции отображаются внизу страницы после выбора как минимум одного инцидента.

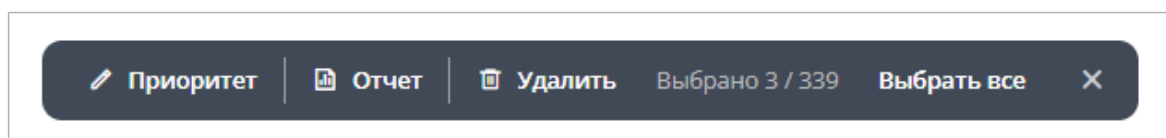


Рис. 97. Меню групповых операций

При работе с групповыми операциями возможны следующие виды статусов:

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



Подсказка:

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

6.7. Настройка инцидентов

В этом разделе:

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

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

Корреляция — способность системы выявлять закономерности в событиях и формировать инциденты на их основе. Служба корреляции событий работает на основе инструмента Esper. Для выполнения корреляции создаются правила обработки событий на языке EPL (Event Processing Language).

Механизм корреляции можно применять как для событий, поступающих в данный момент (текущий анализ), так и событий, полученных ранее (ретроспективный анализ).

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

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

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

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

Примеры элементов схемы корреляции событий:

- Элемент схемы представления событий аутентификации пользователей Комплекса:

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

- Элемент схемы представления событий о конфигурациях активов:

```
@public @buseventtype create json schema host_config as (action string,
  additional_information string, observer_id string, category string, create_time
  string, description string, event_code string, observer_id string, observer_name
  string, id string, observer_ip string, protocol string, receive_time string, severity
```

```
string, listener string, source_id string, source_ip string, source_hostname string,
source_mac string, source_port string, tags string, target_id string, target_ip string,
target_hostname string, target_port string, target_mac string, timestamp string, user
string)
```

- Элемент схемы представления событий инфообмена Комплекса:

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

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

Примеры правил для корреляции событий:

- подбор пароля в ОС Windows:

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

- удаленная чистка журнала безопасности в ОС Windows:

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

- удаленный вход в систему Windows с помощью службы RDP:

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



Подсказка:

Подробнее о синтаксисе, возможностях и примерах создания правил корреляции см. в разделе [Синтаксис правил корреляции событий](#).

Веб-интерфейс Комплекса позволяет создавать правила корреляции событий и загружать готовые списки правил из файлов формата *.json.

6.7.1. Экспорт и импорт политики корреляции и статусов инцидентов

В этом разделе:

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

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

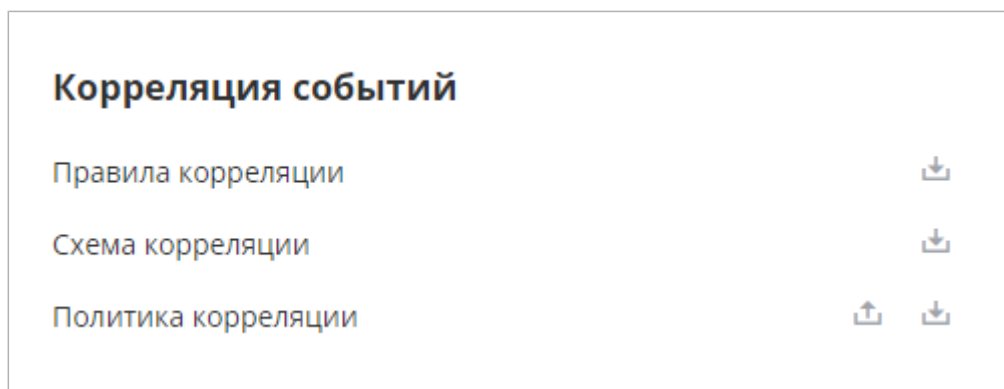


Рис. 98. Панель «Корреляция событий» на странице «Импорт и экспорт»

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

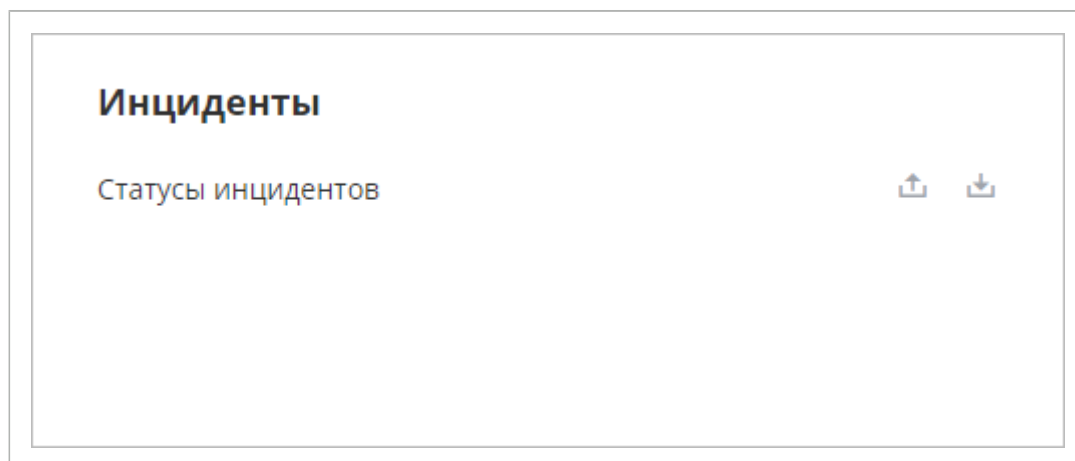


Рис. 99. Панель «Инциденты» на странице «Импорт и экспорт»

6.7.1.1. Импорт правил корреляции



Внимание:

Рекомендуется импортировать правила корреляции в составе политики корреляции (вместе со схемой).
Подробнее см. в разделе «[Импорт политики корреляции](#)».

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

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

Импорт

Перед обработкой выберите:

Действие для элементов, которые отсутствуют в новом справочнике:

☒ Оставить ⓘ

☐ Удалить ⓘ

Активность службы корреляции после импорта:

☐ Запустить принудительно ⓘ

☒ Оставить в текущем состоянии ⓘ

Статус активности элементов справочника после импорта:

☒ Оставить как есть ⓘ

☐ Присвоить старым статус, как в файле ⓘ

ИмпортироватьОтменить

Рис. 100. Окно импорта правил корреляции

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

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

6.7.1.2. Импорт схемы корреляции



Внимание:

Рекомендуется импортировать схему корреляции в составе политики корреляции (вместе с правилами).
Подробнее см. в разделе «[Импорт политики корреляции](#)».

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

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

Импорт

Перед обработкой выберите:

Действие для элементов, которые отсутствуют в новом справочнике:

☒ Оставить ⓘ

☐ Удалить ⓘ

Активность службы корреляции после импорта:

☐ Запустить принудительно ⓘ

☒ Оставить в текущем состоянии ⓘ

Статус активности элементов справочника после импорта:

☒ Оставить как есть ⓘ

☐ Присвоить старым статус, как в файле ⓘ

ИмпортироватьОтменить

Рис. 101. Окно «Подготовка к импорту» при загрузке схемы корреляции

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

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

6.7.1.3. Импорт политики корреляции

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

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

Импорт

Перед обработкой выберите:

Действие для элементов, которые отсутствуют в новом справочнике:

☒ Оставить ⓘ

☐ Удалить ⓘ

Активность службы корреляции после импорта:

☐ Запустить принудительно ⓘ

☒ Оставить в текущем состоянии ⓘ

Статус активности элементов справочника после импорта:

☒ Оставить как есть ⓘ

☐ Присвоить старым статус, как в файле ⓘ

ИмпортироватьОтменить

Рис. 102. Окно импорта политики корреляции

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

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

6.7.1.4. Экспорт политики корреляции

В составе политики корреляции экспортируются правила корреляции и схема корреляции.

Для экспорта политики корреляции событий в файл формата `.json`:

1. Перейдите на страницу **Администрирование** → **Основные настройки** → **Импорт и экспорт**.
2. На панели **Корреляция событий** в строке **Политика корреляции** нажмите кнопку  (**Экспортировать**).
 - **Результат шага:** файл с политикой корреляции `policy_correlation_[дата_и_время].json` будет сформирован и доступен для скачивания в правом верхнем углу страницы **Импорт и экспорт** под заголовком **Результат последнего экспорта**.
3. Для скачивания файла нажмите на название сформированного файла под заголовком **Результат последнего экспорта**.
4. В открывшемся окне укажите расположение для экспортируемого файла, введите название файла и нажмите **Сохранить**.
 - **Результат шага:** файл `policy_correlation_[дата_и_время].json` будет загружен на компьютер.

6.7.1.5. Экспорт статусов инцидентов

Для экспорта статусов инцидентов в файл формата `.json`:

1. Перейдите на страницу **Администрирование** → **Основные настройки** → **Импорт и экспорт**.
2. На панели **Инциденты** в строке **Статусы инцидентов** нажмите кнопку  (**Экспортировать**).
 - **Результат шага:** файл со статусами инцидентов `incidents_statuses_[дата_и_время].json` будет сформирован и доступен для скачивания в правом верхнем углу страницы **Импорт и экспорт** под заголовком **Результат последнего экспорта**.
3. Для скачивания файла нажмите на название сформированного файла под заголовком **Результат последнего экспорта**.
4. В открывшемся окне укажите расположение для экспортируемого файла, введите название файла и нажмите **Сохранить**.
 - **Результат шага:** файл `policy_correlation_[дата_и_время].json` будет загружен на компьютер.

6.7.2. Управление службой корреляции событий

В верхней части страницы **Администрирование** → **События и инциденты** → **Правила корреляции** доступны следующие возможности по управлению службой:

1. Запуск службы корреляции событий. Для запуска нажмите  (**Запустить службу**).
2. Остановка службы корреляции событий. Для остановки нажмите  (**Остановить службу**).
3. Перезапуск службы корреляции событий. Для перезапуска нажмите  (**Перезапустить службу**).
► **Результат шага:** Появится уведомление **Служба корреляции событий перезапущена**.
4. Просмотр событий и текущего состояния службы корреляции событий. Для просмотра:
 - а. Нажмите  (**Состояние службы корреляции**).
► **Результат шага:** Откроется окно **Состояние службы корреляции**.
 - б. Ознакомьтесь со списком событий службы корреляции.

Состояние службы корреляции

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

Заккрыть

Рис. 103. Окно «Состояние службы корреляции»



Подсказка:

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

6.7.3. Управление схемой корреляции



Подсказка:

Для применения изменений перезапуск службы не требуется. При редактировании или удалении элемента схемы, задействованного в текущем анализе, происходит автоматический перезапуск службы.

Веб-интерфейс предоставляет следующие возможности по изменению состава элементов схемы корреляции:

1. Создание. Для создания элемента схемы:

а. На странице **Схема корреляции** нажмите **Создать элемент схемы**.

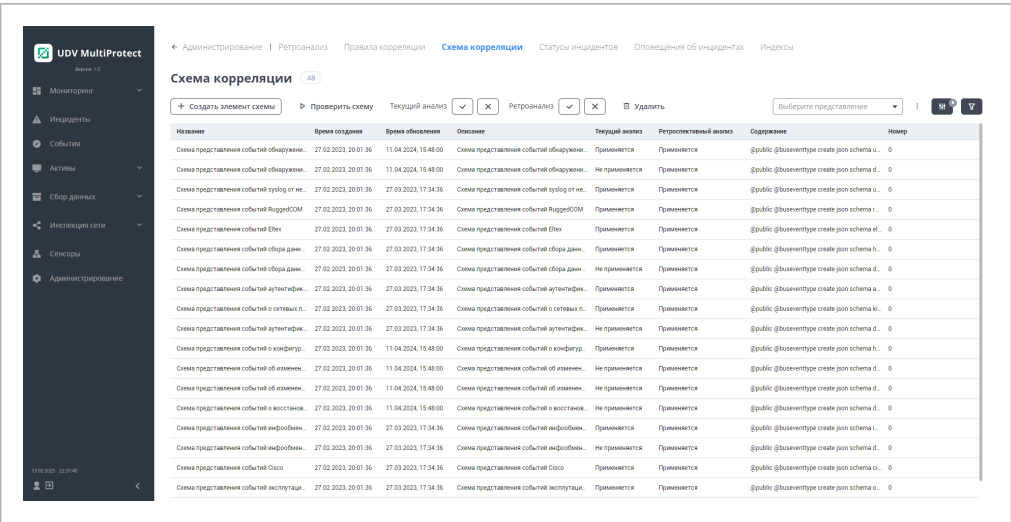


Рис. 104. Страница «Схема корреляции»

► **Результат шага:** появится окно **Создание элемента схемы**.

б. Заполните следующие обязательные поля:

- **Наименование** — отображаемое название элемента схемы;
- **Содержание** — состав схемы: переменные, контексты, окна;
- **Номер** — номер по порядку применения схемы.



Подсказка:

Если необходимости в определении порядка нет, введите в поле значение 0.

Создание элемента схемы ✕

Наименование *

Содержание *

Номер *

Описание

☐ Применять в текущем анализе

☐ Применять в ретроспективном анализе

Создать
Отменить

Рис. 105. Окно «Создание элемента схемы»

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

💡

Подсказка:

Подробнее о запуске анализа см. в разделе [«Анализ событий для генерации инцидентов»](#).

г. Нажмите **Создать**.

2. Проверка — позволяет оценить корректность созданных элементов схемы без запуска анализа. Для проверки схемы:

- а. Воспользуйтесь фильтрами на странице **Схема корреляции**. Для этого нажмите  в правом верхнем углу.
- б. Нажмите **Проверить схему**.
- в. Дождитесь окончания проверки.

► **Результат шага:** В правом верхнем углу появится уведомление *Отфильтрованные элементы схемы корректны.*


Внимание:

В случае получения ошибок измените элементы схемы.

3. Редактирование. Для редактирования элемента схемы:

- а. Наведите курсор на строку с элементом схемы, который нужно отредактировать.
- б. В правой части страницы нажмите  (**Редактировать**).

► **Результат шага:** откроется окно **Редактирование элемента схемы**.

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

Редактирование элемента схемы

✕

Наименование *

Содержание *

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

Номер *

Описание

☒ Применять в текущем анализе

☒ Применять в ретроспективном анализе

Сохранить

Отменить

Рис. 106. Окно «Редактирование элемента схемы»

4. Удаление. Для удаления одного элемента схемы:

- а. Наведите курсор на строку с элементом, который нужно удалить.
- б. Нажмите  (**Удалить элемент схемы**).

► **Результат шага:** появится окно подтверждения удаления.

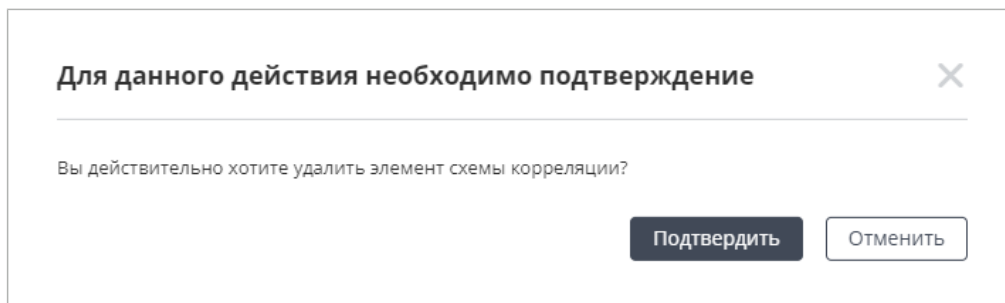


Рис. 107. Окно подтверждения удаления элемента схемы корреляции

в. Нажмите **Подтвердить**.

5. Групповое удаление. Для удаления всех отображаемых на странице элементов:

а. Воспользуйтесь фильтрами на странице **Схема корреляции**. Для этого нажмите  в правом верхнем углу.

б. В верхней части страницы нажмите  (**Удалить**).

► **Результат шага:** появится окно подтверждения удаления.

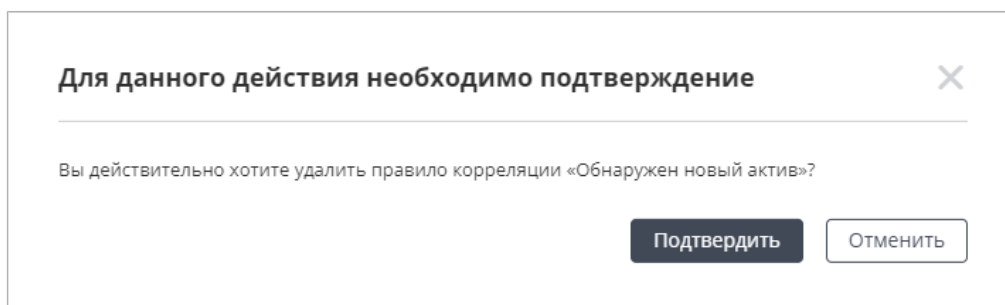


Рис. 108. Окно подтверждения удаления элементов схемы корреляции

в. Нажмите **Подтвердить**.

6.7.4. Управление правилами корреляции событий

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

- Создание правил корреляции событий;
- Редактирование правил корреляции событий;
- Копирование правил корреляции событий;
- Удаление правила корреляции событий;
- Групповое удаление правил корреляции событий.

6.7.4.1. Создание правил корреляции событий

Для создания правила:

1. Перейдите на страницу **Администрирование → События и инциденты → Правила корреляции.**

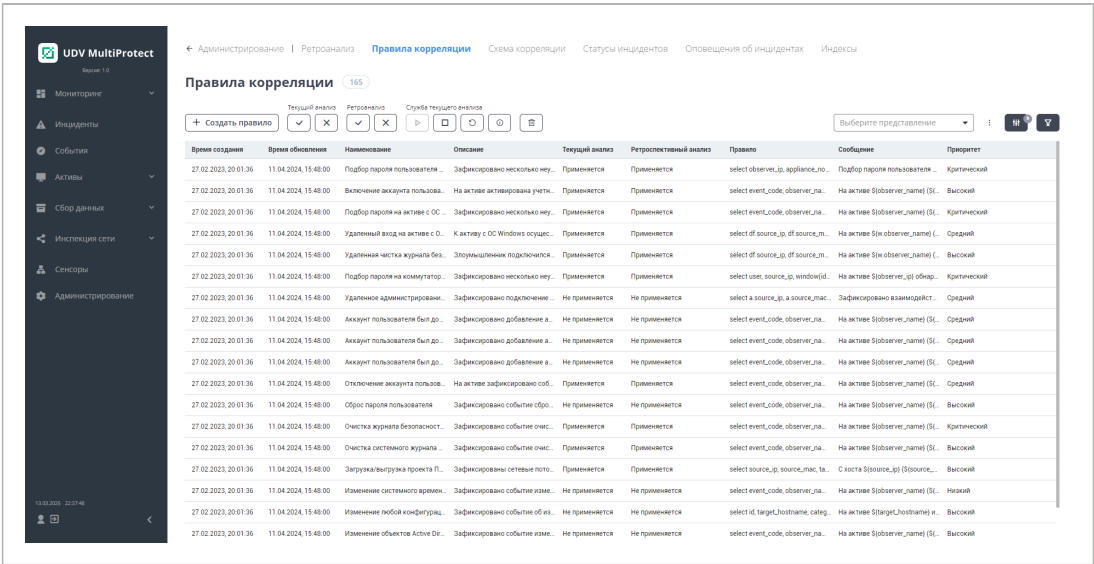


Рис. 109. Страница «Правила корреляции»

2. Нажмите **Создать правило**. В открывшемся окне настройте следующие параметры:

- наименование и описание;

 **Внимание:**

Для поля **Описание** установлен лимит, равный 2000 символов.

- правило;
- сообщение, которое будет отображаться при возникновении события;
- при необходимости установите чекбоксы для применения в текущем и (или) ретроспективном анализе.

Создание правила корреляции

✕

Наименование *

Описание

Правило *

Сообщение *

Приоритет *

Средний ▼

☐ Применять в текущем анализе

☐ Применять в ретроспективном анализе

Создать

Отменить

Рис. 110. Окно «Создание правила корреляции»

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

⚠

Внимание:

В процессе сохранения правило будет проверено на корректность синтаксиса для выбранного анализа. В случае появления несоответствий и ошибок, правило не будет сохранено.

► **Результат шага:** Правило будет доступно для применения в текущем и ретроспективном анализе.

6.7.4.2. Редактирование правил корреляции событий

Для редактирования правила:

1. Перейдите на страницу **Правила корреляции**.
2. В правой части страницы нажмите  (**Редактировать**).
 - **Результат шага:** Откроется окно **Редактирование правила корреляции**.
3. Измените необходимые параметры и нажмите **Сохранить**.

Редактирование правила корреляции

Наименование *

Обнаружен новый актив

Описание

Зафиксировано событие о появлении неизвестного активаТактика: TA0001 Пер

Правило *

```
select id, target_id, target_ip, target_mac, appliance_node_id from
unknown_host_detected
```

Сообщение *

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

Приоритет *

Критический

☒ Применять в текущем анализе

☒ Применять в ретроспективном анализе

Сохранить

Отменить

Рис. 111. Окно «Редактирование правила корреляции»

- **Результат шага:** отредактированное правило будет сохранено как новое правило корреляции. Исходное правило также сохранится.

6.7.4.3. Копирование правил корреляции событий

Для копирования правила:

1. Наведите курсор на строку с правилом, которое нужно скопировать.
2. Нажмите кнопку  (**Создать копию правила**), расположенную справа в списке правил.
 - **Результат шага:** Откроется окно **Создание копии правила корреляции**.
3. Измените необходимые параметры и нажмите **Сохранить**.

Создание копии правила корреляции

✕

Наименование *

Копия Обнаружен новый актив

Описание

Зафиксировано событие о появлении неизвестного активаТактика: TA0001 Пер

Правило *

```
select id, target_id, target_ip, target_mac, appliance_node_id from
unknown_host_detected
```

Сообщение *

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

Приоритет *

Критический

☐ Применять в текущем анализе
☐ Применять в ретроспективном анализе

Создать

Отменить

Рис. 112. Окно «Создание копии правила корреляции»

- **Результат шага:** Созданная копия правила корреляции событий появится в списке правил и будет доступна для применения в текущем и ретроспективном анализе. Исходное правило также сохранится.

6.7.4.4. Удаление правила корреляции событий

Для удаления одного правила:

1. Наведите курсор на строку с правилом, которое нужно удалить.
2. Нажмите  (**Удалить правило**).
 - **Результат шага:** Появится окно ввода обоснования удаления.
3. Введите обоснование удаления и нажмите **Подтвердить**.

6.7.4.5. Групповое удаление правил корреляции событий

1. Воспользуйтесь фильтрами на странице **Правила корреляции**.
2. В верхней части страницы нажмите  (**Удалить правила**).

- **Результат шага:** Появится окно ввода обоснования удаления.

3. Введите обоснование и нажмите **Удалить**.

6.7.5. Анализ событий для генерации инцидентов

В этом разделе:

- Текущий анализ событий
- Ретроспективный анализ событий
- Управление ретроспективными проверками

После настройки правил и схемы корреляции последним шагом для появления инцидентов является запуск анализа событий. Комплекс позволяет производить как анализ событий реального времени (текущий), так и анализ событий, полученных ранее (ретроспективный).

Для управления использованием схем и правил корреляции в текущем и ретроспективном анализах в верхней части страниц расположены управляющие элементы, позволяющие отрегулировать список схем и правил, используемых в том или ином анализе.

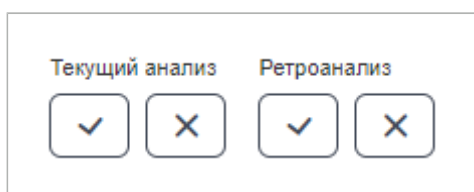


Рис. 113. Кнопки управления активностью элементов в анализах

Разница в запуске текущего и ретроспективного анализа заключается в том, что для запуска текущего анализа достаточно установить активность соответствующих политик корреляции (правил и схем корреляции), а для ретроспективного анализа нужно также выбрать период, за который будут проанализированы события в соответствии с политикой корреляции.

6.7.5.1. Текущий анализ событий

Для запуска текущего анализа событий:

1. Убедитесь в наличии элементов схемы корреляции. Для этого перейдите на страницу **Администрирование → События и инциденты → Схема корреляции**.
2. Активируйте один или несколько элементов схем корреляции. Для этого:
 - а. Воспользуйтесь фильтрами на странице **Схема корреляции**. Для этого нажмите  в верхнем правом углу страницы.
 - б. Для активации элемента схемы:
 - наведите курсор на строку с элементом схемы и нажмите  (**Редактировать**);
 - установите чекбокс **Применение в текущем анализе**;
 - нажмите **Сохранить**.
 - в. Для активации всех выбранных в фильтре элементов схемы нажмите  (**Включить элементы схемы для текущего анализа**).
3. Убедитесь в наличии правил корреляции. Для этого перейдите на страницу **Инциденты → Правила корреляции**.
4. Активируйте одно или несколько правил корреляции. Для этого:

а. Воспользуйтесь фильтрами в левой части страницы **Правила корреляции**.

б. Для активации отдельных правил:

- в строке с правилом нажмите  (**Редактировать**);
- установите чекбокс **Активно в текущем анализе**;
- нажмите **Сохранить**.

в. Для активации всех выбранных в фильтре правил нажмите  (**Применить правила для текущего анализа**).

► **Результат шага:** правила будут задействованы в текущем анализе без необходимости перезапуска службы.

5. Убедитесь в том, что произведенные настройки были применены. Для этого:

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

б. Убедитесь, что список последних событий службы не содержит ошибок.

Возможные затруднения: Для устранения ошибок, связанных с применением правил, вы можете перезапустить службу корреляции. Для этого в верхней части страницы **Правила корреляции** нажмите



(**Перезапустить службу**).

6.7.5.2. Ретроспективный анализ событий

Для запуска ретроспективного анализа событий:

1. Убедитесь в наличии элементов схемы корреляции. Для этого перейдите на страницу

Администрирование → События и инциденты → Схема корреляции.

2. Активируйте один или несколько элементов схемы корреляции. Для этого:

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

- б. Для активации элемента схемы:

- наведите курсор на строку со схемой и нажмите  (**Редактировать**);
- установите чекбокс **Применение в ретроспективном анализе**;
- нажмите **Сохранить**.

- в. Для активации всех выбранных в фильтре элементов схемы нажмите  (**Включить элементы схемы для ретроспективного анализа**).

3. Убедитесь в наличии правил корреляции. Для этого перейдите на страницу **Администрирование → События и инциденты → Правила корреляции**.

4. Активируйте одно или несколько правил корреляции. Для этого:

- а. Воспользуйтесь фильтрами на странице **Правила корреляции**.

- б. Для активации отдельных правил:

- в строке с правилом нажмите  (**Редактировать**);
- установите чекбокс **Активно в ретроспективном анализе**;
- нажмите **Сохранить**.

- в. Для активации всех выбранных в фильтре правил нажмите  (**Включить правила для ретроспективного анализа**).

5. Запустите ретроспективную проверку. Для этого:



Внимание:

Возможен запуск только одной проверки за раз.

- а. Перейдите на страницу **Администрирование → События и инциденты → Ретроанализ**.

- б. Нажмите **Запустить анализ**.

► **Результат шага:** появится окно **Запуск ретроспективного анализа**.

- в. В открывшемся окне задайте следующие обязательные параметры анализа:

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

Запуск ретроспективного анализа

Название *

Период для анализа событий *

От

До

Фильтр ⓘ

Описание

Запустить

Отменить

Рис. 114. Окно запуска ретроспективного анализа

**Внимание:**

При указании периода ретроспективного анализа вы можете указать дату окончания в будущем. Этот способ позволит учитывать события, которые могут возникнуть из-за разницы часовых поясов на распределенных инсталляциях или из-за некорректно настроенного времени на источнике данных.

г. При необходимости введите описание и фильтр в формате Lucene.

д. Нажмите **Запустить**.

**Подсказка:**

Если необходимо остановить процесс анализа, нажмите кнопку **Остановить анализ** в верхней части страницы.

**Внимание:**

Запуск других ретроспективных анализов будет недоступен до окончания проверки. Удалять анализ до окончания проверки не рекомендуется.

- е. Дождитесь окончания выполнения анализа.
 - **Результат шага:** по завершении анализа будет получен статус и число выявленных инцидентов. Для просмотра списка инцидентов нажмите на число в колонке **Число инцидентов**.
- 6. Если был получен статус *Ошибка* или *Выполнено с ограничениями*:
 - а. Наведите курсор на строку с выполненной проверкой.
 - б. Нажмите на ячейку статуса или кнопку  (**Просмотреть статус анализа**) в конце строки.
 - **Результат шага:** появится окно **Статус анализа**.
 - в. Ознакомьтесь с представленной в окне информацией.

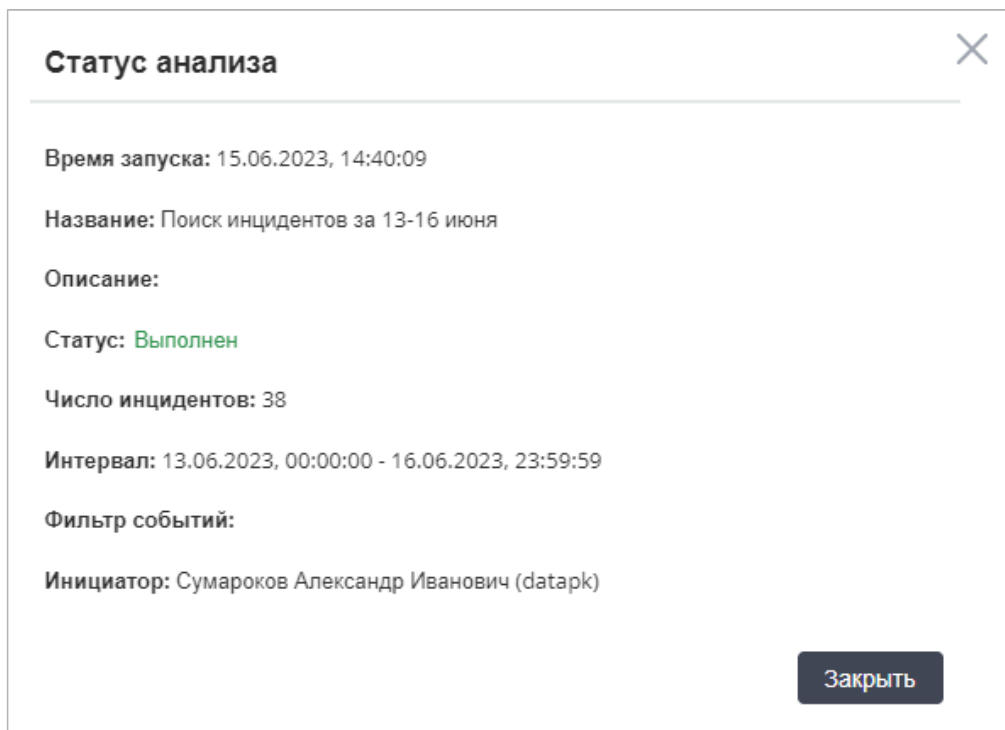


Рис. 115. Окно «Статус анализа»

6.7.5.3. Управление ретроспективными проверками

Помимо первичного запуска ретроспективного анализа можно перезапускать, удалять проверки и создавать по ним отчет.

Возможности для управления ретроспективными проверками:

1. Просмотр статуса проверки. Для просмотра:
 - а. Наведите курсор на строку с выполненной проверкой.
 - б. Нажмите на ячейку статуса или кнопку  (**Просмотреть статус анализа**) в конце строки.
 - **Результат шага:** появится окно **Статус анализа**.
 - в. Ознакомьтесь с представленной в окне информацией.

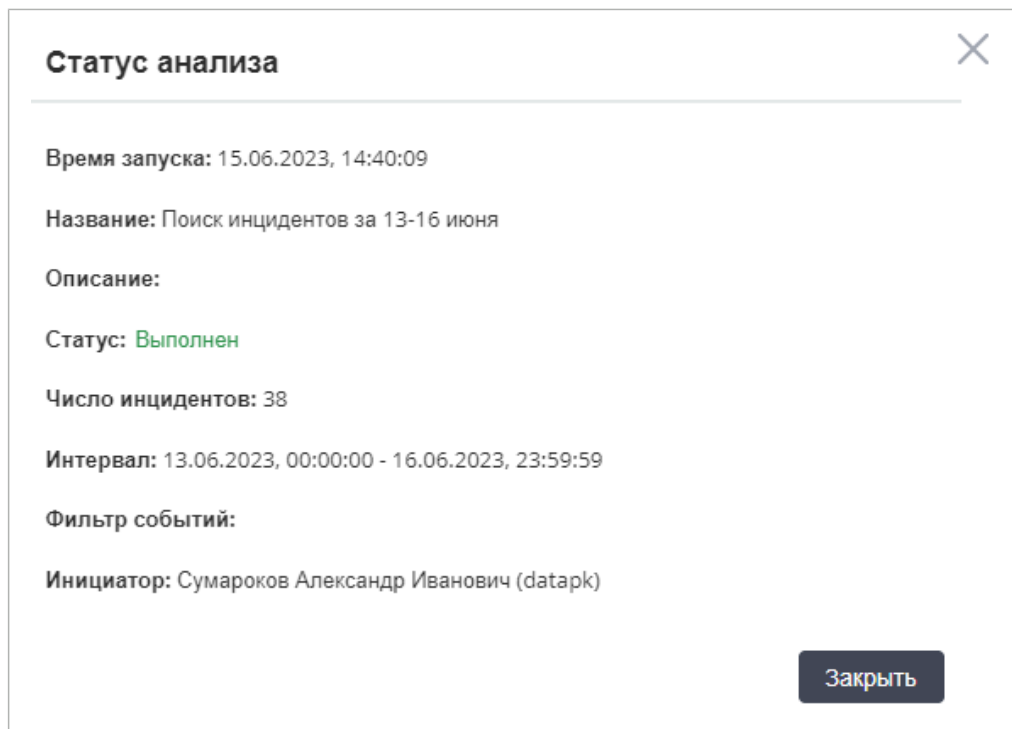


Рис. 116. Окно «Статус анализа»

2. Просмотр инцидентов по результатам проверки. Для просмотра всех выявленных в рамках анализа инцидентов:
 - а. Наведите курсор на строку с выполненной проверкой.
 - б. Нажмите на число в колонке **Число инцидентов**.

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

Рис. 117. Переход к просмотру инцидентов по результатам ретроспективной проверки

- **Результат шага:** будет выведен список всех инцидентов, полученных в результате ретроспективного анализа.

3. Перезапуск. Для перезапуска созданного ранее ретроспективного анализа:

а. Наведите курсор на строку с выполненной проверкой.

б. В правой части страницы нажмите  (**Повторить анализ**).

► **Результат шага:** на месте кнопки запуска анализа появится кнопка **Остановить анализ**.

При необходимости вы можете воспользоваться возможностью прервать проверку, нажав соответствующую кнопку.

4. Удаление одной проверки. Для удаления ретроспективной проверки:



Внимание:

Инциденты, полученные в результате анализа, будут сохранены.

а. Наведите курсор на строку с выполненной проверкой.

б. Убедитесь, что удаляемый анализ не запущен. Если запущен — остановите выполнение проверки.

в. В правой части страницы нажмите  (**Удалить анализ**).

► **Результат шага:** проверка будет удалена.

5. Удаление проверок, отображаемых на странице. Для удаления ретроспективных проверок:



Внимание:

Инциденты, полученные в результате проверок, будут сохранены.

а. Наведите курсор на строку с выполненной проверкой.

б. Убедитесь, что ни один из удаляемых анализов не запущен. Если запущен — остановите выполнение проверки.

в. В правой части страницы нажмите  (**Удалить анализ**).

► **Результат шага:** проверка будет удалена.

6.7.6. Настройка оповещений при появлении инцидентов

В этом разделе:

- Настройка оповещения пользователей по электронной почте
- Настройка правила для отправки оповещений на OPC-сервер

После того как служба корреляции событий формирует инциденты, можно автоматически отправлять оповещения пользователям на электронную почту или на OPC-сервер.

Управление отправкой оповещений осуществляется на странице **Оповещения об инцидентах**.

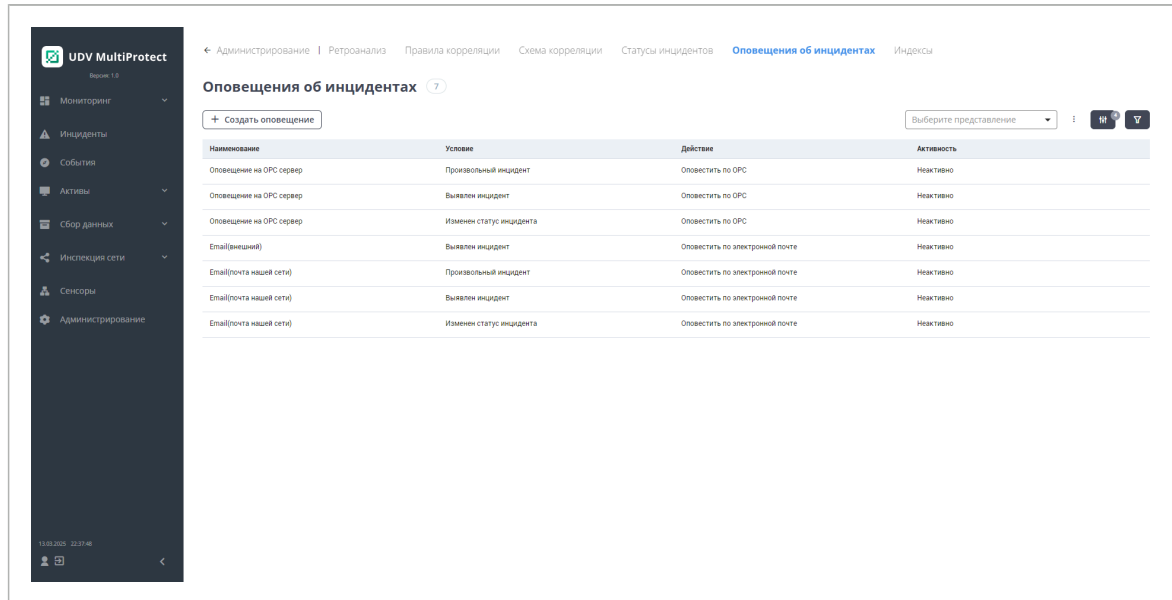


Рис. 118. Страница «Оповещения об инцидентах»

6.7.6.1. Настройка оповещения пользователей по электронной почте

Для настройки правила для оповещения пользователей по электронной почте (с использованием протокола SMTP/SMTPS) при появлении любых инцидентов или изменении их статуса:

1. Перейдите на страницу **Администрирование** → **События и инциденты** → **Оповещения об инцидентах**.
2. Нажмите **Создать оповещение** в верхней части страницы.
3. В открывшемся окне **Создание оповещения** настройте следующие параметры:
 - а. тип оповещения — **Оповестить по электронной почте**;
 - б. наименование оповещения;
 - в. условие, при котором будет выполняться оповещение, в поле **Условие**;
 - г. если выбрано условие **Произвольный инцидент**, в появившемся поле **Ключевое слово** введите ключевое слово для одного из полей инцидента;



Подсказка:

В качестве значения поля **Ключевое слово** можно задать наименование, описание или Комплекс, на котором был обнаружен инцидент.

**Внимание:**

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

- д. адрес SMTP сервера;
- е. Email-адрес отправителя;
- ж. TCP-порт для обращения к почтовому серверу по протоколу SMTP — целое число от 1 до 65535;
- з. добавьте Email-адреса получателей писем. Для этого:
 - введите адрес в поле **Email Адрес получателя**;
 - нажмите кнопку ;
 - добавьте другие адреса при необходимости.
- и. тему письма, которое будет получать пользователь при возникновении указанного события;
- к. протокол шифрования;
- л. установите чекбокс **Использовать авторизацию**, если необходим пароль для входа на почтовый сервер;
- м. если чекбокс **Использовать авторизацию** установлен, введите пароль для возможности аутентификации на почтовом сервере;
- н. установите чекбокс **Активность** для активации правила.

Рис. 119. Окно «Создание оповещения» при настройке оповещения о любых инцидентах по электронной почте

4. Нажмите кнопку **Создать**.

► **Результат шага:** созданное правило оповещения будет отображаться на странице **Оповещения об инцидентах**.

6.7.6.1.1. Отправка тестового оповещения об инциденте

Для отправки тестового оповещения об инциденте:

1. Перейдите на страницу **Администрирование** → **События и инциденты** → **Оповещения об инцидентах**.
2. Наведите курсор на необходимое правило оповещения.
3. Нажмите кнопку  (**Отправить тестовое оповещение**).

► **Результат шага:** появится уведомление **Тестовое оповещение успешно отправлено**.



Подсказка:

оповещения будут приходить в следующем формате:

Описание события: [Текст с описанием события].
 Инцидент: [Наименование инцидента].
 Дата создания: [дата и время с указанием часового пояса в формате UTC].
 Активы: [наименования активов].
 Описание инцидента: [Текст с описанием инцидента].
 Ссылка на инцидент: [https://\[IP-адрес текущего Комплекса\]/app/incidents/\[идентификатор инцидента\]](https://[IP-адрес текущего Комплекса]/app/incidents/[идентификатор инцидента])



Внимание:

В случае установки некорректных настроек при отправке тестового оповещения будет отображаться уведомление **Не удастся отправить тестовое оповещение: почтовый сервер недоступен, либо один или несколько параметров оповещения имеют некорректные значения**

6.7.6.1.2. Изменение пароля для подключения к почтовому серверу

У ранее созданного правила оповещения можно изменить пароль для подключения к почтовому серверу. Для этого:

1. Перейдите на страницу **Администрирование** → **События и инциденты** → **Оповещения об инцидентах**.
2. Нажмите кнопку (**Редактировать оповещение**) в таблице оповещений.
3. В открывшемся окне **Редактирование оповещения** нажмите кнопку **Изменить пароль**.
4. В открывшемся окне **Изменение пароля для подключения к SMTP серверу** введите новый пароль в поля **Новый пароль** и **Подтверждение нового пароля** и нажмите кнопку **Сохранить**.

Рис. 120. Окно «Изменение пароля для подключения к SMTP серверу»

5. Нажмите кнопку **Сохранить** в окне **Редактирование оповещения**.
 - **Результат шага:** изменения, внесенные в оповещение, будут перезаписаны.

6.7.6.2. Настройка правила для отправки оповещений на OPC-сервер

Для настройки правила отправки оповещений на OPC-сервер при появлении инцидентов или изменении их статуса:

1. Перейдите на страницу **Администрирование** → **События и инциденты** → **Оповещения об инцидентах**.
2. Нажмите кнопку **Создать оповещение**.
3. В открывшемся окне **Создать оповещения** настройте следующие параметры:
 - а. выберите **Оповестить по OPC** в поле **Тип оповещения**;
 - б. наименование создаваемого оповещения;
 - в. условие, при котором будет выполняться оповещение, в поле **Условие**;
 - г. если выбрано условие **Произвольный инцидент**, в появившемся поле **Ключевое слово** введите ключевое слово для одного из полей инцидента;



Подсказка:

В качестве значения поля **Ключевое слово** можно задать наименование, описание или Комплекс, на котором был обнаружен инцидент.



Внимание:

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

- д. IP-адрес OPC-сервера;
- е. TCP-порт для обращения к OPC-серверу по протоколу OPC UA — целое число от 1 до 65535;
- ж. URL-ссылку на OPC-сервер (при наличии);
- з. индекс пространства имен, в котором расположен тег, в поле **NamespaceIndex**;
- и. формат значения поля **Identifier** в поле **IdentifierType**;



Подсказка:

Для отправки сообщений с текстом необходимо создавать оповещения со значением поля **IdentifierType**, равным **String**.

- к. идентификатор тега OPC-сервера в соответствии с выбранным форматом данных в поле **Identifier**;
- л. логин и пароль для входа на OPC-сервер (если требуется);
- м. формат значения тега в поле **Тип тега**;

**Внимание:**

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

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

Рис. 121. Окно «Создание оповещения» при настройке оповещения об инцидентах по протоколу OPC

4. Нажмите кнопку **Создать**.

► **Результат шага:** созданное правило оповещения будет отображаться на странице **Оповещения об инцидентах**.

6.7.6.2.1. Отправка тестового оповещения об инциденте

Для отправки тестового оповещения об инциденте:

1. Перейдите на страницу **Администрирование** → **События и инциденты** → **Оповещения об инцидентах**.
2. Наведите курсор на необходимое правило оповещения.
3. Нажмите кнопку  (**Отправить тестовое оповещение**).

► **Результат шага:** появится уведомление **Тестовое оповещение успешно отправлено**.

 Подсказка:

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

Описание события: [Текст с описанием события].
 Инцидент: [Наименование инцидента].
 Дата создания: [Дата и время с указанием часового пояса в формате UTC].
 Активы: [Наименования активов].
 Описание инцидента: [Текст с описанием инцидента].
 Ссылка на инцидент: [Ссылка на инцидент].

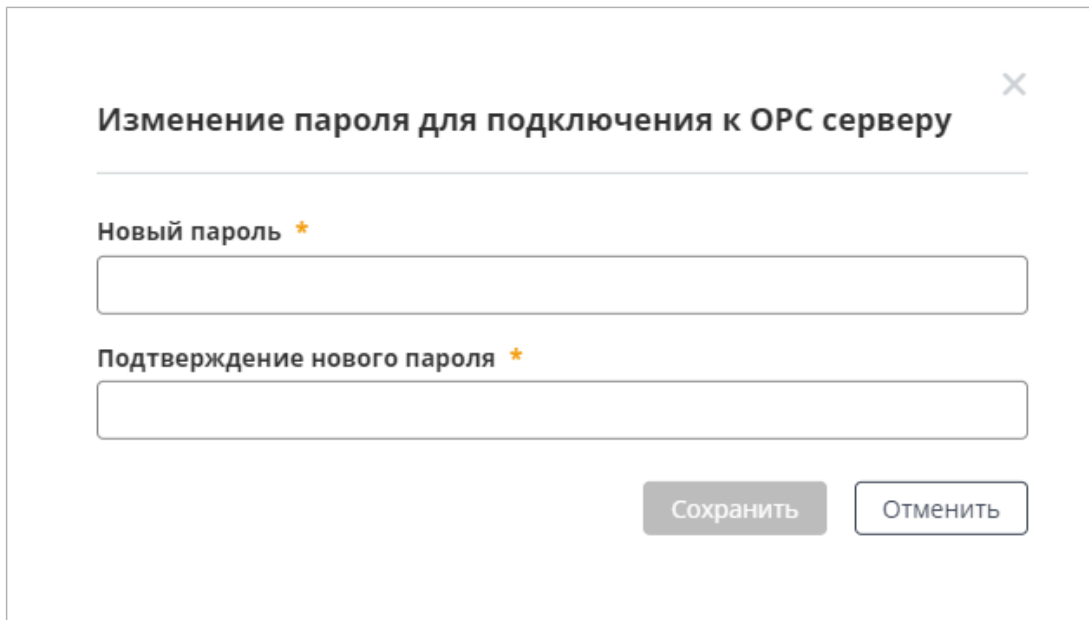
 Внимание:

В случае установки некорректных настроек при отправке тестового оповещения будет отображаться уведомление **Не удастся отправить тестовое оповещение: OPC-сервер недоступен, либо один или несколько параметров оповещения имеют некорректные значения**

6.7.6.2.2. Изменение пароля для подключения к OPC-серверу

У ранее созданного правила оповещения можно изменить пароль для подключения к OPC-серверу. Для этого:

1. Перейдите на страницу **Администрирование** → **События и инциденты** → **Оповещения об инцидентах**.
2. Нажмите кнопку  (**Редактировать оповещение**) в таблице оповещений.
3. В открывшемся окне **Редактирование оповещения** нажмите кнопку  **Изменить пароль**.
4. В открывшемся окне **Изменение пароля для подключения к OPC серверу** введите новый пароль в поля **Новый пароль** и **Подтверждение нового пароля** и нажмите кнопку **Сохранить**.



The image shows a dialog box titled "Изменение пароля для подключения к OPC серверу" (Change password for OPC server connection). It has a close button (X) in the top right corner. Below the title, there are two input fields: "Новый пароль *" (New password) and "Подтверждение нового пароля *" (Confirm new password). At the bottom right, there are two buttons: "Сохранить" (Save) and "Отменить" (Cancel).

Рис. 122. Окно «Изменение пароля для подключения к OPC серверу»

5. Нажмите кнопку **Сохранить** в окне **Редактирование оповещения**.

- **Результат шага:** изменения, внесенные в оповещение, будут перезаписаны.

6.8. Выгрузка отчетов по инцидентам

Для выгрузки отчета по инцидентам:

1. Перейдите на страницу **Инциденты**.
2. Установите чекбокс возле нужных инцидентов.
3. В открывшемся внизу меню нажмите **Отчет**.
 - **Результат шага:** Откроется окно **Создание отчета по инцидентам**.

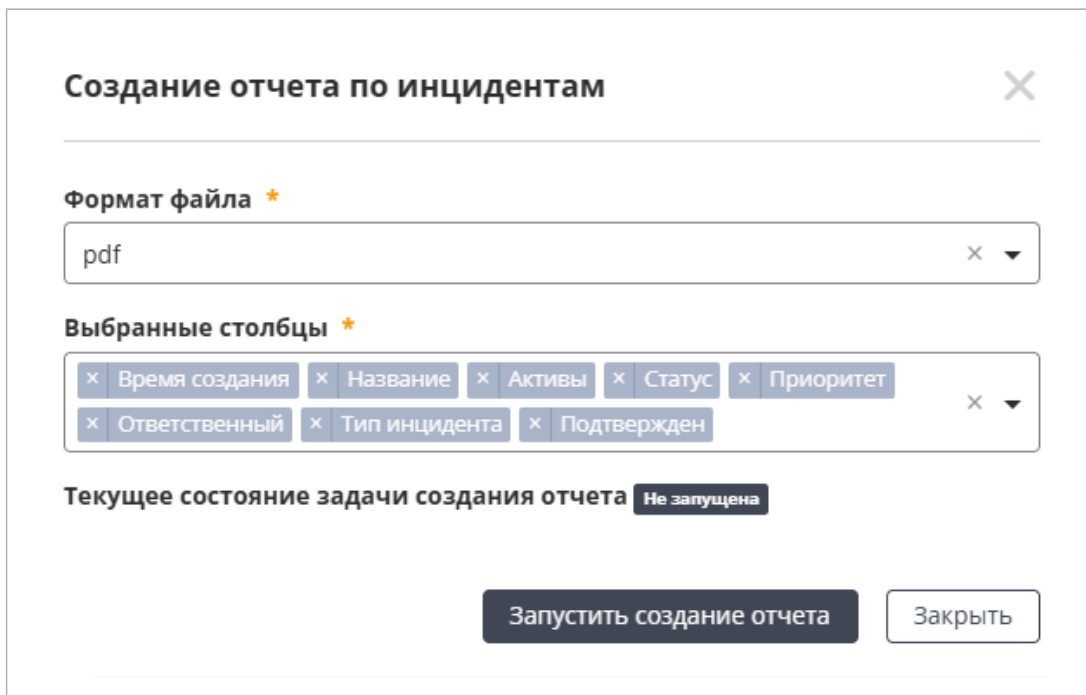


Рис. 123. Окно «Создание отчета по инцидентам»

4. Выберите формат файла отчета из выпадающего списка **Формат файла** — pdf или xlsx.
5. Выберите столбцы, которые будут отражены в отчете.

💡 Подсказка:

По умолчанию в окне создания отчета указаны те же столбцы, которые ранее были выбраны для отображения в таблице.

6. Нажмите **Запустить создание отчета**.
 - **Результат шага:** В правом верхнем углу появится всплывающее уведомление **Задача создания отчета запущена**
7. Для сохранения отчета нажмите на ссылку с названием файла.

7. Работа с активами

Актив — это сетевой узел, подлежащий защите от потенциальных угроз и неправомерных действий, таких как несанкционированный доступ и изменение данных третьими лицами.

На странице **Активы** → **Технические средства** отображается список всех найденных автоматически и добавленных пользователем активов. На странице присутствуют широкие возможности фильтрации и перехода к отдельным страницам различных аспектов активов (карточка актива, события, инциденты, учетные данные актива, конфигурации), кнопки экспорта, импорта, поиска уязвимостей, создания отчетов и удаления активов, столбцы статусов и статистики по сбору данных, отклонениям конфигураций, инцидентам, уязвимостям.

Актив	Наименование	Группа	Описание	Тип	IP-адрес интерфейса сб...	MAC-адрес интерфей...
☐	CISCO IOU		CISCO-IOU_TK1_DEVELOPE...	Маршрутизатор	10.51.244.22	00:50:56:b7:d8:74
☐	Manager		Хост на котором располож...	APM	10.51.244.3	00:50:56:b7:d8:78
☐	S7		PLC-S7_TK1	ПЛК	10.51.201.141	00:50:56:b7:1c:3a
☐	SE_CEI4		SE_CEI4_DEVELOPERS	ПЛК	10.51.202.28	00:50:56:b7:21:e1
☐	WIN7-SP10VMS		WIN7_SP1-OVMS_TK1_DEV...	APM	10.51.244.16	00:50:56:b7:36:25
☐	WIN10_TK2		DESKTOP-C326I3E	APM	10.51.202.19	00:50:56:9d:4e:ee
☐	Win2003SP2_TK1		Win2003_Server_SP2_TK1	Сервер	10.51.201.145	00:50:56:9d:00:41
☐	Win2KservSP4_TK1		Win2000_Server_SP4_TK1	Сервер	10.51.201.146	00:50:56:9d:2c:ed
☐	Win2KSP4_TK1		Win2000_SP4_TK1	APM	10.51.201.147	00:50:56:9d:51:a6
☒	WIN_7_Company		Win7-SP1 company local	APM	10.51.200.133	00:50:56:9d:25:49
☐	WinCC		WinCC_WS2008R2x64_TK1...	APM	10.51.244.26	00:50:56:b7:f6:8b

Рис. 124. Страница «Активы → Технические средства»

На основе данных из трафика Комплекс может автоматически определять следующие параметры активов:

- IP и MAC-адреса интерфейсов;
- производителя;
- тип актива;
- операционную систему и ее версию (для активов с типом **инженерное оборудование** — информацию о прошивке);
- по наличию трафика — доступность актива.

На странице доступно табличное представление списка активов с возможностью сортировки по столбцам. В таблице можно настроить отображение столбцов со статусами и статистикой по выполненным операциям активного сбора данных и по обнаруженным инцидентам и уязвимостям.



Подсказка:

Подробнее о статусах активов см. разделы [Статусы активов](#) и [Цветовая индикация активов](#).

☐	Актив	Наименование	Тип	Конфигурации	Сбор данных	Инциденты	Уязвимости	Результаты сканиро...	Интерфейсы
☐		CISCO IOU	Маршрутизатор					6/0/2	10.51.244.22 00:50:56:b7:d8:74
☐		CISCO-ASA_BRANCH	Маршрутизатор					1/0/1	10.51.201.9 00:50:56:9d:23:d8
☐		Manager	APM						10.51.203.37 00:50:56:b7:df:78
☐		S7	ПЛК					1	10.51.201.141 00:50:56:b7:1c:3a
☐		SE_CE14	ПЛК					4/0/4	10.51.202.28 00:50:56:b7:21:e1
☐		WIN-7SP10VMS	APM					10	10.51.244.16 00:50:56:b7:36:25

Рис. 125. Табличное представление активов

Обнаруженные или созданные вручную активы можно сгруппировать, чтобы потом использовать эти группы для сбора данных и управления.

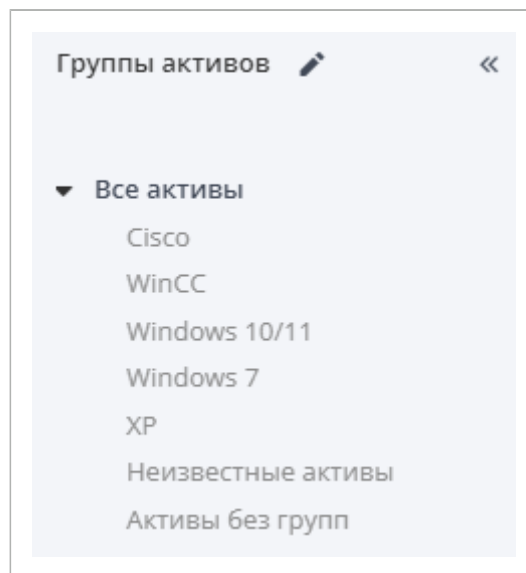


Рис. 126. Панель управления группами активов

Чтобы открыть карточку актива, нажмите на его значок или наименование. В карточке содержатся следующие сведения:

- характеристики актива: наименование, описание, производитель, тип, группа, ИС, дата и время создания, дата и время, когда актив последний раз был доступен;
- учетные данные;
- информация об ОС (для активов с типом **инженерное оборудование** — информация о прошивке): дату и время последнего изменения указанных данных, производителя, наименование и версию ОС;
- сетевые атрибуты: название, IP и MAC-адреса;
- набор присвоенных меток;
- статистику по задачам сбора данных, собранным конфигурациям, инцидентам и уязвимостям;
- связанные данные, позволяющие просмотреть данные об активе в других разделах:
 - инциденты;
 - конфигурации;
 - события;
 - потоки данных;
 - источники;
 - учетные данные актива;
 - перечень ПО, установленного на активе.

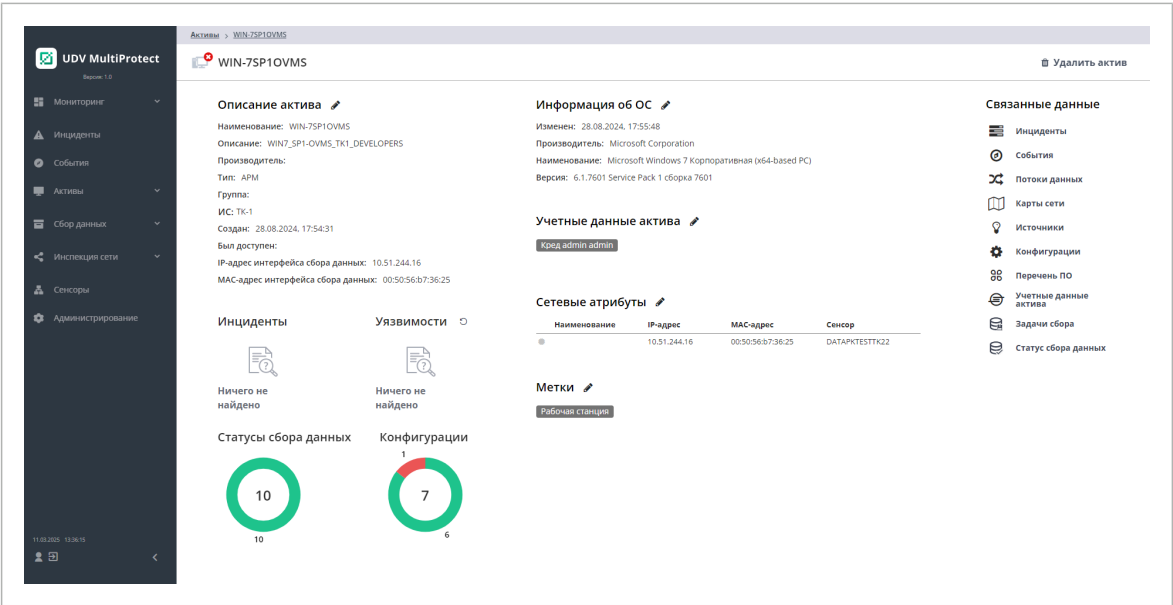


Рис. 127. Карточка актива

7.1. Экспорт и импорт активов и их групп

В этом разделе:

- Экспорт активов
- Экспорт групп активов
- Импорт активов
- Импорт групп активов

Экспорт и импорт активов доступен на странице **Активы** → **Технические средства** на панели **Управление**.

Экспорт и импорт групп активов доступен на странице **Администрирование** → **Основные настройки** → **Импорт и экспорт** на панели **Элементы иерархии**.

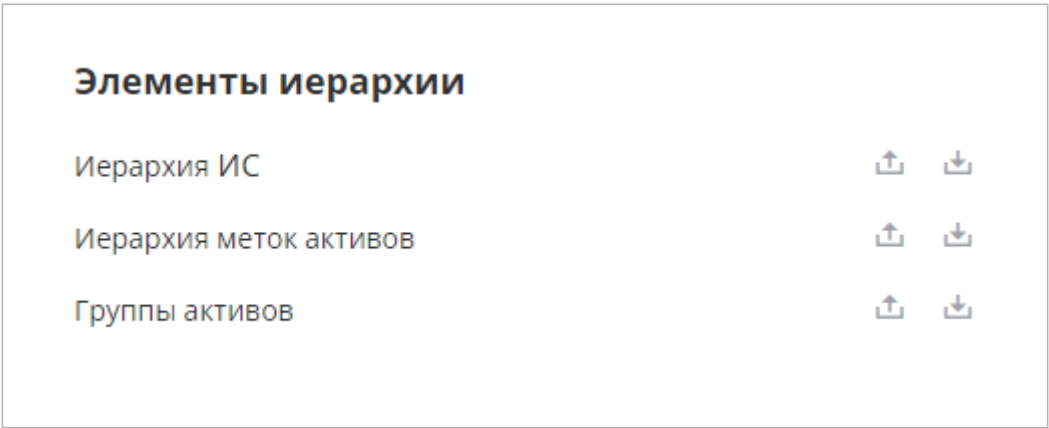


Рис. 128. Панель «Элементы иерархии» на странице «Импорт и экспорт»

7.1.1. Экспорт активов

Для экспорта всех активов в файл формата *.json:

1. Перейдите на страницу **Активы** → **Технические средства**.
2. Нажмите кнопку  (**Экспортировать активы**) на панели **Управление** в верхней части страницы.
 - **Результат шага:** Файл со списком активов, их групп, меток, ИС с названием `hosts_[дата_и_время].json` будет загружен на компьютер в директорию загрузки по умолчанию.



ОСТОРОЖНО:

В файл будут добавлены все активы, независимо от выбора и фильтрации активов.

7.1.2. Экспорт групп активов

Для экспорта справочника с иерархией групп активов в файл формата *.json:

1. Перейдите на страницу **Администрирование** → **Основные настройки** → **Импорт и экспорт**.
2. На панели **Элементы иерархии** в строке **Группы активов** нажмите кнопку  (**Экспортировать**) .
 - **Результат шага:** Файл со списком групп активов `asset_groups_[дата_и_время].json` будет сформирован и доступен для скачивания в правом верхнем углу страницы **Импорт и экспорт** под заголовком **Результат последнего экспорта**
3. Для скачивания файла нажмите на название сформированного файла под заголовком **Результат последнего экспорта**.
4. В открывшемся окне укажите расположение для экспортируемого файла, введите название файла и нажмите **Сохранить**.
 - **Результат шага:** Файл `asset_groups_[дата_и_время].json` будет загружен на компьютер.

7.1.3. Импорт активов

Для импорта активов из файла формата *.json в Комплекс:

1. Перейдите на страницу **Активы** → **Технические средства**.
2. Нажмите кнопку  (**Импортировать актив**) на панели **Управление** в верхней части страницы.
3. В открывшемся окне **Импорт активов** нажмите левой кнопкой мыши на область выбора файла или перетащите файл из проводника. В открывшемся окне укажите расположение импортируемого файла формата *.json и подтвердите выбор.

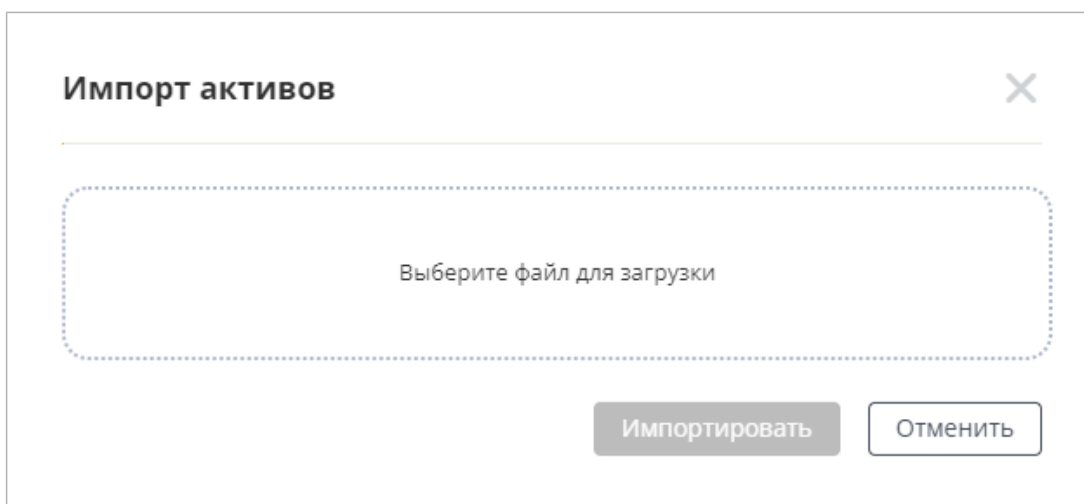


Рис. 129. Окно «Импорт активов»

4. Нажмите кнопку **Импортировать** для выполнения импорта списка активов.
5. Убедитесь, что активы успешно загрузились и отображаются на странице.

7.1.4. Импорт групп активов

Для импорта справочника с пользовательской иерархией групп активов из файла формата *.json в Комплекс:

1. Перейдите на страницу **Администрирование** → **Основные настройки** → **Импорт и экспорт**.
2. На панели **Элементы иерархии** в строке **Группы активов** нажмите кнопку  (**Импортировать**).
3. В открывшемся окне укажите расположение импортируемого файла формата *.json и подтвердите выбор.
 - **Результат шага:** Появится окно подтверждения импорта.
4. Нажмите **Импортировать**.

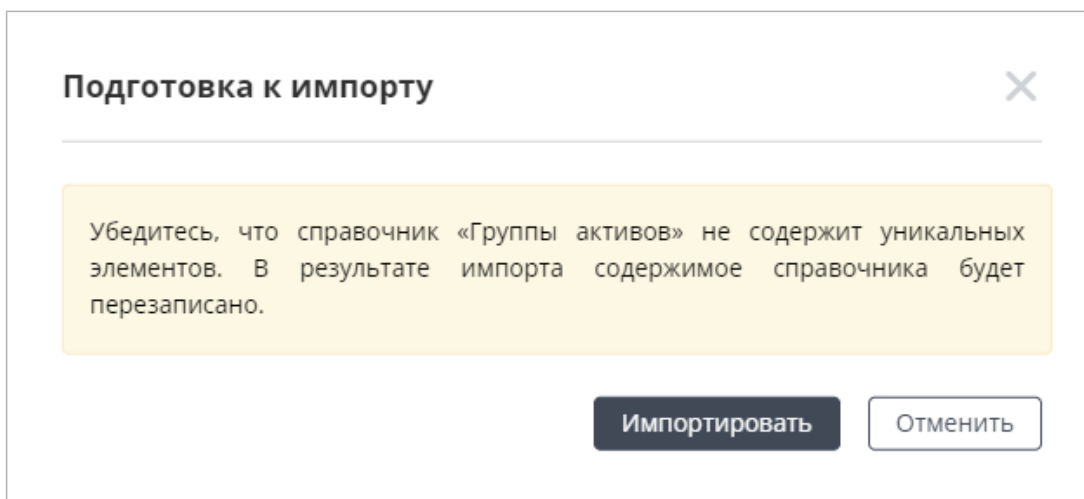


Рис. 130. Окно «Подготовка к импорту» при импорте групп активов

5. Убедитесь, что группы активов были успешно загружены.
 - **Результат шага:** После загрузки файла в правом верхнем углу страницы в поле **Результат последнего импорта** появится статус **Успешно**, и группы активов будут загружены на страницу **Активы** → **Технические средства**.
6. Перейдите на страницу **Активы** и убедитесь, что группы активов были успешно загружены.

7.2. Управление активами

В этом разделе:

- Кнопки управления активами
- Фильтрация списка активов

7.2.1. Кнопки управления активами

В верхней части страницы **Активы** расположен ряд кнопок для управления выбранными активами. В таблице ниже приведено описание этих элементов.

Табл. 90. Кнопки управления активами

КНОПКА	ДЕЙСТВИЕ	СТРАНИЦА	УСЛОВИЯ ДОСТУПНОСТИ
Создать актив	Создание актива	Создание актива	—
	Удаление выбранных активов	Удаление активов	Кнопки доступны, если выбран хотя бы один актив
	Создание отчета по выбранным активам	Выгрузка отчетов	
	Поиск уязвимостей в базе CVE для выбранных активов	Запуск поиска уязвимостей в базах CVE, CPE и БДУ ФСТЭК России	
	Экспорт активов	Экспорт активов	Выполняется для всех активов независимо от того, какие активы были выбраны или отфильтрованы
	Импорт активов	Импорт активов	—



Рис. 131. Кнопки управления активами

При выборе с помощью чекбокса ☒ одного актива появляется панель с подробной информацией об активе. Кнопки перехода на смежные страницы доступны на соседней вкладке **Связанные данные**.

