RT Protect EDR

Руководство администратора

Версия 1.0.33 от 29 июня 2026
Разработано компанией АО «РТ-ИБ»

RT Protect

Оглавление

1. Общие положения 8
1.1 Идентификация документа 8
1.2 Аннотация документа 8
1.3 Термины и определения 9
1.4 Условные обозначения 12
2. Общие сведения 14
2.1 Назначение и архитектура Программы 14
2.2 Функциональные возможности 15
3. Организационно-распорядительные меры 17
3.1 Общие сведения 17
3.2 Комплектность поставки 17
3.2.1. Процедуры и меры безопасности при распространении Программы к месту назначения 18
4. Структура Программы 19
4.1 Общие сведения 19
4.2 Архитектура агента Windows 20
4.2.1. Функции системы со стороны клиентской части 21
4.3 Архитектура агента Linux 21
4.4 Архитектура серверной части 22
4.4.1. Общие сведения 22
4.4.2. Функции системы со стороны серверной части 24
5. Настройка Программы 25
5.1 Требования к среде функционирования 25
5.2 Установка и удаление 28
5.2.1. Установка агента Windows 28
5.2.2. Установка агента Linux 33
5.2.3. Точка восстановления ОС, созданная при установке агента 51

5.2.4. Идентификация агента ... 52
5.2.5. Удаление агента Windows ... 52
5.2.6. Удаление агента Linux ... 53
5.2.7. Установка сервера ... 53
5.3 Особенности работы Программы с антивирусными средствами сторонних производителей ... 54
5.3.1. Срабатывание антивирусных средств при работе с веб-приложением RT Protect EDR ... 54
6. Ролевая модель ... 57
6.1 Общая информация ... 57
6.2 Основные роли ... 57
6.3 Роль «Администратор безопасности» ... 58
6.3.1. Назначение роли ... 58
6.3.2. Основные задачи администратора безопасности ... 58
6.3.3. Права роли по разделам ... 59
6.3.4. Отличие от роли «Администратор» ... 60
6.4 Роль «Администратор» ... 60
6.5 Назначение роли ... 60
6.5.1. Основные задачи администратора ... 61
6.5.2. Права роли по разделам ... 61
6.5.3. Ограничения роли ... 62
6.6 Роль «Аналитик L1» ... 62
6.6.1. Назначение роли ... 62
6.6.2. Основные задачи аналитика первой линии ... 63
6.6.3. Права роли по разделам ... 63
6.6.4. Ограничения роли ... 64
6.7 Роль «Аналитик L2» ... 65
6.7.1. Назначение роли ... 65
6.7.2. Основные задачи аналитика второй линии ... 65
6.7.3. Права роли по разделам ... 66

6.7.4. Отличие от роли «Аналитик первой линии» 67
6.7.5. Ограничения роли 67
6.8 Роль «Аналитик L3» 67
6.8.1. Назначение роли 67
6.8.2. Основные задачи аналитика третьей линии 68
6.8.3. Права роли по разделам 68
6.8.4. Отличие от роли «Аналитик второй линии» 69
6.8.5. Ограничения роли 69
6.9 Роль «Наблюдатель» 70
6.10 Роль «Оператор поиска угроз» 70
6.11 Роль с доступом к терминалу реагирования и файлам агентов 71
6.12 Права, предоставляемые пользователям 71
7. Модель данных в RT Protect EDR 78
7.1 Общие сведения 78
7.2 События мониторинга сети 92
7.3 События мониторинга файловых операций 95
7.4 События монитора реестра 101
7.5 События журналов 102
7.6 События мониторинга процессов 104
7.7 События мониторинга системы 107
7.8 События пользовательских сессий 109
7.9 События монитора вызовов 111
7.10 События модуля Антишифра 112
7.11 События модуля контроля USB 113
7.12 События статистики 114
7.13 Телеметрия RT Protect EDR 117
8. Интерфейс Программы 120
8.1 Окно авторизации и общие сведения 120

8.2 Горизонтальная панель управления 122
8.2.1. Онлайн-терминал 123
8.2.2. Оповещения 123
8.2.3. Меню «Пользователь» 127
8.3 Главная страница 129
8.4 События 131
8.4.1. Инциденты 132
8.4.2. Активность 144
8.4.3. Проверка с помощью TI-платформы 157
8.4.4. Процессы 159
8.4.5. Обзор событий 171
8.4.6. Артефакты TI 172
8.5 Агенты 173
8.5.1. Агенты 174
8.5.2. Агент 192
8.5.3. Группы 205
8.5.4. Конфигурации 206
8.5.5. Верификация 207
8.5.6. Терминал 210
8.5.7. Планировщик задач 222
8.5.8. Графики 237
8.5.9. Хранилище 239
8.5.10. Уязвимости 247
8.6 Аналитика 251
8.6.1. Индикаторы атак 252
8.6.2. Индикаторы компрометации 260
8.6.3. YARA-правила (файлы) 268
8.6.4. YARA-правила (память) 272

8.6.5. Журналы 275
8.7 Исключения 279
8.7.1. Исключения для программ 279
8.7.2. Исключения для файлов 284
8.7.3. Сетевые исключения 289
8.7.4. Исключения индикаторов атак 293
8.8 Профили 295
8.8.1. Профиль Антишифра 296
8.8.2. Профили безопасности агента 304
8.8.3. Профили контроля USB 322
8.9 Параметры 328
8.9.1. Пользователи и роли 328
8.9.2. Журнал безопасности 337
8.9.3. Дистрибутивы 342
8.9.4. Лицензирование 343
8.9.1. Интеграции 347
8.9.2. Настройки 372
9. Машинное обучение в Программе 373
9.1 Классификация на сервере 373
9.2 Классификация на агенте 375
9.3 Список компонентов, используемых в модели ИИ 377
10. Проверка Программы 379
10.1 Проверка доступности агента 379
10.2 Контроль целостности исполняемых файлов и файлов конфигурации 379
11. Сообщения администратору 380
11.1 Общие сведения 380
11.2 Сообщения об ошибках 380
11.2.1. Общие сообщения 380

11.2.2. Специфичные сообщения....381
12. Процедура обновления программного обеспечения....392
12.1 Общие сведения....392
12.2 Обновление агента....394
12.3 Оповещение покупателя об обновлении....394
12.4 Доставка и контроль целостности обновления программного обеспечения на стороне покупателя....395
13. Действия после сбоя и ошибки....396
13.1 Общие сведения....396
13.2 Инструкция по удалению агента в случае блокировки ОС....396
13.3 Установка и применение обновления программного обеспечения....397
13.4 Контроль установки обновления....397
14. Перечень сокращений....398
15. Заключение....400

1. Общие положения

1.1 Идентификация документа

Данное руководство кратко можно идентифицировать согласно таблице 1.

Таблица 1 – Идентификация документа

Название документа	«RT Protect EDR» Руководство Администратора
Версия документа	Версия 1.0.33 (актуально для версии агента 4.0.0.4000, версии сервера 4.0 (фронтенд 3.1.3, бэкенд 1.27.1-19-g790aba84)
Идентификация программы	«RT Protect EDR»
Идентификация разработчика	АО «РТ-ИБ»
Уровень доверия	Оценочный уровень доверия 4 (ОУД4) «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий, утвержденным приказом ФСТЭК России от 2 июня 2020 г. № 76 (зарегистрирован Минюстом России 11 сентября 2020 г., регистрационный № 59772) (с изменениями, внесенными приказом ФСТЭК России от 18 апреля 2022 г. № 68 (зарегистрирован Минюстом России 20 июля 2022 г., регистрационный № 69318).)»
Требования по безопасности	«Требования по безопасности информации к средствам обнаружения и реагирования на уровне узла, утвержденные приказом ФСТЭК России от 26 февраля 2025 № 58»

1.2 Аннотация документа

Документ предназначен для ознакомления пользователей сервера управления с ролями администратор и администратор безопасности с технической информацией о программе «RT Protect EDR» (далее по тексту Программа) и содержит общие сведения о Программе, организационно-распорядительные меры, сведения о структуре, описание настроек Программы и тексты сообщений, выдаваемых в ходе выполнения настройки, проверки, а также о процессе функционирования Программы.

1.3 Термины и определения

В настоящем документе используются термины и определения согласно ГОСТ Р ИСО/МЭК 15408 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий» и ГОСТ Р ИСО/МЭК 12207-2010 «Информационная технология. Системная и программная инженерия. Процессы жизненного цикла программных средств» согласно таблице 2.

Таблица 2 – Термины и определения

Термин	Описание
Администратор	Уполномоченный пользователь, ответственный за установку, администрирование и эксплуатацию программы
Верификация	Проверка и подтверждение подлинности ПО
Дерево процесса	Графическое отображение взаимосвязи процесса-родителя и дочернего процесса
Демон	Программа в UNIX-системах, запускаемая самой системой и работающая в фоновом режиме без прямого взаимодействия с пользователем
Домен	Символьное обозначение для определенной области вычислительной сети
Задание по безопасности	Совокупность требований безопасности и спецификаций, предназначенная для использования в качестве основы для оценки конкретной программы
Индикаторы атак	Правила, с помощью которых анализируется динамическая активность в защищаемой ИТ-инфраструктуре на наличие атак
Индикаторы компрометации	Правила, с помощью которых в программе отслеживается объект (или активность), который с большой долей вероятности указывает на несанкционированный доступ к системе (то есть ее компрометацию)
Инстанцирование	Создание экземпляра класса в программировании. Экземпляр класса – это описание конкретного объекта в памяти
Исполняемый модуль процесса	Набор инструкций, загружаемый в виде исполняемого файла или dll в процесс
Нити (Threads)	Наименьшая единица обработки, исполнение которой может быть назначено ядром операционной системы. Нити исполняются внутри процесса
Оверлей	Метод программирования, позволяющий создавать программы, требующие меньше оперативной памяти. Метод заключается в разделении программы на исполняемые блоки, которые поочерёдно записываются в одну область памяти поверх предыдущих, выполняют свои функции и перезаписываются следующими
Пагинация	Структурирование большого объема информации на сайте, путем ее разделения на отдельные страницы, иными словами – постраничный вывод данных
Политика безопасности	Совокупность правил, регулирующих управление, защиту и распределение информационных ресурсов, контролируемых программой
Профиль защиты	Совокупность требований безопасности для программы
Процесс	В простейших терминах – это исполняемая в операционной системе программа, активный объект ОС, а иначе последовательность инструкций, исполняемых в ОС предопределенным образом. В данном случае такими инструкциями будет программный код. Программа будет называться процессом в том случае, если загружается в память вместе со всеми ресурсами, которые необходимы для ее работы

Термин	Описание
Разработчик	АО «РТ-ИБ»
Токен	Токен представляет собой случайную строку, с произвольным набором символов, которая служит ключом для верификации агента на сервере программы. Токен уникален для каждого агента
Угроза безопасности информации	Совокупность условий и факторов, определяющих потенциальную или реально существующую опасность нарушения безопасности информации
Файловые сигнатуры	Данные, используемые для идентификации или проверки содержимого файла
Функции безопасности программы	Совокупность всех функций безопасности программы, направленных на осуществление политики безопасности (ПБ)
Хеширование	Преобразование, производимое хеш-функцией
Хост	Электронно-вычислительная машина, являющаяся конечной точкой вычислительной сети. В узком смысле хост – это любое устройство, предоставляющее сервисы формата «клиент-сервер» в режиме сервера по каким-либо интерфейсам и уникально определённое на этих интерфейсах
Эвристический анализ	Совокупность функций антивируса, нацеленных на обнаружение неизвестных вирусным базам вредоносных программ. Термин обозначает и один из конкретных способов
Энтропия	Статистический параметр, который показывает вероятность встречаемости определённых байтов в файле
Active Directory	Иерархически организованное хранилище данных об объектах сети, обеспечивающее удобные средства для поиска и использования этих данных. Компьютер, на котором работает Active Directory, называется контроллером домена. С Active Directory связаны практически все административные задачи
Alerts	Оповещение об атаке на защищаемую инфраструктуру
Ansible	Система управления конфигурациями, написанная на языке программирования Python, с использованием декларативного языка разметки для описания конфигураций. Применяется для автоматизации настройки и развёртывания программного обеспечения
APT-атака	Термин кибербезопасности, означающий действия злоумышленника, обладающего современным уровнем специальных знаний и значительными ресурсами, которые позволяют ему создавать угрозу опасных кибератак
Backend	Программно-аппаратная часть сервиса, отвечающая за функционирование его внутренней части
Code Signing	Цифровая подпись кода – электронный сертификат, полученный от удостоверяющего центра, подтверждающий безопасность программы
Deb	Расширение имён файлов «бинарных» пакетов для распространения и установки программного обеспечения в операционной системе проекта Debian, и других, использующих систему управления пакетами dpkg
Desktop.ini	Файл конфигурации, который содержит данные настроек внешнего вида системной папки в ОС Microsoft Windows: значок, цвет текста, фоновый рисунок и т. д.
DNS	Компьютерная распределённая система для получения информации о доменах
Docker	Программное обеспечение для автоматизации развёртывания и управления приложениями в средах с поддержкой контейнеризации, контейнеризатор приложений

Термин	Описание
Elasticsearch	Тиражируемая свободная программная поисковая система
Endpoint	Конечная точка сетевой связи, узел сети
Enum	Перечисляемый тип данных, чьё множество значений представляет собой ограниченный список идентификаторов
ETW	(Event Tracing for Windows) – это системный компонент ОС Windows, который используется для диагностики, отладки и исследования производительности тех или иных частей ОС, а также приложений
Frontend	Клиентская сторона пользовательского интерфейса к программно-аппаратной части сервиса
Golden ticket	Атака, заключающаяся в получении TGT-билета, который позволяет в свою очередь неограниченно выдавать билеты, что дает возможность злоумышленнику получить доступ ко всему домену
HTTPS	Расширение протокола HTTP для поддержки шифрования в целях повышения безопасности
Imphash	Хеш импортируемых библиотек
Informational alerts	Оповещения о событиях, прямо не угрожающих безопасности инфраструктуры
Int	Целочисленный тип данных, один из простейших и самых распространённых типов данных в языках программирования. Служит для представления целых чисел
Int64	Int64 является неизменяемым типом данных, представляющим собой целые числа со знаком в диапазоне от отрицательного значения -9223372036854775808 (Int64.MinValue) до положительного значения 9 223 372 036 854 775 807 (Int64.MaxValue)
JSON	Текстовый формат обмена данными, основанный на JavaScript
JSON-объект	Неупорядоченный набор пар ключ/значение. Объект начинается с открывающей фигурной скобки { и заканчивается закрывающей фигурной скобкой }. Каждое имя сопровождается двоеточием, пары ключ/значение разделяются запятой
Kerberos	Сетевой протокол аутентификации, который предлагает механизм взаимной аутентификации клиента и сервера перед установлением связи между ними, причём в протоколе учтён тот факт, что начальный обмен информацией между клиентом и сервером происходит в незащищенной среде, а передаваемые пакеты могут быть перехвачены и модифицированы
Linux	Семейство Unix-подобных операционных систем на базе ядра Linux
Malware Bazaar	Проект сайта abuse.ch, целью которого является обмен образцами вредоносного ПО с сообществом информационной безопасности, поставщиками антивирусных программ и поставщиками информации об угрозах
MD5	128-битный алгоритм хеширования
NTFS	Стандартная файловая система для семейства операционных систем Windows NT фирмы Microsoft. NTFS поддерживает хранение метаданных
Powershell	Утилита для запуска инфраструктуры управления конфигурацией и автоматизации задач Microsoft. Инфраструктура Powershell состоит из оболочки командной строки и связанного языка сценариев
SSDEEP	Алгоритм нечеткого хеширования

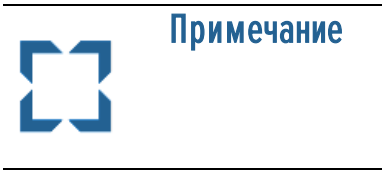
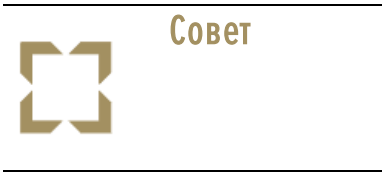
Термин	Описание
TCP	Один из основных протоколов передачи данных интернета. Предназначен для управления передачей данных интернета. Пакеты в TCP называются сегментами. В стеке протоколов TCP/IP выполняет функции транспортного уровня модели OSI
TLSH	Вероятностный алгоритм хеширования
Ubuntu	Дистрибутив GNU/Linux, основанный на Debian GNU/Linux
Unsigned	Модификатор целочисленного типа данных, который показывает, что значение не может быть отрицательным
UTC	Всемирное координированное время – стандарт, по которому общество регулирует часы и время. Отличается на целое количество секунд от атомного времени и на дробное количество секунд от всемирного времени UT1
UUID	Стандарт идентификации, используемый в создании программного обеспечения, стандартизированный Open Software Foundation (OSF) как часть DCE – среды распределённых вычислений. Основное назначение UUID – это позволить распределённым системам уникально идентифицировать информацию без центра координации
VirusTotal	Бесплатная служба, осуществляющая анализ подозрительных файлов и ссылок (URL) на предмет выявления вирусов, червей, троянов и всевозможных вредоносных программ
Web-сервер	Сервер, принимающий HTTP-запросы от клиентов, чаще всего веб-браузеров, и выдающий HTTP-ответы, как правило, вместе с HTML-страницей, изображением, файлом, медиа-потоком или другими данными
WHOIS	Сетевой протокол прикладного уровня, базирующийся на протоколе TCP. Основное применение – получение регистрационных данных о владельцах доменных имён, IP-адресов и автономных систем
Windows	Группа семейств коммерческих операционных систем корпорации Microsoft, ориентированных на управление с помощью графического интерфейса
WMI	Инструментарий управления Windows. Одна из базовых технологий для централизованного управления и слежения за работой различных частей компьютерной инфраструктуры под управлением платформы Windows

1.4 Условные обозначения

Условные обозначения, применяемые в документе, представлены в таблице 3.

Таблица 3 – Условные обозначения

Обозначение	Описание
ПРОПИСНЫЕ БУКВЫ	Акронимы, аббревиатуры
«Times New Roman»	Названия документов, команд, каталогов, файлов и т.д.
Жирный шрифт	Подписи таблиц, рисунков, названия разделов, подразделов, пунктов и подпунктов, название кнопок меню модуля администрирования Программы
	Обозначения кнопок меню, операций модуля администрирования Программы

Times New Roman/Times New Roman	Перечисление альтернативных вариантов, путь меню, путь файла
	Информация, требующая внимания пользователя
	Информация, связанная с важными конфигурационными настройками и особенностями работы EDR
	Рекомендации и предположения, которые могут помочь в работе с EDR

2. Общие сведения

2.1 Назначение и архитектура Программы

RT Protect EDR – это система для обнаружения целенаправленных атак на конечных устройствах. Она обеспечивает быстрое обнаружение вторжений, эффективное автоматическое противодействие, наглядную визуализацию событий и инцидентов, а также сбор цифровых улик и тщательное расследование инцидентов и поиск аномальной активности.

Программа генерирует предупреждения для проведения расследований сотрудниками информационной безопасности на основе данных, поступивших от конечных систем (хостов) в защищаемой вычислительной сети. В результате расследования сотрудник, проводящий экспертную оценку события, может определить, является ли событие несущим угрозу или нет, и предпринять соответствующие действия.

RT Protect EDR имеет клиент-серверную архитектуру.

Клиентская часть Программы функционирует под управлением ОС Windows версий 7, 8, 8.1, 10, 11, Windows Server 2008 R2 и выше, ОС Linux различных версий. Клиент устанавливается на отдельные устройства защищаемой IT-инфраструктуры (далее агент).

Серверная часть Программы функционирует под управлением ОС Linux Ubuntu 20.04.5 LTS или Astra Linux 1.8 на сервере предприятия-изготовителя. В таком случае Заказчику предоставляется доступ к серверному компоненту и его инструментам как услуга.



Примечание

Программа может поставляться в составе отдельного аппаратно-программного комплекса, разворачиваемого на территории Заказчика.

Программа предназначена для обработки информации, не являющейся секретной.

Решение имеет механизм самозащиты от вредоносных действий (выполнение пользователями/другими приложениями действий, которые могут нарушить работоспособность решения) за счет:

— защиты собственных файлов и директорий (предотвращение изменения и удаления файлов программы на жестком диске);

— защиты собственных конфигурационных данных в реестре (предотвращение изменения и удаления записей в системном реестре);

— защиты собственных процессов (предотвращение изменения процессов в памяти);

— защиты от внешнего управления (блокировка попыток управления службами программы и ее настройками с удаленного компьютера).

Программа имеет многофункциональный пользовательский интерфейс и подразумевает наличие следующих ролей пользователя:

Администратор безопасности – выполняет установку и корректную настройку Программы в соответствии с настоящим руководством, а также отвечает за обновление программных компонентов EDR;

Администратор – пользователь, ответственный за анализ поступающих от Программы данных. Принимает решения по дальнейшей реакции на обнаруженные угрозы;

Пользователь – сотрудник, выполняющий работу на персональном компьютере, на котором установлен модуль агента. Пользователь не взаимодействует с Программой напрямую, ему доступны только оповещения в области уведомления панели задач ОС о состоянии защищаемой машины.

2.2 Функциональные возможности

Программа обеспечивает следующие функциональные возможности:

— сбор информации о сетевом трафике, проходящем через контролируемые узлы ИС;

— сбор информации о событиях, регистрируемых в журналах аудита операционной системы (ОС), прикладного ПО;

— сбор информации о вызове функций и обращении к ресурсам системы;

— выполнение анализа собранных данных о сетевом трафике в режиме, близком к реальному времени, и по результатам анализа фиксация информации о дате и времени, результате анализа, идентификаторе источника данных, протоколе, используемом для проведения вторжения;

— обнаружение вторжения по отношению к контролируемым узлам ИС в режиме, близком к реальному времени, на уровне отдельных узлов;

— анализ собранных данных для обнаружения компьютерных вторжений с использованием сигнатурного и эвристических методов;

— анализ собранных данных с целью обнаружения вторжений с использованием эвристических методов, основанных на методах выявления аномалий сетевого трафика и аномалий в действиях пользователя ИС, на заданном уровне эвристического анализа;

— фиксация факта обнаружения вторжений или нарушений безопасности в журналах аудита;

— уведомление администратора Программы об обнаруженных вторжениях и нарушениях безопасности с помощью отображения карточки события в консоли управления;

— обнаружение вторжений на основе анализа служебной информации протоколов сетевого уровня, базовой эталонной модели взаимосвязи открытых систем;

— автоматизированное обновление базы решающих правил;

— наличие интерфейса администрирования;

— возможность уполномоченным администраторам (ролям) управлять режимом выполнения функций безопасности Программы;

— возможность уполномоченным администраторам (ролям) управлять данными Программы, используемыми функциями безопасности;

— поддержка определенных ролей для Программы и их ассоциация с конкретными администраторами и пользователями ИС;

— управление данными функций безопасности Программы в части установления и контроля ограничений на эти данные;

— тестирование (самотестирование) функций безопасности Программы;

— генерация записей аудита для событий, потенциально подвергаемых аудиту;

— возможность чтения информации из записей аудита;

— ассоциация каждого события аудита с идентификатором субъекта, его инициировавшего;

— ограничение доступа к чтению записей аудита;

— поиск, сортировка, упорядочение данных аудита.

3. Организационно-распорядительные меры

3.1 Общие сведения

Программа поставляется Заказчику на основании договора о поставке, заключенного между заказчиком и правообладателем.

Сведения о порядке предоставления Программы, ее обновлении, гарантийных обязательствах, и порядке направления рекламаций от потребителя описаны в документе «Формуляр».

Программа и документация на нее хранятся на сервере предприятия-изготовителя.

Поставка возможна в двух вариантах.

Программа поставляется Заказчику согласно комплектности поставки.

3.2 Комплектность поставки

Комплектность поставки для каждого варианта представлена в таблице 4 и таблице 5 .

Таблица 4 – Комплектность поставки (вариант 1)

Обозначение	Наименование	Кол.	Примечание
-01	«RT Protect EDR» Модуль агента	1	Поставляется по сети (пакет-установщик)
	«RT Protect EDR» Модуль администрирования с консолью на сервере*	1	Доступ к модулю как услуга
-01 30 01	«RT Protect EDR» Формуляр	1	Поставляется в печатном виде (формат А4)
-20 01	«RT Protect EDR» Комплект эксплуатационных документов согласно ведомости ЭД	1	Поставляется по сети

*Не входит в комплект поставки. Разворачивается на сервере предприятия-изготовителя ПО.

Таблица 5 – Комплектность поставки (вариант 2)

Обозначение	Наименование	Кол.	Примечание
-01	«RT Protect EDR » Модуль агента	1	Поставляется по сети (пакет msi)
	«RT Protect EDR» Модуль администрирования с консолью на сервере	1	Разворачивается на сервере предприятия Заказчика
-01 30 01	«RT Protect EDR» Формуляр	1	Поставляется в печатном виде (формат А4)
-01 20 01	«RT Protect EDR» Комплект эксплуатационных документов согласно ведомости ЭД	1	Поставляется по сети

3.2.1. Процедуры и меры безопасности при распространении Программы к месту назначения

Процедуры и меры безопасности при распространении Программы к месту назначения решают следующие задачи:

— обеспечивают идентификацию и целостность Программы во время пересылки;

— обеспечивают обнаружение несанкционированных модификаций Программы;

— препятствуют попыткам подмены Программы от имени разработчика.

4. Структура Программы

4.1 Общие сведения

Программа имеет клиент-серверную архитектуру.

Клиентская часть системы – это системный агент поведенческого анализа, который работает на конечном компьютере пользователя (endpoint) в следующих ОС:

– Microsoft Windows 7 и выше (разрядность: 64-бита и 32-бита);

– Microsoft Windows Server 2008 R2 и выше;

– Linux Ubuntu 18.04;

– Linux Ubuntu 20.04;

– Linux Ubuntu 22.04;

– Linux Ubuntu 24.04;

– Debian 11;

– Debian 12;

– Debian 13;

– Astra Linux SE 1.6;

– Astra Linux SE 1.7;

– Astra Linux 1.8;

– Red OS 7.3;

– ALT Linux 10;

– CentOS.

Агент спроектирован таким образом, чтобы принимать от сервера правила анализа и другую информацию, необходимую для выявления и реагирования на угрозы.

Агент вводит объектную модель и интерфейс взаимодействия с ней по сети, который предоставляется в распоряжение сервера и посредством которого сервер может передавать на конечные компьютеры правила поведенческого анализа, ставить на контроль определенные точки системы, задавать реакцию на определенные события, а также получать статистику системной активности конечного компьютера, собирать,

обобщать и при необходимости предоставлять администратору (аналитику) возможность динамически ее отслеживать.

Технически, клиент представляет собой программное средство, устанавливаемое на компьютере конечного пользователя с целью выявления и борьбы с вредоносным ПО и возможными атаками на этот компьютер.