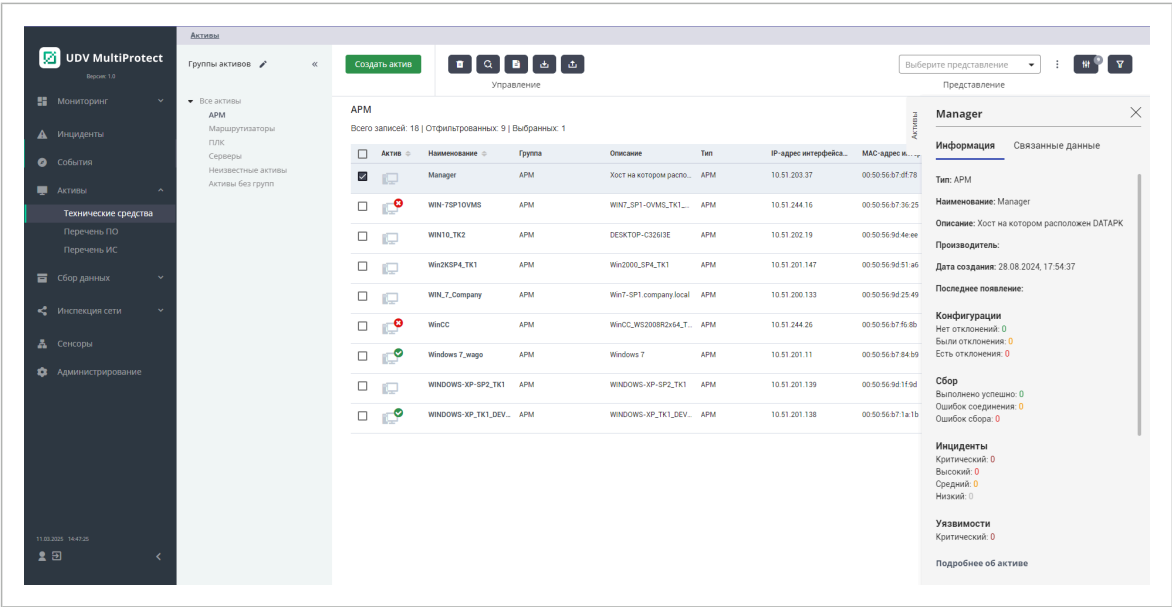


Рис. 132. Панель с подробной информацией о выбранном активе

При выборе нескольких активов с помощью чекбоксов ☒ появляется панель с кнопками для просмотра содержания смежных страниц с использованием фильтров по активам.

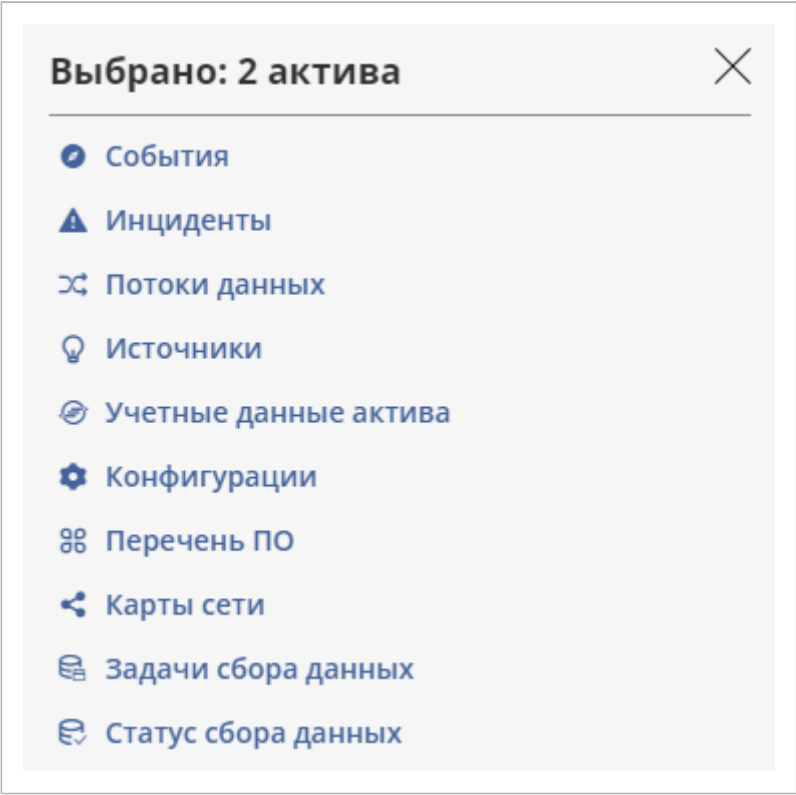


Рис. 133. Кнопки перехода на смежные страницы



Внимание:

Для кнопок перехода на страницы предусмотрен лимит, равный 20 активам. Это значит, что для большего количества активов использование кнопок перехода на страницы недоступно.

7.2.2. Фильтрация списка активов

Список активов на странице **Активы** можно фильтровать. Нажмите , чтобы выбрать из следующих доступных фильтров:

1. **Типы активов.** Фильтрация выполняется по типам, назначенным активам. Можно выбирать несколько типов активов.
2. **Производители.** Фильтрация выполняется по наименованиям производителей аппаратного обеспечения актива, информация о которых получена Комплексом. Можно выбирать несколько наименований.
3. **Активы.** Фильтрация выполняется по наименованиям обнаруженных активов. Можно выбирать несколько наименований.
4. **Статус проблемности.** Статусы **Сбор данных** и **Конфигурации** формируют единый показатель актива **Статус проблемности**. Проблемность для каждого актива принимает одно из следующих значений:
 - **Критический:** хотя бы один из статусов актива — **Сбор данных** или **Конфигурации** — имеет красный индикатор.
 - **Важный:** хотя бы один из статусов актива — **Сбор данных** или **Конфигурации** — имеет оранжевый индикатор, но красные индикаторы отсутствуют.
 - **ОК:** оба статуса имеют зеленый индикатор.
 - **Нет данных:** сбор данных не выполнялся.



Подсказка:

Подробнее о статусах **Сбор данных** и **Конфигурации** см. раздел [Статусы активов](#).

Фильтрация выполняется по указанным выше значениям. Можно выбирать несколько значений.

5. **ИС.** Фильтрация выполняется по наименованиям классификаторов ИС, назначенным активам. В раскрывающемся списке можно выбирать несколько классификаторов с помощью чекбоксов. Поле для ввода текста предназначено для поиска классификаторов в раскрывающемся списке.
6. **IP-адреса.** Фильтрация выполняется по IP-адресам, привязанным к сетевым атрибутам активов. Для выбора нескольких IP-адресов:
 - a. Полностью введите IP-адрес в поле.



Внимание:

В поля IP-адресов допускается копирование из других источников списков IP-адресов, их диапазонов или подсетей. Элементы в исходном списке должны разделяться с помощью: „ „, „ „, **Tab**, **Enter**, **Space**. Подсети задаются в формате CIDR.

- b. Нажмите **Добавить** в строке ниже для подтверждения выбора.
 - c. Повторите пункты **6.a-6.b** для других IP-адресов, по которым необходимо отфильтровать активы.
7. **MAC-адреса.** Фильтрация выполняется по ключевому слову среди MAC-адресов, привязанных к сетевым атрибутам активов. Для ввода в поле разрешены цифры и английские символы.

**Внимание:**

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

8. **Метки.** Фильтрация выполняется по меткам, назначенным активам. В раскрывающемся списке можно выбирать несколько меток с помощью чекбоксов. Поле для ввода текста предназначено для поиска меток в раскрывающемся списке.

Рис. 134. Результаты поиска среди значений фильтра «Метки»

9. **Производитель ОС.** Фильтрация выполняется по ключевому слову среди наименований производителей ОС или прошивок, информация о которых получена Комплексом.
10. **ОС.** Фильтрация выполняется по ключевому слову среди наименований ОС или прошивок, информация о которых получена Комплексом.
11. **Версия ОС.** Фильтрация выполняется по ключевому слову среди версий ОС или прошивок, информация о которых получена Комплексом.
12. **Сенсор.** Фильтр содержит наименования сенсоров, подключенных к Комплексу. Можно выбирать несколько наименований. При применении фильтра отобразятся активы, чьи интерфейсы сбора данных привязаны к выбранным сенсорам.

**Внимание:**

Фильтрация может повлиять на доступность кнопки  (**Групповое удаление**). Она деактивируется при следующих условиях:

- применен хотя бы один из фильтров: **Статус проблемности, Производитель ОС, ОС, Версия ОС;**
- по результатам фильтрации получилось больше 100 записей;
- применено действие **Выбрать все записи (>100) в данной таблице.**

7.3. Создание актива

Новые активы в Комплексе можно создавать в ручном режиме. Для этого:

1. Перейдите на страницу **Активы**.
2. Нажмите **Создать актив**.
3. В открывшемся окне **Создание актива** задайте параметры для нового актива в следующем порядке:
 - а. Выберите тип актива.



Подсказка:

При выборе любого типа актива, кроме **Неизвестный тип** и **Комплекс**, для редактирования станет доступным поле **Наименование**.

- б. Введите наименование в зависимости от выбранного типа актива:
 - при выборе типа **Сенсор** выберите из выпадающего списка наименование сенсора, подключенного к текущему Комплексу;
 - при выборе типа **Комплекс** наименование актива будет присвоено автоматически;
 - в остальных случаях введите наименование актива вручную.
- в. При необходимости введите описание, выберите ИС и укажите группу.
- г. При необходимости введите наименование производителя.



Внимание:

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

Создание актива ✕

Тип *

APM ▾

Наименование *

ARM_WUN

Описание

PM оператора

Производитель

определить

ИС

Введите текст для поиска

▾ ИС

Группа

at ▾

Создать

Отменить

Рис. 135. Окно создания нового актива

4. Нажмите **Создать**.

7.4. Группировка активов

В этом разделе:

- [Создание группы активов](#)
- [Добавление активов в группу](#)
- [Управление группами активов](#)

Активы с типом, отличным от **неизвестного**, можно собирать в группы. Эти группы используются в задачах сбора данных и для упрощения управления активами.

По умолчанию доступны следующие группы:

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

Эти группы нельзя удалять и редактировать, в том числе вручную менять их состав.

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

7.4.1. Создание группы активов

Для создания группы активов:

1. Перейдите на страницу **Активы**.

 Подсказка:

Управление группами активов также доступно на странице [Задачи сбора](#).

2. Над панелью с группами активов в левой части страницы нажмите  (**Редактировать**).
 - **Результат шага:** Появится окно **Редактирование групп активов**.
3. Нажмите кнопку  напротив группы, которая будет вышестоящей для создаваемой.

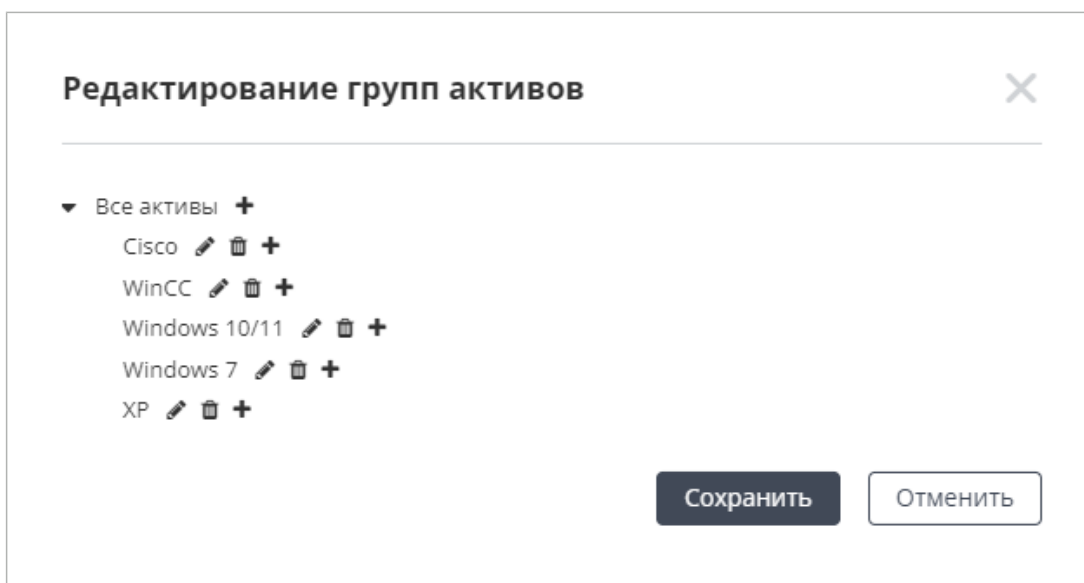


Рис. 136. Окно «Редактирование групп активов»

► **Результат шага:** Появится окно **Создание группы активов**.

4. В окне создания задайте наименование и описание новой группы. При необходимости выберите другую вышестоящую группу.

Рис. 137. Окно «Создание группы активов»

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

Внимание:

Без сохранения в окне редактирования групп изменения не будут отражены в Комплексе.

► **Результат шага:** Созданная группа появится в списке в окне **Редактирование групп активов**.

6. При необходимости добавляйте другие группы активов.
 7. В окне **Редактирование групп активов** нажмите **Сохранить**.

► **Результат шага:** Появится предупреждение о неизменности задач сбора данных в результате изменения состава групп.

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

► **Результат шага:** Изменения будут сохранены, окно редактирования групп будет закрыто, появится уведомление **Список "Группы активов" успешно обновлен**.

7.4.2. Добавление активов в группу



Внимание:

Актив может находиться только в одной группе.

Для добавления активов в ранее созданную группу активов:

1. Перейдите на страницу **Активы**.

2. При необходимости отфильтруйте список активов: нажмите , выберите настройки фильтрации и нажмите **Применить**.

3. Убедитесь, что активам, которые будут добавлены в группу, назначен тип, отличный от **неизвестного**.

4. Добавьте активы в группу. Для этого:

- а. Отметьте **все** отфильтрованные активы с помощью чекбокса в заголовке таблицы либо отметьте с помощью чекбоксов **отдельные** активы, которые необходимо добавить в группу.



Подсказка:

Для выделения множества строк выше или ниже выбранной нажмите клавишу **Shift** и выделите строку с последним активом, который необходимо добавить в группу.

б. Наведите курсор на один из выделенных активов и зажмите левую кнопку мыши.

► **Результат шага:** Появится полупрозрачный квадрат с количеством выделенных активов.

в. Не отпуская левую кнопку мыши, перетащите активы в левую часть страницы так, чтобы курсор оказался на наименовании группы, в которую будут перемещены активы.

г. Отпустите левую кнопку мыши.

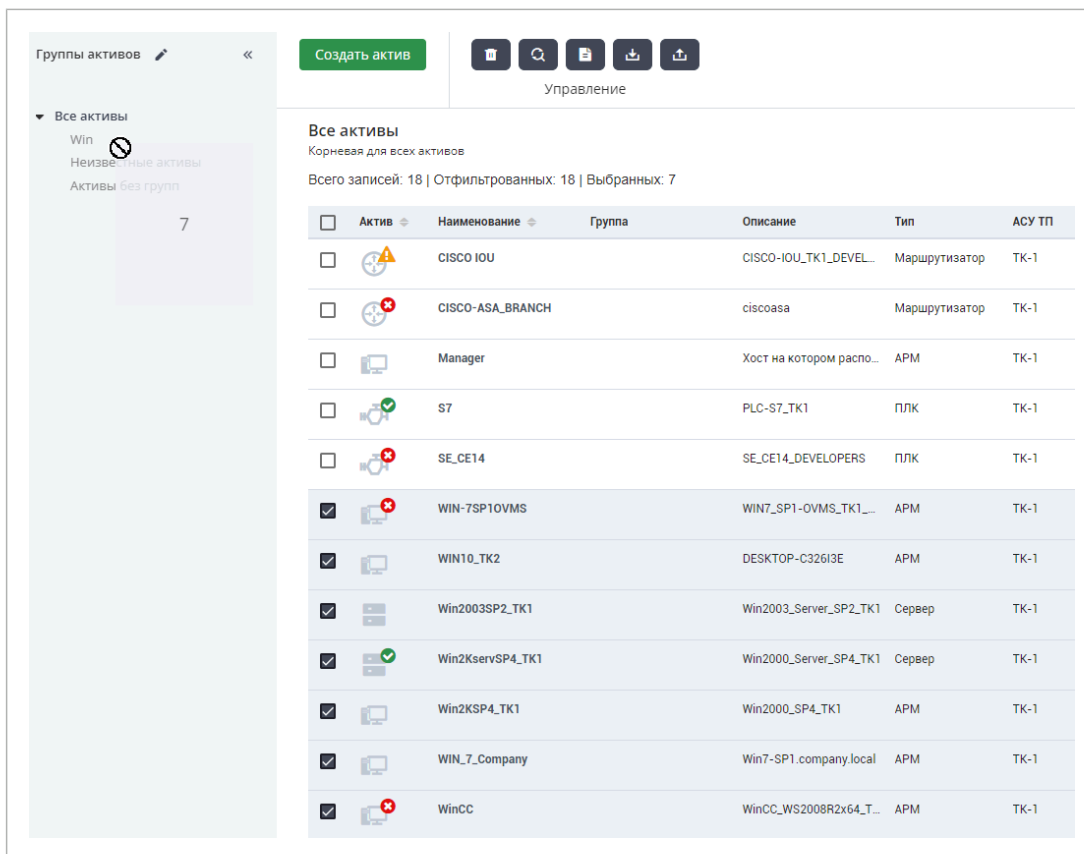


Рис. 138. Добавление активов в группу

- **Результат шага:** Появится окно подтверждения добавления активов в группу.

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

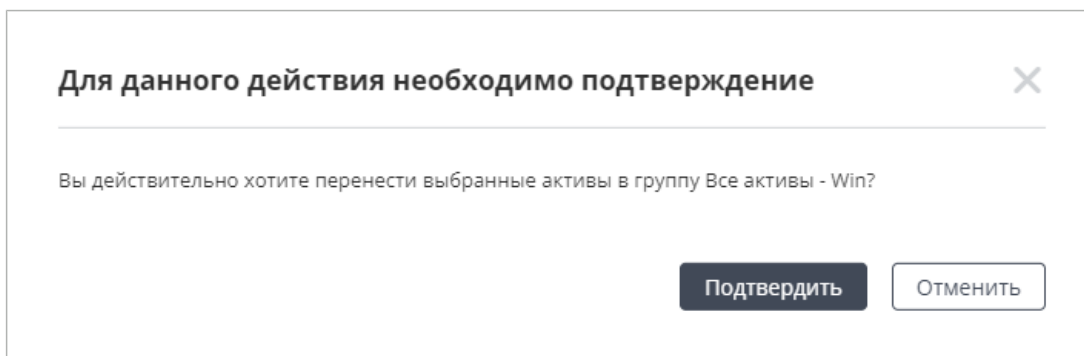


Рис. 139. Окно подтверждения перемещения актива

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

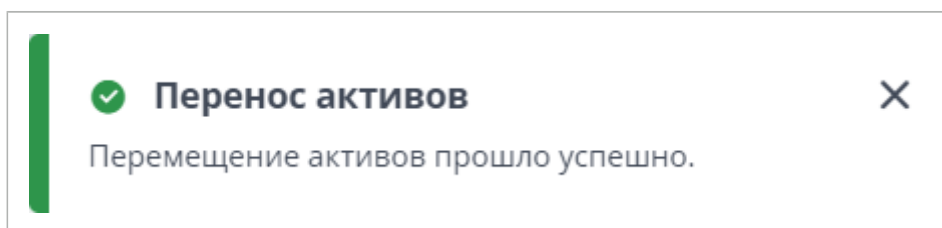


Рис. 140. Уведомление «Перемещение актива прошло успешно»

6. При необходимости изменить группу можно также в карточке актива. Для этого:

- а. Откройте карточку актива.
- б. Нажмите  (**Редактировать**) напротив подзаголовка **Описание актива**.
 - **Результат шага:** Появится окно **Основная информация об активе**.
- в. Измените значение поля **Группа**.
- г. Нажмите **Сохранить**.
 - **Результат шага:** Группа актива будет изменена.

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

7.4.3. Управление группами активов

Управлять группами активов можно на страницах **Активы** и **Задачи сбора**. В решении предусмотрены следующие возможности для управления группами активов:

1. Изменение группы. Для изменения:
 - а. Над панелью с группами активов в левой части страницы нажмите кнопку  (**Редактировать**).
 - **Результат шага:** Появится окно **Редактирование групп активов**.
 - б. Нажмите кнопку  (**Редактировать**) напротив группы, которую необходимо изменить.

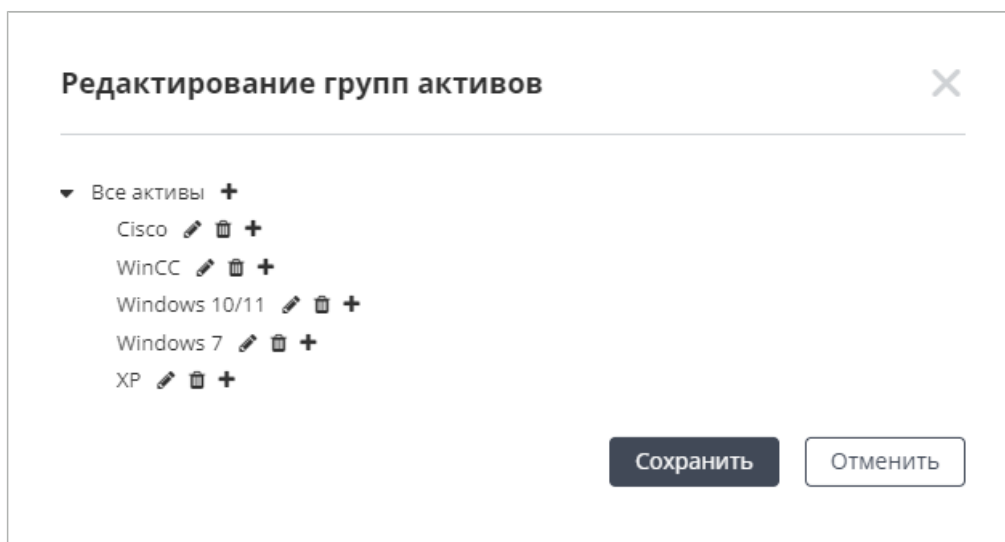
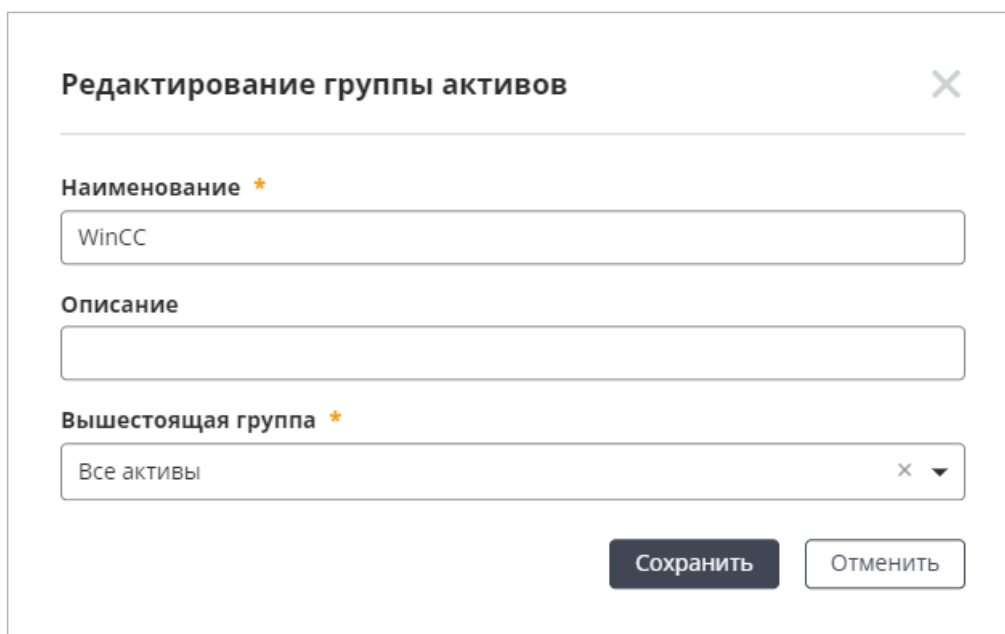


Рис. 141. Окно «Редактирование групп активов»

- **Результат шага:** появится окно **Редактирование группы активов**.
- в. Измените необходимые параметры группы активов.



Редактирование группы активов ✕

Наименование *

Описание

Вышестоящая группа *

 ✕ ▾

Рис. 142. Окно «Редактирование группы активов»

г. Нажмите **Сохранить** для подтверждения локальных изменений.

 **Внимание:**

Без сохранения изменения в окне редактирования групп не будут отражены в Комплексе.

► **Результат шага:** Изменения названия группы появятся в окне **Редактирование групп активов**.

д. При необходимости измените другие группы активов.

е. В окне **Редактирование групп активов** нажмите **Сохранить**.

► **Результат шага:** Появится предупреждение о неизменности задач сбора данных в результате изменения состава групп.

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

► **Результат шага:** Изменения будут сохранены, окно редактирования групп будет закрыто, появится уведомление **Список "Группы активов" успешно обновлен**.

2. Удаление группы. Для удаления:

а. Над панелью с группами активов в левой части страницы нажмите кнопку  (**Редактировать**).

► **Результат шага:** Появится окно **Редактирование групп активов**.

б. Нажмите кнопку  (**Удалить**) напротив группы, которую необходимо удалить.

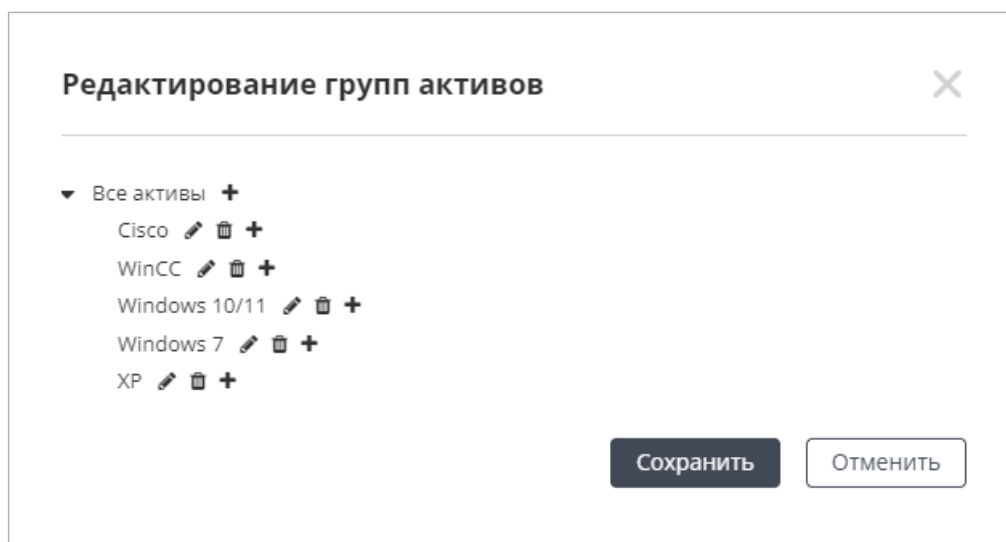


Рис. 143. Окно «Редактирование групп активов»

► **Результат шага:** Группа активов будет удалена, но данные изменения не будут сохранены до нажатия **Сохранить** в окне редактирования групп активов.

в. При необходимости измените другие группы активов.

г. В окне **Редактирование групп** Актив нажмите **Сохранить**.

► **Результат шага:** Появится предупреждение о неизменности задач сбора данных в результате изменения состава групп. Это значит, что удаляемые группы останутся в задачах сбора данных, если такие были созданы. Для возобновления периодического сбора измените или создайте задачи заново, в том числе с помощью копирования.

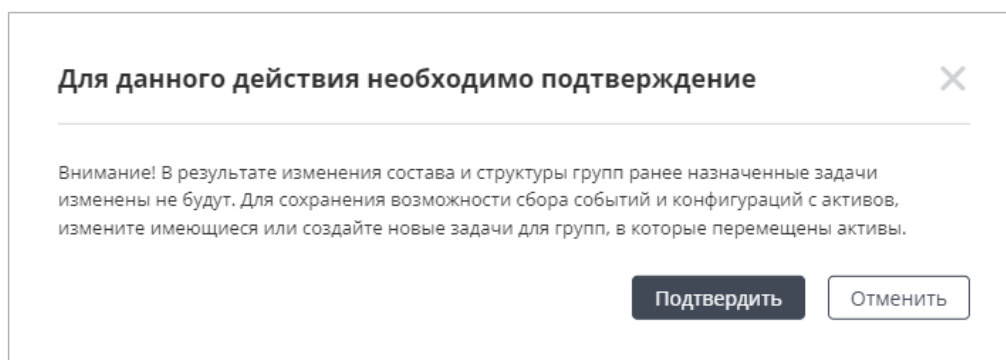


Рис. 144. Окно подтверждения изменений групп

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

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

7.5. Редактирование активов

Для изменения актива:

1. Перейдите на страницу **Активы**.
2. Нажмите на значок или наименование актива.

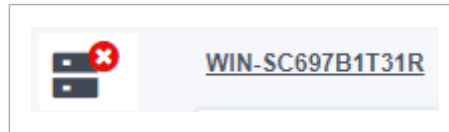


Рис. 145. Переход к карточке актива

► **Результат шага:** Откроется карточка актива.

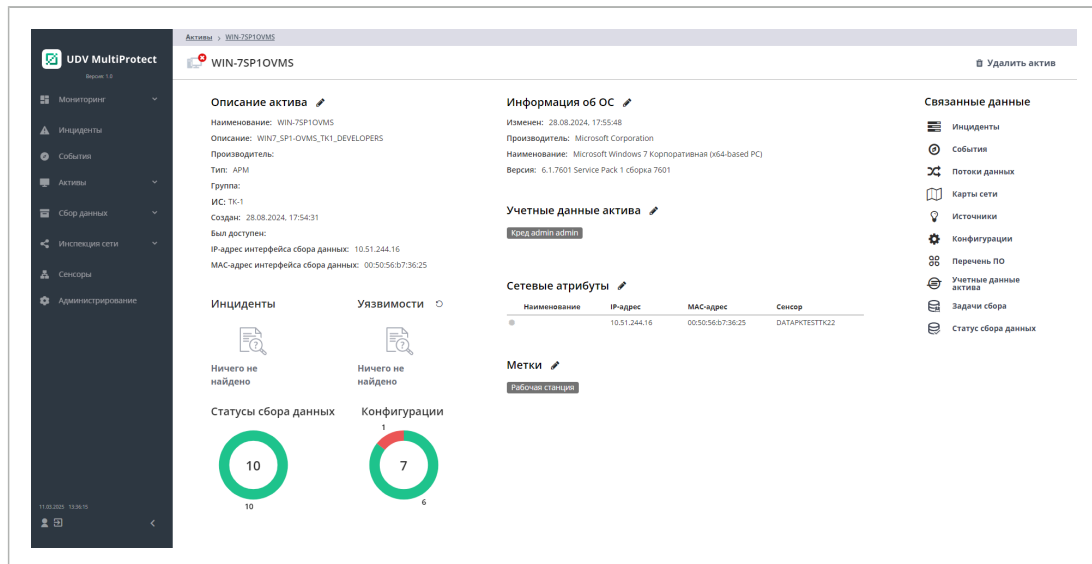


Рис. 146. Карточка актива

3. Убедитесь в доступности актива для Комплекса. Для этого между активом и прослушивающими интерфейсами Комплекса должен быть сетевой трафик.



Подсказка:

Если актив доступен, его индикатор будет иметь темно-синий цвет. Подробнее об индикации активов см. в разделе [Цветовая индикация и виды уведомлений](#).

Описание актива

Наименование: WIN10_TK2

Описание: DESKTOP-C326I3E

Производитель:

Тип: АРМ

Группа:

ИС: ТК-1

Создан: 28.08.2024, 17:54:30

Был доступен:

IP-адрес интерфейса сбора данных: 10.51.202.19

MAC-адрес интерфейса сбора данных: 00:50:56:9d:4e:ee

Рис. 147. Содержание полей блока «Описание актива»

4. Для редактирования общей информации об активе:

а. Нажмите кнопку  (**Редактировать**) напротив блока **Описание актива**.

► **Результат шага:** Откроется окно **Основная информация об активе**.

б. Измените необходимые параметры актива:

- тип и наименование актива;


Внимание:

Повторное присвоение активу типа **Неизвестный тип** будет запрещено, если ранее он был сохранен с другим типом.

Если активу назначен новый тип **Сенсор**, в качестве нового наименования необходимо выбрать из выпадающего списка сенсор, подключенный к текущему Комплексу.

Если активу назначен новый тип **Комплекс**, ему автоматически будет присвоено наименование текущего Комплекса.

При изменении типа актива на **Инженерное оборудование** или обратно необходимо обновить информацию в блоке **Информация об ОС**. Для этого выполните шаг 6 после редактирования общей информации.

- описание;
- ИС;
- группу;

- наименование производителя.



Подсказка:

Если активу назначен интерфейс для сбора данных, возможно автоматическое распознавание производителя на основе первых трех октетов его MAC-адреса. Для этого нажмите кнопку **определить** под полем **Производитель**.

Основная информация об объекте защиты

Тип*

Сервер

Наименование*

WIN-SC697B1T31R

Описание

WINCC

Производитель

VMware

определить

ИС

Введите текст для поиска

▼ ИС

Группа

Не выбрано

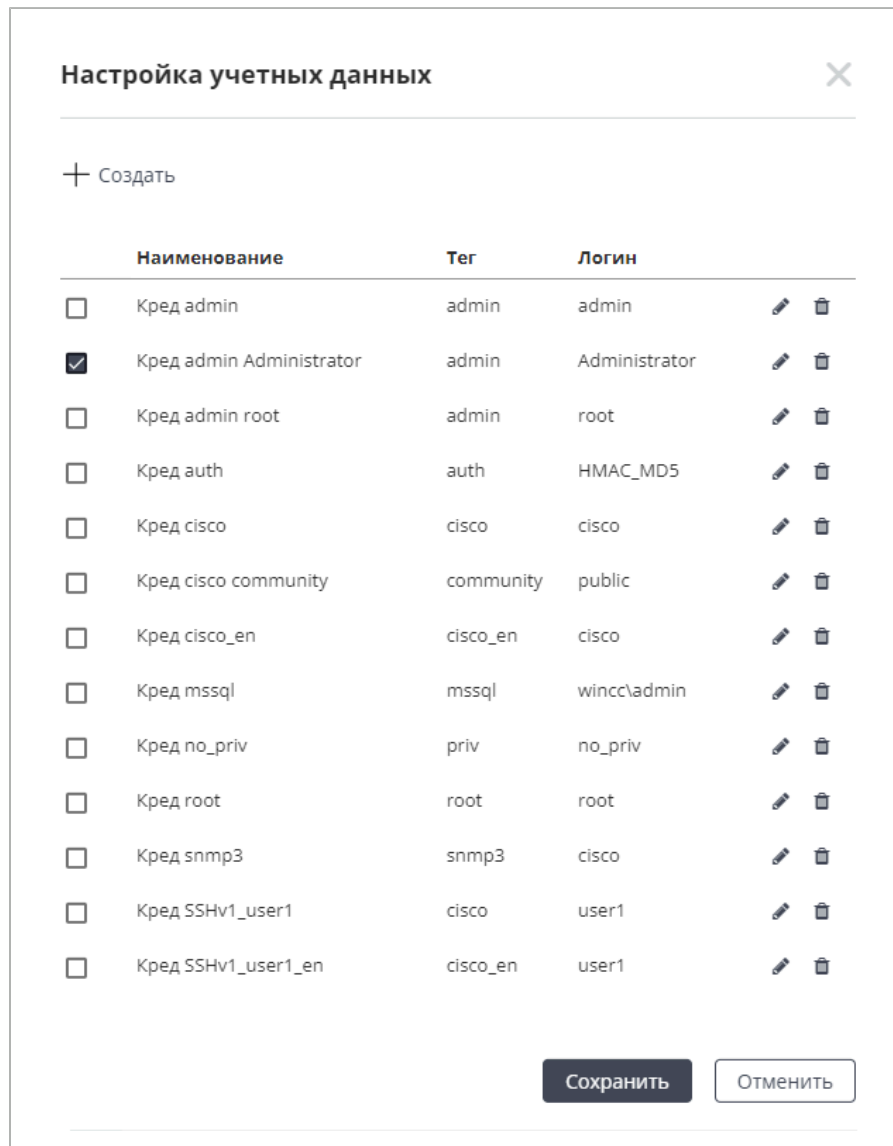
Сохранить

Отменить

Рис. 148. Окно «Основная информация об активе»

5. Для изменения учетных данных актива:

- а. Нажмите кнопку  напротив блока **Учетные данные актива**.
- б. Установите чекбокс рядом с добавленной ранее учетной записью для привилегированного доступа к активу и нажмите кнопку **Сохранить**.



Настройка учетных данных

+ Создать

	Наименование	Тер	Логин		
☐	Кред admin	admin	admin		
☒	Кред admin Administrator	admin	Administrator		
☐	Кред admin root	admin	root		
☐	Кред auth	auth	HMAC_MD5		
☐	Кред cisco	cisco	cisco		
☐	Кред cisco community	community	public		
☐	Кред cisco_en	cisco_en	cisco		
☐	Кред mssql	mssql	wincc\admin		
☐	Кред no_priv	priv	no_priv		
☐	Кред root	root	root		
☐	Кред snmp3	snmp3	cisco		
☐	Кред SSHv1_user1	cisco	user1		
☐	Кред SSHv1_user1_en	cisco_en	user1		

Сохранить **Отменить**

Рис. 149. Окно «Настройка учетных данных»

6. Для изменения информации об ОС актива:
 - а. Нажмите кнопку  напротив блока **Информация об ОС**.
 - **Результат шага:** появится окно **Редактирование информации об ОС**.
 - б. Измените данные операционной системы актива:
 - производителя;
 - название;
 - версию.



Внимание:

Тип информации, сохраняемой в блоке **Информация об ОС**, зависит от настроенного типа актива: для активов с типом **ПЛК** собирается и сохраняется информация о прошивке, для остальных активов — информация об операционной системе.

При изменении типа актива на **Инженерное оборудование** или обратно необходимо обновить информацию в блоке **Информация об ОС**.

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

Рис. 150. Окно «Редактирование информации об ОС»

► **Результат шага:** Появится надпись **Автообновление заблокировано**.

г. Нажмите кнопку **Сохранить**.

7. Для настройки сетевых атрибутов актива:

Внимание:

Настройка сетевых атрибутов актива возможна только для активов с типом, отличным от **Неизвестного**.

а. Нажмите кнопку напротив блока **Сетевые атрибуты**.

► **Результат шага:** появится окно **Редактирование сетевых атрибутов актива**.

б. В открывшемся окне сетевых атрибутов измените следующие параметры:

- название сетевого интерфейса;
- IP-адрес сетевого интерфейса;
- MAC-адрес сетевого интерфейса;

Внимание:

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

- выберите из списка сенсор, в чью домашнюю сеть входит новый IP-адрес.

**Подсказка:**

Если ранее было проведено сканирование домашней сети, можно привязать интерфейсы неизвестного актива. Для этого:

- Отметьте параметр **Выбрать сетевой атрибут неизвестного актива**.
- В выпадающем списке выберите интерфейс неизвестного актива.

в. При необходимости установите чекбокс **Интерфейс для сбора данных** напротив интерфейса.

**Внимание:**

У актива всегда должен быть интерфейс сбора данных — при попытке сохранения сетевых атрибутов актива при условии, что ни один атрибут не выбран в качестве интерфейса сбора, появится предупреждение: **Ошибка! Не выбран интерфейс сбора данных. Установите чекбокс напротив сетевых атрибутов для их выбора в качестве интерфейса сбора данных.**

Только один сетевой атрибут актива может быть выбран в качестве интерфейса сбора данных.

г. Нажмите  (**Создать сетевой атрибут**) для подтверждения изменений.

Редактирование сетевых атрибутов объекта защиты

Наименование	IP-адрес	MAC-адрес	Сенсор	
☒	10.51.201.11	00:50:56:b7:84:b9	datapk-vm-develop-1...	✓ ✕ 🔍 🗑️
☐ with_router_mac	10.51.201.11	00:50:56:B7:B1:3A	datapk-vm-develop-1...	✓ ✕ 🔍 🗑️
☐	_____	_____	Выберите сенсор	+ ✕ 🔍 🗑️

☐ Выбрать сетевой атрибут неизвестного объекта защиты

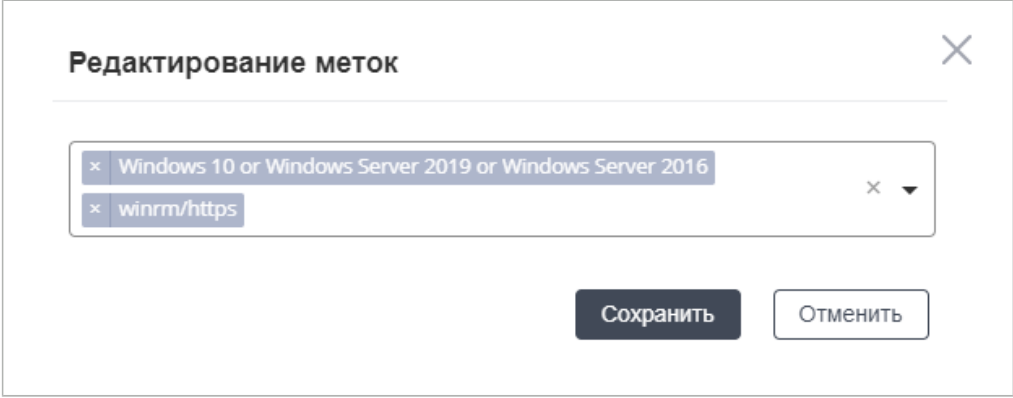
Рис. 151. Окно «Редактирование сетевых атрибутов актива»

8. Для изменения списка меток, к которым относится редактируемый актив:

а. Нажмите кнопку  напротив блока **Метки**.

► **Результат шага:** Откроется окно **Редактирование меток**.

- б. Измените состав присвоенных активу меток и нажмите **Сохранить**.



Редактирование меток

- × Windows 10 or Windows Server 2019 or Windows Server 2016
- × winrm/https

Сохранить Отменить

Рис. 152. Окно «Редактирование меток»

7.6. Удаление активов



ОСТОРОЖНО:

При удалении одного или нескольких активов из Комплекса будут удалены все связанные с ними данные: конфигурации, потоки, данные об операционной системе и программном обеспечении, информация о найденных уязвимостях.

7.6.1. Удаление актива

Для удаления актива:

1. Перейдите на страницу **Активы**.
2. Нажмите на значок или наименование актива.
► **Результат шага:** Откроется **Карточка актива**.
3. Нажмите кнопку  **Удалить актив** в правом верхнем углу.

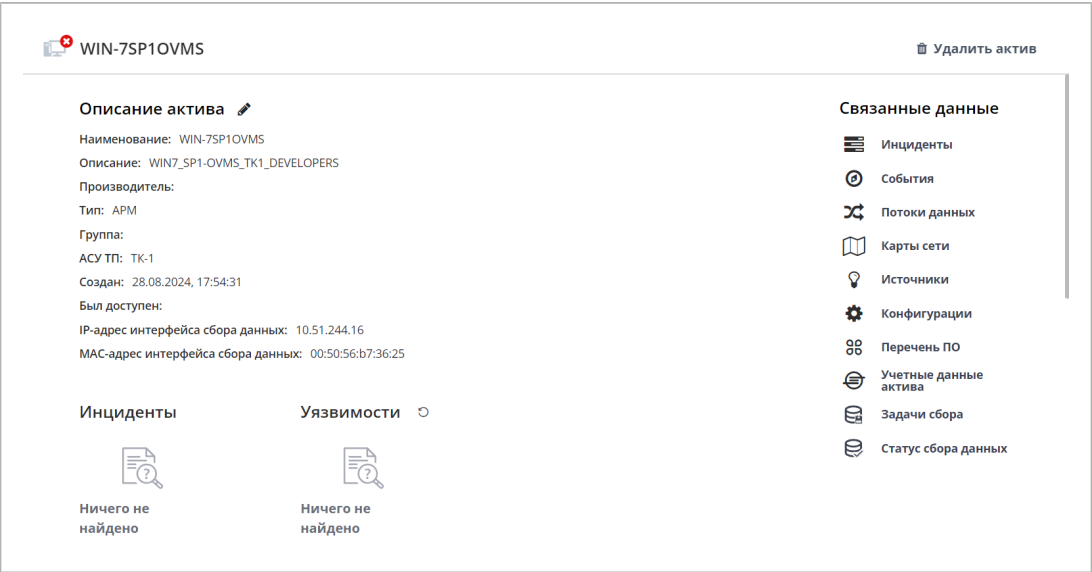


Рис. 153. Кнопка «Удалить актив» в карточке актива

4. В открывшемся окне введите обоснование действия и нажмите **Подтвердить**.

Для данного действия необходимо обоснование

Вместе с объектом защиты будут удалены связанные потоки и конфигурации. Вы действительно хотите удалить объект защиты?

Введите текст обоснования

Подтвердить

Отменить

Рис. 154. Окно обоснования удаления актива

► **Результат шага:** Актив будет удален. Откроется страница **Активы**.

7.6.2. Групповое удаление активов

Для удаления нескольких активов:

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

Внимание:

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

- в. Отметьте все отфильтрованные активы на удаление с помощью чекбокса в заголовке таблицы или отметьте отдельные активы с помощью чекбоксов рядом с активами. Для выбора всех активов в таблице нажмите **Выбрать все записи в данной таблице**.

3. На панели **Управление** нажмите кнопку  (**Групповое удаление**).

437

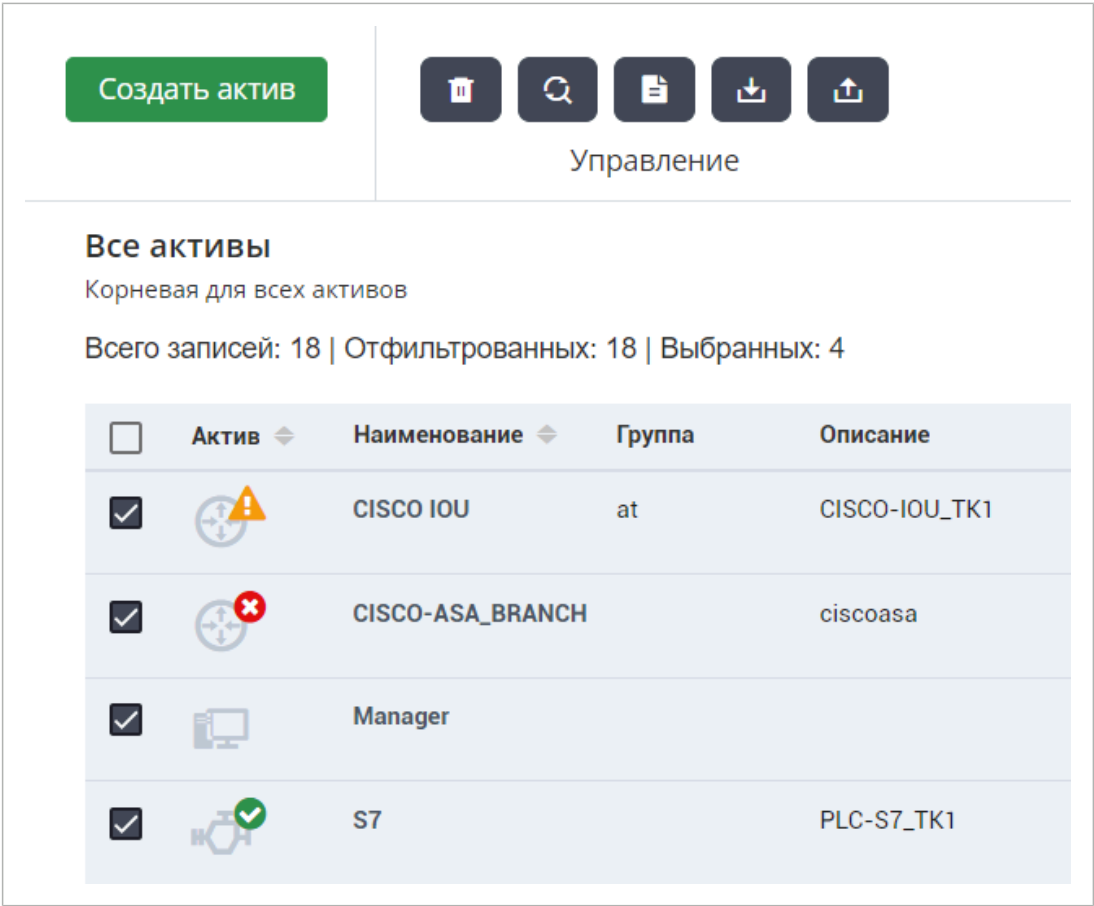


Рис. 155. Кнопка «Групповое удаление» на панели управления активами

Внимание:

(Групповое удаление) недоступна, если после применения действия **Выбрать все записи в данной таблице** выбрано более 100 активов.

4. В открывшемся окне введите обоснование действия и нажмите **Подтвердить**.
- **Результат шага:** Появится всплывающее уведомление об успешном удалении: **Удаление активов запущено**.

7.7. Выгрузка отчетов по активам

Для выгрузки отчета по активам:

1. Перейдите на страницу **Активы**.
2. Установите чекбокс возле нужных активов.
3. Нажмите кнопку **Создать отчет** () над списком активов.
 - **Результат шага:** Откроется окно **Создание отчета**.

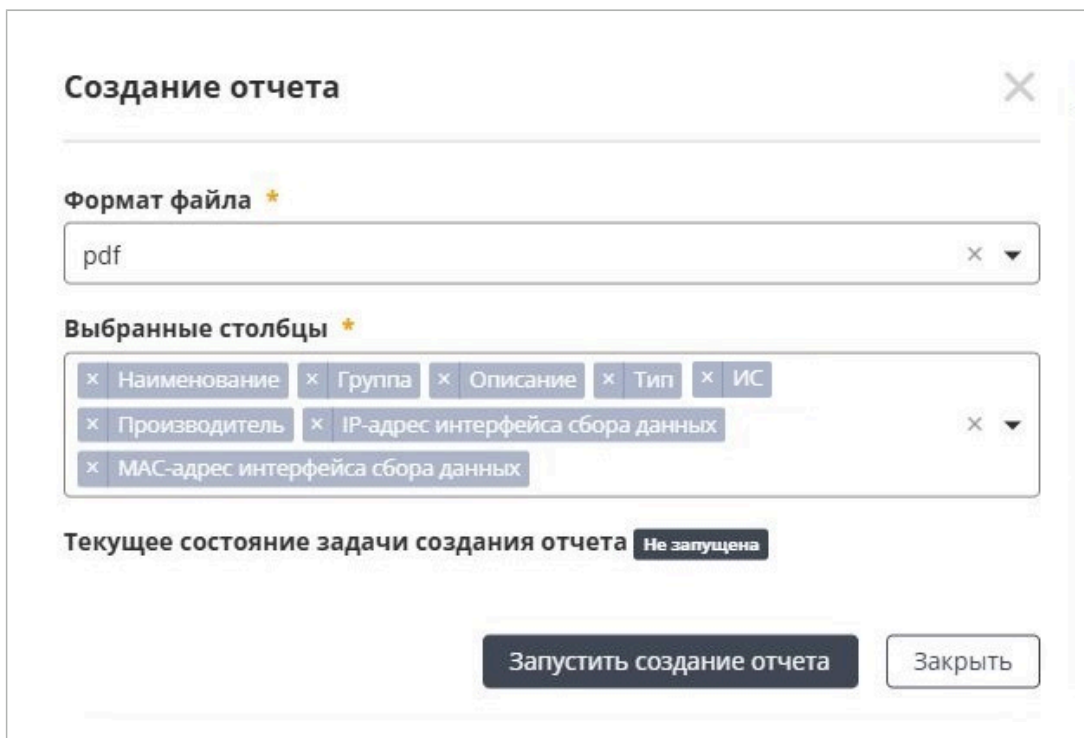


Рис. 156. Окно «Создание отчета»

4. Выберите формат файла отчета из раскрывающегося списка **Формат файла** — pdf или xlsx.
5. Выберите столбцы, которые будут отражены в отчете.

 Подсказка:

По умолчанию в окне создания отчета указаны те же столбцы, которые ранее были выбраны для отображения в таблице.

6. Нажмите **Запустить создание отчета**.
 - **Результат шага:** В правом верхнем углу будет отображено всплывающее уведомление **Задача создания отчета запущена**.
7. Чтобы сохранить сформированный отчет, нажмите на ссылку с его названием.

7.8. Настройки активов

В этом разделе:

- [Настройка учетных данных активов](#)
 - [Добавление учетных данных актива](#)
 - [Редактирование и удаление учетных данных активов](#)
 - [Импорт учетных данных активов](#)
- [Настройка классификаторов](#)
 - [Создание информационных систем](#)
 - [Создание меток](#)
 - [Редактирование и удаление классификаторов](#)
 - [Экспорт и импорт классификаторов](#)

Пользователи могут создавать, редактировать и удалять группы (классификаторы) ИС и других активов.

Для активного сбора данных (конфигураций и проверок на соответствие требованиям ИБ) пользователи могут добавлять учетные данные активов.

7.8.1. Настройка учетных данных активов

В этом разделе:

- [Добавление учетных данных актива](#)
- [Редактирование и удаление учетных данных активов](#)
- [Импорт учетных данных активов](#)

Для сбора конфигурации и событий с активов создайте и настройте учетные записи в операционных системах активов. При настройке необходимо учесть права, обеспечивающие доступ к информации о конфигурации и событиях актива. Учетные данные (логин и пароль) таких учетных записей указываются в Комплексе и используются сканерами и источниками событий для привилегированного доступа к активам.

В веб-интерфейсе Комплекса можно просмотреть как список всех учетных данных активов, так и учетные данные конкретного актива.

Чтобы просмотреть список всех учетных данных активов Комплекса, перейдите на страницу [Администрирование](#) → [Настройка активов](#) → [Учетные данные актива](#). Для фильтрации элементов в списке используется фильтр по активам и поля поиска по наименованию и логину.

2. В открывшемся окне введите следующие параметры:

- наименование и описание новой учетной записи;
- тег (может совпадать с логином учетной записи, созданной в операционной системе актива) — используется в Python-скриптах сбора данных для поиска соответствующей учетной записи в списке;



Подсказка:

См. подробнее в разделе [Содержание Python-скриптов](#).

- логин (должен совпадать с логином учетной записи, созданной в операционной системе актива);
- пароль (должен совпадать с паролем учетной записи, созданной в операционной системе актива);
- подтверждение пароля.

Добавление учетных данных актива

×

Наименование *

Описание

Тег *

Обязательно заполните хотя бы одно из полей "Логин" или "Пароль"

Логин *

Пароль *

Подтверждение пароля *

Создать

Отменить

Рис. 158. Окно «Добавление учетных данных актива»

3. Нажмите **Создать**.

Подсказка:

Для использования учетных данных при сборе конфигураций, событий и OVAL-объектов необходимо связать созданные учетные данные с активом. См. подробнее в разделе [Настройка активов для сбора данных](#).

Пример

Примеры учетных данных для доступа к активам:

- Доступ к устройствам производителя Cisco в привилегированном режиме (enable).
 - Тег: cisco_en.
 - Логин: —.
 - Пароль: [пароль].
- Доступ к устройствам производителя Cisco по протоколу SNMP:
 - Тег: community.
 - Логин: public.
 - Пароль: —.
- Доступ по протоколу telnet:
 - Тег: cisco.
 - Логин: —.
 - Пароль: [пароль].

7.8.1.2. Редактирование и удаление учетных данных активов

Менять состав учетных данных активов в веб-интерфейсе можно несколькими способами. К ним относятся:

1. Редактирование учетных данных на странице **Учетные данные актива**. Для редактирования:
 - а. Перейдите на страницу **Администрирование** → **Настройка активов** → **Учетные данные актива**.
 - б. Выберите учетную запись в списке и нажмите кнопку  (**Редактировать учетные данные**).
 - ▶ **Результат шага:** Откроется окно **Редактирование учетных данных актива**.
 - в. Измените необходимые параметры и нажмите кнопку **Сохранить**.

✕

Редактирование учетных данных актива

Наименование *

Кред admin root

Описание

Тег *

admin

Обязательно заполните хотя бы одно из полей "Логин" или "Пароль"

Логин *

root

Пароль *

Подтверждение пароля *

Сохранить

Отменить

Рис. 159. Окно «Редактирование учетных данных актива»

2. Редактирование учетных данных в карточке актива. Для редактирования:
 - а. Перейдите в карточку актива.
 - б. Перейдите по ссылке **Учетные данные актива** в блоке **Связанные данные**.
 - в. Нажмите  (**Редактировать учетные данные**) напротив учетной записи, которую нужно изменить.
 - **Результат шага:** Откроется окно **Редактирование учетных данных актива**.
 - г. Измените необходимые параметры и нажмите кнопку **Сохранить**.
3. Удаление одной записи об учетных данных на странице **Учетные данные актива**. Для удаления:
 - а. Перейдите на страницу **Администрирование** → **Настройка активов** → **Учетные данные актива**.
 - б. Нажмите  (**Удалить**) напротив учетных данных, которые необходимо удалить.
 - **Результат шага:** Откроется окно ввода обоснования удаления учетных данных.

в. Укажите обоснование действия и нажмите **Подтвердить**.

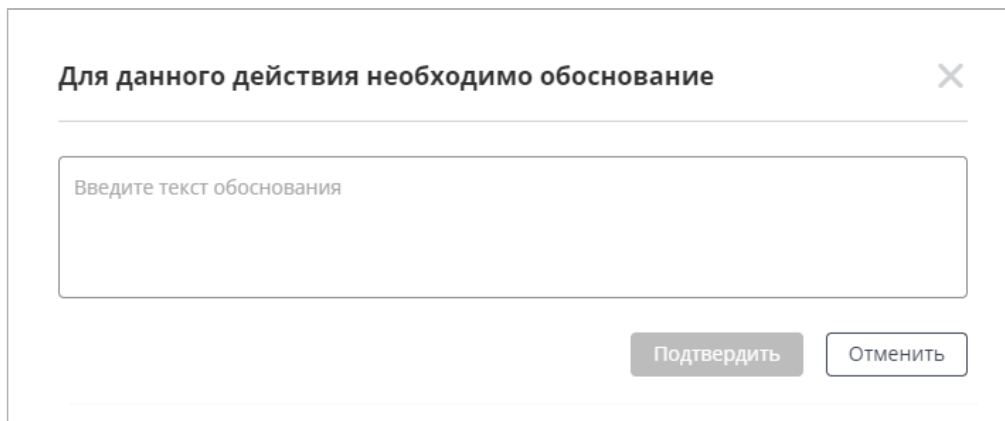


Рис. 160. Окно обоснования удаления учетных данных

4. Удаление учетных данных, отфильтрованных на странице **Учетные данные актива**. Для удаления:
 - а. Перейдите на страницу **Администрирование** → **Настройка активов** → **Учетные данные актива**.
 - б. Воспользуйтесь фильтрами для получения списка учетных данных, подлежащих удалению.
 - в. В верхней части страницы нажмите  (**Удалить учетные данные актива**).
 - **Результат шага:** Откроется окно ввода обоснования удаления учетных данных.
 - г. Укажите обоснование действия и нажмите **Подтвердить**.
5. Удаление учетной записи в карточке актива. Для удаления:
 - а. Перейдите в карточку актива.
 - б. Нажмите кнопку  напротив блока **Учетные данные актива**.
 - **Результат шага:** откроется окно **Настройка учетных данных**.
 - в. Нажмите  (**Удалить**) напротив учетной записи, которую нужно удалить.
 - **Результат шага:** Откроется окно ввода обоснования удаления учетных данных.
 - г. Укажите обоснование действия и нажмите **Подтвердить**.

7.8.1.3. Импорт учетных данных активов

Для импорта списка учетных записей активов из файла формата *.json:

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

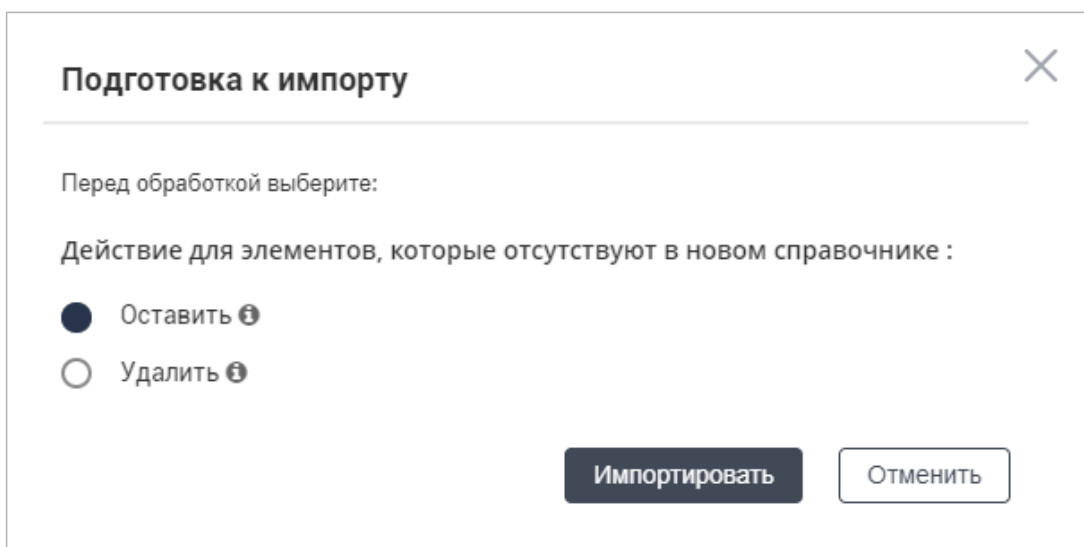


Рис. 161. Окно «Подготовка к импорту»

5. Нажмите **Импортировать**.

6. Убедитесь, что список учетных данных был успешно загружен.

- **Результат шага:** После загрузки файла в правом верхнем углу страницы **Импорт и экспорт** появится уведомление: **Список «Учетные данные активов» успешно обновлен**, и на странице **Администрирование** → **Настройка активов** → **Учетные данные актива** появится импортированный список учетных записей.

7.8.2. Настройка классификаторов

Классификаторы активов загружаются в систему при первичной установке. Некоторые из них можно редактировать и дополнять.

Информация о редактируемых классификаторах приведена в таблице ниже (Таблица 91. Редактируемые классификаторы Комплекса).

Табл. 91. Редактируемые классификаторы Комплекса

КЛАССИФИКАТОР	ХАРАКТЕРИСТИКА КЛАССИФИКАТОРА	ОТНОШЕНИЕ К АКТИВАМ
ИС	предустановленный редактируемый	необязательный атрибут классификации активов
OVAL	редактируемый	необязательный атрибут классификации активов
Метки	редактируемый	необязательный атрибут классификации активов

Классификаторы предназначены для фильтрации активов. Их содержимое генерируется автоматически при появлении новых элементов в Комплексе. Информация о встроенных классификаторах приведена в таблице ниже.

Табл. 92. Встроенные классификаторы Комплекса

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

Табл. 92. Встроенные классификаторы Комплекса

КЛАССИФИКАТОР	ХАРАКТЕРИСТИКА КЛАССИФИКАТОРА	ОТНОШЕНИЕ К АКТИВАМ
Операционные системы, распознанные Комплексом	предустановленный, автоматически дополняемый нерекладируемый	необязательный атрибут классификации активов; присваивается активам с операционной системой семейства Windows автоматически (при возможности получения информации от активов по протоколу Microsoft Windows Browser)

В Комплексе возможно автоматическое присваивание меток операционных систем для активов. При сканировании узлов домашней сети (на странице **Сенсоры**) метка CPE, полученная в результате сканирования актива и содержащая информацию об операционной системе актива и ее версии, сравнивается с метками CPE, присвоенными созданным ранее пользовательским меткам. В случае совпадения активу присваивается соответствующая метка.

Для поиска активов в списке на странице **Активы** используется фильтрация по реквизитам активов, в том числе с помощью встроенных и пользовательских классификаторов.

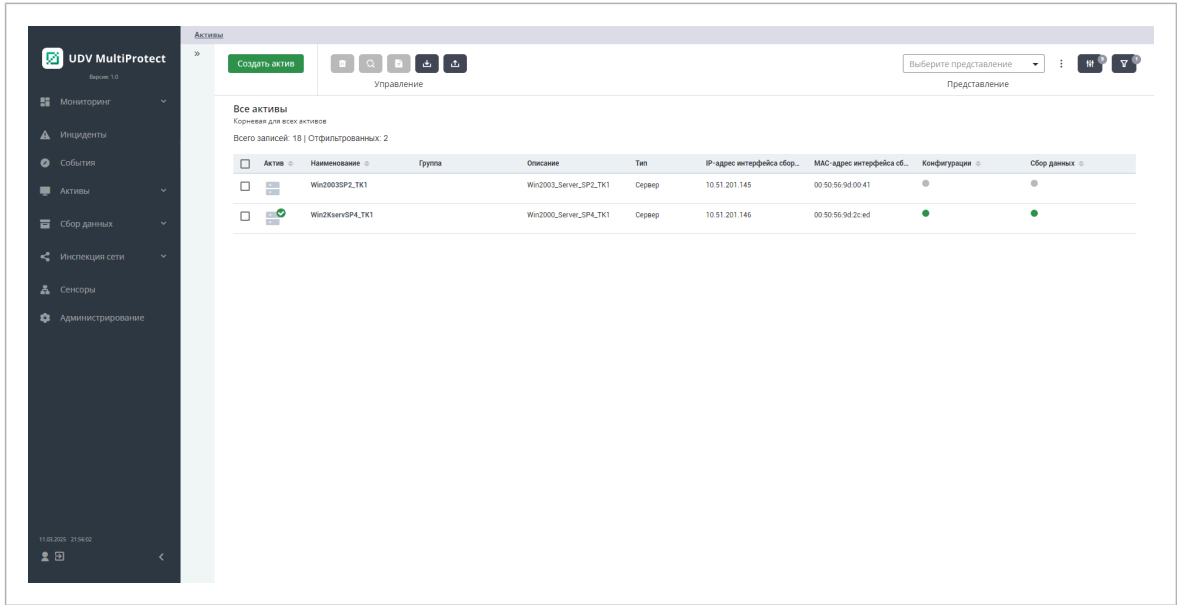


Рис. 162. Список активов с типом «Сервер» из классификатора «Типы активов»

7.8.2.1. Создание информационных систем

Для создания ИС:

**Внимание:**

Максимальная вложенность при создании дочерних классификаторов равна 10.

1. В веб-интерфейсе Комплекса перейдите на страницу **Активы** → **Перечень ИС**.

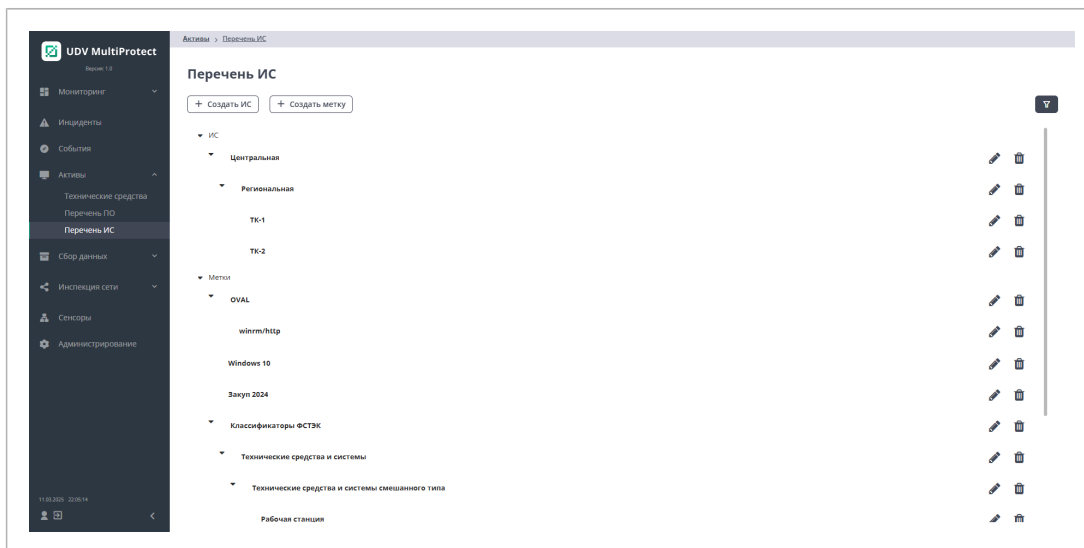


Рис. 163. Страница «Перечень ИС»

2. Нажмите **Создать ИС**. В открывшемся окне укажите наименование, описание и вышестоящую систему.

Создание ИС

Наименование *

Описание

Вышестоящая ИС *

Выберите ИС

Создать

Отменить

Рис. 164. Окно «Создание ИС»

3. Нажмите **Создать**.

7.8.2.2. Создание меток

Для создания метки:

**Внимание:**

Максимальная вложенность при создании дочерних классификаторов равна 10.

1. Перейдите на страницу **Активы** → **Перечень ИС**.
2. Нажмите **Создать метку**. В открывшемся окне **Создание метки** укажите наименование новой метки и вышестоящую метку.

Рис. 165. Окно «Создание метки»

3. Нажмите **Создать**.

7.8.2.3. Редактирование и удаление классификаторов

Для управления созданными ранее классификаторами доступны следующие возможности:

1. Редактирование. Для редактирования классификатора:
 - а. Перейдите на страницу **Администрирование** → **Перечень ИС**.
 - б. Напротив классификатора, который необходимо изменить, нажмите  (**Редактировать**).

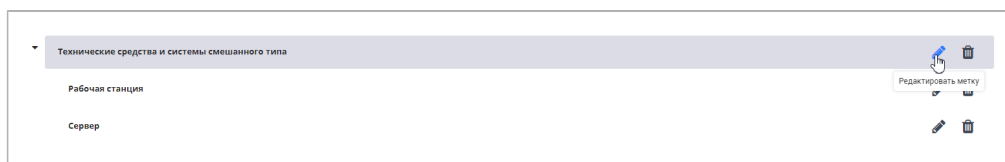


Рис. 166. Кнопка редактирования классификатора

- **Результат шага:** Откроется окно **Редактирование метки** или **Редактирование ИС**, в зависимости от выбора типа классификатора.
- в. Измените необходимые параметры.

Рис. 167. Окно «Редактирование метки»

г. Нажмите **Сохранить**.

2. Удаление. Для удаления классификатора:

а. Перейдите на страницу **Перечень ИС**.

б. Напротив классификатора, который необходимо удалить, нажмите  (**Удалить**).

► **Результат шага:**

Откроется окно подтверждения удаления ИС или метки, в зависимости от выбора типа классификатора.

Рис. 168. Окно подтверждения удаления ИС

Рис. 169. Окно подтверждения удаления метки

в. Нажмите **Подтвердить**.