Взаимодействие с сервером происходит по протоколу HTTPS.

4.2 Архитектура агента Windows

Архитектура агента системы предполагает наличие следующих основных функциональных компонентов:

– драйвер, работающий в режиме ядра системы;

– драйвер контроля USB;

– служба, работающая в режиме пользователя;

– системный трей (опционально).

Схематично архитектура агента представлена на рисунке 1.

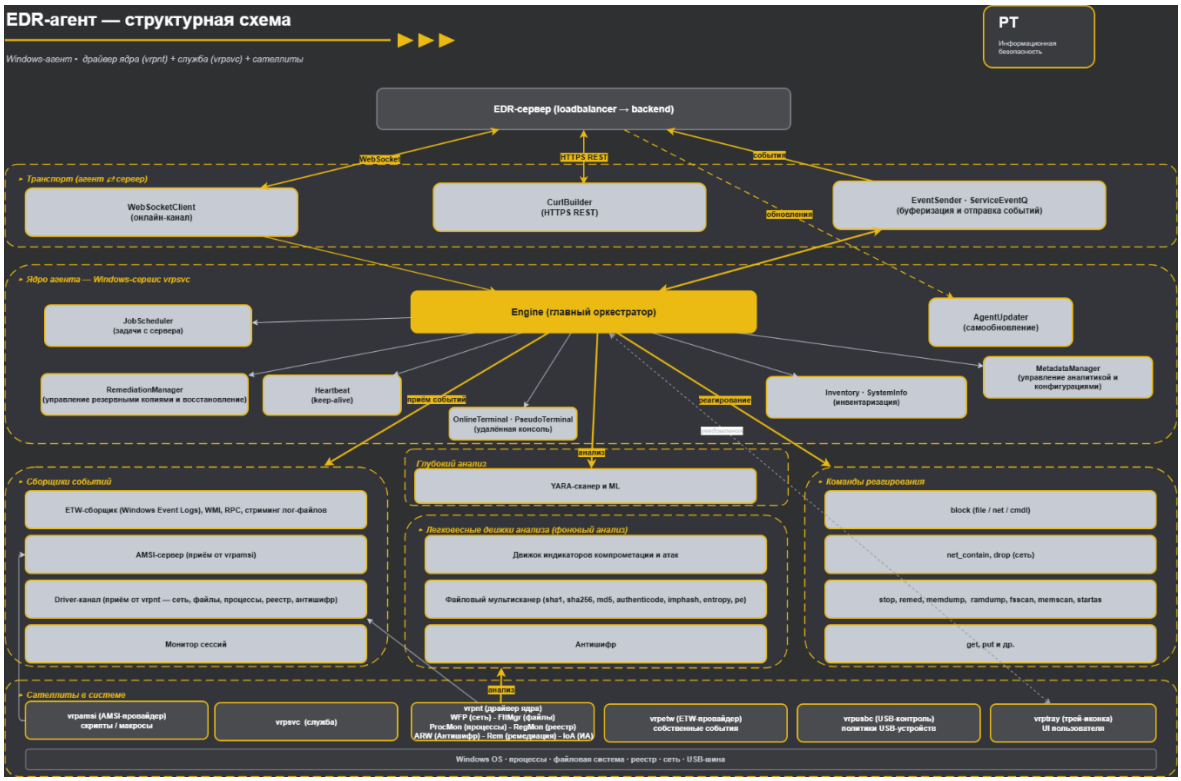


Рисунок 1 – Архитектура агента Windows

4.2.1. Функции системы со стороны клиентской части

Клиент осуществляет мониторинг системной активности с целью выявления вредоносного поведения согласно правилам поведенческого анализа, полученным им от сервера. Клиент собирает статистику системной активности и периодически отправляет ее на сервер.

4.3 Архитектура агента Linux

Агент Linux состоит из следующих компонентов:

1) Демон – читает конфигурационный файл и запускает BPF-программу или модуль ядра;
2) Конфигурационный файл работы агента – определяет особенности работы Linux-агента;
3) Профиль поведения агента – настройки сервера (пароль, предпочитаемый режим работы, признак сетевой изоляции и др.);
4) Файлы конфигураций – используются для управления настройками безопасности, позволяют задавать правила работы агента;
5) BPF-программа – набор BPF-программ, загружаемый в ядро ОС по инициативе сервиса, выполняет передачу событий и защитные функции агента в режиме eBPF;
6) Модуль ядра – загружается в ядро ОС по инициативе сервиса, выполняет защитные функции агента и отправляет на сервер события ОС в режиме ядра;
7) Модуль получения смещений символов ядра – компонент отвечает за нахождение адресов, требуемых символов ядра ОС (может использовать BTF);
8) Файл смещения структур, необходимых для работы модуля eBPF – в файле содержатся адреса символов ядра, полученных при установке агента.

Схематично архитектура агента Linux представлена на рисунке 2.

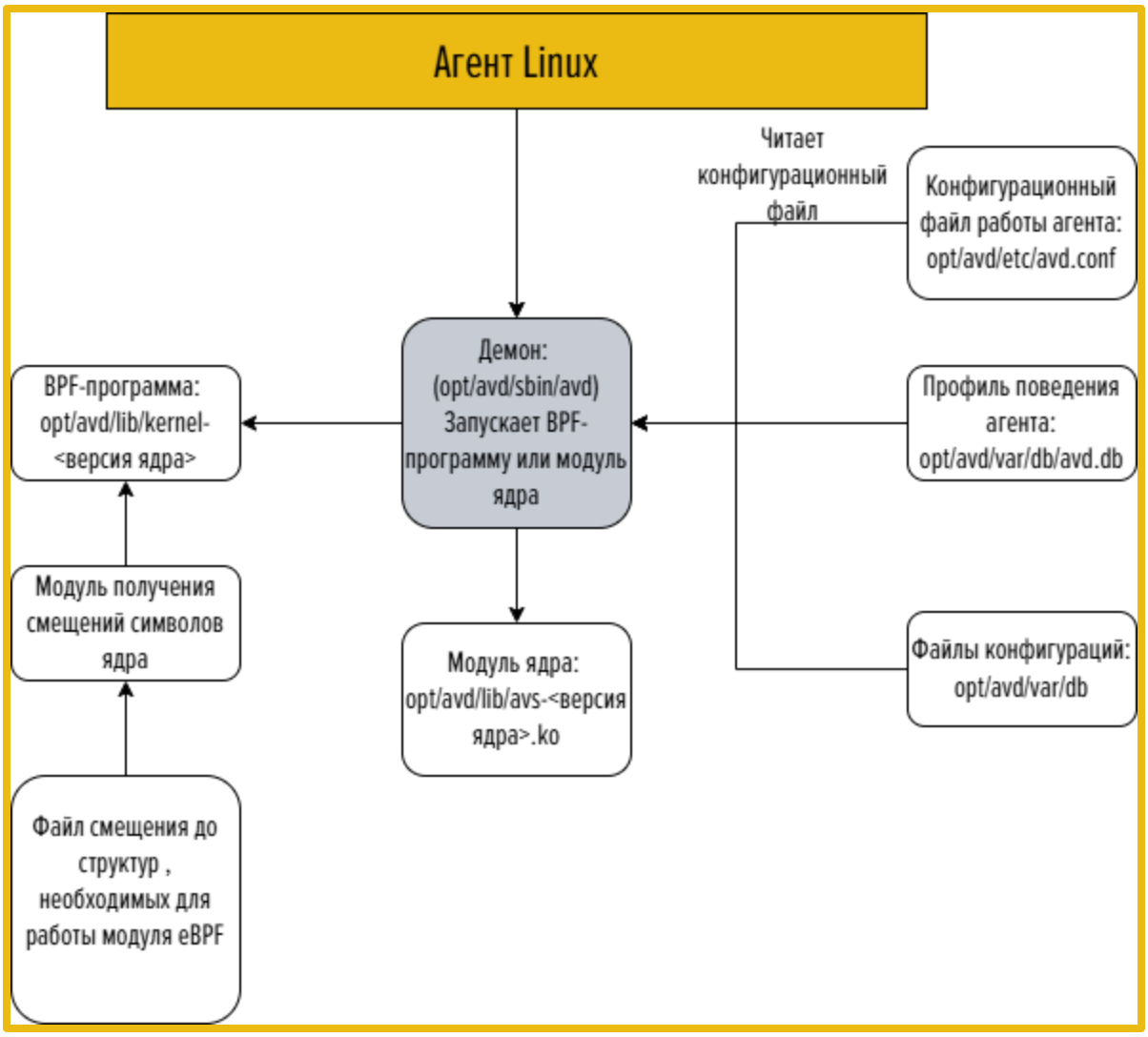


Рисунок 2 – Архитектура агента Linux

4.4 Архитектура серверной части

4.4.1. Общие сведения

Серверная часть системы представляет собой микросервисы в контейнерах Docker, развёрнутые на серверной платформе.

Loadbalancer — это единственный компонент, к которому обращаются браузер пользователя и агенты на компьютерах. Он принимает HTTPS на портах 443 (и 8443, если выделен отдельный канал для агентов) и передаёт запросы внутрь.

Webserver — принимает запросы от Loadbalancer, маршрутизирует их нужному сервису, раздаёт статику веб-консоли.

Frontend (eas-front) — сама веб-консоль: окна, таблицы, графики, которые видит пользователь. Это React-приложение.

DjangoApp — основной сервер приложения. Именно он реализует бизнес-логику: управляет агентами, пользователями, правами, конфигурациями, инцидентами, задачами, интеграциями.

PostgreSQL — основная база данных. Хранит пользователей, права, конфигурации, инциденты, метаданные агентов.

Elasticsearch — хранилище событий с агентов и журнала безопасности. Позволяет быстро искать и фильтровать миллионы событий.

MinIO — объектное хранилище (S3-совместимое). Хранит файлы: конфигурации, образцы файлов с агентов, дистрибутивы обновлений.

Кеш (Redis) — быстрая оперативная память: токены сессий, одноразовые коды, кеш часто используемых данных.

EventQ (Redis) — очередь-буфер для событий, поступающих от агентов. Сглаживает всплески нагрузки.

Worker — «конвейер», читает события из EventQ, распаковывает, обогащает дополнительными данными и аккуратно пакетами пишет в Elasticsearch. Он же отвечает за экспорт событий во внешние системы.

IOA-python — это микросервис валидации и анализа правил IOA (Indicators of Attack — индикаторы атак, то есть поведенческие правила обнаружения). работы с IOA-правилами на сервере: проверяет синтаксис, прогоняет события через условия, конвертирует Sigma в формат EDR. Пользователь видит результат его работы в редакторе правил, в кнопке проверки и в ретроспективных проверках.

Серверная часть функционирует под управлением ОС семейства Linux.

Архитектура серверной части Программы схематично представлена на рисунке 3.

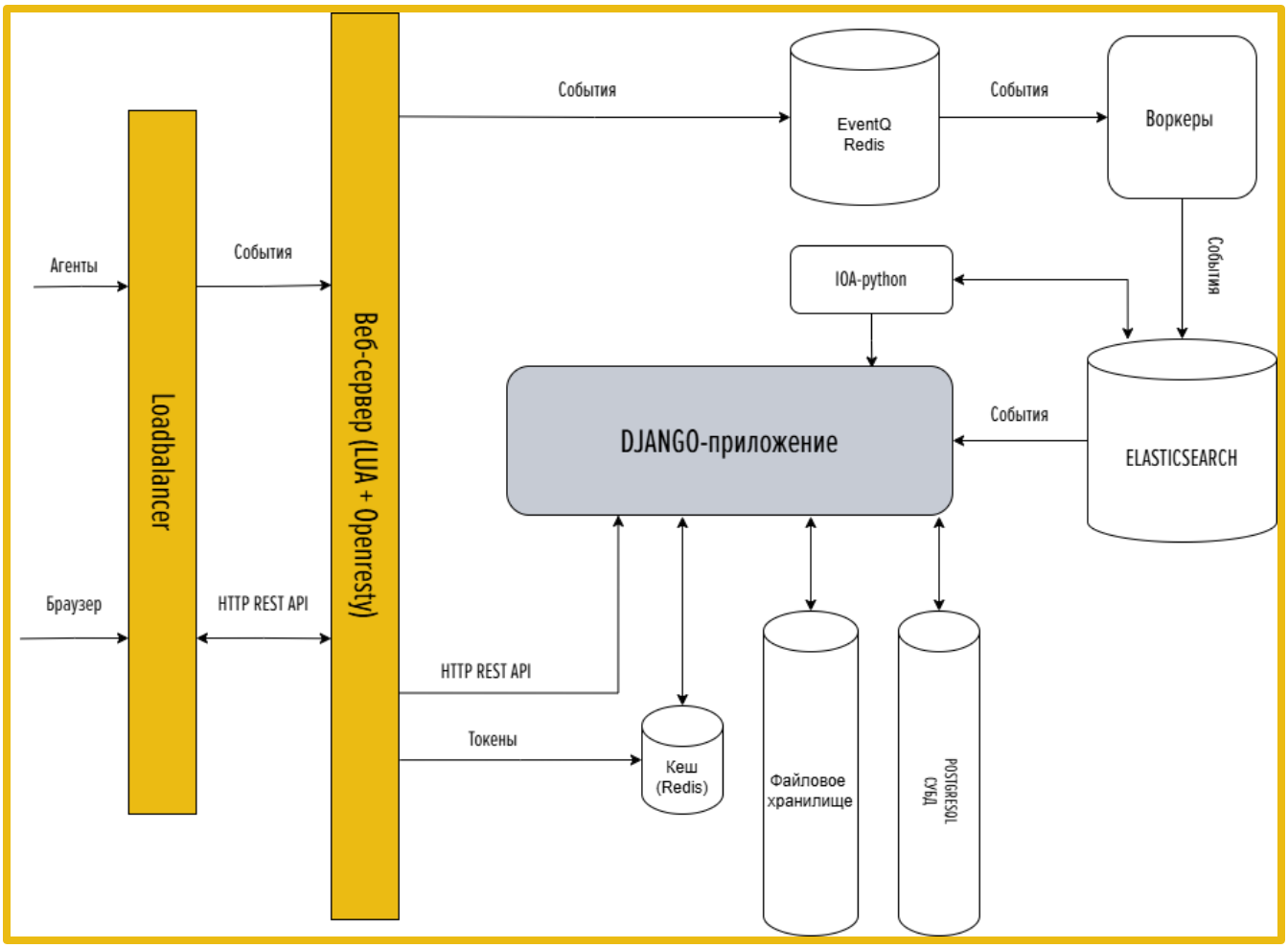


Рисунок 3 – Архитектура серверной части «RT Protect EDR»

4.4.2. Функции системы со стороны серверной части

Сервер предоставляет администратору возможность регистрации агентов.

Сервер принимает поток событий, отправляемых ему агентами, и структурирует их с целью последующего анализа.

Сервер имеет административный модуль (frontend) для визуального представления профиля агента, его состояния, статистических данных, обнаруженных инцидентов безопасности и другой информации, которая может быть полезна администратору для наблюдения за агентом в динамике.

Административный модуль сервера имеет функции управления агентом – блокировки сети, отправки скрипта на выполнение и другое. Интерфейсы сервера позволяют административному модулю получать необходимую информацию для ее визуального представления и отправлять команды и данные агенту.

5. Настройка Программы

5.1 Требования к среде функционирования

Программа в клиентской части (агент) работает на 32-х и 64-х разрядной платформе, начиная с Windows 7, на серверных версиях Windows Server 2008 R2, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019, Windows Server 2022, Windows Server 2025, а также на различных версиях ОС Linux (Ubuntu 20.04.5 LTS с ядром linux-5.15.0, Ubuntu 18.04, Ubuntu 22.04, Ubuntu 24.04, Astra Linux SE 1.6, Astra Linux SE 1.7 _x86-64, Astra Linux 1.8, ALT Linux 10, Red OS 7.3, Debian 11, Debian 12, Debian 13, CentOS.



Примечание

Для ОС Windows 7 либо Windows Server 2008 R2 должны быть установлены пакеты обновлений KB4474419 и KB4490628.

На всех версиях Windows для корректной работы агента EDR требуется наличие установленного компонента .NET Framework версии 4.5 или выше.

Требования клиента к аппаратуре совпадают с соответствующими требованиями Windows и Linux. Дополнительные требования не предъявляются.



Важно

Агент для Windows не поддерживает полноценную работу в безопасном режиме Windows. В безопасном режиме с загрузкой сетевых драйверов загружается драйвер EDR. При этом служба драйвера не будет выполнять свои функции. В этом случае функционируют индикаторы атак, индикаторы компрометации, примененные к агенту, и внутренние правила EDR. События сохраняются на диск компьютера с установленным агентом, но не отправляются на сервер. На сервере управления такой агент будет отображаться со статусом **Не активен**.

Серверная часть Программы работает на 64-х разрядной платформе семейства Linux (Ubuntu 20.04.5 LTS, Astra Linux 1.8). Аппаратная платформа сервера обеспечивает возможность выполнения функциональных требований, предъявляемых к серверу, с учетом технологии его построения, критериев производительности и отказоустойчивости.

Клиентская часть программы пригодна для функционирования на аппаратных платформах, указанных в таблице 6.

Таблица 6 – Программно-аппаратное обеспечение и среда функционирования клиента (минимальные и рекомендуемые настройки для установки агента)

Характеристики	Клиентская часть	
Операционная система	Windows/Linux	
	Минимальные требования	Рекомендуемые требования
Процессор	x86 с тактовой частотой 1 ГГц и выше	x86 с тактовой частотой от 2 ГГц и выше
Оперативная память	2 ГБ	4 ГБ
Жесткий диск (свободное пространство)	2 ГБ	4 ГБ

Минимальные требования для сервера, обслуживающего 500 и 5000 агентов с периодом хранения событий 30 дней, представлены в таблице 7.

Таблица 7 – Требования к серверу

Характеристика	Количество агентов	
	500	5000*
Процессор	12 ядер с частотой не менее 3 GHz	24 ядра с частотой не менее 3 GHz
Оперативная память	32 ГБ	96 ГБ
Жесткий диск** (свободное пространство)	SSD: 630 ГБ HDD: 2 ТБ	SSD: 6 ТБ HDD: 20 ТБ
Пропускная способность канала	4 Мбит/с	40 Мбит/с

*Нагрузка на жесткий диск зависит от времени хранения событий и рассчитывается исходя из того, что на одно событие приходится 1,5 килобайта данных. Нагрузка на сетевой канал рассчитывается исходя из того, что в 1 секунду отправляется 0,5 килобайта данных на 1 событие.

При расчете требований к среде функционирования серверной части необходимо учитывать, что среднее количество событий, приходящих от агента в секунду должно составлять не более 1 события.

Все расчеты для требований аппаратных платформ указаны с учетом EPS равного единице. Такое количество событий в секунду достигается работой аналитиков в части создания исключений для программ и файлов, сетевых исключений и исключений для индикаторов атак, а также с помощью настроек профиля безопасности агента.

**При необходимости до 2000 агентов можно использовать только HDD.



Примечание

Для показателя EPS (количество событий в секунду) в среднем равного 1,0 инфраструктура из 1000 агентов дает, соответственно, 1000 EPS. В таком случае в сутки необходимо хранить 86,4 млн событий. Событие RT Protect EDR в среднем занимает примерно 1,5 Кб дисковых данных на сервере. Это означает, что в сутки потребуется примерно 130 Гб дискового пространства для хранения событий 1000 агентов с 1,0 EPS на агента. Минимальный период хранения на практике составляет 7 дней, максимальный – 90 дней. Соответственно, минимально необходим диск размером около 0,9 Тб, а максимально – 11,7 Тб. Данные цифры справедливы, если при разворачивании сервера не используются дополнительные реплики БД событий. В противном случае приведенные цифры необходимо умножать на количество реплик. Данные цифры легко пересчитать для любого суммарного показателя EPS по формуле: S(Гб/сутки) = EPS * 0.1296 * r, где r – количество реплик.

Серверная часть Программы поддерживает работу в браузерах, представленных в таблице 8.

Таблица 8 – Список поддерживаемых браузеров

№ п/п	Тип браузера	Минимальная рекомендуемая версия
1	Google Chrome	Версия не ниже 92.0.4515.107
2	Firefox Browser	Версия не ниже 83.0

Примечание

Программа совместима с другими браузерами, однако корректная работа в них не гарантируется. В случае обращения к серверу управления из неподдерживаемого браузера рекомендуется отключать блокировщик рекламы (AdBlock).

Важно

Перед установкой агентов на конечных точках защищаемой корпоративной инфраструктуры необходимо добавить IP-адреса и доменные имена используемых в этой корпоративной инфраструктуре VPN-серверов и прокси-серверов в список сетевых исключений (выбрать тип действия **Разрешить (всегда)**).

5.2 Установка и удаление

5.2.1. Установка агента Windows

Установщик модуля агента поддерживает установку в режиме командной строки.

В случае необходимости установка может быть осуществлена вручную с помощью запуска на исполнение установщика на компьютере, на котором необходимо установить модуль агента. Для этого следует записать файл установщика на носитель информации.

Примечание

Агент EDR после установки регистрирует ETW-провайдер RT Protect EDR (GUID: 76967044-F243-4ABA-9B87-33D19F23D050). Для просмотра журнала необходимо перейти в директорию **Панель управления/Администрирование/Просмотр событий/Журналы приложений и служб/RT Protect EDR**.

Установка Агента с помощью инсталлятора с графическим интерфейсом

Инсталляционная версия агента представлена в виде собственного инсталлятора.

Для установки необходимо выполнить следующие шаги:

1) Скачать инсталлятор последней версии ПО с сервера предприятия-изготовителя.

2) Запустить процесс установки двойным кликом по инсталлятору. Откроется окно, представленное на рисунке 4.



Рисунок 4 – Окно установки Программы

3) Заполнить поле ID клиента (не менее 8 символов) IP-адрес и имя сервера. Взаимодействие между сервером EDR и агентом происходит по 443 порту, он устанавливается по умолчанию. ID клиента можно увидеть на сервере управления в разделе **Лицензия/Информация о лицензии**.

Важно

Значение /host (**Имя сервера**) должно точно совпадать с именем в сертификате сервера (CN/SAN – общее/альтернативное имя субъекта), например, edr.rt.ru.

4) При необходимости создания точки восстановления следует поставить флажок в строке **Точка восстановления**.

5) Нажать кнопку **Установить**, после чего появится окно **Индексирование файлов** (рис. 5).

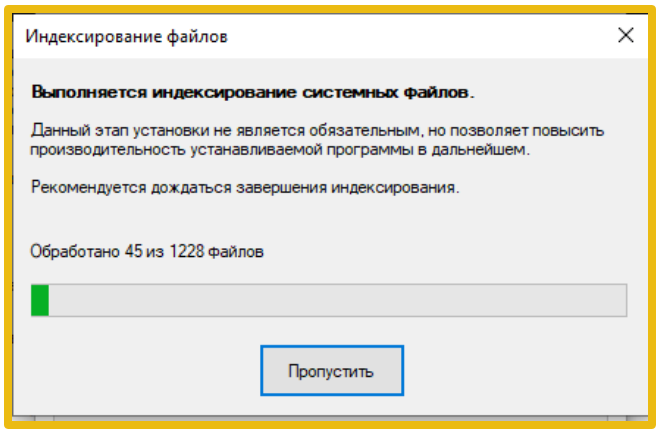


Рисунок 5 – Подтверждение установки

Примечание

Этап индексирования позволяет улучшить производительность файловой системы, рекомендуется дождаться завершения этого этапа при установке агента.

6) После окончания процесса установки появится информационное окно (рис. 6).

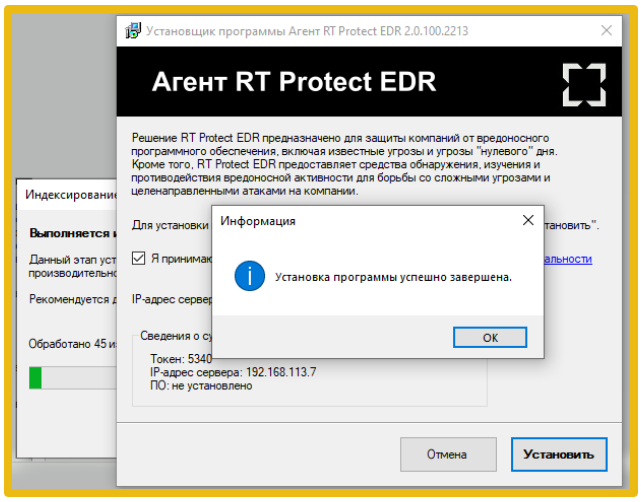


Рисунок 6 – Процесс установки

7) Нажать кнопку **OK**.

8) После завершения всех процедур установки в правом углу экрана в системном трее появится иконка установленного агента.



Примечание

После завершения установки на диске C в папке Program Files создается папка **PT-Информационная безопасность\Агент RT Protect EDR**.

9) После первоначальной установки агента его необходимо верифицировать. Операция доступна только пользователям системы с ролью «Администратор».

Установка агента с помощью инсталлятора в режиме командной строки

Установка агента с помощью инсталлятора **setup.exe** осуществляется пользователем с правами администратора.

Типичные операции и соответствующие им комбинации командных строк:

1) Первоначальная установка агента в silent-режиме с индексированием файлов:

```
Setup /noUI /server=192.168.77.77:5000 /customerId=12345678
```

2) Первоначальная установка агента в silent-режиме с пропуском этапа индексирования файлов:

```
Setup /noUI /skipIndexing /server=192.168.77.77:5000 /customerId=12345678
```

Для разрешения перезагрузки (в случае необходимости) без запроса пользователя допускается указать параметр /canReboot.

В параметре customerId указывается действительный код клиента из лицензии.

3) Обновление установленного агента:

```
Setup /noUI /update
```



Совет

Команда Setup /noUI /update, запущенная из каталога, в котором находится установочный файл текущего агента, позволяет перезапустить службу.

4) Обновление установленного агента с перезагрузкой:

```
Setup /noUI /updatesafe /canReboot
```

5) Обновление endpoint-сервера:

```
Setup /noUI /update /server=192.168.77.77:5000
```



Совет

В параметре /server указывается endpoint сервера (допускается не указывать номер порта). Если требуется обновить только порт, то вместо IP-адреса сервера допускается указывать символ * (пример: /server=*:5000).

6) Обновление идентификатора клиента:

```
Setup /noUI /update /customerId=12345678
```

Опции установки в командной строке

Интерфейс командной строки программы установки агента:

- /noUI – запуск программы установки без показа пользовательского интерфейса;
- /canReboot – разрешение перезагрузки без запроса к пользователю (если перезагрузка требуется);
- /skipIndexing – пропуск этапа установки, связанного с индексированием файлов;
- /update – режим «обновление на лету»;
- /updatesafe – режим «обновление с перезагрузкой»;
- /server – идентификация серверной части;
- /customerId – идентификатор клиента (выдается вместе с лицензией);
- /restore_point – создание точки восстановления;
- /no_driver – режим «без драйвера»;

— /no_proxy – режим установки агента, при котором не используются системные настройки проксирования сетевого трафика при взаимодействии с сервером;

— /preVerifyEvents – опции отслеживания событий на этапе верификации:

— /preVerifyEvents=0 – не отслеживать (после верификации агента на сервере не будут отображаться события, произошедшие в системе до этапа верификации);

— /preVerifyEvents=1 – отслеживать только события **Старт процесса** (после верификации на сервере будут отображаться только события запусков процессов);

— /preVerifyEvents=2 – отслеживать все события (все события после установки и до верификации будут накапливаться в кеше до этапа его переполнения, после которого новые события будут перетирать старые события, при стандартных условиях наполнение кеша событий происходит в течение 7 дней).

— По умолчанию агент устанавливается с опцией /preVerifyEvents=0.

— /tray=[<Уровень>] – управление значком и уведомлениями в трее.

Уровни управления уведомлениями в трее:

0 – нет значка в трее, уведомления не выводятся;

1 – есть значок, уведомления не выводятся;

2 – есть значок, показывать только критические уведомления;

3 – есть значок, показывать все уведомления.

Пример записи: /tray 0 – установка агента без значка в трее и без вывода уведомлений.

5.2.2. Установка агента Linux

Установка агента в операционной системе Linux поддерживается в следующих системах:

1) Astra SE 1.6 (поддерживаемые ядра):

— 5.15.0-33-generic;

— 5.15.0-33-hardened;

— 5.10.142-1-generic;

— 5.10.142-1-hardened;

— 5.4.0-110-generic;

— 5.4.0-110-hardened;

– 4.15.3.177-generic;

– 4.15.3.177-hardened;

– 4.15.3-1-generic.

2) Astra SE 1.7 (поддерживаемые ядра):

– 6.1.90-1-generic;

– 6.1.50-1-generic;

– 6.1.50-1-generic-1;

– 5.15.0-111-generic;

– 5.15.0-83-generic;

– 5.15.0-70-generic;

– 5.15.0-33-generic;

– 5.15.0-33-generic-1;

– 5.10.216-1-generic;

– 5.10.190-1-generic;

– 5.10.176-1-generic;

– 5.10.142-1-generic;

– 5.10.0-1057-generic;

– 5.10.0-1045-generic;

– 5.4.0-186-generic;

– 5.4.0-162-generic;

– 5.4.0-110-generic;

– 5.4.0-110-generic-1;

– 5.4.0-81-generic;

– 5.4.0-54-generic.

3) Astra 1.8 (только в режиме ядра);

4) Debian 11 (поддерживаемые ядра):

– 5.10.0-34-amd64;

– 5.10.0-33-amd64;

– 5.10.0-32-amd64;

– 5.10.0-31-amd64;

– 5.10.0-30-amd64;

– 5.10.0-29-amd64;

– 5.10.0-28-amd64;

– 5.10.0-27-amd64;

– 5.10.0-26-amd64;

– 5.10.0-25-amd64;

– 5.10.0-23-amd64;

– 5.10.0-19-amd64;

– 5.10.0-11-amd64.

5) Debian 12(поддерживаемые ядра):

– 6.1.0-32-amd64;

– 6.1.0-31-amd64;

– 6.1.0-30-amd64;

– 6.1.0-29-amd64;

– 6.1.0-28-amd64;

– 6.1.0-27-amd64;

– 6.1.0-26-amd64;

– 6.1.0-25-amd64;

– 6.1.0-23-amd64;

– 6.1.0-22-amd64;

– 6.1.0-21-amd64;

– 6.1.0-20-amd64;

– 6.1.0-18-amd64;

– 6.1.0-17-amd64;

– 6.1.0-16-amd64;

– 6.1.0-15-amd64;

– 6.1.0-14-amd64;

– 6.1.0-13-amd64;

– 6.1.0-12-amd64;

– 6.1.0-11-amd64;

– 6.1.0-10-amd64.

6) Ubuntu 20.04 (поддерживаемые ядра):

– 5.15.0-134-generic;

– 5.15.0-131-generic;

– 5.15.0-130-generic;

– 5.15.0-127-generic;

– 5.15.0-126-generic;

– 5.15.0-125-generic;

– 5.15.0-124-generic;

– 5.15.0-122-generic;

– 5.15.0-121-generic;

– 5.15.0-119-generic;

– 5.15.0-118-generic;

– 5.15.0-117-generic;

– 5.15.0-116-generic;

– 5.15.0-113-generic;

– 5.15.0-107-generic;

– 5.15.0-106-generic;

– 5.15.0-105-generic;

– 5.15.0-102-generic;

– 5.15.0-101-generic;

– 5.15.0-100-generic;

– 5.15.0-97-generic;

– 5.15.0-94-generic;

– 5.15.0-92-generic;

– 5.15.0-91-generic;

– 5.15.0-89-generic;

– 5.15.0-88-generic;

– 5.15.0-87-generic;

– 5.15.0-86-generic;

– 5.15.0-84-generic;

– 5.15.0-83-generic;

– 5.15.0-82-generic;

– 5.15.0-78-generic;

– 5.15.0-76-generic;

– 5.15.0-75-generic;

– 5.15.0-73-generic;

– 5.15.0-72-generic;

– 5.15.0-71-generic;

– 5.15.0-70-generic;

– 5.15.0-69-generic;

– 5.15.0-67-generic;

– 5.4.0-208-generic;

– 5.4.0-205-generic;

– 5.4.0-204-generic;

– 5.4.0-202-generic;

– 5.4.0-200-generic;

– 5.4.0-198-generic;

– 5.4.0-196-generic;

– 5.4.0-195-generic;

– 5.4.0-193-generic;

– 5.4.0-192-generic;

– 5.4.0-190-generic;

– 5.4.0-189-generic;

– 5.4.0-187-generic;

– 5.4.0-186-generic;

– 5.4.0-182-generic;

– 5.4.0-181-generic;

– 5.4.0-177-generic;

– 5.4.0-176-generic;

– 5.4.0-174-generic;

– 5.4.0-173-generic;

– 5.4.0-172-generic;

– 5.4.0-171-generic;

– 5.4.0-170-generic;

– 5.4.0-169-generic;

– 5.4.0-167-generic;

– 5.4.0-166-generic;

– 5.4.0-165-generic;

– 5.4.0-164-generic;

– 5.4.0-163-generic;

– 5.4.0-162-generic;

– 5.4.0-159-generic;

– 5.4.0-155-generic;

– 5.4.0-153-generic;

– 5.4.0-152-generic;

– 5.4.0-150-generic;

– 5.4.0-148-generic;

– 5.4.0-139-generic;

– 5.4.0-137-generic.

7) Ubuntu 22.04 (поддерживаемые ядра):

– 5.15.0-25-generic;

– 5.15.0-56-generic;

– 5.15.0-60-generic;

– 5.15.0-71-generic;

– 5.15.0-73-generic;

– 5.15.0-75-generic;

– 5.15.0-76-generic;

– 5.15.0-78-generic;

– 5.15.0-79-generic;

– 5.15.0-82-generic;

– 5.15.0-83-generic;

– 5.15.0-84-generic;

– 5.15.0-86-generic;

– 5.15.0-87-generic;

– 5.15.0-88-generic;

– 5.15.0-89-generic;

– 5.15.0-91-generic;

– 5.15.0-92-generic;

– 5.15.0-94-generic;

– 5.15.0-97-generic;

– 5.15.0-100-generic;

– 5.15.0-101-generic;

– 5.15.0-102-generic;

– 5.15.0-105-generic;

– 5.15.0-106-generic;

– 5.15.0-107-generic;

– 5.15.0-112-generic;

– 5.15.0-113-generic;

– 5.15.0-116-generic;

– 5.15.0-117-generic;

– 5.15.0-118-generic;

– 5.15.0-119-generic;

– 5.15.0-121-generic;

– 5.15.0-122-generic;

– 5.15.0-124-generic;

– 5.15.0-125-generic;

– 5.15.0-126-generic;

– 5.15.0-127-generic;

– 5.15.0-128-generic;

– 5.15.0-130-generic;

– 5.15.0-131-generic;

– 5.15.0-133-generic;

– 5.15.0-134-generic;

– 5.19.0-41-generic;

– 5.19.0-42-generic;

– 5.19.0-43-generic;

– 5.19.0-45-generic;

– 5.19.0-46-generic;

– 5.19.0-50-generic;

– 6.2.0-25-generic;

– 6.2.0-26-generic;

– 6.2.0-31-generic;

– 6.2.0-32-generic;

– 6.2.0-33-generic;

– 6.2.0-34-generic;

– 6.2.0-35-generic;

– 6.2.0-36-generic;

– 6.2.0-37-generic;

– 6.2.0-39-generic;

– 6.5.0-14-generic;

– 6.5.0-15-generic;

– 6.5.0-17-generic;

– 6.5.0-18-generic;

– 6.5.0-21-generic;

– 6.5.0-25-generic;

– 6.5.0-26-generic;

– 6.5.0-27-generic;

– 6.5.0-28-generic;

– 6.5.0-35-generic;

– 6.5.0-41-generic;

– 6.5.0-44-generic;

– 6.5.0-45-generic;

– 6.5.0-47-generic;

– 6.5.0-48-generic;

– 6.5.0-49-generic;

– 6.5.0-50-generic;

– 6.5.0-51-generic;

– 6.5.0-52-generic.

8) Ubuntu 24.04 (поддерживаемые ядра):

– 6.8.0-31-generic;

– 6.8.0-35-generic;

– 6.8.0-36-generic;

– 6.8.0-38-generic;

– 6.8.0-39-generic;

– 6.8.0-40-generic;

– 6.8.0-41-generic;

– 6.8.0-44-generic;

– 6.8.0-45-generic;

– 6.8.0-47-generic;

– 6.8.0-48-generic;

– 6.8.0-49-generic;

– 6.8.0-50-generic;

– 6.8.0-51-generic;

– 6.8.0-52-generic;

– 6.8.0-53-generic;

– 6.8.0-54-generic;

– 6.8.0-55-generic;

– 6.11.0-17-generic;

– 6.11.0-19-generic.

9) ALT Linux 10.

– 6.1.130-un-def-alt1;

– 6.1.129-un-def-alt1;

– 6.1.128-un-def-alt1;

– 6.1.127-un-def-alt1;

– 6.1.124-un-def-alt1;

– 6.1.123-un-def-alt1;

– 6.1.121-un-def-alt1;

– 6.1.119-un-def-alt1;

– 6.1.115-un-def-alt1;

– 6.1.113-un-def-alt1;

– 6.1.112-un-def-alt1;

– 6.1.111-un-def-alt1;

– 6.1.100-un-def-alt1;

– 5.10.234-std-def-alt1;

– 5.10.233-std-def-alt1;

– 5.10.231-std-def-alt1;

– 5.10.228-std-def-alt1;

– 5.10.227-std-def-alt1;

– 5.10.226-std-def-alt1;

– 5.10.224-std-def-alt1;

– 5.10.223-std-def-alt1;

– 5.10.221-std-def-alt1;

– 5.10.213-std-def-alt1;

10) RedOs 7.3:

– 6.1.128-2.el7.3.x86_64;

– 6.1.110-1.el7.3.x86_64;

– 6.1.94-1.el7.3.x86_64;

– 6.1.52-1.el7.3.x86_64;

– 6.1.44-1.el7.3.x86_64;

– 6.1.38-2.el7.3.x86_64;

– 6.1.20-2.el7.3.x86_64;

– 5.15.178-1.el7.3.x86_64;

– 5.15.167-1.el7.3.x86_64;

– 5.15.161-1.el7.3.x86_64;

– 5.15.131-1.el7.3.x86_64;

– 5.15.125-1.el7.3.x86_64;

– 5.15.87-1.el7.3.x86_64;

– 5.15.78-2.el7.3.x86_64;

– 5.15.72-1.el7.3.x86_64;

– 5.15.35-5.el7.3.x86_64;

– 5.15.35-4.el7.3.x86_64;

– 5.15.35-1.el7.3.x86_64;

– 5.15.10-4.el7.x86_64;

– 5.15.10-3.el7.x86_64;

– 5.15.10-2.el7.x86_64;

– 5.15.10-1.el7.x86_64;

– 5.10.29-3.el7.x86_64;

– 5.10.29-1.el7.x86_64;

– 5.10.24-3.el7.x86_64.

11) RedOS 8;

12) CentOS 8 и 9 (в режиме eBPF).

Дистрибутив Агента EDR под Linux представлен в виде следующих пакетов:

– deb-пакет;

– rpm-пакет.

Агент EDR в формате deb-пакета, рассчитан на установку в следующих ОС:

– Ubuntu 20.04;

– Ubuntu 22.04;

– Ubuntu 24.04;

– Debian GNU/Linux 11;

– Debian 12;

– Astra SE 1.6 _x86-64;

– Astra SE 1.7 _x86-64;

– Astra 1.8;

Агент EDR в формате rpm-пакета, рассчитан на установку в следующих ОС:

– Red OS 7.3;

– ALT Linux 10;

– CentOS.

Совет

Совместимость ядер для различных версий ОС Linux желательно уточнять у Производителя, так как список поддерживаемых ядер постоянно меняется.

Общие сведения

Для работы агента требуются следующие пакеты (большая часть из них входит в состав базовой части ОС):

1) libbrotli1 (>= 0.6.0);
2) libc6 (>= 2.22);
3) libcurl3-gnutls (>= 7.16.3);
4) libelf1 (>= 0.131);
5) libev4 (>= 1:4.04);
6) libgcc-s1 (>= 3.0);
7) libjansson4 (>= 2.1);
8) libprocps8 (>= 2:3.3.16-1);
9) libsqlite3-0 (>= 3.5.9);
10) libssl1.1 (>= 1.1.0);
11) libstdc++6 (>= 7);
12) libuuid1 (>= 2.16);
13) zlib1g (>= 1:1.1.4).

Порядок установки

1) Установить пакеты из зависимостей, выполнив в терминале в ОС (Ubuntu/ Debian/Astra) следующую команду:

```
sudo apt install libbrotli1 libcurl3-gnutls libelf1 libev4 libjansson4 libsqlite3-0 libssl1.1 libuuid1 zlib1g
```



Совет

Для значительной части ОС (Debian, Ubuntu) достаточно ввести команду `sudo apt install libev4`

2) Перейти в директорию с распакованным архивом инсталлятора, например, выполнить команду:

   `cd Загрузки`

3) Установить deb-пакет агента EDR в ОС (Ubuntu/Debian/Astra), выполнив в терминале следующую команду:

   `sudo dpkg -i avd_1.0.0_amd64.deb` (подставить текущую версию агента)



Совет

Чтобы в ОС Debian запустить установку от пользователя, его необходимо внести в файл sudoers.

4) Для установки пакетов из зависимостей в ОС Red OS 7.3 в терминале выполнить следующие команды:

   `sudo yum -y install jansson`

   `sudo yum -y install libev`

5) Установить rpm-пакет агента EDR в ОС ReD OS 7.3, выполнив в терминале следующую команду:

   `sudo rpm –U avd-1.3.0-redos.x86_64.rpm` (подставить текущую версию агента).

Установка CentOS

Для установки CentOS достаточно распаковать архив с инсталлятором и запустить установку двойным кликом по rpm-пакету.

Установка агента в ОС ALT Linux 10

1) Открыть терминал и выполнить команду `su –`

2) Установить пакеты из зависимостей, выполнив команды:

   `epm install libcurl.so.4`

   `epm install libev.so.4`

3) Распаковать архив с инсталлятором в файловом менеджере и нажать ПКМ на rpm-пакете, после чего выбрать пункт **Открыть** в **Установка RPM**;
4) Установить rpm-пакет;
5) Изменить с помощью команды mc (должна запускаться от root) конфигурационный файл /opt/avd/etc/avd.conf в терминале, указав IP-адрес сервера EDR вместо localhost;
6) Запустить службу агента с помощью команды systemctl start avd (должна запускаться от root).



Совет

Чтобы проверить статус агента, необходимо ввести команду sudo systemctl status avd.

Первая настройка

После установки пакета (для любой ОС) необходимо указать в конфигурационном файле /opt/avd/etc/avd.conf актуальное значение для customerId, а также адрес сервера EDR – вместо localhost указать IP-адрес или доменное имя сервера, например:

```
customerId=9e391e34f921fa4e
http {
  ...
  server=
  ...
}
```

Вместо имени можно указать адрес сервера:

```
  server=192.168.1.1
```

По умолчанию взаимодействие между агентом Linux и сервером EDR осуществляется по 443 порту.

Генерация токена выполняется агентом автоматически при первом запуске, однако токен можно задать принудительно, указав в конфигурационном файле его значение в формате: token=...

Совет

Чтобы в ОС Ubuntu или Debian открыть конфигурационный файл с правами root, необходимо ввести команду `SUDO_EDITOR=gedit sudoedit /opt/avd/etc/avd.conf`

Чтобы открыть в РедОС конфигурационный файл с правами root, необходимо ввести команду `sudo mc`.

После настройки конфигурационного файла необходимо запустить сервис агента, выполнив в терминале следующую команду:

```
sudo systemctl start avd
```

В дальнейшем сервис будет стартовать автоматически при запуске ОС.

После успешной установки агент появится в списке верификации на сервере EDR.

После установки DEB-пакета в системе появится systemd-сервис avd.

Примечание

В режиме замкнутой программной среды в Astra Linux требуется перезагрузка после установки дистрибутива и настройки конфигурационного файла

Изменение параметров конфигурационного файла после запуска сервиса при указании ошибочной информации

Для изменения параметров в конфигурационном файле при уже включенном сервисе следует выполнить следующие действия:

1. Отключить защиту от остановки сервиса, выполнив следующую команду в терминале:

`sudo /opt/avd/sbin/avd --password` (по умолчанию указывается пустой пароль, если не установлен пароль для удаления агента);

2. Остановить сервис, выполнив команду:

`sudo systemctl stop avd`

3. Поправить конфигурационный файл (например, данное действие можно выполнить в ОС Red OS, выполнив команду:

`sudo pluma /opt/avd/etc/avd.conf .`

3. Запустить сервис, выполнив команду:

```
sudo systemctl start avd
```

Изменение и настройка режима работы агента после установки

Агент EDR поддерживает два механизма сбора телеметрии:

BPF (Berkeley Packet Filter) – обеспечивает полный мониторинг системных событий, включая события доступа к процессам.

KMOD (kernel module) – модуль ядра, обеспечивающий мониторинг системных вызовов, не собирает события доступа к процессам.

Режим работы агента определяется совокупностью двух источников конфигурации:

1) Локальный файл avd.conf (параметры bpf, kmod);
2) Централизованная настройка cmode, передаваемая с сервера управления.

Режим работы агента может находиться в двух состояниях для режима kmod (вкл и выкл) и в трех состояниях для bpf-режима: включенное состояние (как основной поставщик телеметрии), включенное состояние в дополнение к kmod (перехватывает только событие доступа к процессу) и выключенное состояние.

Агент осуществляет выбор режима работы путем формирования битового флага (первый бит – BPF вкл/выкл, второй бит KMOD вкл/выкл).

Итоговый флаг формируется побитовым И двух флагов:

1) При запуске агента он читает конфиг (avd.conf), смотрит есть ли там записи bpf= или kmod= (по умолчанию данные поля отсутствуют и их нужно задавать вручную), составляет битовый флаг (по умолчанию 11, если было, например, kmod=false, то будет флаг 10).
2) Читает флаг в базе данных (этот флаг управляется через cmode) По умолчанию или при cmode 0 - флаг в БД 11 (BPF и KMOD), при cmode 1 - флаг в БД 10(только BPF).

Итоговый режим работы формируется через побитовое И.

Например, если в конфигурации bpf = true, kmod = false (флаг от конфигурации будет 10), а с сервера прописан cmode 0 (флаг от сервера будет 11), то итоговый флаг 10 & 11 = 10, а значит только BPF.

Запуск мониторинга после формирования флага осуществляется по следующему алгоритму:

Если в состоянии KMOD-режима работы агента установлено 1, то будет выполняться загрузка режима KMOD, если 0 – загрузка не выполняется.

Если в состоянии BPF-режима работы агента устанавливается 1, то проверяется, успешно ли загрузился KMOD. Если успешно, то загружается режим «только события доступа к процессу». Если KMOD не был успешно загружен, то BPF загружается как основной монитор. Если в флаге BPF стояло значение 0, то BPF не будет загружен. Если в конфигурации написать kmod = 1, bpf = 0, то будет загружен или KMOD (без событий доступа к процессу) или не будет загружен ни один из режимов работы. Например, если с сервера установлен cmode 0 или cmode вообще не было, то итоговая маска при конфигурации выше будет 01, что приведет к отсутствию попыток загрузки BPF при успешно запущенном KMOD и, как следствие, к отсутствию событий доступа к процессу. При отключении защиты на сервере в БД агента выставляется маска 00, что отключает попытки загрузки как KMOD, так и BPF. Для того, чтобы клиент подхватил обновленную маску из конфигурации, требуется перезагрузка агента.

Чтобы агент выполнил загрузку новой маски с сервера, отправляется команда CMODE со сменой режима на отличный от текущего или отключение/включение защиты.

Необходимо избегать написания конфигураций с итоговой маской 01 (KMOD включен, BPF выключен) т.к. при ней в дополнение к KMOD не будет запущен BPF в режиме детектирования доступа к процессу, что приведет к потере соответствующей группы событий.

Таблица 9 – Типы итоговых масок.

Тип маски	Описание
Маска 11	Запущен KMOD и BPF (только для события доступа к процессу). Если KMOD не смог стартовать, то будет запущен только BPF, но как основной монитор.
Маска 00	Защита отключена, ни KMOD, ни BPF не будут загружаться
Маска 01	Загружается KMOD, но без событий доступа к процессу (т.к. за них отвечает BPF, а он выключен), или ни kmod, ни BPF не загружаются.
Маска 10	Загружается только BPF как основной монитор.

Настройка поддержки сетевой изоляции и получения событий DNS в ОС RHEL 8 и Oracle Linux 8 для режима eBPF (ядра младше 5.8).

На ОС RHEL8 и Oracle Linux 8 для функционала сетевой изоляции в режиме eBPF и поддержки получения DNS-событий обязательно включение механизма cgroup v2.

Cgroups – это механизм ядра Linux для группировки процессов и управления/учёта их ресурсов (CPU, память, I/O, сеть, число задач), v2 — вторая, унифицированная версия этой подсистемы. По умолчанию этот механизм отключен в указанных ОС.

Команда для включения cgroup v2:

```
sudo grubby --update-kernel=ALL --args="systemd.unified_cgroup_hierarchy=1"
```

После выполнения команды произведите перезагрузку узла.

5.2.3. Точка восстановления ОС, созданная при установке агента

Перед созданием точки восстановления при установке агента необходимо убедиться, что служба VSS включена, а заданный объем дискового пространства для точек восстановления достаточен для сохранения всех существующих и создаваемой точек восстановления.



Примечание

Точка восстановления – специальная функция в операционной системе Windows, которая позволяет сохранить текущие настройки компьютера. После выполнения этой операции пользователь сможет без особого труда вернуться к рабочему состоянию устройства после появления неполадок или сбоя в работе системы.

Если при установке агента была создана точка восстановления, то для восстановления состояния системы в состояние, предшествующее установке агента, следует произвести следующие действия (в зависимости от версии Windows шаги могут отличаться, приведена последовательность действий для Windows 10):

1) Нажать правой кнопкой мыши на меню **Пуск** и зайти в раздел **Система**. Открывается окно **Параметры**.
2) В области **Сопутствующие параметры** открыть раздел **Защита системы**.
3) В открывшемся окне **Свойства системы** нажать кнопку **Восстановить**.
4) В открывшемся окне **Восстановление системы** поставить флаг для кнопки выбора **Выбрать другую точку восстановления**.

5) Выбрать точку восстановления, созданную при установке агента EDR, выделив соответствующую строчку из списка.
6) Подтвердить действие, нажав кнопку **Готово**.

5.2.4. Идентификация агента

Запросы от агента, посылаемые на сервер, содержат в теле сообщения идентификатор агента. Каждый запрос от агента содержит параметр **token**. Этот параметр передается как query-параметр URL. Если **token** не будет передан или верифицирован сервером, то такой запрос будет отклонен с ошибкой.

Токен представляет собой случайную строку с произвольным набором символов. В Программе предусмотрена реализация уникальности токенов для агентов, то есть существование агентов с одинаковыми токенами невозможно.

Идентификатор позволяет серверу связать агента с событием в базе данных. По факту, идентификатор выступает как поле в таблице событий, по которому строится индекс.

Вместе идентификатор и токен образуют пару, схожую с концепцией «логин и пароль», однако, более строгую, так как одинаковые «пароли» (токены) не допускаются даже для разных «логинов» (идентификаторов). При этом идентификатор агента не является чувствительной информацией. Таким образом, все тело сообщения может быть передано для анализа доверенному лицу/Программе, и это не раскроет токенов доступа.

5.2.5. Удаление агента Windows

Удаление агента с конечной точки можно произвести следующими способами:

1) С помощью программы деинсталлятора **uninstall.exe**, которая находится в директории Program Files/PT-информационная безопасность/Агент_RT_Protect_EDR/<Папка с версией Программы>/uninstall.exe;
2) Штатным способом удаления программ через приложение Windows (Панель управления/Установка и удаление программ);
3) В режиме командной строки, набрав команды:

– Uninstall /noUI – запуск удаления Программы без показа пользовательского интерфейса;

– Uninstall /noUI /canReboot – запуск удаления Программы без показа пользовательского интерфейса и разрешением перезагрузки без запроса к пользователю.



Примечание

Агент устанавливается по умолчанию с выключенной опцией парольной защиты от удаления. Если данная опция была включена с сервера, то для удаления агента необходимо будет ввести пароль для удаления. Пароль удаления можно увидеть и скопировать на странице агента на сервере управления.

5.2.6. Удаление агента Linux

Перед удалением ПО агента необходимо предварительно предъявить пароль, заданный на сервере. Выполняется это с помощью команды:

sudo /opt/avd/sbin/avd --password

После запуска команды и ввода пароля администратора системы необходимо ввести пароль защиты от удаления и нажать Enter. Если пароль не был задан, необходимо ввести пустой пароль (Enter).

При успешном предъявлении пароля отсутствуют какие-либо сообщения, при ошибке предъявления пароля, например, если он неверен, то будет выведено в консоль соответствующее сообщение.

После того как пароль предъявлен успешно, можно выполнить удаление ПО агента с использованием штатных процедур, предусмотренных в ОС.

Например, для удаления агента (в ОС Astra Linux) с конечной точки можно набрать в терминале команду: sudo dpkg -r avd

Для удаления агента (в ОС RED OS) с конечной точки можно набрать в терминале команду:

«sudo rpm –e avd»

5.2.7. Установка сервера

Подробная информация об установке и обновлении сервера содержатся в документе «Инструкция по установке сервера EDR».