7.8.2.4. Экспорт и импорт классификаторов

В этом разделе:

- Экспорт справочника с классификаторами ИС
- Экспорт меток
- Импорт справочников с классификаторами ИС
- Импорт меток

Экспорт и импорт справочников с иерархической структурой, содержащих классификаторы осуществляется на странице **Администрирование** → **Основные настройки** → **Импорт и экспорт**.

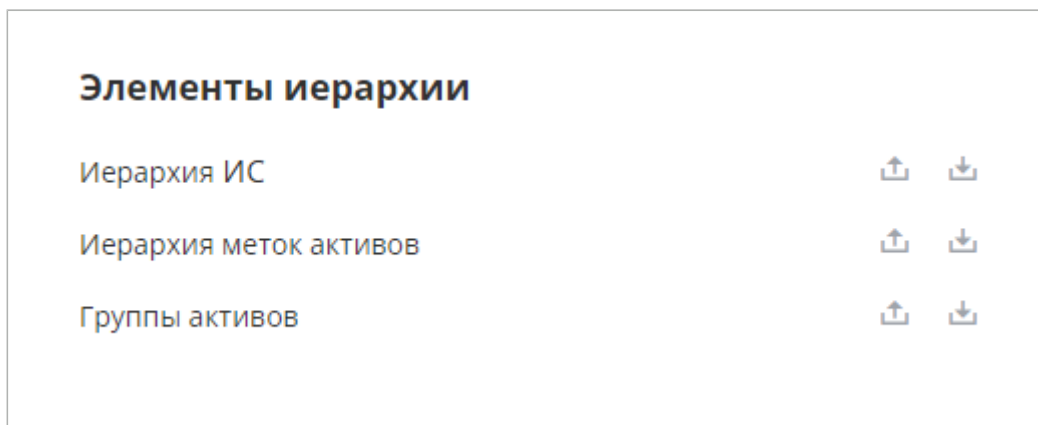


Рис. 170. Панель «Элементы иерархии» на странице «Импорт и экспорт»

7.8.2.4.1. Экспорт справочника с классификаторами ИС

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

1. Перейдите на страницу **Администрирование** → **Основные настройки** → **Импорт и экспорт**.
2. На панели **Элементы иерархии** в строке **Иерархия ИС** нажмите кнопку  (**Экспортировать**).
 - **Результат шага:** Файл со списком классификаторов ИС и их иерархией `ics_[дата_и_время].json` будет сформирован и доступен для скачивания в правом верхнем углу страницы **Импорт и экспорт** под заголовком **Результат последнего экспорта**.
3. Для скачивания файла нажмите на название сформированного файла под заголовком **Результат последнего экспорта**.
4. В открывшемся окне укажите расположение для экспортируемого файла, введите название файла и нажмите **Сохранить**.

7.8.2.4.2. Экспорт меток

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

1. Перейдите на страницу **Администрирование** → **Основные настройки** → **Импорт и экспорт**.
2. На панели **Элементы иерархии** в строке **Иерархия меток активов** нажмите кнопку  (**Экспортировать**).
 - **Результат шага:** Файл со списком меток и их иерархией `tags_[дата_и_время].json` будет сформирован и доступен для скачивания в правом верхнем углу страницы **Импорт и экспорт** под заголовком **Результат последнего экспорта**.
3. Для скачивания файла нажмите на название сформированного файла под заголовком **Результат последнего экспорта**.
4. В открывшемся окне укажите расположение для экспортируемого файла, введите название файла и нажмите **Сохранить**.

7.8.2.4.3. Импорт справочников с классификаторами ИС



Внимание:

Как правило, файлы в формате *.json не создаются вручную, а экспортируются из других Комплексов.

Для импорта справочника с пользовательской иерархией ИС из файла формата *.json в Комплекс:

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

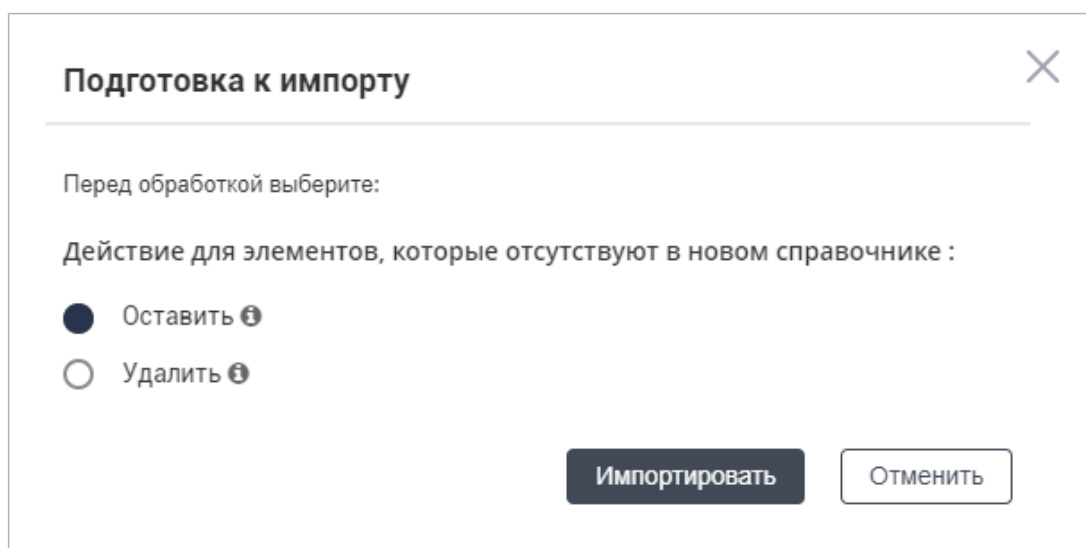


Рис. 171. Окно «Подготовка к импорту»

5. Нажмите **Импортировать**.
6. Убедитесь, что классификаторы были успешно загружены.
 - **Результат шага:** После загрузки файла в правом верхнем углу страницы **Импорт и экспорт** появится уведомление: **Список «Иерархия ИС» успешно обновлена**, и на странице **Активы** → **Перечень ИС** появится импортированный справочник.

7.8.2.4.4. Импорт меток

Для импорта справочника с пользовательской иерархией групп и меток из файла формата *.json в Комплекс:

1. Перейдите на страницу **Администрирование** → **Основные настройки** → **Импорт и экспорт**.
2. На панели **Элементы иерархии** в строке **Иерархия меток активов** нажмите кнопку  (**Импортировать**).
3. В открывшемся окне укажите расположение импортируемого файла формата *.json и подтвердите выбор.
4. В открывшемся окне **Подготовка к импорту** выберите действие для элементов, которые отсутствуют в новом (загружаемом) справочнике:

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

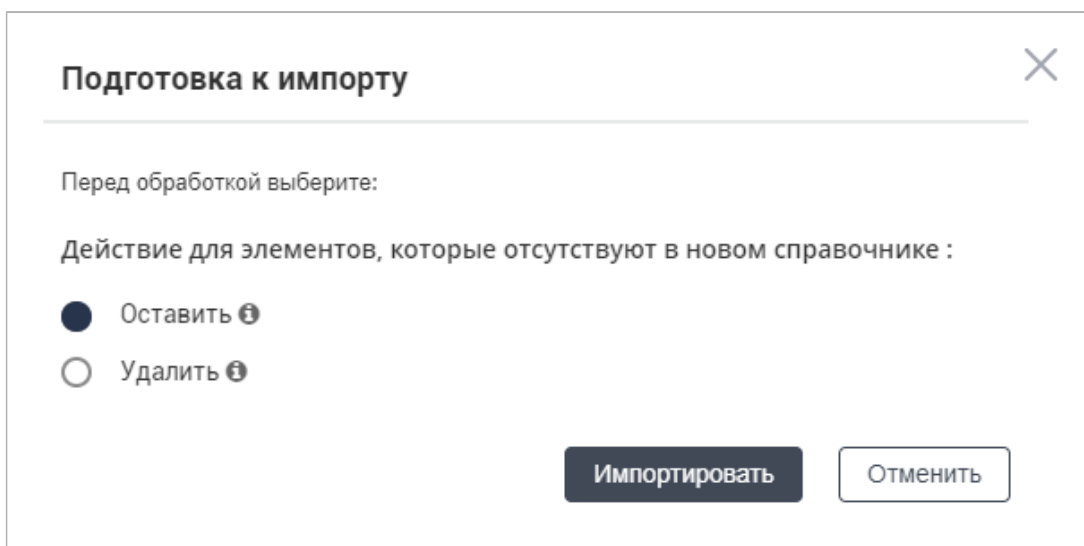


Рис. 172. Окно «Подготовка к импорту»

5. Убедитесь, что метки были успешно загружены.

- **Результат шага:** После загрузки файла в правом верхнем углу страницы **Импорт и экспорт** появится уведомление **Список «Иерархия меток активов» успешно обновлен**, и на странице **Активы** → **Перечень ИС** появится импортированный справочник.

8. Активный сбор данных с активов

В Комплексе предусмотрен режим взаимодействия с активами «запрос–ответ», в результате использования которого полученные данные обрабатываются и могут быть интерпретированы как: конфигурации, события, информация об ОС или ПО или результаты проверок на соответствие требованиям ИБ. Такой режим называется активным сбором данных.

Активный сбор данных с актива предполагает, что Комплекс «посещает» актив от имени пользователя, чьи учетные данные привязаны к активу. Подробнее см. раздел [Настройка активов для сбора данных](#).

Для активного сбора доступны следующие данные:

- Конфигурации. См. подробнее в разделе [Просмотр сводки конфигураций](#).
- События. См. подробнее в разделе [Настройка активного сбора событий](#).
- Параметры безопасности. См. подробнее в разделе [Поиск уязвимостей и проверка соответствия требованиям информационной безопасности](#).
- Информация об ОС и ПО.

Настройка сбора осуществляется на страницах меню [Администрирование](#) → .



Внимание:

Перед настройкой сбора данных ознакомьтесь со справочным разделом [Рекомендации по настройке сбора данных](#).

Просмотр результатов активного сбора данных и настройка сбора осуществляется на страницах:

- **Конфигурации**, где отображается список последних данных, собранных в рамках задач сканерами сбора конфигураций.
- **События**, где среди прочих отображаются события, которые были загружены в результате работы сканеров сбора событий, входящих в задачи сбора данных.
- **Статус сбора**, где отображаются новейшие итоговые статусы выполнения всех сканеров сбора данных.
- **Результаты проверок**, где отображается список ранее созданных проверок на соответствие требованиям информационной безопасности — подробнее см. в разделе [Поиск уязвимостей и проверка соответствия требованиям информационной безопасности](#).
- Вкладка **Перечень ПО** в **карточке актива**, где отображается список собранных с актива данных об установленном на нем ПО.

8.1. Просмотр сводки конфигураций

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

На странице [Конфигурации](#) можно оперативно получать сводку о последних собранных сканерами данных с активов, а также найти интересные. Последними считаются новейшие просканированные конфигурации (подробнее см. раздел [Сбор данных с активов](#)).

Чтобы просмотреть последние конфигурации, перейдите на страницу → **Конфигурации**. На странице конфигурации отображаются в виде таблицы, содержащей следующие данные:

- статус конфигурации;
- дата создания конфигурации
- название актива, с которого собиралась конфигурация;

 Подсказка:

При нажатии на название актива, для которого была создана конфигурация, можно открыть окно **Информация об активе**, в котором будет отображаться краткая информация о выбранном активе.

- наименование конфигурации.

После подбора списка конфигураций содержимое таблицы можно сохранить в отчет.

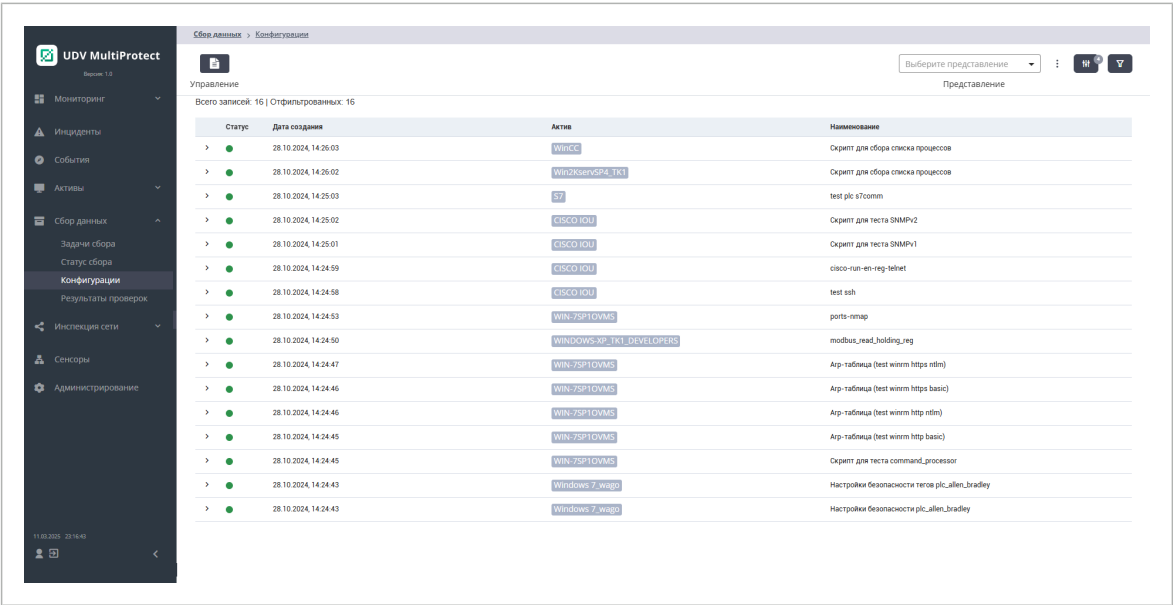


Рис. 173. Страница «Конфигурации»

Статусы конфигураций

Конфигурации могут иметь следующие статусы, которые отображаются при наведении на индикатор статуса:

- **Нет отклонений** — зеленый индикатор;
- **Были отклонения** — желтый индикатор;
- **Есть отклонения** — красный индикатор.

Отображение столбцов

При первом входе на страницу отображаются конфигурации за все время (без фильтров). Отображение колонки

Дата создания по умолчанию выключено. Чтобы регулировать отображение столбцов, нажмите кнопку  в правом верхнем углу. Содержание конфигураций по умолчанию выводится в кратком (свернутом) виде. Для вывода подробностей воспользуйтесь соответствующим фильтром или нажмите  слева от конфигурации.

Фильтры

Чтобы найти нужные конфигурации, воспользуйтесь следующими фильтрами:

- раскрывающийся список **Актив** — содержит список доступных для выбора активов;
- раскрывающийся список **Конфигурации** — содержит список доступных для выбора конфигураций;
- поле **Содержание конфигурации** — может быть заполнено любым текстом, который содержится в конфигурациях;
- поля **Дата и время создания** — позволяет выбрать период с точностью до секунды, по которым необходимо отобразить конфигурации;
- чекбокс **Сравнить с эталонной** позволяет сравнить выбранные фильтром конфигурации с эталоном и вывести только те конфигурации, в которых были обнаружены отклонения от эталона;
- чекбокс **Только с отклонениями** позволяет вывести только те конфигурации, в которых были обнаружены отклонения от эталона, при этом сравнение с эталоном отображаться не будет.

Отчет

Чтобы сохранить отчет по выбранным конфигурациям, нажмите кнопку **Создать отчет** в верхней части страницы. Подробнее о выгрузке отчетов см. раздел Выгрузка отчетов.

В отчете конфигурации отображаются подробно вне зависимости от того, был ли выбран подробный вывод конфигурации. В разделе отчета **Содержание конфигурации** содержится информация о том, является ли конфигурация эталонной.

Сравнение с эталоном

При выборе в фильтрах опции **Сравнить с эталонной** можно просматривать только конфигурации, у которых есть непроверенные изменения.

При просмотре в подробном виде доступны кнопки  (Показать еще по 5 окружающих строк) и  (Скрыть по 5 окружающих строк).

Просмотр конфигурации актива

Чтобы просмотреть архив конфигураций, полученных с актива, наведите курсор на строку с выбранным сканером и нажмите кнопку  **Просмотреть конфигурацию актива**. Подробнее см. раздел «Просмотр архива конфигураций».

8.2. Настройка конфигураций активов

В этом разделе:

- [Содержание Python-скриптов](#)
- [Цифровая подпись Python-скрипта](#)
- [Экспорт и импорт задач сбора данных, сканеров и их групп](#)
- [Настройка сканеров сбора данных](#)
- [Добавление сетевых атрибутов активу с помощью сканера сбора данных по SNMP](#)
- [Сбор данных с активов](#)
- [Просмотр статуса сбора данных](#)
- [Работа с архивом изменений конфигурации актива](#)

Задача сбора данных — сущность, позволяющая при помощи групп сканеров собирать конфигурации и события с активов и их групп, в том числе с использованием расписания cron. Создание и управление задачами производится на странице [Задачи сбора](#) (подробнее см. разделы Создание задачи сбора данных, Управление задачами сбора данных).

Сканер — После импорта или создания сканеров их можно собрать в группы. Управление сканерами и их группами производится на странице [Администрирование](#) → [Сканеры](#) (подробнее см. раздел [Настройка сканеров сбора данных](#)).

Скрипт — это Подробнее о создании скриптов см. в разделе [Содержание Python-скриптов](#). Скрипты сбора данных доступны к импорту при создании сканера. Скрипт также можно экспортировать при редактировании сканера.

В результате выполнения отдельных сканеров либо в составе задач сбора данных формируются конфигурации и события активов.

По умолчанию эталонной считается конфигурация, которая была получена первой в результате успешного сбора данных по расписанию, указанному в настройках задачи сбора данных актива.

Просмотреть последние собранные конфигурации можно на странице [Конфигурации](#) (подробнее см. раздел Просмотр сводки конфигураций).

Сбор информации о конфигурациях ведется при помощи задач сбора данных, он может быть разовым или периодическим, с отложенным временем запуска или начиная с момента сохранения.



Внимание:

Перед настройкой сбора данных ознакомьтесь со справочным разделом [Рекомендации по настройке сбора данных](#).

8.2.1. Содержание Python-скриптов

Скрипты для сбора данных выполняются в среде, поддерживающей подмножество синтаксиса языка Python (RestrictedPython).



Внимание:

Скрипт необходимо сохранять в файле формата *.py (кодировка – UTF-8 без BOM).

В скриптах запрещен импорт произвольных пакетов, по умолчанию в среду выполнения импортированы следующие пакеты из стандартной библиотеки Python: `re`, `string`, `unicodedata`, `hashlib`, `datetime`, `textwrap`, `struct`, `dbfread`, `dateutil`, `dateutil.tz`.

В скриптах доступны следующие переменные:

- `host` – IP-адрес актива, на котором выполняется сбор данных;
- `domain` – имя домена (используется в том случае, если с помощью скрипта осуществляется доступ к активам, находящимся в домене);
- `host_id` – идентификатор актива, на котором выполняется сбор данных;
- `credentials` – словарь (dict) с реквизитами доступа к активу; значение данной переменной – словарь с двумя ключами (`user`, `password`). Сканер получает данные о ключах из учетной записи актива Комплекса, тег которой совпадает с названием словаря;
- `store` – (any, dict) сохраненные данные с предыдущего запуска скрипта. Если скрипт запускается первый раз, то `store = None`;
- `expiration` – максимальное время выполнения скрипта;
- `execute` – метод, выполняющий запрос к коннектору.

Результат выполнения скрипта возвращается с помощью оператора `return`.

Ниже приведен пример скрипта для сбора ARP-таблицы в ОС семейства Unix по протоколу SSH с помощью учетной записи с тегом `admin`:

```
try:
    credential = credentials['admin']
except KeyError as e:
    raise KeyError('Учетные данные для %s не найдены' % e)
protocol_args = {
    'host': host,
    'username': credential.get('user'),
    'password': credential.get('password'),
    'interface': 'ssh',
    'port': 22,
    'query': [{
        'command': 'arp -an\r\n',
        'expects': [],
        'timeout': 10
    }]
}
def escape_ansi(line):
    ansi_escape = re.compile(r'(\x9B|\x1B\[)[0-?]*[ -\/]*[@-~]')
    return ansi_escape.sub('', line)
data = execute('terminal', protocol_args, expiration)
lines = bytes.fromhex(data).decode()
lines = escape_ansi(lines)
regex = r'((?P<ip>((\d{1,3}\.){4}))\sat\s(?P<mac>((\w{2}:?){6})).*\son\s(?P<interface>(.*))\r\n'
matches = re.finditer(regex, lines)
interfaces = [[match.group(g) for g in ['ip', 'mac', 'interface']]
```

```

        for match in matches]
return {
    'visible_keys': {
        'ip': 'IP-адрес',
        'mac': 'MAC-адрес',
        'interface': 'Интерфейс',
    },
    'keys': ['ip', 'mac', 'interface'],
    'data': interfaces,
    'ignore_delete': True,
}

```

Для возможности сбора конфигурации с активов необходимо создать и настроить учетные записи на активах с соответствующими правами. Учетную запись, настроенную в операционной системе актива, необходимо добавить в список учетных данных в веб-интерфейсе Комплекса. Порядок настройки учетных данных в Комплексе приведен в разделе Настройка учетных данных активов.



Подсказка:

Создание сканера описано в разделе [Создание сканеров сбора данных](#). Создание скрипта OVAL описано в разделе [Управление скриптами OVAL](#).

8.2.2. Цифровая подпись Python-скрипта

Для предотвращения запуска вредоносных исполняемых файлов в сети ИС все сканеры, создаваемые в Комплексе, должны иметь цифровую подпись импортируемых при их создании Python-файлов (скриптов). Возможность подписывать Python-файлы имеется у производителя Комплекса, а также у администратора безопасности или другого сотрудника при наличии закрытого ключа от сертификата. Подпись можно выполнять с помощью библиотеки OpenSSL. Комплекс верифицирует цифровую подпись Python-файла при создании сканера с помощью сертификата открытого ключа. Сертификат хранится в операционной системе Комплекса.

Для создания цифровой подписи Python-файла:

1. Запросите у поставщика закрытый ключ от сертификата `datapk-script.key`.
2. Подключитесь к операционной системе Комплекса по протоколу SFTP.
3. Скопируйте Python-файл в директорию `/usr/share/udv/scripts-certs`.



Подсказка:

Вы также можете скопировать Python-файл в директорию `scripts-certs` с помощью USB-носителя.

4. Подключитесь к операционной системе Комплекса или сенсора, который будет собирать данные.
5. Перейдите в директорию `/usr/share/udv/scripts-certs`. Для этого выполните команду:

```
cd /usr/share/udv/scripts-certs
```

6. Создайте цифровую подпись Python-файла с использованием закрытого ключа `datapk_script.key` (или ключа с другим названием, расположенного в директории `scripts-certs`). Для этого выполните команду:

```
openssl dgst -sha256 -sign datapk_script.key "[Наименование_Python-файла].py" | openssl  
enc -base64 -in /dev/stdin
```

7. Скопируйте полученную цифровую подпись в буфер обмена или в текстовый файл.

Используйте Python-файл и его цифровую подпись при создании или редактировании сканера сбора данных — подробнее см. раздел Настройка сканеров сбора данных.

8.2.3. Экспорт и импорт задач сбора данных, сканеров и их групп

В этом разделе:

- Импорт сканеров и их групп
- Импорт задач сбора данных
- Экспорт сканеров и их групп
- Экспорт задач сбора данных

Экспорт и импорт задач сбора данных, сканеров и их групп осуществляется на странице **Администрирование** → **Основные настройки** → **Импорт и экспорт** на панели **Сбор данных**.

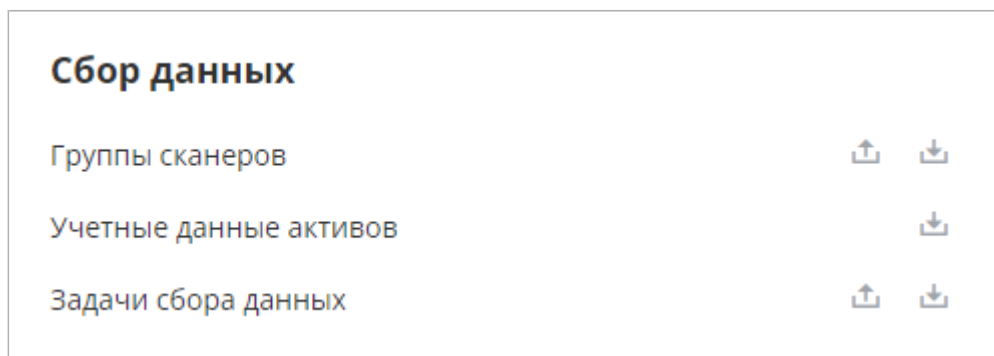


Рис. 174. Панель «Сбор данных» на странице «Импорт и экспорт»

8.2.3.1. Импорт сканеров и их групп

Для импорта сканеров из файла формата *.json в Комплекс:

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

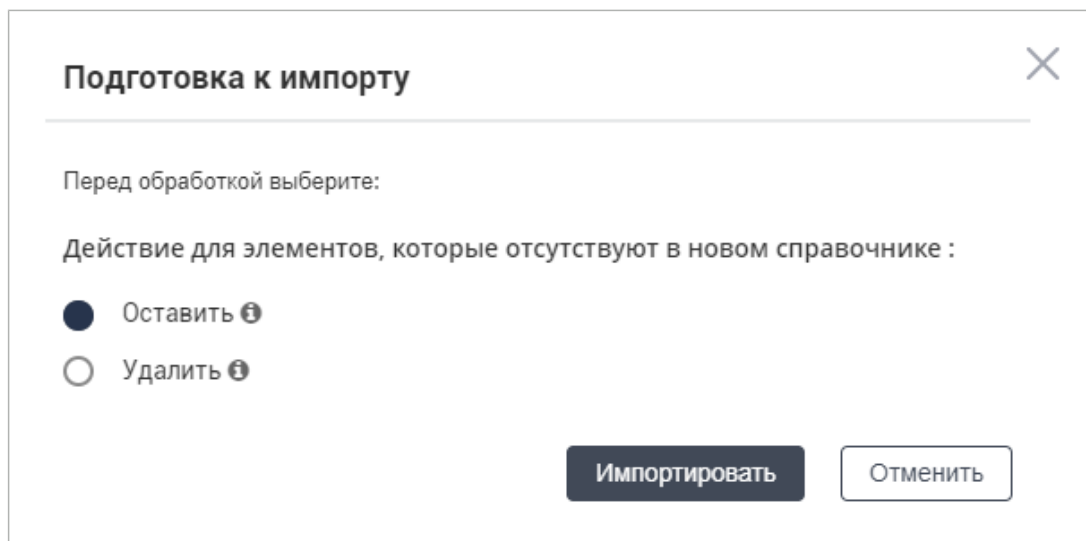


Рис. 175. Окно «Подготовка к импорту»

5. Нажмите **Импортировать**.

- **Результат шага:** Будет запущен процесс импорта: в правом верхнем углу появится уведомление **Запущен импорт справочника**, а под заголовком **Результат последнего импорта** будет символ -.



Подсказка:

Операции импорта являются фоновыми — со страницы можно безопасно уходить.

6. Убедитесь, что сканеры и их группы были успешно загружены. Для этого перейдите на страницу **Администрирование** → **Сканеры**.

8.2.3.2. Импорт задач сбора данных

Для импорта задач сбора данных из файла формата *.json в Комплекс:

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

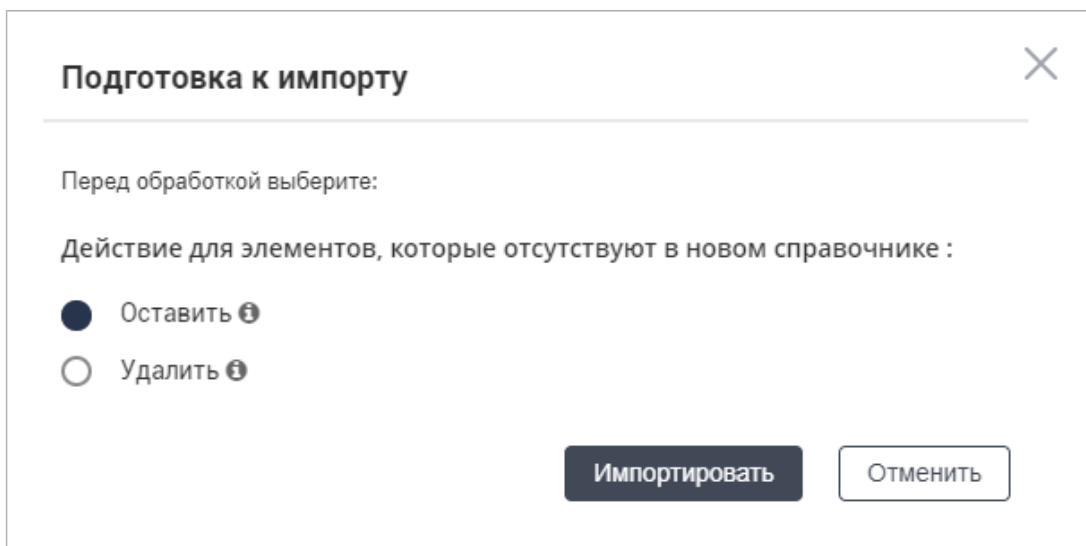


Рис. 176. Окно «Подготовка к импорту»

5. Нажмите **Импортировать**.
 - **Результат шага:** Будет запущен процесс импорта: в правом верхнем углу появится уведомление **Запущен импорт справочника**, а под заголовком **Результат последнего импорта** будет символ -.



Подсказка:

Операции импорта являются фоновыми — со страницы можно безопасно уходить.

6. Убедитесь, что задачи были успешно загружены. Для этого перейдите на страницу **Задачи сбора**.

8.2.3.3. Экспорт сканеров и их групп

Для экспорта списка сканеров сбора данных и их групп в файл формата *.json:

1. Перейдите на страницу **Администрирование** → **Основные настройки** → **Импорт и экспорт**.
2. На панели **Сбор данных** в строке **Группы сканеров** нажмите кнопку  (**Экспортировать**).
 - **Результат шага:** файл со списком сканеров и их групп `scanner_groups_[дата_и_время].json` будет сформирован и доступен для скачивания в правом верхнем углу страницы **Импорт и экспорт** под заголовком **Результат последнего экспорта**.
3. Для скачивания файла нажмите на его название в верхнем правом углу под заголовком **Результат последнего экспорта**.
4. В открывшемся окне укажите расположение для экспортируемого файла, введите название файла и нажмите **Сохранить**.
 - **Результат шага:** файл `scanner_groups_[дата_и_время].json` будет загружен на компьютер.

8.2.3.4. Экспорт задач сбора данных

Для экспорта списка задач сбора данных в файл формата *.json:

1. Перейдите на страницу **Администрирование** → **Основные настройки** → **Импорт и экспорт**.
2. На панели **Сбор данных** в строке **Задачи сбора данных** нажмите кнопку  (**Экспортировать**).
 - **Результат шага:** файл со списком задач `collection_tasks_[дата_и_время].json` будет сформирован и доступен для скачивания в правом верхнем углу страницы **Импорт и экспорт** под заголовком **Результат последнего экспорта**.
3. Для скачивания файла нажмите на название сформированного файла под заголовком **Результат последнего экспорта**.
4. В открывшемся окне укажите расположение для экспортируемого файла, введите название файла и нажмите **Сохранить**.
 - **Результат шага:** файл `collection_tasks_[дата_и_время].json` будет загружен на компьютер.

8.2.4. Настройка сканеров сбора данных

В этом разделе:

- Создание сканеров сбора данных
- Управление сканерами сбора данных
- Группировка сканеров сбора данных

В веб-интерфейсе Комплекса имеется возможность создания сканера для сбора данных с актива путем загрузки Python-скрипта сбора данных из файла в Комплекс. Создать сканер можно на странице **Сканеры**.

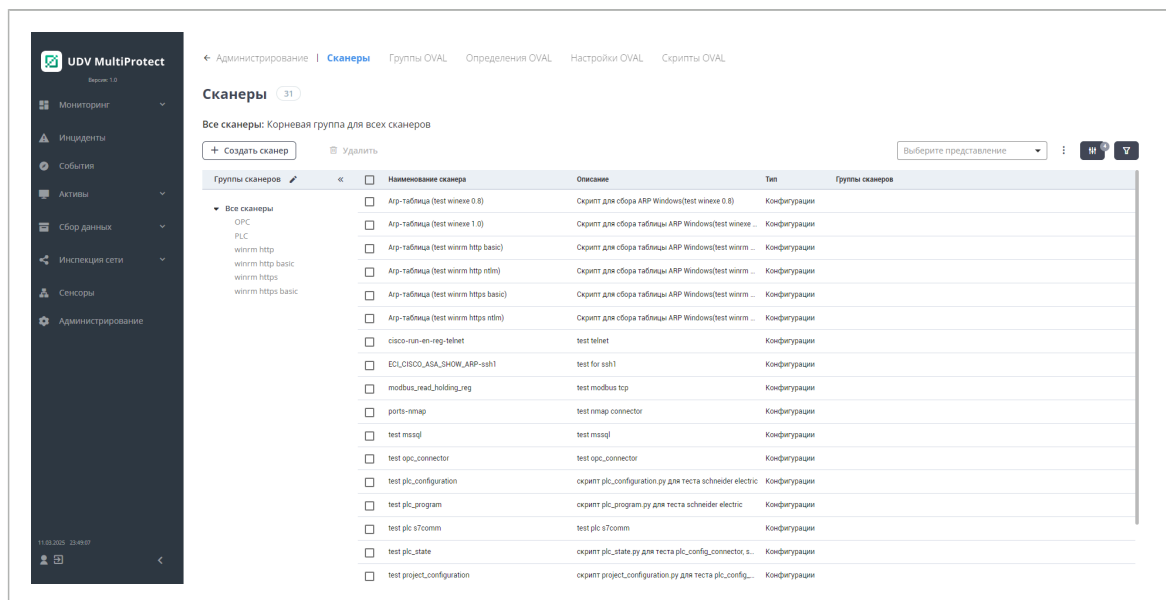


Рис. 177. Страница «Сканеры»

8.2.4.1. Создание сканеров сбора данных

Для создания сканера вручную:

1. Создайте или получите от сервисного центра файл формата *.py, содержащий скрипт для сбора необходимых данных. См. подробнее о содержании скрипта в разделе [Содержание Python-скриптов](#).
2. Если вы создали файл формата *.py вручную, обратитесь в сервисный центр или к вашему администратору безопасности для получения закрытого ключа от сертификата datapk_script.crt и создайте цифровую подпись файла. См. подробнее о цифровой подписи в разделе [Цифровая подпись Python-скрипта](#).
3. Перейдите на страницу **Администрирование** → **Сканеры**.
4. Нажмите **Создать сканер**. В открывшемся окне **Настройки сканера** задайте следующие параметры:
 - а. наименование и описание сканера;



Внимание:

Максимальная длина текста в поле **Наименование** — 255 символов. Максимальная длина текста в поле **Описание** — 100 символов.

- б. тип сканера (конфигурации, события, версия ОС или установленное ПО);
- в. группы сканеров (подробнее см. в разделе [Группировка сканеров сбора данных](#));

- г. цифровую подпись (подробнее см. в разделе [Цифровая подпись Python-скрипта](#));
- д. максимальное время ожидания выполнения задачи в минутах, при достижении которого сбор завершится [ошибкой соединения](#);



Внимание:

Вводимое значение максимального времени ожидания выполнения задачи должно быть в диапазоне от 1 до 30.

- е. нажмите кнопку **Импортировать** для загрузки скрипта из файла. В проводнике выберите и откройте подписанный ранее файл скрипта формата *.ру;

Создание сканера

Наименование *

Введите наименование

Описание

Введите описание

Тип *

Конфигурации

Группы сканеров

Не выбрано

Цифровая подпись *

Введите цифровую подпись

Максимальное время ожидания выполнения задачи, мин

10

Скрипт *

Не выбран

Импортировать

Создать

Отменить

Рис. 178. Окно «Создание сканера»

5. Нажмите **Создать**.

8.2.4.2. Управление сканерами сбора данных

8.2.4.2.1. Просмотр информации о сканере

Для просмотра:

1. Наведите курсор на строку со сканером, информацию о котором необходимо просмотреть.
2. Нажмите кнопку  (**Просмотреть информацию о сканере**) напротив него.
 - **Результат шага:** Откроется окно **Просмотр информации о сканере**.

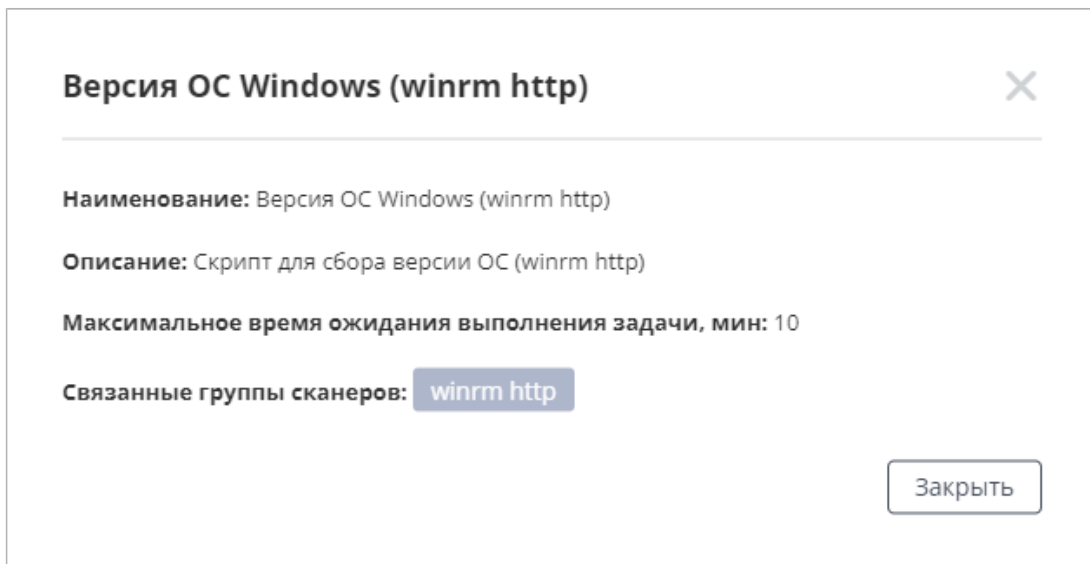


Рис. 179. Окно просмотра информации о сканере

3. Для выхода из окна нажмите **Заккрыть**.

8.2.4.2.2. Запуск сканера

Для запуска:

1. Наведите курсор на строку со сканером, который необходимо запустить.
2. Нажмите кнопку  (**Запустить сканирование**) напротив него.
 - **Результат шага:** Откроется окно **Запуск сканера**.
3. Выберите Комплекс и актив для сбора данных.

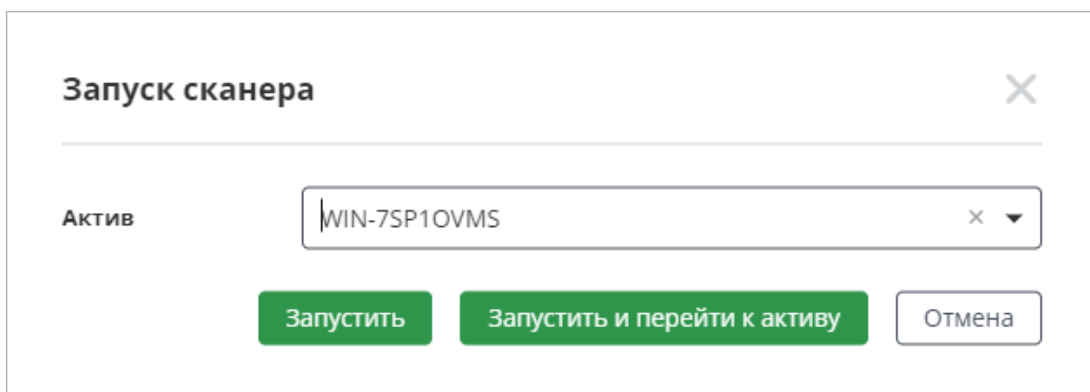


Рис. 180. Окно «Запуск сканера»

4. Нажмите **Запустить** или **Запустить и перейти к активу**.

8.2.4.2.3. Повторный запуск сканера

Для повторного запуска однократного сбора данных на активе:

1. Перейдите в раздел **Инспекция активов** → **Статус сбора**.
 - **Результат шага:** Откроется таблица **Статус сбора**.
2. При необходимости отфильтруйте список статусов, чтобы найти строку с требуемым активом и сканером, который ранее запускался на этом активе.
3. Нажмите кнопку **(Запустить сканирование повторно)** справа в выбранной строке таблицы.
 - **Результат шага:** Появится уведомление об успешном запуске сканирования.

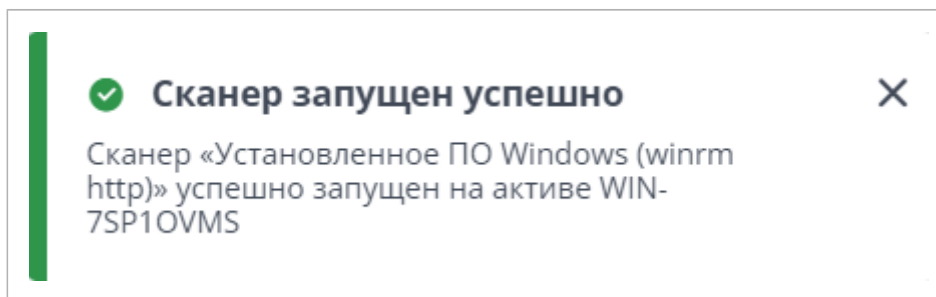


Рис. 181. Уведомление о запуске сканирования

8.2.4.2.4. Редактирование сканера

Для редактирования:

1. Наведите курсор на строку со сканером, который необходимо изменить.
2. Нажмите кнопку  **(Редактировать)** напротив него.
 - **Результат шага:** Откроется окно **Редактирование сканера**.
3. Измените необходимые параметры сканера.

✕

Редактирование сканера

Наименование *

Версия ОС Windows (winrm http)

Описание

Скрипт для сбора версии ОС (winrm http)

Тип *

Версия ОС

Группы сканеров

✕

Группа для скриптов сбора ОС/ПО winrm http

✕

Цифровая подпись *

H1ahC7Vgi8E/ifLAAacC4gAim7XZ6b5HzgTeyCanKBeI7BLScx4OigLunooMkxENVQoP1

Максимальное время ожидания выполнения задачи, мин

10

Скрипт *

script_2024-08-30_17-55.py

Импортировать

Экспортировать

Сохранить

Отменить

Рис. 182. Окно «Редактирование сканера»

4. Нажмите **Сохранить**.

8.2.4.2.5. Удаление сканера

Для удаления:

1. Наведите курсор на строку со сканером, который необходимо удалить.
2. Нажмите кнопку  (**Удалить сканер**) напротив него.

► **Результат шага:** появится окно предупреждения *При удалении сканера будут удалены конфигурации, собранные этим сканером.*

3. Введите обоснование удаление сканера и нажмите **Подтвердить**.

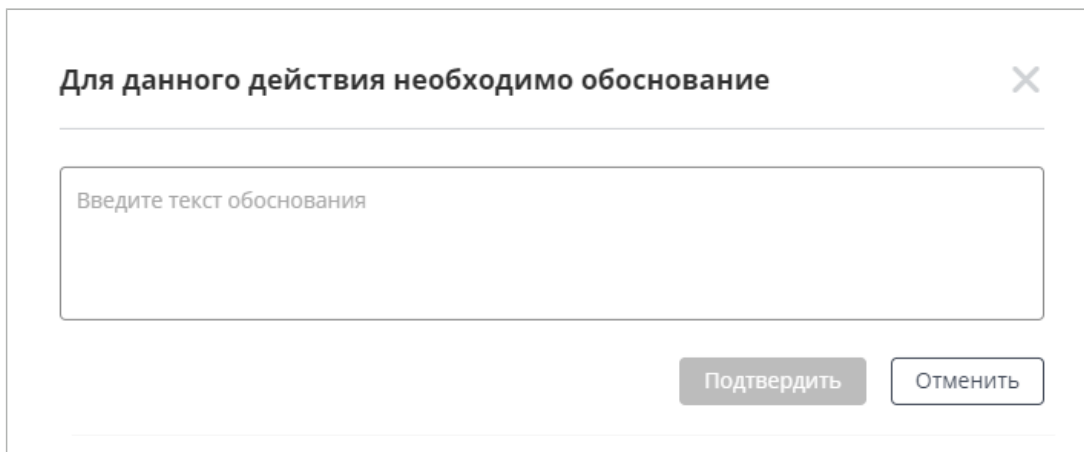


Рис. 183. Окно предупреждения и ввода обоснования удаления сканера

8.2.4.2.6. Групповое удаление сканеров

Для удаления группы сканеров:

1. Получите необходимую выборку сканеров:
 - а. Выберите группу сканеров в левой части страницы.
 - б. При необходимости отфильтруйте список сканеров: нажмите кнопку , выберите настройки фильтрации и нажмите кнопку **Применить**.
 - в. Отметьте все отфильтрованные сканеры на удаление с помощью чекбокса в заголовке таблицы, либо отметьте отдельные сканеры с помощью чекбоксов рядом со сканерами.
2. Нажмите кнопку  **Удалить** в верхней части страницы.
 - **Результат шага:** появится окно предупреждения *При удалении сканеров будут удалены конфигурации, собранные этими сканерами.*
3. В открывшемся окне введите обоснование удаления сканеров и нажмите кнопку **Подтвердить**.

8.2.4.3. Группировка сканеров сбора данных

В этом разделе:

- [Создание группы сканеров](#)
- [Добавление сканеров в группу](#)
- [Управление группами сканеров](#)

Для использования сканеров в задачах необходима группировка существующих сканеров сбора данных. Группы сканеров отображаются на странице **Сканеры** в левой части страницы.

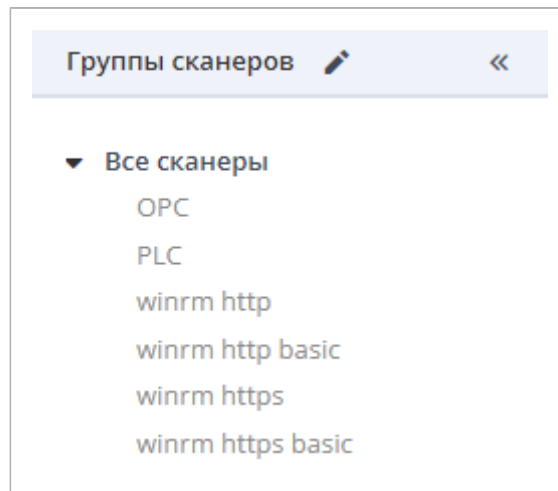


Рис. 184. Панель управления сканерами сбора данных

Если в списке выбрана конкретная группа сканеров, то фильтры будут применяться только для элементов этой группы.

8.2.4.3.1. Создание группы сканеров

Для создания группы сканеров:

1. Перейдите на страницу **Администрирование** → **Сканеры**.
2. Над панелью с группами сканеров в левой части страницы нажмите **Редактировать**.
 - **Результат шага:** Откроется окно **Редактирование групп сканеров**.
3. Нажмите кнопку **+** напротив группы, которая будет вышестоящей для создаваемой.

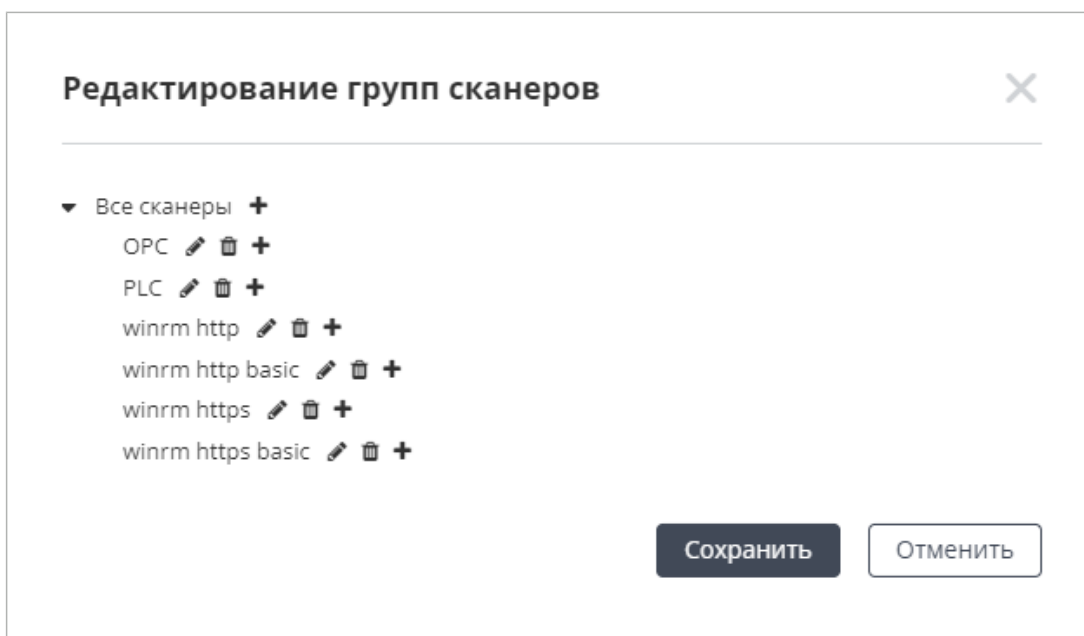


Рис. 185. Окно «Редактирование групп сканеров»

► **Результат шага:** Откроется окно **Создание группы сканеров**.

- В окне создания задайте наименование и описание новой группы. При необходимости выберите другую вышестоящую группу.

 **Внимание:**

Наименование группы сканеров должно быть уникальным.

Рис. 186. Окно «Создание группы сканеров»

- Нажмите **Сохранить**.



Внимание:

Без сохранения всех изменений групп в **в окне редактирования групп сканеров** изменения не будут отражены в Комплексе.

► **Результат шага:** Созданная группа появится в списке в окне **Редактирование групп сканеров**.

6. При необходимости добавьте другие группы сканеров.

7. В окне **Редактирование групп сканеров** нажмите **Сохранить**.

► **Результат шага:** Появится предупреждение о неизменности задач сбора данных в результате изменения состава групп.

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

► **Результат шага:** Окно редактирования групп будет закрыто, изменения появятся в Комплексе.



Внимание:

В одну группу сканеров можно добавить до 10 групп. При попытке добавления более 10 групп сканеров возникнет предупреждение об ошибке **Уровень вложенности групп превышает максимальный (10)**

8.2.4.3.2. Добавление сканеров в группу



Подсказка:

Сканер может быть добавлен в несколько групп.

Для добавления сканеров в ранее созданную группу:

- 1. Перейдите на страницу **Администрирование** → **Сканеры**.
- 2. Добавьте сканеры в группу. Для этого:
 - а. Выделите при помощи курсора сканеры, которые будут добавлены в группу.



Подсказка:

Для выделения множества строк выше или ниже выбранной нажмите клавишу **Shift** и выделите строку с последним сканером, который необходимо добавить в группу.



Внимание:

Рекомендуется добавлять в группу не более 30 сканеров сбора данных.

- б. Наведите курсор на один из выделенных сканеров и нажмите левую кнопку мыши.
 - **Результат шага:** появится полупрозрачный квадрат с количеством выделенных сканеров.
- в. Не отпуская левую кнопку мыши, перетащите сканеры в левую часть страницы так, чтобы курсор оказался на наименовании группы, в которую будут перемещены сканеры.
- г. Отпустите левую кнопку мыши.

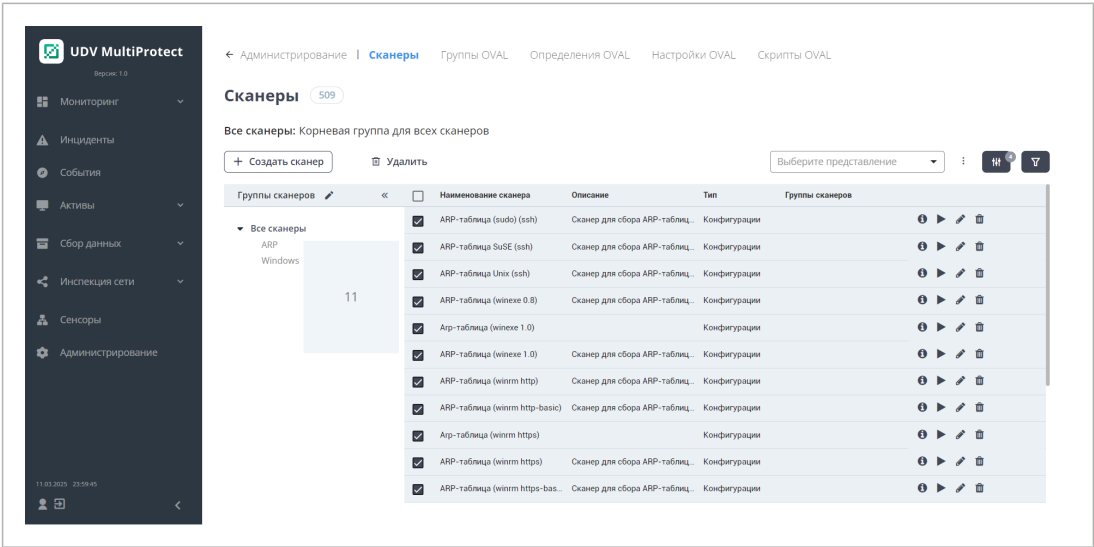


Рис. 187. Добавление сканеров в группу

- **Результат шага:** Откроется окно подтверждения добавления сканеров в группу.
- 3. Нажмите **Подтвердить**.

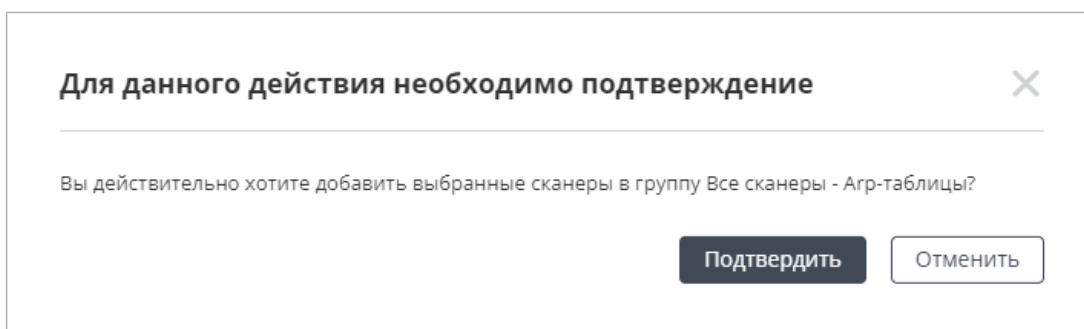


Рис. 188. Окно подтверждения перемещения сканеров

- **Результат шага:** В правом верхнем углу появится уведомление: **Добавление в группу выбранных сканеров успешно завершено**, и сканеры будут добавлены в группу. Если некоторые сканеры уже были в выбранной группе, отобразится предупреждение: **Объект уже существует**, и в группу будут добавлены сканеры, которых не было в группе.
4. При необходимости изменить группу можно также в окне редактирования сканера. См. подробнее в разделе [Управление сканерами сбора данных](#).

Если необходимо исключить сканер из группы, измените соответствующее поле в окне **Редактирование сканера**.

8.2.4.3.3. Управление группами сканеров

На странице **Администрирование** → → **Сканеры** предусмотрены следующие возможности для управления группами сканеров:

1. Изменение группы. Для изменения:

а. Над панелью с группами сканеров в левой части страницы нажмите **Редактировать**.

► **Результат шага:** появится окно **Редактирование групп сканеров**.

б. Нажмите кнопку  напротив группы, которую необходимо изменить.

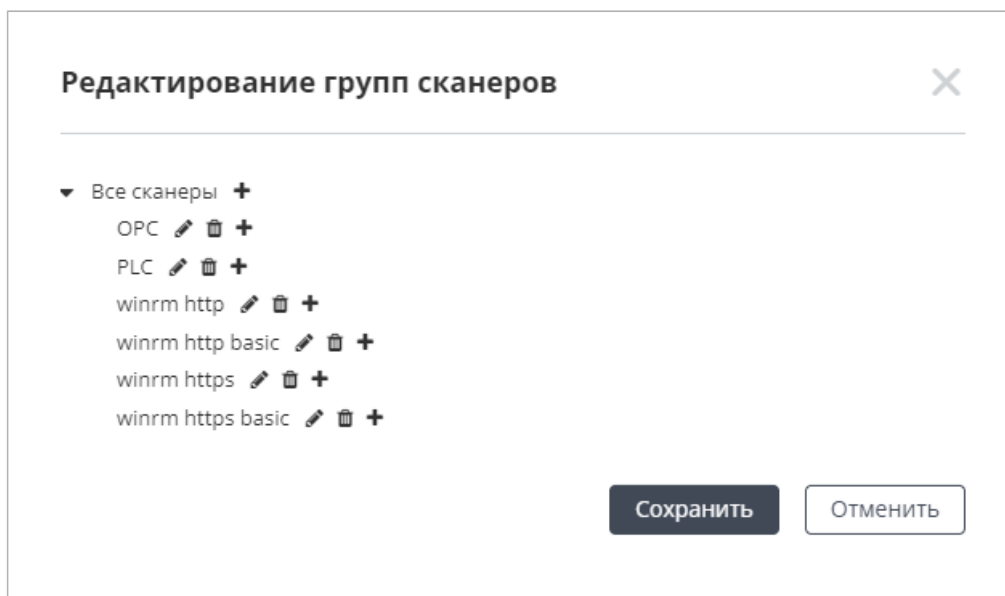


Рис. 189. Окно «Редактирование групп сканеров»

► **Результат шага:** Откроется окно **Редактирование группы сканеров**.

в. Измените необходимые параметры группы сканеров.

Рис. 190. Окно «Редактирование группы сканеров»

г. Нажмите **Сохранить**.

**Внимание:**

Без сохранения всех изменений групп в окне редактирования групп сканеров изменения не будут отражены в Комплексе.

► **Результат шага:** Изменения названия группы появятся в окне **Редактирование групп активов**.

д. При необходимости измените другие группы сканеров.

е. В окне **Редактирование групп сканеров** нажмите **Сохранить**.

► **Результат шага:** Появится предупреждение о неизменности задач сбора данных в результате изменения состава групп.

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

► **Результат шага:** Окно редактирования групп будет закрыто, изменения появятся в Комплексе.

2. Удаление группы. Для удаления:

а. Над панелью с группами сканеров в левой части страницы нажмите **Редактировать**.

► **Результат шага:** появится окно **Редактирование групп сканеров**.

б. Нажмите кнопку  напротив группы, которую необходимо удалить.

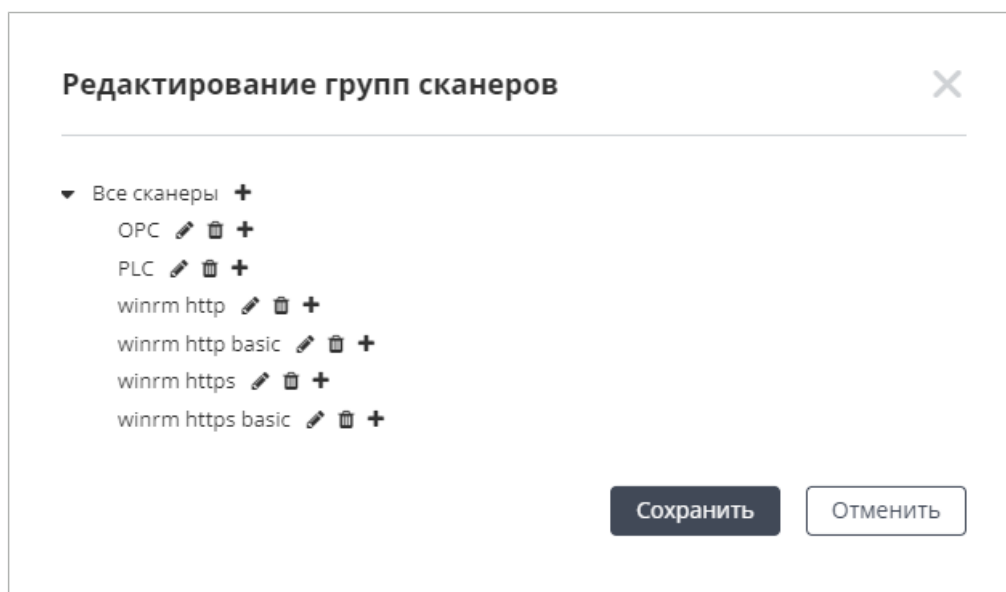


Рис. 191. Окно «Редактирование групп сканеров»

► **Результат шага:** Группа сканеров будет удалена, но данные изменения не будут сохранены до нажатия **Сохранить** в окне редактирования групп сканеров.

в. При необходимости измените другие группы сканеров.

г. В окне «Редактирование групп сканеров» нажмите **Сохранить**.

► **Результат шага:** Появится предупреждение о неизменности задач сбора данных в результате изменения состава групп. Это значит, что удаляемые группы останутся в задачах сбора данных, если такие были созданы. Для возобновления периодического сбора измените или создайте задачи заново, в том числе при помощи копирования.

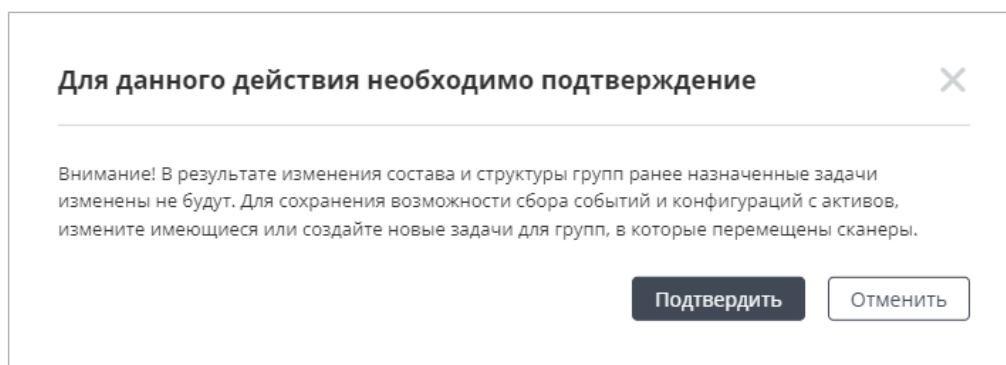


Рис. 192. Окно подтверждения изменений групп

д. Нажмите **Подтвердить**.

8.2.5. Добавление сетевых атрибутов активу с помощью сканера сбора данных по SNMP

Если на активе настроен доступ по протоколу SNMP, с него возможно получить конфигурацию подключенных сетевых интерфейсов. Полученную конфигурацию можно использовать, чтобы автоматически назначить активу новые сетевые атрибуты.



Внимание:

Чтобы Комплекс мог добавлять сетевые атрибуты из конфигурации, ее необходимо собрать сканерами SNMP, которые содержат Python-скрипты с ключами `ip_for_iface` и `mac_for_iface`.

Чтобы назначить активу сетевые атрибуты из конфигурации:

1. Убедитесь, что в операционной системе сенсора, который будет собирать данные с актива, присутствует директория `/usr/share/udv/snmp-connector/snmp_mibs` и она содержит необходимые MIB-словари.
2. Загрузите в Комплекс сканеры сбора конфигурации интерфейсов актива по протоколу SNMP и добавьте их в группу.



Подсказка:

См. подробнее в разделах [Настройка сканеров сбора данных](#) и [Импорт сканеров и их групп](#).

3. Создайте и привяжите к активу учетные данные для сбора конфигурации по протоколу SNMP (в качестве тега укажите `community`, в качестве логина — значение параметра **community**).



Подсказка:

См. подробнее в разделах [Добавление учетных данных актива](#) и [Импорт учетных данных активов](#).

4. Выполните однократный сбор данных с актива с помощью сканера SNMP или создайте задачу сбора данных для периодического сбора данных по расписанию.



Подсказка:

См. подробнее в разделах [Однократный сбор данных](#) и [Управление задачами сбора данных](#).

5. Дождитесь завершения сбора данных и откройте полученную конфигурацию в карточке актива.
Подробнее см. в разделах [Карточка актива](#) и [Конфигурации актива](#).
6. На странице **Конфигурации актива** нажмите **Создать сетевые атрибуты**.

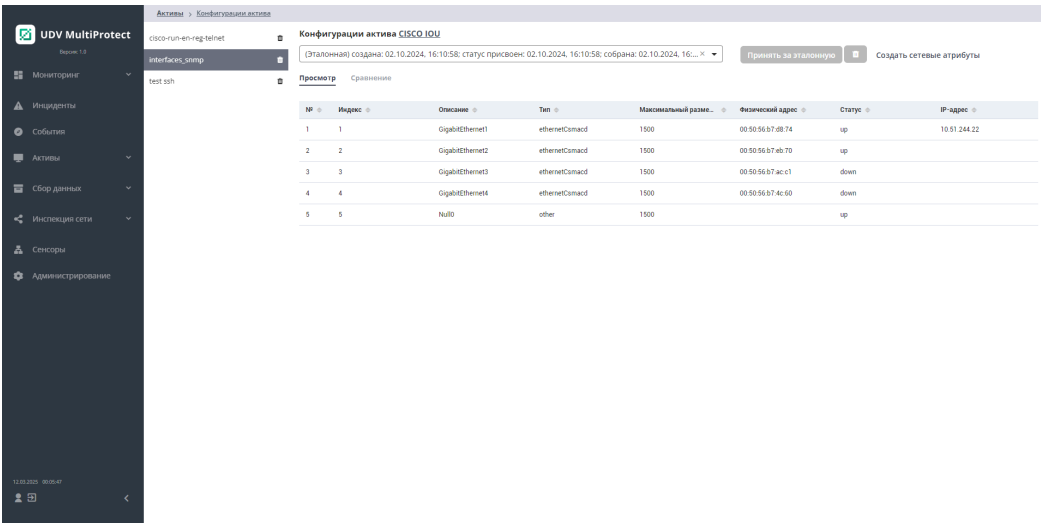


Рис. 193. Создание сетевых атрибутов со страницы конфигурации актива

► **Результат шага:**

- В правом верхнем углу появится статус *Сетевые атрибуты созданы*.
- Сетевые атрибуты, указанные в конфигурации, будут назначены текущему активу и удалены из других активов.



Внимание:

Если для активов удаленные сетевые атрибуты были единственными, такие активы будут удалены.

- Новым сетевым атрибутам актива будет назначен такой же сенсор, как у существующего интерфейса сбора данных. Присвоенный сенсор будет отображаться в поле **Сенсор** блока **Сетевые атрибуты** в карточке актива.

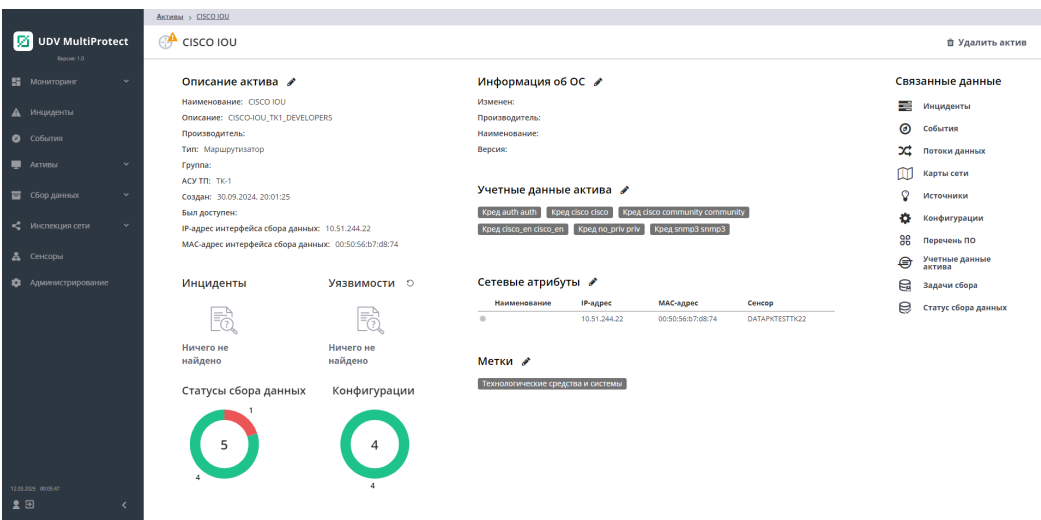


Рис. 194. Новые сетевые атрибуты в карточке актива

8.2.6. Сбор данных с активов

В этом разделе:

- Настройка активов для сбора данных
- Создание задачи сбора данных
- Управление задачами сбора данных
- Однократный сбор данных

Для сбора конфигураций и событий в веб-интерфейсе Комплекса доступна настройка задач сбора данных. Задачи позволяют сбор событий и конфигураций. Настройка задач производится на странице **Задачи сбора**.

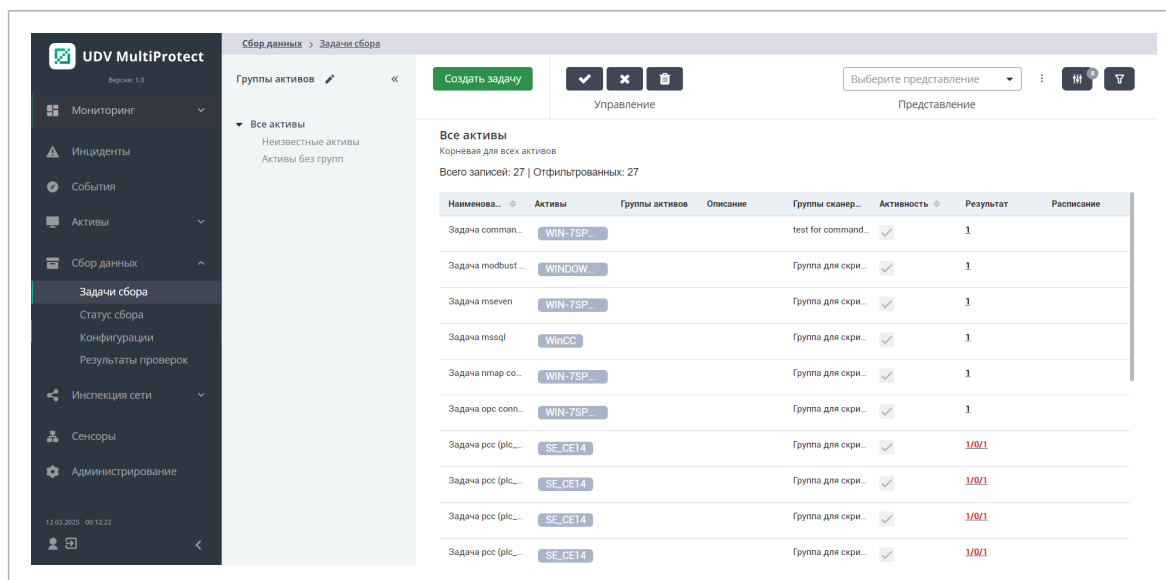


Рис. 195. Страница «Задачи сбора данных»

После выполнения задач доступен запуск сканеров в их составе по одному. Запуск сканеров осуществляется из карточки актива.

8.2.6.1. Настройка активов для сбора данных

Для сбора данных необходимо убедиться, что на активах добавлены и применены учетные данные и выбран сетевой интерфейс сбора данных.

Для подготовки актива к активному сбору данных:

1. Убедитесь, что учетные данные для доступа к активу были добавлены ранее. Для этого перейдите на страницу **Активы** → **Настройка активов** → **Учетные данные актива**.



Подсказка:

Подробнее о добавлении учетных данных см. в разделе «[Добавление учетных данных актива](#)».

2. Перейдите на страницу **Активы**.
3. Выберите из списка актив, для которого будет настроен сбор данных, и нажмите на его иконку или наименование.
 - **Результат шага:** откроется карточка актива.
4. Нажмите кнопку  напротив блока **Учетные данные актива**.

5. Установите чекбокс рядом с добавленной ранее учетной записью для привилегированного доступа к активу и нажмите кнопку **Сохранить**.

Настройка учетных данных

Создать

	Наименование	Тег	Логин		
☐	Кред admin	admin	admin		
☒	Кред admin Administrator	admin	Administrator		
☐	Кред admin root	admin	root		
☐	Кред auth	auth	HMAC_MD5		
☐	Кред cisco	cisco	cisco		
☐	Кред cisco community	community	public		
☐	Кред cisco_en	cisco_en	cisco		
☐	Кред mssql	mssql	winccladmin		
☐	Кред no_priv	priv	no_priv		
☐	Кред root	root	root		
☐	Кред snmp3	snmp3	cisco		
☐	Кред SSHv1_user1	cisco	user1		
☐	Кред SSHv1_user1_en	cisco_en	user1		

Сохранить

Отменить

Рис. 196. Окно «Настройка учетных данных»



Внимание:

Невозможно назначить активу учетные записи с одинаковыми тегами. При попытке назначения активу учетных записей с одинаковыми тегами появится уведомление *Ошибка: Выбор нескольких учетных данных с одинаковым тегом запрещен*

6. Если интерфейс для сбора данных с актива не был выбран ранее:
- Нажмите напротив блока **Сетевые атрибуты**;
 - В открывшемся окне **Редактирование сетевых атрибутов актива** выберите из списка интерфейс для сбора данных и отметьте параметр **Интерфейс для сбора данных** при помощи чекбокса в левой части таблицы.



Внимание:

У актива всегда должен быть интерфейс сбора данных — при попытке сохранения сетевых атрибутов актива при условии, что ни один атрибут не выбран в качестве интерфейса сбора, появится предупреждение: **Ошибка! Не выбран интерфейс сбора данных. Установите чекбокс напротив сетевых атрибутов для их выбора в качестве интерфейса сбора данных.**

Только один сетевой атрибут актива может быть выбран в качестве интерфейса сбора данных.



в. Нажмите кнопку (Сохранить изменения) напротив редактируемого сетевого интерфейса.

8.2.6.2. Создание задачи сбора данных

Для создания задачи сбора данных:

1. Перейдите на страницу **Задачи сбора**.

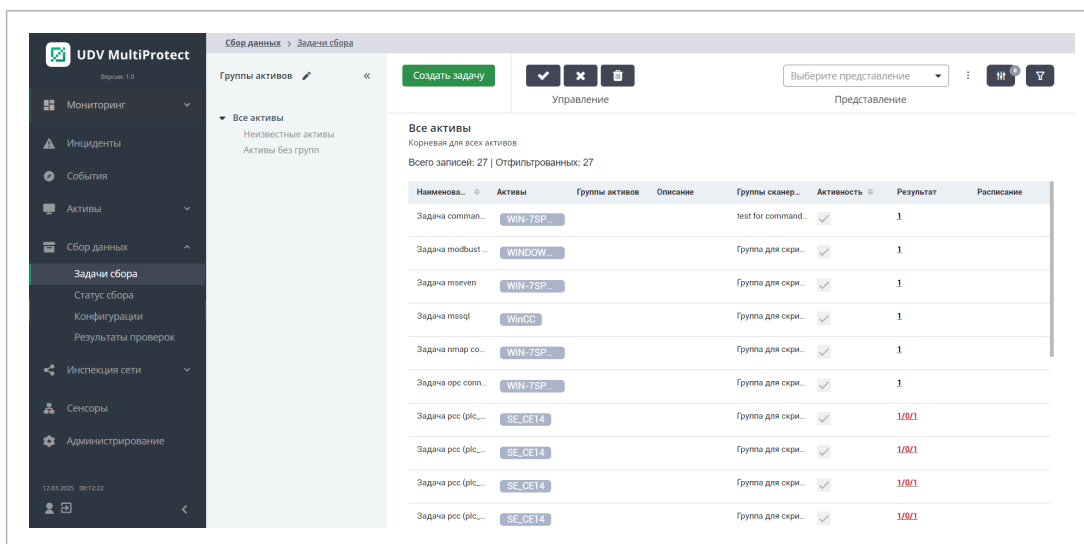


Рис. 197. Страница «Задачи сбора данных»

2. В верхней части страницы нажмите **Создать задачу**.

► **Результат шага:** Откроется окно **Создание задачи**.

3. Задайте следующие параметры создаваемой задаче:

- наименование;



Внимание:

Допускается вводить не более 255 символов.

- описание;
- чекбокс **Активность задачи** для запуска выполнения задачи по установленному расписанию;
- дату и время начала отсчета расписания;
- тип запуска: однократный для сбора в указанную дату и время, либо периодический для повторяющегося многократного сбора после указанной даты и времени;



Внимание:

При выборе периодического типа запуска первый сбор данных по задаче произойдет через указанный период в указанную дату. Например, если 01.01.2022 в 10.00 выбрать время запуска расписания **Сейчас** и периодический тип запуска с интервалом в один час (0 * * * *), то первый сбор данных произойдет 01.01.2022 в 11.00, второй — в 01.01.2022 в 12.00 и будет продолжаться, пока пользователь не удалит задачу.

- активы и (или) их группы;

**Внимание:**

При использовании групп активов сбор производится для всех вложенных групп. Например, при использовании в задаче группы активов **Windows** сбор данных будет также производиться с вложенных групп **Windows 7** и **Windows 10**.

- группы сканеров.

**Внимание:**

Не рекомендуется использовать группы, количество сканеров в которых превышает 30. Подробнее о группах сканеров см. в разделе [Группировка сканеров сбора данных](#).

Создание задачи

✕

Наименование *

Описание

☒ Активность задачи

Время запуска расписания * ⓘ

☐ Дата

Введите дату

📅

__ : __ : __

☒ Сейчас

Тип запуска *

☒ Однократный ⓘ

☐ Периодический

Раз в час; Раз в сутки; Раз в неделю

Обязательно заполните хотя бы одно из полей "Активы" или "Группы активов"

Активы *

Выберите активы

Группы активов *

Не выбрано

Группы сканеров *

Не выбрано

Создать

Отменить

Рис. 198. Окно «Создание задачи»

4. Нажмите **Создать**.

► **Результат шага:** Состояние сбора данных будет отображаться на странице **Статус сбора**, а также на странице **Задачи сбора**.



Подсказка:

При возникновении ошибок см. раздел «Просмотр статуса сбора данных».

8.2.6.3. Управление задачами сбора данных

Для управления задачами сбора конфигураций и событий веб-интерфейсе Комплекса предусмотрены следующие возможности:

1. Редактирование задачи сбора данных.



Внимание:

Редактирование доступно только для задач, содержащих расписание. Для задач с однократным типом запуска воспользуйтесь возможностью копирования.

Для изменения параметров задачи:

- а. Перейдите на страницу **Задачи сбора**.
- б. Наведите курсор на правую часть строки с задачей, которую необходимо изменить.
- в. Нажмите кнопку  (**Редактировать**).
- **Результат шага:** Откроется окно **Редактирование задачи**.
- г. Измените необходимые параметры задачи.

Рис. 199. Окно «Редактирование задачи»

- д. Нажмите **Сохранить**.
2. Копирование задачи сбора данных. Для копирования:
- Перейдите на страницу **Задачи сбора**.
 - Наведите курсор на правую часть строки с задачей, которую необходимо скопировать.
 - Нажмите  (**Копировать задачу**).
- **Результат шага:** появится окно **Копирование задачи**, в котором автоматически будет добавлена текущая дата и время в конце наименования задачи.
- г. При необходимости измените параметры задачи.

Копирование задачи

✕

Наименование *

Задача modbust tcp 05.09.2024 13:20:18

Описание

☒ Активность задачи

Время запуска расписания * ⓘ

☐ Дата

Введите дату

☒ Сейчас

Тип запуска *

☒ Однократный ⓘ

☐ Периодический

Раз в час; Раз в сутки; Раз в неделю

Обязательно заполните хотя бы одно из полей "Активы" или "Группы активов"

Активы *

✕ WINDOWS-XP_TK1_DEVELOPERS

✕ ▼

Группы активов *

Не выбрано ▼

Группы сканеров *

Не выбрано ▼

Создать

Отменить

Рис. 200. Окно «Копирование задачи»

д. Нажмите **Создать**.

► **Результат шага:** Задача будет запускаться с новыми параметрами. Если наименование задачи изменено, на странице **Статус сбора** новое наименование задачи будет отображаться только для новых процессов сбора.

3. Удаление задачи сбора данных. Для удаления:

- а. Перейдите на страницу **Задачи сбора**.
- б. Наведите курсор на правую часть строки с задачей, которую необходимо удалить.
- в. Нажмите кнопку  (**Удалить задачу**).

► **Результат шага:** Откроется окно подтверждения удаления задачи.

г. Введите обоснование действия и нажмите **Подтвердить**.

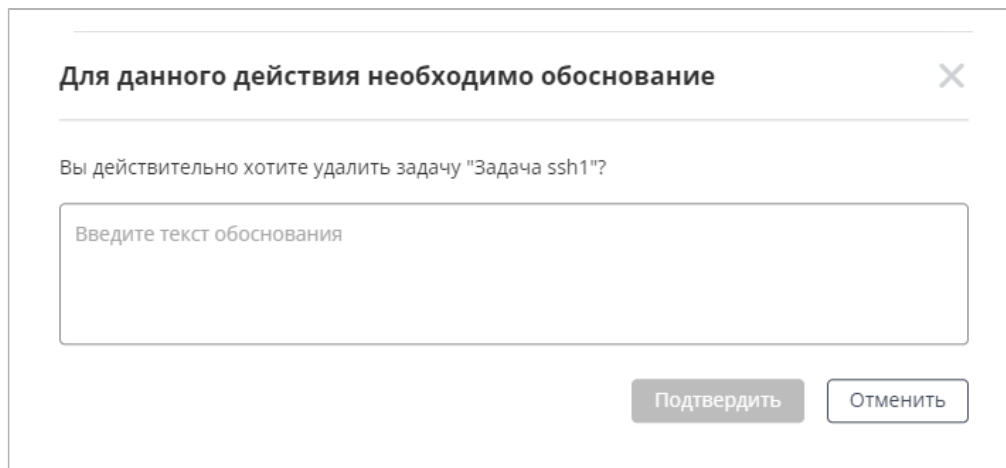


Рис. 201. Окно ввода обоснования удаления задачи

4. Групповое удаление задач сбора данных. Для удаления:

а. Перейдите на страницу **Задачи сбора**.

а. Нажмите кнопку  (**Удалить**).

► **Результат шага:** Откроется окно подтверждения удаления задач.

б. Введите обоснование действия и нажмите **Подтвердить**.

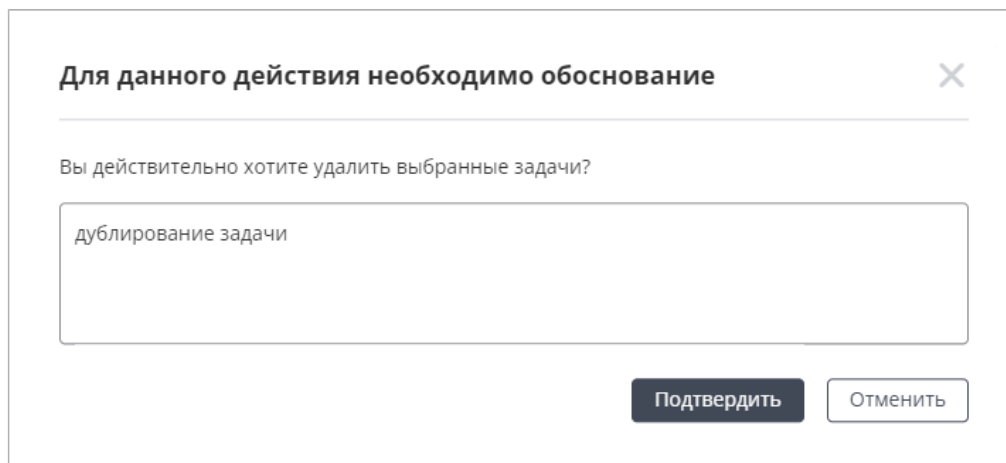


Рис. 202. Окно ввода обоснования удаления задачи

► **Результат шага:** Задача будет удалена. На странице **Статус сбора** сохранятся записи о процессах, завершенных в рамках удаленной задачи.

8.2.6.4. Однократный сбор данных

Для однократного запуска сбора данных с актива:

1. Перейдите на страницу **Администрирование** → **Сканеры**.
2. Наведите курсор на сканер, который планируется запустить.
3. Нажмите кнопку  (**Запустить сканирование**) справа от сканера.
 ► **Результат шага:** Откроется окно **Запуск сканера**.
4. В открывшемся окне выберите актив, с которого необходимо собрать данные.

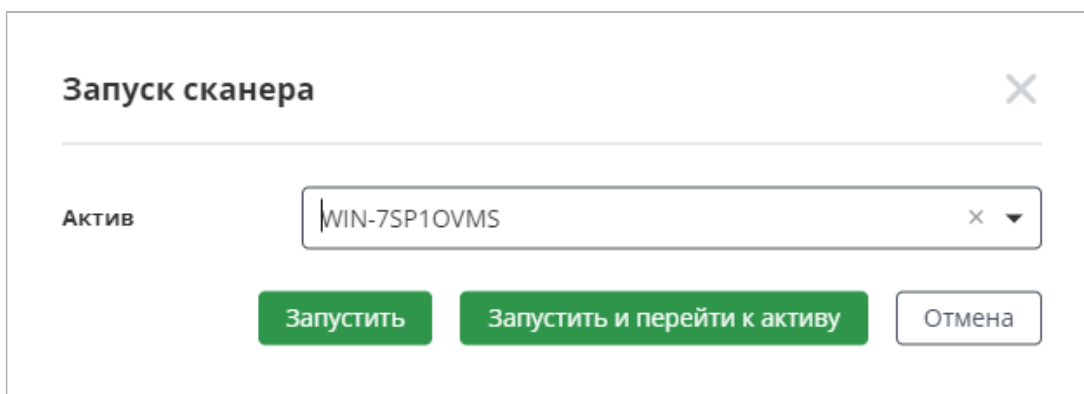


Рис. 203. Окно «Запуск сканера»

5. Нажмите **Запустить и перейти к активу**.
 ► **Результат шага:** Откроется карточка актива.
6. Нажмите на ссылку  **Статус сбора данных** в разделе **Связанные данные**.
 ► **Результат шага:** откроется страница **Статус сбора** с информацией о состоянии сбора данных выбранного актива.


Подсказка:

При возникновении ошибок сбора данных см. раздел Просмотр статуса сбора данных.

8.2.7. Просмотр статуса сбора данных

Если на каком-то этапе выполнения задач сбора данных возникают ошибки или сбор данных завершается не так, как ожидалось, краткие результаты сбора можно просмотреть на странице **Задачи сбора** в колонке **Результат**.

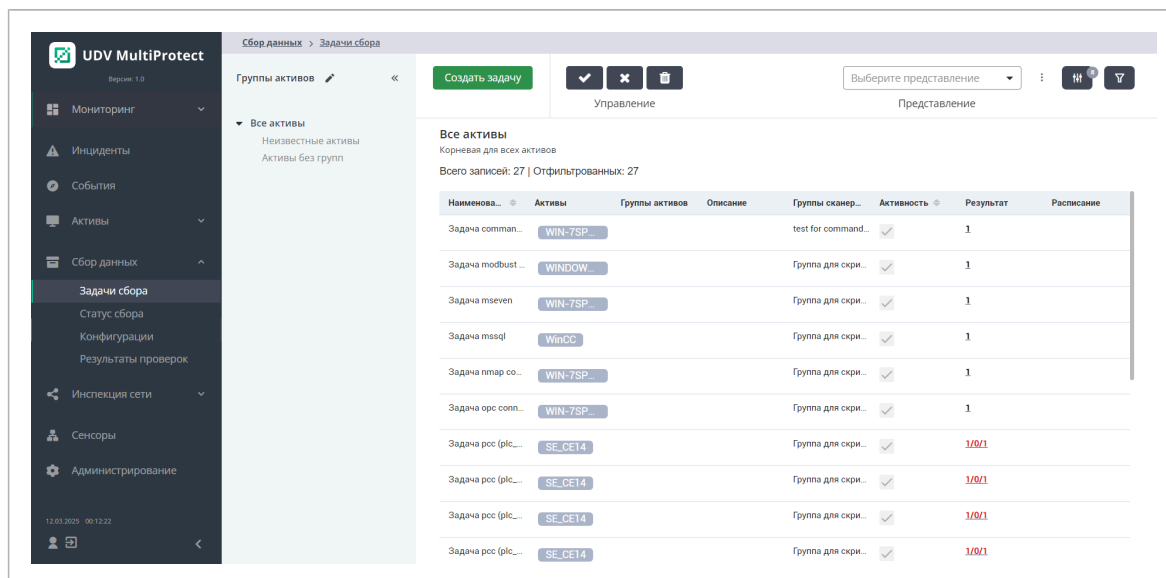


Рис. 204. Страница «Задачи сбора данных»

Значение, которое отображается в колонке, показывает, сколько было выполнено попыток сбора, и количество полученных результатов по типам. Подробнее см. в таблице ниже (Таблица 93. Обозначение цифр результатов задач).

Табл. 93. Обозначение цифр результатов задач

ПОРЯДКОВЫЙ НОМЕР ЦИФРЫ РЕЗУЛЬТАТА	НА-ЗВАНИЕ	ОБОЗНАЧЕНИЕ
1	На-значено	Общее количество процессов задачи сбора данных. Одним процессом задачи сбора данных считается пара сканер-актив
2	Ошибка со-единения	Количество процессов, которые не удалось завершить из-за проблем с соединением
3	Ошибка сбора	Количество процессов, которые не удалось завершить из-за проблем со сканером или Комплексом

В качестве примера приведем результат сбора данных 4/1/2. Такой результат будет говорить о том, что в задаче есть 4 процесса, один из которых не удалось завершить вследствие потери соединения с активом, два — из-за проблем со сканером.

В таблице на странице **Активы** в столбце **Результаты сканирования** можно просматривать статистику по попыткам сбора данных с цветной индикацией для каждого актива. Подробнее см. раздел Статусы активов.

При нажатии на результат происходит переход на страницу **Статус сбора**, где можно изучить подробности о статусах по каждому отдельному сканеру, который входит в задачу.

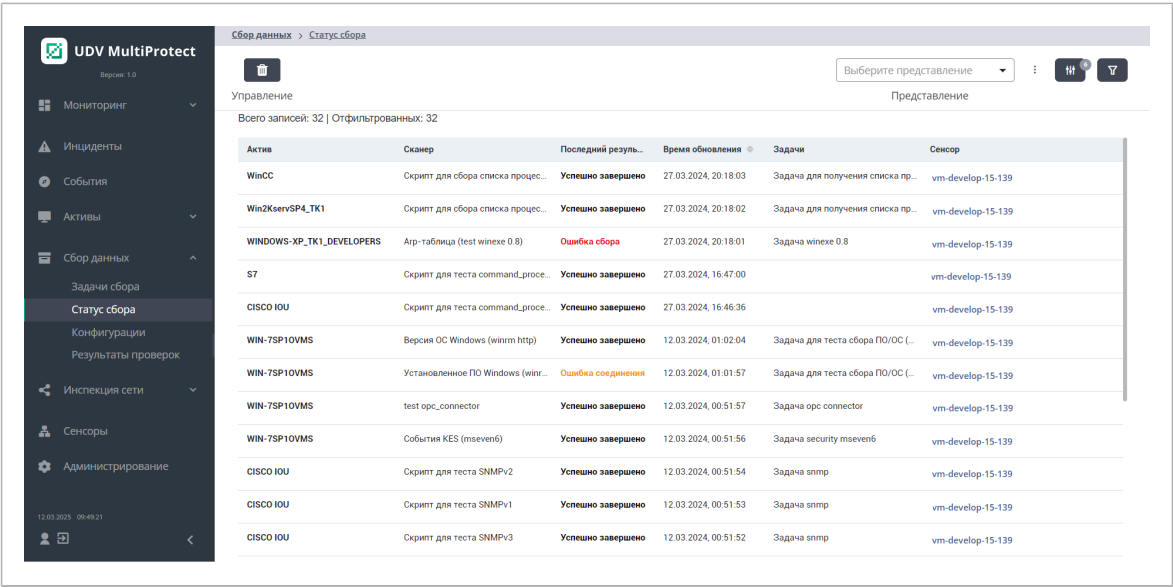


Рис. 205. Страница «Статус сбора»

На странице **Статус сбора** отображаются основные данные о попытке сбора: актив, сканер, последний результат, дата и время обновления, задачи, которым принадлежит сканер, сенсор, на котором выполняется сбор, время в очереди, длительность сбора.

По кнопке  можно настроить отображение информации о сборе данных по следующим фильтрам:

- **Задача**
- **Сканер**
- **Актив**
- **Последний результат**
- **Сенсор**
- **Дата и время обновления**

Задача

Выберите задачу

Сканер

Выберите сканер

Актив

Выберите активы

Последний результат

Выберите результат

Сенсор

Введите название сенсора

Дата и время обновления

От

До

Установить текущие сутки

Применить

Сбросить

Рис. 206. Фильтры на странице «Статус сбора»

В колонке **Последний результат** отображаются статусы сбора по каждому запуску сканеров. Типы статусов совпадают с представленными в цифровом виде на странице **Задачи сбора**. Перечень статусов, их обозначение и причины получения см. в таблице ниже (Таблица 94. Результаты сбора данных).

Табл. 94. Результаты сбора данных

РЕ-ЗУЛЬТАТ	ЦВЕТ	ОБО-ЗНАЧЕНИЕ	ОПИСАНИЕ	ВОЗМОЖНЫЕ ПРИЧИНЫ
Ошибка со-единения	Оранжевый	Ошибка со-единения	Не удалось подключиться к активу в течение периода, заданного в поле Максимальное время ожидания при создании сканера	Скорость передачи данных в сети не позволяет получить результат за заданное в переменной время. Актив недоступен: физически выключен, отсутствует доступ в сеть

Табл. 94. Результаты сбора данных

РЕ-ЗУЛЬТАТ	ЦВЕТ	ОБО-ЗНАЧЕНИЕ	ОПИСАНИЕ	ВОЗМОЖНЫЕ ПРИЧИНЫ
Ошибка сбора	Оранжевый	Ошибка сбора	Не удалось завершить непосредственно сбор данных	Не заданы корректные учетные данные. Ошибки в сканерах. Работоспособность Комплекса нарушена
Успешно завершено	Черный	Соответствует эталону	Соответствие собранной конфигурации эталонной	
		Успешный импорт событий	Обнаружены события	

При нажатии на результат, содержащий ошибки, открывается окно с описанием полученной ошибки.

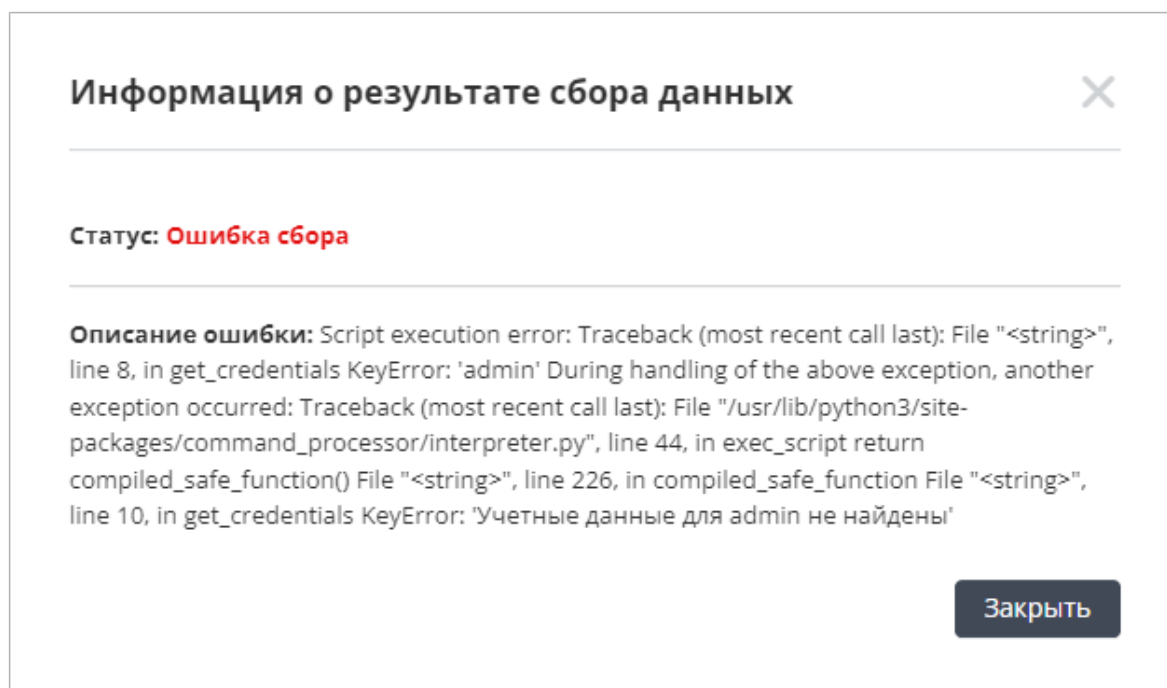


Рис. 207. Окно «Информация о результате сбора данных»

При необходимости неактуальные результаты сбора данных можно удалить. Для группового удаления воспользуйтесь фильтрами и нажмите  (**Удалить**) в верхней части страницы. Для удаления одного результата нажмите  (**Удалить статус сбора**) в строке с удаляемым результатом.

8.2.8. Работа с архивом изменений конфигурации актива

В этом разделе:

- Просмотр архива конфигураций
- Принятие конфигурации за эталонную
- Сравнение конфигурации с эталонной
- Удаление конфигураций

В результате выполнения сканеров, входящих в задачи сбора данных, формируются конфигурации. Просмотреть список таких сканеров можно при переходе из карточки актива на страницу **Активы** → **Конфигурации актива** (подробнее о задачах и результатах сбора данных см. в разделах Сбор данных с активов и Просмотр статуса сбора данных).

Конфигурации конкретных активов доступны к просмотру при переходе из карточки актива или со страницы → **Конфигурации** (подробнее см. раздел Просмотр архива конфигураций).

Все последние собранные конфигурации доступны на странице → **Конфигурации** (подробнее см. раздел Просмотр сводки конфигураций).

Список конфигураций пополняется в том случае, если вновь полученная конфигурация отличается от последней зафиксированной конфигурации.

8.2.8.1. Просмотр архива конфигураций

Для просмотра архива конфигураций вы можете воспользоваться двумя представленными способами:

1. Просмотр архива конфигураций, полученных с определенного актива. Для просмотра:
 - а. Перейдите на страницу **Активы** и нажмите на иконку или наименование актива.
▶ **Результат шага:** Откроется карточка актива.
 - б. В карточке актива нажмите на ссылку  **Конфигурации** в разделе **Связанные данные**.
▶ **Результат шага:** Откроется страница **Активы** → **Конфигурации актива**.
 - в. Выберите интересующую конфигурацию актива из списка в левой части страницы.

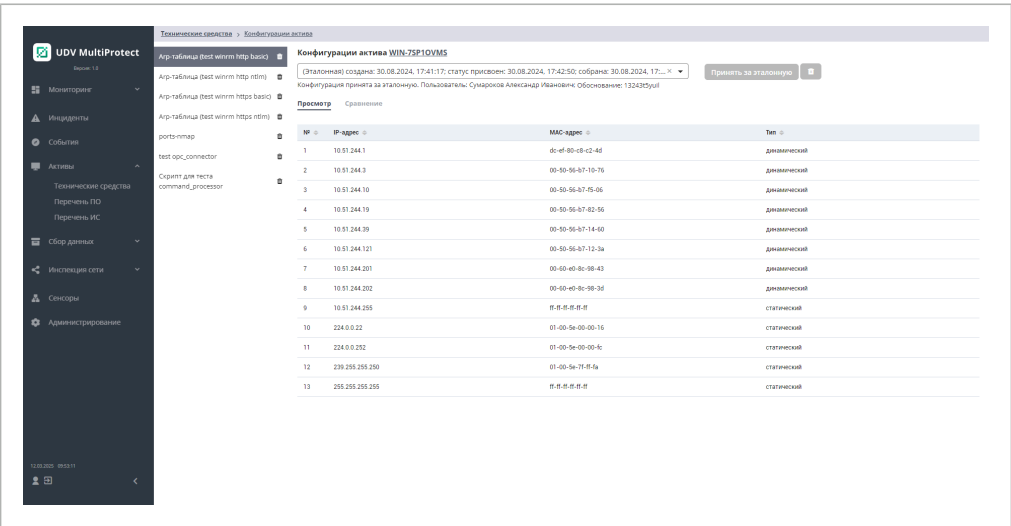


Рис. 208. Результат сбора данных с актива на странице «Конфигурации актива»

2. Просмотр конфигурации актива из списка всех конфигураций, собранных Комплексом. Для просмотра:

а. Перейдите на страницу → **Конфигурации**.

б. Воспользуйтесь фильтрами в левой части страницы по кнопке  для изменения выборки конфигураций.

в. Наведите курсор на строку с выбранной конфигурацией и нажмите кнопку  (**Просмотреть конфигурацию актива**).

► **Результат шага:** Откроется страница **Активы** → **Конфигурации актива** с выбранной конфигурацией актива.

8.2.8.2. Принятие конфигурации за эталонную

Для изменения эталонной конфигурации, полученной с помощью выбранного сканера:

1. Перейдите к конфигурациям актива со страницы **Активы** или из карточки актива. Для этого нажмите кнопку  **Конфигурации** в строке с названием сканера на панели **Результаты сбора данных**.
2. В верхней части страницы напротив названия конфигурации нажмите кнопку **Принять за эталонную**.

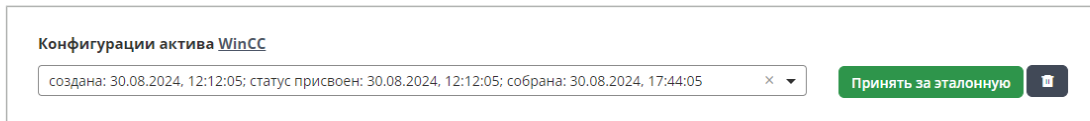


Рис. 209. Кнопка «Принять за эталонную» в списке конфигураций

3. Введите обоснование действия и нажмите **Подтвердить**.
 - **Результат шага:** После подтверждения под выпадающим списком конфигураций появится уведомление о принятии конфигурации за эталонную. Значок неэталонной конфигурации () перестанет отображаться возле названия сканера.

8.2.8.3. Сравнение конфигурации с эталонной

Для отслеживания изменений конфигурации актива, получаемой с помощью выбранного сканера:

- 1. Перейдите к конфигурациям актива из карточки актива. Для этого нажмите на ссылку  **Конфигурации** в разделе **Связанные данные**.
- 2. Выберите из списка конфигурацию, которая не является эталонной.
- 3. Под строкой выбора конфигураций нажмите **Сравнение**.
- 4. Выберите одну из доступных опций:

НАЗВАНИЕ ОПЦИИ	ОПИСАНИЕ
Таблицей	Сравнение в виде таблицы: в верхней части отображаются изменения текущей конфигурации, в нижней части — сравниваемые строки эталонной конфигурации
Строка под строкой	Сравнение с подсветкой изменений по строкам и конкретным символам в них
Два экрана	Отображение всех строк сравниваемых файлов друг напротив друга с подсветкой добавленных и удаленных строк, а также символов в них



Подсказка:

Индикация изменений между версиями конфигурации:

- Элементы, отсутствующие в открытой на странице конфигурации, но присутствующие в эталонной, имеют красный цвет.
- Элементы, появившиеся в открытой конфигурации, но отсутствующие в эталонной, имеют зеленый цвет.

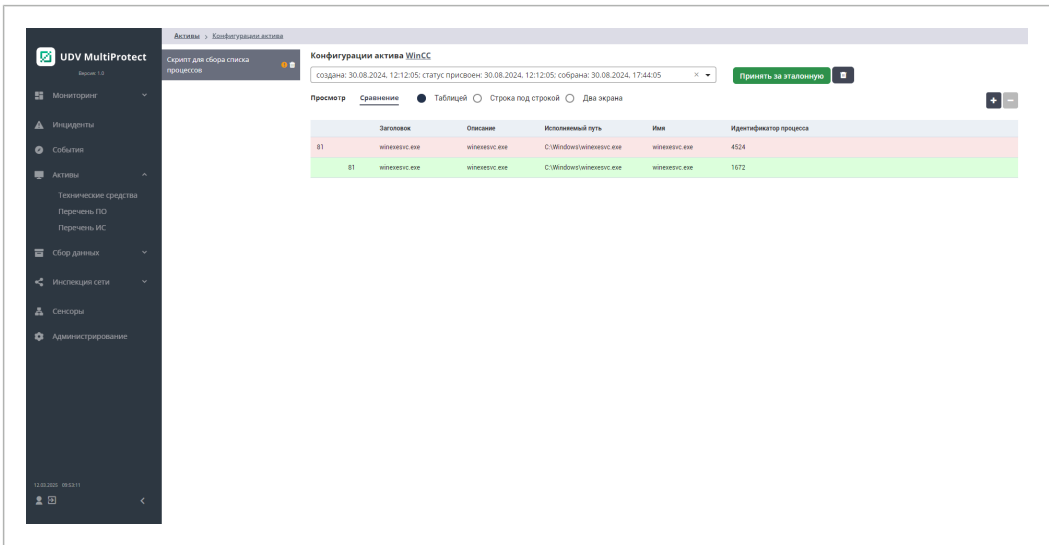


Рис. 210. Список изменений в конфигурации актива при сравнении с эталонной

- 5. Просмотрите список изменений в конфигурации.

**Подсказка:**

При необходимости воспользуйтесь кнопками  (**Показать еще по 5 окружающих строк**) и  (**Скрыть по 5 окружающих строк**), а также возможностью отображения спецсимволов.

**ОСТОРОЖНО:**

Если вы увидите сообщение **Текущая конфигурация совпадает с эталонной. В период между получением эталонной конфигурации и текущей было обнаружено отклонение. Убедитесь в легитимности изменений**, убедитесь в том, что изменения не были произведены злоумышленником.

8.2.8.4. Удаление конфигураций

Для удаления конфигураций вы можете воспользоваться следующими возможностями:

1. Удаление одной конфигурации. Для удаления:

 **Внимание:**

Удаление возможно только для тех конфигураций, которые не были приняты за эталонную.

- а. Перейдите к конфигурациям актива из карточки актива. Для этого нажмите на ссылку  **Конфигурации** в разделе **Связанные данные**.
- б. В верхней части страницы напротив названия конфигурации нажмите кнопку  (**Удалить**).

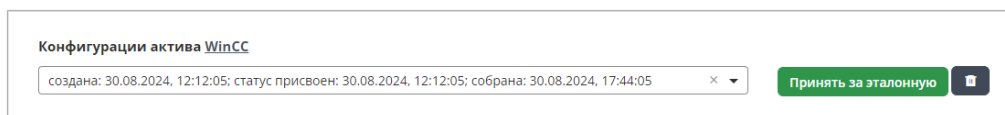


Рис. 211. Кнопка удаления неэталонной конфигурации

- **Результат шага:** Откроется окно ввода обоснования удаления конфигурации.

- в. Введите текст обоснования действия.

Для данного действия необходимо обоснование



Введите текст обоснования

Подтвердить

Отменить

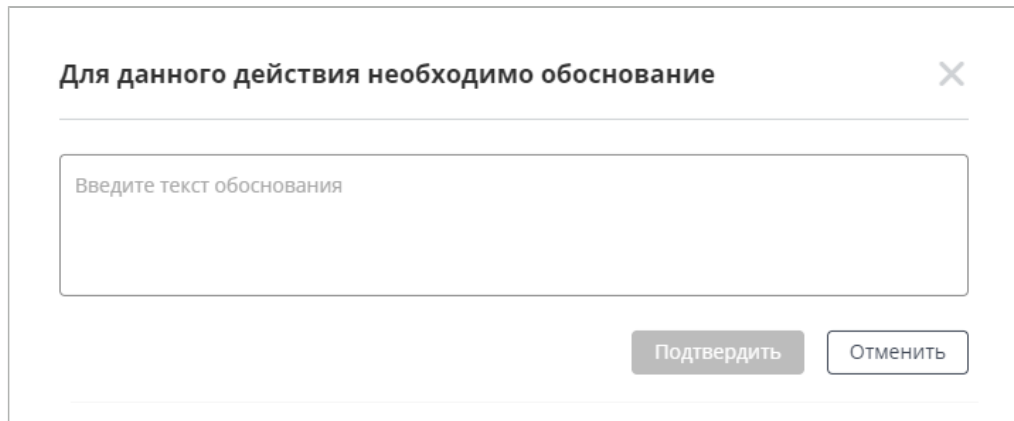
Рис. 212. Окно обоснования удаления неэталонной конфигурации

2. Удаление всех конфигураций, собранных сканером. Для удаления:

- а. Перейдите к конфигурациям актива из карточки актива. Для этого нажмите на ссылку  **Конфигурации** в разделе **Связанные данные**.
- б. Нажмите  (**Удалить конфигурации**) напротив названия сканера.

- **Результат шага:** Откроется окно ввода обоснования.

в. Введите обоснование действия и нажмите **Подтвердить**.



The image shows a modal dialog box with a light gray background and a thin border. At the top, the title "Для данного действия необходимо обоснование" is displayed in bold black text, followed by a close button (X) in the top right corner. Below the title is a horizontal line. Underneath this line is a large, empty rectangular text input field with a light gray border. Inside the input field, the placeholder text "Введите текст обоснования" is visible in a light gray font. At the bottom right of the dialog, there are two buttons: "Подтвердить" (Confirm) and "Отменить" (Cancel). The "Подтвердить" button is a solid gray button with white text, while the "Отменить" button is a white button with a gray border and gray text. A horizontal line is located at the very bottom of the dialog box.

Рис. 213. Окно ввода обоснования удаления конфигураций актива

8.3. Настройка активного сбора событий

События — это списки, которые Комплекс собирает с активов. Например, журналы Windows.

Просмотр событий, полученных в результате выполнения сканеров, доступен на странице **События**.

Для настройки активного сбора событий с актива:

1. Импортируйте или создайте сканеры для сбора событий.



Подсказка:

См. подробнее в разделах [Импорт сканеров и их групп](#), [Создание сканеров сбора данных](#), [Управление сканерами сбора данных](#).

2. Добавьте сканеры в группы.



Подсказка:

См. подробнее в разделе [Группировка сканеров сбора данных](#).

3. Убедитесь, что объектам защиты назначены учетные данные.



Подсказка:

См. подробнее в разделе [Настройка активов для сбора данных](#).

4. Выполните сбор данных одним из доступных способов:

- однократный сбор сканером сбора данных;



Подсказка:

См. подробнее в разделе [Однократный сбор данных](#).

- сбор данных задачами сбора данных.



Подсказка:

См. подробнее в разделах [Создание задачи сбора данных](#), [Управление задачами сбора данных](#).

5. Убедитесь, что сбор данных произведен успешно.



Подсказка:

См. подробнее в разделе [Просмотр статуса сбора данных](#).

6. Ознакомьтесь с результатами сбора.

8.4. Настройка сбора данных об операционной системе и установленном ПО

В веб-интерфейсе Комплекса доступен сбор данных о производителе актива и об установленных на активе операционной системе и программном обеспечении.

Сбор данных о производителе и операционной системе

Для сбора общей информации о производителе и операционной системе предусмотрены следующие возможности:

- 1. Автоматическое определение данных о производителе на основе первых трех октетов MAC-адреса. Собранная информация отображается в поле **Производитель** блока **Описание актива** в карточке.

Подсказка:

Для ознакомления с возможностью определения производителя на основе трафика см. пункт 4.b раздела [Редактирование активов](#).

- 2. Определение производителя, названия операционной системы и ее версии по результатам работы сканеров. Собранная информация отображается в блоке **Информация об ОС** в карточке.
- 3. Указание информации о производителе и операционной системе актива вручную.

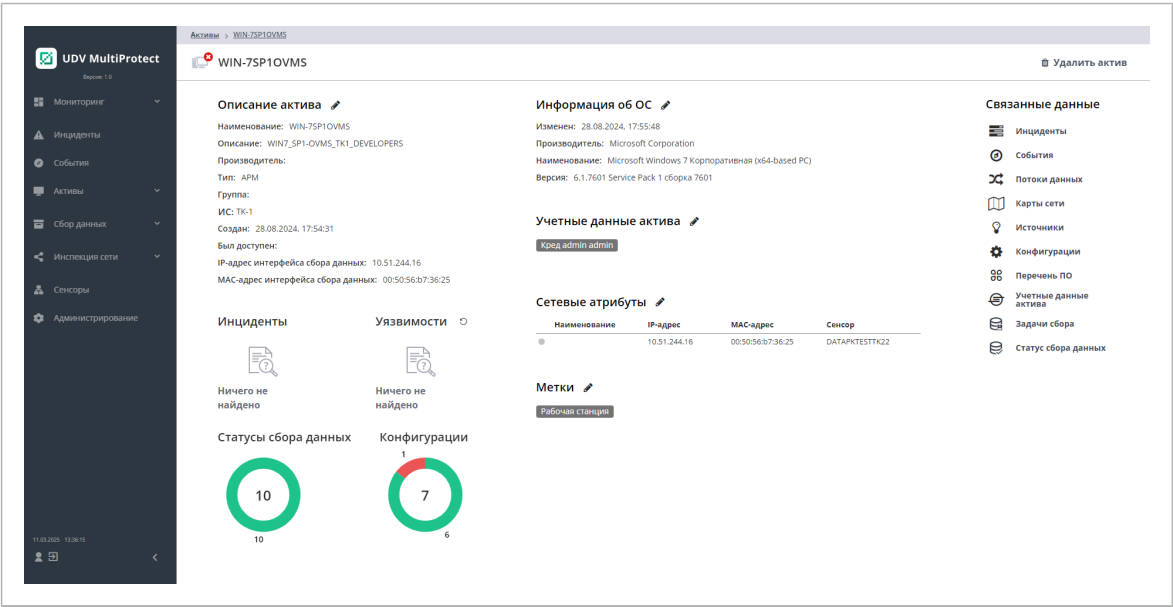


Рис. 214. Карточка актива

Тип информации, сохраняемой в блоке **Информация об ОС**, зависит от настроенного типа актива: для активов с типом **ПЛК** собирается и сохраняется информация о прошивке, для остальных активов — информация об операционной системе.

Тип актива и информация в блоке **Информация об ОС** влияют на список уязвимостей, которые возможно обнаружить на активе с помощью справочников Common Vulnerabilities and Exposures и Common Platform Enumeration:

- для активов с типом **ПЛК** поиск уязвимостей выполняется только для прошивки. Поиск уязвимостей ПО и ОС не выполняется;
- для остальных активов поиск уязвимостей выполняется для ОС и ПО, но не выполняется для прошивки.

При изменении типа актива на **Инженерное оборудование** или обратно необходимо обновить информацию в блоке **Информация об ОС**.

При повторном сборе информации об ОС предыдущие данные удаляются и заменяются новыми. Автообновление данных об ОС можно отключить в карточке актива — см. пункт 6 раздела «Редактирование активов».

Сбор данных о программном обеспечении

Для сбора информации об установленном на активах программном обеспечении могут быть использованы сканеры сбора данных. После сбора список отображается на странице . Получить перечень ПО для определенного актива можно с помощью фильтра по наименованию актива либо перейдя к списку из карточки актива по ссылке **Перечень ПО**.

При повторном сборе информации о ПО предыдущие данные удаляются и заменяются новыми.

Версия: 1.0

Мониторинг

Статус защищенности

Инциденты

События

Активы

Технические средства

Перечень ПО

Перечень ИС

Сбор данных

Инспекция сети

Сенсоры

Администрирование

12.05.2025 10:14:08

Исследование активов > Перечень ПО

Управление

Выберите представление

Представление

Всего записей: 110 | Отфильтрованных: 110

Производитель ПО	Наименование ПО	Версия ПО	Обновление
Zabbix SIA	Zabbix Agent (64-bit)	4.2.8.2400	28.08.2024, 18:05:33
Microsoft Corporation	Microsoft Visual C++ 2008 Redistributable - x64 9.0.30729.4148	9.0.30729.4148	28.08.2024, 18:05:33
Microsoft Corporation	Microsoft Visual C++ 2019 X64 Additional Runtime - 14.24.28127	14.24.28127	28.08.2024, 18:05:33
Microsoft Corporation	Hotfix for Microsoft Visual Studio 2007 Tools for Applications - ENU (KB947540)	1	28.08.2024, 18:05:33
VMware, Inc.	VMware Tools	11.1.1.16303738	28.08.2024, 18:05:33
Microsoft Corporation	Файлы поддержки установки SQL Server 2008 (на русском языке)	10.0.1600.22	28.08.2024, 18:05:33
Oracle Corporation	Java Auto Updater	2.8.221.11	28.08.2024, 18:05:33
Microsoft Corporation	Службы синхронизации контроля версий Microsoft SQL Server	10.0.1600.22	28.08.2024, 18:05:33
Microsoft Corporation	Microsoft(R) MSXML 3.0 SP1	8.110.7601.17988	28.08.2024, 18:05:33
Microsoft Corporation	Microsoft(R) .NET Framework	4.0.30319.1	28.08.2024, 18:05:33
The OpenSSL Project, http://www.openssl.org/	The OpenSSL Toolkit	1.0.2n	28.08.2024, 18:05:33
Microsoft Corporation	Microsoft Visual C++ 2013 Redistributable (x86) - 12.0.30501	12.0.30501.0	28.08.2024, 18:05:33
Microsoft Corporation	Microsoft SQL Server 2008 Database Engine Services	10.0.1600.22	28.08.2024, 18:05:33
Microsoft Corporation	Windows(R) Internet Explorer	10.00.9200.16521	28.08.2024, 18:05:33
Microsoft Corporation	Microsoft SQL Server	10.0.1600.22	28.08.2024, 18:05:33
Microsoft Corporation	Средства работы с запросами SQL Server Compact 3.5 SP1 (jvc)	3.5.5602.0	28.08.2024, 18:05:33
Microsoft Corporation	Microsoft Visual Studio 2008 Remote Debugger CO - RUS	9.0.21022.08	28.08.2024, 18:05:33
MySQL AB	MySQL Server 5.0	5.0.41	28.08.2024, 18:05:33
Oracle Corporation	Java(TM) Platform SE Bu221	8.0.2210.11	28.08.2024, 18:05:33

Рис. 215. Страница «Перечень ПО»

8.4.1. Запуск сбора данных об операционной системе и установленном ПО

Для настройки возможности сбора подробной информации об операционной системе и установленном ПО актива:

1. Импортируйте или создайте сканеры для сбора данных об ОС и ПО с типами **Версия ОС** и **Установленное ПО**.



Подсказка:

См. подробнее в разделах **Импорт сканеров и их групп**, **Создание сканеров сбора данных**, **Управление сканерами сбора данных**.



Внимание:

При повторном сборе информации об ОС или ПО предыдущие данные удаляются и заменяются новыми. Автообновление данных об ОС можно отключить в карточке актива — см. пункт 6 раздела Редактирование активов.

2. Добавьте сканеры в группы.



Подсказка:

См. подробнее в разделе [Группировка сканеров сбора данных](#).

3. Убедитесь, что объектам защиты назначены учетные данные.



Подсказка:

См. подробнее в разделе [Настройка активов для сбора данных](#).

4. Выполните сбор данных одним из доступных способов:

- однократный сбор сканером сбора данных;



Подсказка:

См. подробнее в разделе [Однократный сбор данных](#).

- сбор данных задач сбора данных.



Подсказка:

См. подробнее в разделах [Создание задачи сбора данных](#), [Управление задачами сбора данных](#).

5. Убедитесь, что сбор данных произведен успешно.



Подсказка:

См. подробнее в разделе [Просмотр статуса сбора данных](#).

6. Ознакомьтесь с результатами сбора.

► **Результат шага:**

- Результаты сбора данных об ОС отображаются в карточке актива в блоке **Информация об ОС**.
- Результаты сбора данных об установленном ПО отображаются на странице .

9. Поиск уязвимостей и проверка соответствия требованиям информационной безопасности

С целью контроля и оценки состояния защищенности активов в Комплексе реализованы следующие функции:

1. Анализ уязвимостей активов. Реализуется двумя способами:
 - Проверка на уязвимости выбранной группы ПО с помощью загруженных в Комплекс справочников OVAL (OVAL). Предварительный сбор данных о ПО, установленном на активе, не требуется.
 - Предварительный сбор данных о ПО и ОС, установленных на активе, и проверка полученного списка на уязвимости с помощью загруженных в Комплекс справочников CVE (CVE), CPE (CPE) и Банк данных угроз безопасности информации ФСТЭК России (Банк данных угроз безопасности информации ФСТЭК России).
2. Контроль соответствия отдельных настроек и конфигураций активов требованиям информационной безопасности. Реализуется только с помощью OVAL.

Табл. 95. Сравнение функций поиска уязвимостей в Комплексе

СРАВНИВАЕМАЯ ХАРАКТЕРИСТИКА	CVE И CPE	OVAL
Возможности	Поиск уязвимостей	Поиск уязвимостей Контроль соответствия конфигураций активов требованиям информационной безопасности
Раздел документации	Поиск уязвимостей ПО и ОС в базах CVE, CPE и БДУ ФСТЭК России	Проверки на уязвимости и соответствие требованиям информационной безопасности с помощью OVAL
Страница запуска	Активы Карточка актива	Результаты проверок
Результат	Отчет с результатами поиска уязвимостей формата *.csv в окне Запуск поиска уязвимостей Диаграмма и список уязвимостей в карточке актива Статистика по обнаруженным уязвимостям на странице Активы Отчет сопоставления ОС и ПО со справочником CPE формата *.csv на странице  по кнопке 	На странице Результаты проверки напротив успешно выполненной проверки: таблица результатов проверок по кнопке  (Просмотреть результаты) отчет формата pdf или xlsx по кнопке  (Создать отчет)
Ограничения по запуску	Нет ограничений — каждый актив опрашивается один раз для получения списка	Рекомендуется запускать в технологические окна — для выполнения проверки

Табл. 95. Сравнение функций поиска уязвимостей в Комплексе

СРАВНИВАЕМАЯ ХАРАКТЕРИСТИКА	CVE И CPE	OVAL
	ОС или ПО, а поиск уязвимостей выполняется в Комплексе в фоновом режиме	каждый актив опрашивается несколько раз, что может кратковременно влиять на его доступность и быстродействие

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

Пользователи с ролями **Администратор** и **Инженер** могут выполнить поиск уязвимостей активов с помощью справочников CVE и CPE в следующем порядке:

1. Убедиться в актуальности импортированных справочников CVE, CPE и Банк данных угроз безопасности информации ФСТЭК России — подробнее см. раздел [Проверка актуальности справочников поиска уязвимостей](#).
2. Импортировать справочники CVE, CPE — подробнее см. раздел [Импорт справочников CVE и CPE и файла сопоставления ПО с CPE](#).
3. При необходимости импортировать справочник Банк данных угроз безопасности информации ФСТЭК России — подробнее см. раздел [Импорт справочника БДУ ФСТЭК России](#).



Подсказка:

Импорт справочника Банк данных угроз безопасности информации ФСТЭК России позволяет добавить в отчеты о проверках дополнительную информацию об уязвимостях, но не обязателен для успешного выполнения проверок.

4. Получить с актива информацию об установленных на нем ОС и ПО с помощью сканеров с типами **Версия ОС** и **Установленное ПО** — подробнее см. раздел [Запуск сбора данных об операционной системе и установленном ПО](#).



Внимание:

Полученная информация об ОС сохраняется в блоке **Информация об ОС карточки актива** (подробнее см. раздел [Редактирование активов](#)).

Тип информации, сохраняемой в блоке **Информация об ОС**, зависит от настроенного типа актива: для активов с типом **ПЛК** собирается и сохраняется информация о прошивке, для остальных активов — информация об операционной системе.

Тип актива и информация в блоке **Информация об ОС** влияют на список уязвимостей, которые возможно обнаружить на активе с помощью справочников CVE и CPE:

- для активов с типом **ПЛК** поиск уязвимостей выполняется только для прошивки. Поиск уязвимостей ПО и ОС не выполняется;
- для остальных активов поиск уязвимостей выполняется для ОС и ПО, но не выполняется для прошивки.

При изменении типа актива на **Инженерное оборудование** или обратно необходимо обновить информацию в блоке **Информация об ОС**.

5. Запустить поиск уязвимостей. Поиск уязвимостей можно запустить для одного или нескольких активов разными способами — подробнее см. раздел [Запуск поиска уязвимостей в базах CVE, CPE и БДУ ФСТЭК России](#). На данном этапе Комплекс:
- Сопоставляет наименования и версии ОС и ПО, полученные с актива, со справочником CPE.
 - Сравнивает результаты сопоставления со справочниками CVE и Банк данных угроз безопасности информации ФСТЭК России.

Результаты поиска уязвимостей с помощью CVE, CPE и Банк данных угроз безопасности информации ФСТЭК России можно просмотреть в Комплексе несколькими способами:

- Скачать отчет формата *.csv, который будет содержать список уязвимостей активов, для которых выполнялся последний поиск. Подробнее см. раздел [«Запуск поиска уязвимостей в базах CVE, CPE и БДУ ФСТЭК России»](#).
- Просмотреть диаграмму и список уязвимостей в **карточке актива**, для которого когда-либо выполнялся поиск.
- Просмотреть статистику по обнаруженным уязвимостям для каждого актива. Статистика отображается на странице **Активы** в столбце **Уязвимости**. Подробнее см. раздел [«Статусы активов»](#).
- Скачать отчет формата *.csv, который будет содержать результаты сопоставления ОС и ПО со справочником CPE. Подробнее см. раздел [«Выгрузка отчета по результатам сопоставления собранного ПО со справочником CPE»](#).



ОСТОРОЖНО:

Точность, с которой для ПО подобран элемент CPE, указывается в отчете в виде относительного коэффициента **map_confidence** в диапазоне от 0 до 1.

Минимальное значение относительного коэффициента **map_confidence** для подбора элемента CPE = 60% или 0,6. При меньшем значении подбор CPE для ПО выполняться не будет.

9.1.1. Проверка актуальности справочников поиска уязвимостей

Перед импортом справочников ПО и уязвимостей (CPE, CVE и Банк данных угроз безопасности информации ФСТЭК России) и файла сопоставления собранного ПО со справочником CPE проверьте актуальность загруженных справочников по дате их последнего обновления. Для этого:

- Перейдите на страницу **Активы**.
- При помощи чекбокса выберите любой актив.
- Нажмите кнопку  (**Запустить поиск уязвимостей**).

► **Результат шага:** появится окно запуска поиска уязвимостей с датами последнего обновления баз.

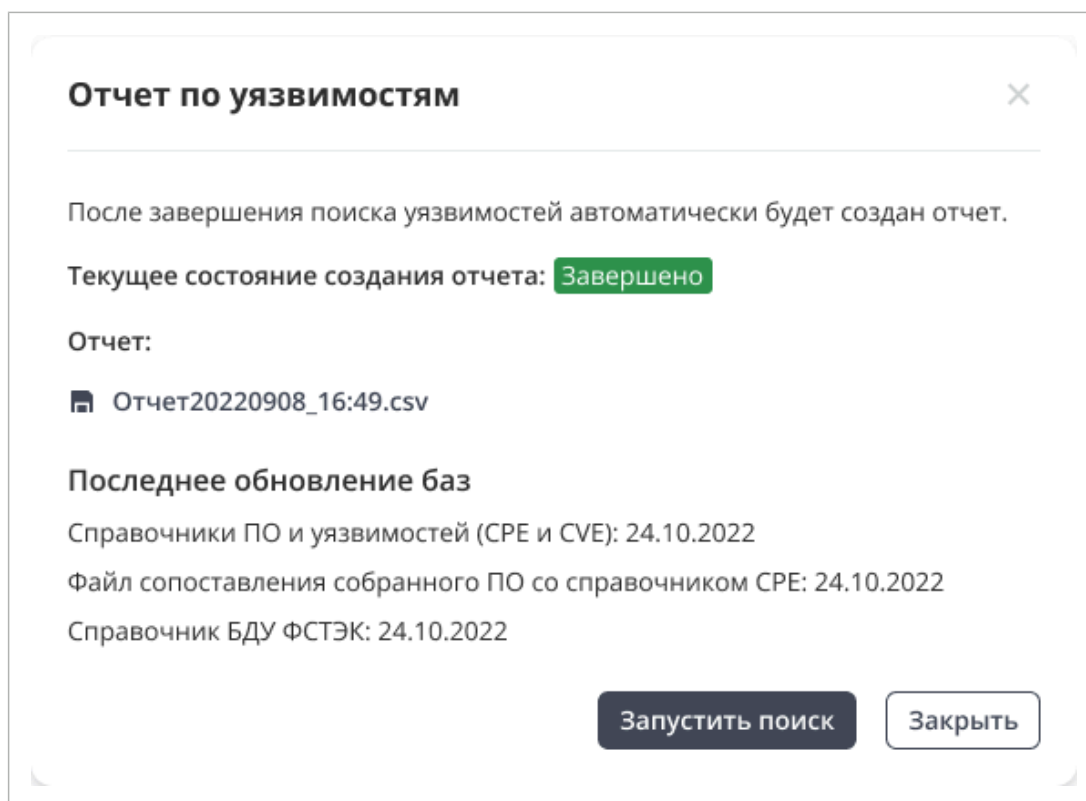


Рис. 216. Окно запуска поиска уязвимостей

 **Внимание:**

Если справочник не был загружен ранее, вместо даты будет символ -.

9.1.2. Импорт справочников CVE и CPE и файла сопоставления ПО с CPE



Внимание:

Невозможно экспортировать справочники ПО и уязвимостей (CVE и CPE) и файл сопоставления собранного сканерами ПО со справочником CPE.

9.1.2.1. Импорт справочников ПО и уязвимостей (CPE и CVE)

Для импорта справочников CPE и CVE:

1. Перейдите на страницу **Администрирование** → **Основные настройки** → **Импорт и экспорт**.
2. На панели **Обнаружение уязвимостей (CVE)** в строке **Справочники ПО и уязвимостей (CPE и CVE)** нажмите кнопку (**Импортировать**).
3. В открывшемся окне укажите расположение импортируемого файла `cve_cpe_db_[дата].tar.bz` и подтвердите выбор.

► **Результат шага:** Будет запущен процесс импорта: в правом верхнем углу появится уведомление **Запущен импорт справочника**, а под заголовком **Результат последнего импорта** будет символ **-**.



Подсказка:

Операции импорта являются фоновыми — со страницы можно безопасно уходить.

4. Дождитесь загрузки справочника и убедитесь, что файл был успешно загружен.
 - Если файл импортирован успешно, в правом верхнем углу под заголовком **Результат последнего импорта** появится уведомление: **Успешно**.
 - Если произошла ошибка, в правом верхнем углу под заголовком **Результат последнего импорта** появится уведомление **Ошибка**. Для просмотра информации об ошибке нажмите ссылку **Подробнее** в подсказке рядом с уведомлением.

9.1.2.2. Импорт файла сопоставления собранного сканерами ПО со справочником CPE

Для импорта файла сопоставления собранного сканерами ПО со справочником CPE:

1. Перейдите на страницу **Администрирование** → **Основные настройки** → **Импорт и экспорт**.
2. На панели **Обнаружение уязвимостей (CVE)** в строке **Сопоставление собранного сканерами ПО со справочником CPE** нажмите кнопку (**Импортировать**).
3. В открывшемся окне укажите расположение импортируемого файла `mappings_[дата].tar.bz2` и подтвердите выбор.

► **Результат шага:** Будет запущен процесс импорта: в правом верхнем углу появится уведомление **Запущен импорт справочника**, а под заголовком **Результат последнего импорта** будет символ **-**.



Подсказка:

Операции импорта являются фоновыми — со страницы можно безопасно уходить.

4. Убедитесь, что файл был успешно загружен.

- Если файл импортирован успешно, в правом верхнем углу под заголовком **Результат последнего импорта** появится уведомление: **Успешно**.
- Если произошла ошибка, в правом верхнем углу под заголовком **Результат последнего импорта** появится уведомление **Ошибка**. Для просмотра информации об ошибке нажмите ссылку **Подробнее** в подсказке ⓘ рядом с уведомлением.

9.1.3. Импорт справочника БДУ ФСТЭК России



Подсказка:

Актуальный справочник Банк данных угроз безопасности информации ФСТЭК России в формате *.xlsx можно скачать с [сайта БДУ ФСТЭК России](#) (см. ссылку **Скачать сведения об угрозах** внизу страницы).



Внимание:

Экспортировать справочник Банк данных угроз безопасности информации ФСТЭК России из Комплекса невозможно.

Для импорта справочника Банк данных угроз безопасности информации ФСТЭК России:

1. Перейдите на страницу **Администрирование** → **Основные настройки** → **Импорт и экспорт**.
2. На панели **Обнаружение уязвимостей (CVE)** в строке **Справочник БДУ ФСТЭК** нажмите кнопку  (**Импортировать**).
3. В открывшемся окне укажите расположение импортируемого файла формата *.xlsx и подтвердите выбор.
 - **Результат шага:** Будет запущен процесс импорта: в правом верхнем углу появится уведомление **Запущен импорт справочника**, а под заголовком **Результат последнего импорта** будет символ -.



Подсказка:

Операции импорта являются фоновыми — со страницы можно безопасно уходить.

4. Дождитесь загрузки справочника и убедитесь, что файл был успешно загружен.
 - Если файл импортирован успешно, в правом верхнем углу под заголовком **Результат последнего импорта** появится уведомление: **Успешно**.
 - Если произошла ошибка, в правом верхнем углу под заголовком **Результат последнего импорта** появится уведомление **Ошибка**. Для просмотра информации об ошибке нажмите ссылку **Подробнее** в подсказке  рядом с уведомлением.

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

9.1.4.1. Запуск поиска уязвимостей актива

Поиск уязвимостей для одного актива можно выполнить двумя способами:

- со страницы **Активы**;
- из карточки актива.

1. Для поиска уязвимостей актива со страницы **Активы**:

- а. Перейдите на страницу **Активы**.
- б. При помощи чекбокса выберите актив.
- в. Нажмите кнопку  (**Запустить поиск уязвимостей**).
- **Результат шага:** Откроется окно **Запуск поиска уязвимостей**.
- г. Нажмите **Запустить поиск**.

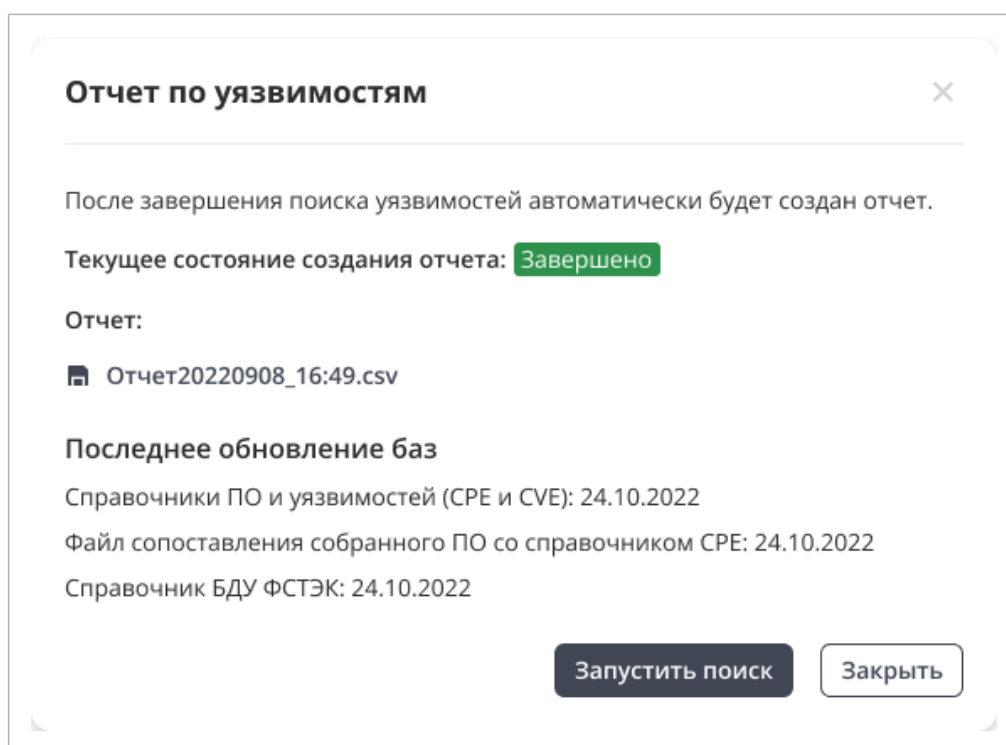


Рис. 217. Окно «Запуск поиска уязвимостей»



Подсказка:

Поиск уязвимостей и создание отчета может занять продолжительное время. Вы можете безопасно закрыть окно — поиск продолжится в фоновом режиме. Для просмотра статуса поиска уязвимостей заново откройте окно **Запуск поиска уязвимостей** — для этого на странице

Активы выберите любой актив и нажмите кнопку



Вы также можете отменить поиск уязвимостей, нажав кнопку **Остановить поиск** в окне **Запуск поиска уязвимостей**

д. Дождитесь завершения поиска.

► **Результат шага:** в окне **Запуск поиска уязвимостей** отобразится текущее состояние создания отчета: **Завершено**. В случае возникновения ошибки см. раздел **Ошибки поиска уязвимостей** в базах CVE, CPE и БДУ ФСТЭК России.

2. Для поиска уязвимостей актива из карточки актива:

а. Перейдите в карточку актива.

б. Нажмите кнопку  (**Запустить поиск уязвимостей**) рядом с заголовком **Уязвимости**.

► **Результат шага:** появится окно **Запуск поиска уязвимостей**.

в. Нажмите **Запустить поиск**.



Подсказка:

Поиск уязвимостей и создание отчета может занять продолжительное время. Вы можете безопасно закрыть окно — поиск продолжится в фоновом режиме. Для просмотра статуса поиска уязвимостей заново откройте окно **Запуск поиска уязвимостей** — для этого повторно нажмите кнопку  в карточке актива или на странице **Активы** выберите любой актив и



нажмите кнопку .

Вы также можете отменить поиск уязвимостей, нажав кнопку **Остановить поиск** в окне **Запуск поиска уязвимостей**

г. Дождитесь завершения поиска.

► **Результат шага:** в окне **Запуск поиска уязвимостей** отобразится текущее состояние создания отчета: **Завершено**. В случае возникновения ошибки см. раздел **Ошибки поиска уязвимостей** в базах CVE, CPE и БДУ ФСТЭК России.

9.1.4.2. Запуск группового поиска уязвимостей активов

Для поиска уязвимостей нескольких активов:

1. Перейдите на страницу **Активы**.

2. При помощи чекбоксов выберите активы.



3. Нажмите кнопку (Запустить поиск уязвимостей).

► **Результат шага:** Откроется окно **Запуск поиска уязвимостей**.

4. Нажмите **Запустить поиск**.

**Подсказка:**

Поиск уязвимостей и создание отчета может занять продолжительное время. Вы можете безопасно закрыть окно — поиск продолжится в фоновом режиме. Для просмотра статуса поиска уязвимостей заново откройте окно **Запуск поиска уязвимостей** — для этого на странице **Активы** выберите любой



актив и нажмите кнопку

Вы также можете отменить поиск уязвимостей, нажав кнопку **Остановить поиск** в окне **Запуск поиска уязвимостей**

5. Дождитесь завершения поиска.

- **Результат шага:** в окне **Запуск поиска уязвимостей** отобразится текущее состояние создания отчета: *Завершено*. В случае возникновения ошибки см. раздел *Ошибки поиска уязвимостей в базах CVE, CPE и БДУ ФСТЭК России*.

9.1.4.3. Просмотр обнаруженных уязвимостей и рекомендаций по их устранению

Пользователи могут просматривать уязвимости и рекомендации по их устранению в карточках активов или в отчетах.

1. Для просмотра уязвимостей и рекомендаций в карточке актива:

- Перейдите в карточку актива и нажмите на круговую диаграмму **Уязвимости** либо перейдите на страницу **Активы** и в строке с активом в столбце **Уязвимости** нажмите на его статус.