5.3 Особенности работы Программы с антивирусными средствами сторонних производителей

Антивирусные компоненты (процессы и модули), отмечаются в системе RT Protect EDR специальным признаком – AVEngine (может быть использован в виде флага **Антивирусный компонент** в исключениях для программ). Этот признак учитывается, так чтобы избегать конфликтов с антивирусами, в следующих случаях:

1) При контроле межпроцессного взаимодействия – чтение/запись памяти процессов и внедрении кода;
2) При анализе файловой активности на предмет выявления вредоносных паттернов подсистемой защиты от вирусов-шифровальщиков;
3) При срабатывании индикаторов компрометации – блокирующее действие переопределяется;
4) При получении команды от TI-платформы на уничтожение процесса – команда переопределяется.

Также признак можно использовать, например, при написании индикаторов атак, чтобы переопределить логику индикатора для антивирусного ПО.

В остальном антивирусные процессы с точки зрения реагирования ничем не отличаются от других, например, если индикатор атак предписывает блокировать запуск процесса или пользователь отправляет команду на уничтожение процесса, то желаемое действие будет выполнено. Также запуск антивирусного процесса будет заблокирован, если его хеш или имя файла добавлено в перечень индикаторов компрометации или файловые исключения с действием «Запрещено».

5.3.1. Срабатывание антивирусных средств при работе с веб-приложением RT Protect EDR

Срабатывание антивирусных средств при работе с веб-приложением EDR возникает в том случае, если в данных, получаемых фронтендом от сервера (в основном они приходят в формате JSON) содержится какая-то информация, которую антивирусное средство распознает как потенциально опасную. Это может быть хеш, имя файла, командная строка и т.д. (ниже такие информационные фрагменты называются артефактами).

Список экранов приложения, где высока вероятность срабатывания антивирусных средств:

— **Инциденты**, **Инцидент** (incidents, incident): внутри инцидентов могут содержаться артефакты;

— (!) любой экран (edr/*): в оповещении о новом инциденте содержится информация об инциденте (всплывающие нотификации в правом верхнем углу);

— **Активность** (events): внутри событий могут содержаться артефакты;

— **Оповещения** (user-messages): внутри оповещений содержится информация об инцидентах;

— **Процессы и модули** (modules): внутри событий могут содержаться артефакты;

— **Процесс** (process): в информации о процессе могут содержаться артефакты;

— **Журнал** (users-actions): в событиях журнала могут содержаться артефакты (внутри инцидентов и тд);

— отчет TI-платформы (ti): в отчете могут содержаться артефакты.

Список экранов приложения, где вероятность срабатывания ниже:

— **Уязвимости** (vuln): в информации об уязвимостях могут содержаться артефакты;

— **Хранилище** (storage): файлы могут определяться как вредоносные;

— **Агенты**, **Агент** (agents): из-за виджета сканера уязвимостей на экране **Агент**;

— **Терминал** (terminal): внутри команд могут содержаться артефакты;

— **Главная страница** (dashboard): в некоторых местах могут быть артефакты (например, топ-10 модулей);

— экраны наборов и элементов (config-set, config-item): внутри элементов наборов могут содержаться артефакты.

Список экранов приложения, где вероятность срабатывания можно считать нулевой:

— **Администрирование** (administration);

— Профиль пользователя (user-profile);

— **Группы** (groups);

— **Верификация** (verification);

— **Графики** (charts);

— **Дистрибутивы** (distributions);

— **Лицензия** (license);

— экраны профилей (profile);

— экраны множеств профилей и наборов (profiles, config-sets);

— экран сброса пароля (reset-password).

Важно

Для полного исключения ложных срабатываний антивирусных средств при работе с веб-приложением EDR целесообразно добавить в исключения соответствующий домен/адрес полностью: <host/ip>/*.

6. Ролевая модель

6.1 Общая информация

При развертывании сервера в Программе формируется пользователь с администраторскими правами, который может создавать группы прав для других пользователей, назначая для них произвольный набор прав.

В разделе **Пользователи и роли** во вкладке **Роли** администратор может создать группу прав и добавить в нее пользователей, которые будут наделены соответствующими группе правами.

При нажатии кнопки **Создать роль,** администратору необходимо выбрать в открывшемся окне, какие права будут назначены группе пользователей. Обязательным при назначении группы прав является определение ее имени. После назначения всех прав, необходимых для выбранной группы, администратору следует нажать кнопку **Создать** для создания группы.

На странице **Пользователи и роли** вкладки **Роли** администратор может выполнить следующие операции с группой:

1) Редактировать группу прав ( );
2) Добавить пользователей в группу прав ( );
3) Исключить пользователей из группы прав ( );
4) Удалить группу прав ( ).

6.2 Основные роли

Требования к ролевой модели пользователей, взаимодействующих с программой основаны на требованиях, изложенных в документе «Требования по безопасности информации к средствам обнаружения и реагирования на уровне узла, утвержденные приказом ФСТЭК России от 26 февраля 2025 № 58» и полностью удовлетворяют им.

Всех пользователей, взаимодействующих с Программой, можно распределить по следующим функциональным ролям:

– Администратор безопасности;

– Администратор;

– Аналитики L1;

— Аналитики L2;

— Аналитики L3;

— Наблюдатель;

— Оператор поиска угроз;

— Роль с доступом к терминалу реагирования и файлам агентов.

Распределение по ролям производится на основании наличия или отсутствия определенных прав, что в свою очередь дает возможность гибкой настройки вектора действий в рамках каждой роли.

6.3 Роль «Администратор безопасности»

6.3.1. Назначение роли

Администратор безопасности — это роль с максимальным уровнем привилегий в RT Protect EDR. Она предназначена для специалиста, который несёт полную ответственность за защиту инфраструктуры: от развёртывания и настройки системы до расследования инцидентов, реагирования на угрозы и контроля аудита безопасности.

В отличие от роли «Администратор», администратору безопасности дополнительно предоставляется полный набор прав по работе с журналом безопасности. Доступны не только просмотр, но и управление журналом и настройка состава регистрируемых событий аудита. Таким образом, роль обладает полным набором прав системы без каких-либо ограничений.

6.3.2. Основные задачи администратора безопасности

Основные задачи администратора безопасности представлены в следующем списке:

— управление агентами и их обновление на защищаемых узлах;

— настройка аналитики, профилей и наборов правил обнаружения угроз;

— расследование и обработка инцидентов безопасности;

— реагирование на угрозы через терминал реагирования и сценарии реагирования;

— настройка интеграций (TI, LDAP, локальная среда проверки файлов, экспорт событий);

— управление учётными записями пользователей, их ролями и правами;

— полное управление журналом безопасности: просмотр, администрирование и настройка состава регистрируемых событий аудита;

— контроль состояния системы с помощью диагностики;

— управление лицензией продукта.

6.3.3. Права роли по разделам

В таблице 10 приведён полный перечень прав, назначенных роли «Администратор безопасности», в соответствии с настройками системы. Роли предоставлены все права во всех разделах. Знаком «✓» отмечены предоставленные права.

Таблица 10 – Права для роли администратор безопасности

Раздел	Право	Доступ
Пользователи	Изменение пароля своей учётной записи	✓
	Доступ к разделу «Пользователи и роли»	✓
	Создание учётных записей пользователей	✓
	Управление правами пользователей	✓
	Управление учётными записями пользователей	✓
Планировщик задач	Управление планировщиком задач	✓
	Включение/выключение сценариев и задач	✓
	Использование сценариев реагирования	✓
Реагирование	Доступ к терминалу реагирования	✓
	Доступ к файлам, загруженным с агентов	✓
Журнал безопасности	Доступ к журналу безопасности	✓
	Управление журналом безопасности	✓
	Выбор событий, регистрируемых в журнале безопасности	✓
Диагностическая информация	Диагностика системы	✓
Агенты	Управление агентами	✓
Обновление агентов	Управление обновлением ПО агентов	✓
Интеграции	Настройка интеграции с TI	✓
	Настройка интеграции с локальной средой проверки файлов	✓
	Настройка интеграции с LDAP	✓
	Настройка экспорта событий журнала безопасности	✓
	Настройка экспорта событий мониторинга	✓
Аналитика	Доступ к аналитике	✓

	Управление наборами и конфигурациями	✓
	Изменение аналитики и профилей	✓
	Включение/выключение элементов аналитики	✓
Инциденты	Управление инцидентами	✓
	Ограниченное управление инцидентами	✓
Лицензия	Управление лицензией	✓

6.3.4. Отличие от роли «Администратор»

Набор прав администратора безопасности полностью включает права роли «Администратор» и расширяет их за счёт двух дополнительных прав в разделе «Журнал безопасности»:

– управление журналом безопасности — изменение, очистка и иное администрирование записей аудита.

– выбор событий, регистрируемых в журнале безопасности — настройка состава регистрируемых событий аудита.

Эти права делают администратора безопасности ответственным за полный цикл работы с аудитом безопасности системы. В связи с этим роль следует назначать ограниченному кругу доверенных сотрудников.

6.4 Роль «Администратор»

6.4.1. Назначение роли

Администратор — это основная привилегированная роль, предназначенная для специалиста, отвечающего за развёртывание, настройку и повседневную эксплуатацию системы. Роль объединяет в себе функции управления инфраструктурой защиты и работы с угрозами: администрирование агентов и их обновлений, настройку аналитики и интеграций, расследование инцидентов, реагирование на конечных устройствах, управление пользователями и лицензией.

Администратор обладает практически полным набором прав в системе. Единственное ограничение касается работы с журналом безопасности: администратору доступен просмотр журнала, однако права на управление самим журналом и на выбор регистрируемых в нём событий ему не предоставляются. Это обеспечивает неизменность аудита действий администраторов и соответствует принципу разделения полномочий.

6.4.2. Основные задачи администратора

Основные задачи администратора представлены в следующем списке:

– управление агентами и их обновлением на защищаемых узлах;

– настройка аналитики, профилей и наборов правил обнаружения угроз;

– расследование и обработка инцидентов безопасности;

– реагирование на угрозы через терминал реагирования и сценарии реагирования;

– настройка интеграций (TI, LDAP, локальная среда проверки файлов, экспорт событий);

– управление учётными записями пользователей, их ролями и правами;

– контроль состояния системы с помощью диагностики и просмотра журнала безопасности;

– управление лицензией продукта.

6.4.3. Права роли по разделам

В таблице 11 приведён полный перечень прав, назначенных роли «Администратор», в соответствии с настройками системы. Знаком «✓» отмечены предоставленные права, знаком «–» – отсутствующие.

Таблица 11 – Права для роли администратора

Раздел	Право	Доступ
Пользователи	Изменение пароля своей учётной записи	✓
	Доступ к разделу «Пользователи и роли»	✓
	Создание учётных записей пользователей	✓
	Управление правами пользователей	✓
	Управление учётными записями пользователей	✓
Планировщик задач	Управление планировщиком задач	✓
	Включение/выключение сценариев и задач	✓
	Использование сценариев реагирования	✓
Реагирование	Доступ к терминалу реагирования	✓
	Доступ к файлам, загруженным с агентов	✓
Журнал безопасности	Доступ к журналу безопасности	✓
	Управление журналом безопасности	–
	Выбор событий, регистрируемых в журнале безопасности	–
Диагностическая информация	Диагностика системы	✓
Агенты	Управление агентами	✓
Обновление агентов	Управление обновлением ПО агентов	✓

Интеграции	Настройка интеграции с TI	✓
	Настройка интеграции с локальной средой проверки файлов	✓
	Настройка интеграции с LDAP	✓
	Настройка экспорта событий журнала безопасности	✓
	Настройка экспорта событий мониторинга	✓
Аналитика	Доступ к аналитике	✓
	Управление наборами и конфигурациями	✓
	Изменение аналитики и профилей	✓
	Включение/выключение элементов аналитики	✓
Инциденты	Управление инцидентами	✓
	Ограниченное управление инцидентами	✓
Лицензия	Управление лицензией	✓

6.4.4. Ограничения роли

При практически полном наборе прав администратору не предоставляются следующие права в разделе «Журнал безопасности»:

– управление журналом безопасности — изменение, очистка и иное администрирование записей аудита.

– выбор событий, регистрируемых в журнале безопасности — настройка состава регистрируемых событий аудита.

Эти ограничения гарантируют, что действия администратора сами фиксируются в журнале аудита и не могут быть им скорректированы или скрыты. Управление журналом безопасности осуществляется администратором безопасноссти.

6.5 Роль «Аналитик L1»

6.5.1. Назначение роли

Аналитик первой линии — это операционная роль, предназначенная для специалиста, который выполняет первичный мониторинг, разбор (триаж) и обработку инцидентов безопасности. Это исполнительская роль дежурной смены центра мониторинга: аналитик первой линии работает с потоком срабатываний, квалифицирует инциденты и принимает по ним первичные меры реагирования в рамках предусмотренных сценариев.

Роль намеренно ограничена правами, необходимыми для повседневной работы с инцидентами и аналитикой. Аналитику первой линии не предоставляются права на администрирование инфраструктуры, изменение конфигурации обнаружения, настройку интеграций и управление пользователями. Это соответствует принципу минимальных привилегий и разделению функций между линиями мониторинга и администрированием системы.

6.5.2. Основные задачи аналитика первой линии

Основные задачи аналитика первой линии представлены в следующем списке:

- мониторинг и первичный разбор (триаж) поступающих инцидентов безопасности;
- обработка инцидентов, в том числе с использованием режима ограниченного управления;
- реагирование на угрозы с помощью готовых сценариев реагирования;
- включение и выключение сценариев и задач планировщика;
- работа с файлами, загруженными с агентов, в ходе расследования;
- просмотр журнала безопасности и использование диагностики системы;
- работа с аналитикой: доступ к разделу и включение/выключение элементов аналитики.

6.5.3. Права роли по разделам

В таблице 12 приведён полный перечень прав, назначенных роли «Аналитик первой линии», в соответствии с настройками системы. Знаком «✓» отмечены предоставленные права, знаком «–» – отсутствующие.

Таблица 12 – Права для роли аналитика первой линии

Раздел	Право	Доступ
Пользователи	Изменение пароля своей учётной записи	✓
	Доступ к разделу «Пользователи и роли»	–
	Создание учётных записей пользователей	–
	Управление правами пользователей	–
	Управление учётными записями пользователей	–
Планировщик задач	Управление планировщиком задач	–
	Включение/выключение сценариев и задач	✓
	Использование сценариев реагирования	✓

Реагирование	Доступ к терминалу реагирования	–
	Доступ к файлам, загруженным с агентов	✓
Журнал безопасности	Доступ к журналу безопасности	✓
	Управление журналом безопасности	–
	Выбор событий, регистрируемых в журнале безопасности	–
Диагностическая информация	Диагностика системы	✓
Агенты	Управление агентами	–
Обновление агентов	Управление обновлением ПО агентов	–
Интеграции	Настройка интеграции с TI	–
	Настройка интеграции с локальной средой проверки файлов	–
	Настройка интеграции с LDAP	–
	Настройка экспорта событий журнала безопасности	–
	Настройка экспорта событий мониторинга	–
Аналитика	Доступ к аналитике	✓
	Управление наборами и конфигурациями	–
	Изменение аналитики и профилей	–
	Включение/выключение элементов аналитики	✓
Инциденты	Управление инцидентами	✓
	Ограниченное управление инцидентами	✓
Лицензия	Управление лицензией	–

6.5.4. Ограничения роли

Аналитику первой линии не предоставляются административные права. В частности, роль не позволяет:

— управлять учётными записями пользователей, их правами и ролями (доступен только раздел смены собственного пароля);

— управлять агентами и их обновлением;

— настраивать интеграции (TI, LDAP, локальная среда проверки файлов, экспорт событий);

— изменять аналитику и профили, управлять наборами и конфигурациями обнаружения;

— использовать терминал реагирования и управлять планировщиком задач;

— управлять журналом безопасности и составом регистрируемых событий;

— управлять лицензией продукта.

Такой набор прав позволяет аналитику первой линии эффективно работать с инцидентами и аналитикой, не затрагивая настройки системы. Задачи, требующие более широких полномочий передаются аналитикам следующей линии или администраторам:

— изменение правил обнаружения;

— активное реагирование через терминал;

— эскалация (передача инцидента на более высокий уровень компетенции) сложных инцидентов.

6.6 Роль «Аналитик L2»

6.6.1. Назначение роли

Аналитик второй линии — это операционная роль, предназначенная для специалиста, который выполняет углублённое расследование инцидентов безопасности и активное реагирование на угрозы. Аналитик второй линии принимает в работу инциденты, эскалированные первой линией, проводит детальный анализ, применяет активные меры реагирования на конечных устройствах и развивает правила обнаружения угроз.

По сравнению с аналитиком первой линии роль обладает расширенными правами: полный доступ к терминалу реагирования, управление планировщиком задач, управление агентами и полный набор прав по работе с аналитикой (изменение правил, профилей, наборов и конфигураций обнаружения). При этом роль не включает административные функции — управление пользователями, обновление агентов, настройку интеграций, управление журналом безопасности и лицензией.

6.6.2. Основные задачи аналитика второй линии

Основные задачи аналитика второй линии представлены в следующем списке:

— углублённое расследование инцидентов, эскалированных первой линией;

— полное управление инцидентами, включая режим ограниченного управления;

— активное реагирование на угрозы через терминал реагирования и сценарии реагирования;

— управление планировщиком задач, включение/выключение сценариев и задач;

— управление агентами на защищаемых узлах;

— развитие обнаружения: управление наборами и конфигурациями, изменение аналитики и профилей, включение/выключение элементов аналитики;

– работа с файлами, загруженными с агентов, просмотр журнала безопасности и диагностика системы.

6.6.3. Права роли по разделам

В таблице 13 приведён полный перечень прав, назначенных роли «Аналитик второй линии», в соответствии с настройками системы. Знаком «✓» отмечены предоставленные права, знаком «–» – отсутствующие.

Таблица 13 – Права для роли аналитика второй линии

Раздел	Право	Доступ
Пользователи	Изменение пароля своей учётной записи	✓
	Доступ к разделу «Пользователи и роли»	–
	Создание учётных записей пользователей	–
	Управление правами пользователей	–
	Управление учётными записями пользователей	–
Планировщик задач	Управление планировщиком задач	✓
	Включение/выключение сценариев и задач	✓
	Использование сценариев реагирования	✓
Реагирование	Доступ к терминалу реагирования	✓
	Доступ к файлам, загруженным с агентов	✓
Журнал безопасности	Доступ к журналу безопасности	✓
	Управление журналом безопасности	–
	Выбор событий, регистрируемых в журнале безопасности	–
Диагностическая информация	Диагностика системы	✓
Агенты	Управление агентами	✓
Обновление агентов	Управление обновлением ПО агентов	–
Интеграции	Настройка интеграции с TI	–
	Настройка интеграции с локальной средой проверки файлов	–
	Настройка интеграции с LDAP	–
	Настройка экспорта событий журнала безопасности	–
	Настройка экспорта событий мониторинга	–
Аналитика	Доступ к аналитике	✓
	Управление наборами и конфигурациями	✓
	Изменение аналитики и профилей	✓
	Включение/выключение элементов аналитики	✓
Инциденты	Управление инцидентами	✓

	Ограниченное управление инцидентами	✓
Лицензия	Управление лицензией	–

6.6.4. Отличие от роли «Аналитик первой линии»

Аналитик второй линии располагает всеми правами первой линии и дополнительно получает следующие права:

– доступ к терминалу реагирования – активное реагирование на конечных устройствах.

– управление планировщиком задач – создание и настройка задач планировщика.

– управление агентами – администрирование агентов на защищаемых узлах.

– управление наборами и конфигурациями и изменение аналитики и профилей – развитие правил обнаружения угроз.

6.6.5. Ограничения роли

Аналитику второй линии по-прежнему не предоставляются административные права:

– управление учётными записями пользователей, их правами и ролями;

– управление обновлением ПО агентов;

– настройка интеграций (TI, LDAP, локальная среда проверки файлов, экспорт событий);

– управление журналом безопасности и составом регистрируемых событий;

– управление лицензией продукта.

Эти задачи относятся к компетенции администратора или администратора безопасности и выходят за рамки функций линии мониторинга.

6.7 Роль «Аналитик L3»

6.7.1. Назначение роли

Аналитик третьей линии — это операционная роль с наивысшим уровнем экспертизы среди линий мониторинга. Роль предназначена для ведущего специалиста, который занимается наиболее сложными расследованиями, проактивным поиском угроз (threat hunting), развитием правил обнаружения и сопровождением парка агентов, включая управление их обновлением.

Аналитик третьей линии располагает всеми правами аналитика второй линии и дополнительно получает право на управление обновлением ПО агентов. Таким образом, роль охватывает полный цикл работы с угрозами и сопровождения агентов на конечных устройствах. При этом административные функции — управление пользователями, настройка интеграций, управление журналом безопасности и лицензией в роль не входят.

6.7.2. Основные задачи аналитика третьей линии

Основные задачи аналитика третьей линии представлены в следующем списке:

– расследование наиболее сложных инцидентов и проактивный поиск угроз;

– полное управление инцидентами, включая режим ограниченного управления;

– активное реагирование через терминал реагирования и сценарии реагирования;

– управление планировщиком задач, включение/выключение сценариев и задач;

– управление агентами и управление обновлением ПО агентов на защищаемых узлах;

– развитие обнаружения: управление наборами и конфигурациями, изменение аналитики и профилей, включение/выключение элементов аналитики;

– работа с файлами, загруженными с агентов, просмотр журнала безопасности и диагностика системы.

6.7.3. Права роли по разделам

В таблице 14 приведён полный перечень прав, назначенных роли «Аналитик третьей линии», в соответствии с настройками системы. Знаком «✓» отмечены предоставленные права, знаком «–» – отсутствующие.

Таблица 14 – Права для роли аналитика третьей линии

Раздел	Право	Доступ
Пользователи	Изменение пароля своей учётной записи	✓
	Доступ к разделу «Пользователи и роли»	–
	Создание учётных записей пользователей	–
	Управление правами пользователей	–
	Управление учётными записями пользователей	–

Планировщик задач	Управление планировщиком задач	✓
	Включение/выключение сценариев и задач	✓
	Использование сценариев реагирования	✓
Реагирование	Доступ к терминалу реагирования	✓
	Доступ к файлам, загруженным с агентов	✓
Журнал безопасности	Доступ к журналу безопасности	✓
	Управление журналом безопасности	–
	Выбор событий, регистрируемых в журнале безопасности	–
Диагностическая информация	Диагностика системы	✓
Агенты	Управление агентами	✓
Обновление агентов	Управление обновлением ПО агентов	✓
Интеграции	Настройка интеграции с TI	–
	Настройка интеграции с локальной средой проверки файлов	–
	Настройка интеграции с LDAP	–
	Настройка экспорта событий журнала безопасности	–
	Настройка экспорта событий мониторинга	–
Аналитика	Доступ к аналитике	✓
	Управление наборами и конфигурациями	✓
	Изменение аналитики и профилей	✓
	Включение/выключение элементов аналитики	✓
Инциденты	Управление инцидентами	✓
	Ограниченное управление инцидентами	✓
Лицензия	Управление лицензией	–

6.7.4. Отличие от роли «Аналитик второй линии»

Аналитик третьей линии располагает всеми правами второй линии и дополнительно получает одно право:

– управление обновлением ПО агентов — планирование и установка обновлений программного обеспечения агентов на защищаемых узлах.

Это право позволяет аналитику третьей линии самостоятельно сопровождать парк агентов в части обновлений, не привлекая администратора.

6.7.5. Ограничения роли

Аналитику третьей линии по-прежнему не предоставляются административные права:

— управление учётными записями пользователей, их правами и ролями;

— настройка интеграций (TI, LDAP, локальная среда проверки файлов, экспорт событий);

— управление журналом безопасности и составом регистрируемых событий;

— управление лицензией продукта.

Эти задачи относятся к компетенции администратора или администратора безопасности и выходят за рамки функций линии мониторинга.

6.8 Роль «Наблюдатель»

Наблюдатель — это роль с минимальным уровнем привилегий в системе RT Protect EDR. Его основная функция и возможности заложены в самом названии роли. Наблюдатель может только просматривать некоторые разделы сервера управления, но не вмешиваться или как-то влиять на его работу. Основные возможности наблюдателя:

— просмотр графической информации на Главной странице;

— просмотр инцидентов;

— просмотр событий на странице **Активность**;

— просмотр агрегаций в разделе **Обзор событий**;

— просмотр артефактов TI;

— просмотр информации раздела **Управление** (агенты, группы, конфигурации, задачи и т.д)

— просмотр исключений и профилей безопасности агентов;

— просмотр загруженных дистрибутивов, информации о лицензии и настройках elasticsearch.

6.9 Роль «Оператор поиска угроз»

Оператор поиска угроз — это узкоспециализированная операционная роль в системе RT Protect EDR. Роль предоставляет пользователю возможность работать с инцидентами в режиме ограниченного управления, а также изменять пароль собственной учётной записи. Иных функциональных прав роли не предоставлено.

Оператор поиска угроз — это «регистратор» инцидентов: он проактивно ищет угрозы на странице **Активность**, заводит новые инциденты (всегда в статусе «Новый», без владельца) и может дорабатывать/комментировать именно их, пока они новые. Как только инцидент берут в работу аналитики с

полным правом работы с инцидентами (назначают владельца и переводят в статус «Назначен»), оператор теряет к нему доступ на редактирование. Передать инцидент кому-то напрямую, назначить ответственного или взять инцидент на себя он не может. Это позволяет отделить поиск/регистрацию от ведения инцидента.

6.10 Роль с доступом к терминалу реагирования и файлам агентов

Роль в RT Protect EDR, сфокусированная исключительно на реагировании на конечных устройствах. В соответствии с приведённой конфигурацией прав роль предоставляет пользователю два права из раздела «Реагирование»: доступ к терминалу реагирования и доступ к файлам, загруженным с агентов. Иных функциональных прав роли не предоставлено.

Роль предназначена для специалиста, который выполняет активные действия по реагированию на угрозы на защищаемых узлах — подключается к терминалу реагирования и работает с файлами, полученными с агентов в ходе расследования. При этом оператор не имеет доступа к управлению инцидентами, аналитике, настройкам системы и администрированию, что соответствует принципу минимальных привилегий и чёткому разделению функций.

Так как пользователь в RT Protect EDR может обладать набором из нескольких ролей, то удобно добавлять эту роль доверенным специалистам первой линии, так как роль аналитиков первой линии не подразумевает наличие прав терминального реагирования.

6.11 Права, предоставляемые пользователям

В списке доступных для назначения прав представлены права, описанные в таблице 15.

Таблица 15 – Список прав, назначаемых пользователям

Право пользователя	Описание
Пользователи	
Доступ к разделу Пользователи и роли	**Обязательное право.** Отсутствие данного права делает разделы «Пользователи и роли» недоступным для пользователя. Если обязательное право будет не выбрано, то дочерние права будут недоступны.