- **Результат шага:** Откроется окно **Просмотр уязвимостей** со списком уязвимостей, обнаруженных на активе.

Просмотр уязвимостей: WIN-7SP1OVMS

CVE	Оценка уязвимости	CVSS	БДУ ФСТЭК
CVE-2016-0174	Высокий	7.8	BDU:2016-01339
CVE-2016-7248	Высокий	7.8	BDU:2016-02346
CVE-2016-7221	Высокий	7.8	BDU:2017-00001
CVE-2010-4669	Высокий	7.8	
CVE-2016-7184	Высокий	7.8	BDU:2016-02370
CVE-2016-3338	Высокий	7.8	
CVE-2016-7260	Высокий	7.8	
CVE-2016-0196	Высокий	7.8	BDU:2016-01320
CVE-2016-3308	Высокий	7.8	BDU:2016-01972
CVE-2017-0250	Высокий	7.8	BDU:2017-01913
CVE-2016-3270	Высокий	7.8	BDU:2016-02409

Уязвимость CVE-2016-7221

Описание

Рекомендации

БДУ ФСТЭК России

BDU:2017-00001

Уязвимость компонента Input Method Editor операционной системы Windows связана с ошибками при загрузке DLL. Эксплуатация уязвимости может позволить нарушителю, действующему локально, повысить свои привилегии

Заккрыть

Рис. 218. Окно «Просмотр уязвимостей»

- Для просмотра рекомендаций выберите уязвимость из списка и откройте вкладку **Рекомендации**.

- **Результат шага:** Отобразится текстовая ссылка на рекомендации производителя и кнопка **Ссылка на источник**, при нажатии которой откроется веб-страница с рекомендациями по устранению уязвимости.



Внимание:

Веб-страница с рекомендациями откроется только при наличии доступа в Интернет.

Просмотр уязвимостей: WIN-7SP1OVMS

CVE	Оценка уязвимости	CVSS	БДУ ФСТЭК
CVE-2016-7185	Высокий	7.8	
CVE-2016-0173	Высокий	7.8	BDU:2016-01340
CVE-2016-3335	Высокий	7.8	
CVE-2016-7259	Высокий	7.8	
CVE-2018-6947	Высокий	7.8	BDU:2018-00524
CVE-2016-3254	Высокий	7.8	BDU:2016-01893
CVE-2016-3303	Высокий	7.8	BDU:2016-01974
CVE-2016-3239	Высокий	7.8	BDU:2016-01906
CVE-2016-0051	Высокий	7.8	BDU:2016-00432
CVE-2016-3311	Высокий	7.8	BDU:2016-01969
CVE-2016-0182	Высокий	7.8	BDU:2016-01332

Уязвимость CVE-2016-3303

Описание

Рекомендации

Источник

Ссылка на источник

Использование рекомендаций производителя:
<https://technet.microsoft.com/library/security/MS16-097>

Заккрыть

Рис. 219. Вкладка «Рекомендации»

2. Для просмотра уязвимостей в отчете формата *.csv:

- а. Перейдите в карточку актива, на котором выполнялся поиск уязвимостей, и откройте окно **Запуск поиска уязвимостей**.

- б. В открывшемся окне скачайте отчет формата *.csv.

- **Результат шага:** Файл с отчетом формата *.csv будет загружен на компьютер в директорию загрузки по умолчанию.

9.1.5. Выгрузка отчета по результатам сопоставления собранного ПО со справочником CPE

Для экспорта отчета, содержащего результаты сопоставления собранного сканерами ПО и ОС со справочником CPE всех активов, для которых когда-либо выполнялся поиск уязвимостей:

1. Перейдите на страницу .

2. При необходимости очистите предыдущий файл отчета — для этого нажмите кнопку  (**Очистить отчет по результатам сопоставления собранного ПО со справочником CPE**).
3. Запустите поиск уязвимостей на активах — подробнее см. раздел [Запуск поиска уязвимостей в базах CVE, CPE и БДУ ФСТЭК России](#).



Подсказка:

Отчет по результатам сопоставления собранного ПО со справочником CPE может содержать объединенный список ПО с нескольких активов — для этого перед выгрузкой отчета необходимо запустить и дождаться завершения поиска уязвимостей на всех требуемых активах.

4. Нажмите кнопку  (**Экспортировать отчет по результатам сопоставления собранного ПО со справочником CPE**).
- **Результат шага:** Файл с отчетом формата *.csv будет загружен на компьютер в директорию загрузки по умолчанию.

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

В этом разделе приведен порядок настройки и выполнения проверок активов на уязвимости и соответствие требованиям информационной безопасности с помощью OVAL:

1. Экспорт и импорт скриптов, настроек, групп определений OVAL
2. Настройка OVAL-проверки актива на соответствие требованиям информационной безопасности
3. Запуск OVAL-проверки актива на соответствие требованиям информационной безопасности
4. Просмотр и выгрузка результатов проверки актива на соответствие требованиям информационной безопасности
5. Повторный запуск OVAL-проверки на соответствие требованиям ИБ
6. Удаление OVAL-проверок актива на соответствие требованиям информационной безопасности

Пример содержимого файла формата *.xml, содержащего OVAL-определения для оценки соответствия парольной политики Windows:

```
<?xml version="1.0" encoding="UTF-8"?>
<oval_definitions xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5" xmlns:oval="http://oval.mitre.org/XMLSchema/oval-common-5" xmlns:oval-def="http://oval.mitre.org/XMLSchema/oval-definitions-5" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <generator>
    <oval:product_name>The UDV OVAL Repository</oval:product_name>
    <oval:schema_version>5.10.1</oval:schema_version>
    <oval:timestamp>2018-05-14T14:06:41.489-04:00</oval:timestamp>
  </generator>
  <definitions>
    <definition class="compliance" id="oval:udv.group.ru:def:1" version="1">
      <metadata>
        <title>Password age check</title>
        <description>Password age check</description>
      </metadata>
      <criteria>
        <criterion comment="Password min age check" test_ref="oval:udv.group.ru:tst:1"/>
        <criterion comment="Password max age check" test_ref="oval:udv.group.ru:tst:2"/>
      </criteria>
    </definition>
    <definition class="compliance" id="oval:udv.group.ru:def:2" version="1">
      <metadata>
        <title>Password complexity check</title>
        <description>Password complexity check</description>
      </metadata>
      <criteria>
        <criterion comment="Password length check" test_ref="oval:udv.group.ru:tst:3"/>
        <criterion comment="Password complexity check" test_ref="oval:udv.group.ru:tst:4"/>
        <criterion comment="Password history size check" test_ref="oval:udv.group.ru:tst:5"/>
      </criteria>
    </definition>
  </definitions>
</oval_definitions>
```

```
</definition>
<definition class="compliance" id="oval:udv.group.ru:def:3" version="1">
  <metadata>
    <title>Password encryption check</title>
    <description>Password encryption check</description>
  </metadata>
  <criteria>
    <criterion comment="Password reversible encryption check" test_ref="oval:udv.group.ru:tst:6"/>
  </criteria>
</definition>
</definitions>
<tests>
  <passwordpolicy_test check="all" check_existence="at_least_one_exists" comment="Test if
the min_passwd_age is compliant." id="oval:udv.group.ru:tst:1" version="1" xmlns="http://
oval.mitre.org/XMLSchema/oval-definitions-5#windows">
    <object object_ref="oval:udv.group.ru:obj:1"/>
    <state state_ref="oval:udv.group.ru:ste:1"/>
  </passwordpolicy_test>
  <passwordpolicy_test check="all" check_existence="at_least_one_exists" comment="Test if
the max_passwd_age is compliant." id="oval:udv.group.ru:tst:2" version="1" xmlns="http://
oval.mitre.org/XMLSchema/oval-definitions-5#windows">
    <object object_ref="oval:udv.group.ru:obj:1"/>
    <state state_ref="oval:udv.group.ru:ste:2"/>
  </passwordpolicy_test>
  <passwordpolicy_test check="all" check_existence="at_least_one_exists" comment="Test if
the min_passwd_len is compliant." id="oval:udv.group.ru:tst:3" version="1" xmlns="http://
oval.mitre.org/XMLSchema/oval-definitions-5#windows">
    <object object_ref="oval:udv.group.ru:obj:1"/>
    <state state_ref="oval:udv.group.ru:ste:3"/>
  </passwordpolicy_test>
  <passwordpolicy_test check="all" check_existence="at_least_one_exists" comment="Test if the
password_complexity is compliant." id="oval:udv.group.ru:tst:4" version="1" xmlns="http://
oval.mitre.org/XMLSchema/oval-definitions-5#windows">
    <object object_ref="oval:udv.group.ru:obj:2"/>
    <state state_ref="oval:udv.group.ru:ste:4"/>
  </passwordpolicy_test>
  <passwordpolicy_test check="all" check_existence="at_least_one_exists" comment="Test if the
password_hist_len is compliant." id="oval:udv.group.ru:tst:5" version="1" xmlns="http://
oval.mitre.org/XMLSchema/oval-definitions-5#windows">
    <object object_ref="oval:udv.group.ru:obj:2"/>
    <state state_ref="oval:udv.group.ru:ste:5"/>
  </passwordpolicy_test>
  <passwordpolicy_test check="all" check_existence="at_least_one_exists" comment="Test if the
reversible_encryption is compliant." id="oval:udv.group.ru:tst:6" version="1" xmlns="http://
oval.mitre.org/XMLSchema/oval-definitions-5#windows">
    <object object_ref="oval:udv.group.ru:obj:2"/>
    <state state_ref="oval:udv.group.ru:ste:6"/>
  </passwordpolicy_test>
</tests>
```

```
</passwordpolicy_test>
</tests>
<objects>
<passwordpolicy_object comment="Retrieves a passwordpolicy_object." id="oval:udv.group.ru:obj:1"
version="1" xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5#windows"/>
<passwordpolicy_object comment="Retrieves a passwordpolicy_object." id="oval:udv.group.ru:obj:2"
version="1" xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5#windows"/>
</objects>
<states>
<passwordpolicy_state comment="This passwordpolicy_state represents a password policy that
has a min_passwd_age greater than or equal to 2." id="oval:udv.group.ru:ste:1" version="1"
xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5#windows">
<min_passwd_age datatype="int" operation="greater than or equal">2</min_passwd_age>
</passwordpolicy_state>
<passwordpolicy_state comment="This passwordpolicy_state represents a password policy that has a
max_passwd_age less than or equal to 6." id="oval:udv.group.ru:ste:2" version="1" xmlns="http://
oval.mitre.org/XMLSchema/oval-definitions-5#windows">
<max_passwd_age datatype="int" operation="less than or equal">6</max_passwd_age>
</passwordpolicy_state>
<passwordpolicy_state comment="This passwordpolicy_state represents a password policy that
has a min_passwd_len greater than or equal to 6." id="oval:udv.group.ru:ste:3" version="1"
xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5#windows">
<min_passwd_len datatype="int" operation="greater than or equal">6</min_passwd_len>
</passwordpolicy_state>
<passwordpolicy_state comment="This passwordpolicy_state represents a password policy that has
a password_complexity equal to true." id="oval:udv.group.ru:ste:4" version="1" xmlns="http://
oval.mitre.org/XMLSchema/oval-definitions-5#windows">
<password_complexity datatype="boolean">true</password_complexity>
</passwordpolicy_state>
<passwordpolicy_state comment="This passwordpolicy_state represents a password policy that
has a password_hist_len greater than or equal to 2." id="oval:udv.group.ru:ste:5" version="1"
xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5#windows">
<password_hist_len datatype="int" operation="greater than or equal">2</password_hist_len>
</passwordpolicy_state>
<passwordpolicy_state comment="This passwordpolicy_state represents a password policy that has
a reversible_encryption equal to false." id="oval:udv.group.ru:ste:6" version="1" xmlns="http://
oval.mitre.org/XMLSchema/oval-definitions-5#windows">
<reversible_encryption datatype="boolean">false</reversible_encryption>
</passwordpolicy_state>
</states>
</oval_definitions>
```

9.2.1. Экспорт и импорт скриптов, настроек, групп определений OVAL

В этом разделе:

- Экспорт групп OVAL-определений
- Экспорт скриптов OVAL
- Экспорт настроек OVAL
- Импорт OVAL-определений
- Импорт групп OVAL-определений
- Импорт скриптов OVAL
- Импорт настроек OVAL

Экспорт и импорт OVAL-объектов осуществляется на странице **Администрирование** → **Основные настройки** → **Импорт и экспорт** в блоке **OVAL**.



Внимание:

Экспорт OVAL-определений доступен только в составе групп OVAL-определений.

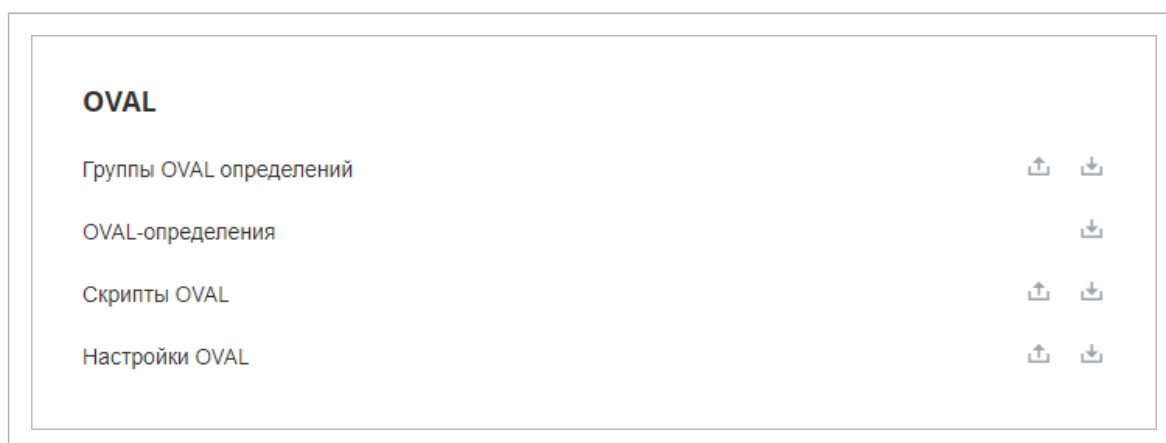


Рис. 220. Блок «OVAL» на странице «Импорт и экспорт»

9.2.1.1. Экспорт групп OVAL-определений

Для экспорта групп OVAL-определений вместе с OVAL-определениями в файл формата *.json:

1. Перейдите на страницу **Администрирование** → **Основные настройки** → **Импорт и экспорт**.
2. На панели **OVAL** в строке **Группы OVAL-определений** нажмите кнопку (**Экспортировать**).
 - **Результат шага:** Файл со списком групп OVAL-определений `oval_groups_[дата_и_время].json` будет сформирован и доступен для скачивания в правом верхнем углу страницы **Импорт и экспорт** под заголовком **Результат последнего экспорта**.
3. Для скачивания файла нажмите на его название в верхнем правом углу под заголовком **Результат последнего экспорта**.
4. В открывшемся окне укажите расположение для экспортируемого файла, введите название файла и нажмите **Сохранить**.

9.2.1.2. Экспорт скриптов OVAL

Для экспорта списка скриптов OVAL в файл формата *.json:

1. Перейдите на страницу **Администрирование** → **Основные настройки** → **Импорт и экспорт**.
2. На панели **OVAL** в строке **Скрипты OVAL** нажмите кнопку  (**Экспортировать**).
 - **Результат шага:** Файл со списком скриптов OVAL `oval_scripts_[дата_и_время].json` будет сформирован и доступен для скачивания в правом верхнем углу страницы **Импорт и экспорт** под заголовком **Результат последнего экспорта**.
3. Для скачивания файла нажмите на его название в верхнем правом углу под заголовком **Результат последнего экспорта**.
4. В открывшемся окне укажите расположение для экспортируемого файла, введите название файла и нажмите **Сохранить**.

9.2.1.3. Экспорт настроек OVAL

Для экспорта списка настроек OVAL в файл формата *.json:

1. Перейдите на страницу **Администрирование** → **Основные настройки** → **Импорт и экспорт**.
2. На панели **OVAL** в строке **Настройки OVAL** нажмите кнопку  (**Экспортировать**).
 - **Результат шага:** Файл со списком настроек OVAL `oval_settings_[дата_и_время].json` будет сформирован и доступен для скачивания в правом верхнем углу страницы **Импорт и экспорт** под заголовком **Результат последнего экспорта**.
3. Для скачивания файла нажмите на название сформированного файла под заголовком **Результат последнего экспорта**.
4. В открывшемся окне укажите расположение для экспортируемого файла, введите название файла и нажмите **Сохранить**.

9.2.1.4. Импорт OVAL-определений

Для импорта OVAL-определений из файла формата *.xml в Комплекс:

1. Перейдите на страницу **Администрирование** → **Основные настройки** → **Импорт и экспорт**.
2. В блоке **OVAL** в строке **OVAL-определения** нажмите кнопку .
3. В открывшемся окне укажите расположение импортируемого файла формата *.xml и подтвердите выбор.
 - **Результат шага:** Будет запущен процесс импорта: в правом верхнем углу появится уведомление **Запущен импорт справочника**, а под заголовком **Результат последнего импорта** будет символ -.



Подсказка:

Операции импорта являются фоновыми — со страницы можно безопасно уходить.

4. Убедитесь, что OVAL-определения были успешно загружены.
 - Если файл импортирован успешно, в правом верхнем углу под заголовком **Результат последнего импорта** появится уведомление: **Успешно**.
 - Если произошла ошибка, в правом верхнем углу под заголовком **Результат последнего импорта** появится уведомление **Ошибка**. Для просмотра информации об ошибке нажмите ссылку **Подробнее** в подсказке  рядом с уведомлением.
 - **Результат шага:** в результате успешного импорта на странице **Администрирование** → **Инспекция активов** → **Определения OVAL** появится импортированный справочник.

9.2.1.5. Импорт групп OVAL-определений

Для импорта групп OVAL-определений из файла формата *.json в Комплекс:

1. Перейдите на страницу **Администрирование** → **Основные настройки** → **Импорт и экспорт**.
2. В блоке **OVAL** в строке **Группы OVAL-определений** нажмите кнопку .
3. В открывшемся окне укажите расположение импортируемого файла формата *.xml и подтвердите выбор.
4. В открывшемся окне **Подготовка к импорту** выберите действие для элементов, которые отсутствуют в новом (загружаемом) справочнике:
 - **Оставить** — новые элементы будут добавлены к уже существующим;
 - **Удалить** — старые элементы будут удалены и добавлены новые.

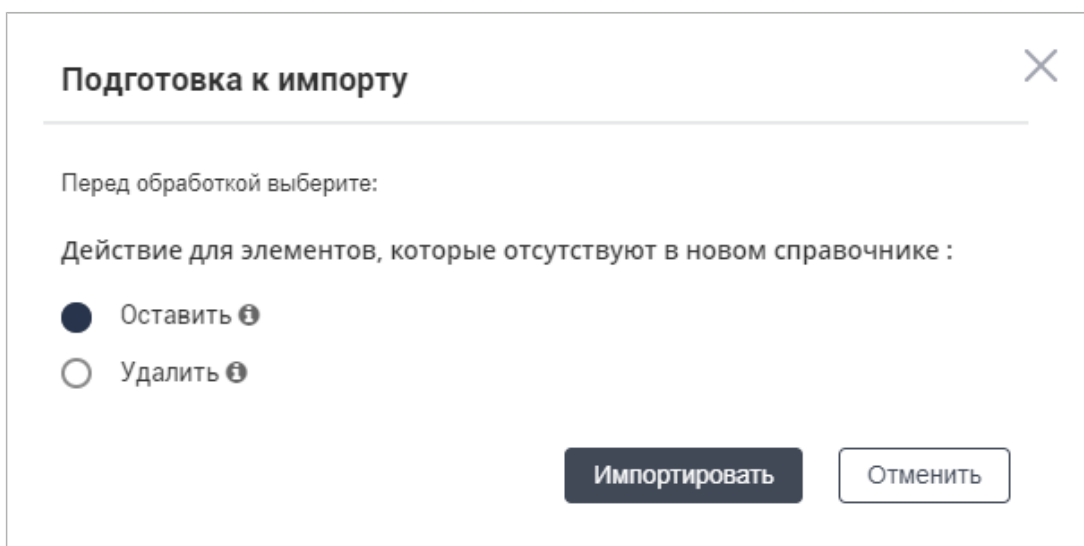


Рис. 221. Окно «Подготовка к импорту»

5. Нажмите **Импортировать**.
 - **Результат шага:** Будет запущен процесс импорта: в правом верхнем углу появится уведомление **Запущен импорт справочника**, а под заголовком **Результат последнего импорта** будет символ .

 Подсказка:

Операции импорта являются фоновыми — со страницы можно безопасно уходить.

6. Убедитесь, что группы OVAL-определений были успешно загружены.
 - Если файл импортирован успешно, в правом верхнем углу под заголовком **Результат последнего импорта** появится уведомление: **Успешно**.
 - Если произошла ошибка, в правом верхнем углу под заголовком **Результат последнего импорта** появится уведомление **Ошибка**. Для просмотра информации об ошибке нажмите ссылку **Подробнее** в подсказке  рядом с уведомлением.
 - **Результат шага:** в результате успешного импорта на странице **Администрирование** → **Инспекция активов** → **Группы OVAL** появится импортированный справочник.

9.2.1.6. Импорт скриптов OVAL

Для импорта скриптов OVAL из файла формата *.json в Комплекс:

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

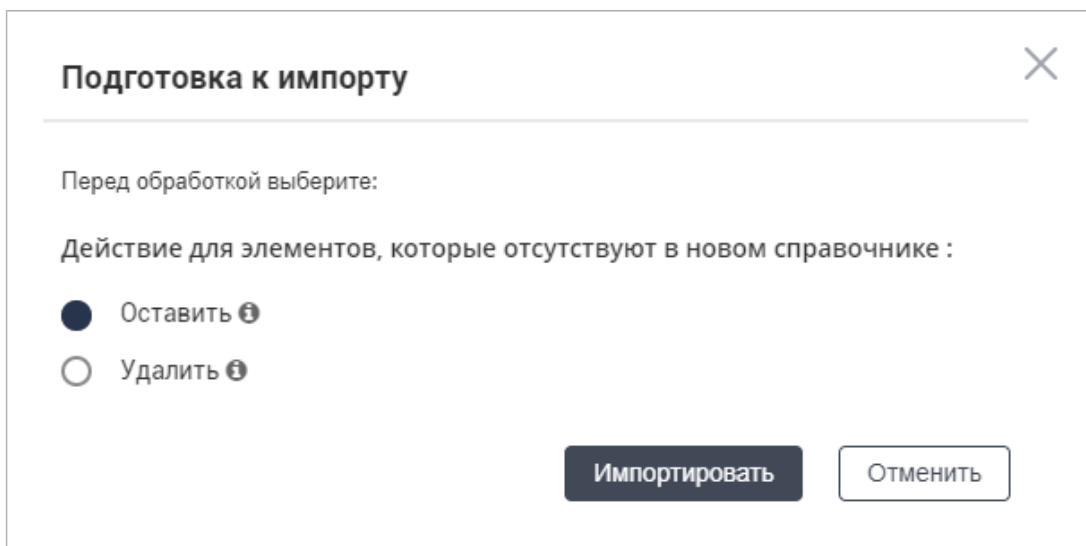


Рис. 222. Окно «Подготовка к импорту»

5. Нажмите **Импортировать**.
 - **Результат шага:** Будет запущен процесс импорта: в правом верхнем углу появится уведомление **Запущен импорт справочника**, а под заголовком **Результат последнего импорта** будет символ -.

 Подсказка:

Операции импорта являются фоновыми — со страницы можно безопасно уходить.

6. Убедитесь, что скрипты OVAL были успешно загружены.
 - Если файл импортирован успешно, в правом верхнем углу под заголовком **Результат последнего импорта** появится уведомление: **Успешно**.
 - Если произошла ошибка, в правом верхнем углу под заголовком **Результат последнего импорта** появится уведомление **Ошибка**. Для просмотра информации об ошибке нажмите ссылку **Подробнее** в подсказке  рядом с уведомлением.
 - **Результат шага:** в результате успешного импорта на странице **Администрирование** → **Инспекция активов** → **Скрипты OVAL** появится импортированный справочник.

9.2.1.7. Импорт настроек OVAL

Убедитесь, что настройки OVAL в импортируемом файле подготовлены для корректной загрузки, а именно:

- в Комплекс уже импортированы скрипты OVAL, id которых указаны в каждой импортируемой настройке OVAL;



Подсказка:

Подробнее об импорте OVAL скриптов см. раздел [Импорт скриптов OVAL](#).

- в каждой настройке OVAL указан хотя бы один из следующих параметров, который будет связывать скрипты OVAL с существующими активами:
 - метка актива;
 - параметр **По умолчанию** (`is_default`);
 - список активов.



ОСТОРОЖНО:

Если в импортируемом файле присутствуют не все параметры (метка, параметр **По умолчанию**, список активов), настройка будет импортирована без них.

Для импорта групп настроек OVAL из файла формата *.json в Комплекс:

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

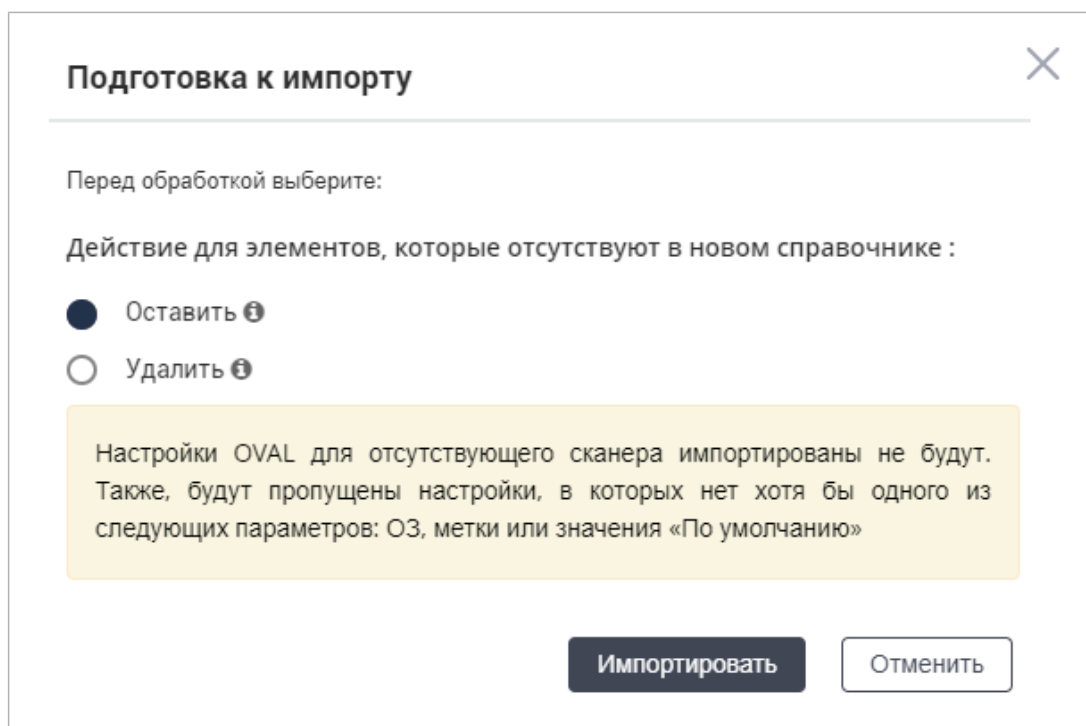


Рис. 223. Окно подготовки к импорту настроек OVAL

5. Нажмите кнопку **Импортировать** для выполнения импорта.

- **Результат шага:** Будет запущен процесс импорта: в правом верхнем углу появится уведомление **Запущен импорт справочника**, а под заголовком **Результат последнего импорта** будет символ -.

 Подсказка:

Операции импорта являются фоновыми — со страницы можно безопасно уходить.

6. Убедитесь, что настройки OVAL были успешно загружены.

- Если файл импортирован успешно, в правом верхнем углу под заголовком **Результат последнего импорта** появится уведомление: **Успешно**.
- Если произошла ошибка, в правом верхнем углу под заголовком **Результат последнего импорта** появится уведомление **Ошибка**. Для просмотра информации об ошибке нажмите ссылку **Подробнее** в подсказке ⓘ рядом с уведомлением.
- **Результат шага:** в результате успешного импорта на странице **Администрирование** → **Инспекция активов** → **Настройки OVAL** появится импортированный справочник.

9.2.2. Настройка OVAL-проверки актива на соответствие требованиям информационной безопасности

Для запуска OVAL-проверок на соответствие требованиям ИБ пользователь Комплекса должен убедиться, что все необходимые для этого элементы были ранее настроены. Для настройки вы можете последовательно воспользоваться следующими разделами:

- Содержание Python-скриптов
- Цифровая подпись Python-скрипта
- Управление скриптами OVAL
- Настройка доступа к активу для сбора OVAL-объектов
- Проверка привязки OVAL-скрипта к активу
- Создание группы определений OVAL
- Добавление и исключение OVAL-определений из групп

9.2.2.1. Управление скриптами OVAL

Для работы со скриптами в веб-интерфейсе Комплекса доступны следующие возможности:

1. Создание скрипта. Для создания:

- Перейдите в подраздел **Администрирование** → **Результаты проверок** → **Инспекция активов** → **Скрипты OVAL**.

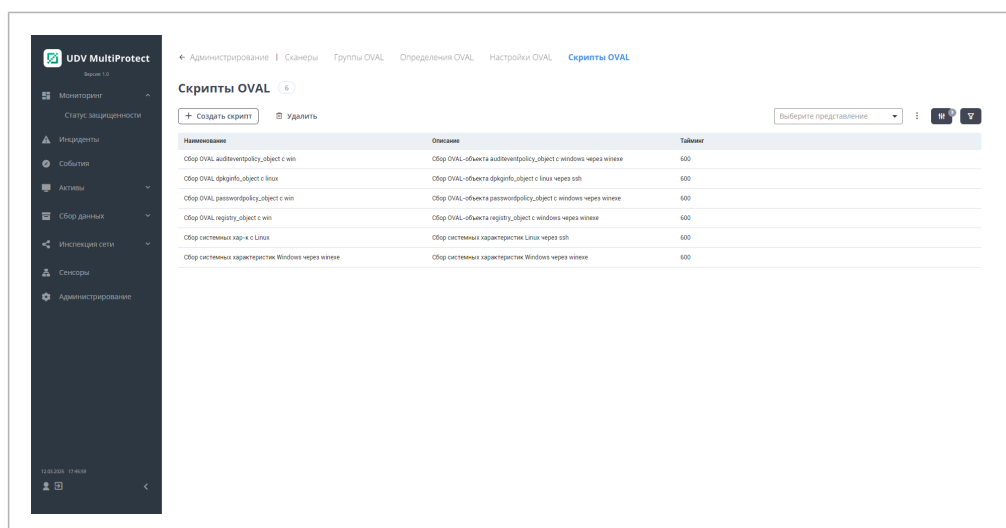


Рис. 224. Страница «Скрипты OVAL»

б. Нажмите кнопку **Создать скрипт**. В открывшемся окне **Создание скрипта OVAL** задайте следующие параметры:

- наименование и описание скрипта;
- тип OVAL-объекта;
- цифровую подпись скрипта (подробнее см. в разделе «Цифровая подпись Python-скрипта»);
- при необходимости введите максимальное время ожидания выполнения задачи в секундах;
- нажмите **Импортировать** для загрузки скрипта из файла. В проводнике выберите и откройте подписанный ранее файл скрипта формата *.py;

Создание скрипта OVAL

Наименование *

system_characteristics WIN

Описание

Тип OVAL-объекта *

system_characteristics

Цифровая подпись *

ZC4kEHuCH7K0l9vkb6ADuPYudixZhoPABunNMpVuMMzsqsNFvp/Fra5Kr1W+4G0oL

Максимальное время ожидания выполнения задачи, сек

600

ИмпортироватьЭкспортировать

СоздатьОтменить

Рис. 225. Окно «Создание скрипта OVAL»

- в. Нажмите кнопку **Создать** для подтверждения изменений.
2. Изменение скрипта. Для изменения:
- Перейдите в подраздел **Администрирование** → **Результаты проверок** → **Инспекция активов** → **Скрипты OVAL**.
 - Наведите на правую часть строки изменяемого скрипта.
 - Нажмите кнопку  (**Редактировать**).
- **Результат шага:** Откроется окно **Редактирование скрипта OVAL**
- г. Измените необходимые параметры

Редактирование скрипта OVAL

Наименование *

Сбор системных характеристик Windows через winexe

Описание

Сбор системных характеристик Windows через winexe

Тип OVAL-объекта *

system_characteristics

Цифровая подпись *

W2wlgXRxG/eFtHizlZWUAvArtialoGppS6DYBHaxri5cGPs2ZUiD5o+fBXeUTIhmVPq3N

Максимальное время ожидания выполнения задачи, сек

600

Импортировать

Экспортировать

Сохранить

Отменить

Рис. 226. Окно «Редактирование скрипта OVAL»

- д. Нажмите кнопку **Сохранить** для подтверждения изменений.
3. Удаление скрипта. Для удаления:
- Наведите курсор на правую часть строки удаляемого скрипта.
 - Нажмите кнопку  (**Удалить скрипт**).
 - **Результат шага:** Откроется окно подтверждения удаления.
 - Введите обоснование действия и нажмите **Подтвердить**.
4. Удаление группы скриптов. Для удаления:
- При помощи фильтров отрегулируйте выборку так, чтобы отображались только скрипты, которые будут удалены.
 - Нажмите  (**Удалить скрипты**).
 - **Результат шага:** появится окно подтверждения удаления.
 - Введите обоснование действия и нажмите **Подтвердить**.

9.2.2.2. Настройка доступа к активу для сбора OVAL-объектов

Для настройки доступа к активу для сбора OVAL-объектов:

1. Добавьте учетную запись актива (см. раздел [Настройка учетных данных активов](#)).
2. Привяжите учетную запись к активу. Для этого:
 - а. Откройте окно **Карточка актива**.
 - б. На панели **Учетные данные** нажмите  .
► **Результат шага:** Откроется окно **Настройка учетных данных**.
 - в. Выберите подходящие учетные данные из списка и нажмите **Сохранить**.
3. Убедитесь, что загружены скрипты для сбора OVAL-объектов на странице **Администрирование** → **Результаты проверок** → **Инспекция активов** → **Скрипты OVAL**.
4. Привяжите скрипты для сбора OVAL-объектов к активу. Для этого:
 - а. Перейдите на страницу **Администрирование** → **Результаты проверок** → **Инспекция активов** → **Настройки OVAL**.

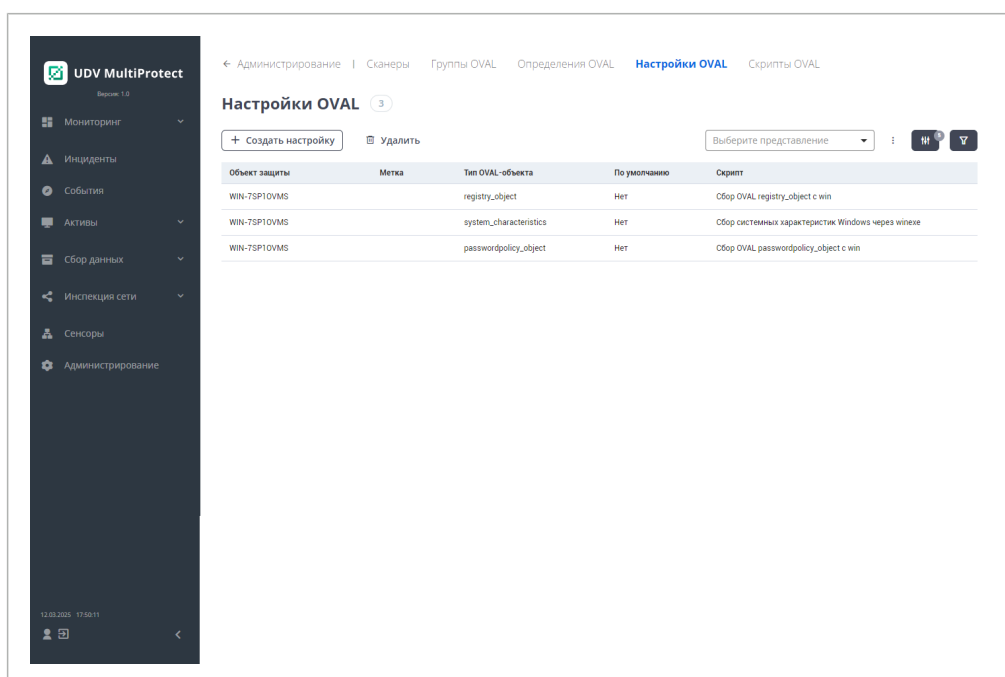


Рис. 227. Страница «Настройки OVAL»

- б. Нажмите **Создать настройку**.
- в. В открывшемся окне **Создание настройки OVAL** задайте следующие параметры для привязки скрипта к отдельным активам:

- В поле **Скрипт** выберите из списка скрипт для сбора выбранного OVAL-объекта.



Подсказка:

Тип OVAL-объекта будет отображен автоматически.

- В поле **Активы** выберите один или несколько активов, к которым будет привязан скрипт для выполнения OVAL-проверок;

- В поле **Метка** выберите из списка метку, к которой необходимо привязать скрипт для выполнения проверок на соответствие требованиям ИБ
- Отметьте параметр **По умолчанию**, чтобы установить настройку для всех активов, которым не присвоена другая настройка.

Рис. 228. Окно «Создание настройки OVAL»

- г. Нажмите **Создать**.
5. Повторите шаги из п. 4 для остальных OVAL-объектов.

9.2.2.3. Проверка привязки OVAL-скрипта к активу

Для проверки привязки (наличия OVAL-настройки) OVAL-скрипта к активу в зависимости от используемого типа объекта:

1. Проверьте наличие персональной OVAL-настройки для актива по используемому типу OVAL-объекта.
2. Если для актива нет индивидуальных настроек по типу OVAL-объекта, проверьте наличие OVAL-настройки для меток, в которые входит актив. Если активу присвоено несколько групп, которые имеют OVAL-настройки для одного типа объекта, OVAL-настройка для актива выбирается случайным образом из настроек, назначенных меткам.
3. Если активу невозможно назначить OVAL-настройку исходя из меток, ему назначается настройка, указанная по умолчанию.



Внимание:

Если OVAL-настройки по умолчанию не заданы и активу не назначена индивидуальная настройка или настройка по меткам, в ходе выполнения OVAL-проверки для выбранного актива будет выведена ошибка.

9.2.2.4. Создание группы определений OVAL

Для создания группы определений OVAL:

1. Перейдите на страницу → **Результаты проверок** → **Инспекция активов** → **Группы OVAL**.
2. Нажмите **Создать группу**. В открывшемся окне **Создание группы OVAL-определений** заполните следующие параметры:
 - а. уникальное наименование группы OVAL определений;
 - б. описание группы;
 - в. в поле **OVAL-определения** выберите из списка импортированные определения, которые будут принадлежать новой группе.

Подсказка:
Добавить или исключить OVAL-определения из группы можно также на странице [Определения OVAL](#). Подробнее см. в разделе «Добавление и исключение OVAL-определений из групп».

Создание группы OVAL-определений

Наименование *

Описание

OVAL-определения

× Минимальная длина пароля

× Соответствие требованиям журналирования паролей

× Максимальный срок действия пароля

× Соответствие требованиям шифрования пароля

× ▼

Создать

Отменить

Рис. 229. Окно «Создание группы OVAL-определений»

3. Нажмите **Создать**.

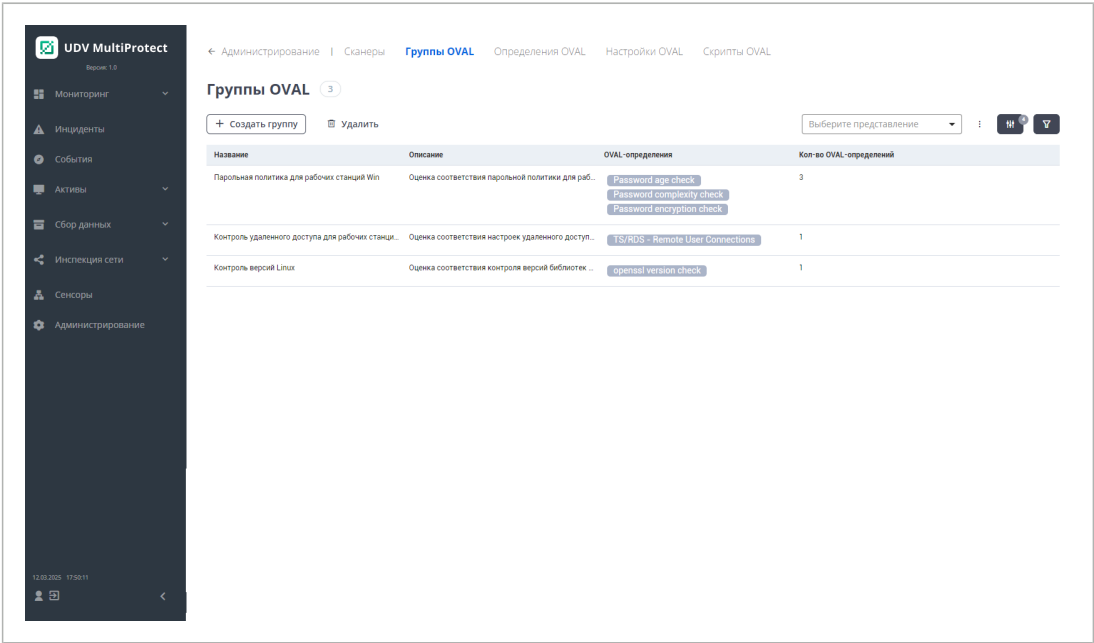


Рис. 230. Страница «Группы OVAL»

9.2.2.5. Добавление и исключение OVAL-определений из групп

Для добавления или исключения OVAL-определений из созданной группы:

1. Перейдите на страницу **Результаты проверок** → **Инспекция активов** → **Определения OVAL**.
2. Выберите OVAL-определения, которые необходимо добавить в созданную группу или исключить из нее.

Для этого вы можете воспользоваться следующими возможностями:

- а. Выбор определений по одному. Для выбора одного определения нажмите кнопку  (**Выбрать определение для добавления в группу**) в строке с требуемым OVAL-определением для выбора отдельных определений, либо установите чекбокс слева от OVAL-определения;
- б. Выбор нескольких OVAL-определений. Для группового выбора OVAL-определений:
 - Выполните фильтрацию списка определений;
 - Нажмите **Выбрать определения** в верхней части списка определений для выбора всех определений, отображаемых в данный момент, либо установите чекбокс в заголовке таблицы;



Подсказка:

Доступен выбор до 300 определений за раз. Для изменения количества определений, которые можно выбрать, измените значения переменной `OVAL_DEFINITION_SELECT_MAX_LIMIT` в файле `manager.env`. Список всех переменных файла см. в разделе [Переменные Комплекса уровня Management](#).

- в. Отмена выбора OVAL-определения. Для отмены нажмите  (**Исключить определение из выбора**) напротив выбранного определения.
 - г. Отмена выбора нескольких OVAL-определений. Для групповой отмены выбора OVAL-определений:
 - выполните фильтрацию списка определений;
 - нажмите кнопку (**Отменить выбор**) в верхней части страницы для отмены выбора всех определений, отображаемых в данный момент;
3. Для добавления в группу:
 - а. Нажмите кнопку  **Добавить в группу**.
 - б. В открывшемся окне **Добавление в группу OVAL-определений**:
 - выберите из списка название созданной ранее группы;
 - при необходимости измените состав OVAL-определений для добавления в группу.

The dialog box is titled "Добавление в группу OVAL-определений". It contains two sections: "Группа OVAL-определений" with a dropdown menu showing "Log4j", and "OVAL-определения" with a list containing one item: "Уязвимость в Apache Log4j до 2.15.0 (Log4j)". At the bottom right, there are two buttons: "Добавить" (Add) and "Отменить" (Cancel).

Рис. 231. Окно «Добавление в группу OVAL-определений»

- в. Нажмите кнопку **Добавить**.
4. Для исключения из группы:
- а. Нажмите кнопку  **Исключить из группы**.
- б. В открывшемся окне **Исключение OVAL-определений из групп**:
- Выберите из списка название созданной ранее группы;
 - При необходимости измените состав OVAL-определений для исключения из группы.

The dialog box is titled "Исключение OVAL-определений из групп". It contains two sections: "Группа OVAL-определений" with a dropdown menu showing "Log4j", and "OVAL-определения" with a list containing one item: "Уязвимость в Apache Log4j до 2.15.0 (Log4j)". At the bottom right, there are two buttons: "Исключить" (Exclude) and "Отменить" (Cancel).

Рис. 232. Окно «Исключение OVAL-определений из групп»

- в. Нажмите **Исключить**.

9.2.3. Запуск OVAL-проверки актива на соответствие требованиям информационной безопасности

Перед запуском OVAL-проверки актива на соответствие требованиям информационной безопасности убедитесь, что актив имеет сетевой атрибут. Для настройки сетевого атрибута выполните шаг 7 раздела Редактирование активов.

Для проверки актива на соответствие требованиям информационной безопасности с помощью OVAL:

1. Перейдите на страницу **Сбор данных** → **Результаты проверок**.

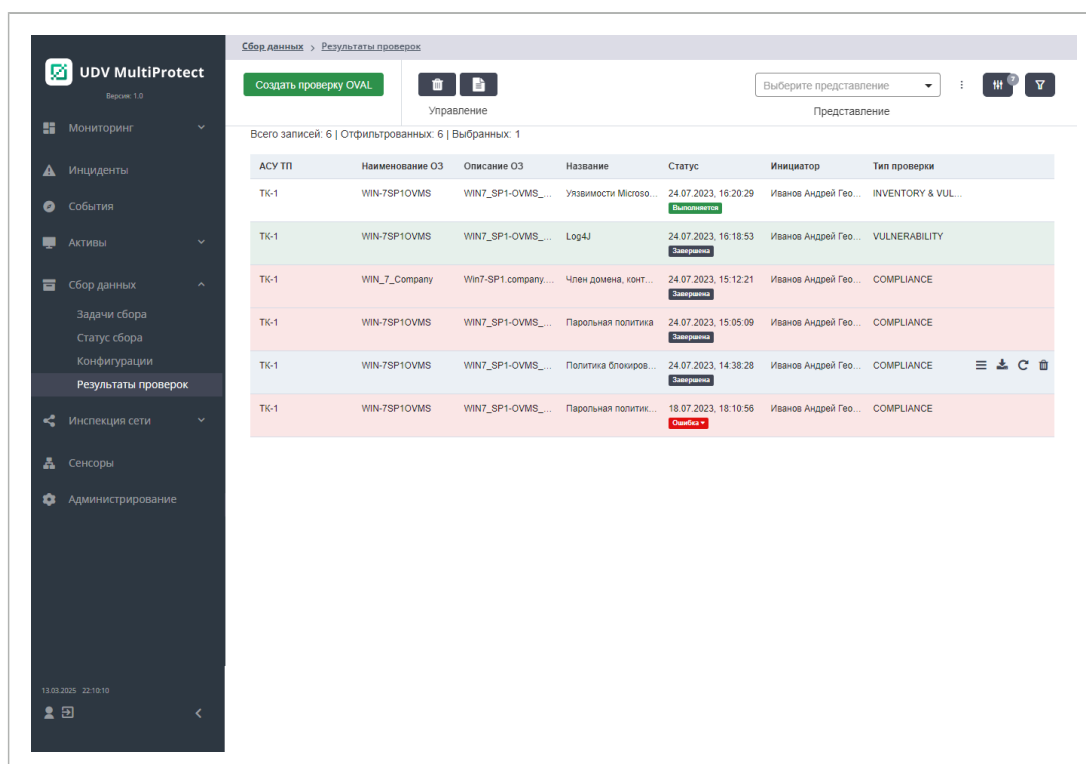


Рис. 233. Страница «Результаты проверок»

2. Нажмите **Создать проверку OVAL**. В открывшемся окне **Создание проверки OVAL-определений** настройте следующие параметры:
 - а. группу OVAL-определений;
 - б. наименование проверки;
 - в. описание цели выполнения проверки;
 - г. статус проверки;
 - д. активы, к которым был настроен доступ.



Внимание:

Если поля **Цель проверки**, **Статус проверки** и **Наименование оставить** неизменными, то они будут заполнены автоматически. Поле **OVAL -определения** недоступно для редактирования и заполняется автоматически после выбора группы OVAL-определений.

Создание проверки OVAL-определений

Группа OVAL-определений *

Log4j

OVAL-определения

Уязвимость в Ruby gem log4j-jars since 2.0.0.rc1 (slyphon-log4j, log4j-jars)

Уязвимость в Ruby gem log4j-jars since 2.0.0.rc1 (slyphon-log4j, log4j-jars)

Уязвимость в Apache log4net до 2.0.10 (reab1c277c95310bad1038255e0757857b2fbe291411b4fa84552028a%40%3Cd ev)

Уязвимость атаки «man-in-the-middle» в Ruby gem log4j-jars во всех версиях, slyphon-log4j во всех версиях (slyphon-log4j, log4j-jars)

Уязвимость в Apache Log4j до 2.15.0 (Log4j)

Наименование

Проверка наличия уязвимости Log4j

Цель проверки

Статус проверки

Объекты защиты *

Win2003SP2_TK1

Создать

Отменить

Рис. 234. Окно «Создание проверки OVAL-определений»

3. Нажмите **Создать**.

- **Результат шага:** Выполнение проверки запустится автоматически.

4. Обновите страницу **Результаты проверок**.

- **Результат шага:** На странице отобразятся результаты проверки с цветовой индикацией. Подробнее см. раздел Просмотр и выгрузка результатов проверки актива на соответствие требованиям информационной безопасности.

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

Для просмотра результатов проверок на соответствие требованиям ИБ в веб-интерфейсе Комплекса:

1. Перейдите на страницу .

2. Воспользуйтесь фильтрами по кнопке  для получения необходимой выборки. При необходимости настройте отображение столбцов на странице. Подробнее см. раздел [Элементы управления таблицами](#).

Если проверка выполнена успешно и для актива не было обнаружено несоответствие по любому из критериев оценки соответствия (тип проверки: COMPLIANCE) либо ни одна из уязвимостей не была обнаружена (тип проверки: VULNERABILITY), в таблице результатов в строке **Статус** появится надпись *Завершена*, и строка таблицы будет выделена зеленым цветом.

TK-1	WIN-7SP1OVMS	WIN7_SP1-OVMS_TK1_DEVELOPERS	Уязвимости Microsoft SQL	24.07.2023, 16:21:50	Иванов Андрей Георгиевич (datapk)	INVENTORY & VULNERABILITY

Рис. 235. Результат успешной проверки на соответствие требованиям ИБ в случае выполнения всех критериев оценки

Если проверка выполнена, но для актива обнаружено несоответствие хотя бы по одному из критериев оценки (тип проверки: COMPLIANCE) либо была обнаружена хотя бы одна из уязвимостей (тип проверки: VULNERABILITY), в таблице результатов в строке **Статус** появится статус: *Завершена*, а строка таблицы будет выделена красным цветом.

TK-1	WIN_7_Company	Win7-SP1.company.local	Член домена, контроллер домена	24.07.2023, 15:12:21	Иванов Андрей Георгиевич (datapk)	COMPLIANCE

Рис. 236. Результат успешной проверки на соответствие требованиям ИБ в случае невыполнения критериев оценки

Если проверка не выполнена, в таблице результатов в столбце **Статус** появится статус: *Ошибка* с описанием ошибки.

TK-1	WIN-7SP1OVMS	WIN7_SP1-OVMS_TK1_DEVELOPERS	Парольная политика для работн...	18.07.2023, 18:10:56	Иванов Андрей Георгиевич (datapk)	COMPLIANCE

Рис. 237. Результат неуспешной проверки на соответствие требованиям ИБ

Результаты проверок будут выделены желтым цветом, если в случае проверок типа COMPLIANCE и VULNERABILITY хотя бы один критерий имеет результат, отличный от true и false (например, в случае ошибки или невозможности получить данные с актива).

Результаты проверок типа INVENTORY (проверка наличия установленного ПО и версий ПО) и MISCELLANEOUS (иные виды проверок) не выделяются цветом.

3. Нажмите кнопку  (**Просмотреть результаты**) в строке с успешно выполненной проверкой на соответствие требованиям ИБ.

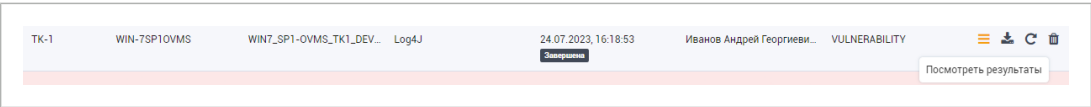


Рис. 238. Кнопка «Посмотреть результаты» в строке с проверкой на соответствие требованиям ИБ

 **Внимание:**

На странице **Результаты проверки** будут приведены результаты по каждому из критериев соответствия. Для критериев наличия уязвимости (с классом **VULNERABILITY**) в колонке **Меры по исправлению уязвимостей** приводятся рекомендации по устранению как для обнаруженных, так и не обнаруженных уязвимостей.

Наименование OVAL-группы: Log4j									
Наименование O3: WIN-7SP1OVMS									
Всего записей: 7 Отфильтрованных: 7									
Идентификатор	Название	Описание	Класс	Результат	Идентификатор CVE	Базовая оценка уязвимости	Базовый вектор атаки	Меры по исправлению уязвимости	
oval.ru.altx-soft.win.def.568...	Ruby is installed	Ruby is installed.	INVENTORY	False					
oval.ru.altx-soft.win.def.568...	RubyGems is installed	RubyGems is installed.	INVENTORY	False					
oval.ru.altx-soft.win.def.659...	Уязвимость в Ruby gem log...	Уязвимость в SocketServer...	VULNERABILITY	Уязвимость не обнаружена	CVE-2019-17571	Критический уровень опасности (Базовая оценка CVSS 2.0 составляет 10.0)	AV:N/AC:L/Au:N/C:C/I:C/A:C	Обновление библиотеки журнал...	
oval.ru.altx-soft.win.def.659...	Уязвимость в Ruby gem log...	Apache Log4j 2.x до 2.8.2 н...	VULNERABILITY	Уязвимость не обнаружена	CVE-2017-9645	Критический уровень опасности (Базовая оценка CVSS 2.0 составляет 10.0)	AV:N/AC:L/Au:N/C:C/I:C/A:C	Использование рекомендаций...	
oval.ru.altx-soft.win.def.659...	Уязвимость в Apache Log4j...	Уязвимость XML External E...	VULNERABILITY	Уязвимость не обнаружена	CVE-2018-1285	Критический уровень опасности (Базовая оценка CVSS 2.0 составляет 10.0)	AV:N/AC:L/Au:N/C:C/I:C/A:C	Использование рекомендаций...	
oval.ru.altx-soft.win.def.659...	Уязвимость атаки «tap-in»...	Уязвимость атаки «tap-in»...	VULNERABILITY	Уязвимость не обнаружена	CVE-2020-9488	Средний уровень опасности (Базовая оценка CVSS 2.0 составляет 4.3)	AV:N/AC:M/Au:N/CP:IN/A:N	Использование рекомендаций...	
oval.ru.altx-soft.win.def.801...	Уязвимость в Apache Log4j...	Apache Log4j2 2.14.1 и рек...	VULNERABILITY	Уязвимость не обнаружена	CVE-2021-44228	Критический уровень опасности (Базовая оценка CVSS 2.0 составляет 10.0)	AV:N/AC:L/Au:N/C:C/I:C/A:C	Использование рекомендаций...	

Рис. 239. Результаты успешной проверки на соответствие требованиям ИБ

4. Для выгрузки отчета по результатам проверок:

 **Подсказка:**

Подробнее см. раздел **Выгрузка отчетов**.

- а. Воспользуйтесь фильтрами по кнопке  для получения необходимой выборки.
- б. В верхней части страницы нажмите кнопку  (**Создать отчет**).
- в. В окне **Создание отчета** выберите формат файла (pdf или xlsx).
- г. Нажмите **Создать**.
- д. В открывшемся окне **Сохранение** выберите путь для сохранения файла.

► **Результат шага:** Файл отчета

oval_assessments_[дата_и_время_в_формате_ДД.ММ.ГГГ_ЧЧ.ММ.СС] выбранного формата будет загружен.

5. Для экспорта файла с результатами успешной проверки на соответствие требованиям ИБ:

- а. Нажмите кнопку  (**Сохранить результаты в файл**) в строке с успешно выполненной проверкой на соответствие требованиям ИБ.
- б. В открывшемся окне **Сохранение результатов** выберите формат файла (pdf, xlsx или xml).

в. В открывшемся окне **Сохранение** выберите путь для сохранения файла.

► **Результат шага:** Файл с результатом проверки `oval_assessment_results_[дата_и_время]` выбранного формата будет загружен.

9.2.5. Повторный запуск OVAL-проверки на соответствие требованиям ИБ

Для повторного запуска ранее выполненной проверки OVAL на соответствие требованиям ИБ (успешной или неуспешной):

1. Перейдите на страницу .
2. Нажмите кнопку  (**Перезапустить проверку**) в строке с проверкой OVAL, которую необходимо выполнить повторно.



Подсказка:

При необходимости остановки проверки нажать  (**Отменить проверку**) в строке с проверкой в статусе *Выполняется*.

3. Обновите страницу **Результаты проверок** для получения результата проверки.

9.2.6. Удаление OVAL-проверок актива на соответствие требованиям информационной безопасности

Если данных слишком много или они уже не нужны, их можно удалить.

Для удаления проверки:

1. Перейдите на страницу .
2. Если необходимо удалить одну проверку, нажмите кнопку  (**Удалить**) в строке напротив нее.
3. Если необходимо удалить несколько проверок:
 - а. отфильтруйте содержимое страницы так, чтобы отображались только удаляемые проверки;
 - б. нажмите кнопку  (**Удалить проверки**).
4. Во всплывающем окне введите обоснование удаления.

 **Внимание:**

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

Для данного действия необходимо обоснование 

Введите текст обоснования

Подтвердить

Отменить

Рис. 240. Окно «Обоснование удаления проверки»

5. Нажмите **Подтвердить**.
 - **Результат шага:** После удаления проверки будет зафиксировано соответствующее событие, в котором отображено обоснование удаления.

10. Инспекция сети Комплекса

Для просмотра и управления объектами в локальной сети Комплекса предусмотрен просмотр карты сети, потоков на ней и на отдельной странице, а также служба обнаружения вторжений.

На странице **Карта сети** отображается карта локальной сети Комплекса. На карте отображаются добавленные узлы, элемент внешней сети и потоки между ними. Для управления отображением используются представления. Подробнее см. в разделе Настройка представлений на карте.

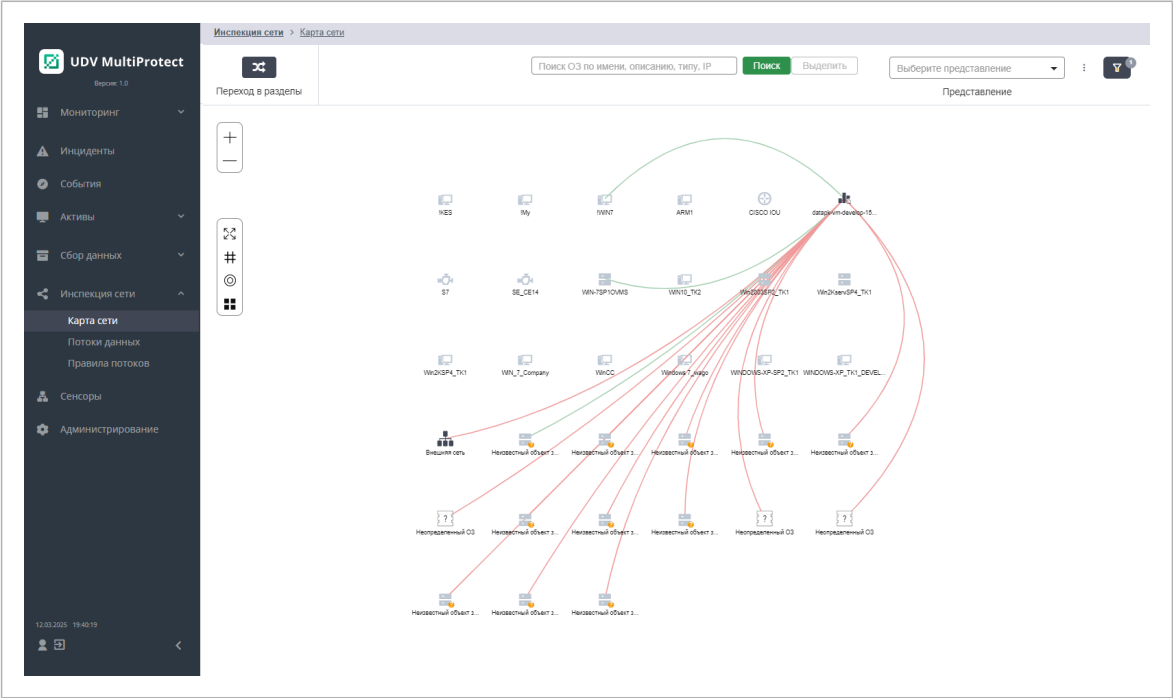


Рис. 241. Страница «Карта сети»

На странице **Потоки данных** отображается список взаимодействий в отсканированной ранее сети. Потоки можно редактировать, одобрять, отменять одобрение, удалять. Управление потоками данных, отображаемыми на карте, также выполняется на этой странице.

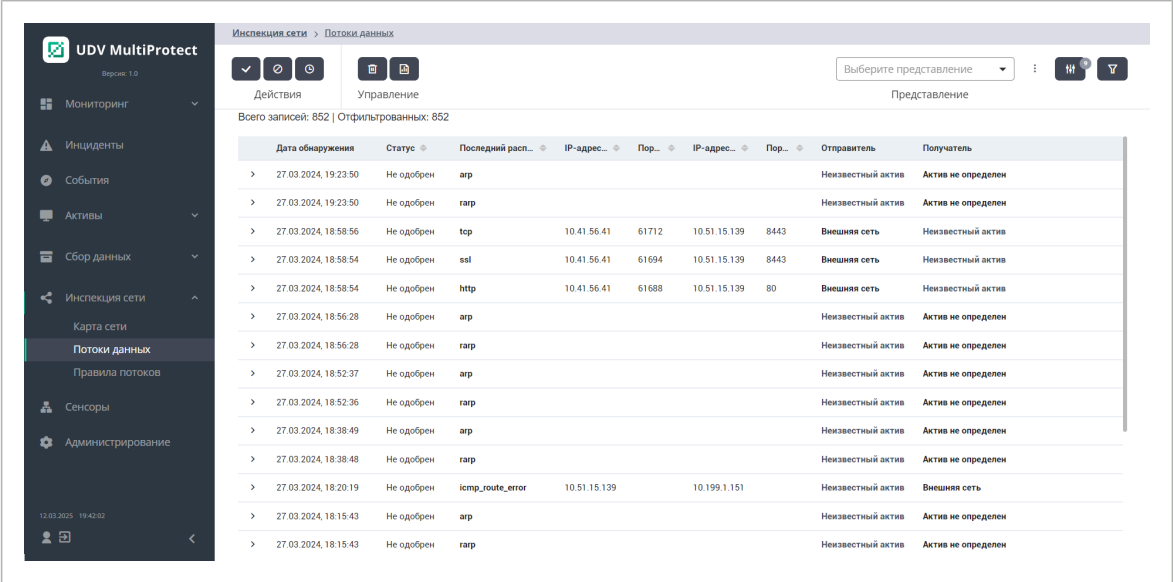


Рис. 242. Страница «Потоки данных»

На странице **Правила обнаружения** отображаются правила, при помощи которых могут быть выявлены угрозы для локальной сети. Можно запускать, редактировать и удалять созданные правила.

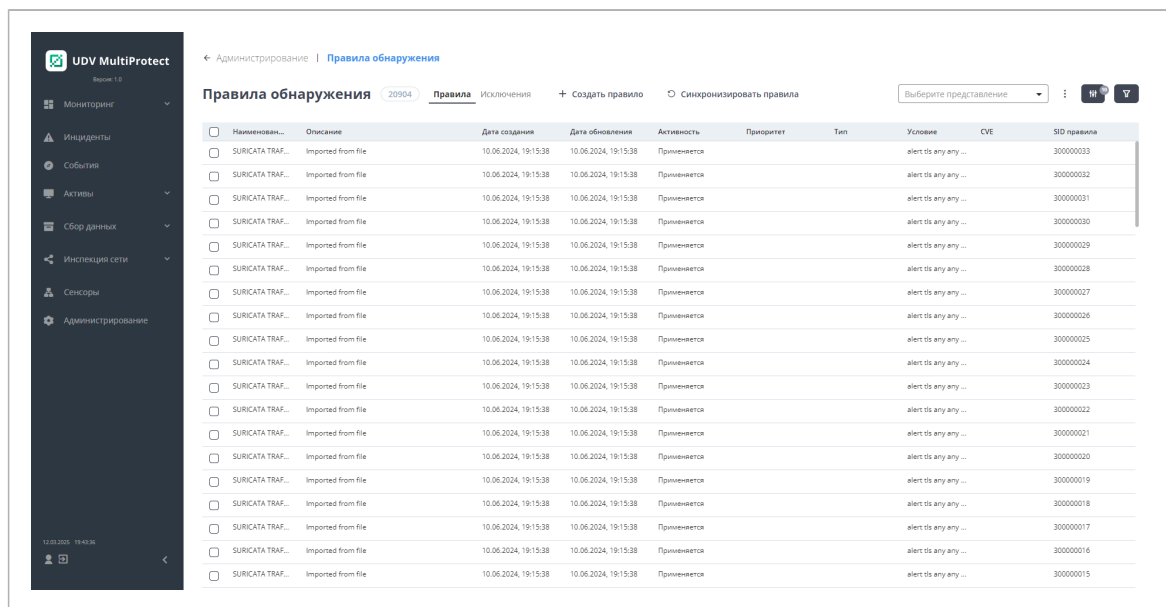


Рис. 243. Страница «Обнаружение вторжений»

10.1. Просмотр карты сети

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

Узлы и потоки, обнаруженные в анализируемом трафике, добавляются на карту автоматически, после чего пользователь может менять их состав и отображение при помощи фильтров, кнопок настройки расположения и группировки.

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

На картах могут быть отображены узлы локальной сети и элемент внешней сети.

Внешняя сеть — специфический элемент на карте, который включает в себя потоки из внешней сети в локальную и из локальной во внешнюю. Такой элемент может быть только один на карте.

Корректная работа карты сети возможна при выборе не более 500 активов для одновременного отображения.

Расположение и группировка активов

Для регулировки отображения активов на карте воспользуйтесь следующими кнопками:

-  (**Показать все узлы**) для сброса масштабирования;
-  (**Расположить на сетке**) для расположения узлов на прямоугольной плоскости равными рядами;
-  (**Расположить по кругу**) для расположения узлов на круге;
-  (**Сгруппировать по количеству потоков**) для группировки узлов в зависимости от потоков, относящихся к активам.

Фильтрация активов и потоков

Для просмотра интересующих узлов и потоков воспользуйтесь фильтрами в правой части страницы по кнопке



. Можно выбрать IP-адреса, типы активов, адреса отправителей и получателей, тип потоков (одобренные и неодобренные), последние протоколы.



Внимание:

В поля IP-адресов допускается копирование из других источников списков IP-адресов, их диапазонов или подсетей. Элементы в исходном списке должны разделяться с помощью: „ „, „ „, **Tab**, **Enter**, **Space**. Подсети задаются в формате CIDR.

Название/описание
Введите текст

IP-адреса активов
Введите IP-адреса или диапазоны

Типы активов
Выберите типы

MAC-адреса отправителя
Введите MAC-адреса

☒ Использовать условие "AND"

MAC-адреса получателя
Введите MAC-адреса

IP-адреса отправителя
Введите IP-адреса или диапазоны

☒ Использовать условие "AND"

IP-адреса получателя
Введите IP-адреса или диапазоны

Одобрённые/неодобрённые
☐ Только одобренные
☐ Только неодобренные

Последние протоколы
Последние протоколы

Применить Сбросить

Рис. 244. Фильтры на странице «Карта сети»

Масштабирование



Для масштабирования карты воспользуйтесь кнопками в левом верхнем углу страницы.

Поиск на карте

Одним из способов выделения активов и потоков данных является поиск непосредственно на карте. Поиск расположен в верхней части страницы.

Для поиска активов или потоков введите IP-адрес, имя, описание или тип актива.

После того как актив найден, вы можете нажать **Выделить**, чтобы потоки, относящиеся к активу, были выделены и появились на соответствующей вкладке в правой части страницы.

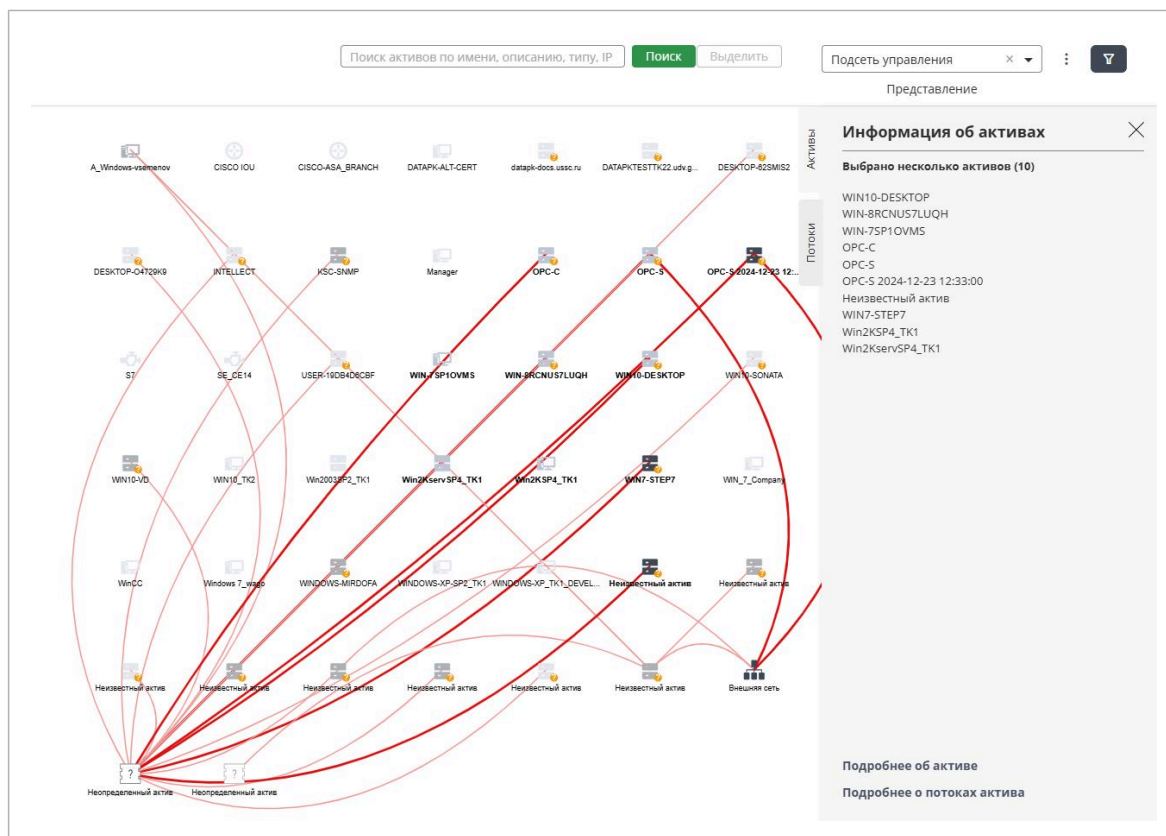


Рис. 245. Результат работы поиска и выделения

Выделение активов и потоков

На карте сети доступно выделение нескольких потоков и групп.

Для выделения активов или потоков по одному нажмите клавишу **Ctrl** и удерживайте ее во время выделения активов и (или) потоков. При таком типе выделения возможно как совместное, так и раздельное выделение активов с потоками.

Для массового выделения активов нажмите клавишу **Shift** и удерживайте ее во время выделения активов.

Для снятия выделения с отдельных активов или потоков нажмите клавишу **Ctrl** и удерживайте ее во время выделения выбранных активов или потоков. Для снятия выделения со всех активов и потоков нажмите на пустую область на карте.

10.2. Настройка представлений на карте

На странице **Карта сети** вы можете создавать, редактировать и удалять представления.

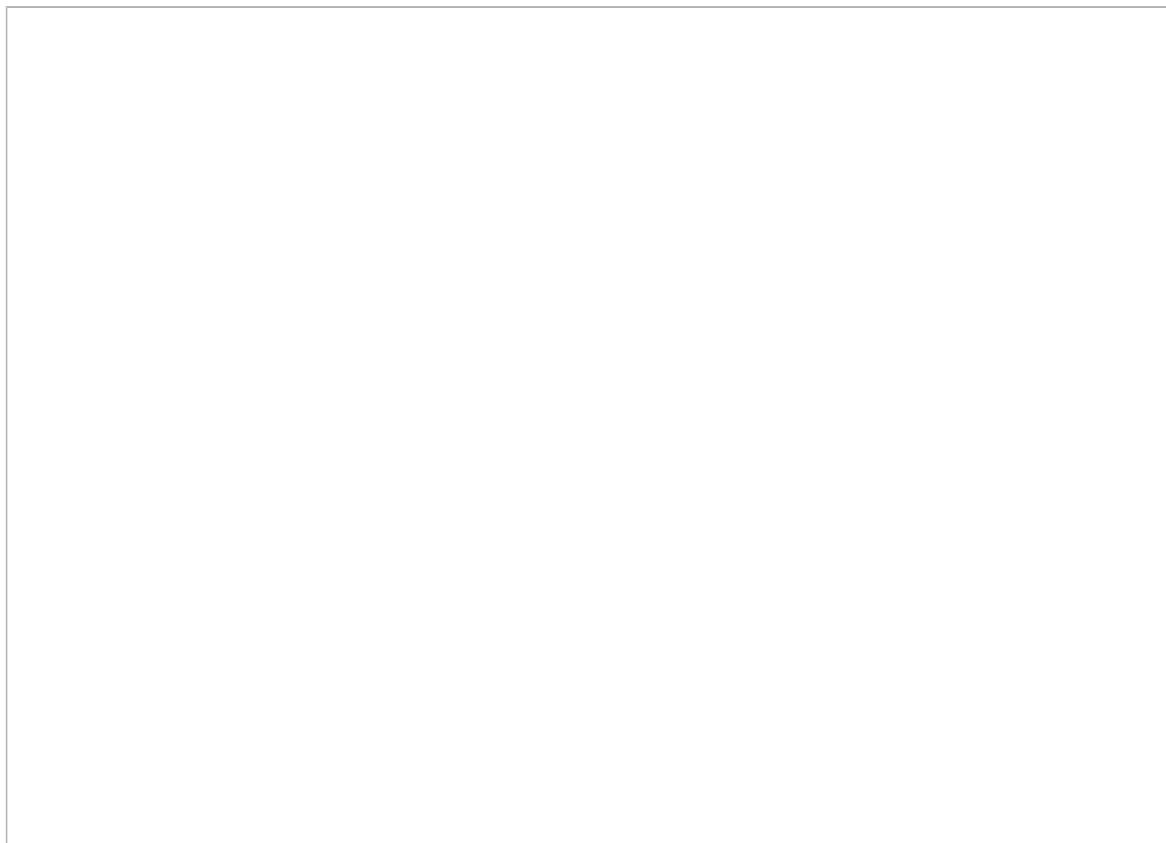


Рис. 249. Представления на странице Карта сети

К сохранению в составе представлений доступны:

- фильтры;
- группировка узлов по количеству потоков (**Сгруппировать по количеству потоков**);
- расположение элементов на карте (**Расположить на сетке**, **Расположить по кругу**).

В составе представлений не учитывается масштабирование, поиск и выделение по его результатам.

В качестве примера приводится изменение параметров фильтрации и отображения, последующее сохранение и изменение представления. Для работы с представлением на карте:

1. Измените необходимые параметры фильтров.

Пример

Например, выберите типы активов **АРМ, Маршрутизатор, Периферийное оборудование, Инженерное оборудование, Сервер, Сетевое средство защиты, Неизвестный тип**.

2. Измените параметры отображения узлов на карте.

Пример

Например, выберите группировку по количеству потоков (**Сгруппировать по количеству потоков**).

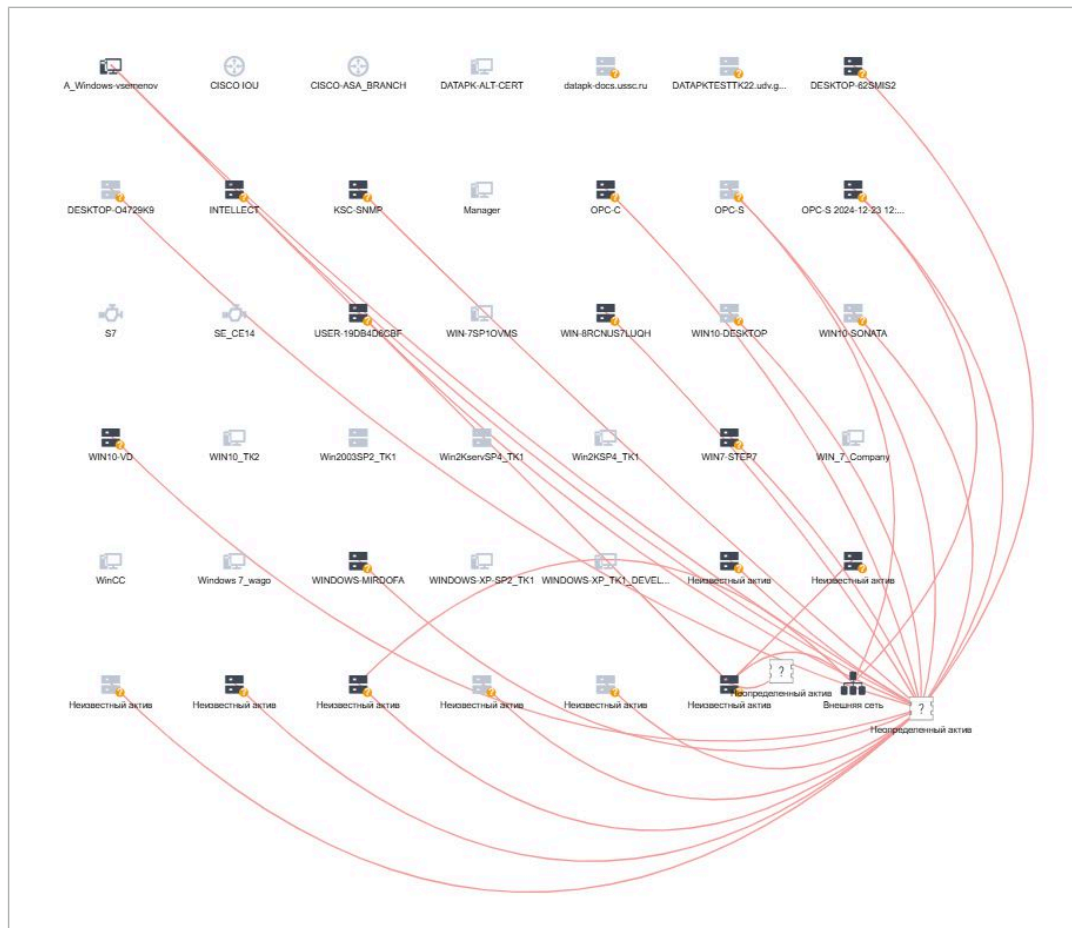


Рис. 250. Карта в результате фильтрации и изменения параметров отображения

3. В верхней правой части страницы нажмите ;
4. В раскрывающемся меню выберите опцию **Сохранить как**;
- **Результат шага:** Откроется окно сохранения представления.
5. В окне сохранения представления:

- введите наименование;



Внимание:

Имя не должно совпадать с уже существующим.

- выберите, будет ли представление доступно для использования другими пользователями.

Пример

Например, введите название **Подсеть управления** и выберите тип использования **Только для меня**.

Сохранить представление «Подсеть управления»

Наименование *

Подсеть управления

☒ Сохранить только для меня

☐ Сохранить для всех пользователей

Сохранить Отменить

Рис. 251. Окно сохранения представления

6. Нажмите **Сохранить**.

► **Результат шага:** Новое представление станет доступно для выбора.

7. В верхней части панели фильтров выберите из выпадающего списка только что созданное представление.

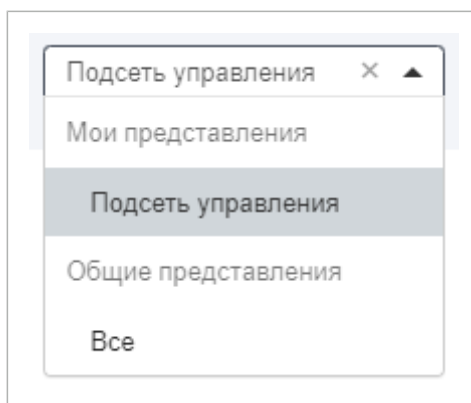


Рис. 252. Выпадающий список с доступными представлениями

8. Измените параметры фильтрации и отображение узлов на карте.

Пример

Например, выберите потоки за один месяц и расположение узлов по кругу.

► **Результат шага:** Возле названия представления в верхней части панели фильтров появится оранжевый символ *. Это означает, что есть несохраненные изменения представления.

9. Нажмите  в верхней правой части страницы.

10. В появившемся меню выберите **Редактировать**.

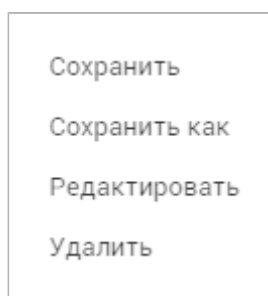
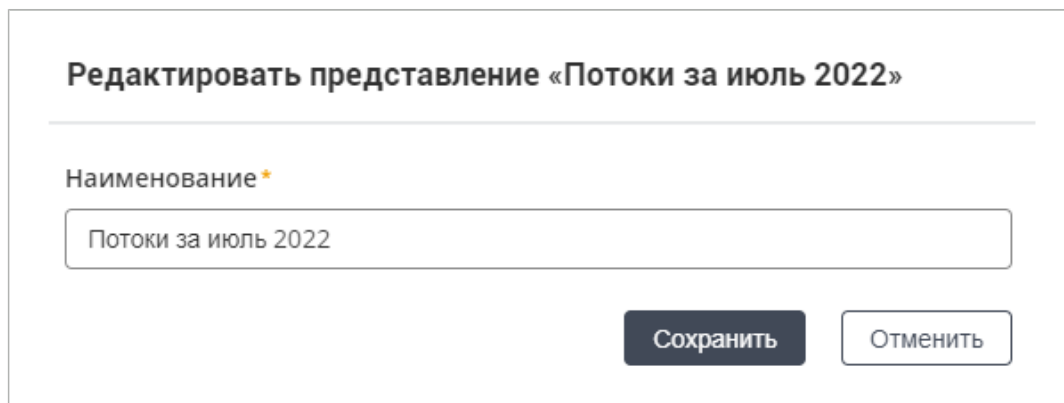


Рис. 253. Меню управления представлением

11. В окне сохранения представления введите новое имя представления.

Пример

Например, **Потоки за июль 2022**.



Редактировать представление «Потоки за июль 2022»

Наименование *

Потоки за июль 2022

Сохранить Отменить

Рис. 254. Окно редактирования представления

12. Нажмите **Сохранить**.

10.3. Просмотр потоков данных

Далее приведена основная информация о работе с информационными потоками в Комплексе.

О потоках

Информационный поток — взаимодействие, зарегистрированное сенсором между двумя узлами сети. Потоки данных регистрируются автоматически на основе известных Комплексу интерфейсов активов.

Список потоков данных представлен в виде таблицы на странице **Потоки данных**. Для навигации по списку используется область фильтров и кнопки изменения текущей страницы.

UDV MultiProtect

Версия: 1.0

Мониторинг

Инциденты

События

Активы

Сбор данных

Инспекция сети

Карта сети

Потоки данных

Правила потоков

Сенсоры

Администрирование

12.03.2025 19:42:02

Инспекция сети > Потоки данных

ДействияУправление

Всего записей: 852 | Отфильтрованных: 852

Выберите представление

Представление

Дата обнаружения	Статус	Последний расп...	IP-адрес...	Пор...	IP-адрес...	Пор...	Отправитель	Получатель
> 27.03.2024, 19:23:50	Не одобрен	arp					Неизвестный актив	Актив не определен
> 27.03.2024, 19:23:50	Не одобрен	garp					Неизвестный актив	Актив не определен
> 27.03.2024, 18:58:56	Не одобрен	tcp	10.41.56.41	61712	10.51.15.139	8443	Внешняя сеть	Неизвестный актив
> 27.03.2024, 18:58:54	Не одобрен	saf	10.41.56.41	61694	10.51.15.139	8443	Внешняя сеть	Неизвестный актив
> 27.03.2024, 18:58:54	Не одобрен	http	10.41.56.41	61688	10.51.15.139	80	Внешняя сеть	Неизвестный актив
> 27.03.2024, 18:56:28	Не одобрен	arp					Неизвестный актив	Актив не определен
> 27.03.2024, 18:56:28	Не одобрен	garp					Неизвестный актив	Актив не определен
> 27.03.2024, 18:52:37	Не одобрен	arp					Неизвестный актив	Актив не определен
> 27.03.2024, 18:52:36	Не одобрен	garp					Неизвестный актив	Актив не определен
> 27.03.2024, 18:38:49	Не одобрен	arp					Неизвестный актив	Актив не определен
> 27.03.2024, 18:38:48	Не одобрен	garp					Неизвестный актив	Актив не определен
> 27.03.2024, 18:20:19	Не одобрен	icmp_route_error	10.51.15.139		10.199.1.151		Неизвестный актив	Внешняя сеть
> 27.03.2024, 18:15:43	Не одобрен	arp					Неизвестный актив	Актив не определен
> 27.03.2024, 18:15:43	Не одобрен	garp					Неизвестный актив	Актив не определен

Рис. 255. Страница «Потоки данных»

Для получения подробной информации о потоке данных нажмите кнопку  в строке с выбранным потоком. Для просмотра карточки актива кликните по названию в колонках **Отправитель** либо **Получатель**. Для получения подробностей о протоколе, обнаруженном в потоке данных, нажмите  **Посмотреть информацию о протоколе** рядом с названием протокола.

Ethernet 802.3 

dst: 00:50:56:9d:1b:fa, src: 00:50:56:b7:cb:99, type: 2048

IPv4 (Internet Protocol version 4) 

dst: 188.43.75.32, nextp: 6, src: 192.168.243.82

TCP (Transmission Control Protocol) 

dport: 80

Рис. 256. Протоколы, обнаруженные в потоке данных

Подсказка:

Описание всех сетевых протоколов, обнаруживаемых Комплексом, вы можете найти в разделе **Протоколы, обнаруживаемые Комплексом**.

Анализ сетевых пакетов для обнаружения потоков данных выполняется сервисом глубокой инспекции пакетов (Сервис глубокой инспекции пакетов). Разбор промышленных сетевых протоколов осуществляется вплоть до управляющих команд. Список поддерживаемых промышленных протоколов см. в разделе Протоколы, обнаруживаемые Комплексом.

Элементы списка потоков данных представлены в виде пары активов «Источник — Получатель» с описанием потока: даты обнаружения и одобрения, идентификатора сенсора, зафиксировавшего поток, IP-адресов отправителя и получателя и протокола, по которому осуществляется соединение.



Внимание:

Сервис Сервис глубокой инспекции пакетов анализирует поля сетевых пакетов на базе правил на языке NetPDL. Описание пакетов может быть расширено без изменения программного кода Комплекса за счет изменения базы правил.

Для просмотра списка потоков отдельного актива перейдите в карточку актива и нажмите кнопку  **Потоки данных** на вкладке **Связанные данные**.

На странице **Карта сети** неодобренные информационные потоки между узлами будут автоматически отображаться в виде красных линий. Одобренные потоки имеют зеленый цвет.

Для получения информации о неодобренном потоке данных на карте нажмите на его изображение, после чего в правой части страницы на открывшейся панели можно просмотреть информацию о потоках, а также перейти на страницу **Потоки данных** со списком потоков данных между выбранными объектами на карте.

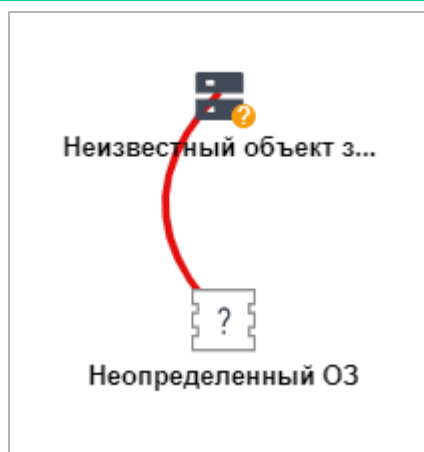


Рис. 257. Изображение неодобренных потоков данных на карте сети



Рис. 258. Изображение одобренных потоков данных на карте сети

10.4. Управление потоками данных

В этом разделе:

- Фильтрация списка потоков данных
- Отчет по потокам данных
- Изменение потоков данных
- Экспорт и импорт правил управления потоками данных

Для управления потоками пользователю доступно одобрение, временное одобрение, отмена одобрения, генерация отчета, экспорт и импорт правил управления потоками.

10.4.1. Фильтрация списка потоков данных

Комплекс позволяет фильтровать отображаемые потоки данных. На странице **Потоки данных** по кнопке  доступны следующие фильтры:

1. **MAC-адреса отправителя.** Фильтрация выполняется по распознанным MAC-адресам источника.
2. **Использовать условие «AND».** Позволяет отображать только те потоки данных, в которых одновременно присутствуют указанные IP и (или) MAC-адреса для источника и получателя. При отмене параметра **Использовать условие «AND»** будут отображены потоки данных, в которых присутствуют указанные параметры хотя бы для одного из узлов.



Внимание:

Нельзя указывать суммарно более 10000 IP-адресов отправителей и получателей.

3. **MAC-адреса получателя.** Фильтрация выполняется по распознанным MAC-адресам получателя.



Внимание:

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

4. **IP-адреса отправителя.** Фильтрация выполняется по распознанным IP-адресам источника.
5. **IP-адреса получателя.** Фильтрация выполняется по распознанным IP-адресам получателя.



Внимание:

В поля IP-адресов допускается копирование из других источников списков IP-адресов, их диапазонов или подсетей. Элементы в исходном списке должны разделяться с помощью: ,, ,, **Tab**, **Enter**, **Space**. Подсети задаются в формате CIDR.

6. **Только содержащие IP.** Позволяет отфильтровать только потоки с IP-адресами. Фильтр не влияет на наличие MAC-адресов в потоках.
7. **Только без IP.** Позволяет отфильтровать только потоки, не имеющие IP-адресов. Фильтр не влияет на наличие MAC-адресов в потоках.

**Внимание:**

Фильтры **Только содержащие IP** и **Только без IP** взаимоисключающие.

8. **Использовать "AND" для пар IP и MAC.** Фильтрация выполняется только при наличии указанных IP и MAC-адресов отправителя и получателя.
9. **Источник не находится в подсетях.** Позволяет фильтровать только отправителей, которые находятся в подсетях, отличных от указанных.
10. **Получатель не находится в подсетях.** Позволяет фильтровать только получателей, которые находятся в подсетях, отличных от указанных.
11. **Порты отправителя.** Фильтрация выполняется по распознанным портам, с которых были отправлены данные.

**Подсказка:**

Между фильтрами по портам источника и получателя располагается текст Или. Это означает, что фильтрация потоков будет осуществлена, если найдется хотя бы один порт, принадлежащий источнику или получателю.

12. **Порты получателя.** Фильтрация выполняется по распознанным портам, на которые были получены данные.
13. **Изменил статус.** Фильтрация выполняется по субъекту, выполнившему изменение статуса потока данных.
14. **Одобрённые/неодобрённые.** Фильтрация выполняется по статусу потока данных.
15. **Сенсор.** Фильтр содержит наименования сенсоров, подключенных к Комплексу. Можно выбирать несколько наименований. При применении фильтра отобразятся потоки, обнаруженные выбранными сенсорами.
16. **Последние протоколы.** Фильтрация выполняется по распознанному протоколу.
17. **Дата и время обнаружения.** Фильтрация выполняется по потокам данных, обнаруженным в указанный временной период. Существует возможность указания текущих суток в качестве быстрого фильтра.
18. **Дата и время изменения статуса.** Фильтрация выполняется по потокам данных, чей статус был изменен в указанный временной период.
19. **Комментарий.** Фильтрация выполняется по потокам данных, которым добавлен указанный комментарий или его часть.

**Подсказка:**

Поле **Комментарий** является регистронезависимым.

MAC-адреса отправителя
Введите MAC-адреса

☒ Использовать условие "AND"

MAC-адреса получателя
Введите MAC-адреса

IP-адреса отправителя
Введите IP-адреса или диапазоны

Порты получателя
Введите порты или диапазоны

Изменил статус
Введите имя пользователя

Одобренные/неодобранные
☐ Только одобренные
☐ Только неодобранные

Сенсор

Рис. 259. Панель фильтров на странице «Потоки данных»

Комплекс позволяет выполнять групповые операции над потоками, выбранными фильтрами, а именно:

- одобрить потоки;
- временно одобрить потоки;
- убрать одобрение с потоков;
- создать отчет;
- удалить потоки.

10.4.2. Отчет по потокам данных

После формирования списка необходимых потоков можно выгрузить их в отчет. Для этого:

1. В верхней части страницы нажмите кнопку **Создать отчет** в верхней части страницы.
2. В окне **Создание отчета** выберите формат файла (pdf или **xlsx**).
3. Выберите столбцы, которые будут отражены в отчете. Для выбора доступны следующие столбцы:
 - Дата обнаружения
 - Сенсор
 - Дата изменения статуса
 - Дата окончания временного одобрения
 - Статус
 - Последний распознанный протокол
 - IP-адрес отправителя
 - Порт отправителя
 - IP-адрес получателя
 - Порт получателя
 - Отправитель
 - Получатель
 - Пользователь
 - Комментарий
 - MAC-адрес отправителя
 - MAC-адрес получателя
 - EtherType
 - VLANType
 - Следующий за IP протокол
 - Следующий заголовок IPv6
4. Нажмите **Запустить создание отчета**.
 - **Результат шага:** В правом верхнем углу появится уведомление **Задача создания отчета запущена**, а статус в строке **Текущее состояние задачи создания отчета** изменится на **Выполняется**.
5. Для сохранения отчета после того, как он сформирован, нажмите на ссылку на файл с отчетом.



Подсказка:

Подробнее см. в разделе [Выгрузка отчетов](#).

10.4.3. Изменение потоков данных

При появлении нового потока данных необходимо принять решение по его одобрению или удалению. Новые неподтвержденные потоки данных не имеют записи в столбце **Дата изменения статуса**.

В интерфейсе Комплекса возможно одобрение и удаление потоков в ручном и автоматическом режимах. Чтобы ознакомиться с предложенными способами, перейдите в следующие разделы:

- [Одобрение и удаление потоков данных в ручном режиме](#)
- [Одобрение потоков данных в автоматическом режиме](#)
 - [Создание правил управления потоками данных](#)

10.4.3.1. Одобрение и удаление потоков данных в ручном режиме

Интерфейс Комплекса предоставляет широкие возможности по работе с потоками данных:

1. [Одобрение, в том числе групповое.](#)
2. [Временное одобрение, в том числе групповое.](#)
3. [Отмена одобрения, в том числе групповая.](#)
4. [Удаление, в том числе групповое.](#)

10.4.3.1.1. Одобрение потоков данных

В интерфейсе Комплекса возможно как единичное одобрение потока, так и групповое одобрение потоков, а также одобрение потоков, отображаемых на карте. Порядок действий:

1. Перейдите на страницу **Инспекция сети** → **Потоки данных**.
2. Для одобрения потока:
 - а. Выберите из списка необходимый поток и в правой колонке нажмите кнопку  (**Одобрить поток**).
 - б. В открывшемся окне введите комментарий для обоснования одобрения потока данных и нажмите кнопку **Подтвердить**.

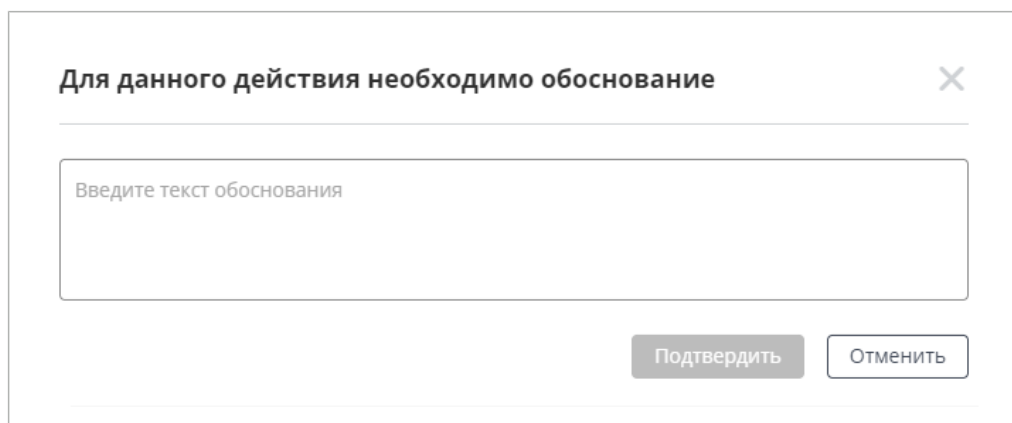


Рис. 260. Подтверждение одобрения потока

3. Для группового одобрения потоков:

- а. На странице **Потоки данных** выполните необходимую настройку фильтров и нажмите кнопку **Применить**.
 - б. Нажмите кнопку  (**Одобрить потоки**) над областью фильтров.
 - в. В появившемся окне введите обоснование одобрения списка потоков данных и нажмите кнопку **Подтвердить**.
4. Для одобрения потоков данных, отображаемых на карте:
 - а. Перейдите на страницу **Инспекция сети** → **Карта сети**.
 - б. Выберите интересующие потоки данных или актив на карте.



Подсказка:

Подробнее см. в разделе [Просмотр карты сети](#).

- **Результат шага:** Откроются вкладки **Активы** и **Потоки** в правой части страницы.
- в. На одной из вкладок нажмите кнопку **Подробнее о потоках**.
 - **Результат шага:** Откроется страница **Потоки данных** со списком выбранных потоков.
 - г. Выполните групповое одобрение потоков согласно шагу 3.

10.4.3.1.2. Временное одобрение потоков данных

В интерфейсе Комплекса возможно как единичное временное одобрение потока, так и групповое временное одобрение потоков. Порядок действий:

1. Перейдите на страницу **Инспекция сети** → **Потоки данных**.
2. Для временного одобрения потока:
 - а. Выберите из списка необходимый поток и в правой колонке нажмите кнопку  (**Временно одобрить поток**).
 - б. В открывшемся окне выберите дату и время, когда поток вновь станет неодобренным, и нажмите кнопку **Далее**.

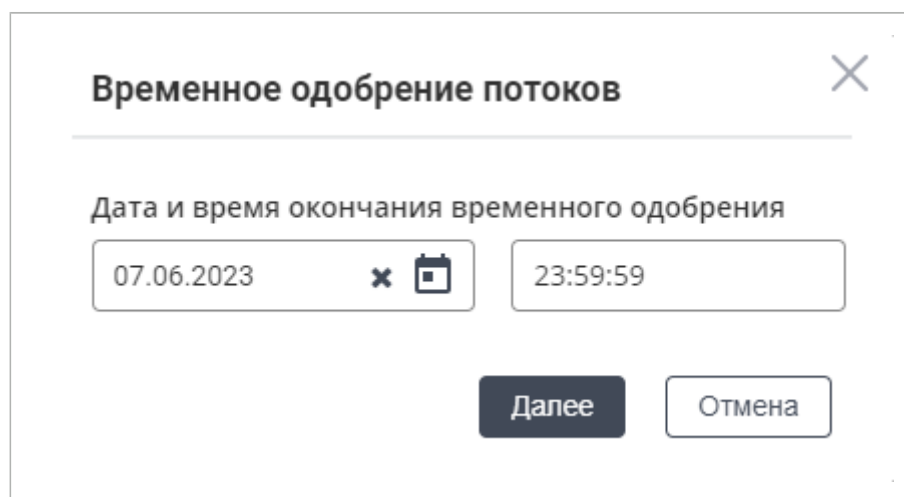


Рис. 261. Окно выбора даты окончания временного одобрения потока

► **Результат шага:** Откроется окно ввода обоснования.

- в. Введите обоснование временного одобрения потока данных и нажмите кнопку **Подтвердить**.

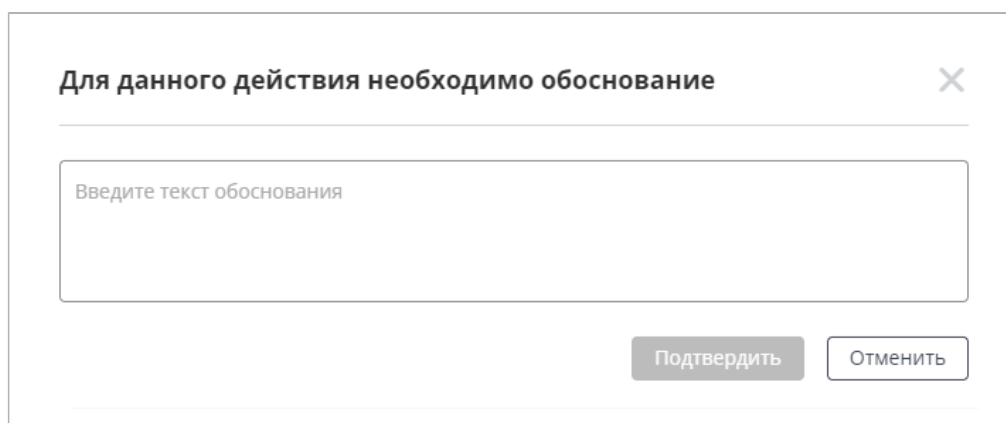


Рис. 262. Окно ввода обоснования изменения потока

► **Результат шага:** Дата одобрения и дата окончания временного одобрения отобразятся в строке с временно одобренным потоком. По истечении срока одобрения поток будет удален.

Дата обнаружения	Статус	Последний распознанный протокол	Отправитель	Получатель	Дата окончания временного одобрения	
> 07.06.2023, 15:03:14	Одобен	mDNS	WIN-TSP10VMS	Multicast	11.06.2023, 23:59:59	✓ ⌕ ⌚ 🗑

Рис. 263. Временно одобренный поток

3. Для группового временного одобрения потоков:

а. На странице **Потоки данных** выполните необходимую настройку фильтров и нажмите **Применить**.

б. Нажмите кнопку  (**Временно одобрить потоки**) на панели **Действия** в верхней части страницы. В появившемся окне выберите дату и время, когда потоки вновь станут неодобренными, и нажмите кнопку **Далее**.

в. В появившемся окне введите обоснование временного одобрения списка потоков данных и нажмите **Подтвердить**.

10.4.3.1.3. Отмена одобрения потока данных

В интерфейсе Комплекса возможна отмена одобрения как одного, так и нескольких потоков данных. Порядок действий:

1. Перейдите на страницу **Инспекция сети** → **Потоки данных**.
2. Для отмены одобрения потока:
 - а. Выберите из списка одобренный поток и в правой колонке нажмите кнопку  (**Убрать одобрение с потока**).
 - б. В открывшемся окне введите комментарий для обоснования отмены одобрения потока данных и нажмите **Подтвердить**.

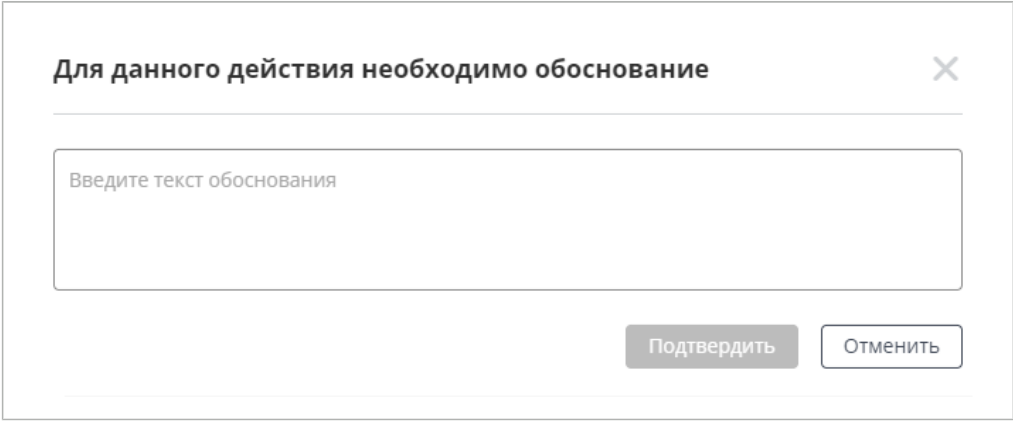


Рис. 264. Подтверждение отмены одобрения потока

3. Для групповой отмены одобрения потоков:
 - а. На странице **Потоки данных** установите чекбокс **Только одобренные**, выполните необходимую настройку других фильтров и нажмите **Применить**.
 - б. Нажмите кнопку  (**Убрать одобрение с потоков**) над областью фильтров.
 - в. В появившемся окне введите обоснование действия (отмены одобрения списка потоков данных) и нажмите **Подтвердить**.

10.4.3.1.4. Удаление потоков данных

В интерфейсе Комплекса возможно удаление как одного, так и нескольких потоков данных. Порядок действий:

1. Перейдите на страницу **Инспекция сети** → **Потоки данных**.
2. Для удаления потока:
 - а. Выберите из списка необходимый поток и в правой колонке нажмите кнопку  (**Удалить поток**).
 - б. В открывшемся окне введите обоснование удаления потока данных и нажмите **Подтвердить**.

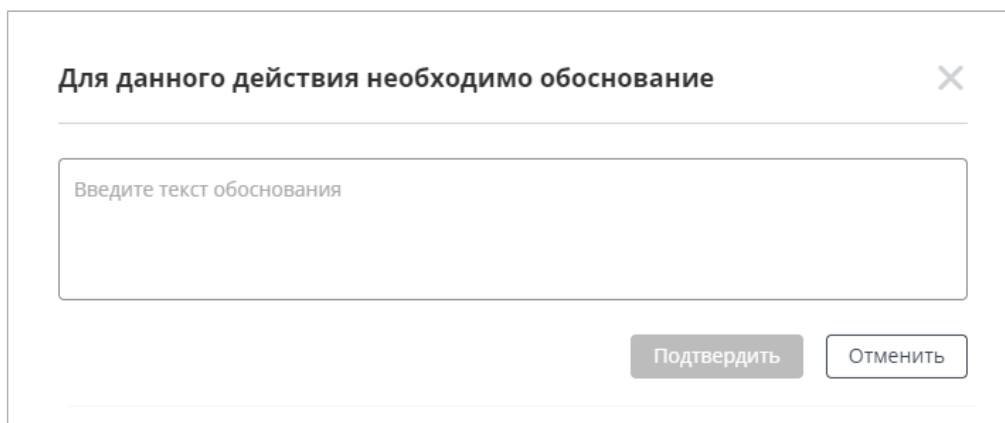


Рис. 265. Подтверждение удаления потока

3. Для группового удаления потоков:
 - а. На странице **Потоки данных** выполните необходимую настройку фильтров и нажмите **Применить**.
 - б. Нажмите кнопку  (**Удалить потоки**) над областью фильтров.
 - в. В появившемся окне введите обоснование удаления списка потоков данных и нажмите **Подтвердить**.

10.4.3.2. Изменение комментария

Для изменения комментария, указанного при обосновании одобрения потока данных:

1. Перейдите на страницу **Инспекция сети** → **Потоки данных**.
2. Выберите из списка необходимый поток и в правой колонке нажмите кнопку  (**Редактировать комментарий**).
3. В открывшемся окне отредактируйте комментарий и нажмите **Сохранить**.

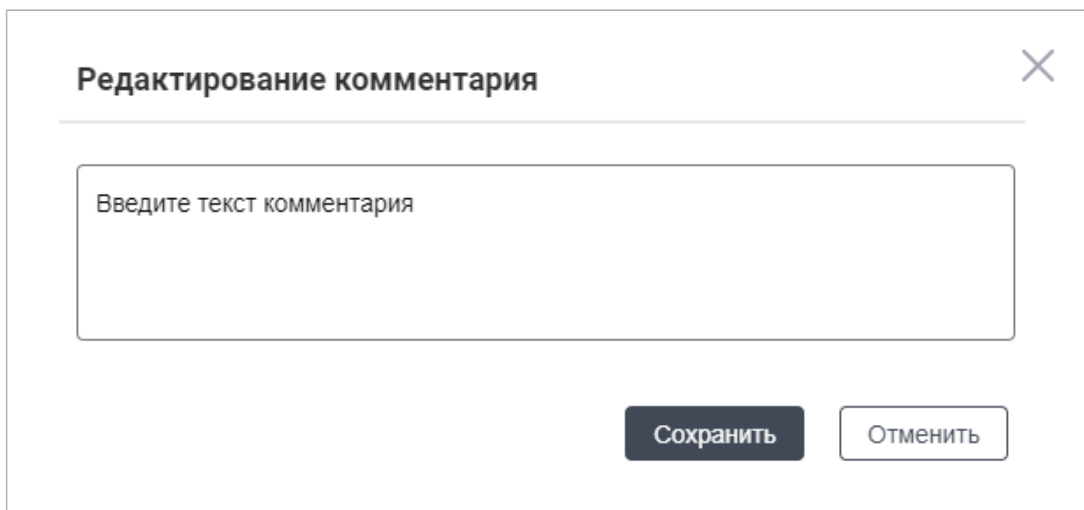


Рис. 266. Окно «Редактирование комментария»

10.4.3.3. Одобрение потоков данных в автоматическом режиме

В интерфейсе Комплекса верхнего уровня есть возможность создания правил для автоматического присвоения статуса потокам данных, либо для автоматического удаления. Правила применяются к потокам, попадающим под параметры потоков, указанные в правиле.

Для настройки правил доступны следующие параметры:

1. **Номер** — целое число, определяющее приоритет (порядок применения) правил: чем меньше число, тем выше приоритет. Правила при создании автоматически нумеруются с интервалом в 100 единиц. Возможно изменять номера правила вручную на любое другое число, отличное от уже номеров, уже присвоенных другим правилам.
2. **Наименование правила** (должно быть уникальным).
3. **Комментарий к правилу**. Указывается администратором в качестве причины установления статуса потокам выбранным правилом. Указанный комментарий отображается на странице «Потоки» для тех потоков, статус которых был изменен в результате применения правила.
4. **Фильтр** — один или несколько параметров потоков, к которым необходимо применить выбранное правило. Список фильтров для настройки правила совпадает со списком фильтров на странице [Инспекция сети](#) → [Потоки данных](#) (описание фильтров приведено в разделе «[Фильтрация списка потоков данных](#)»).
5. **Действие**, которое необходимо выполнить с потоками (одобрить или временно одобрить).
6. Чекбокс **Активность правила**.

Параметры правил потоков данных, недоступные для редактирования:

- время создания правила;
- время изменения правила;
- автор правила — последний пользователь, изменивший правило. Если правило настроено для автоматического одобрения потоков, его автор будет отображаться на странице [Потоки данных](#) в качестве пользователя, который выполнил одобрение потоков с помощью этого правила.



Внимание:

Особенности работы правил :

- Управлять потоками данных с использованием правил можно только для новых потоков, которые были обнаружены после создания правил, под которые они попадают.
- Правила, которые необходимо применять к новым потокам данных, не должны содержать фильтры **Дата и время обнаружения, Дата и время одобрения, Комментарий, Только одобренные/неодобренные**.
- Один поток обрабатывается первым по приоритету подходящим правилом. Оставшиеся подходящие правила с меньшим приоритетом к тому же потоку не будут применяться.
- Если в фильтре правила настроен параметр **Протокол**, указанный фильтр будет применяться только к последнему распознанному в потоке протоколу.
- Правила временного одобрения потоков в автоматическом режиме перестают действовать по истечении указанных даты и времени окончания одобрения. Если поток был обнаружен после окончания действия правила временного одобрения, то статус этого потока не изменится.

10.4.3.3.1. Создание правил управления потоками данных

Для создания правила управления потоками данных:

1. Перейдите на страницу **Инспекция сети** → **Правила потоков**.

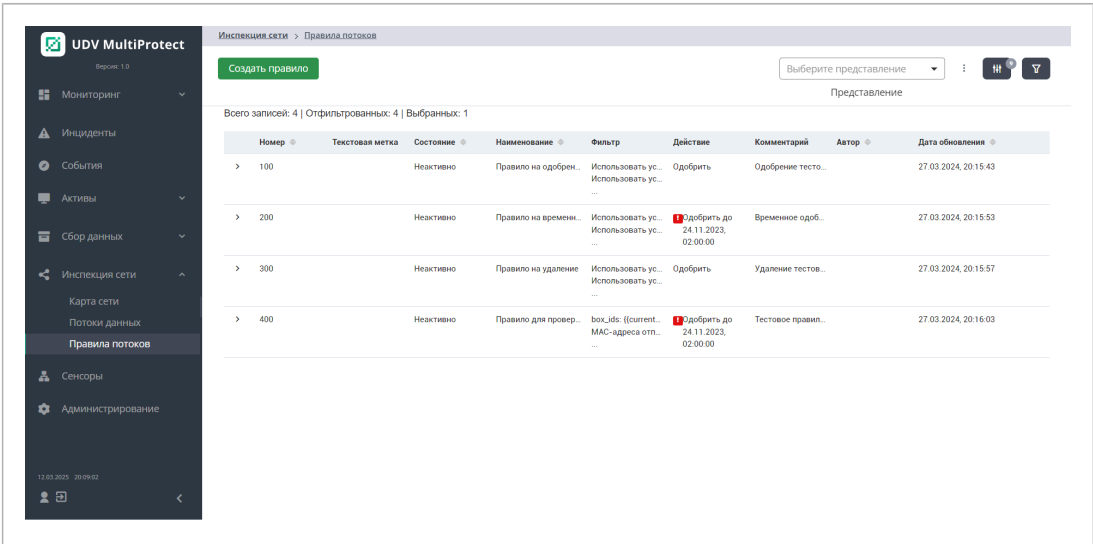


Рис. 267. Страница «Правила потоков»

2. Нажмите **Создать правило**.
3. В открывшемся окне задайте следующие параметры:
- а. номер правила;
 - б. маркирующий текст в поле **Текстовая метка**;
 - в. наименование нового правила;
 - г. выберите из списка действие, которое будет применяться к потокам: **Одобрить** или **Временно одобрить**;



Внимание:

При выборе действия **Временно одобрить** выберите дату и время окончания одобрения потоков.

- д. введите обоснование, которое будет отображаться в событиях при выполнении действия с событиями;
- е. установите чекбокс **Активность правила** для включения работы правила;
- ж. настройте фильтры для определения потоков, к которым необходимо применять правило в разделе **Фильтр**. Доступны следующие фильтры:
 - MAC-адреса отправителя;
 - MAC-адреса получателя;



Внимание:

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

- IP-адреса отправителя;
- IP-адреса получателя;



Внимание:

В поля IP-адресов допускается копирование из других источников списков IP-адресов, их диапазонов или подсетей. Элементы в исходном списке должны разделяться с помощью: „ „, „ „, **Tab**, **Enter**, **Space**. Подсети задаются в формате CIDR.

- порты отправителя;
- порты получателя;
- чекбоксы использования IP и MAC-адресов;
- последние протоколы;
- дата и время обнаружения.

4. Нажмите **Создать**.

10.4.4. Фильтрация списка правил управления потоками данных

Комплекс позволяет фильтровать отображаемые правила управления потоками данных. На странице **Правила потоков** по кнопке  доступны следующие фильтры:

1. **Наименование** — фильтрация выполняется по названию правила.
2. **Автор правила** — позволяет отфильтровать правила потоков, которые были созданы пользователем с указанными фамилией, именем и отчеством.
3. **Статус активности** — позволяет отфильтровать правила потоков по статусу их активности. Для выбора доступен чекбокс **Только активные** или **Только неактивные**
4. **Дата и время создания** — фильтрация выполняется по правилам потоков, созданным в указанный временной период. Также для фильтрации можно указать текущие сутки, нажав кнопку **Установить текущие сутки**
5. **Текстовая метка** — позволяет отфильтровать правила по описанию.
6. **IP-адреса отправителя** — фильтрация выполняется по распознанным IP-адресам источников.
7. **IP-адреса получателя** — фильтрация выполняется по распознанным IP-адресам получателей.
8. **Порты отправителя** — фильтрация выполняется по распознанным портам, с которых были отправлены данные.
9. **Порты получателя** — фильтрация выполняется по распознанным портам, на которые были получены данные.

Наименование

Автор правила

Статус активности
☐ Только активные
☐ Только неактивные

Дата и время создания

От

До

Установить текущие сутки

Текстовая метка

IP-адреса отправителя

IP-адреса получателя

Порты отправителя

Порты получателя

Применить

Сбросить

Рис. 269. Панель фильтров на странице «Правила потоков»

10.4.5. Экспорт и импорт правил управления потоками данных

Экспорт и импорт правил управления потоками данных осуществляется на странице **Администрирование** → **Основные настройки** → **Импорт и экспорт** на панели **Правила потоков**.

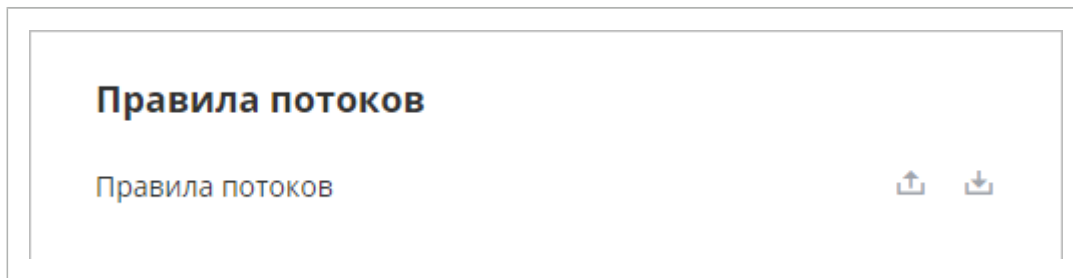


Рис. 270. Панель управления экспортом и импортом правил потоков

В этом разделе:

- Экспорт правил управления потоками данных
- Импорт правил управления потоками данных

10.4.5.1. Экспорт правил управления потоками данных

Для экспорта правил управления потоками данных в файл формата *.json:

1. Перейдите на страницу **Администрирование** → **Основные настройки** → **Импорт и экспорт**.
2. На панели **Правила потоков** нажмите кнопку  (**Экспортировать**).
 - **Результат шага:** Файл со списком правил управления потоками данных `adfh_rules[дата и время].json` будет сформирован и доступен для скачивания в правом верхнем углу страницы **Импорт и экспорт** под заголовком **Результат последнего экспорта**.
3. Для скачивания файла нажмите на название сформированного файла под заголовком **Результат последнего экспорта**.
4. В открывшемся окне укажите расположение для экспортируемого файла, введите название файла и нажмите **Сохранить**.

10.4.5.2. Импорт правил управления потоками данных

Для импорта справочника с правилами управления потоками данных из файла формата *.json:

1. Перейдите на страницу **Администрирование** → **Основные настройки** → **Импорт и экспорт**.
2. На панели **Правила потоков** нажмите кнопку  (**Импортировать**).
3. В открывшемся окне укажите расположение импортируемого файла формата *.json и подтвердите выбор.
4. Убедитесь, что список правил был успешно загружен. Сразу после загрузки файла в правом верхнем углу страницы **Импорт и экспорт** появится уведомление **Список «Правила потоков» успешно обновлен**, а на странице **Правила потоков** отобразятся импортированные правила.

10.5. Служба обнаружения вторжений

В этом разделе:

- Создание правил обнаружения вторжений
- Управление службой обнаружения вторжений
- Экспорт и импорт правил службы обнаружения вторжения
- Импорт правил обнаружения вторжений в формате *.json
- Импорт правил обнаружения вторжений в формате *.rules
- Экспорт правил службы обнаружения вторжений
- Создание исключений для правил обнаружения вторжений
- Удаление исключений для правил обнаружения вторжений

Правила обнаружения вторжений

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

Правила обнаружения вторжений расположены во вкладке **Правила** на странице **Правила обнаружения**.

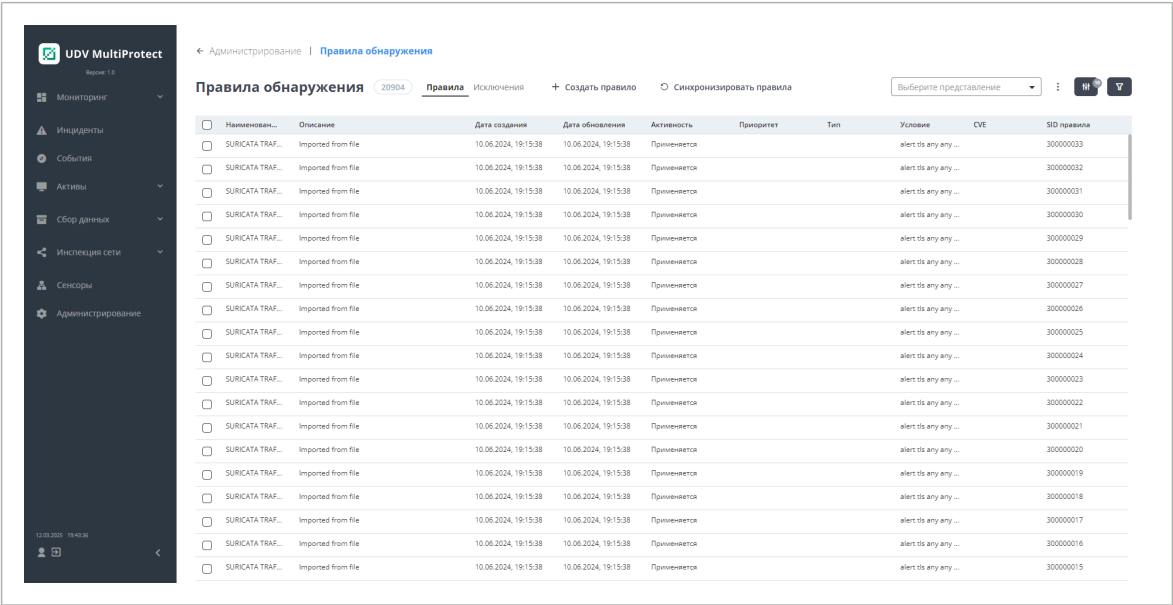


Рис. 271. Страница «Правила обнаружения»

Правила обнаружения состоят из заголовка и опций. Заголовок содержит следующую информацию:

- описание действия;
- протокол передачи данных;
- IP-адреса;
- сетевые маски;
- порты источника и назначения.

После заголовка правила следуют опции. Они включают определение дополнительных критериев выполнения правила и определение дополнительных реагирующих действий. Они используются для организации более направленной фильтрации трафика. Весь набор опций заключается в круглые скобки, сами опции отделяются друг от друга с помощью точки с запятой (последняя опция в списке тоже должна заканчиваться данным символом). Ключевые слова опций отделяются от своих аргументов двоеточием.

Синтаксис записи правил в формате Suricata:

```
[Действие] [Протокол] [IP-адреса отправителей] [Порты отправителей] [Оператор направления] [IP-адреса получателей] [Порты получателей] (ключ_1 : значение_1; ключ_2 : значение_2; ... ключ_N : значение_N;)
```

Пример содержимого файла с правилами обнаружения формата Suricata:

```
# test rule that catches all ICMP packets:
alert icmp any any -> any any (msg:"ICMP test detected"; GID:1; sid:11111111; rev:001;
  classtype:icmp-event;)
# rules for S7
alert tcp any any -> any 102 (msg:"Response (when error)"; content:"|02|"; offset:17; depth:1;
  sid:10000001; rev:001; priority:10;)
alert tcp any any -> any 102 (msg:"Read area"; content:"|04|"; offset:17; depth:1;sid:10000002;
  rev:001; priority:10;)
```

Веб-интерфейс Комплекса позволяет загрузить правила обнаружения несколькими способами:

- создавать запись о новом правиле вручную на странице **Правила обнаружения**;
- импортировать файл формата Suricata с расширением *.rules, содержащий список правил;
- импортировать файл формата *.json, содержащий список правил.

Зарегистрированные службой обнаружения вторжений события отображаются в списке событий на странице **События**, а также на панелях мониторинга. Подробнее см. раздел «Обнаружение вторжений».

Пользователь с ролью **Администратор** может фильтровать правила на странице **Правила обнаружения** по следующим признакам:

- статус активности — только активные или только неактивные правила;
- дата и время создания правила;
- дата и время обновления правила;
- тип правила — значение поля classtype (для правил без типа это поле имеет значение Без типа);
- приоритет — Очень низкий, Незначительный, Низкий, Средний, Высокий, Без приоритета.

Исключения для правил обнаружения вторжений

Также пользователь с ролью **Администратор** может создавать исключения для правил обнаружения вторжений для того, чтобы исключить определенные правила, которые не должны работать на одном выбранном сенсоре.

Исключения для правил обнаружения вторжений расположены во вкладке **Исключения** на странице **Правила обнаружения**.

Исключения можно отфильтровать по следующим признакам:

- дата и время создания исключений;
- автор — пользователь, создавший исключения;
- сенсор — сенсор, на котором применяются исключения;

- SID правил — идентификаторы правил обнаружения вторжений, для которых были созданы исключения.



Внимание:

В фильтре **SID правил** можно указать как один идентификатор правила, так и определенный диапазон идентификаторов правил через тире.

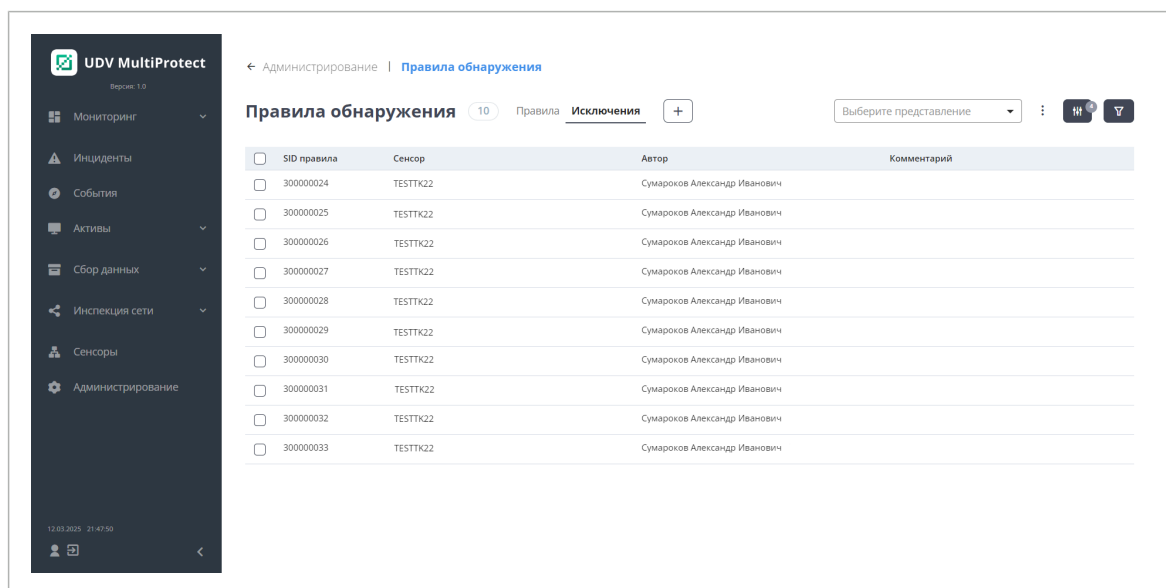


Рис. 272. Вкладка «Исключения» на странице «Обнаружение вторжений»



Внимание:

Для создания исключения с более точными сетевыми параметрами (например, с определенным IP-адресом) необходимо вручную создавать pass-правило обнаружения вторжений (подробнее см. в разделе [Изменение правила с SID в диапазоне, отличающемся от пользовательского](#)).

10.5.1. Создание правил обнаружения вторжений

Для создания правил обнаружения в веб-интерфейсе Комплекса.

1. Перейдите на страницу **Администрирование** → **Правила обнаружения**.
2. Нажмите **Создать правило**. В открывшемся окне задайте следующие параметры:
 - наименование и описание создаваемого правила;
 - правило обнаружения в формате Suricata в поле **Условие**;



Внимание:

Убедитесь, что уникальный идентификатор сигнатуры (sid) не совпадает с sid других правил, загруженных ранее в Комплекс. Рекомендуемый диапазон пользовательских правил: от 94000000 до 94999999.

- чекбокс **Активность** для активации правила.

Создание правила обнаружения вторжений

Наименование *

PLC Allen Bradley Stopped

Описание

Allen Bradley operations

Условие *

alert tcp any any -> any 44818 (msg:"PLC Allen Bradley Stop Command";content:"|07 02 20 8e 24 01|"; sid:94123635;)

☒ Активность

Создать

Отменить

Рис. 273. Окно «Создание правила обнаружения вторжения»

3. Нажмите **Создать**.

10.5.2. Управление службой обнаружения вторжений

Доступны следующие действия со службой обнаружения вторжений:

- Запуск и остановка службы обнаружения вторжений на сенсорах
- Активация и деактивация правил обнаружения вторжений
- Редактирование правил обнаружения вторжений
- Изменение правила с SID в диапазоне, отличающемся от пользовательского
- Удаление правил обнаружения вторжений, синхронизация правил



Внимание:

При внесении изменений правила синхронизируются с сенсорами автоматически. При возникновении ошибки **Не удалось автоматически синхронизировать правила на сенсорах. Синхронизируйте правила вручную по кнопке «Синхронизировать правила»** нажмите **Синхронизировать правила**.

10.5.2.1. Запуск и остановка службы обнаружения вторжений на сенсорах

Для запуска или остановки службы на сенсорах:

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

10.5.2.2. Активация и деактивация правил обнаружения вторжений

При работе с правилами обнаружения вторжений их можно активировать или деактивировать. Доступна активация и деактивация как одного, так и нескольких правил.

1. Для активации или деактивации одного правила:
 - а. Перейдите на страницу **Администрирование** → **Правила обнаружения**.
 - б. Для включения одного правила нажмите на необходимое правило из списка и в открывшейся справа карточке правила нажмите кнопку  **Активировать** в левом верхнем углу.
 - в. Для отключения одного правила нажмите на необходимое правило из списка и в открывшейся карточке правила нажмите кнопку  **Деактивировать** в верхней части карточки правила.
2. Для активации или деактивации нескольких правил:
 - а. Перейдите на страницу **Администрирование** → **Правила обнаружения**.
 - б. Для включения нескольких правил установите чекбоксы возле необходимых правил и в открывшемся внизу меню нажмите кнопку  **Активировать**
 - в. Для выключения нескольких правил установите чекбоксы возле необходимых правил и в открывшемся внизу меню нажмите кнопку  **Деактивировать**

10.5.2.3. Редактирование правил обнаружения вторжений

Для редактирования правила:

1. Нажмите на необходимое правило из списка.
2. Нажмите  (**Редактировать**) в открывшейся карточке правила.
 - **Результат шага:** Откроется карточка **Редактирование правила обнаружения**.
3. Измените необходимые параметры в окне **Редактирование правила обнаружения вторжений** и нажмите **Сохранить**.

 **Внимание:**

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

Редактирование правила обнаружения

×

Наименование *

Описание

Условие *

```
alert tls any any -> any any (msg:"SURICATA TRAFFIC-ID: twitter"; tls_sni;
content:"twitter.com"; isdataat:!1,relative; flow:to_server,established; flowbits:
set,traffic/id/twitter; flowbits:set,traffic/label/social-network; noalert; sid:300000029;
rev:1;)
```

☒ **Активность**

Сохранить

Отменить

Рис. 274. Окно редактирования правила обнаружения вторжения

- **Результат шага:** Отредактированное правило будет сохранено как новое правило обнаружения вторжений. Исходное правило также сохранится.

10.5.2.4. Изменение правила с SID в диапазоне, отличающемся от пользовательского

Для изменения правила с SID в диапазоне, отличающемся от пользовательского (94000000-94999999):

1. Нажмите на необходимое правило из списка.
2. Нажмите  (**Редактировать**) в открывшейся карточке правила.
 - **Результат шага:** Откроется карточка **Редактирование правила обнаружения**.
3. Скопируйте значения полей окна.
4. При необходимости отмените выбор чекбокса **Активность** и нажмите **Сохранить**
5. Нажмите **Создать правило**
6. Вставьте скопированные ранее значения полей окна в соответствующие поля окна создания правила.
7. Измените sid так, чтобы он входил в пользовательский диапазон (94000000-94999999) и не совпадал с другими правилами.
8. Измените необходимые параметры правила.



Подсказка:

Для ограничения срабатывания правила на конкретные IP-адреса замените значение свойства Action с alert на pass и адреса отправителей и получателей.

Пример

Например, оригинальное правило с условием:

```
alert tcp any any -> any [139,445]
(msg:"ET NETBIOS Tree Connect AndX Request IPC$ Unicode";
flow:established,to_server; content:"|00|";
depth:1; content:"|FF|SMBu"; within:5; distance:3;
content:"| 00 5c 00 69 00 70 00 63 00 24 00 00 00|";
nocase; flowbits:set,smb.tree.connect.ipc; flowbits:noalert;
reference:cve,2006-4691;
classtype:protocol-command-decode; sid:2025090;
rev:1; metadata:created_at 2016_06_14, former_category NETBIOS,
updated_at 2020_08_20;)
```

После редактирования будет иметь следующий вид:

```
pass tcp 192.168.1.1 any -> 192.168.1.10 [139,445]
(msg:"ET NETBIOS Tree Connect AndX Request IPC$ Unicode";
flow:established,to_server; content:"|00|";
depth:1; content:"|FF|SMBu"; within:5; distance:3;
content:"| 00 5c 00 69 00 70 00 63 00 24 00 00 00|";
nocase; flowbits:set,smb.tree.connect.ipc; flowbits:noalert;
reference:cve,2006-4691;
classtype:protocol-command-decode; sid:94000000;
rev:1; metadata:created_at 2016_06_14, former_category NETBIOS,
updated_at 2020_08_20;)
```

В измененном правиле заменен `sid` на `94000000`, что соответствует пользовательскому диапазону, а значение свойства `Action` заменено на `pass`, что позволяет отключить срабатывание правила при получении на IP-адресе 192.268.1.10 пакетов от IP-адреса 192.268.1.1.

Пример

В данном примере создано следующее правило: службы обнаружения вторжений:

```
alert tcp any any -> any any (msg:"ET SCAN NMAP -sS window 1024"; fragbits:!D; dsize:0;
  flags:S,12; ack:0; window:1024; reference:url,doc.emergingthreats.net/2009582;
  classtype:attempted-recon; sid:2009582; rev:3; metadata:created_at 2010_07_30,
  updated_at 2010_07_30;)
```

После редактирования будет иметь следующий вид:

```
pass tcp 192.168.0.1 any -> 192.168.0.2 any (msg:"ET SCAN NMAP -sS window 1024";
  fragbits:!D; dsize:0; flags:S,12; ack:0; window:1024; sid: 94000000-94999999;)
```

9. Установите чекбокс **Активность**

10. Нажмите **Создать**.

► **Результат шага:** Новое правило будет применяться для обнаружения вторжений. Старое правило останется в системе и может быть обновлено при импорте, но применяться не будет, если при импорте не будет активировано автоматически.

10.5.2.5. Удаление правил обнаружения вторжений, синхронизация правил

Удалить можно как одно правило обнаружения вторжений, так и несколько правил.

1. Для удаления одного правила:

- а. Нажмите на необходимое правило из списка.
- б. В открывшейся справа карточке правила нажмите  (**Удалить**).
- в. Введите обоснование действия и нажмите **Подтвердить**

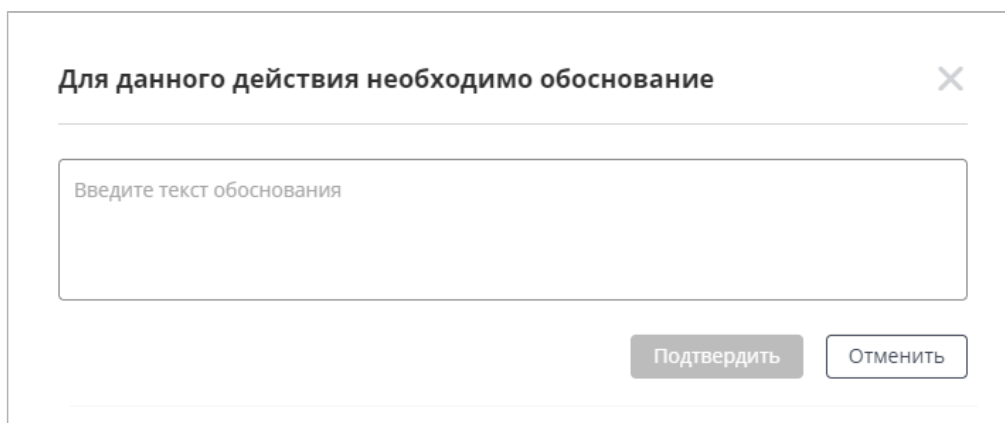


Рис. 275. Обоснование удаления правила обнаружения вторжений

► **Результат шага:** Правило обнаружения вторжений будет удалено из сенсора.



Подсказка:

Правило также можно удалить следующим способом:

- Установите чекбокс возле необходимого правила.
- В открывшемся внизу меню нажмите  →  (**Удалить**).
- Введите обоснование действия и нажмите **Подтвердить**

2. Для удаления нескольких правил:

- а. Установите чекбоксы возле необходимых правил.
- б. В открывшемся внизу меню нажмите  →  (**Удалить**).
- в. Введите обоснование действия и нажмите **Подтвердить**

10.5.3. Экспорт и импорт правил службы обнаружения вторжения

В этом разделе:

- Импорт правил обнаружения вторжений в формате *.json
- Импорт правил обнаружения вторжений в формате *.rules
- Экспорт правил службы обнаружения вторжений

Экспорт и импорт правил обнаружения вторжений осуществляется на странице **Администрирование** → **Основные настройки** → **Импорт и экспорт** на панели **Обнаружение вторжений**.

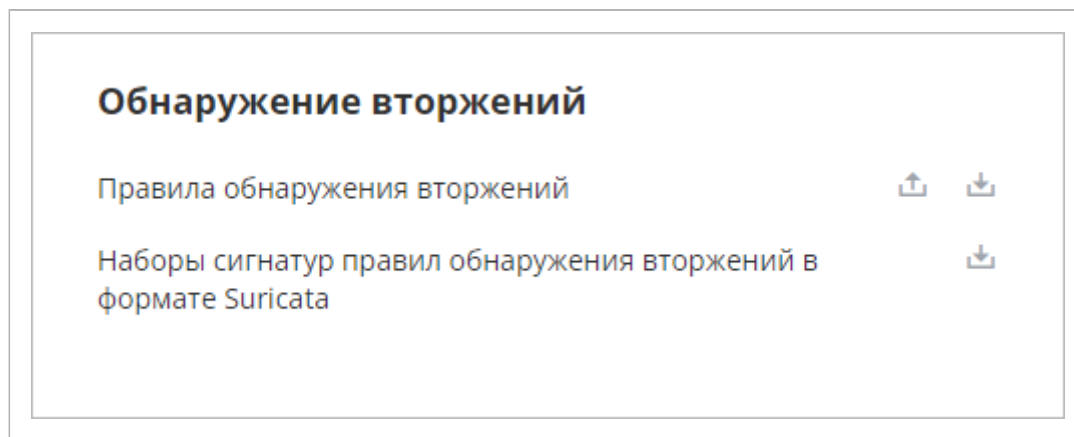


Рис. 276. Панель «Обнаружение вторжений» на странице «Импорт и экспорт»

10.5.3.1. Импорт правил обнаружения вторжений в формате *.json

Перед импортом необходимо обратить внимание, что при импорте правил, чьи уникальные идентификаторы сигнатуры (sid) совпадают с уже загруженными правилами, будет проведена проверка на номер ревизии (rev), и возможны следующие варианты:

- если rev импортируемого меньше, чем в уже загруженном, новое правило не будет импортировано;
- если rev импортируемого больше, чем в уже загруженном, новое правило будет импортировано, старое правило будет заменено. Активность правила сохранится, если для параметра **Статус активности сигнатур после импорта** будет выбран вариант **Сохранить**.