Право пользователя		Описание
	Создание учетных записей пользователей	Данное право зависит от обязательного права «Доступ к разделу пользователи и роли». При включенном обязательном праве, данное право будет разблокировано, в ином случае данное право будет заблокировано для изменений. При отсутствии данного права у пользователя отключается возможность регистрации новых пользователей в системе. При этом доступность других операций определяется отдельными правами. При наличии данного права пользователю автоматически добавляются права управления учетными записями и правами пользователей.
	Управление учетными записями пользователей	Данное право зависит от обязательного права «Доступ к разделу пользователи и роли». При включенном обязательном праве, данное право будет разблокировано, в ином случае данное право будет заблокировано для изменений. Также данное право зависит от права «Создание учетных записей пользователей». При включенном праве «Создание учетных записей пользователей», данное право будет автоматически включено и заблокировано для изменений.
	Управление правами пользователей	Данное право зависит от обязательного права «Доступ к разделу пользователи и роли». При включенном обязательном праве, данное право будет разблокировано, в ином случае данное право будет заблокировано для изменений. Также данное право зависит от права «Создание учетных записей пользователей». При включенном праве «Создание учетных записей пользователей», данное право будет автоматически включено и заблокировано для изменений.
Изменение пароля своей учетной записи		При отсутствии данного права у пользователя пропадает возможность сброса пароля своей УЗ. В таком случае пароль ему может сменить другой пользователь, имеющий право управления пользователями.
Планировщик задач		
Управление планировщиком задач		Основное право. При включенном основном праве, дочерние права автоматически будут включены и заблокированы для изменений.
Включение/выключение сценариев и задач		Данное право зависит от права «Управление планировщиком задач». При включенном праве «Управление планировщиком задач», данное право автоматически будет включено и заблокировано для изменений.

Право пользователя	Описание
Использование сценариев реагирования	Данное право зависит от права «Управление планировщиком задач». При включенном праве «Управление планировщиком задач», данное право автоматически будет включено и заблокировано для изменений.
Реагирование	
Право доступа к терминалу реагирования	При отсутствии данного права следующие возможности становятся недоступными: - открытие live-сессии с агентом; - API «старого» терминала.
Право доступа к файлам, загруженным с агентов	При отсутствии данного права у пользователя отключается возможность тем или иным способом получать содержимое и имена файлов, загруженных в Хранилище с агентов, включая скачивание одного файла или нескольких (в виде архива) файлов, получение ссылки на скачивание, просмотр, отправка в TI. Также исключается возможность удаления файлов, загруженных с агентов, из Хранилища. При этом сохраняется возможность полноценной работы с пользовательскими файлами, т.е. с файлами, предназначенными для скачивания с сервера (вкладка «Загрузка файлов в Хранилище»). В разделе «Хранилище»: - исключаются вкладки Файлы с агентов и «Задачи по загрузке архивов». В разделе «Планировщик задач»: - исключается возможность работы с файлами, загруженными в рамках задачи.
Журнал безопасности	
Доступ к журналу безопасности	Обязательное право. Если обязательное право не выбрано, то дочерние права будут недоступны. При отсутствии данного права у пользователя блокируется возможность любого доступа к журналу безопасности. Раздел «Журнал безопасности» исключается целиком из интерфейса. При наличии данного права в дополнение к нему подразумевается наличие списка (вектора) типов событий, которые доступны пользователю в разделе «Журнал безопасности».
Управление журналом безопасности	Зависит от обязательного права «Доступ к журналу безопасности». При включенном обязательном праве данное право будет разблокировано, в ином случае данное право будет заблокировано для изменений.

Право пользователя	Описание
Выбор событий, регистрируемых в журнале безопасности	Зависит от обязательного права «Доступ к журналу безопасности». При включенном обязательном праве данное право будет разблокировано, в ином случае данное право будет заблокировано для изменений.
Диагностическая информация	
Диагностика системы	При отсутствии данного права у пользователя отключается функционал предоставления статуса «здоровья» сервера и агента (check-engine), а также пропадает возможность выборки агентов по фильтру Проблемный. Возможность найти проблемных агентов иными способами (например, через DSL) не зависит от данного права.
Обновление агентов	
Управление обновлением ПО Агентов	При отсутствии права следующий функционал отключается (кнопки и переключатели скрываются или переходит в read-only режим, текстовые поля переходят в read-only режим): – загрузка, скачивание, удаление дистрибутивов обновления агентского ПО; – изменение параметра автообновления агента. На странице **Агенты** отсутствует переключатель **Автообновление**. На странице **Дистрибутивы** отсутствуют: - кнопка **Загрузить** дистрибутив; - столбец **Управление** в таблице дистрибутивов.
Агенты	
Управление агентами	При отсутствии права следующий функционал отключается (кнопки и переключатели скрываются или переходят в read-only режим, текстовые поля переходя в read-only режим): – изменение имени агента; – изменение критичности агента; – изменение группы агента; – создание, удаление, редактирование групп агентов; – возможность верификации и удаления (деверификации) агентов; – управление защитой агента; – управление золотым образом агента; – управление защитой от удаления агента; – изменение описания агента. **Страница Агент:** – Имя агента; – Критичность агента; – кнопка **Удалить агента**;

Право пользователя	Описание
	– переключатель **Защита**; – кнопка **Управление** в блоке **Золотой образ**; – переключатель **Защита от удаления**; – управление группой агента; – блок **Описание агента**. **Страница Агенты:** – кнопки управления группами агентов; – кнопка удаления агентов; – кнопки управления изоляций, защитой, защитой от удаления, золотым образом; – кнопка изменения критичности агента. **Страница Группы:** – кнопка **Создать группу**; – кнопка **Удалить выбранные**; – столбец **Управление в таблице групп** (редактирование, удаление). **Страница Верификация:** – кнопка **Верифицировать выбранных**.
Интеграции	
Настройка интеграции с TI	Данное право подразумевает возможность изменения настройки интеграции с TI в разделе **Интеграции**.
Настройка интеграции с локальной средой проверки файлов	Данное право подразумевает возможность изменения настройки интеграции с локальной средой проверки файлов в разделе **Интеграции**.
Настройка интеграции с LDAP	Данное право подразумевает возможность изменения настройки интеграции с LDAP в разделе **Интеграции.**
Настройка экспорта событий журнала безопасности	Данное право зависит от обязательного права «Доступ к журналу безопасности». При включенном обязательном праве, данное право будет разблокировано, в ином случае данное право будет заблокировано для изменений. Данное право подразумевает возможность изменения настройки экспорта событий в разделе **Интеграции.**
Настройка экспорта событий мониторинга	Данное право подразумевает возможность изменения настройки интеграции с SIEM для экспорта событий мониторинга в разделе **Интеграции**.
Аналитика	
Доступ к аналитике	**Обязательное право.** Если обязательное право будет не выбрано, то дочерние права будут недоступны.

Право пользователя	Описание
	При отсутствии данного права пользователю становятся недоступны любые операции модификации, касающиеся аналитики, исключений, профилей и конфигураций. В части аналитики (т.е. ИА, ИК, YARA и Журналы) и профилей USB и Антишифра «закрываются» операции чтения содержимого наборов (профилей), а соответствующие одноименные разделы при этом полностью исключаются из интерфейса. При этом все же остается доступным вызов set перечисления наборов, необходимый для визуализации бейджа набора (имя, признак TI и т.д.) в конфигурации агента на странице Агент и др. местах. Также в режиме «только чтение» остаются доступными исключения (всех типов) и профиль безопасности агента. При наличии данного права у пользователя все разделы аналитики, исключений и профилей становятся доступны, при этом для исключений допускаются операции модификации, а аналитика и профили работают в режиме «только чтение» - доступность операций модификации определяется другими правами. Логика выключения данного функционала уже заложена у нас в роли Оператора поиска угроз и включает в себя следующее: - из сайд бара исключается раздел Аналитика (Исключения и Профили остаются доступными); - возможность перехода на недоступные элементы аналитики (ИА, ИК, YARA-правила) исключается (страницы Активность, Инциденты, Инцидент, Обзор событий, возможно еще где-то, нужно все места найти). При этом сохраняется возможность перехода к исключениям; - раздел Конфигурации сохраняется, но работает в режиме «только чтение»; - на странице Агент блок Конфигурации также работает в режиме «только чтение»; - со страницы Агенты также убирается возможность применения конфигурации; - в раскрывашке агента на странице Агенты убираются ссылки на разделы аналитики и профилей.
Управление наборами и конфигурациями	Зависит от обязательного права «Доступ к аналитике». При включенном обязательном праве, данное право будет разблокировано, в ином случае данное право будет заблокировано для изменений.
Изменение аналитики и профилей	При включенном обязательном праве, данное право будет разблокировано, в ином случае данное право будет заблокировано для изменений.
Включение/выключение элементов аналитики	При включенном обязательном праве, данное право будет разблокировано, в ином случае данное право будет заблокировано для изменений.

Право пользователя	Описание
	Также данное право зависит от права «Изменение аналитики и профилей». При включенном праве «Изменение аналитики и профилей» данное право автоматически будет включено и заблокировано для изменений.
Инциденты	
Управление инцидентами	При наличии данного права весь раздел Инциденты работает без ограничений. При этом право ограниченного управления инцидентами включено автоматически. При отсутствии данного права управление инцидентами регулируется правом ограниченного доступа к инцидентам – либо в режиме оператора поиска угроз (если право есть), согласно существующей схеме ограничений для этой роли, либо в режиме «только чтение» (если права нет).
Ограниченное управление инцидентами	Зависит от права «Управление инцидентами». При включенном основном праве, данное право автоматически будет включено и заблокировано для изменений. При отсутствии данного права, пользователю запрещены какие-либо модифицирующие действия с инцидентами. Раздел Инциденты и карточка инцидента работают в режиме «только чтение».
Лицензия	
Управление лицензией	При отсутствии данного права отключается возможность загрузки новой лицензии в разделе **Лицензия**. Доступ к просмотру параметров текущей лицензии не ограничивается.

7. Модель данных в RT Protect EDR

7.1 Общие сведения

События, зарегистрированные агентом, отправляются на сервер в формате JSON. Отправка событий с агента осуществляется блоками. Каждый блок содержит заголовок и массив событий разного типа. Каждое событие включает в себя 2 набора полей – общий набор и набор, специфичный для определенного вида события. Полный список полей событий и их JSON-представления, которые могут быть применены для написания DSL-запросов или индикаторов атак, представлен в таблице 16.

Таблица 16 – Общий список полей событий

Назначение	Тип данных	JSON	Подсистема
Тип события	enum	**t**	Общая
Время регистрации события	timestamp	**time**	Общая
Действие, связанное с событием	enum	**act**	Общая
Причина предпринятого действия	enum	**rsn**	Общая
Правило, относящееся к событию	string	**rul**	Общая
Идентификатор техники/тактики MITRE	string	**mitre**	Общая
Критичность (уровень важности) события	enum	**svrt** (по умолчанию: 0)	Общая
Уникальный идентификатор процесса	int (индекс в массиве GUID'ов)	**uuid**	Общая
Уникальный идентификатор группы процессов	int (индекс в массиве GUID'ов)	**hid**	Общая
Уникальный идентификатор корреляции событий	string (индекс в массиве GUID'ов)	**cid**	Общая
Идентификатор процесса на агентской системе	unsigned	**pid**	Общая
Идентификатор родительского процесса на агентской системе	unsigned	**ppid**	Общая
Полное имя исполняемого файла процесса	string MANGLED	**app**	Общая
Командная строка процесса	string	**cmdl**	Общая
Номер сессии, в которой работает процесс на агентской системе	unsigned	**sess** (по умолчанию: 0)	Общая
SID пользователя, создавшего процесс	string	**sid**	Общая
Издатель ЭП исполняемого файла процесса	string	**app_sgnr**	Общая
Имя пользователя, запустившего процесс	string	**usr**	Общая
Домен (имя компьютера) пользователя, запустившего процесс	string	**dom**	Общая
Подтип события	enum	**st**	Общая

Назначение	Тип данных	JSON	Подсистема
Поведенческие признаки процесса (первая группа)	uint64	**rf0**	Общая
Поведенческие признаки процесса (вторая группа)	uint64	**rf1**	Общая
Флаги исполняемого файла процесса	int64	**exclf**	Общая
Исключения для программ, назначенные процессу	string	**excls**	Общая
Синтетическое событие (принимает значения true или false)	int (0/1)	**syn**	Общая
Версия события	unsigned	**efmt**	Общая
Протокол	enum	**proto**	Сеть
Признак работы по IPv6 (принимает значения true или false)	int (0/1)	**ipv6**	Сеть
Уникальный идентификатор сетевого потока	string (индекс в массиве GUID'ов в текстовой форме)	**fluuid**	Сеть
Идентификатор сетевого потока	int64	**flow**	Сеть
Отправка или прием (принимает значения true или false)	int (0/1)	**out**	Сеть
Размер полезных данных (payload) сетевого пакета	int64	**size**	Сеть
Имя хоста, соответствующее удаленному IP-адресу	string	**host**	Сеть
Тип DNS-запроса	enum	**dnsq_t**	Сеть
Статус DNS-запроса	unsigned	**dnsq_s**	Сеть
Результат DNS-запроса	string	**dnsq_r**	Сеть
Имя хоста из DNS-запроса	string	**dnsq_h**	Сеть
Идентификатор транзакции DNS-обмена	unsigned	**dns_trx**	Сеть
Имя хоста (server_name) из сообщения SSL Client Hello	string	**ssl_h**	Сеть
Удаленный IP-адрес	string	**r_ip**	Сеть
Удаленный порт	unsigned	**r_p**	Сеть
Локальный IP-адрес	string	**l_ip**	Сеть
Локальный порт	unsigned	**l_p**	Сеть
Исключение для удаленного IP-адреса	unsigned	**r_ip_excl**	Сеть
Исключение для имени хоста, соответствующего удаленному IP-адресу	unsigned	**h_excl**	Сеть
Исключение для имени хоста в запросе	unsigned	**rqh_excl**	Сеть
Тип ICMP-сообщения	unsigned (код или мнемоника)	**icmp_t**	Сеть
Код ICMP-сообщения	unsigned (код или мнемоника)	**icmp_c**	Сеть
Имя хоста в индикаторе компрометации	string	**ioc_h**	Сеть

Назначение	Тип данных	JSON	Подсистема
Флаги сетевого события	unsigned	**netf**	Сеть
Общий размер исходящих данных за время жизни подключения, байт	uint64	**o_sz**	Сеть
Общий размер входящих данных за время жизни подключения, байт	uint64	**i_sz**	Сеть
Время жизни подключения, в 100-наносекундных интервалах	uint64	**lt**	Сеть
Полное имя файла	string MANGLED	**name**	Файлы, Защита данных
Время создания файла	timestamp	**crtime**	Файлы, Процессы
Время последнего изменения файла	timestamp	**chtime**	Файлы, Процессы
Размер файла	int64	**fsize**	Файлы, Процессы
Тип файла	enum	**ftype**	Файлы, Процессы
Атрибуты файла	unsigned	**attr**	Файлы, Процессы
SHA-1 файла	string	**sha1**	Файлы, Процессы
MD5 файла	string	**md5**	Файлы, Процессы
SHA-256 файла	string	**sha256**	Файлы, Процессы
Imphash файла	string	**imphash**	Файлы, Процессы
Электронная подпись файла	string	**sgnr**	Файлы, Процессы
Статус электронной подписи файла	enum	**sgnr_s**	Файлы, Процессы
Признак доверенной электронной подписи файла	int (-/1)	**sgnr_t**	Файлы, Процессы
Оригинальное имя файла	string	**ofn**	Файлы, Процессы
Компания-издатель файла	string	**fcomp**	Файлы, Процессы
Версия файла	string	**fver**	Файлы, Процессы
Описание файла	string	**fdesc**	Файлы, Процессы
Продукт, к которому относится файл	string	**fprod**	Файлы, Процессы

Назначение	Тип данных	JSON	Подсистема
Тип упаковщика файла	string	**pack**	Файлы, Процессы
Файл находится в "белом" списке	int (-/1)	**fwhite**	Файлы, Процессы
Исключение для файла по хешу	string	**fh_excl**	Файлы, Процессы
Исключение для файла по имени	string	**fn_excl**	Файлы, Процессы
Файл расположен в директории автозапуска (принимает значения true или false)	int (0/1)	**arun**	Файлы
Новое имя файла	string MANGLED	**fnew**	Файлы, Защита данных
Файл был заменен (принимает значения true или false)	int (0/1)	**owrt**	Файлы
Предыдущее время создания файла	timestamp	**old_t**	Файлы
Новое время создания файла	timestamp	**new_t**	Файлы
Файл содержит атрибут "скрытый" (принимает значения true или false)	int (0/1)	**hdn**	Файлы
Файл содержит атрибут "системный" (принимает значения true или false)	int (0/1)	**sys**	Файлы
Операция совершается над альтернативным потоком данных файла (принимает значение только true)	int (-/1)	**ads**	Файлы
Для файла была создана резервная копия (принимает значение только true)	int (-/1)	**save**	Файлы
Доступ на удаление (принимает значение только true)	int (-/1)	**delete**	Файлы
Доступ на чтение (принимает значение только true)	int (-/1)	**read**	Файлы
Доступ на модификацию (принимает значение только true	int (-/1)	**modify**	Файлы
Обмен именами (принимает значение только true) (поле доступно только в ОС Linux)	int (-/1)	**nxchg**	Файлы
Имя альтернативного потока данных файла	string	**strm**	Файлы
SID предыдущего владельца файла	string	**own_old**	Файлы
Домен предыдущего владельца файла	string	**own_old_dom**	Файлы
Имя предыдущего владельца файла	string	**own_old_usr**	Файлы
Предыдущий владелец файла был задан по умолчанию	int (-/1)	**own_old_def**	Файлы
SID нового владельца файла	string	**own_new**	Файлы

Назначение	Тип данных	JSON	Подсистема
Домен нового владельца файла	string	**own_new_dom**	Файлы
Имя нового владельца файла	string	**own_new_usr**	Файлы
Новый владелец файла был задан по умолчанию	int (-/1)	**own_new_def**	Файлы
SID предыдущей основной группы владельца файла	string	**grp_old**	Файлы
Домен предыдущей основной группы владельца файла	string	**grp_old_dom**	Файлы
Имя предыдущей основной группы владельца файла	string	**grp_old_usr**	Файлы
Предыдущая основная группа владельца файла была задана по умолчанию	int (-/1)	**grp_old_def**	Файлы
SID новой основной группы владельца файла	string	**grp_new**	Файлы
Домен новой основной группы владельца файла	string	**grp_new_dom**	Файлы
Имя новой основной группы владельца файла	string	**grp_new_usr**	Файлы
Новая основная группа владельца файла была задана по умолчанию	int (-/1)	**grp_new_def**	Файлы
Предыдущий DACL файла	string	**dacl_old**	Файлы
Предыдущий DACL файла был задан по умолчанию	int (-/1)	**dacl_old_def**	Файлы
Новый DACL файла	string	**dacl_new**	Файлы
Новый DACL файла был задан по умолчанию	int (-/1)	**dacl_new_def**	Файлы
Предыдущий SACL файла	string	**sacl_old**	Файлы
Предыдущий SACL файла был задан по умолчанию	int (-/1)	**sacl_old_def**	Файлы
Новый SACL файла	string	**sacl_new**	Файлы
Новый SACL файла был задан по умолчанию	int (-/1)	**sacl_new_def**	Файлы
Предыдущая мандатная метка файла	unsigned	**mlbl_old**	Файлы
Предыдущая маска мандатной метки файла	unsigned	**mlbl_old_mask**	Файлы
Новая мандатная метка файла	unsigned	**mlbl_new**	Файлы
Новая маска мандатной метки файла	unsigned	**mlbl_new_mask**	Файлы
Код оповещения	enum	**detect**	Сеть, Файлы, Процессы, Реестр
Полное имя исполняемого модуля–инициатора операции	string MANGLED	**who**	Файлы, Процессы, Реестр
Идентификатор нити–инициатора операции	unsigned	**whotid**	Файлы,

Назначение	Тип данных	JSON	Подсистема
			Процессы, Реестр
Стартовый адрес нити–инициатора операции	uint64	**whoaddr**	Файлы, Процессы, Реестр
Флаги исполняемого модуля-инициатора операции	uint64	**whof**	Файлы, Процессы, Реестр
Исключения для программ, назначенные инициатору операции	string	**who_excls**	Сеть, Файлы, Процессы, Реестр
Стек вызовов операции	string	**trace**	Процессы
Командная строка родительского процесса	string	**cmdlp**	Процессы
Электронная подпись родительского процесса	string	**sgnrp**	Процессы
Командная строка прародителя (grand parent)	string	**cmdlg**	Процессы
Рабочий каталог процесса	string MANGLED	**wdir**	Процессы
Уровень защиты процесса	unsigned	**prot**	Процессы
Уровень доверия (integrity level) процесса	unsigned	**integ**	Процессы
Время создания процесса	timestamp	**when**	Процессы
Уникальный идентификатор родительского процесса	int (индекс в массиве GUID'ов)	**parent**	Процессы
Уникальный идентификатор процесса-создателя	int (индекс в массиве GUID'ов)	**caller**	Процессы
Идентификатор процесса-инициатора операции	unsigned	**cpid**	Процессы
Полное имя процесса-инициатора операции	string MANGLED	**cpath**	Процессы
Код завершения процесса	unsigned	**code**	Процессы
Уникальный идентификатор целевого процесса	int (индекс в массиве GUID'ов)	**targ**	Процессы
Полное имя целевого процесса	string MANGLED	**tpath**	Процессы
Идентификатор целевого процесса	unsigned	**tpid**	Процессы
Флаги образа целевого процесса	uint64	**targf**	Процессы
Поведенческие признаки целевого процесса (первая группа)	uint64	**trf0**	Процессы
Поведенческие признаки целевого процесса (вторая группа)	uint64	**trf1**	Процессы
Имя модуля целевой нити	string	**tmod**	Процессы
Имя функции целевой нити	string	**tfunc**	Процессы
Полное имя файла образа	string MANGLED	**path**	Процессы
Флаги нити	unsigned	**tf**	Процессы

Назначение	Тип данных	JSON	Подсистема
Флаги операции загрузки образа	unsigned	**ldf**	Процессы
Флаги образа	int64	**imgf**	Процессы
Базовый адрес образа	int64	**base**	Процессы
Размер образа	unsigned	**isize**	Процессы
Идентификатор целевой нити	unsigned	**tid**	Процессы
Стартовый адрес целевой нити	int64	**taddr**	Процессы
Запрашиваемые права	unsigned	**dsrd**	Процессы
Предоставленные права	unsigned	**grnt**	Процессы
Новый уровень защиты процесса	int	**prot1**	Процессы
Новая командная строка	string	**cmdl1**	Процессы
Идентификатор контейнера целевого процесса (только для агентов Linux)	string	**container**	Процессы
AMSI: имя содержимого	string	**amsi_cname**	Процессы
AMSI: содержимое	string	**amsi_data**	Процессы
AMSI: имя приложения	string	**amsi_appname**	Процессы
AMSI: ссылка на скачивание зарезервированного содержимого	string	**amsi_blink**	Процессы
Локальная сессия (принимает значения true или false)	int (0/1)	**local**	Сессии
Номер сессии	unsigned	**sess_id**	Сессии
Тип дистанционного управления	unsigned (опционально)	**sess_opt**	Сессии
Тип сессии	unsigned (опционально)	**sess_proto**	Сессии
Имя оконной станции	string	**win_stn**	Сессии
Имя клиента	string (опционально)	**sess_cl**	Сессии
IP-адрес клиента	string (опционально)	**sess_claddr**	Сессии
Имя пользователя	string (опционально)	**sess_usr**	Сессии
Имя домена\компьютера	string (опционально)	**sess_dom**	Сессии
Путь ключа	string	**key**	Реестр
Имя значения	string	**val_n**	Реестр
Тип данных значения	enum	**val_t**	Реестр
Размер данных значения	unsigned	**val_s**	Реестр
Данные значения	string	**val_d**	Реестр
Новое имя ключа	string	**new**	Реестр
Имя файла-источника загружаемой в реестр информации	string MANGLED	**src**	Реестр
Имя файла, в который записываются данные из реестра	string MANGLED	**dst**	Реестр
Ключ/значение относится к категории автозапуска (принимает значение только true)	int (-/1)	**asep**	Реестр

Назначение	Тип данных	JSON	Подсистема
WMI: Тип события	enum	**wmi**	Система: WMI
WMI: Путь	string	**wmi_pth**	Система: WMI
WMI: SID пользователя	string	**wmi_sid**	Система: WMI
WMI: Пространство имен	string	**ns**	Система: WMI
WMI: Путь до исполняемого файла	string MANGLED	**exe_path**	Система: WMI
WMI: Имя файла	string MANGLED	**fname**	Система: WMI
WMI: Имя фильтра событий	string	**wmi_nm**	Система: WMI
WMI: Строка запроса	string	**qstr**	Система: WMI
WMI: Имя файла скрипта	string MANGLED	**scrfname**	Система: WMI
WMI: Текст скрипта	string	**scrtxt**	Система: WMI
WMI: Имя источника	string MANGLED	**sname**	Система: WMI
WMI: SMTP	string	**smtp**	Система: WMI
WMI: Фильтр	string	**flt**	Система: WMI
WMI: Потребитель	string	**cnsm**	Система: WMI
WMI:Идентификатор процесса клиента	unsigned (по умолчанию 0)	**wmi_clpid**	Система: WMI
WMI: Уникальный идентификатор процесса клиента	int (индекс в массиве GUID'ов)	**wmi_cluuid**	Система: WMI
WMI: Время создания процесса клиента	timestamp	**wmi_cltime**	Система: WMI
WMI: Командная строка процесса клиента	string	**wmi_clcmdl**	Система: WMI
WMI: Локальный запрос (принимает значение только true)	int (-/1)	**wmi_local**	Система: WMI
WMI: Идентификатор созданного процесса	unsigned	**wmi_crpid**	Система: WMI
WMI: Уникальный идентификатор созданного процесса	int (индекс в массиве GUID'ов)	**wmi_cruuid**	Система: WMI
WMI: Время создания созданного процесса	timestamp	**wmi_crtime**	Система: WMI
WMI: Командная строка созданного процесса	string	**wmi_crcmdl**	Система: WMI
WMI: Имя машины, выполнившей запрос	string	**wmi_cl**	Система: WMI
WMI: FQDN машины, выполнившей запрос	string	**wmi_clfqdn**	Система: WMI
WMI: Имя пользователя клиента, выполнившего запрос	string	**wmi_usr**	Система: WMI
WMI: Имя домена клиента, выполнившего запрос	string	**wmi_dom**	Система: WMI
WMI: Имя вызываемого метода	string	**wmi_mthd**	Система: WMI
Новое время	timestamp	**new_stime**	Система: Изменение системного времени

Назначение	Тип данных	JSON	Подсистема
Предыдущее время	timestamp	**prev_stime**	Система: Изменение системного времени
Причина завершения	unsigned	**sht**	Система: Завершение работы
Уровень	unsigned	**e_lvl**	Журналы
Дополнительные данные	JSON object	**e_ex**	Журналы
Описание событий	string (опционально)	**e_msg**	Журналы
Блок информации **winlogbeat**	JSON object	**winlog**	Журналы
RPC: UUID интерфейса	int (индекс в массиве GUID'ов)	**rpc_id**	Вызовы: RPC
RPC: Номер процедуры	unsigned	**rpc_opnum**	Вызовы: RPC
RPC: Имя процедуры	string	**rpc_opname**	Вызовы: RPC
RPC: Протокол	unsigned	**rpc_proto**	Вызовы: RPC
RPC: Сервис аутентификации	unsigned	**rpc_authsvc**	Вызовы: RPC
RPC: Конечная точка	string	**endp**	Вызовы: RPC
RPC: Сетевой адрес	string (опционально)	**n_addr**	Вызовы: RPC
RPC: Уникальный идентификатор процесса клиента	int (индекс в массиве GUID'ов)	**c_uuid**	Вызовы: RPC
RPC: PID процесса клиента	unsigned	**c_pid**	Вызовы: RPC
RPC: Исполняемый файл процесса клиента	string MANGLED	**c_path**	Вызовы: RPC
RPC: Уникальный идентификатор процесса сервера	int (индекс в массиве GUID'ов)	**s_uuid**	Вызовы: RPC
RPC: PID процесса сервера	unsigned	**s_pid**	Вызовы: RPC
RPC: Исполняемый файл процесса сервера	string MANGLED	**s_path**	Вызовы: RPC
Количество открытий/созданий файлов с последующими обращениями к ним	unsigned	**cf_ac**	Защита файлов
Количество открытых файлов из защищаемых каталогов	unsigned	**cf_oc**	Защита файлов
Количество созданных процессом файлов после активации мониторинга	unsigned	**cf_cc**	Защита файлов
Количество удалённых файлов в защищаемых каталогах	unsigned	**si_dc**	Защита файлов
Количество переименованных файлов в защищаемых каталогах	unsigned	**si_rc**	Защита файлов
Количество перемещённых файлов в защищаемые каталоги	unsigned	**si_mi**	Защита файлов
Количество перемещённых файлов из защищаемых каталогов	unsigned	**si_mo**	Защита файлов

Назначение	Тип данных	JSON	Подсистема
Количество файлов из защищаемых каталогов, которые только читали	unsigned	ro_fc	Защита файлов
Количество файлов из защищаемых каталогов, в которые только писали	unsigned	wo_fc	Защита файлов
Количество файлов из защищаемых каталогов, которые читали и писали	unsigned	rw_fc	Защита файлов
Среднее значений файловой энтропии по чтению	unsigned	pr_re	Защита файлов
Среднее значений файловой энтропии по записи	unsigned	pr_we	Защита файлов
Правило блокировки процесса	unsigned	pr_lr	Защита файлов
Реакция модуля на идентификацию шифровальщика	unsigned	pr_ra	Защита файлов
Количество файлов с нарушенной целостностью	unsigned	a_fcc	Защита файлов
Количество файлов с превышенной энтропией	unsigned	a_eoc	Защита файлов
Количество расширений файлов, из которых читали	unsigned	exrac_	Защита файлов
Количество расширений файлов, в которые писали	unsigned	exwac_	Защита файлов
Количество уникальных расширений файлов, из которых только читали	unsigned	exurac	Защита файлов
Количество уникальных расширений файлов, в которые только писали	unsigned	exuwac	Защита файлов
Категории файлов, к которым осуществлялся доступ	unsigned	gf_am	Защита файлов
Категории файлов, из которых производилось чтение	unsigned	gf_rm	Защита файлов
Категории файлов, в которые производилась запись	unsigned	gf_wm	Защита файлов
Категории файлов, которые удалялись	unsigned	gf_dm	Защита файлов
Группа, к которой относится файл	unsigned	gf_ai	Защита файлов
Тип контролируемого устройства	unsigned	usb_dt	Контроль USB-устройств
Класс устройства	unsigned	usb_dc	Контроль USB-устройств
Подкласс устройства	unsigned	usb_dsc	Контроль USB-устройств
Идентификатор производителя	unsigned	usb_vid	Контроль USB-устройств
Идентификатор продукта	unsigned	usb_pid	Контроль USB-устройств

Назначение	Тип данных	JSON	Подсистема
Номер интерфейса	unsigned (опционально)	**usb_mi**	Контроль USB-устройств
Серийный номер	string	**usb_sn**	Контроль USB-устройств
Наименование производителя	string	**usb_mr**	Контроль USB-устройств
Наименование продукта	string	**usb_pt**	Контроль USB-устройств
Имя модуля, который был запущен с носителя	string	**usb_exec**	Контроль USB-устройств



Примечание

(-/1) в таблице обозначает, что событие можно будет найти в DSL-запросе, только в том случае, если такое событие придет в базу данных, то есть будет содержать значение **true**.

Типы событий представлены в таблице 17.

Таблица 17 – Типы событий (t)

Код типа	Описание типа
0	Сеть
1	Файлы
2	Реестр
3	Журналы
4	Процессы
5	Система
6	Сессии
7	Вызовы
8	Защита файлов

Поля общей части событий представлены в таблице 18.

Таблица 18 – Поля общей части событий

Назначение	JSON	Тип
Тип события	**t**	unsigned
Время регистрации события (в формате UTC)	**time**	timestamp

Назначение	JSON	Тип
Действие, связанное с событием (0 – блокировать, 1 – разрешить, 2 – продолжить наблюдение)	**act** (по умолчанию – 2)	unsigned
Причина предпринятого действия	**rsn**	unsigned
Правило, относящееся к событию	**rul**	string
Идентификатор техники/тактики MITRE	**mitre**	string
Критичность (уровень важности) события	**svrt** (по умолчанию – 0)	unsigned
Уникальный идентификатор процесса	**uuid**	int (индекс в массиве GUID'ов)
Уникальный идентификатор группы процессов	**hid**	string (индекс в массиве GUID'ов)
Уникальный идентификатор корреляции событий	**cid**	string (индекс в массиве GUID'ов)
Идентификатор процесса на агентской системе	**pid**	unsigned
Идентификатор родительского процесса на агентской системе	**ppid**	unsigned
Полное имя (вместе с путем) исполняемого модуля процесса	**app**	string MANGLED
Командная строка процесса	**cmdl**	string (index string 2650+)
Номер сессии, в которой работает процесс на агентской системе	**sess** (по умолчанию – 0)	unsigned
SID пользователя, запустившего процесс	**sid**	string
Издатель ЭП исполняемого файла процесса	**app_sgnr**	string
Имя пользователя, запустившего процесс	**usr**	string
Домен (имя компьютера) пользователя, запустившего процесс	**dom**	string
Подтип события (интерпретируется в зависимости от типа)	**st**	unsigned
Поведенческие признаки процесса (первая группа)	**rf0**	uint64
Поведенческие признаки процесса (вторая группа)	**rf1**	uint64
Флаги исполняемого файла процесса	**exclf**	uint64
Синтетическое событие (0 или 1)	**syn**	int (0/1)
Версия события	**efmt**	unsigned

В поле **time** передается UTC-время регистрации события. Система построена таким образом, что в штатной ситуации в пределах одного агента не бывает событий с одинаковым значением поля **time**. Если события зарегистрированы в одно и то же время, то между ними вносится временной сдвиг, который для последующих событий компенсируется за счет естественного течения времени.

В поле **svrt** (severity) передается критичность события.

Критичность события может принимать следующие значения:

1) **NORMAL** (код 0, значение по умолчанию) — информация ("зеленый", нет угрозы);

2) **GUARDED** (код 1) – низкая/пограничная ("серый", малой степени вероятная угроза);
3) **ELEVATED** (код 2) – средняя/повышенная ("синий", средней степени вероятная угроза);
4) **HIGH** (код 3) – высокая ("оранжевый", вероятная угроза);
5) **SEVERE** (код 4) – критичная ("красный", максимальной степени вероятная угроза).



Примечание

Критичность также можно трактовать следующим образом: NORMAL – телеметрия, GUARDED – информирующие обнаружения (informational alerts), ELEVATED+ – обнаружения (alerts). Предполагается, что аналитик работает преимущественно с обнаружениями, редко обращаясь к информирующим обнаружениям и крайне редко – к телеметрии.

В поле **act** (action) передается действие, предпринятое в связи с событием. Это может быть одно из трех значений:

BLOCK (код 0) – блокирование. Означает, что в контексте события сработала какая-то логика («черный» список, эвристическое правило, политика и т.п.), и в результате то или иное действие было заблокировано. При этом поля **rsn** (reason – причина) и **rul** (правило) будут содержать информацию, определяющую, почему принято блокирующее решение.

ALLOW (код 1) – разрешение. Означает, что в контексте события сработала какая-то логика («белый» список, эвристическое правило, политика и т.п.) и в результате то или иное действие было разрешено. Поля **rsn** и **rul** в этом случае содержат информацию, показывающую, почему принято разрешающее решение.

MORE_PROCESSING (код 2, значение по умолчанию, т.е. непосредственно в теле события этот код не передается) – трактуется по-разному в зависимости от контекста. В контексте события телеметрии означает, что никакого действия, связанного с событием, не предпринято. В контексте обнаружения (alert) код 2 означает, что логика обнаружения не предписывает никакого действия, кроме фиксации самого факта обнаружения – обнаруженная активность не блокируется, что не отменяет самого факта ее обнаружения.

Для события телеметрии поля **rsn** и **rul**, как правило (но необязательно), не заполняются, а для события-обнаружения поле **rul** содержит правило, идентифицирующее обнаружение. И тогда поле **rsn**, как и в других случаях, содержит причину, по которой установлена такая реакция на обнаружение.

Поле **mitre** заполняется, если событие соответствует какой-то технике/тактике MITRE. Одно событие может соответствовать сразу нескольким элементам MITRE, в этом случае техники/тактики перечисляются через запятую, например, «T1490, T1047/001».

Поля **pid**, **ppid**, **uuid**, **app**, **sess**, **usr**, **dom** определяют приложение (процесс), ассоциированный с событием. Поле **pid** содержит системный ID процесса, **ppid** – системный ID его родителя, **uuid** – индекс элемента в массиве **uuids** заголовка блока событий (см. выше), определяющий внутренний уникальный ID процесса (предназначен для внутреннего использования), **app** – полное имя файла процесса вместе с путем, **sess** (session) – номер сессии процесса (по умолчанию 0), **usr** (user) – имя пользователя, от имени которого работает процесс, **dom** (domain) – домен/имя компьютера пользователя, от имени которого запущен процесс.

Поля **rf0**, **rf1** определяют поведенческий профиль процесса. Поле **rf0** – это runtime-флаги процесса (первая группа); **rf1** – runtime-флаги процесса (вторая группа). Флаги в явном виде не отображаются, а используются для удобочитаемого представления поведенческого профиля процесса. Поведенческие признаки процесса могут меняться от события к событию сообразно с поведением процесса в системе.

Поле **st** определяет подтип события в рамках определенной подсистемы.

Поле **app**, а также другие поля событий, в которых присутствуют пути, могут быть декорированы (mangled). Декорация заключается в замене известного префикса пути его кодом. У декорированных путей в начале следует один или несколько компонентов, кодирующих заранее определенные подстроки, затем следует недекорированный остаточный путь.

Поле **syn** устанавливается в 1, если событие, которое в обычной ситуации отражает реально имеющую место активность агента, в данном конкретном случае является синтезированным, т.е. исскуственным. Например, если агентский модуль деактивируется, то он публикует синтетические события завершения процессов системы, за которыми он наблюдает и для которых были отправлены события старта процесса. И наоборот, при запуске агентского модуля "на лету" сразу после установки (или его активации после деактивации), когда в системе уже работают те или иные процессы, агент публикает синтетические события создания этих процессов. Это позволяет сохранять целостную картину состояния агентской системы с точки зрения административного модуля в разных сценариях работы агента.

Поле **efmt** (версия события) содержит номер сборки агента, который сформировал данное событие.

Предусматривается 2 схемы декорирования (см. таблицы 19 и 20).

Таблица 19 – Декорируются стандартные префиксы путей

Путь	Заменяется на
\Device\HarddiskVolume1\Windows	*0
\Device\HarddiskVolume1\Windows\System32\	*1
\Device\HarddiskVolume1\Windows\SysWOW64\	*2
\Device\HarddiskVolume1\Program Files\	*3
\Device\HarddiskVolume1\Program Files (x86)\	*4
\Device\HarddiskVolume1\ProgramData\Microsoft\	*5

Пример: \device\harddiskvolume1\windows\system32\kernel32.dll декорируется в *1\kernel32.dll.

Таблица 20 – Декорирование первых 2-х компонент пути

Путь	Заменяется на
\Device\HarddiskVolumeX\	?X\
\Device\HarddiskVolumeX\Windows\	?X*0\
\Device\HarddiskVolumeX\Windows\System32\	?X*1\
\Device\HarddiskVolumeX\Windows\SysWOW64\	?X*2\
\Device\HarddiskVolumeX\Program Files\	?X*3\
\Device\HarddiskVolumeX\Program Files (x86)\	?X*4\
\Device\HarddiskVolumeX\ProgramData\Microsoft\	?X*5\

X - символ 0-9.

Пример: \device\harddiskvolume5\programdata\microsoft\Office\AssetLibrary.ico декорируется в ?5*5\Office\AssetLibrary.ico.

Синтаксис декорирования таков, что при обратном декорировании позволяет однозначно идентифицировать схему декорирования.

7.2 События мониторинга сети

При любых сетевых взаимодействиях и проверках, которые осуществляются между агентом и удаленным компьютером, будь то матчинг индикаторов атак, индикаторов компрометации, в сетевых

исключениях и т.д. важен прежде всего удаленный хост, его имя, IP-адрес и порт, то есть на него идет основное внимание в момент сетевого соединения.

Подтипы событий (**st**) и их текстовые описания представлены в таблице 21.

Таблица 21 – События монитора сети

Код события	Имя события	Описание
0	Сеть: Исходящее подключение	Исходящее подключение к удаленному хосту (заменяется на **host** (**r_ip:r_p**), если заполнено поле **host**, иначе на **r_ip:r_p**) по **proto**
1	Сеть: Входящее подключение	Входящее подключение к порту **l_p** от удаленного хоста (заменяется на **host** (**r_ip:r_p**), если заполнено поле **host**, иначе на **r_ip:r_p**) по **proto**
16	Сеть: Завершение сетевого подключения	Завершение исходящего подключения к удаленному хосту заменяется на **host** (**r_ip:r_p**), если заполнено поле **host**, иначе на **r_ip:r_p**) по **proto** или 2. Завершение входящего подключения к порту l_p от удаленного хоста (заменяется на **host** (**r_ip:r_p**), если заполнено поле **host**, иначе на **r_ip:r_p**) по **proto**
2	Сеть: Отправка	Отправка **size** байт на удаленный хост (заменяется на **host** (**r_ip:r_p**), если заполнено поле **host**, иначе на **r_ip:r_p**) по **proto**
3	Сеть: Прием	Прием **size** байт на порт **l_p** от удаленного хоста (заменяется на **host** (**r_ip:r_p**), если заполнено поле **host**, иначе на **r_ip:r_p**) по **proto**
5	Сеть: DNS запрос	DNS-запрос **dnsq_t** к удаленному хосту (заменяется на **host** (**r_ip:r_p**), если заполнено поле **host**, иначе на **r_ip:r_p**) на имя **dnsq_h** размером **size** байт
11	Сеть: DNS-ответ	DNS-ответ со статусом dnsq_s на запрос dnsq_t к удаленному хосту на имя **dnsq_h** размером **size** байт, результат – **dnsq_r** (ответ может не выводиться)
13	Сеть: Входящий DNS запрос	DNS-запрос **dnsq_t** от **%remote_endpoint%** на имя **dnsq_h** размером **size** байт
14	Сеть: Исходящий DNS-ответ	DNS-ответ со статусом **dnsq_s** на запрос **dnsq_t** от **%remote_endpoint%** на имя **dnsq_h** размером **size** байт, результат: **dnsq_r** (ответ может не выводиться)
6	Сеть: SSL HELLO	SSL HELLO (**ssl_h**) с удаленного хоста (заменяется на **host** (**r_ip:r_p**), если заполнено поле **host**, иначе на **r_ip:r_p**) размером **size** байт
7	Другие обнаружения*	Расшифровка кода **detect**
8	Обнаружение: срабатывание индикатора компрометации*	Срабатывание индикатора компрометации при сетевом взаимодействии с удаленным хостом (заменяется на **host** (**r_ip:r_p**), если заполнено поле **host**, иначе на **r_ip:r_p**)
10	Сеть: Открытие локального порта на прием (LISTEN)	Открытие локального порта **l_p** на прием
15	ICMP-сообщение	ICMP-сообщение типа icmp_t (код icmp_c)

События, отмеченные значком * отправляются на сервер только в формате обнаружений (st>50), **%remote_endpoint%** заменяется на **host (r_ip:r_p)** если заполнено поле **host**, иначе на **r_ip:r_p**.

Поля сетевых событий представлены в таблице 22.

Таблица 22 – Поля сетевых событий

Назначение	JSON	Тип
Полное имя исполняемого модуля–инициатора операции	**who**	string MANGLED
Идентификатор нити–инициатора операции	**whotid**	unsigned
Стартовый адрес нити–инициатора операции	**whoaddr**	uint64
Флаги исполняемого модуля–инициатора операции	**whof**	uint64
Исключения для программ, назначенные инициатору операции	**who_excls**	string
Стек вызовов операции	**trace**	string
Номер протокола 6 – TCP, 17 – UDP, 1 – ICMP, 58 – ICMPv6	**proto**	unsigned
Признак работы по IPv6 (принимает значения true или false)	**ipv6**	int (0/1)
Идентификатор сетевого потока (служебное значение, позволяет группировать события, относящиеся к одному сетевому потоку)	**flow**	int64
Уникальный идентификатор сетевого потока	**fluuid**	string (индекс в массиве GUID'ов в текст. форме)
Отправка (1) или прием (0)	**out**	int (0/1)
Размер полезных данных (payload) сетевого пакета	**size**	int64
Имя хоста, соответствующее удаленному IP	**host**	string
Тип DNS запроса: 0x1 – A, 0x5 – CNAME, 0x1C – AAAA, 0x0F – MX, 0x21 – SRV, 0x0C – PTR, 0x41 HTTPS. Остальные типы запросов выводятся кодом (2 байта), пример: 0x0002	**dnsq_t**	unsigned
Имя хоста из DNS-запроса	**dnsq_h**	string
Статус DNS-запроса	**dnsq_s**	unsigned
Результат DNS-запроса	**dnsq_r**	string
Идентификатор транзакции DNS-обмена	**dns_trx**	unsigned
Имя хоста (server_name) из SSL Client Hello сообщения	**ssl_h**	string
Удаленный IP-адрес	**r_ip**	string
Удаленный порт	**r_p**	unsigned
Локальный IP-адрес	**l_ip**	string
Локальный порт	**l_p**	unsigned
Флаги сетевого события	**netf**	unsigned
Исключение для удаленного IP-адреса	**r_ip_excl**	string
Исключение для имени хоста, соответствующего удаленному IP-адресу	**h_excl**	string
Исключение для имени хоста в запросе	**rqh_excl**	string
Код обнаружения	**detect**	unsigned
Тип ICMP-сообщения	**icmp_t**	unsigned

Назначение	JSON	Тип
Код ICMP-сообщения	**icmp_c**	unsigned
Имя хоста в индикаторе компрометации	**loc_h**	string
Общий размер исходящих данных за время жизни подключения, байт	**o_sz**	uint64
Общий размер входящих данных за время жизни подключения, байт	**i_sz**	uint64
Время жизни подключения, в 100-наносекундных интервала	**lt**	uint64

Тип DNS-запроса — это параметр в DNS-сообщении, который указывает, какую именно информацию хочет получить клиент (например, браузер) от DNS-сервера. Проще говоря, это вопрос, который клиент задает DNS-серверу. Вопросы бывают разные: «Какой IP-адрес у этого домена?», «Какой почтовый сервер его обслуживает?» и так далее. Тип запроса как раз и определяет, какой именно вопрос задается.

SSL ClientHello — это первое и одно из самых важных сообщений в процессе установления безопасного (шифрованного) соединения по протоколу SSL (например, когда вы заходите на сайт по HTTPS), в процессе которого выполняются следующие шаги:

1) Приветствие с сервером;
2) Сообщение о своих возможностях (версии протокола, шифры);
3) Просьба об установлении безопасного соединения для конкретного сайта;
4) Начало процесса генерации уникальных ключей шифрования для текущего сеанса.

ICMP (Internet Control Message Protocol) — это вспомогательный протокол в составе сетевого стека TCP/IP. Его главная задача — обмен служебной информацией между сетевыми устройствами (маршрутизаторами, серверами, обычными хостами) для диагностики проблем и управления передачей данных.

7.3 События мониторинга файловых операций

Подтипы событий (**st**) мониторинга файловых операций и их текстовые описания представлены в таблице 23.

Таблица 23 – События мониторинга файловых операций

Код события	Имя события	Описание
0	Файлы: Создан новый файл	Создан новый файл **name**
1	Файлы: Файл переименован	Файл **name** переименован в **fnew**
2	Файлы: Удален файл	Удален файл **name**

Код события	Имя события	Описание
3	Файлы: У файла изменен атрибут или время создания	У файла **name** [установлен/снят атрибут "системный" (если присутствует **sys**, **sys** = 0, то снят, **sys** = 1 - установлен)], [установлен атрибут "скрытый" (если присутствует **hdn**)], [изменено время создания с **old_t** на **new_t** (если присутствуют **old_t** и **new_t**)]
4	Файлы: Другие обнаружения*	<Описание кода **detect**>
7	Файлы: Файл был модифицирован	Файл **name** был модифицирован (запись файла)
8	Файлы: Файл был прочитан	Файл **name** был прочитан
12	Файлы: Прямой доступ к тому на чтение	Прямой доступ к диску (тому) **name** на чтение
13	Файлы: Прямой доступ к тому на запись	Прямой доступ к диску (тому) **name** на запись
14	Файлы: Создан именованный канал	Создан именованный канал **name**
15	Файлы: Подключение к именованному каналу	Подключение к именованному каналу **name**
16	Файлы: Обнаружение: доступ к файлу	Доступ к файлу **name**
17	Файлы: Обнаружение: срабатывание индикатора компрометации для файла*	Срабатывание индикатора компрометации для файла **name**
19	Файлы: Обнаружение: файл классифицирован как вредоносный (ML на агенте)*	Файл **name** классифицирован как вредоносный (ML на агенте)
20	Файлы: Обнаружение: файл классифицирован как вредоносный (Yara-правила)*	Файл **name** классифицирован как вредоносный (Yara-правила)
22	Файлы: Создан альтернативный поток для файла	Создание альтернативного поток **strm** для файла **name**
23	Файлы: Создан файл с потенциально активным содержимым	Создан файл **name** с потенциально активным содержимым
24	Файлы: Модифицирован файл с потенциально активным содержимым	Модифицирован файл **name** с потенциально активным содержимым

События, отмеченные значком *, отправляются на сервер только в формате обнаружений (st>50).

Расшифровка значений поля detect приведена в таблице 24.

Таблица 24 – Расшифровка значений поля detect

Значение	Мнемоника	Расшифровка
1001	FS_DETECT_NATIVE_FILE_DELETE_OR_RENAME	Попытка удаления или переименования файла агента **name**
1002	FS_DETECT_NATIVE_FILE_MODIFY	Попытка модификации файла агента **name**
1003	FS_DETECT_CHANGE_NATIVE_FILE_SECURITY	Попытка изменения атрибутов безопасности файла агента **name**
1004	FS_DETECT_SAVE_FILE_TO_NATIVE_DIR	Попытка сохранения файла **name** в директорию агента

Значение	Мнемоника	Расшифровка
1005	FS_DETECT_SET_SYMLINK_TO_NATIVE_FILE	Попытка установки символической ссылки на файл агента **name**
2001	REG_DETECT_QUERY_SECURITY_VALUE	Попытка чтения значения, содержащего конфиденциальную информацию
2002	REG_DETECT_DUMP_SECURITY_KEY	Попытка дампа ключа, содержащего конфиденциальную информацию
2003	REG_DETECT_QUERY_CLSID_INPROCSERVER_VALUE	Обнаружено создание COM-объекта
4012	PM_DETECT_PROCESS_TAMPERING	Подмена образа процесса в памяти: общая техника
4013	PM_DETECT_PROCESS_CALLBACK_MISS	Нарушение функции защиты (фильтр создания/завершения процессов)
4014	PM_DETECT_IMAGE_CALLBACK_MISS	Нарушение функции защиты (фильтр загрузки модулей)
4015	PM_DETECT_THREAD_CALLBACK_MISS	Нарушение функции защиты (фильтр создания/завершения нитей)
4016	PM_DETECT_OBJECT_CALLBACK_MISS	Нарушение функции защиты (фильтр доступа к объектам)
4017	PM_DETECT_REGISTRY_CALLBACK_MISS	Нарушение функции защиты (фильтр реестровых операций)
4018	PM_DETECT_FILE_SYSTEM_CALLBACK_MISS	Нарушение функции защиты (фильтр файловых операций)
4019	PM_DETECT_WRONG_CALLBACK_DETECTION	Нарушение функции защиты (контроль фильтров)
4020	PM_DETECT_DRIVER_VERIFICATION_ENABLED	Нарушение функции защиты (верификация драйвера)
4021	PM_DETECT_DRIVER_IMAGE_INTEGRITY	Нарушение целостности системного компонента защиты
4022	PM_DETECT_SERVICE_IMAGE_INTEGRITY	Нарушение целостности прикладного компонента защиты
4023	PM_DETECT_MIRROR_DUMP_LSASS	Дампинг памяти процесса LSASS (кража credentials)
4024	PM_DETECT_SHELLCODE_EXECUTION	Исполнение shell-кода (потенциальный эксплойт)
4025	PM_DETECT_UNABLE_TO_TERMINATE_THREADS	Нарушение функции защиты (нет функции уничтожения нити)
4026	PM_DETECT_HANDLE_THEFT_LSASS	Кража описателя процесса LSASS (потенциальный дампинг памяти LSASS)
4027	PM_DETECT_ILLEGAL_CSS_PROCESS_ACCESS	Недопустимый доступ к критическому системному процессу
4028	PM_DETECT_USB_IMAGE_INTEGRITY	Нарушение целостности компонента контроля USB-устройств

Значение	Мнемоника	Расшифровка
4029	PM_DETECT_YARA	Обнаружена сигнатура вредоносного кода в памяти процесса
4030	PM_DETECT_SHELLCODE_INSIDE_NATIVE_SERVICE	Shellcode внутри прикладного компонента защиты
4031	PM_DETECT_NET_FILTER_MISS	Нарушение функции защиты (фильтр сетевых событий)
4032	PM_DETECT_KERNEL_MODULE_ABUSE	Попытка нелегального доступа к системному компоненту защиты

Поля событий мониторинга файловой системы представлены в таблице 25.