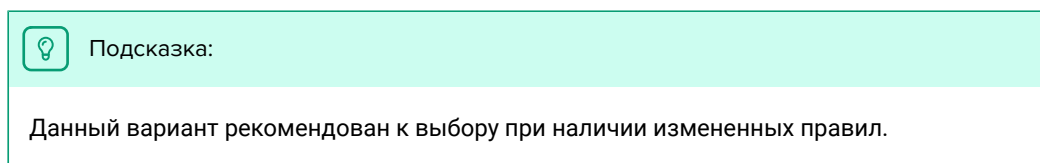
При импорте группы правил уникальность проверяется для каждого отдельно, и неудачный импорт некоторых правил группы не повлияет на импорт других.

Для импорта файла формата *.json с правилами обнаружения:

1. Перейдите на страницу **Администрирование** → **Основные настройки** → **Импорт и экспорт**.
2. На панели **Обнаружение вторжений** в строке **Правила обнаружения вторжений** нажмите кнопку  (**Импортировать**).
3. В открывшемся окне укажите расположение импортируемого файла формата *.json и подтвердите выбор.
4. В окне **Подготовка к импорту** выберите:

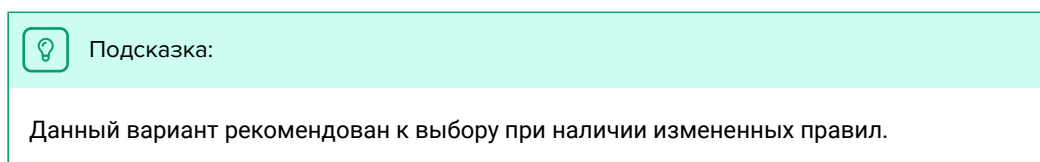
- действие для элементов, которые отсутствуют в новом (загружаемом) справочнике:

- **Оставить** — новые элементы будут добавлены к уже существующим;



- **Удалить** – старые элементы будут удалены и добавлены новые.
- статус активности элементов справочника после импорта:

- **Оставить как есть** — статус активности элементов справочника будет сохранен;



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

5. Нажмите **Импортировать**.

Подготовка к импорту

Перед обработкой выберите:

Действие для элементов, которые отсутствуют в новом справочнике :

☒ Оставить 

☐ Удалить 

Статус активности элементов справочника после импорта:

☒ Оставить как есть 

☐ Присвоить старым статус, как в файле 

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

Импортировать

Отменить

Рис. 277. Окно «Подготовка к импорту» при загрузке правил обнаружения вторжений

6. Дождитесь успешного результата импорта.

- **Результат шага:** После загрузки файла в правом верхнем углу страницы в поле **Результат последнего импорта** появится статус **Успешно**, и правила будут загружены на страницу **Правила обнаружения**.

7. Перейдите на страницу **Правила обнаружения** и убедитесь, что правила были успешно загружены.

10.5.3.2. Импорт правил обнаружения вторжений в формате *.rules

Перед импортом необходимо обратить внимание, что при импорте правил, чьи уникальные идентификаторы сигнатуры (sid) совпадают с уже загруженными правилами, будет проведена проверка на номер ревизии (rev), и возможны следующие варианты:

- если rev импортируемого меньше, чем в уже загруженном, новое правило не будет импортировано;
- если rev импортируемого больше, чем в уже загруженном, новое правило будет импортировано, старое правило будет заменено. Активность правила сохранится, если для параметра **Статус активности сигнатур после импорта** будет выбран вариант **Сохранить**.

При импорте группы правил уникальность проверяется для каждого отдельно, и неудачный импорт некоторых правил группы не повлияет на импорт других.

Для импорта файла формата Suricata (*.rules) с правилами обнаружения:

1. Перейдите на страницу **Администрирование** → **Основные настройки** → **Импорт и экспорт**.
2. На панели **Обнаружение вторжений** в поле **Наборы сигнатур правил обнаружения вторжений в формате Suricata** нажмите кнопку  (**Импортировать**).
3. В открывшемся окне укажите расположение импортируемого файла формата *.rules и подтвердите выбор.
 - **Результат шага:** Откроется окно **Подготовка к импорту**.
4. В окне **Подготовка к импорту** выберите:
 - действие для элементов, которые отсутствуют в новом (загружаемом) справочнике:

- **Оставить** — новые элементы будут добавлены к уже существующим;

 Подсказка:

Данный вариант рекомендован к выбору при наличии измененных правил.

- **Удалить** — старые элементы будут удалены и добавлены новые.
- статус активности элементов справочника после импорта:
- **Оставить как есть** — статус активности элементов справочника будет сохранен;

 Подсказка:

Данный вариант рекомендован к выбору при наличии измененных правил.

- **Присвоить старым статус, как в файле** — статус активности элементов справочника будет перезаписан в соответствии со значениями в импортируемом файле.
5. Нажмите **Импортировать**.

Подготовка к импорту

Перед обработкой выберите:

Действие для элементов, которые отсутствуют в новом справочнике :

☒ Оставить 

☐ Удалить 

Статус активности элементов справочника после импорта:

☒ Оставить как есть 

☐ Присвоить старым статус, как в файле 

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

Импортировать

Отменить

Рис. 278. Окно «Подготовка к импорту» при загрузке наборов сигнатур

- **Результат шага:** После загрузки файла в правом верхнем углу страницы в поле **Результат последнего импорта** появится статус **Успешно**, и правила будут загружены на страницу **Правила обнаружения**.
6. Убедитесь, что правила были успешно загружены. Для этого перейдите на страницу **Правила обнаружения**.

10.5.3.3. Экспорт правил службы обнаружения вторжений

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

1. Перейдите на страницу **Администрирование** → **Основные настройки** → **Импорт и экспорт**.
2. На панели **Обнаружение вторжений** в строке **Правила обнаружения вторжений** нажмите кнопку  (Экспортировать).
 - **Результат шага:** Файл со списком правил `suricata_rules_[дата_и_время].zip` будет сформирован и доступен для скачивания в правом верхнем углу страницы **Импорт и экспорт** под заголовком **Результат последнего экспорта**.
3. Для скачивания файла нажмите на название сформированного файла под заголовком **Результат последнего экспорта**.
4. В открывшемся окне укажите расположение для экспортируемого файла, введите название файла и нажмите **Сохранить**.

10.5.4. Создание исключений для правил обнаружения вторжений

Чтобы создать исключения для правил обнаружения вторжений, можно воспользоваться одним из следующих способов:

- создать исключение в карточке правила обнаружения вторжений;
- создать исключение во вкладке **Исключения** на странице **Правила обнаружения**;
- создать исключения для нескольких правил во вкладке **Правила** на странице **Правила обнаружения**.

10.5.4.1. Создание исключения в карточке правила обнаружения вторжений

Для создания исключения в карточке правила обнаружения вторжений:

1. Перейдите на страницу **Администрирование** → **Правила обнаружения**.
 2. Откройте карточку создания исключения одним из способов:
 - Выберите необходимое правило обнаружения вторжений из списка правил во вкладке **Правила**.
 - Установите чекбокс возле правила в списке.
- **Результат шага:** Откроется карточка правила обнаружения вторжений.

Правило обнаружения

✕ Деактивировать

✚ Создать исключения

Наименование:

SURICATA TRAFFIC-ID: instagram

SID правила:

300000033

Тип:

—

Описание:

Imported from file

Условие:

alert tls any any -> any any (msg:"SURICATA TRAFFIC-ID: instagram"; tls_sni; content:"cdninstagram.com"; isdataat:!1,relative; flow:to_server,established; flowbits: set,traffic/id/instagram; flowbits:set,traffic/label/social-network; noalert; sid:300000033; rev:1;)

CVE:

—

Приоритет:

—

Активность:

Применяется

Количество исключений:

—

Дата создания:

10.06.2024, 19:15:38

Дата обновления:

10.06.2024, 19:15:38

🗑 Удалить

Рис. 279. Карточка правила обнаружения вторжений

3. Нажмите **Создать исключение**.

- **Результат шага:** Откроется окно создания исключений.

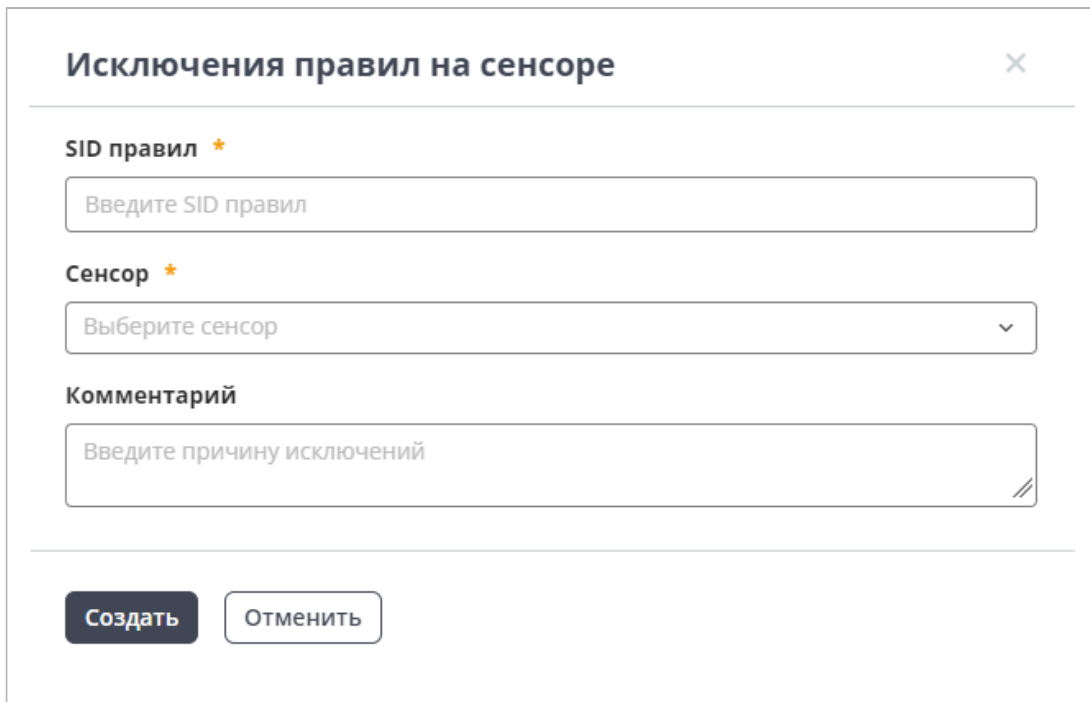


Рис. 280. Окно создания исключений

4. В окне создания исключений выберите сенсор, на котором будут созданы исключения, и введите комментарий к создаваемым исключениям.
5. После ввода данных нажмите **Создать**.
 - **Результат шага:** Созданные исключения будут отображаться в списке исключений во вкладке **Исключения**. В карточке правила обнаружения счетчик количества исключений в поле **Количество исключений** будет увеличен на 1.

10.5.4.2. Создание исключения во вкладке «Исключения»

Для создания исключения во вкладке **Исключения**:

1. Перейдите на страницу **Администрирование** → **Правила обнаружения**.
2. Во вкладке **Исключения** нажмите кнопку **+ Создать исключения**.
 - **Результат шага:** откроется окно создания исключений.
3. В окне создания исключений введите SID правила и комментарий, а также выберите сенсор, на котором будут созданы исключения.
4. После ввода данных нажмите **Создать**.
 - **Результат шага:** Созданные исключения будут отображаться в списке исключений во вкладке **Исключения**.

10.5.4.3. Создание исключения для нескольких правил обнаружения вторжений

Для создания исключения для нескольких правил обнаружения вторжений:

1. Перейдите на страницу **Администрирование** → **Правила обнаружения**.
2. Установите чекбокс возле правил обнаружения вторжений из списка или установите чекбокс **Выбрать видимые строки**.



Внимание:

При установке чекбокса **Выбрать видимые строки** будет выбрано 100 правил.

- **Результат шага:** Откроется меню выбора действий с правилами обнаружения вторжений.
3. В открывшемся меню выберите пункт **Создать исключения**.
 - **Результат шага:** Откроется окно создания исключений.
 4. В окне создания исключений выберите сенсор, на котором будет создано исключение, и введите комментарий к создаваемому исключению.
 5. Нажмите **Создать**.
 - **Результат шага:** Созданное исключение будет отображаться в списке исключений во вкладке **Исключения**.

10.5.5. Удаление исключений для правил обнаружения вторжений

В Комплексе реализована возможность удаления как одного, так и нескольких исключений для правил обнаружения вторжений.

Для удаления нескольких исключений для правил обнаружения вторжений выполните следующие действия:

- а. Установите чекбоксы возле необходимых исключений.
- б. В открывшемся меню нажмите **Удалить**.
- в. Введите обоснование действия и нажмите **Подтвердить**.

10.5.5.1. Удаление исключения для правила обнаружения вторжений

Для удаления исключения:

1. Выберите необходимое исключение из списка во вкладке **Исключения**.
 - **Результат шага:** Откроется карточка исключения для правила обнаружения вторжений.

Исключение

×

Наименование правила:	SURICATA TRAFFIC-ID: skype
SID правила:	300000024
Условие:	alert tls any any -> any any (msg:"SURICATA TRAFFIC-ID: skype"; tls_sni; content:"skype.com"; isdataat:!1,relative; flow:to_server,established; flowbits: set,traffic/id/skype; flowbits:set,traffic/label/im; noalert; sid:300000024; rev:1;)
Сенсор:	TESTTK22
Дата создания:	24.06.2024, 18:36:27
Автор:	Сумароков Александр Иванович
Комментарий:	—

🗑
Удалить

Рис. 281. Карточка исключения для правила обнаружения вторжений

2. Нажмите **Удалить**.
3. Введите обоснование действия и нажмите **Подтвердить**.

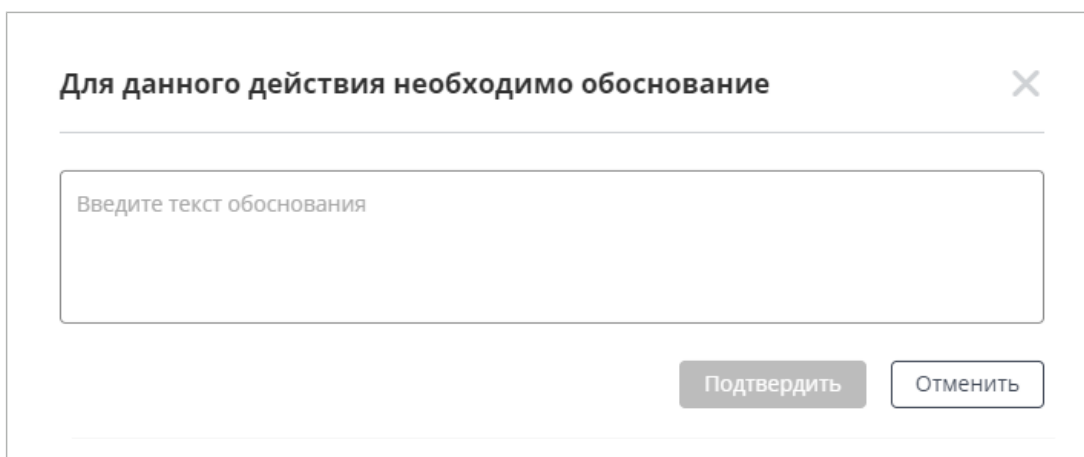


Рис. 282. Обоснование удаления исключения

- **Результат шага:** Исключение будет удалено из сенсора.
4. Вы также можете удалить исключение следующим способом:
 - а. Установите чекбоксы возле необходимых исключений.
 - **Результат шага:** откроется меню выбора действий с правилами обнаружения вторжений.
 - б. В открывшемся меню нажмите **Удалить**.
 - в. Введите текст обоснования удаления исключения и нажмите **Подтвердить**.

10.5.5.2. Удаление нескольких исключений для правил обнаружения вторжений

Для удаления нескольких исключений:

1. Установите чекбоксы возле необходимых исключений.
2. В открывшемся меню нажмите **Удалить**.
3. Введите обоснование действия и нажмите **Подтвердить**.

11. Управление Комплексом

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

11.1. Изменение сведений о Комплексе и сенсорах

11.1.1. Изменение сведений о текущем Комплексе

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

The screenshot shows the 'UDV MultiProtect' interface. On the left is a dark sidebar with a menu: Мониторинг, Инциденты, События, Активы, Сбор данных, Инспекция сети, Сенсоры, and Администрирование. The main area has a top navigation bar with links: Администрирование, О системе (active), Импорт и экспорт, Диагностика, and Настройки мониторинга. Below this is the 'О системе' section. It contains a 'Сведения о Комплексе' block with four input fields: 'Наименование' (pre-filled with 'lrp-vm-staging-244-47'), 'Описание' (pre-filled with 'Демонстрационный стенд'), 'Эксплуатирующая организация' (pre-filled with 'ООО «КИТ.Р»'), and 'Место установки' (pre-filled with 'Сколково'). To the right of these fields is the 'Информация об изготовителе' block, which contains text: 'UDV MultiProtect', 'Разработчик: ООО «КИТ.Р»', 'www.udv.group', and 'Версия: 1.0'. At the bottom right of the form are two buttons: 'Сохранить' (green) and 'Отмена' (grey). A status bar at the bottom left shows the date and time: '12.03.2025 22:46:23'.

Рис. 283. Страница «О системе»

3. Нажмите **Сохранить**.

11.1.2. Изменение сведений о сенсорах, подключенных к Комплексу

1. Перейдите на страницу **Сенсоры**.
2. Выберите сенсор из списка.
 - **Результат шага:** Откроется боковая панель настроек выбранного сенсора.
3. В открывшейся панели нажмите кнопку  (**Редактировать**) напротив наименования сенсора.

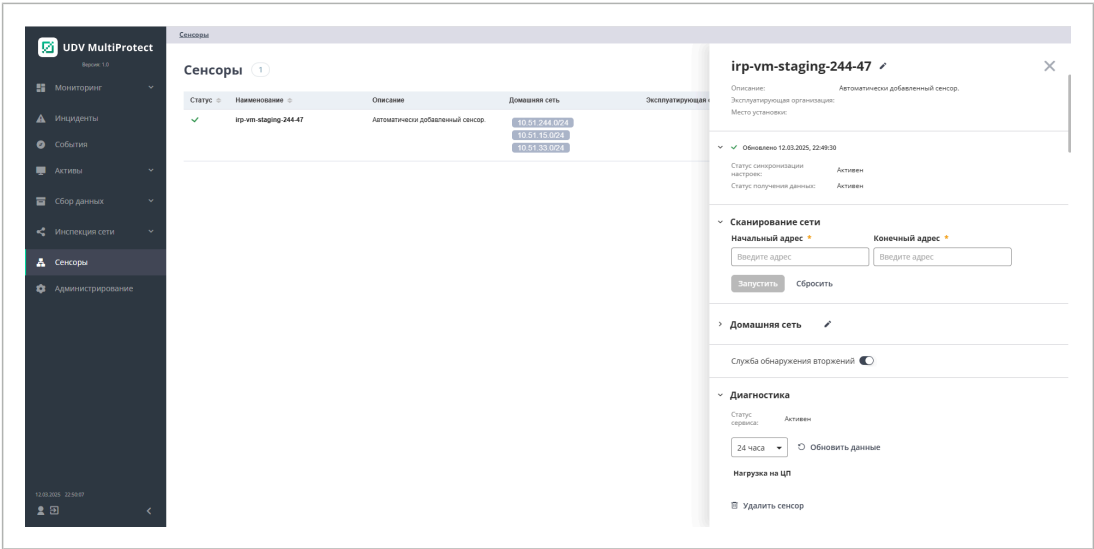


Рис. 284. Страница «Сенсоры»

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

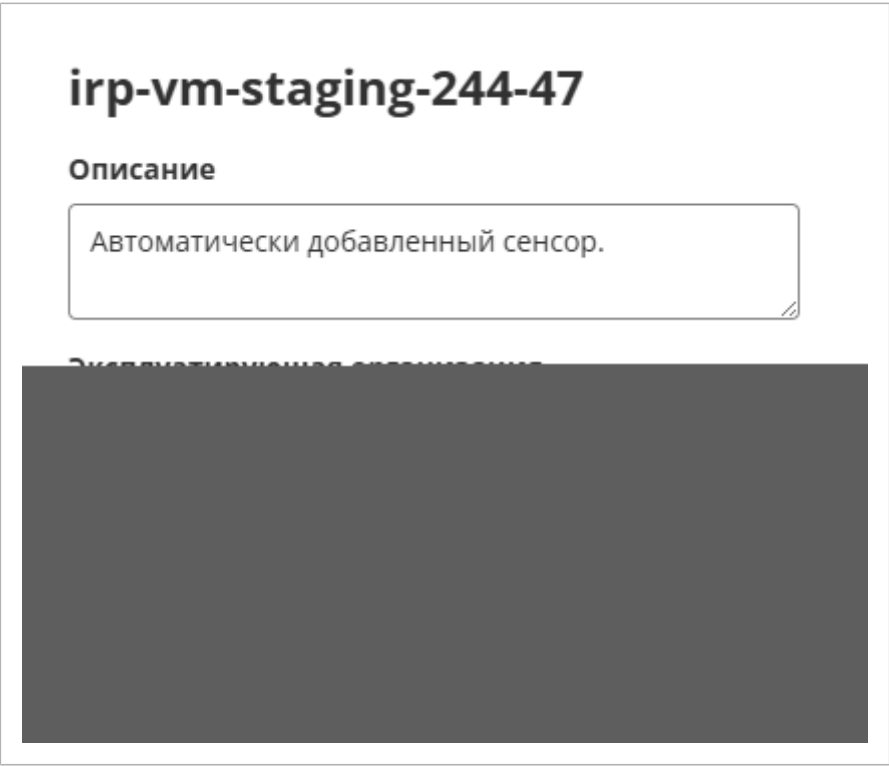


Рис. 285. Блок редактирования информации о сенсоре

5. Нажмите **Сохранить**.

11.2. Сканирование сети и определение интерфейсов активного сетевого оборудования

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



Внимание:

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

- Если переменная имеет значение `false`, либо она не задана в `manager.env`, Комплекс фиксирует активы только по MAC-адресу независимо от наличия у них IP-адреса. В списке активов отображаются все найденные активы (до настройки домашней сети активы отображаются только с MAC-адресами).
- Если переменная имеет значение `true`, Комплекс фиксирует активы по MAC-адресу (если IP-адрес не обнаружен) и по связке MAC-адреса и IP-адреса. В списке активов будут отображаться только активы, IP-адреса которых входят в домашнюю сеть, а также активы, IP-адреса которых не обнаружены.

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

Сканирование определяет новые доступные сетевые узлы. Также возможно определение их IP-адреса, MAC-адреса и сетевого имени (если данная информация доступна в режиме быстрого сканирования). В случае определения сетевого имени узла наименование соответствующего актива в Комплексе меняется на сетевое имя.

Для сканирования сети:

1. Перейдите на страницу **Сенсоры**.
2. Выберите сенсор.
 - **Результат шага:** Справа откроется карточка с описанием и настройками выбранного сенсора.
3. На панели **Сканирование сети** введите начальный и конечный адреса для сканирования.

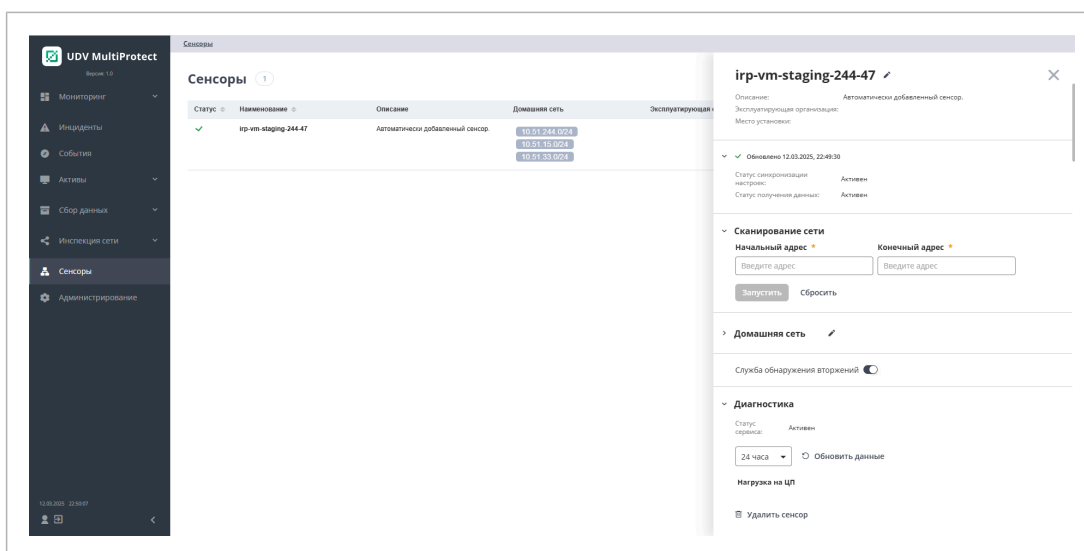


Рис. 286. Панель «Сканирование сети»

4. Нажмите **Запустить**.



Внимание:

При уменьшении количества IP-адресов, входящих в домашнюю подсеть (при изменении подсети в меньшую сторону), активы с типом **Неизвестный** тип, IP-адреса которых больше не входят в нее, будут удалены даже при наличии сетевого имени.

► **Результат шага:** появится уведомление **Сканирование адресов домашней сети запущено успешно**.

11.2.1. Интерпретация результатов пассивного сканирования сети

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

- Активу может быть присвоен дополнительный интерфейс с таким же IP-адресом, как у одного из его интерфейсов, но с другим MAC-адресом. Это может произойти из-за того, что в сетевых пакетах, отправленных с IP-адреса этого актива, был указан MAC-адрес интерфейса маршрутизатора. Тогда Комплекс в первую очередь проверяет принадлежность MAC-адреса одному из интерфейсов маршрутизатора, к которому подключен Комплекс. Если MAC-адрес принадлежит маршрутизатору, Комплекс автоматически присваивает новый интерфейс активу, который уже имеет интерфейс с таким же IP-адресом, и дополнительный интерфейс получает отметку *with_router_mac*. Если автоматическое присвоение интерфейса выполнено по ошибке, создайте вручную новый актив и присвойте ему найденный интерфейс — тогда он будет автоматически удален из списка интерфейсов исходного актива.
- На странице **Активы** могут присутствовать несколько активов с разными интерфейсами, хотя они должны принадлежать одному активу (часто такие активы являются активным сетевым оборудованием). Если на таком активе открыт доступ по протоколу SNMP, то есть возможность привязать к нему необходимые интерфейсы и удалить лишние активы с помощью специального сканера сбора данных. Подробнее см. в разделе [Добавление сетевых атрибутов активу с помощью сканера сбора данных по SNMP](#).

11.3. Настройка домашней сети

Настройка домашней сети необходима для отображения на странице **Активы** активов, IP-адреса которых входят в домашнюю сеть. До выполнения настройки домашней сети, в зависимости от настроек Комплекса, в списке активов отображаются все активы, найденные только по MAC-адресу, независимо от наличия у них IP-адреса, либо только активы, у которых не определен IP-адрес (подробнее см. раздел Сканирование сети и определение интерфейсов активного сетевого оборудования).

Для настройки домашней сети Комплекса:

1. Перейдите на страницу **Сенсоры**.
2. Выберите сенсор из списка.
 - **Результат шага:** Откроется боковая панель настроек выбранного сенсора.
3. В открывшейся панели в блоке **Домашняя сеть** нажмите кнопку  (**Редактировать сеть**).
4. Нажмите кнопку **+ Добавить сеть** и введите IP-адрес и маску подсети управляющего контура в качестве домашней подсети. Если требуется удалить добавленную ранее подсеть из списка, нажмите кнопку (**Удалить сеть**).
5. Нажмите **Применить**.
 - **Результат шага:** Появится окно с предупреждением: **При смене домашней сети активы и потоки, не входящие в новую сеть, будут удалены.**
6. Нажмите **Подтвердить** для подтверждения всех изменений и запуска обновления списка активов в соответствии с указанными домашними сетями.
7. Выполните шаги 2–6 для всех подключенных сенсоров, для которых нужно настроить домашнюю сеть.
 - **Результат шага:**
 - В список активов на странице **Активы** будут добавлены обнаруженные активы, IP-адреса которых входят в настроенные домашние сети.
 - Каждому сетевому атрибуту обнаруженного актива будет присвоен сенсор, в чью домашнюю сеть входит IP-адрес атрибута. Присвоенный сенсор будет отображаться в поле **Сенсор** блока **Сетевые атрибуты** в карточке актива.

11.4. Управление пользователями

В этом разделе:

- Управление учетными записями пользователей
 - Создание локальной учетной записи
 - Создание учетной записи службы каталогов
 - Редактирование учетных записей пользователей
- Настройка парольной политики

Об учетных записях

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

Управление учетными записями осуществляется на странице **Администрирование** → **Пользователи**. При создании учетной записи помимо стандартной пары логин-пароль необходимо задать тип учетной записи и ее роль.

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

По умолчанию в веб-интерфейсе Комплекса разрешена только одна активная сессия для каждой учетной записи. При успешном входе пользователя с нового устройства предыдущая сессия завершится. Отключить ограничение на количество сессий можно в файле `manager.env` (подробнее см. раздел Отключение ограничения на количество сессий пользователей).

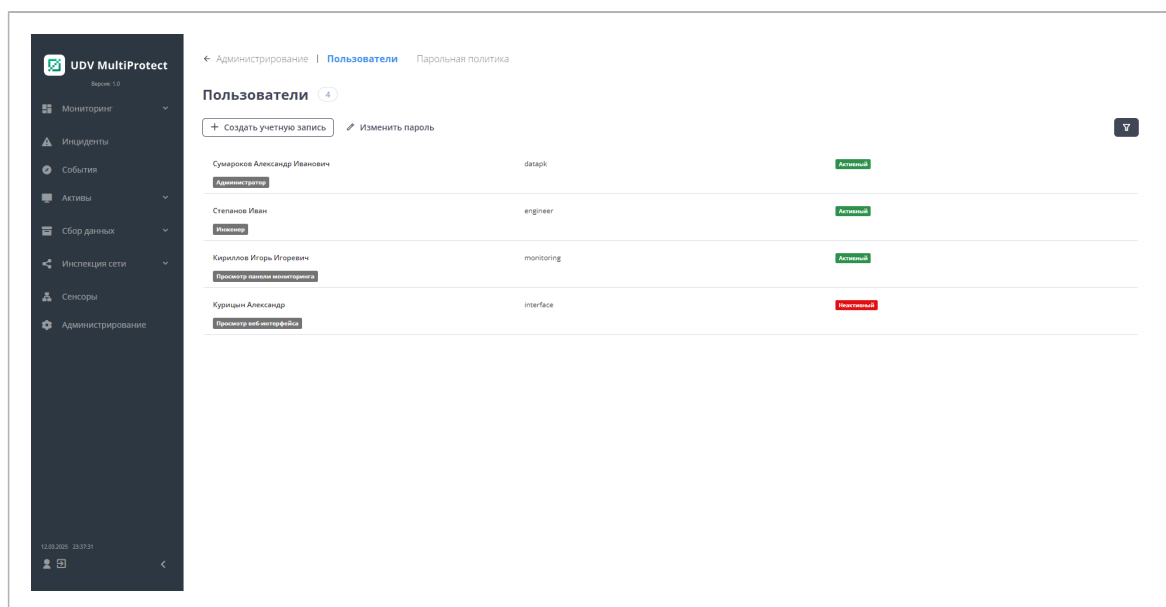


Рис. 287. Страница «Пользователи»

О ролях

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

Каждая пользовательская роль связывается с набором разрешений. При создании пользователя и назначении ему роли пользователь становится обладателем набора разрешений роли.

В Комплексе есть встроенный набор пользовательских ролей, представленный в таблице ниже. Для роли Администратор указаны дополнительные функции, которые ему доступны помимо функций роли Инженер. Данные роли соответствуют разделению функций пользователей, предложенному в разделе Разделение функций по администрированию.



Прим.:

Роль «Просмотр панели мониторинга» не представлена в таблице. Пользователи с этой ролью могут **только** просматривать страницу **Статус защищенности**.

Табл. 96. Пользовательские роли по умолчанию

ФУНКЦИОНАЛЬНАЯ ОБЛАСТЬ / РАЗДЕЛ ВЕБ-ИНТЕРФЕЙСА	ДЕЙСТВИЯ		
	АДМИНИСТРАТОР	ИНЖЕНЕР	ПРОСМОТР ВЕБ-ИНТЕРФЕЙСА
Пользователи	Создание, удаление, изменение учетной записи и пароля	Просмотр списка учетных записей	Просмотр всех страниц
Сканеры	Создание, изменение, удаление	Запуск	
Поиск уязвимостей в базах CPE и CVE	Удаление результатов	Запуск	
Справочники OVAL (определения, группы, настройки) и проверки OVAL	Добавление OVAL-определений в группу		
	Создание, удаление группы OVAL-опре- делений, удаление OVAL-определений из группы, создание, изменение, удаление настроек OVAL, создание, изменение, удаление скриптов OVAL	Просмотр всех справочников OVAL и проверок OVAL	
Отчеты	Создание		
Оповещения	Создание, изменение, удаление	Просмотр	
Справочники	Экспорт		
	Импорт	—	
Потоки	Удаление потоков и групп потоков данных, из- менение статуса потока или группы потоков		

Табл. 96. Пользовательские роли по умолчанию

ФУНКЦИОНАЛЬНАЯ ОБЛАСТЬ / РАЗДЕЛ ВЕБ-ИНТЕРФЕЙСА	ДЕЙСТВИЯ		
	АДМИНИСТРАТОР	ИНЖЕНЕР	ПРОСМОТР ВЕБ-ИНТЕРФЕЙСА
	Редактирование коммента- рия к потоку данных	Просмотр коммен- тариев к потоку данных	
Правила корреляции	Управление службой кор- реляции событий, пра- вилами корреляции событий	Просмотр правил корреляции событий	
Правила обнаружения вторжений	Управление правилами обна- ружения вторжений: импорт правил обнаружения вторжений; создание, изменение, удаление правил обнаружения вторжений; создание, изменение, удаление исключений для правил обна- ружения вторжений; активация и деактивация правил обнаружения вторжений; активация и деактивация службы обнаружения вторжений	Просмотр правил обнаружения вторжений, активация и деактивация службы обнаружения вторжений	
Активы	Настройка конфигурации активов, карточки активов, изменение учетных данных активов, экспорт и импорт активов, запуск поиска уязвимостей, создание, изменение, удаление активов		
	Удаление конфигурации активов	—	

Табл. 96. Пользовательские роли по умолчанию

ФУНКЦИОНАЛЬНАЯ ОБЛАСТЬ / РАЗДЕЛ ВЕБ-ИНТЕРФЕЙСА	ДЕЙСТВИЯ		
	АДМИНИСТРАТОР	ИНЖЕНЕР	ПРОСМОТР ВЕБ-ИНТЕРФЕЙСА
Источники	Создание, остановка, запуск, редактирование, удаление источника событий		
Инциденты	Изменение параметров и удаление инцидента или группы инцидентов		
	Создание статусов инцидентов	Просмотр статусов инцидентов	
Индексы	Создание и удаление шаблонов индекса		
	Архивирование, удаление индексов	Просмотр списка индексов	
Задачи сбора данных	Создание, изменение, удаление, экспорт		
	Импорт	—	
Сканирование сети	Запуск	—	
Сенсоры, иерархия	Управление сенсорами	Перезапуск синхронизации	
События	Просмотр событий и создание запросов		
	Запуск текущего и ретроспек- тивного анализа событий	—	
Карты сети	Просмотр карты сети, настройка представлений на карте		

Табл. 96. Пользовательские роли по умолчанию

ФУНКЦИОНАЛЬНАЯ ОБЛАСТЬ / РАЗДЕЛ ВЕБ-ИНТЕРФЕЙСА	ДЕЙСТВИЯ		
	АДМИНИСТРАТОР	ИНЖЕНЕР	ПРОСМОТР ВЕБ-ИНТЕРФЕЙСА
Страница Статус защищенности	Просмотр, переход на страницы Активы , Инциденты , Инспекция сети → Потоки данных , События для получения подробной информации		

11.4.1. Управление учетными записями пользователей

В этом разделе:

- Создание локальной учетной записи
- Создание учетной записи службы каталогов
- Редактирование учетных записей пользователей

Веб-интерфейс Комплекса предоставляет возможность управления учетными записями пользователей. При создании пользователя и назначении ему роли пользователь станет обладать набором разрешений роли.

Перейдите на страницу **Администрирование** → **Пользователи** → **Пользователи**, чтобы просмотреть список учетных записей пользователей Комплекса.

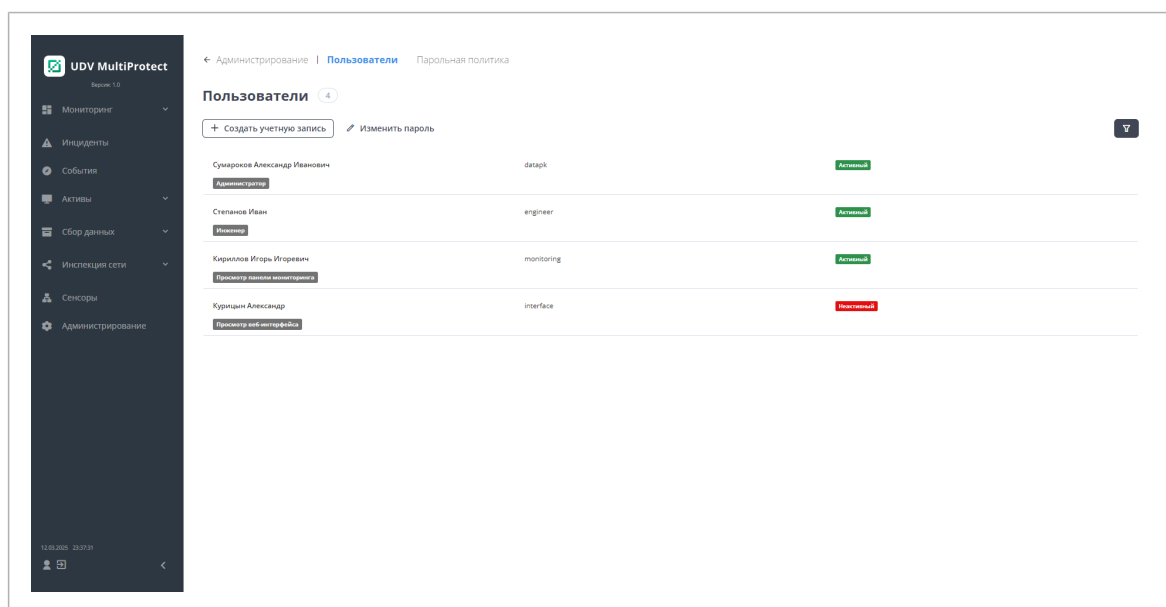


Рис. 288. Страница «Пользователи»

Для фильтрации списка учетных записей пользователей веб-интерфейс Комплекса предоставляет возможность использования предустановленных фильтров активности учетной записи.

В списке учетных записей выводится наименование, описание, роль пользователя, а также статус активности.

Предусмотрено создание локальных учетных записей и учетных записей службы каталогов. При выборе типа **Локальная** аутентификация происходит локально. При выборе типа **Служба каталогов** аутентификация происходит с использованием службы каталогов, а создаваемой учетной записи сопоставляется учетная запись из службы каталогов.

11.4.1.1. Создание локальной учетной записи

Для создания локальной учетной записи:

1. Перейдите на страницу **Администрирование** → **Пользователи**.
2. Нажмите **Создать учетную запись**.
3. В открывшемся окне **Создание учетной записи** задайте следующие параметры:
 - тип учетной записи — **Локальная**;
 - логин;
 - пароль;

- фамилию, имя и отчество пользователя;
- роль;
- чекбокс **УЗ пользователя активна**;



ОСТОРОЖНО:

При отмене выбора данного параметра учетная запись пользователя будет заблокирована.

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

Рис. 289. Окно «Создание учетной записи» при создании локальный учетной записи

4. Нажмите **Создать**.

11.4.1.2. Создание учетной записи службы каталогов

Для создания учетной записи службы каталогов:

1. Подключитесь к операционной системе Комплекса.
2. Перейдите в рабочую директорию Комплекса (по умолчанию путь к рабочей директории Комплекса — `/usr/share/udv/datapk`):

```
cd /usr/share/udv/datapk
```

3. Остановите работу сервисов следующей командой:

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

4. Дождитесь остановки работы всех сервисов.
5. Для подключения по протоколу LDAPS добавьте в файл `manager.env` переменную `LDAP_TLS` и присвойте ей значение `true`.
6. Добавьте в конфигурационный файл `manager.env` переменную `LDAP_CONNECTION_STRING`:

```
LDAP_CONNECTION_STRING=[protocol]://[domain_or_IP-address]:[port]
```

где `[protocol]` — протокол для соединения с сервером, `[domain_or_IP-address]` — доменное имя или IP-адрес сервера службы каталогов, `[port]` — порт назначения (при необходимости).



Подсказка:

Если в вашей сети настроена служба DNS, разрешающая адреса внутри домена, то вы можете указать полное имя домена в качестве адреса для соединения со службой каталогов. В этом случае Комплекс будет перебирать все контроллеры домена, пока не найдет доступный.

Например, для подключения по протоколу LDAPS с использованием доменного имени `udv.dev` через порт 636 значение переменных будет следующим:

```
LDAP_TLS=true
LDAP_CONNECTION_STRING=ldaps://udv.dev:636
```

Для подключения по протоколу LDAPS с использованием IP-адреса `192.168.0.110` значение переменных будет следующим:

```
LDAP_TLS=true
LDAP_CONNECTION_STRING=ldaps://192.168.0.110
```

7. Запустите работу сервисов командой:

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

8. Дождитесь запуска работы всех сервисов.
9. Откройте веб-интерфейс Комплекса.
10. Перейдите на страницу **Администрирование** → **Пользователи**.
11. Нажмите **Создать учетную запись**.
12. В открывшемся окне **Создание учетной записи** задайте следующие параметры:
 - тип учетной записи — `Служба каталогов`;
 - логин;

- имя учетной записи в службе каталогов в формате [логин]@[доменное_имя_нижнего_уровня].[...].[доменное_имя_верхнего_уровня], где вместо [...] укажите промежуточные доменные имена, если доменных имен больше двух;
- фамилию, имя, отчество пользователя;
- роль;
- для изменения активности учетной записи выберите или отмените выбор параметра УЗ **пользователя активна**.



Внимание:

При отмене выбора данного параметра учетная запись пользователя будет заблокирована.

Создание учетной записи

Тип учетной записи *

Служба каталогов

Логин * ⓘ

mlebyadkina

Новый пароль *

Новый пароль

Подтверждение нового пароля *

Подтверждение нового пароля

Имя учетной записи в службе каталогов

mlebyadkina@corp.example.com

Фамилия *

Лебядкина

Имя *

Мария

Отчество

Тимофеевна

Роль пользователя *

Просмотр веб-интерфейса

☒ Учетная запись пользователя активна

☐ Сменить пароль при входе

Создать

Отменить

Рис. 290. Окно «Создание учетной записи» при создании учетной записи службы каталогов

13. Нажмите **Создать**.

11.4.1.3. Редактирование учетных записей пользователей

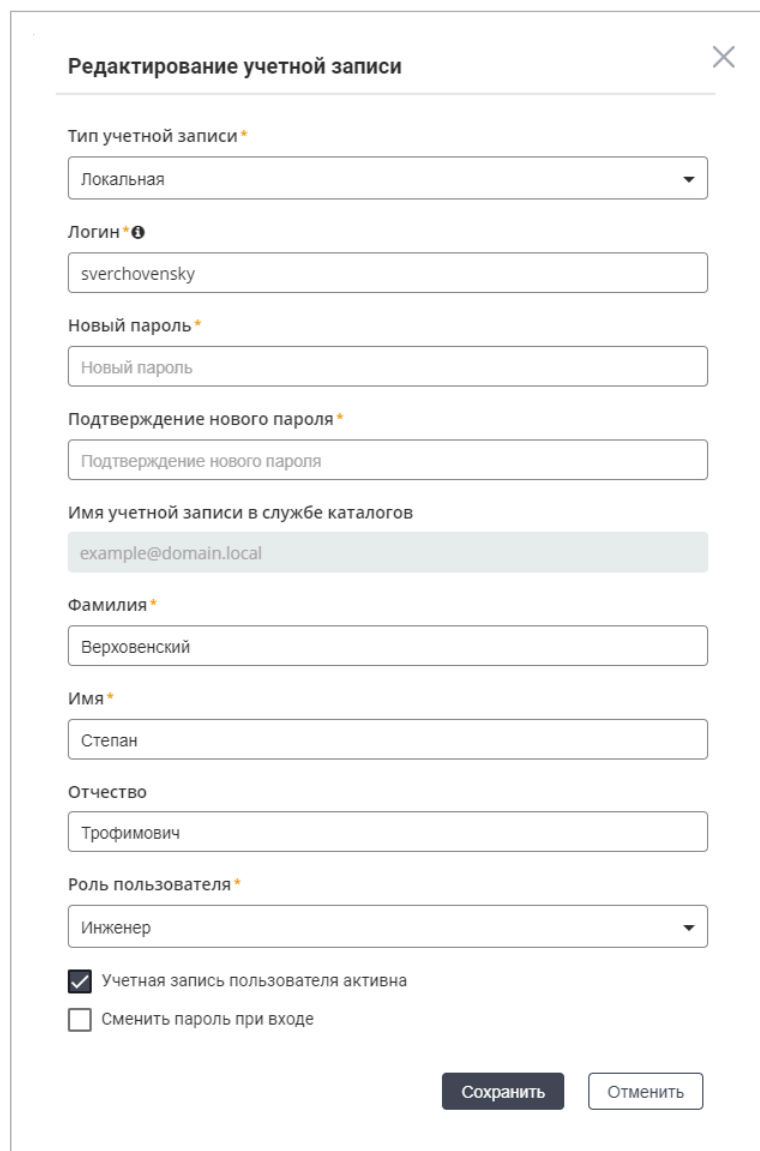
Для редактирования учетных записей пользователей в интерфейсе Комплекса предусмотрены следующие возможности:

- Изменение учетных записей
- Смена пароля учетной записи
- Блокировка и удаление учетной записи

11.4.1.3.1. Изменение учетных записей

Для изменения настроек учетной записи пользователя:

1. Перейдите на страницу **Администрирование** → **Пользователи**.
2. Выберите учетную запись в списке пользователей и нажмите кнопку  (**Редактировать учетную запись**).
 - **Результат шага:** Откроется окно **Редактирование учетной записи**.
3. Измените необходимые параметры учетной записи и нажмите кнопку **Сохранить**.



Редактирование учетной записи

Тип учетной записи *

Локальная

Логин * ⓘ

sverchovensky

Новый пароль *

Новый пароль

Подтверждение нового пароля *

Подтверждение нового пароля

Имя учетной записи в службе каталогов

example@domain.local

Фамилия *

Верховенский

Имя *

Степан

Отчество

Трофимович

Роль пользователя *

Инженер

☒ Учетная запись пользователя активна

☐ Сменить пароль при входе

Сохранить

Отменить

Рис. 291. Окно «Редактирование учетной записи»

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

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

11.4.1.3.2. Смена пароля учетной записи

Для смены пароля текущего пользователя:

1. Перейдите на страницу **Администрирование** → **Пользователи**.
2. Нажмите кнопку **Изменить пароль**.
 - **Результат шага:** появится окно **Изменение пароля учетной записи**.
3. Введите текущий пароль, новый пароль и подтверждение нового пароля.

 **Внимание:**

Требования к паролю устанавливаются парольной политикой (подробнее см. в подразделе Настройка парольной политики). Парольная политика по умолчанию имеет следующие параметры:

- длина пароля — не менее 6 символов;
- содержание пароля — не менее одного буквенного и не менее одного числового символа;
- пароль не должен содержать логин учетной записи.

Изменение пароля учетной записи пользователя рк

✕

Логин * ⓘ

Старый пароль *

Новый пароль *

Подтверждение нового пароля *

Рис. 292. Окно «Изменение пароля учетной записи»

4. Для применения изменений выполните повторный вход в веб-интерфейс Комплекса:
 - а. Нажмите кнопку  (**Выход**) в верхнем правом углу страницы веб-интерфейса.
 - б. Выполните повторный вход в систему с измененной учетной записью.

11.4.1.3.3. Блокировка и удаление учетной записи

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

1. Перейдите на страницу **Администрирование → Пользователи**.
2. Для блокировки учетной записи пользователя Комплекса:
 - а. Выберите учетную запись в списке пользователей и нажмите кнопку  (**Редактировать учетную запись**). Откроется окно **Редактирование учетной записи**.
 - б. Отмените выбор чекбокса **Активность**.
3. Для удаления учетной записи пользователя Комплекса:
 - а. Напротив утратившей актуальность учетной записи нажмите кнопку  (**Удалить учетную запись**).
 - б. Во всплывающем окне введите текст обоснования.
 - в. Нажмите **Подтвердить**.

11.4.2. Настройка парольной политики

Для настройки единой парольной политики для всех пользователей:

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

Рис. 293. Страница «Парольная политика»

2. Настройте следующие параметры парольной политики:

- общее минимальное количество символов, которое должен содержать пароль;



Внимание:

Доступен ввод значений в диапазоне от 6 до 14. Суммарное количество цифровых символов, заглавных букв и спецсимволов не должно превышать это значение.

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



Внимание:

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

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



Внимание:

Доступен ввод значений в диапазоне от 1 до 24.

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



Внимание:

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

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



Внимание:

Чтобы отключить автоматическую блокировку, введите значение 0.

3. Нажмите **Сохранить изменения**.

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

11.4.3. Отключение ограничения на количество сессий пользователей

Чтобы отключить ограничение на количество одновременных сессий пользователя в веб-интерфейсе Комплекса:

1. Подключитесь к операционной системе Комплекса.
2. Перейдите в рабочую директорию Комплекса (по умолчанию `/usr/share/udv/datapk`):

```
cd /usr/share/udv/datapk
```

3. Остановите работу сервисов следующей командой:

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

4. Дождитесь остановки работы всех сервисов.
5. Откройте конфигурационный файл `manager.env` в режиме редактирования.
6. Добавьте в файл `manager.env` переменную `LIMIT_USER_SESSIONS` и присвойте ей значение `false`:

```
LIMIT_USER_SESSIONS=false
```

7. Сохраните и закройте файл `manager.env`.
8. Запустите работу сервисов командой:

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

9. Дождитесь запуска работы всех сервисов.

11.5. Экспорт отдельных справочников

В качестве дополнительного способа создания резервных копий в веб-интерфейсе можно выгружать справочники объектов в файлы и сохранять их. В таблице ниже приведены ссылки на разделы с описанием экспорта резервных копий объектов Комплекса.

Табл. 97. Ссылки на разделы документа с описанием экспорта объектов Комплекса

НАИМЕНОВАНИЕ	ССЫЛКА	ФОРМАТ
Правила разбора событий	Экспорт правил разбора событий	zip
Правила обогащения событий	Экспорт правил обогащения событий	zip
Схема событий	Экспорт схемы событий	zip
Иерархия ИС	Экспорт справочника с классификаторами ИС	json
Иерархия меток активов	Экспорт меток	json
Группы активов (без активов)	Экспорт групп активов	json
Политика корреляции	Экспорт политики корреляции	json
Сканеры в составе групп сканеров	Экспорт сканеров и их групп	json
Задачи сбора данных	Экспорт задач сбора данных	json
Статусы инцидентов	Экспорт статусов инцидентов	json
Правила службы обнаружения вторжений	Экспорт правил службы обнаружения вторжений	json
Группы OVAL-определений	Экспорт групп OVAL-определений	json
Скрипты OVAL	Экспорт скриптов OVAL	json
Настройки OVAL	Экспорт настроек OVAL	json
Правила потоков	Экспорт правил управления потоками данных	json
Источники событий	Экспорт источников событий	json
Сохраненные запросы, визуализации, панели мониторинга	Экспорт сохраненных объектов	json
Активы	Экспорт активов	json

**Внимание:**

Экспорт следующих справочников недоступен в веб-интерфейсе:

- учетные данные активов;
- справочники ПО и уязвимостей (CPE и CVE) и база сопоставления собранного сканерами ПО со справочником CPE. Экспорт этих справочников доступен только в операционной системе Комплекса путем копирования директории `/cve` вместе с содержимым (по умолчанию расположена в директории `/usr/share/udv/vulnerability-backend`);
- правила корреляции и схема корреляции — экспорт доступен только в составе политики корреляции;
- наборы сигнатур правил обнаружения вторжений в формате Suricata — экспорт доступен только в составе правил обнаружения вторжений;
- OVAL-определения — экспорт доступен только в составе групп OVAL-определений.

11.6. Диагностика состояния системы Комплекса

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

Для просмотра доступны следующие временные периоды:

- 1 час;
- 24 часа;
- 7 дней.

Для выбора периода воспользуйтесь выпадающим списком в верхней части страницы и нажмите **Обновить данные**.

На странице представлены следующие графики:

- **Нагрузка на ЦП** — показывает загруженность центрального процесса за выбранное время. На графике отображаются две линии: программы и ядро. Таким образом можно точно определить, что нагружает систему.



Подсказка:

При превышении заданного в переменной `MAX_CPU_LOAD_CONSUMED_PERCENTAGE` лимита, а также последующей нормализации значения нагрузки на центральный процессор, будет получено соответствующее событие.

- **Средняя нагрузка на систему** — сводный коэффициент нагрузки на основные компоненты.



Подсказка:

При превышении заданного в переменной `DATAPK_MAX_LA` лимита, а также последующей нормализации значения средней нагрузки (LA) будет получено соответствующее событие.

- **Оперативная память** — график показывает общее доступное количество оперативной памяти и занятое количество.



Подсказка:

При превышении заданного в переменной `DATAPK_MAX_RAM_PERCENTAGE_CONSUMED` лимита оперативной памяти будет получено соответствующее событие.

- **Сетевой трафик** — отображает все сетевые интерфейсы и объем данных, которые они передают.
- **Нагрузка на диск** — показывает то, насколько занят жесткий диск во времени. На графике присутствуют две линии: чтение и запись.
- **Место на диске** — отображает занятое пространство относительно всего доступного для каждого диска.

**Подсказка:**

При превышении заданного в переменной `MAX_DISK_SPACE_CONSUMED_PERCENTAGE` лимита, а также последующей нормализации значения нагрузки на диск будет получено соответствующее событие.

- **Swap** — график отражает место на жестком диске, которое используется для «выгрузки» в него неиспользуемых страниц из оперативной памяти.
- **События от сенсоров** — отображает количество внешних и внутренних событий, которые поступают с сенсоров.

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

11.7. Диагностика состояния сенсора

На странице **Сенсоры** вы можете ознакомиться с графиками нагрузки сенсоров, действующих на текущем Комплексе и доступных в списке на этой странице.

Для просмотра доступны следующие временные периоды:

- 1 час;
- 24 часа;
- 7 дней.

Для выбора периода воспользуйтесь выпадающим списком в верхней части страницы и нажмите **Обновить данные**.

На странице представлены следующие графики:

- **Нагрузка на ЦП** — показывает загруженность центрального процесса за выбранное время. На графике отображаются две линии: программы и ядро. Таким образом можно точно определить, что нагружает систему.
- **Средняя нагрузка на систему** — сводный коэффициент нагрузки на основные компоненты.
- **Оперативная память** — график показывает общее доступное количество оперативной памяти и занятое количество.
- **Сетевой трафик** — отображает все сетевые интерфейсы и объем данных, которые они передают.
- **Нагрузка на диск** — показывает то, насколько занят жесткий диск во времени. На графике присутствуют две линии: чтение и запись.
- **Место на диске** — отображает занятое пространство относительно всего доступного для каждого диска.
- **Swap** — график отражает место на жестком диске, которое используется для «выгрузки» в него неиспользуемых страниц из оперативной памяти.
- **События от сенсора к Комплексу** — отображает количество внешних и внутренних событий, которые поступают с сенсора на Комплекс.
- **Обработанные события** — отображает количество событий, которые поступили с сенсора и были обработаны Комплексом.
- **Обработанные сетевые пакеты** — отображает количество сетевых пакетов, которые были обработаны Комплексом.

При наведении на график можно увидеть легенду, где указано, какие параметры используются на этом графике, и цвет их линий.

11.8. Удаление сенсора

Для удаления сенсора и связанной с ним информации из Комплекса:

1. Перейдите на страницу **Сенсоры**.
2. Выберите сенсор из списка.
 - **Результат шага:** Откроется боковая панель настроек выбранного сенсора.
3. В открывшейся панели нажмите внизу кнопку  **Удалить сенсор**.
 - **Результат шага:** Появится окно с предупреждением: **Вместе с сенсором будут удалены связанные сетевые атрибуты и потоки. Вы действительно хотите удалить сенсор [имя]?**

4.  **ОСТОРОЖНО:**
 - При удалении сенсора будут удалены связанные с ним данные: сетевые атрибуты активов, конфигурации, потоки, статусы сбора.
 - Если при удалении связанных сетевых атрибутов актива будет удален его интерфейс сбора данных, то новым интерфейсом сбора данных станет случайный из оставшихся сетевых атрибутов.
 - Актив не будет удален, если у него не останется ни одного сетевого атрибута после удаления сенсора. При необходимости измените или удалите такие активы вручную.

Введите обоснование удаления сенсора и нажмите **Подтвердить**.

Для данного действия необходимо обоснование

Вместе с сенсором будут удалены связанные сетевые атрибуты и потоки. Вы действительно хотите удалить сенсор vm-develop-15?

Введите текст обоснования

Подтвердить

Отменить

- **Результат шага:** Сенсор и связанные с ним данные будут удалены из Комплекса.

12. Регламентные работы

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

Для своевременного исполнения регламентных работ администратор системы в интерфейсе Комплекса может создавать резервные копии ключевых данных и изменять пароли пользователей.

12.1. Резервное копирование данных

В этом разделе:

- Резервное копирование рабочей директории и данных Комплекса уровня Management
- Выгрузка событий Комплекса в архив
- Экспорт отдельных справочников
- Экспорт нескольких справочников

Периодическому архивированию и резервному копированию на резервные машинные носители подлежат следующие объекты Комплекса:

1. Базы данных Комплекса.
2. Рабочая директория Комплекса.
3. Файлы, содержащие описания объектов мониторинга.
4. Индексы событий.
5. Информация о подключенных сенсорах и домашних сетях, которые прослушивают сенсоры.
6. Информация из подраздела **О системе**.
7. Активность службы обнаружения вторжений по отдельным сенсорам.
8. Оперативные данные:
 - список активов;
 - список потоков данных;
 - события активов (в том числе инциденты);
 - связи потоков, активов и инцидентов с сенсорами.
9. Справочные данные:
 - иерархия ИС;
 - иерархия меток активов;
 - группы сканеров;
 - источники событий;
 - задачи сбора данных;
 - правила разбора событий;
 - правила обогащения событий;
 - схема событий;
 - правила службы обнаружения вторжений;
 - исключения для правил службы обнаружения вторжений;
 - политика корреляции (схема и правила корреляции);
 - OVAL-определения и группы OVAL-определений.
 - скрипты OVAL;
 - настройки OVAL;

- правила потоков;
- справочники ПО и уязвимостей (CPE и CVE);
- сопоставление собранного сканерами ПО со справочником CPE.

Периодичность резервного копирования определяется внутренними регламентами эксплуатирующей организации.

12.1.1. Резервное копирование рабочей директории и данных Комплекса уровня Management

В этом разделе:

- [Запуск резервного копирования рабочей директории и баз данных Комплекса уровня Management](#)
- [Содержание архива резервной копии рабочей директории и баз данных Комплекса](#)

Модуль резервного копирования `backup_manager` локального Комплекса уровня Management сохраняет следующие данные в резервной копии:

- директорию `/usr/share/udv` вместе со справочниками ПО и уязвимостей (CPE, CVE и Банк данных угроз безопасности информации ФСТЭК России) и файлом сопоставления собранного ПО со справочником CPE;
- базы данных локального Комплекса, содержащие все накопленные данные.



Внимание:

Модуль не сохраняет следующие данные Комплекса:

- события Комплекса (индексы). Для архивирования индексов событий воспользуйтесь инструкцией в разделе [Выгрузка событий Комплекса в архив](#);
- проверки OVAL.

12.1.1.1. Содержание архива резервной копии рабочей директории и баз данных Комплекса

Архив резервной копии `dtbk-backup-[version]-[YYYYmmddhhmmss].tar` содержит:

- `data.tar.bz2` — архив с незашифрованной директорией `/usr/share/udv`, включающей в себя справочники уязвимостей (CPE, CVE и Банк данных угроз безопасности информации ФСТЭК России).
- `redis_db_dump.aes` и `postgres_db_dump.aes` — резервные копии баз данных, зашифрованные паролем, который задается при запуске резервного копирования (в ключе `--password`).
- `info.json` — метаданные, включающие контрольные суммы файлов резервной копии.



Внимание:

При восстановлении баз данных из резервной копии и дальнейшего функционирования Комплекса всегда используется пароль баз данных Комплекса, с которого получена резервная копия — пароль хранится в переменной `DB_PASS` конфигурационного файла `manager.env`.

12.1.1.2. Запуск резервного копирования рабочей директории и баз данных Комплекса уровня Management

Для выполнения резервного копирования рабочей директории и баз данных локального Комплекса уровня Management в режиме командной строки:

1. Подключитесь к операционной системе Комплекса.
2. Перейдите в рабочую директорию (/usr/share/udv/datapk).
3. Убедитесь, что директория /usr/share/udv/datapk занимает менее 500 Мбайт:

```
du -h -d 1 /usr/share/udv/datapk | sort -h
```

4. Выполните следующую команду для запуска резервного копирования:

```
python3 -m backup_manager --create --justification 'Регламентные работы' --username 'datapk' --password '1234567890'
```

где:

- `--justification` — комментарий к создаваемой резервной копии;
- `--username` — имя пользователя, который создает резервную копию;
- `--password` — пароль для архива резервной копии.

► **Результат шага:**

- по окончании резервного копирования будут отображена следующая строка:

```
INFO:backup_manager.operations.create:Backup creation started
INFO:backup_manager.operations.create:Creating a postgres database dump
...
INFO:backup_manager.operations.check:dump.rdb Ok
INFO:backup_manager.main:Backup created: /var/backups/dtpk-backup-v2.2.[минорная версия].[патч-версия]-20241022161015.tar
```

- будет создан архив резервной копии `dtpk-backup-[version]-[YYYYmmddhhmmss].tar` в директории по умолчанию `/var/backups`.

5. Проверьте корректность созданного архива резервной копии. Для этого выполните следующую команду:

```
python3 -m backup_manager --check --file=dtpk-backup-[version]-[YYYYmmddhhmmss].tar --password='1234567890'
```

где:

- `--file` — название созданного ранее архива резервной копии, который нужно проверить на корректность;
- `--password` — пароль от архива, заданный в одноименном ключе при запуске резервного копирования в шаге 4.

6. Скопируйте созданный архив резервной копии из директории `/var/backups` на отдельный физический носитель.

12.1.2. Резервное копирование Комплекса уровня Sensor

Комплексы уровня Sensor не хранят данные, поэтому их резервное копирование заключается только в ручном сохранении следующих локальных файлов сенсора:

- `/etc/machine-id` — идентификатор текущего сенсора;
- `/usr/share/udv/datapk/sensor.env` — конфигурационный файл сенсора.

Восстановление сенсоров из резервной копии заключается в их развертывании с нуля согласно разделам Установка Комплекса уровня Sensor или Установка Комплекса уровня Management+Sensor на одном аппаратном средстве Руководства по внедрению и поддержке.

12.1.3. Выгрузка событий Комплекса в архив

Комплекс сохраняет архивы индексов событий в операционную систему в директорию `indices`. Директория `indices` расположена по умолчанию в `/var/backups/elasticsearch`, либо в другой директории, указанной в переменной `DATAPK_ELASTICSEARCH_BACKUP_DIR` конфигурационного файла `manager.env`.

12.1.3.1. Выгрузка индекса событий в архив

Чтобы сохранить отдельный индекс с событиями в архив:

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

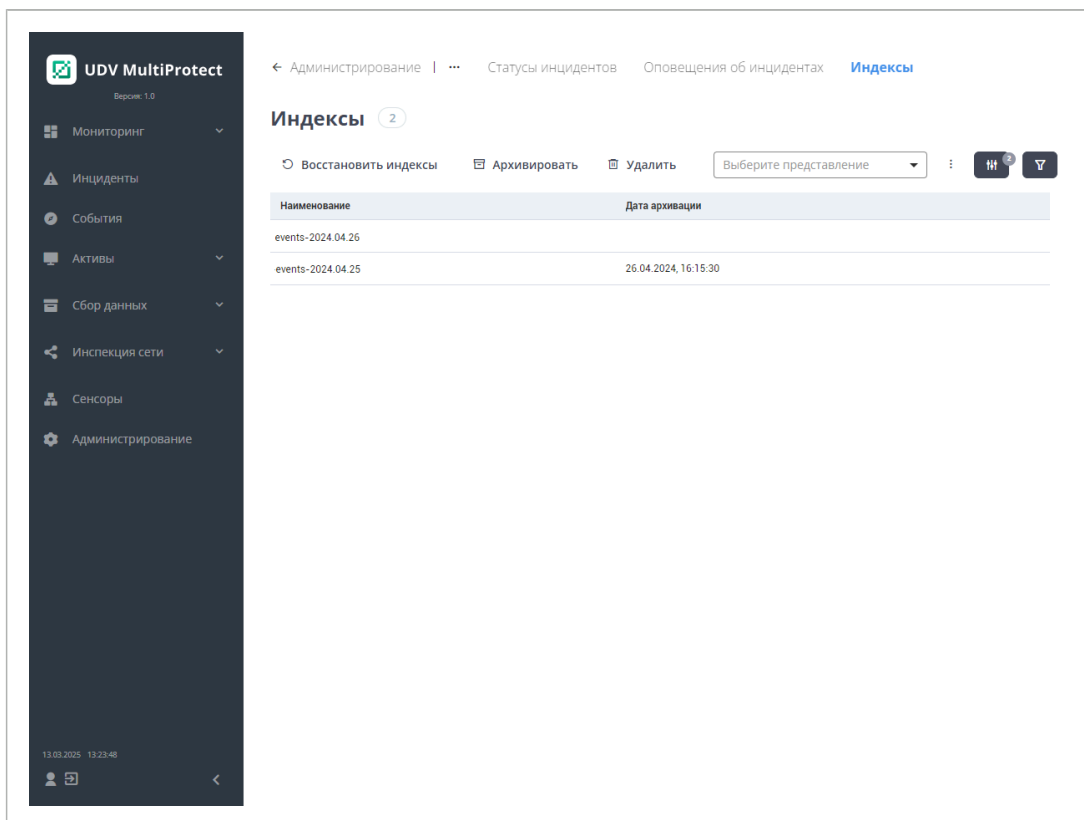


Рис. 294. Страница «Индексы»

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

12.1.3.2. Выгрузка нескольких индексов событий в архив

Чтобы сохранить отфильтрованные индексы с событиями в архивы:

1. Перейдите на страницу **Администрирование** → **События и инциденты** → **Индексы**.
2. Воспользуйтесь фильтрами для получения списка индексов, подлежащих архивированию.
3. Нажмите кнопку  (**Архивировать**) в верхней части страницы.
 - **Результат шага:** Для каждого отфильтрованного индекса отдельный архив `datapk_events_[тип_индекса]_[дата_индекса]` будет загружен в директорию `indices` (путь по умолчанию `/var/backups/elasticsearch/indices`).

12.1.4. Экспорт отдельных справочников

В качестве дополнительного способа создания резервных копий в веб-интерфейсе можно выгружать справочники объектов в файлы и сохранять их. В таблице ниже приведены ссылки на разделы с описанием экспорта резервных копий объектов Комплекса.

Табл. 98. Ссылки на разделы документа с описанием экспорта объектов Комплекса

НАИМЕНОВАНИЕ	ССЫЛКА	ФОРМАТ
Правила разбора событий	Экспорт правил разбора событий	zip
Правила обогащения событий	Экспорт правил обогащения событий	zip
Схема событий	Экспорт схемы событий	zip
Иерархия ИС	Экспорт справочника с классификаторами ИС	json
Иерархия меток активов	Экспорт меток	json
Группы активов (без активов)	Экспорт групп активов	json
Политика корреляции	Экспорт политики корреляции	json
Сканеры в составе групп сканеров	Экспорт сканеров и их групп	json
Задачи сбора данных	Экспорт задач сбора данных	json
Статусы инцидентов	Экспорт статусов инцидентов	json
Правила службы обнаружения вторжений	Экспорт правил службы обнаружения вторжений	json
Группы OVAL-определений	Экспорт групп OVAL-определений	json
Скрипты OVAL	Экспорт скриптов OVAL	json
Настройки OVAL	Экспорт настроек OVAL	json
Правила потоков	Экспорт правил управления потоками данных	json
Источники событий	Экспорт источников событий	json
Сохраненные запросы, визуализации, панели мониторинга	Экспорт сохраненных объектов	json
Активы	Экспорт активов	json

**Внимание:**

Экспорт следующих справочников недоступен в веб-интерфейсе:

- учетные данные активов;
- справочники ПО и уязвимостей (CPE и CVE) и база сопоставления собранного сканерами ПО со справочником CPE. Экспорт этих справочников доступен только в операционной системе Комплекса путем копирования директории `/cve` вместе с содержимым (по умолчанию расположена в директории `/usr/share/udv/vulnerability-backend`);
- правила корреляции и схема корреляции — экспорт доступен только в составе политики корреляции;
- наборы сигнатур правил обнаружения вторжений в формате Suricata — экспорт доступен только в составе правил обнаружения вторжений;
- OVAL-определения — экспорт доступен только в составе групп OVAL-определений.