Таблица 25 – Поля событий мониторинга файловой системы

Назначение	JSON	Тип
Полное имя исполняемого модуля-инициатора операции	**who**	string MANGLED
Идентификатор нити-инициатора операции	**whotid**	unsigned
Стартовый адрес нити-инициатора операции	**whoaddr**	uint64
Флаги исполняемого модуля-инициатора операции	**whof**	uint64
Исключения для программ, назначенные инициатору операции	**who_excls**	string
Стек вызовов операции	**trace**	string
Полное имя файла	**name**	string MANGLED
Время создания файла	**crtime**	timestamp
Время последнего изменения файла	**chtime**	timestamp
Размер файла	**fsize**	int64
Тип файла	**ftype**	enum
Атрибуты файла	**attr**	unsigned
SHA-1 файла	**sha1**	string
MD5 файла	**md5**	string
SHA-256 файла	**sha256**	string
Imphash файла	**imphash**	string
Электронная подпись файла	**sgnr**	string
Статус электронной подписи файла	**sgnr_s**	enum
Оригинальное имя файла	**ofn**	string
Компания-издатель файла	**fcomp**	string
Версия файла	**fver**	string
Описание файла	**fdesc**	string
Продукт, к которому относится файл	**fprod**	string
Файл находится в белом списке	**fwhite**	int (-/1)
Тип упаковщика файла	**pack**	string
Файл расположен в директории автозапуска	**arun**	int (-/1)

Новое имя файла	fnew	string MANGLED
Файл был заменен	owrt	int (-/1)
Время создания файла до изменения атрибутов	old_t	timestamp
Время создания файла после изменения атрибутов	new_t	timestamp
Файл содержит атрибут "скрытый"	hdn	int (0/1)
Файл содержит атрибут "системный"	sys	int (0/1)
Операция совершается над альтернативным потоком данных файла	ads	int (-/1)
Код обнаружения	detect	unsigned
Доступ на удаление	delete	int (-/1)
Доступ на чтение	read	int (-/1)
Доступ на модификацию	modify	int (-/1)
Обмен именами (доступен только в Linux)	nxchg	int (-/1)
Имя альтернативного потока данных файла	strm	string
Исключение для файла по хешу	fh_excl	string
Исключение для файла по имени	fn_excl	string
SID предыдущего владельца файла	own_old	string
Домен предыдущего владельца файла	own_old_dom	string
Имя предыдущего владельца файла	own_old_usr	string
Предыдущий владелец файла был задан по умолчанию	own_old_def	int (-/1)
SID нового владельца файла	own_new	string
Домен нового владельца файла	own_new_dom	string
Имя нового владельца файла	own_new_usr	string
Новый владелец файла был задан по умолчанию	own_new_def	int (-/1)
SID предыдущей основной группы владельца файла	grp_old	string
Домен предыдущей основной группы владельца файла	grp_old_dom	string
Имя предыдущей основной группы владельца файла	grp_old_usr	string
Предыдущая основная группа владельца файла была задана по умолчанию	grp_old_def	int (-/1)
SID новой основной группы владельца файла	grp_new	string
Домен новой основной группы владельца файла	grp_new_dom	string
Имя новой основной группы владельца файла	grp_new_usr	string
Новая основная группа владельца файла была задана по умолчанию	grp_new_def	int (-/1)
Предыдущий DACL файла	dacl_old	string
Предыдущий DACL файла был задан по умолчанию	dacl_old_def	int (-/1)
Новый DACL файла	dacl_new	string
Новый DACL файла был задан по умолчанию	dacl_new_def	int (-/1)
Предыдущий SACL файла	sacl_old	string
Предыдущий SACL файла был задан по умолчанию	sacl_old_def	int (-/1)
Новый SACL файла	sacl_new	string
Новый SACL файла был задан по умолчанию	sacl_new_def	int (-/1)
Предыдущая мандатная метка файла	mlbl_old	unsigned

Предыдущая маска мандатной метки файла	**mlbl_old_mask**	unsigned
Новая мандатная метка файла	**mlbl_new**	unsigned
Новая маска мандатной метки файла	**mlbl_new_mask**	unsigned

Поле **ftype** принимает следующие значения, представленные в таблице 26.

Таблица 26 – Значение поля ftype

Значение	Описание
2	PE
3	Active content
4	PowerShell script

Если было получено значение, отсутствующее в таблице, отображается только его значение (например, **Тип файла: 1**).

Поле **sgnr_s** (статус электронной подписи) событий мониторинга файлов и процессов может принимать следующие значения:

– 0 (нет подписи);

– 1 (есть подпись);

– 2 (неизвестно).



Примечание

Список всех возможных атрибутов файлов для ОС Windows содержится в документации Microsoft.

Альтернативный поток данных файла (ADS)– это специальная возможность файловой системы NTFS в Windows, позволяющая хранить дополнительную информацию в виде отдельного скрытого «потока» внутри обычного файла.

DACL (Discretionary Access Control List) — это список управления доступом, который определяет, кто и какие действия может выполнять с объектом (файлом, папкой, разделом реестра и т.д.) в операционных системах Windows.

SACL (System Access Control List) — это список управления доступом для аудита, который определяет, какие попытки доступа к файлу или папке нужно регистрировать в журнале событий Windows (Event Log).

Мандатная метка файла — это специальный атрибут, который присваивается файлу для определения уровня его секретности (конфиденциальности) и категорий информации, которые он содержит. В отличие от прав доступа (как в DACL), которые определяются владельцем файла, мандатная метка назначается системой или администратором безопасности и является принудительной. Пользователь не может по своему желанию изменить её или проигнорировать.

7.4 События монитора реестра

Подтипы событий (**st**) мониторинга реестра и их текстовые описания представлены в таблице 27.

Таблица 27 – Подтипы событий мониторинга реестра

Код события	Имя события	Описание
0	Реестр: Создан новый ключ	Создан новый ключ **key**
1	Реестр: Удален ключ	Удален ключ **key**
2	Реестр: в значение ключа записаны данные	В значение **val_n** ключа **key** записаны данные **val_d** (тип: **val_t**, размер: **val_s**)
3	Реестр: Удалено значение ключа	Удалено значение **val_n** ключа **key**
4	Реестр: Ключ переименован	Ключ **key** переименован в **new**
5	Реестр: Ключ восстановлен из файла	Ключ **key** восстановлен из файла **src**
6	Реестр: Данные ключа заменены файлом	Данные ключа **key** заменены файлом **src**
7	Реестр: Другие обнаружения*	Описание поля **detect**

События, отмеченные значком *, отправляются на сервер только в формате обнаружений (st>50).

Поля событий монитора реестра представлены в таблице 28.

Таблица 28 – Поля событий мониторинга реестра

Назначение	JSON	Тип
Полное имя исполняемого модуля-инициатора операции	**who**	string MANGLED
Идентификатор нити-инициатора операции	**whotid**	unsigned
Стартовый адрес нити-инициатора операции	**whoaddr**	uint64
Флаги исполняемого модуля-инициатора операции	**whof**	uint64
Исключения для программ, назначенные инициатору операции	**who_excls**	string
Стек вызовов операции	**trace**	string
Путь ключа реестра	**key**	string
Имя значения	**val_n**	string

Назначение	JSON	Тип
Тип данных значения: 1 – REG_SZ; 2 – REG_EXPAND_SZ; 3 – REG_BINARY; 4 – REG_DWORD; 5 – REG_DWORD_BE; 6 – REG_LINK; 7 – REG_MULTI_SZ; 8 – REG_RES_LIST; 9 – REG_FULL_RES_DESC; 10 – REG_RES_REQ_LIST; 11 – REG_QWORD	**val_t**	unsigned
Размер данных значения	**val_s**	unsigned
Данные значения	**val_d**	string
Новое имя ключа	**new**	string
Имя файла-источника загружаемой в реестр информации	**src**	string MANGLED
Ключ/значение относится к категории автозапуска	**asep**	int (-/1)
Код обнаружения	**detect**	unsigned

Поле **asep** принимает значение **true**.

Autostart Extensibility Points (ASEP) — это механизмы в операционных системах (в частности, Windows), которые позволяют программам, службам, драйверам или скриптам автоматически запускаться при загрузке системы, входе пользователя или выполнении определенных условий. Они играют ключевую роль в обеспечении функциональности и удобства, но также представляют значительный риск для информационной безопасности, поскольку часто используются злоумышленниками для закрепления вредоносного ПО в системе.

7.5 События журналов

Подтипы событий журналов и их текстовые описания представлены в таблице 29.

Таблица 29 – Подтипы событий журналов (st)

Код события	Имя события	Описание
0	WINLOGBEAT_EVENT	Событие журнала
1	FILEBEAT_EVENT	Строка лог-файла

Поля событий журнала и их текстовые описания представлены в таблице 30.

Таблица 30 – Поля событий журнала (st=0)

Назначение	JSON	Тип
Подтип события	**st**	unsigned
Уровень (возможно значение: Критическая ошибка = 1, Ошибка = 2, Предупреждение = 3, Информация = 4, Подробно = 0 или 5)	**e_lvl**	unsigned
Дополнительные данные (выводятся в поле карточки событий в JSON-формате)	**e_ex**	string (опционально)
Описание события	**e_msg**	string (опционально)
ID события	**e_id**	unsigned

Назначение	JSON	Тип
ID провайдера	**e_prv_id**	unsigned (индекс в массиве GUID'ов) (опционально)
Провайдер	**e_prv**	string
Имя канала	**e_chn**	string
Событие в формате winlogbeat (см. winlogbeat), является JSON-объектом	**winlog**	JSON-объект

События формата winlogbeat могут принимать значения, представленные в таблице 31.

Таблица 31 – События winlogbeat

Поле	Тип	Расшифровка
winlog.api	keyword	Тип API
winlog.event_id	keyword	Идентификатор события
winlog.activity_id	unsigned (индекс в массиве GUID'ов) (опционально)	Идентификатор действия
winlog.related_activity_id	unsigned (индекс в массиве GUID'ов) (опционально)	Идентификатор действия, которому было передано управление
winlog.computer_name	keyword (опционально)	Имя компьютера
winlog.keywords	keyword (опционально)	Ключевые слова
winlog.channel	keyword (опционально)	Имя канала
winlog.record_id	keyword	Номера записи
winlog.opcode	keyword (опционально)	Код операции
winlog.provider_guid	unsigned (индекс в массиве GUID'ов) (опционально)	Идентификатор провайдера
winlog.provider_name	keyword (опционально)	Имя провайдера
winlog.process.pid	long (опционально)	Идентификатор процесса
winlog.task	keyword (опционально)	Имя задачи
winlog.time_created	date (опционально) (ISO 8601)	Дата и время создания события
winlog.process.thread.id	long (опционально)	Идентификатор нити
winlog.user.identifier	keyword (опционально)	SID пользователя
winlog.user.name	keyword (опционально)	Имя пользователя
winlog.event_data	json_object (опционально) (набор полей отличаются от провайдера к провайдеру, все поля должны иметь тип: keyword)	Поля события
winlog.user_data	json_object (опционально) (набор полей отличаются от провайдера к провайдеру, все поля должны иметь тип: keyword)	Пользовательские поля события



Примечание

Подробное логирование предоставляет максимальную видимость процессов в системе, но требует значительных ресурсов, поэтому желательно его включать для критических компонентов, например, Windows Defender, сетевых служб, это позволит грамотно использовать ресурсы системы.

Описание полей события строки лог-файла (**st = 1**) представлено в таблице 32.

Таблица 32 – Поля события строки лог-файла

Назначение	JSON	Тип
Строка log-файла	**message**	string
Блок информации filebeat	**log**	JSON-объект

События формата filebeat могут принимать значения, представленные в таблице 33

Таблица 33 – События формата filebeat

Поле	Тип	Расшифровка
log.offset	long	Смещение строки в лог-файле
log.file.path	string	Имя лог-файла

7.6 События мониторинга процессов

Подтипы событий и их текстовые описания представлены в таблице 34.

Таблица 34 – Подтипы событий мониторинга процессов и их тестовые описания

Код события	Имя события	Описание
0	Процессы: Загрузка драйвера	Загрузка драйвера **path**
1	Процессы: Старт процесса	Старт процесса командой **cmdl** из **cpath** (**cpid**), нить = **whotid** (из модуля **who**)
2	Процессы: Завершение процесса	Завершение процесса с кодом **code**
3	Процессы: Загрузка образа	Загрузка образа **path**
6	Процессы: Доступ к процессу	Доступ к процессу **tpath** (**tpid**) с правами **dsrd**, {разрешено ИЛИ запрещено **dsrd-grnt**}, нить=**whotid** (из модуля **who**)
7	Процессы: Создание нити в стороннем процессе	Создание нити **tid** в процессе **tpath** (**tpid**), нить = **whotid** (из модуля **who**)
13	Процессы: Обнаружение: подмена командной строки*	Подмена командной строки с **cmdl1** на **cmdl**

Код события	Имя события	Описание
16	Процессы: Обнаружение: изменение системной защиты процесса*	Изменение системной защиты процесса с **prot** на **prot1**
18	Процессы: Доступ к нити процесса	Доступ к нити **tid** процесса **tpath** (**tpid**) с правами **dsrd**, {разрешено ИЛИ запрещено **dsrd-grnt**}, нить = **whotid** (из модуля **who**)
20	Процессы: Загрузка образа в сторонний процесс	Загрузка образа **path** в процесс **tpath** (**tpid**), нить = **whotid** (из модуля **who**)
23	Процессы: Другие обнаружения*	Описание кода **detect**
22	Уведомление модуля Antimalware Scan Interface Windows	Уведомление модуля Antimalware Scan Interface Windows: содержимое **amsi_cname** размером **fsize**, хеш sha256

События, отмеченные значком *, отправляются на сервер только в формате обнаружений (st>50).

Поля событий мониторинга процессов представлены в таблице 35.

Таблица 35 – Поля событий мониторинга процессов

Назначение	JSON	Тип
Полное имя исполняемого модуля–инициатора операции	**who**	string MANGLED
Идентификатор нити–инициатора операции	**whotid**	unsigned
Стартовый адрес нити–инициатора операции	**whoaddr**	uint64
Флаги исполняемого модуля–инициатора операции	**whof**	uint64
Исключения для программ, назначенные инициатору операции	**who_excls**	string
Командная строка родительского процесса	**cmdlp**	string
Электронная подпись родительского процесса	**sgnrp**	string
Командная строка прародителя (grand parent)	**cmdlg**	string
Рабочий каталог процесса	**wdir**	string MANGLED
Уровень защиты процесса	**prot**	unsigned
Уровень доверия (integrity level) процесса	**integ**	unsigned
Время создания процесса	**when**	timestamp
Уникальный идентификатор родительского процесса	**parent**	unsigned (индекс в массиве GUID-ов)
Уникальный идентификатор процесса-создателя	**caller**	unsigned (индекс в массиве GUID-ов)
Идентификатор процесса-инициатора операции	**cpid**	unsigned
Полное имя процесса-инициатора операции	**cpath**	string MANGLED
Код завершения процесса	**code**	unsigned
Уникальный идентификатор целевого процесса	**targ**	unsigned
Полное имя целевого процесса	**tpath**	string MANGLED
Идентификатор целевого процесса	**tpid**	unsigned
Флаги образа целевого процесса	**targf**	uint64

Назначение	JSON	Тип
Поведенческие признаки целевого процесса (первая группа)	trf0	uint64
Поведенческие признаки целевого процесса (вторая группа)	trf1	uint64
Стек вызовов операции	trace	string
Полное имя файла образа	path	string MANGLED
Флаги операции загрузки образа	ldf	unsigned
Флаги образа	imgf	uint64
Базовый адрес образа	base	uint64
Размер образа	isize	unsigned
Идентификатор целевой нити	tid	unsigned
Имя модуля целевой нити	tmod	string
Имя функции целевой нити	tfunc	string
Стартовый адрес целевой нити	taddr	uint64
Флаги операции с нитью	tf	unsigned
Запрашиваемые права	dsrd	unsigned (32 бита)
Предоставленные права	grnt	unsigned (32 бита)
Новый уровень защиты процесса	prot1	int
Новая командная строка процесса	cmdl1	string
Размер файла	fsize	int64
Тип файла	ftype	enum
SHA-1 файла	sha1	string
MD5 файла	md5	string
SHA-256 файла	sha256	string
Imphash файла	imphash	string
Электронная подпись файла	sgnr	string
Статус электронной подписи	sgnr_s	enum
Тип упаковщика файла	pack	string
Атрибуты файла	attr	unsigned
Время создания файла	crtime	timestamp
Время последней записи файла	chtime	timestamp
Оригинальное имя файла	ofn	string
Компания-издатель файла	fcomp	string
Версия файла	fver	string
Описание файла	fdesc	string
Продукт, к которому относится файл	fprod	string
Файл находится в "белом" списке	fwhite	int (-/1)
Код обнаружения	detect	unsigned
Исключение для файла по хешу	fh_excl	string
Исключение для файла по имени	fn_excl	string

Назначение	JSON	Тип
AMSI: имя содержимого	**amsi_cname**	string
AMSI: содержимое	**amsi_data**	string
AMSI: имя приложения	**amsi_appname**	string
AMSI: ссылка на скачивание зарезервированного содержимого	**amsi_blink**	string

Поле **integ** (уровень доверия процесса) событий мониторинга процессов может принимать следующие значения:

– 0 (нет);

– 1 (низкий);

– 2 (средний);

– 3 (высокий);

– 4 (системный);

– 5 (защищенный).

7.7 События мониторинга системы

Подтипы событий (**st**) мониторинга системы представлены в таблице 36.

Таблица 36 – Подтипы событий мониторинга системы

Код события	Имя события	Описание
0	Система: WMI	Событие подсистемы WMI
2	Система: Изменение системного времени	Изменение системного времени
3	Завершение работы	Событие, связанное с завершением работы ОС

События мониторинга систем с кодом события 0 (WMI) представлены в таблице 37.

Таблица 37 – Поля мониторинга системы (код события 0)

Назначение	JSON	Тип
WMI: Тип события (создание = 0, удаление = 1, изменение = 2)	**wmi**	integer
WMI: SID пользователя	**wmi_sid**	string
WMI: Пространство имен	**ns**	string

Назначение	JSON	Тип
WMI: Путь до исполняемого файла	exe_path	string MANGLED
WMI: Имя файла	fname	string MANGLED
WMI: Имя фильтра событий	wmi_nm	string
WMI: Строка запроса	qstr	string
WMI: Имя файла скрипта	scrfname	string MANGLED
WMI: Текст скрипта	scrtxt	string
WMI: Имя источника	sname	string MANGLED
WMI: Путь	wmi_pth	string
WMI: SMTP	smtp	string
WMI: Фильтр	flt	string
WMI: Потребитель	cnsm	string
WMI: Идентификатор процесса клиента	wmi_clpid	unsigned
WMI: Уникальный идентификатор процесса клиента	wmi_cluuid	int
WMI: Время создания процесса клиента	wmi_cltime	timestamp (UTC)
WMI: Командная строка процесса клиента	wmi_clcmdl	string
WMI: Локальный запрос (0 или 1, по умолчанию 1)	wmi_local	int (0/1)
WMI: Идентификатор созданного процесса	wmi_crpid	unsigned
WMI: Уникальный идентификатор созданного процесса	wmi_cruuid	int (индекс в массиве GUID'ов)
WMI: Время создания созданного процесса	wmi_crtime	timestamp (UTC)
WMI: Командная строка созданного процесса	wmi_crcmdl	string
WMI: Имя машины, выполнившей запрос	wmi_cl	string
WMI: FQDN машины, выполнившей запрос	wmi_clfqdn	string
WMI: Имя пользователя клиента, выполнившего запрос	wmi_usr	string
WMI: Имя домена клиента, выполнившего запрос	wmi_dom	string
WMI: Имя вызываемого клиента	wmi_mthd	string



Важно

До ОС Windows 10 и Windows Server 2019, WMI-провайдер не предоставляет информацию о созданном процессе в WMI-запросе, соответственно, информация о созданном процессе будет отсутствовать в событии.

Пример строки события представлен в таблице 38.

Таблица 38 – События WMI

Подтип события	Описание
0	[Система] Зарегистрирован WMI-компонент с возможностью автозапуска по пути **wmi_pth**
1	[Система] Удален WMI-компонент с возможностью автозапуска по пути **wmi_pth**
2	[Система] Модифицирован WMI-компонент с возможностью автозапуска по пути **wmi_pth**

Системное время изменяется с **prev_stime** (предыдущее системное время) на **new_stime** (новое системное время).

Поле **sht** событий мониторинга системы может принимать следующие значения событий:

– 1 (штатное завершение работы компьютера);

– 2 (штатный переход компьютера в состояние сна или гибернации);

– 3 (штатная остановка агента).

7.8 События пользовательских сессий

Подтипы событий и их текстовые описания представлены в таблице 39.

Таблица 39 – Подтипы событий пользовательских сессий

Код события	Имя события	Описание
1	Сессии: Создание пользовательской сессии	Создание **%type%** сессии пользователя **sess_dom\sess_usr (sess_id)**
2	Сессии: Завершение пользовательской сессии	Завершение **%type%** сессии пользователя **sess_dom\sess_usr (sess_id)**
3	Сессии: Подключение к пользовательской сессии	Подключение к **%type%** сессии пользователя **sess_dom\sess_usr (sess_id)**
4	Сессии: Отключение от пользовательской сессии	Отключение от **%type%** сессии пользователя **sess_dom\sess_usr (sess_id)**
5	Сессии: Выполнен вход пользователя	Выполнен **%type2%** вход пользователя **sess_dom\sess_usr (sess_id)**
6	Сессии: Выполнен выход пользователя	Выполнен **%type2%** выход сессии пользователя **sess_dom\sess_usr (sess_id)**
7	Сессии: Блокирование сессии пользователя	Блокирование **%type%** сессии пользователя **sess_dom\sess_usr (sess_id)**
8	Сессии: Разблокирование сессии пользователя	Разблокирование **%type%** сессии пользователя **sess_dom\sess_usr (sess_id)**
9	Сессии: Изменен статус удаленного управления сессии пользователя	Изменен статус удаленного управления сессии пользователя **sess_dom\sess_usr (sess_id)**

Примечание

Обозначение **%type%** заменяется на «локальной», если тип сессии **local**, в противном случае заменяется на «дистанционной». Обозначение **%type2%** заменяется на «локальный», если тип сессии local, иначе заменяется на «дистанционный».

Параметр **sess_opt** (тип дистанционного управления) может принимать одно из значений, указанных в таблице 40.

Таблица 40 – Типы дистанционного управления

Значение	Описание
0	Дистанционное управление отключено
1	Пользователь имеет полный контроль над сеансом пользователя с разрешения локального пользователя
2	Пользователь имеет полный контроль над сеансом пользователя, разрешение локального пользователя не требуется
3	Пользователь может просматривать сеанс удаленно с разрешения локального пользователя, удаленный пользователь не может активно управлять сеансом
4	Пользователь может удаленно просматривать сеанс, но не может активно управлять сеансом, разрешение локального пользователя не требуется

Параметр **sess_proto** (тип дистанционного управления) принимает следующие значения:

– 0 (консольная сессия);

– 2 (RDP-сессия).

Поля событий мониторинга сессий представлены в таблице 41.

Таблица 41 – Поля мониторинга сессий

Назначение	JSON	Тип
Локальная сессия	**local**	int (0/1)
Номер сессии	**sess_id**	unsigned
Тип дистанционного управления	**sess_opt**	unsigned (опционально
Тип сессии	**sess_proto**	unsigned (опционально)
Имя оконной станции	**win_stn**	string (опционально)
Имя клиента	**sess_cl**	string (опционально)
IP-адрес клиента	**sess_claddr**	string (опционально)

Имя пользователя	**sess_usr**	string (опционально)
Имя домена/компьютера	**sess_dom**	string (опционально)

Анализ шаблонов поведения может помочь аналитикам заметить отклонения, которые указывают на активность злоумышленников: необычное время активности пользователей, многократный подбор учетных данных и другие аномалии в поведении пользователей.

7.9 События монитора вызовов

Подтипы событий монитора вызовов представлены в таблице 42.

Таблица 42 – Подтипы событий монитора вызовов

Код события	Имя события	Описание
0	Вызовы: RPC	RPC (remote procedure call)

События монитора вызовов (RPC-вызовы) представлены в таблице 43.

Таблица 43 – Поля монитора вызовов (RPC вызовы)

Назначение	JSON	Тип
RPC: UUID интерфейса	**rpc_id**	unsigned (индекс в массиве GUID-ов)
RPC: Номер процедуры	**rpc_opnum**	unsigned
RPC: Имя процедуры	**rpc_opname**	string (опционально)
RPC: Протокол	**rpc_proto**	unsigned (опционально)
RPC: Сервис аутентификации	**rpc_authsvc**	unsigned (опционально)
RPC: Конечная точка	**endp**	string (опционально)
RPC: Сетевой адрес	**n_addr**	string (опционально)
RPC: Уникальный идентификатор процесса клиента	**c_uuid**	unsigned (индекс в массиве GUID-ов)
RPC: PID процесса клиента	**c_pid**	integer
RPC: Исполняемый файл процесса клиента	**c_path**	string MANGLED
RPC: Уникальный идентификатор процесса сервера	**s_uuid**	unsigned (индекс в массиве GUID-ов) (опционально)
RPC: PID процесса сервера	**s_pid**	integer (опционально)
RPC: Исполняемый файл процесса сервера	**s_path**	string MANGLED (опционально)

Поле **rpc_proto** принимает следующие значения:

1 – TCP;

2 – Named Pipes;

3 – LRPC;

4 – HTTP.

Поле **rpc_authsvc** принимает следующие значения:

0x09 – Negotiate;

0x0A – NTLM;

0x0E – SChannel;

0x10 – Kerberos;

0x14 – Kernel.

В поле **Описание** таблицы событий на странице **Активность**, если **n_addr** пустой или не задан, выводится сообщение в виде:

[Вызовы] Процесс **c_path (c_pid)** выполнил удаленный вызов процедуры **endp** по интерфейсу **rpc_id** в процессе **s_path (s_pid)**.

Если **n_addr** задан, тогда выводится сообщение в виде:

[Вызовы] Процесс **c_path (c_pid)** выполнил удаленный вызов процедуры **n_addr:endp** по интерфейсу **rpc_id** в процессе **s_path (s_pid)**.

7.10 События модуля Антишифра

Подтипы событий и их текстовые описания представлены в таблице 44.