12.1.5. Экспорт нескольких справочников

В Комплексе возможен экспорт справочных данных в единый архив формата `.tar`. Список доступных для экспорта справочников приведен в разделе Экспорт отдельных справочников. Для экспорта:

1. Перейдите на страницу **Администрирование** → **Основные настройки** → **Импорт и экспорт**.
2. Нажмите кнопку  (**Экспортировать...**) в верхней части страницы.
 - **Результат шага:** Справа откроется карточка **Экспорт справочных данных**.
3. В открывшейся справа карточке измените при необходимости набор справочников для выгрузки.



Внимание:

По умолчанию выбраны все справочники, кроме справочников **Правила разбора событий**, **Правила обогащения событий** и **Схема событий**. Такой выбор рекомендован, если планируется дальнейший импорт файла в другие **Комплексы**, так как при импорте настроек событий могут проявляться проблемы с формированием инцидентов.

Экспорт справочных данных

Экспортировать

События

Правила разбора событий

Правила обогащений событий

Схема событий

Корреляция событий

✓ Политика корреляции

Обнаружение вторжений

✓ Правила обнаружения вторжений

Элементы иерархии

✓ Иерархия ИС

✓ Иерархия меток активов

✓ Группы активов

Сбор данных

✓ Группы сканеров

✓ Задачи сбора данных

OVAL

✓ Группы OVAL определений

✓ Скрипты OVAL

✓ Настройки OVAL

Инциденты

✓ Статусы инцидентов

Правила потоков

✓ Правила потоков

Рис. 295. Окно «Экспорт справочных данных»

4. Нажмите **Экспортировать**.

► **Результат шага:** Появится уведомление **Запущен экспорт справочников.**

5. Дождитесь подготовки архива формата `export_[дата_и_время].tar` в поле **Результат последнего экспорта** в правом верхнем углу страницы.
6. Нажмите на подготовленный архив для его скачивания.

12.2. Смена паролей

В этом разделе:

- Смена пароля системной учетной записи администратора
- Смена пароля учетной записи в веб-интерфейсе Комплекса

12.2.1. Смена пароля системной учетной записи администратора

Для смены пароля системной учетной записи администратора Комплекса:

1. Подключитесь к операционной системе Комплекса.
2. Войдите в систему под системной учетной записью администратора.
3. Смените пароль администратора. Для этого введите команду:

```
passwd [имя_пользователя]
```

4. Введите новый пароль администратора и нажмите клавишу **Enter**. После соответствующего запроса повторите ввод нового пароля администратора и нажмите клавишу **Enter**.

12.2.2. Смена пароля учетной записи в веб-интерфейсе Комплекса

Смена паролей учетных записей Комплекса может быть выполнена только пользователем с назначенной ролью **Администратор**.

Для смены пароля учетной записи другого пользователя:

1. Перейдите на страницу **Администрирование** → **Пользователи**.
2. Выберите учетную запись, для которой необходимо сменить пароль, и нажмите кнопку  **(Редактировать)**.
3. В открывшемся окне введите в поле **Пароль** новый пароль пользователя, повторите ввод нового пароля в поле **Подтверждение пароля**.
4. Нажмите **Сохранить**.
5. Выполните шаги 1–3 для других учетных записей Комплекса.



Подсказка:

Порядок смены пароля текущего пользователя приведен в подразделе [Управление учетными записями пользователей](#).

12.3. Обновление серверного сертификата

По истечении срока действия текущих серверных сертификатов необходима их замена в операционной системе Комплекса уровня Management. Также может потребоваться выпуск нового сертификата с параметром `CommonName`, равным сетевому имени Комплекса, если в текущем сертификате значение этого параметра равно IP-адресу сетевого интерфейса управления Комплекса.

Для обновления серверного сертификата `nginx`:

1. Подключитесь к операционной системе Комплекса.
2. Остановите работу Комплекса одной из команд:

- Для Комплекса уровня Management:

```
cd /opt/datapk && docker-compose down
```

- Для Комплекса уровня Management + Sensor, установленных на одной аппаратной платформе:

```
cd /opt/datapk && docker-compose down && cd /opt/sensor && docker-compose down
```

3. Сгенерируйте серверные сертификаты `nginx`. Для этого:

- а. Убедитесь, что заданы необходимые системные переменные, выполнив команды:

- `echo ${HOST_FQDN}`

Значение переменной должно совпадать с сетевым именем Комплекса.

- `echo ${DATAPK_IP}`

Значение переменной должно совпадать с IP-адресом сетевого интерфейса управления Комплекса.

- б. Если переменные отсутствуют или их значения отличаются от требуемых, задайте их по очереди:

```
HOST_FQDN='[hostname]'  
DATAPK_IP='[ip_addr]'
```

Где `[hostname]` — сетевое имя Комплекса, `[ip_addr]` — IP-адрес сетевого интерфейса управления Комплекса.

- в. В директории `/opt/datapk/nginx/certs/` создайте файл `config.txt` и выполните команду, чтобы записать в него данные для создания сертификата:

```
printf "[dn]\nCN=${HOST_FQDN}\n[req]\ndistinguished_name =  
dn  
\n[EXT]\nsubjectAltName=DNS:${HOST_FQDN}\nkeyUsage=digitalSignature\nextendedKeyUsage=serverAuth" > /opt/datapk/nginx/certs/config.txt
```

- г. Создайте сертификат по команде:

```
openssl req -x509 -out /home/datapk/nginx/certs/${DATAPK_IP}.cert \  
-keyout /home/datapk/nginx/certs/${DATAPK_IP}.key -days 3650 \  
-newkey rsa:2048 -nodes -sha256 -subj "/CN=${HOST_FQDN}" \  
-extensions EXT -config /home/datapk/nginx/certs/config.txt
```




Внимание:

При выполнении команды убедитесь, что файл сертификата имеет расширение `.cert`.

д. Удалите файл `config.txt`:

```
rm -f /home/datapk/nginx/certs/config.txt
```

е. Удалите директорию `sites-enabled.d` сервиса `nginx`:

```
rm -rf /home/datapk/nginx/sites-enabled.d/
```

4. Запустите сервисы Комплекса одной из команд:

- Для Комплекса уровня Management:

```
cd /opt/datapk && docker-compose up -d
```

- Для Комплекса уровня Management + Sensor:

```
cd /opt/datapk && docker-compose up -d && cd /opt/sensor && docker-compose up -d
```

5. Дождитесь запуска работы всех сервисов.

12.4. Удаление данных Комплекса

Для удаления данных Комплекса:

1. Остановите работу сервисов, выполнив команду:

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

2. Выполните удаление данных командой:

```
/usr/bin/udv-remove-data
```

3. Запустите работу сервисов командой:

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

4. Дождитесь запуска работы всех сервисов.
5. Войдите в веб-интерфейс Комплекса и убедитесь, что все данные удалены.

13. Нештатные ситуации и действия по их устранению

В процессе использования решения возможно появление неполадок, ограничивающих возможности управления защитными механизмами или открывающих возможности для атаки на активы.

Если вам не удастся самостоятельно устранить нештатную ситуацию, обратитесь в службу поддержки.

13.1. Диагностика сервисов и иерархии

Скрипт `dtpk_get_logs-2_2.bash` однократно собирает количество запросов оперативных данных по иерархии и логи всех сервисов Комплекса на текущей аппаратной платформе за заданный период времени в часах.

Для диагностики работоспособности сервисов и иерархии в операционной системе Комплекса:

1. Запустите скрипт `dtpk_get_logs-2_2.bash` командой:

```
bash dtpk_get_logs-2_2.bash N
```

где N — период, за который будут собраны логи (в часах).

Пример

Чтобы собрать логи за последние 6 часов, выполните команду:

```
bash dtpk_get_logs-2_2.bash 6
```

- **Результат шага:** Будет создана директория `logs-hostname-date`.

2. Заархивируйте полученную директорию.
3. Заполните [анкету](#) и отправьте с ней архив на адрес сервисного центра ООО «КИТ.Р»: support@udv.group.

13.2. Действия по восстановлению комплекса при сбойных ситуациях и ошибках в данных

При эксплуатации Комплекса пользователь может столкнуться с различными видами затруднений, которые также возможно самостоятельно устранить. Основные типы затруднений:

- Веб-интерфейс не загружается
- Соединение с главной страницей веб-интерфейса осуществляется по протоколу HTTP вместо HTTPS
- Время на Комплексе отличается от времени получения события
- После запуска Комплекса при попытке загрузки веб-интерфейса открывается пустая страница
- 502-я ошибка при загрузке страницы авторизации, 500-е ошибки сразу после авторизации
- Не обнаруживаются новые потоки
- Комплекс не обнаруживает активы в автоматическом режиме
- Комплекс не обнаруживает активы без IP-адреса
- Два актива с одинаковым IP-адресом
- Не осуществляется сбор необходимых событий или конфигураций
- При попытке сбора данных в результатах выводится предупреждение «Превышено время ожидания выполнения задачи сбора событий»
- Сбор конфигураций осуществляется, но результаты сбора не отображаются
- Отсутствуют события, генерируемые Комплексом
- Не принимаются Syslog-сообщения от активов
- Не принимаются сообщения от служб корреляции и обнаружения вторжений
- Не принимаются сообщения от службы корреляции
- Не инициализируется стек udv-opensearch, udv-opensearch-dashboards, udv-logstash
- Не создается индекс в экспертном режиме страницы «События»
- Не удастся отфильтровать записи на странице «События» по новым значениям полей после нормализации
- Объекты мониторинга и визуализации импортируются с ошибкой
- Не удастся импортировать сканер сбора данных в веб-интерфейсе
- Не выполняется архивация событий при превышении размера или времени хранения индекса
- Ошибки вида «<...>Cannot start service <...>. Bind for <ip_address>:<TCP/UDP_port> is ready allocated» при попытке запуска сервисов
- Недоступен сервис корреляции событий
- При бездействии в веб-интерфейсе сеанс завершается раньше, чем через 10 минут
- Ошибки поиска уязвимостей в базах CVE, CPE и БДУ ФСТЭК России
- Не устанавливается соединение с сенсором

13.2.1. Веб-интерфейс не загружается

В качестве причины недоступности веб-интерфейса рассмотрены следующие:

- Некорректная инициализация сервисов Комплекса
- Некорректная генерация серверного сертификата и ключа Комплекса уровня Management
- Запрет на доступ к веб-интерфейсу Комплекса с текущей рабочей станции
- Отсутствие свободного места на диске

Некорректная инициализация сервисов Комплекса

Способ устранения

Для устранения затруднения:

1. Подключитесь к операционной системе Комплекса.
2. Просмотрите состояние сервисов, выполнив команду:

```
systemctl list-units udv-* --all
```



Внимание:

Все сервисы в полученном списке должны быть в состоянии *active* (поле **Active**).

3. Если какие-либо сервисы не запущены или имеют статус, отличный от *active*, остановите работу сервисов, выполнив команду:

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

4. Дождитесь остановки работы всех сервисов.
5. В рабочей директории Комплекса уровня Management проверьте и, в случае необходимости, откорректируйте файл `manager.env`.
6. В рабочей директории Комплекса уровня Sensor проверьте и, в случае необходимости, откорректируйте файл `sensor.env`.
7. В случае необходимости восстановите данные из резервной копии.



Подсказка:

Порядок восстановления данных приведен в разделе «[Восстановление данных из резервных копий](#)».

8. Запустите работу сервисов командой:

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

9. Дождитесь запуска работы всех сервисов.



Внимание:

При запуске не должно быть ошибок или предупреждений.

Некорректная генерация серверного сертификата и ключа Комплекса уровня Management

Способ устранения

Для устранения затруднения:

1. Убедитесь, что серверный сертификат и ключ в директории `/var/cache/udv/nginx/certs` корректно инициализированы, срок действия сертификата не истек. При необходимости сгенерируйте или замените сертификат и ключ.
2. Убедитесь, что файл серверного сертификата имеет расширение `.cert`.

3. Убедитесь, что значение переменной `HOST_IP` в файле `manager.env` соответствует наименованию серверного сертификата. Для этого выполните команду:

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

4. Если значение переменной не соответствует наименованию серверного сертификата, выполните следующие действия:

- а. Остановите работу сервисов, выполнив команду:

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

- б. Откройте файл `manager.env` на редактирование, выполнив команду:

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

- в. Измените значение переменной `HOST_IP`.

- г. Сохраните изменения в файле, нажав клавишу **F2**, и закройте файл, нажав клавишу **F10**.

- д. Запустите работу сервисов, выполнив команду:

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

Запрет на доступ к веб-интерфейсу Комплекса с текущей рабочей станции

Способ устранения

Для устранения затруднения:

1. Убедитесь, что в правилах межсетевого экрана `iptables` в файле `/etc/sysconfig/iptables` не указаны правила, разрешающие доступ к веб-интерфейсу Комплекса только с рабочих станций определенной подсети и запрещающий доступ со всех остальных. Для этого проверьте наличие следующего правила:

```
-A INPUT -p tcp -s [IP-адрес_подсети/маска_подсети] -m state --state NEW -m tcp --dport 443 -j ACCEPT
```

2. Если правила присутствуют в файле `/etc/sysconfig/iptables`, выполните вход в веб-интерфейс Комплекса из подсети, разрешенной правилами.

Отсутствие свободного места на диске

Способ устранения

Для устранения затруднения:

1. Проверьте свободное место на диске, выполнив команду:

```
df -h /
```

2. При отсутствии свободного места:

- а. Остановите сервисы Комплекса.
- б. Удалите ненужные данные с диска.
- в. Запустите сервисы Комплекса.

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

Причина: отсутствие серверного сертификата и ключа

Способ устранения

Для устранения затруднения:

1. Остановите работу сервисов, выполнив команду:

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

2. Убедитесь, что серверный сертификат и ключ в директории `/var/cache/udv/nginx/certs` корректно инициализированы, срок действия сертификата не истек. При необходимости сгенерируйте или замените их.
3. Убедитесь, что в файле `manager.env`, расположенном в рабочей директории Комплекса, значение переменной **HOST_IP** совпадает с наименованием серверного сертификата.
4. Запустите работу сервисов, выполнив команду:

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

13.2.3. Время на Комплексе отличается от времени получения события

В качестве причин некорректного отображения времени в Комплексе рассмотрены следующие:

- Время на активе отличается от времени на операционной системе Комплекса
- Время на рабочей станции отличается от времени на операционной системе Комплекса
- Некорректная настройка часового пояса в операционной системе Комплекса

Время на активе отличается от времени на операционной системе Комплекса

Способ устранения

Для устранения затруднения:

1. Авторизуйтесь на операционной системе актива.
2. Измените часовой пояс операционной системы.
3. При необходимости перезагрузите актив.

Время на рабочей станции отличается от времени на операционной системе Комплекса

Способ устранения

Для устранения затруднения:

1. Авторизуйтесь на рабочей станции, с которой ведется работа с веб-интерфейсом Комплекса уровня Management.
2. Измените часовой пояс рабочей станции так, чтобы он совпадал с часовым поясом Комплекса.

Некорректная настройка часового пояса в операционной системе Комплекса

Способ устранения

Для устранения затруднения:

1. Авторизуйтесь на операционной системе Комплекса уровня Management.
2. Настройте синхронизацию времени Комплекса с NTP-сервером.



Подсказка:

Подробнее о настройке NTP-сервера см. в инструкции Руководства по внедрению и поддержке «Настройка сертифицированной ОС Альт Сервер 10 SP».

13.2.4. После запуска Комплекса при попытке загрузки веб-интерфейса открывается пустая страница

Причина: некорректный файл `environment.json`, либо его отсутствие

Способ устранения

Для устранения затруднения:

1. Проверьте наличие и корректность файла `environment.json` в директории `/usr/share/udv/frontend`, расположенной в рабочей директории Комплекса уровня Management.
2. При необходимости переустановите сервис `udv-frontend`, выполнив команду:

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

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

13.2.5. 502-я ошибка при загрузке страницы авторизации, 500-е ошибки сразу после авторизации

В качестве причин ошибок в веб-интерфейсе Комплекса рассмотрены следующие:

- Комплекс не до конца инициализировался после запуска работы сервисов
- Некорректно настроены правила межсетевого экрана для доступа к сервисам Комплекса
- Отсутствие свободного места на диске

Комплекс не до конца инициализировался после запуска работы сервисов

Способ устранения

Для устранения затруднения:

1. Подождите 3-5 минут после запуска сервисов.
2. При повторяющихся ошибках выполните команду:

```
systemctl list-units udv-*
```

3. Все сервисы должны быть в состоянии `active`. При ошибках в журналах сервисов см. п. «Некорректная инициализация сервисов Комплекса» в разделе «Веб-интерфейс не загружается».

Некорректно настроены правила межсетевого экрана для доступа к сервисам Комплекса

Способ устранения

Для устранения затруднения:

1. Убедитесь, что на Комплексе уровня установлены корректные правила межсетевого экранирования `iptables` в файле `/etc/sysconfig/iptables`:
 - правила для уровня Management:

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

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

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

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

```
COMMIT
```

- правила для уровня Management+Sensor:

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

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

COMMIT
```

2. При необходимости настройте правила iptables:

- Остановите работу сервисов, выполнив команду:

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

- Откройте для редактирования конфигурационный файл iptables с правилами межсетевого экранирования:

```
mcedit /etc/sysconfig/iptables
```

- Добавьте правила в конфигурационный файл iptables в зависимости от конфигурации Комплекса согласно шагу 1.

- Перезапустите сервис iptables:

```
systemctl restart iptables
```

- Запустите работу сервисов, выполнив команду:

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

Отсутствие свободного места на диске

Способ устранения

Для устранения затруднения:

1. Проверьте свободное место на диске, выполнив команду:

```
df -h /
```

2. При отсутствии свободного места:
 - а. Остановите сервисы Комплекса.
 - б. Удалите ненужные данные с диска.
 - в. Запустите сервисы Комплекса.

13.2.6. Не обнаруживаются новые потоки

В качестве причин отсутствия обнаружения новых потоков рассмотрены следующие:

- Некорректные настройки домашней сети на странице **Сенсоры**
- Комплекс получает информацию о новых потоках данных с задержкой
- Некорректные настройки интерфейса сенсора, выполняющего прослушивание всего трафика домашней сети
- Некорректные настройки зеркалирования трафика на активном сетевом оборудовании (АСО) или отсутствие сетевого трафика
- Некорректное значение переменной сенсора LISTENING_INTERFACES
- В Комплексе отключено обнаружение потоков для неполных TCP-сессий
- Ошибки в сервисе godpi

Некорректные настройки домашней сети на странице **Сенсоры**

Способ устранения

Для устранения затруднения:

1. На странице **Сенсоры** веб-интерфейса Комплекса убедитесь, что добавлены все домашние сети, которые прослушивают подключенные сенсоры.
2. Убедитесь, что IP-адрес актива принадлежит хотя бы одному из диапазонов адресов домашней сети сенсоров.
3. Выполните сканирование домашней сети (см. раздел «**Сканирование сети и определение интерфейсов активного сетевого оборудования**»).

Комплекс получает информацию о новых потоках данных с задержкой

Способ устранения

Для устранения затруднения:

1. Выполните настройку домашней сети сенсоров согласно инструкции в п. выше «**Некорректные настройки домашней сети на странице **Сенсоры****».
2. Дождитесь обновления информации о потоках на странице **Потоки данных** (до 5 минут) — такая задержка допустима из-за особенностей передачи данных с сенсоров на Комплекс.

Некорректные настройки интерфейса сенсора, выполняющего прослушивание всего трафика домашней сети

Способ устранения

Для устранения затруднения:

1. Выполните команду в операционной системе сенсора:

```
ifconfig [наименование прослушивающего интерфейса сенсора]
```

или:

```
ip -a link show [наименование прослушивающего интерфейса сенсора]
```

2. Убедитесь, что интерфейс в состоянии UP и режиме PROMISC.
3. При необходимости откорректируйте сетевые настройки.

Некорректные настройки зеркалирования трафика на активном сетевом оборудовании (АСО) или отсутствие сетевого трафика

Способ устранения

Для устранения затруднения:

1. Несколько раз выполните команду в операционной системе сенсора:

```
ifconfig [наименование прослушивающего интерфейса сенсора]
или:
ip -s -s link show [наименование прослушивающего интерфейса сенсора]
```

2. Убедитесь в том, что параметр RX packets постепенно увеличивается.
3. Проверьте настройки зеркалирования на АСО. При необходимости откорректируйте их.
4. Убедитесь в наличии связи между интерфейсами АСО и сенсором.
5. Сгенерируйте сетевую активность. Для этого отправьте ICMP-пакеты с интерфейса сенсора на интерфейс любого актива.

Некорректное значение переменной сенсора LISTENING_INTERFACES

Способ устранения

Для устранения затруднения:

1. Остановите работу сервисов, выполнив команду:

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

2. Укажите значения слушающих интерфейсов в переменной LISTENING_INTERFACES файла sensor.env.



Подсказка:

Переменная может быть представлена в виде списка интерфейсов через запятую, и одно из значений должно быть равно названию интерфейса сенсора, выполняющего прослушивание всего трафика.

3. Запустите сервисы, выполнив команду:

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

В Комплексе отключено обнаружение потоков для неполных TCP-сессий

В некоторых случаях Комплекс может не обнаружить заголовков TCP-сессии в прослушиваемом трафике. Например, при поступлении пакетов на анализатор трафика в неправильном порядке, подключении Комплекса в момент уже установившейся TCP-сессии (сессии в АСУ ТП могут существовать продолжительное время), потерями части трафика на сетевых устройствах. Чтобы регистрировать потоки для неполных TCP-сессий, необходимо добавить переменную GODPI_TCP_SKIP_SESSION_WITHOUT_HANDSHAKE=false в файл sensor.env

Способ устранения

Для включения обнаружения неполных TCP-сессий:

1. Остановите работу сервисов, выполнив команду:

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

2. Добавьте в файл `sensor.env` переменную `GODPI_TCP_SKIP_SESSION_WITHOUT_HANDSHAKE` и присвойте ей значение `false`.

3. Запустите сервисы, выполнив команду:

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

Ошибки в сервисе godpi

Способ устранения

Для устранения затруднения:

1. Выполните команду в операционной системе сенсора:

```
systemctl status udv-godpi.service
```



Подсказка:

Сервис должен быть в состоянии `active` (поле **Active**).

2. Просмотрите журнал `godpi` на наличие критичных ошибок, выполнив команду:

```
journalctl -feu udv-godpi.service
```

3. Убедитесь, что в начале инициализации `godpi` корректно подключился к базе, загрузил правила и публикация событий о потоках начата. При ошибках см. п. «[Некорректная инициализация сервисов Комплекса](#)» в разделе «[Веб-интерфейс не загружается](#)».

13.2.7. Комплекс не обнаруживает активы в автоматическом режиме

В качестве причин отсутствия автоматического обнаружения активов рассмотрены следующие:

- Некорректные настройки домашней сети на странице **Сенсоры**
- Отсутствие трафика с актива
- Комплекс получает информацию о новых активах с задержкой
- Частичное зеркалирование сетевого трафика

Некорректные настройки домашней сети на странице **Сенсоры**

Способ устранения

Для устранения затруднения:

1. На странице **Сенсоры** веб-интерфейса Комплекса убедитесь, что добавлены все домашние сети, которые прослушивают подключенные сенсоры.
2. Убедитесь, что IP-адрес актива принадлежит хотя бы одному из диапазонов адресов домашней сети сенсоров.
3. Выполните сканирование домашней сети (см. раздел «[Сканирование сети и определение интерфейсов активного сетевого оборудования](#)»).

Отсутствие трафика с актива

Способ устранения

Для устранения затруднения:

Сгенерируйте сетевую активность требуемого актива. Для этого отправьте ICMP-трафик между интерфейсами сенсора и актива.

► **Результат шага:** при отсутствии проблем с обнаружением потоков требуемый актив должен появиться в списке активов на странице **Активы** веб-интерфейса Комплекса.

Комплекс получает информацию о новых активах с задержкой

Способ устранения

Для устранения затруднения:

1. Выполните настройку домашней сети сенсоров согласно п. выше «[Некорректные настройки домашней сети на странице Сенсоры](#)».
2. Сгенерируйте сетевую активность на активе согласно п. выше «[Отсутствие трафика с актива](#)».
3. Дождитесь обновления информации о потоках на странице **Потоки данных** (до 5 минут) — такая задержка допустима из-за особенностей передачи данных с сенсоров на Комплекс.

Частичное зеркалирование сетевого трафика

Способ устранения

Для устранения затруднения:

1. Создайте актив вручную на странице **Активы** веб-интерфейса Комплекса.
2. Отредактируйте сетевые настройки в реквизитах созданного актива.



Подсказка:

Подробнее см. раздел «[Работа с активами](#)».

13.2.8. Комплекс не обнаруживает активы без IP-адреса

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

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

Способ устранения

Для устранения затруднения:

1. Подключитесь к операционной системе Комплекса уровня Management.
2. Остановите работу сервисов, выполнив команду:

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

3. Дождитесь остановки работы всех сервисов.
4. В конфигурационном файле `manager.env` присвойте переменной `AUTOMATIC_HOST_CREATION_BY_MAC` значение `false`.
5. Запустите работу сервисов командой:

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

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

13.2.9. Два актива с одинаковым IP-адресом

В списке на странице **Активы** отображается новый актив с IP-адресом актива, который уже был в списке. Возможные причины:

- При снятии трафика с нескольких точек актив был обнаружен с MAC-адресом маршрутизатора
- Один актив был обнаружен несколькими сенсорами



Подсказка:

Похожие ошибки см. в разделе «Рекомендуемые действия в случае обнаружения событий на странице «Контроль сетевых узлов»».

При снятии трафика с нескольких точек актив был обнаружен с MAC-адресом маршрутизатора



Подсказка:

Если актив был обнаружен сперва со своим IP-адресом и MAC-адресом маршрутизатора, а уже после был распознан MAC-адрес самого актива, то на странице **Активы** будут отображаться оба актива (с одинаковым IP и разными MAC-адресами). Такое поведение необходимо для отслеживания попыток подмены MAC-адреса.

Способ устранения

Для устранения затруднения:

В карточке более раннего актива присвойте ему интерфейс с MAC-адресом маршрутизатора:

- а. Перейдите в **карточку актива**.
- б. Нажмите кнопку  напротив блока **Сетевые атрибуты**.
 - **Результат шага:** появится окно **Редактирование сетевых атрибутов актива**.
- в. Отметьте параметр **Выбрать сетевой атрибут неизвестного актива**.
- г. В выпадающем списке выберите интерфейс неизвестного актива с тем же IP-адресом.
- д. Нажмите  (**Создать сетевой атрибут**) для подтверждения изменений.
- е. Установите чекбокс **Интерфейс для сбора данных** напротив интерфейса с собственным MAC-адресом.
- ж. Нажмите  (**Сохранить изменения**) для подтверждения изменений.



Подсказка:

Подробнее о присвоении активам интерфейсов других активов см. раздел «Редактирование активов».

► **Результат шага:** Актив, чей единственный интерфейс был привязан к другому активу, будет удален из списка на странице **Активы**.

Один актив был обнаружен несколькими сенсорами

Способ устранения

Для устранения затруднения:

1. На странице **Сенсоры** веб-интерфейса Комплекса убедитесь, что добавленные домашние сети сенсоров не пересекаются друг с другом.
2. В карточке одного актива присвойте ему интерфейс другого актива согласно инструкции в п. выше «[При снятии трафика с нескольких точек актив был обнаружен с MAC-адресом маршрутизатора](#)».

13.2.10. Не осуществляется сбор необходимых событий или конфигураций

Для проблем со сбором событий или конфигураций могут быть следующие причины:

- Некорректные настройки актива
- Ошибки в Python-скрипте сбора данных, неверные настройки учетных данных актива или расписания задачи сбора данных



Подсказка:

Список возможных проблем сбора данных см. в разделе «Рекомендуемые действия в случае обнаружения событий на панели мониторинга «Сбор данных».

Некорректные настройки актива

Способ устранения

Для устранения затруднения:

1. Убедитесь в корректности настроек служб и разрешений для сбора данных с выбранного актива.
2. Убедитесь, что активу присвоены учетные данные с правами, которые:
 - позволяют получать информацию удаленно;
 - позволяют получать критичную информацию, запрашиваемую скриптом сбора данных.

Ошибки в Python-скрипте сбора данных, неверные настройки учетных данных актива или расписания задачи сбора данных

Способ устранения

Для устранения затруднения:

1. Проанализируйте сообщения об ошибках на страницах **Статус сбора**, **Задачи сбора**, **События**, на панели мониторинга **Сбор данных** и на диаграммах в карточке актива.
2. Просмотрите содержание Python-скриптов сбора данных из сканеров, работа которых завершается ошибками, и найдите в них названия сервисов, участвующих в сборе данных (коннекторов). Название расположено в скобках после команды `execute`.

```
table = execute('sql', protocol_args, expiration)
return {
    'visible_keys': {
        'ID': 'Идентификатор группы',
        'name': 'Имя группы',
        'EXPTIME': 'Параметры отключения пользователей',
    },
    'keys': ['ID', 'name', 'EXPTIME'],
    'data': [[str(row[col]) for col in ['ID', 'name', 'EXPTIME']] for row in table]
}
```

Рис. 296. Расположение названия коннектора в Python-скрипте сбора данных

3. На странице **Сенсоры** найдите сенсор, прослушивающий домашнюю сеть актива.
4. Подключитесь к операционной системе сенсора, который собирает данные из домашней сети актива.
5. Просмотрите список имеющихся сервисов-коннекторов:

```
systemctl list-units *-connector.service --all
```

- **Результат шага:** будет выведен список сервисов-коннекторов.

```
[root@DATAKTESTTK22 ~]# systemctl list-units *-connector.service --all
UNIT                                LOAD    ACTIVE SUB    DESCRIPTION
udv-modbus-connector.service        loaded active running Modbus connector
udv-opc-connector.service            loaded active running Opc connector service
udv-plc-config-connector.service     loaded active running Config acquisition from PLC
udv-plc-connector.service            loaded active running Data acquisition from PLC by oven and s7comm protocol.
udv-snmp-connector.service           loaded active running SNMP connector
udv-sql-connector.service            loaded active running Service for connecting to a database
udv-terminal-connector.service       loaded active running Terminal connector

LOAD    = Reflects whether the unit definition was properly loaded.
ACTIVE  = The high-level unit activation state, i.e. generalization of SUB.
SUB     = The low-level unit activation state, values depend on unit type.
7 loaded units listed.
To show all installed unit files use 'systemctl list-unit-files'.
```

Рис. 297. Список коннекторов Комплекса

6. Найдите подходящий коннектор.



Подсказка:

Название коннектора в выводе команды не полностью совпадает с названием в Python-скрипте сбора данных. За исключением `msrpc` название коннектора в выводе команды содержит `_connector`.

7. Просмотрите журналы коннекторов, на которых обнаружены проблемы. Например `udv-host-data-collector`:

```
journalctl -fu udv-host-data-collector.service
```

8. Посмотрите журналы сервиса `udv-command-processor`, который отвечает за все запущенные процессы сбора данных:

```
journalctl -fu udv-command-processor.service
```

9. При необходимости отредактируйте сканеры сбора данных, расписание задачи, учетные данные актива.

13.2.11. При попытке сбора данных в результатах выводится предупреждение «Превышено время ожидания выполнения задачи сбора событий»

Для получения предупреждения *Превышено время ожидания выполнения задачи сбора событий* возможны следующие причины:

- Актив не может принять несколько одновременных подключений к нему по одному или нескольким протоколам
- Переполнена очередь задач сбора данных в сервисе `udv-rabbitmq` Комплекса
- Заканчивается максимальное время ожидания выполнения задачи сбора данных



Подсказка:

Список возможных проблем сбора данных см. в разделе «Рекомендуемые действия в случае обнаружения событий на панели мониторинга «Сбор данных».

Актив не может принять несколько одновременных подключений к нему по одному или нескольким протоколам

Рекомендации по настройке запуска задач сбора данных с одного актива

Для устранения затруднения:

1. Настраивайте сбор событий с промежутком между запусками задач (для каждой задачи установите отдельное от остальных задач время выполнения).
2. Используйте сканеры сбора событий с ОС Windows, которые собирают только критичные события.
3. В одну задачу добавляйте не более одного сканера сбора данных.

Переполнена очередь задач сбора данных в сервисе `udv-rabbitmq` Комплекса

Способ устранения

Для устранения затруднения:

1. Перейдите в карточку актива (или нескольких активов), для которого настроено расписание задачи сбора данных.
2. Отмените выполнение одной или нескольких задач сбора данных по расписанию (отмените выбор чекбокса ☒ в строке с названием задачи).
3. Подключитесь к операционной системе Комплекса уровня Management.
4. Остановите работу сервисов, выполнив команду:

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

5. Выполните команду очистки очереди сервиса `udv-rabbitmq`. Для этого выполните команду:

```
rm -rf /var/lib/rabbitmq/mnesia/*
```

6. Запустите работу сервисов командой:

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

7. Дождитесь запуска работы всех сервисов.
8. Выполните повторный запуск сбора данных.

Заканчивается максимальное время ожидания выполнения задачи сбора данных

Способ устранения

Увеличьте максимальное время ожидания выполнения задачи сбора данных для одного сканера.

1. Перейдите на страницу **Администрирование** → → **Сканеры**.
2. Откройте необходимый сканер сбора данных на редактирование.
3. Увеличьте значение в поле **Максимальное время ожидания выполнения задачи**.
4. Нажмите кнопку **Сохранить** для подтверждения изменений.
5. Дождитесь сбора задачи сбора данных, создайте новую или запустите сканер.

13.2.12. Сбор конфигураций осуществляется, но результаты сбора не отображаются



Подсказка:

Список возможных проблем сбора данных см. в разделе «Рекомендуемые действия в случае обнаружения событий на панели мониторинга «Сбор данных».

Причина: некорректный Python-скрипт сбора данных, неверное регулярное выражение

Способ устранения

Для устранения затруднения:

Проверьте на корректность Python-скрипт из сканера, работа которого завершается с ошибкой.



Внимание:

Для первого запуска рекомендуется отказаться от синтаксического разбора данных в скрипте посредством регулярных выражений.

13.2.13. Отсутствуют события, генерируемые Комплексом

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

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

Генерация событий отключена в настройках переменных

В конфигурационном файле `manager.env` Комплекса уровня Management переменным, отвечающим за отключение и включение генерации событий от служебных источников, присвоены значения `true` (генерация событий отключена).

Способ устранения

Для устранения затруднения:

Присвойте необходимым переменным значение `false` или удалите переменные из файла `manager.env`.



Подсказка:

Порядок работы с указанными переменными приведен в подразделе «Включение и отключение служебных источников» Руководства по эксплуатации. «[Включение и отключение служебных источников](#)».

Диск операционной системы Комплекса заполнен более, чем на 90%

Сервис хранения и поиска событий недоступен в результате заполнения дискового пространства более, чем на 90%.

Способ устранения

Для устранения затруднения:

1. Авторизуйтесь на операционной системе Комплекса уровня Management.
2. Убедитесь, что сервис хранения и поиска событий недоступен:

```
journalctl -fu udv-logstash.service
```

► **Результат шага:** в журнале будут отображаться события вида *Opensearch в режиме read-only*.

3. Остановите работу сервисов Комплекса:

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

4. Удалите ненужные файлы с дискового пространства.
5. При необходимости измените значения переменных `EVENT_INDICES_MAX_SIZE_GB` и `EVENT_ARCHIVES_MAX_SIZE_GB`:

- а. Откройте на редактирование файл `manager.env`.
- б. Найдите и измените значения переменных:

```
EVENT_INDICES_MAX_SIZE_GB=[значение]  
EVENT_ARCHIVES_MAX_SIZE_GB=[значение]
```



Внимание:

Суммарный объем с `EVENT_ARCHIVES_MAX_SIZE_GB` не должен составлять более 50-60% объема дискового пространства.

На Комплексах базового уровня и (или) с HDD — не более 100 ГБ. На Комплексах среднего и верхнего уровней с SSD — не более 300 ГБ

6. Очистите репозиторий с пакетами.

7. Если предыдущие способы не дали результата, очистите метаданные сервиса.



ОСТОРОЖНО:

При очистке будут утеряны все индексы событий и элементы раздела **Мониторинг**: шаблон индекса, панели мониторинга, сохраненные поиски, фильтры.

Для очистки выполните команду:

```
rm -rf /var/lib/opensearch/nodes/*
```

8. Восстановите утерянные данные.



Подсказка:

Подробнее о настройке см. разделы «Создание шаблона индекса», «Импорт сохраненных объектов».

9. Запустите сервисы Комплекса:

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

10. Убедитесь в работоспособности сервиса хранения и поиска событий:

а. Выполните следующий запрос:

```
curl -XPUT "http://127.0.0.1:9200/_settings" -H 'Content-Type: application/json' -d  
'{"index":{"blocks":{"read_only_allow_delete":"false"}}}'
```

► **Результат шага:** запись вида `"acknowledged":true` свидетельствует об успешном выполнении запроса.

б. Выполните действия, в результате которых должны появиться события.



Подсказка:

Например, создайте и удалите новые элементы справочников (правил, классификаторов), выполните сбор событий или конфигураций с актива.

в. Перейдите на страницу **События**.

г. Найдите события по результатам выполненных действий.

11. Если события отсутствуют, ознакомьтесь с инструкциями ниже по устранению нештатных ситуаций.

13.2.14. Не принимаются Syslog-сообщения от активов

Для отсутствия сообщений Syslog от активов могут быть следующие причины:

- Наименование актива не совпадает с сетевым именем (hostname) узла или в списке активов присутствуют активы с такими же IP-адресами
- Не создан или некорректно создан источник для приема Syslog-сообщений
- Некорректная настройка отправки Syslog-сообщений на активе

Наименование актива не совпадает с сетевым именем (hostname) узла или в списке активов присутствуют активы с такими же IP-адресами

Способ устранения

Для устранения затруднения:

1. Убедитесь, что наименование актива совпадает с его hostname.
2. Убедитесь в отсутствии известных активов с такими же IP-адресами.

Не создан или некорректно создан источник для приема Syslog-сообщений

Способ устранения

Для устранения затруднения:

Убедитесь, что источник для приема Syslog-сообщений выбранного актива корректно инициализирован на странице **Администрирование** → **Настройка активов** → **Источники**.

Некорректная настройка отправки Syslog-сообщений на активе

Способ устранения

Для устранения затруднения:

Проверьте настройки отправки Syslog-сообщений на активе, убедитесь, что актив отправляет события на требуемый IP-адрес и порт.

13.2.15. Не принимаются сообщения от служб корреляции и обнаружения вторжений

Причина: наименование служебного актива не совпадает с сетевым именем (hostname) Комплекса

Способ устранения

Для устранения затруднения:

1. Убедитесь, что наименование Комплекса уровня Management совпадает с его сетевым именем на странице **Администрирование → О системе**.
2. Подключитесь к операционной системе Комплекса уровня Management.
3. Выполните команду `export`. Убедитесь, что переменная `HOSTNAME` присутствует в выводе команды и содержит сетевое имя Комплекса.
4. Если переменная `HOSTNAME` отсутствует в выводе команды `export`:

- а. Остановите работу сервисов Комплекса без удаления накопленных данных.
- б. Откройте файл `/etc/profile` в режиме редактирования с помощью редактора `nano`:

```
mcedit /etc/profile
```

- в. Добавьте в конец файла строку:

```
export HOSTNAME
```

- г. Сохраните изменения и закройте файл `/etc/profile`.
- д. Перезагрузите сеанс пользователя или перезагрузите ОС.
- е. Запустите работу сервисов Комплекса.
- ж. Убедитесь, что наименование Комплекса совпадает с его сетевым именем на странице **Администрирование → О системе**.

13.2.16. Не принимаются сообщения от службы корреляции

Причина: некорректная или устаревшая директория logstash

Способ устранения

Для устранения затруднения:

1. Остановите работу сервисов, выполнив команду:

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

2. Дождитесь остановки работы всех сервисов.
3. Переустановите сервис udv-logstash, выполнив команду:

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

4. Запустите работу сервисов командой:

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

5. Дождитесь запуска работы всех сервисов.

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

Возможны следующие причины:

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

Некорректное значение системной переменной `vm.max_map_count`

Способ устранения

Для устранения затруднения:

1. Проверьте значение переменной в операционной системе Комплекса уровня Management. Для этого выполните команду:

```
sysctl vm.max_map_count
```

2. Убедитесь, что данная переменная имеет значение `262144`.
3. При необходимости откорректируйте значение переменной. Для этого:
 - а. Откройте файл `/etc/sysctl.conf`.
 - б. Добавьте строку `vm.max_map_count = 262144`.
 - в. Либо, если строка с переменной уже была добавлена, измените значение переменной.
4. Выполните команду для немедленной установки переменной `vm.max_map_count` (без перезагрузки):

```
sysctl -w vm.max_map_count=262144
```

Ошибки в настройках нормализации

Способ устранения

Для устранения затруднения:

1. Посмотрите журнал сервиса `udv-logstash`. Для этого введите команду:

```
journalctl -fu udv-logstash.service
```

2. Остановите работу сервисов, выполнив команду:

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

3. Дождитесь остановки работы всех сервисов.
4. Переустановите сервис `udv-logstash`, выполнив команду:

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

5. Запустите работу сервисов командой:

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

6. Дождитесь запуска работы всех сервисов.

13.2.18. Не создается индекс в экспертном режиме страницы «События»

Причина: отсутствуют события в Комплексе

Способ устранения

Для устранения затруднения:

1. Сгенерируйте события действий в веб-интерфейсе.



Подсказка:

Например, создайте и удалите новые элементы справочников (правил, классификаторов), выполните сбор событий или конфигураций с актива.

2. Создайте или включите источники активов и сгенерируйте на них события.

13.2.19. Не удастся отфильтровать записи на странице «События» по новым значениям полей после нормализации

Причина: отсутствуют события с новыми полями, не обновлен шаблон индекса

Способ устранения

Для устранения затруднения:

1. Обновите шаблон индекса на странице **Администрирование** → **Настройки мониторинга**, вкладка **Шаблоны Индексов**.
2. Убедитесь, что после нормализации было принято событие с новыми полями (помеченными желтым восклицательным знаком на странице **События** → **Экспертный режим**).

13.2.20. Объекты мониторинга и визуализации импортируются с ошибкой

Причина: отсутствуют нужные поля в шаблоне индекса

Способ устранения

Для устранения затруднения:

1. Убедитесь в целостности директории `/etc/logstash`, расположенном в рабочей директории Комплекса уровня Management.
2. Убедитесь, что все нужные поля присутствуют в шаблоне индекса.
3. При отсутствии необходимых полей:
 - а. Обновите шаблон индекса.
 - б. Убедитесь, что было принято событие с новыми полями.
 - в. Удалите сохраненные объекты (страница **Мониторинг** → **Настройки мониторинга**, вкладка **Сохраненные Объекты**).
 - г. Повторите импорт.

13.2.21. Не удается импортировать сканер сбора данных в веб-интерфейсе

Для проблем с импортом сканера сбора данных могут быть следующие причины:

- Неверная цепочка сертификатов для проверки цифровой подписи Python-скрипта в сканере
- Неверная кодировка Python-скрипта сбора данных
- Сканер сбора данных был изменен с момента создания его последней цифровой подписи

Неверная цепочка сертификатов для проверки цифровой подписи Python-скрипта в сканере

Способ устранения

Для устранения затруднения:

1. Убедитесь, что конечный сертификат `datapk_script.crt`, используемый для проверки подлинности Python-скриптов сбора данных, является клиентским для корневого сертификата `ca.crt`. Для этого выполните следующую команду:

```
openssl verify  
-CAfile /usr/share/udv/certs/ca.crt /usr/share/udv/scripts-certs/datapk_script.crt
```

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

```
/usr/share/udv/scripts-certs/datapk_script.crt: OK
```

2. При необходимости замените конечный сертификат `datapk_script.crt` и повторно выполните верификацию.
3. Повторно выполните цифровую подпись Python-скрипта.
4. Создайте новый сканер или измените существующий, импортировав в него новый Python-скрипт и его цифровую подпись. Либо импортируйте набор сканеров с новыми цифровыми подписями в веб-интерфейсе Комплекса.

Неверная кодировка Python-скрипта сбора данных

Способ устранения

Для устранения затруднения:

1. Откройте Python-скрипт сбора данных с помощью текстового редактора.
2. Убедитесь, что Python-скрипт имеет кодировку UTF-8 без BOM. При необходимости измените кодировку и сохраните изменения.
3. Повторно выполните цифровую подпись Python-скрипта.
4. Создайте новый сканер или измените существующий, импортировав в него новый Python-скрипт и его цифровую подпись. Либо импортируйте набор сканеров с новыми цифровыми подписями в веб-интерфейсе Комплекса.

Сканер сбора данных был изменен с момента создания его последней цифровой подписи

Python-скрипт, размещенный и подписываемый в операционной системе Комплекса, не совпадает со скриптом, размещенным на локальной ОС и загружаемым в веб-интерфейсе Комплекса) при создании сканера.

Способ устранения

Для устранения затруднения:

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

13.2.22. Не выполняется архивация событий при превышении размера или времени хранения индекса

Возможны следующие причины:

- Директориям, в которые выполняется загрузка архивов, не присвоены права для загрузки в них файлов
- В переменной файла `manager.env` настроено удаление индексов вместо сохранения в архив

Директориям, в которые выполняется загрузка архивов, не присвоены права для загрузки в них файлов

Способ устранения

Для устранения затруднения:

1. Подключитесь к операционной системе Комплекса уровня Management.
2. Убедитесь, что следующим директориям, расположенным в рабочей директории Комплекса уровня Management, присвоены права доступа `drwxrwxrwx`:

- `/var/backups/elasticsearch`:
 - `/var/backups/elasticsearch/indices`
 - `/var/backups/elasticsearch/uploads`

Для этого введите команду:

```
ls -la [путь к директории]
```

3. При необходимости измените права на указанные директории с помощью следующих команд:

```
chmod -R 777 /var/backups/elasticsearch
```

где ключ `-R` — рекурсивное изменение прав (они будут применены и к вложенным директориям).

4. Повторно выполните архивацию событий (индексов) через веб-интерфейс Комплекса (подробнее см. раздел «Выгрузка событий Комплекса в архив»).

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

Способ устранения

Для устранения затруднения:

1. Остановите работу сервисов, выполнив команду:

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

2. В конфигурационном файле `manager.env` присвойте переменной `EVENT_INDICES_ACTION_SIZE_EXCEEDED` значение `rotate`.

3. Запустите работу сервисов командой:

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

4. Дождитесь запуска работы всех сервисов.

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

Причина: указанный в тексте ошибки TCP или UDP-порт требуется для запуска сервиса, но он занят сторонним сервисом или утилитой

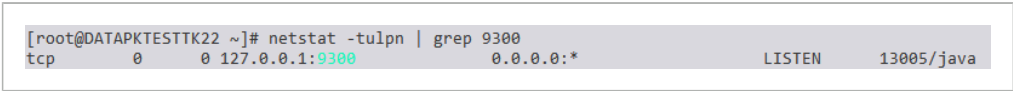
Способ устранения

Для устранения затруднения:

1. Измените номер используемого порта для стороннего сервиса в настройках сервиса.
2. При невозможности изменения номера порта отключите сторонний сервис, которым занят порт:
 - а. Узнайте наименование сервиса, которым занят порт, с помощью команды:

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

► **Результат шага:** в выводе команды отображаются наименование сервиса, занятый им порт и идентификатор процесса.



```
[root@DATAPKTESTTK22 ~]# netstat -tulpn | grep 9300
tcp        0      0 127.0.0.1:9300        0.0.0.0:*        LISTEN      13005/java
```

Рис. 298. Наименование сервиса, занятый им порт и идентификатор процесса

- б. Остановите процесс с полученным номером:

```
kill -9 [идентификатор_процесса]
```
 - в. При необходимости остановки процесса и его дочерних процессов:

```
killall [идентификатор_процесса]
```
 - г. Повторите запуск работы сервисов Комплекса.

13.2.24. Недоступен сервис корреляции событий

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

Способ устранения

Для устранения затруднения:

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

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

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

13.2.25. При бездействии в веб-интерфейсе сеанс завершается раньше, чем через 10 минут

В качестве причин раннего завершения сеанса рассмотрены следующие:

- Время завершения сеанса пользователя при бездействии задано меньше 10 минут
- Под уже используемой учетной записью совершил вход другой пользователь

Время завершения сеанса пользователя при бездействии задано меньше 10 минут

Время бездействия в веб-интерфейсе, после которого текущая сессия пользователя автоматически завершается и происходит переход на страницу авторизации, настраивается в переменной `USER_SESSION_INACTIVITY_TIMEOUT` файла `manager.env` Комплекса уровня Management и по умолчанию равно 600 секунд.

Способ устранения

Для устранения затруднения:

1. Перейдите в командную строку операционной системы Комплекса уровня Management.
2. Остановите работу сервисов, выполнив команду:

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

3. Дождитесь остановки работы всех сервисов.
4. В конфигурационном файле `manager.env` присвойте переменной `USER_SESSION_INACTIVITY_TIMEOUT` необходимый лимит времени бездействия в секундах.
5. Запустите работу сервисов командой:

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

6. Дождитесь запуска работы всех сервисов.
 - **Результат шага:** сессия пользователей будет завершаться после времени бездействия, указанного в переменной `USER_SESSION_INACTIVITY_TIMEOUT`.

Под уже используемой учетной записью совершил вход другой пользователь

Ограничение на количество сессий под одной учетной записью настраивается в переменной `LIMIT_USER_SESSIONS` файла `manager.env` Комплекса уровня Management. По умолчанию разрешается вход с неограниченного количества устройств под одной учетной записью (переменная имеет значение `false`) — при создании новой сессии предыдущая завершается.

Способ устранения

Для устранения затруднения:

1. При необходимости создайте в веб-интерфейсе новые учетные записи для других пользователей.
2. При необходимости отключите ограничение на вход под одной учетной записью:
 - а. Остановите работу сервисов, выполнив команду:

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

- б. В конфигурационном файле `manager.env` добавьте переменную `LIMIT_USER_SESSIONS` и установите ей значение `false`.

в. Запустите работу сервисов командой:

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

г. Дождитесь запуска работы всех сервисов.

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

13.2.26. Ошибки поиска уязвимостей в базах CVE, CPE и БДУ ФСТЭК России

Возможны следующие ошибки поиска уязвимостей в базах CVE и CPE:

- Ошибка вида «Не удалось получить список ПО. Убедитесь, что данные об установленном ПО были собраны корректно»
- Ошибка вида «Не удалось сохранить отчет. Убедитесь в работоспособности Комплекса или обратитесь к администратору»
- Ошибка вида «Непредвиденная ошибка. Убедитесь в работоспособности Комплекса или обратитесь к администратору»
- Ошибка вида «ПО для сканирования уязвимостей в реестре CPE не обнаружено»

13.2.26.1. Ошибка вида «Не удалось получить список ПО. Убедитесь, что данные об установленном ПО были собраны корректно»

Возможны следующие причины:

- Не удается запустить сканер сбора списка ПО, либо запуск завершается с ошибками
- Сканер запустился, но не отображает результаты на странице «Список ПО»

Не удается запустить сканер сбора списка ПО, либо запуск завершается с ошибками

Способ устранения

Для устранения затруднения перейдите в раздел «Не осуществляется сбор необходимых событий или конфигураций» или «При попытке сбора данных в результатах выводится предупреждение «Превышено время ожидания выполнения задачи сбора событий».

Сканер запустился, но не отображает результаты на странице «Список ПО»

Способ устранения

Для устранения затруднения перейдите в раздел «Сбор конфигураций осуществляется, но результаты сбора не отображаются».

13.2.26.2. Ошибка вида «Не удалось сохранить отчет. Убедитесь в работоспособности Комплекса или обратитесь к администратору»

Возможны следующие причины:

- Отсутствие свободного места на диске
- Ошибки в сервисе `udv-vulnerability-backend`

Отсутствие свободного места на диске

Способ устранения

Для устранения затруднения:

1. Проверьте свободное место на диске, выполнив команду:

```
df -h /
```

2. При отсутствии свободного места:
 - а. Остановите сервисы Комплекса.
 - б. Удалите ненужные данные с диска.
 - в. Запустите сервисы Комплекса.

Ошибки в сервисе `udv-vulnerability-backend`

Способ устранения

Для устранения затруднения:

1. Убедитесь, что в журнале системных сообщений сервиса `udv-vulnerability-backend` нет ошибок, по команде:

```
journalctl -fu udv-vulnerability-backend.service
```

2. При ошибках в журналах сервисов см. п. «Некорректная инициализация сервисов Комплекса» в разделе «Веб-интерфейс не загружается».

13.2.26.3. Ошибка вида «Непредвиденная ошибка. Убедитесь в работоспособности Комплекса или обратитесь к администратору»

Причина: ошибки в сервисе поиска уязвимостей

Способ устранения

Для устранения затруднения:

1. Убедитесь, что в журналах системных сообщений сервиса `udv-vulnerability-backend` нет ошибок, по команде:

```
journalctl -fu udv-vulnerability-backend.service
```

2. При ошибках в журналах сервисов см. п. «Некорректная инициализация сервисов Комплекса» в разделе «Веб-интерфейс не загружается».

13.2.26.4. Ошибка вида «ПО для сканирования уязвимостей в реестре CPE не обнаружено»

Причина: для ПО, по которому выполнялся поиск уязвимостей, элементы CPE подобраны с недостаточной точностью, либо их не удалось подобрать

Способ устранения

Для устранения затруднения перейдите в раздел «Выгрузка отчета по результатам сопоставления собранного ПО со справочником CPE».

13.2.27. Не устанавливается соединение с сенсором

В качестве причины недоступности сенсора при первом подключении рассмотрены следующие:

- Отключен межсетевой экран `iptables` на сенсоре или Комплексе уровня Management
- Некорректные настройки подключения сенсора

Если сенсор стал недоступен в процессе корректной работы, см. причину «[Ошибки в работе сервисов в период корректной работы иерархии](#)».

Отключен межсетевой экран `iptables` на сенсоре или Комплексе уровня Management



Внимание:

Если сенсор или Комплекс установлены на ОС Альт Сервер, необходимо использовать `iptables` в качестве межсетевого экрана.

Способ устранения

Для устранения затруднения:

1. В командной строке операционной системы сенсора:

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

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



Внимание:

Значение параметра `CONFIG_FW` должно быть `no`.

б. Убедитесь, что межсетевой экран `iptables` запущен:

```
systemctl status iptables
```



Подсказка:

Сервис должен быть в состоянии `active`.

в. При необходимости выполните настройки `iptables` сенсора и запустите `iptables` согласно инструкциям в следующих разделах Руководства по внедрению и поддержке:

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

2. Выполните шаг 1 в командной строке операционной системы Комплекса уровня Management.

Некорректные настройки подключения сенсора

Способ устранения

Для устранения затруднения убедитесь в корректности настроек подключения сенсора к Комплексу уровня Management — для этого вы можете воспользоваться инструкцией «[Подключение сенсора к другому Комплексу уровня Management](#)».

Ошибки в работе сервисов в период корректной работы иерархии

Способ устранения

Если сенсор стал недоступен в процессе корректной работы, ошибки будут отображаться на странице **Сенсоры** веб-интерфейса Комплекса. В таблице ниже приведен список возможных ошибок, причины их возникновения и сервисы, работоспособность которых необходимо проверить.

Табл. 99. Возможные ошибки в процессе работы иерархии

НАИМЕНОВАНИЕ ОШИБКИ	ВОЗМОЖНАЯ ПРИЧИНА	СЕРВИС, ОТВЕЧАЮЩИЙ ЗА РАБОТУ ИЕРАРХИИ
Не удается получить статус	Не поступает информация о состоянии сервисов <code>udv-rabbitmq</code> , <code>udv-rabbitmq-sensor</code> , <code>udv-redis</code> или <code>udv-redis-sensor</code>	Уровень Sensor: <code>udv-node-exporter-sensor</code> <code>udv-pushgateway</code> Уровень Management: <code>udv-node_exporter</code> <code>udv-prometheus</code>
Получение данных недоступно	Затруднения в работе сервиса отправки оперативных данных с сенсора	<code>udv-rabbitmq-sensor</code> (уровень Sensor)
	Затруднения в работе сервиса получения оперативных данных с сенсора на Комплексе	<code>udv-rabbitmq</code> (уровень Management)
Синхронизация настроек недоступна	Затруднения в работе сервиса отправки справочников с Комплекса на сенсор	<code>udv-redis</code> (уровень Management)
	Затруднения в работе сервиса получения справочников на сенсоре	<code>udv-redis-sensor</code> (уровень Sensor)
Не удается установить соединение с сенсором	Совокупность причин, приведенных выше	Все сервисы, приведенные выше

Для устранения затруднения:

1. Просмотрите ошибку на странице **Сенсоры** веб-интерфейса Комплекса.
2. По таблице **выше** определите список сервисов, для которых необходимо просмотреть журнал.
3. Просмотрите журнал выбранного сервиса при помощи команды:

```
journalctl -fu [наименование_сервиса] -n [количество последних строк журнала, которое  
нужно показать]
```

4. При ошибках в журналах сервисов см. п. «**Некорректная инициализация сервисов Комплекса**» в разделе «**Веб-интерфейс не загружается**».

13.3. Восстановление данных из резервных копий

Восстановление данных на текущей версии Комплекса уровня Management возможно только из резервной копии, выполненной для той же версии Комплекса уровня Management.

Восстановление данных рекомендуется выполнять в следующем порядке:

- Резервное копирование данных Комплекса;
- Проверка наличия резервной копии Комплекса;
- Восстановление данных из резервной копии Комплекса.

Комплексы уровня Sensor не хранят данные, поэтому их восстановление из резервной копии заключается в их развертывании с нуля — необходимо только скопировать сохраненные файлы `machine-id` и `sensor.env`, а не создавать новые перед первым запуском.

Для подготовки к восстановлению данных из резервной копии подготовьте архив с резервной копией `dtpk-backup-[version]-[YYYYmmddhhmmss].tar`.



Внимание:

Не рекомендуется использовать резервную копию данных с целью развернуть еще одну копию Комплекса — идентификатор в файле `machine-id` должен быть уникальным на каждом Комплексе, и не допускается наличие двух Комплексов с одинаковыми идентификаторами в одной сети.

13.3.1. Восстановление данных из резервных копий Комплекса уровня Management и Комплекса уровня Management+Sensor

Для восстановления данных из резервных копий Комплекса уровня Management или Комплекса уровня Management+Sensor необходимо выполнить следующие действия:

- Проверка наличия резервной копии Комплекса уровня Management и Комплекса уровня Management+Sensor;
- Восстановление данных из резервной копии Комплекса уровня Management и Комплекса уровня Management+Sensor.

Также, для восстановления данных из резервной копии Комплекса уровня Management необходимо подготовить следующие файлы:

- архив с резервной копией Комплекса;
- индексы событий.

13.3.1.1. Проверка наличия резервной копии Комплекса уровня Management и Комплекса уровня Management+Sensor

Для проверки наличия резервной копии:

1. Войдите в терминал Комплекса под учетной записью `root`.
2. Убедитесь, что резервная копия расположена в директории `/var/backups`. Для этого выполните команду:

```
python3 -m backup_manager --check --file=dtpk-backup-[version]-[YYYYmmddhhmmss].tar  
--password='1234567890'
```

где:

- {version} — версия Комплекса. Например: v.2.2.[минорная версия].[патч-версия]
- {YYYYmmddhhmmss} — дата и время создания архива резервной копии. Например: 20241022151000
- --password — пароль для архива резервной копии.

3. Убедитесь в отсутствии ошибок после окончания проверки резервной копии.

13.3.1.2. Восстановление данных из резервной копии Комплекса уровня Management и Комплекса уровня Management+Sensor



ОСТОРОЖНО:

При восстановлении Комплекса уровня Management уникальный идентификатор `/etc/machine-id` будет заменен на идентификатор из резервной копии. Во избежание проблем убедитесь в следующем:

- если восстановление Комплекса выполняется на другом устройстве, то на предыдущем устройстве в ОС необходимо изменить `machine-id` во избежание наличия в сети двух устройств с одинаковым `machine-id`;
- на ОС отсутствуют приложения, работа которых может быть нарушена в связи с изменением `machine-id`.

Для восстановления данных из резервной копии:

1. Выполните восстановление баз данных из архива:

- а. Войдите в терминал Комплекса под учетной записью `root`.
- б. Убедитесь, что резервная копия расположена в директории `/var/backups`.
- в. Остановите работу всех сервисов Комплекса, кроме `udv-postgresql.service`. Для этого выполните команду:

```
/usr/bin/stop_services.sh
```

2. Выполните восстановление событий:

- а. Остановите работу всех сервисов Комплекса, кроме `udv-postgresql.service`. Для этого выполните команду:

```
/usr/bin/stop_services.sh
```

- б. После остановки работы сервисов выполните команду для восстановления Комплекса из резервной копии:

```
python3 -m backup_manager --restore  
--file=dtpk-backup-[version]-[YYYYmmddhhmmss].tar --password='12345678'
```

где:

- `{version}` — версия Комплекса. Например: `v.2.2.[минорная версия].[патч-версия]`
 - `{YYYYmmddhhmmss}` — дата и время создания архива резервной копии. Например: `20241022151000`
 - `--password` — пароль для архива резервной копии.
- в. Поместите индексы событий в директорию `/var/backups/elasticsearch/uploads`.
 - г. Поместите с заменой файлы `manager.env` и `sensor.env` в директорию `/usr/share/udv/datapk`.
 - д. После успешного восстановления перезагрузите Комплекс, выполнив команду:

```
shutdown -r now
```

► **Результат шага:** перезагрузка Комплекс успешно выполнена.

- е. Войдите в веб-интерфейс Комплекса под учетной записью администратора.
- ж. Перейдите в раздел **События** → **Экспертный режим**.
- з. Нажмите **Create index pattern**.
- и. В поле **Index pattern name** введите `datapk-events-*` и нажмите **Next step**.
- к. В поле **Time field** выберите `create_time` и нажмите **Create index pattern**.
- л. Перейдите в раздел **Администрирование** → **События и инциденты** → **Индексы**.
- м. Нажмите **Восстановить индексы**.

13.3.2. Восстановление данных из резервных копий Комплекса уровня Sensor

Для восстановления данных из резервных копий Комплекса уровня Sensor необходимо выполнить следующие действия:

- Резервное копирование данных Комплекса уровня Sensor;
- Восстановление данных из резервной копии Комплекса уровня Sensor.

13.3.2.1. Резервное копирование данных Комплекса уровня Sensor

Для выполнения резервного копирования данных:

1. Войдите в терминал Комплекса под учетной записью `root`.
2. Сохраните файл `machine-id` в директории `/etc`.
3. Сохраните файл `sensor.env` в директории `/usr/share/udv/datapk`.

13.3.2.2. Восстановление данных из резервной копии Комплекса уровня Sensor

Для восстановления данных из резервной копии:

1. Выполните развертывание Комплекса уровня Sensor в соответствии с разделом «[Установка Комплекса уровня Sensor](#)».
2. Замените файл `/etc/machine-id` на файл, сохраненный при резервном копировании.
3. Замените файл `/usr/share/udv/datapk/sensor.env` на файл, сохраненный при резервном копировании.
4. Перезагрузите Комплекс, выполнив команду:

```
shutdown -r now
```

5. Войдите в веб-интерфейс Комплекса уровня Management, к которому подключен данный Комплекс уровня Sensor.
6. Перейдите в раздел Сенсоры и убедитесь, что Комплекс уровня Sensor успешно подключился к Комплексу уровня Management.

13.4. Действия в случаях несанкционированного доступа к данным

После обнаружения нелегитимных действий со стороны пользователя администратор может воспользоваться следующими возможностями по блокировке пользователей:

- Просмотр журнала действий пользователей Комплекса
- Изменение статуса активности учетной записи пользователя Комплекса

13.4.1. Просмотр журнала действий пользователей Комплекса

Все действия пользователей Комплекса журналируются. При установлении фактов попыток несанкционированных действий пользователей их работа в веб-интерфейсе Комплекса блокируется. Дальнейшая работа пользователя с Комплексом возможна только после расследования администратора комплекса по выявлению причин возникновения аварийной ситуации.

Для самостоятельного установления или подтверждения фактов несанкционированного доступа администратор может обратиться к журналу действий пользователей. Для просмотра журнала действий пользователей Комплекса:

1. Перейдите на страницу **События**.
2. Настройте фильтрацию событий по значениям `user_action_detected` или `appliance_authentication` поля **Тип**.
3. Нажмите кнопку **Сохранить** для применения фильтра.
4. В «быстром» фильтре **Дата создания** выберите временной интервал, за который необходимо получить события действий пользователей.
5. Проанализируйте полученные события на предмет несанкционированного доступа.

13.4.2. Изменение статуса активности учетной записи пользователя Комплекса

Чтобы изменить статус активности учетной записи пользователя Комплекса:

1. Перейдите на страницу **Администрирование** → **Пользователи**.
2. Выберите учетную запись в списке и нажмите  (**Редактировать учетную запись**).
3. В зависимости от желаемого действия:
 - установите чекбокс **УЗ пользователя активна**, чтобы активировать (разблокировать) доступ пользователя к веб-интерфейсу Комплекса;
 - отмените установку чекбокса **УЗ пользователя активна** для учетной записи, чтобы заблокировать пользователю доступ к веб-интерфейсу Комплекса.
4. Сохраните изменения.
 - **Результат шага:** после подтверждения активность учетной записи пользователя будет изменена.

13.5. Действия в других аварийных ситуациях

Действия в экстремальных условиях осуществляются по правилам, принятым в эксплуатирующей организации.

Аварийные ситуации, связанные с некорректным функционированием Комплекса в сетевой инфраструктуре ИС, устраняются путем проверки и исправлений настроек сети управляющего контура комплекса и локальных настроек Комплекса.

13.6. Диагностика сервиса сбора данных по протоколам SSH, Telnet, WinRM, winexe



Внимание:

Данная инструкция актуальна для следующих сервисов и портов:

- `udv-msrpc`, порт `10008`;
- `udv-plc-connector`, порт `10206`;
- `udv-opc-connector`, порт `10205`;
- `udv-terminal-connector`, порт `10208`;
- `udv-modbus-connector`, порт `10203`;
- `udv-sql-connector`, порт `10202`;
- `udv-snmp-connector`, порт `10204`;

Для расследования причин появления ошибок сбора данных по протоколам SSH, Telnet, WinRM, winexe:

1. Подключитесь к операционной системе Комплекса.
2. Просмотрите текущее состояние журналирования сервиса, выполнив команду:

```
curl http://[IP_адрес_сервиса]:[порт_сервиса]/log/level
```

Пример

Сервис имеет состояние NOTSET. Это значит, что уровень журналирования для этого сервиса не задан.

```
"msrpc.cancellable_pool":"NOTSET", "msrpc":"NOTSET", "im_lib":"NOTSET",
```

Рис. 299. Состояние «NOTSET» журналирования сервиса «msrpc»

3. Измените уровень журналирования сервиса, выполнив команду:

```
curl -X POST
"http://[IP_адрес_сервиса]:[порт_сервиса]/log/level?logger_name=[название_сервиса/название_пакета_в_сервисе]&log_level=[уровень_журналирования]"
```

где:

- `[IP_адрес_сервиса]` — IP-адрес необходимого сервиса;
- `[порт_сервиса]` — порт необходимого сервиса;
- `[название_сервиса/название_пакета_в_сервисе]` — имя необходимого сервиса или пакета в сервисе;
- `[уровень_журналирования]` — требуемый уровень журналирования сервиса (INFO или DEBUG).



Внимание:

На данном шаге название сервиса вводится через нижнее подчеркивание, без добавления приставки `udv-` (например, `udv-terminal-connector.service` → `terminal_connector`)

4. Проверьте установленный уровень журналирования сервиса, выполнив команду:

```
curl http://[IP_адрес_сервиса]:[порт_сервиса]/log/level
```

Пример

Сервис имеет состояние **DEBUG**

```
"msrpc.cancellable_pool":"NOTSET","msrpc":"DEBUG","im_lib":"NOTSET",
```

Рис. 300. Состояние «DEBUG» журналирования сервиса «msrpc»

5. Посмотрите журнал сервиса при помощи команды:

```
journalctl -fu [полное_название_сервиса].service -n [количество последних строк журнала, которое нужно показать]
```

► **Результат шага:** Отображается указанное количество последних строк журнала сервиса.

```
[root@DATAKTESTTK22 ~]# journalctl -fu udv-msrpc.service -n 5
Oct 24 18:14:01 DATAKTESTTK22 python3[366771]: File "/usr/lib/python3/site-packages/im_lib/dcerpc/v5/dcomrt.py", line 1337, in request
Oct 24 18:14:01 DATAKTESTTK22 python3[366771]:     resp = dce.request(req, uuid)
Oct 24 18:14:01 DATAKTESTTK22 python3[366771]: File "/usr/lib/python3/site-packages/im_lib/dcerpc/v5/rpcrt.py", line 880, in request
Oct 24 18:14:01 DATAKTESTTK22 python3[366771]:     raise exception
Oct 24 18:14:01 DATAKTESTTK22 python3[366771]: im_lib.dcerpc.v5.dcom.wmi.DCERPCSessionError: WMI Session Error: code: 0x80041006 - WBEM_E_OUT_OF_MEMORY
```

Рис. 301. Отображение последних пять строк журнала сервиса «udv-msrpc»