Таблица 44 – Подтипы событий модуля Антишифра

Код события	Имя события	Описание
0	Защита файлов: Заблокирован вредоносный процесс	Заблокирован вредоносный процесс
1	Создана резервная копия файла	Создана резервная копия файла **name**

Поля событий модуля защиты от вирусов-шифровальщиков представлены в таблице 45.

Таблица 45 – Поля событий модуля Антишифра

Назначение	JSON	Тип
Количество открытий/созданий файлов с последующими обращениями к ним	cf_ac	unsigned
Количество открытых файлов из защищаемых каталогов	cf_oc	unsigned
Количество созданных процессом файлов после активации мониторинга	cf_cc	unsigned
Количество удалённых файлов в защищаемых каталогах	si_dc	unsigned
Количество переименованных файлов в защищаемых каталогах	si_rc	unsigned
Количество перемещённых файлов в защищаемые каталоги	si_mi	unsigned
Количество перемещённых файлов из защищаемых каталогов	si_mo	unsigned
Количество файлов из защищаемых каталогов, которые только читали	ro_fc	unsigned
Количество файлов из защищаемых каталогов, в которые только писали	wo_fc	unsigned
Количество файлов из защищаемых каталогов, которые читали и писали	rw_fc	unsigned
Среднее значений файловой энтропии по чтению	pr_re	unsigned
Среднее значений файловой энтропии по записи	pr_we	unsigned
Правило блокировки процесса	pr_lr	unsigned
Реакция модуля на идентификацию шифровальщика	pr_ra	unsigned
Количество файлов с нарушенной целостностью	a_fcc	unsigned
Количество файлов с превышенной энтропией	a_eoc	unsigned
Количество расширений файлов, из которых читали	exrac_	unsigned
Количество расширений файлов, в которые писали	exwac_	unsigned
Количество уникальных расширений файлов, из которых только читали	exurac	unsigned
Количество уникальных расширений файлов, в которые только писали	exuwac	unsigned
Категории файлов, к которым осуществлялся доступ	gf_am	unsigned
Категории файлов, из которых производилось чтение	gf_rm	unsigned
Категории файлов, в которые производилось запись	gf_wm	unsigned
Категории файлов, которые удалялись	gf_dm	unsigned

Энтропия файла в контексте информационной безопасности — это статистическая мера неопределенности или случайности данных, содержащихся в файле. Она измеряет, насколько непредсказуемы или хаотичны байты, из которых состоит файл. Низкая энтропия (от 0 до 4) характерна для структурированных данных (тексты, логи, XML, несжатые исполняемые файлы), а высокая энтропия (6-8 и более) типична для случайных данных (зашифрованные файлы, сжатые архивы, упакованные исполняемые файлы, медиафайлы)

7.11 События модуля контроля USB

Тип события – **Контроль USB** (**t**:9 в DSL). Подтипы событий (**st**) и их текстовые описания представлены в таблице 46.

Таблица 46 – Подтипы событий модуля контроля USB

Код события	Имя события	Описание
0	Устройство USB подключено	Подключено устройство **usb_mr usb_pt** MI **usb_mi**
1	Устройство USB отключено	Отключено устройство **usb_mr usb_pt** MI **usb_mi**
2	Зафиксирована запрещенная попытка чтения	Заблокировано чтение с устройства **usb_mr usb_pt** MI **usb_mi**
3	Зафиксирована запрещенная попытка записи	Заблокирована запись на устройство **usb_mr usb_pt** MI **usb_mi**
4	Зафиксирована запрещенная попытка выполнения управляющего запроса	Заблокировано конфигурирование устройства **usb_mr usb_pt** MI **usb_mi**
5	Зафиксирована запрещенная попытка запуска исполняемого кода	Заблокирован запуск исполняемого файла **usb_exec** с накопителя **usb_mr usb_pt**
6	Статистика чтения/записи данных	**usb_mr usb_pt usb_mi :** прочитано **usb_cr** байт, записано **usb_cw** байт

Поля событий модуля контроля USB указаны в таблице 47.

Таблица 47 – События модуля контроля USB

Назначение	Тип	JSON
Тип контролируемого устройства	uint8	**usb_dt**
Класс устройства USB	uint8	**usb_dc**
Подкласс устройства USB	uint8	**usb_dsc**
Идентификатор производителя (VID)	uint16	**usb_vid**
Идентификатор продукта (PID)	uint16	**usb_pid**
Номер интерфейса (MI)	uint8	**usb_mi**
Серийный номер устройства	string	**usb_sn**
Наименование производителя	string	**usb_mr**
Наименование продукта	string	**usb_pt**
Имя модуля, который был запущен с носителя	string	**usb_exec**
Количество прочитанных байтов	uint64	**usb_cr**
Количество записанных байтов	uint64	**usb_cw**
Общее количество прочитанных байтов	uint64	**usb_tr**
Общее количество записанных байтов	uint64	**usb_tw**

7.12 События статистики

Поля событий статистики указаны в таблице 48.

Таблица 48 – События статистики

Назначение	Тип	JSON
Загрузка процессора	unsigned	**cpu_load**
Загрузка памяти	unsigned	**mem_load**
Количество процессов	unsigned	**processes**
Количество нитей	unsigned	**threads**
Количество открытых описателей	unsigned	**handles**
Объем прочитанных с диска данных в секунду	int64	**disk_read**
Объем записанных на диск данных в секунду	int64	**disk_write**
Объем переданных данных по сети в секунду	int64	**net_send**
Объем принятых данных по сети в секунду	int64	**net_recv**
Время регистрации событий (UTC)	timestamp	**time**
Временная зона	string	**timezone**
Признак нахождения в режиме network containment	int(0/1)	**net_locked**
Общее количество сетевых соединений	unsigned	**connections**
Состояние функций защиты (0 – включены, 1 – выключены)	int(0/1)	**disabled**
Время последнего обновления аналитики по наборам	json_object	**config_time**
Причина завершения работы	unsigned	**shutdown**
Парольная защита от удаления агента (1 – включена, 0 –выключена)	int(0/1)	**protect**
Количество системных ошибок	unsigned	**sys_errs**
Количество прикладных ошибок	unsigned	**app_errs**
Максимальная скорость отправки событий (Кбит/сек)	unsigned	**netlimit**
Загрузка процессора службой агента	unsigned	**svc_cpu_load**

Назначение	Тип	JSON
Использование памяти службой (Мбайт) агента	unsigned	**svc_mem_usage**
Использование памяти драйвером (Мбайт) агента	unsigned	**drv_mem_usage**
Загрузка процессора драйвером агента	unsigned	**drv_cpu_load**
Загрузка процессора монитором процессов	unsigned	**drv_pm_load**
Загрузка процессора монитором сетевых соединений	unsigned	**drv_net_load**
Загрузка процессора монитором файловых операций	unsigned	**drv_fs_load**
Загрузка процессора монитором реестра	unsigned	**drv_reg_load**
Загрузка процессора механизмом проверки индикаторов атак/исключений	unsigned	**drv_ioa_load**
Выборка самых тяжеловесных индикаторов атак	json_object	**ioa_util**
Выборка самых тяжеловесных исключений	json_object	**excl_util**
Максимальная скорость отправки событий (Кбит/сек)	unsigned	**netlimit**
Режим работы агента	unsigned	**mode**
Количество блокировок реагирования по командным строкам	unsigned	**cmdl_locks**
Количество файловых блокировок реагирования	unsigned	**file_locks**
Количество сетевых блокировок реагирования	unsigned	**net_locks**

Поле **shutdown** может принимать следующие значения:

1) 0 – агент работает в штатном режиме;

2) 1 – штатное завершение работы компьютера;

3) 2 – штатный переход компьютера в состояние сна или гибернации;

4) 3 – штатная остановка агента.

DSL-запросы по статистике срабатывают, если в поле **Источник события** на странице **Активность** выбран источник **Статистика**.

Поле **ioa_util** является json_object-ом, свойствами которого являются идентификаторы индикаторов атак, а значениями базисные пункты (сотые доли процента) от общего времени проверки индикаторов атак, начиная с момента получения индикаторов агентом. Содержит максимум десять пар значений для самых тяжеловесных индикаторов. Данное поле может отсутствовать, если индикаторы не загружены на агенте, или их проверка не осуществлялась по каким-либо причинам. Поле **excl_util** аналогично **ioa_util**, только его свойствами являются идентификаторы исключений.

7.13 Телеметрия RT Protect EDR

Категории функций телеметрии, которые возможно обнаружить с помощью RT Protect EDR представлены в таблице 49.

Таблица 49 – Телеметрия RT Protect EDR

Категория функций телеметрии	Подкатегория	Реализация в RT Protect EDR
Процессы	Создание процесса	Да
	Завершение процесса	Да
	Доступ к процессу	Да
	Загрузка образа/библиотеки	Да
	Создание нити в стороннем процессе	Да
	Активность, связанная с подменой процесса	Да
Файлы	Создание файла	Да
	Открытие файла	Реализовано только для файлов с потенциально активным содержимым
	Удаление файла	Да
	Модификация файла	Да
	Переименование файла	Да
	Создание локальной учетной записи	Доступно с помощью журнала Windows

Категория функций телеметрии	Подкатегория	Реализация в RT Protect EDR
Активность, связанная с учетной записью пользователя	Модификация локальной учетной записи	Доступно с помощью журнала Windows
	Удаление локальной учетной записи	Доступно с помощью журнала Windows
	Вход в учетную запись	Да
	Выход из учетной записи	Да
Сетевая активность	TCP-соединение	Да
	UDP-соединение	Да
	URL	В данный момент не реализовано
	DNS-запрос	Да
	Загрузка файла	Реализовано только для файлов, загруженных с помощью браузеров и их компонентов
Хеш-алгоритмы	MD5	Да
	SHA	Да
	IMPHASH	В данный момент не реализовано
Активность реестра	Создание ключа/значения	Да
	Модификация ключа/значения	Да
	Удаление ключа/значения	Да
Активность, связанная с планировщиком задач	Создание задачи	Реализовано с помощью индикатора атак
	Модификация задачи	Реализовано с помощью индикатора атак
	Удаление задачи	Реализовано с помощью индикатора атак
Службы	Создание службы	Реализовано с помощью индикатора атак
	Модификация службы	Реализовано с помощью индикатора атак
	Удаление службы	Реализовано с помощью индикатора атак
Активность драйвера/модуля	Загрузка драйвера	Да
	Модификация драйвера	В данный момент не реализовано
	Выгрузка драйвера	В данный момент не реализовано
Операции с устройствами	Монтирование виртуального диска	В данный момент не реализовано

Категория функций телеметрии	Подкатегория	Реализация в RT Protect EDR
	Размонтирование USB-устройства	Да (при включении модуля USB)
	Монтирование USB-устройства	Да (при включении модуля USB)
Другие релевантные события	Модификация групповых политик	В данный момент не реализовано
Активность, связанная с именованными каналами	Создание именованного канала	Да
	Соединение с именованным каналом	Да
Системные операции EDR	Запуск агента	Да
	Остановка агента	Да
	Установка агента	В данный момент не реализовано
	Удаление агента	В данный момент не реализовано
	Агент keep-alive	Да
	Ошибки агента	Да
WMI активность	WmiEventConsumerToFilter	Да
	WmiEventConsumer	Да
	WmiEventFilter	Да
Активность BIT JOBS	Активность BIT JOBS	Реализовано с помощью индикатора атак
Активность PowerShell	Активность блока сценариев	Реализовано с помощью индикатора атак

8. Интерфейс Программы

8.1 Окно авторизации и общие сведения

Модуль управления, находящийся на сервере, предназначен для следующих задач:

– администрирование агентов, установленных на АРМ;

– просмотр событий и инцидентов;

– реагирование на определенные события и инциденты;

– оценка активности на АРМ и т.д.

Вход в Программу производится из поддерживаемой версии браузера. Чтобы открыть окно авторизации, необходимо в строке браузера ввести имя сервера или его ip-адрес. После ввода в строке браузера корректных данных откроется окно авторизации (рис. 7).

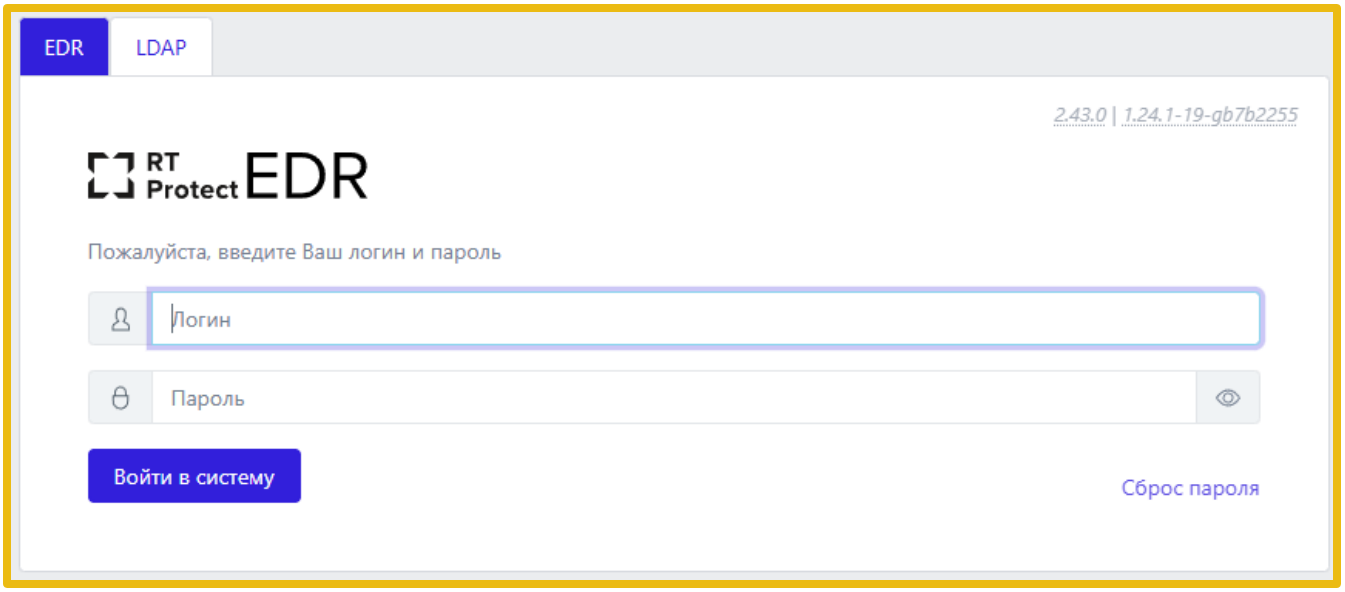


Рисунок 7 – Окно авторизации

При первоначальном входе на вновь установленный сервер, в окне авторизации по вкладке EDR, требуется указать логин – admin и пароль – admin (пользователь создается по умолчанию).

Далее следует в разделе **Параметры** в подразделе **Пользователи и роли** создать пользователя и назначить ему роль с соответствующими правами.

При входе в окне авторизации по вкладке LDAP, следует указать логин и пароль пользователя, которые содержаться в информации о пользователе, созданном в LDAP.

Подробная информация о LDAP-соединении содержится в разделе **Интеграции**.

При входе в EDR по вкладке LDAP создается пользователь с префиксом LDAP_имя. Позже можно переопределить пользователя, привязав его к пользователю EDR.

После ввода в окне авторизации пароля и логина открывается основное окно Программы (рис. 8).

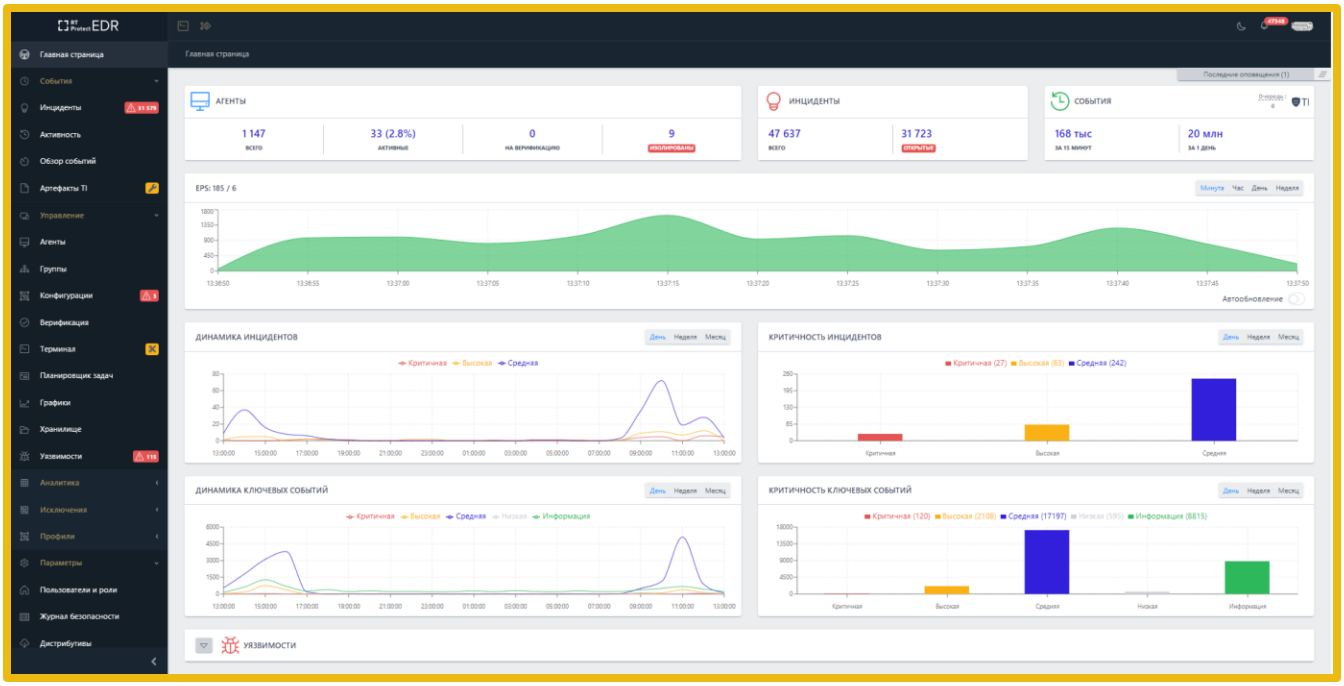


Рисунок 8 – Основное окно Программы

Если в течение 5 минут пользователь выполнит 4 или более неудачных попыток входа, то его учетная запись будет заблокирована. В этом случае разблокировать такого пользователя сможет только администратор или учетная запись пользователя будет разблокирована после 24-часового блока.

Функции, доступные в интерфейсе административного модуля управления:

– просмотр событий и инцидентов;

– администрирование машин, на которых установлен модуль агента, и учетных записей пользователей;

– настройка и просмотр правил детектирования;

– настройка и просмотр конфигурационных параметров;

– настройка и просмотр профилей Антишифра;

– настройка и просмотр профилей безопасности агента;

– настройка и просмотр профилей контроля USB-устройств;

– просмотр действий пользователей;

– просмотр параметров работы Программы.

В левой части основного окна Программы (см. рис. 8) находится вертикальная панель управления, доступная администратору для выполнения различных настроек и просмотра информации по разделам. Пользователь Программы может свернуть большую часть разделов, оставив только нужные ему, или скрыть панель управления, нажав кнопку  в нижней части панели.

В правой части окна представлена информация выбранного раздела и основной инструментарий для работы администратора и аналитика.

В нижней части страницы находится информация о товарном знаке компании – 

.

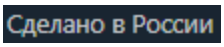
В центре рядом с товарным знаком отображается текущая версия Программы:

1) Frontend – 

;

2) Backend – 

.

Справа от текущей версии Программы отображается надпись о том, где «RT Protect EDR» разработана – 

.

8.2 Горизонтальная панель управления

В верхней части окна находится горизонтальная панель управления.

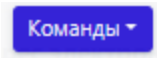
Вертикальная и горизонтальная панели управления являются общими для всех страниц и разделов Программы.

При нажатии кнопки **Темная тема** () основное окно Программы меняется соответствующим образом (большая часть окна Программы становится темной). Для возврата к первоначальному виду необходимо нажать кнопку **Светлая тема** ().

На горизонтальной панели также может присутствовать значок индикации о необходимости проверки состояния сервера  . В этом случае следует проверить подсистему мониторинга состояния сервера, например, Gatus, Zabbix и т.д. (если такая подсистема настроена на сервере) для получения дополнительной информации.

8.2.1. **Онлайн-терминал**

На горизонтальной панели администратор может запустить терминальную онлайн-сессию с помощью кнопки  . Функционал live-сессии повторяет функционал интерпретатора командной строки Windows или Bash (для агентов Linux).

В онлайн-терминале можно выполнять нативные команды RT Protect EDR. Список этих команд отображается при нажатии ЛКМ на иконку 

в окне запуска сессии онлайн-терминала. Подробная информация о командах онлайн-терминала содержится в документе «Руководство аналитика RT Protect EDR».

8.2.2. **Оповещения**

Страница **Оповещения** позволяет просмотреть важную информацию, связанную с защищаемой инфраструктурой.

Для перехода на страницу необходимо нажать на кнопку **Оповещения** 

, которая находится справа от кнопок **Темная тема/Светлая тема.**

В выделенной красным цветом области иконки указано число непрочитанных оповещений, полученных пользователем.

Информация об оповещениях приходит в режиме реального времени и требует совершения действий со стороны пользователей Программы.

Данные о событиях представлены в табличном виде на правой панели отображения информации.

В верхней части, над таблицей, находятся следующие элементы фильтрации:

– Показывать по;

– Критичность;

– Статус оповещения;

– Тип оповещения.

С помощью фильтра **Показывать по** задается значение числа оповещений, отображаемых на странице таблицы: 10, 20, 50, 100 или 500 оповещений.

Если количество записей в таблице превышает установленное количество записей, отображаемых на странице, в верхней и нижней части таблицы отобразится пагинатор, с помощью которого можно переходить по страницам записей (рис. 9).

Пагинатор является сквозным инструментом для всего модуля администрирования, то есть отображается на любой странице с фильтрами.



Рисунок 9 – Пагинатор

С помощью фильтра **Критичность** задается уровень угрозы, которому должны соответствовать отображаемые в таблице оповещения.

Все оповещения можно отфильтровать по следующим уровням угрозы:

1) **Не задана** – при выборе фильтра информация в таблице показывается вне зависимости от уровня угрозы, установленной для события, о котором пришло оповещение;
2) **Информация** – при выборе фильтра в таблице отобразятся оповещения для событий, определенных Программой как события уровня информации, не имеющей признаков угрозы;
3) **Низкая** – при выборе фильтра в таблице отобразятся оповещения для событий, определенных Программой как события маловероятного уровня угрозы;
4) **Средняя** – при выборе фильтра в таблице отобразятся оповещения для событий, определенных Программой как события средневероятного уровня угрозы;
5) **Высокая** – при выборе фильтра в таблице отобразятся оповещения для событий, определенных Программой как события вероятного уровня угрозы;

6) **Критичная** – при выборе фильтра в таблице отобразятся оповещения для событий, определенных Программой как события наиболее опасные для защищаемой IT-инфраструктуры или события крайне вероятного уровня угрозы.

Подробнее о методах и способах реагирования на различные угрозы можно узнать в документе «Руководство аналитика RT Protect EDR».

С помощью фильтра **Статус оповещения** задается фильтрация оповещений по следующим статусам:

1) **Не задан** – при выборе фильтра в таблице будут показаны как прочитанные, так и непрочитанные оповещения;
2) **Прочитанные** – при выборе фильтра в таблице будут показаны только прочитанные пользователем оповещения;
3) **Непрочитанные** – при выборе фильтра в таблице будут показаны только непрочитанные пользователем оповещения.

С помощью фильтра **Тип оповещения** задается фильтрация оповещений по следующим типам:

1) **Все типы** – при выборе на странице будут представлены все типы оповещений;
2) **Инцидент** – при выборе фильтра в таблице будут показаны оповещения об инцидентах;
3) **Потеря связи с агентом** – при выборе фильтра в таблице будут показаны события, которые указывают на разрыв связи агента с модулем администрирования;
4) **Изменился состав ПО** – при выборе фильтра в таблице будут показаны агенты, на которых был изменен состав ПО (на агентах с включенной функцией отслеживания золотого образа).

Ниже строки с фильтрами находится строка с элементами навигации в таблицах (см. рис. 9).

В этой же строке находится элемент отображения количества выбранных в таблице оповещений Выбрано: 0 из 18, а также элемент отображения количества найденных и показанных результатов Найдено: 18, показано: с 1 по 10.

Все элементы этой строки дублируются в нижней части окна Программы, снизу от таблицы, для удобства просмотра и навигации.

В таблице с оповещениями содержатся следующие поля:

1) **Кнопка выбора элемента таблицы** (содержит чекбокс ☐ и элемент раскрытия дополнительной информации о событии ›);

2) **Отметить как прочитанное** (в шапке содержится значок , в полях столбца содержится значок , при наведении на который отображается запись **Отметить как прочитанное**);
3) Тип;
4) Название;
5) Критичность;
6) Время регистрации.

Кнопка выбора является элементом, с помощью которого пользователь Программы может выбрать одну или несколько записей в таблице и применить соответствующую операцию к выбранным записям. Например, в окне просмотра **Оповещения** такой операцией является Прочитать выбранные.

Отмеченные пользователем элементы после нажатия кнопки помечаются как прочитанные. Схожую функциональность имеет поле **Отметить как прочитанное**. При нажатии кнопки выбранное оповещение помечается как прочитанное.

Пользователь может отметить все оповещения как прочитанные с помощью операции **Прочитать все**.

Оповещения можно просматривать с помощью виджета **Последние оповещения** в правом верхнем углу на **Главной странице** (рис. 10).

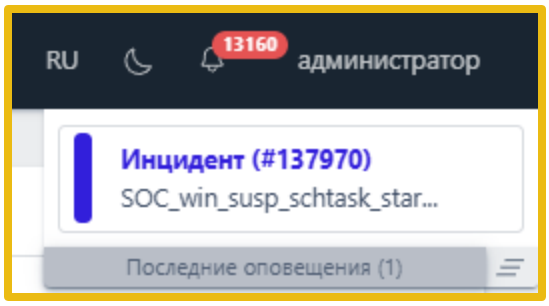


Рисунок 10 –Последние оповещения на Главной странице

При нажатии ЛКМ на значок в строке оповещения открывается область дополнительной информации. Дополнительная информация в зависимости от выбора типа оповещения будет отличаться.

Название инцидента позволяет быстро перейти к странице **Инцидент** для совершения дополнительных действий по выбранному инциденту.

В строке **Описание (при создании)** отображается описание инцидента, в случае его отсутствия поле останется пустым.

Имя агента в строке с оповещениями по типам **Изменился состав ПО** и **Потеря связи с агентом** является активной ссылкой, при нажатии по которой ЛКМ можно быстро перейти на страницу **Агент** (которая соответствует агенту, указанному в оповещении).

8.2.3. Меню «Пользователь»

При нажатии ЛКМ на имени пользователя (логин) в правой верхней части основного окна Программы открывается меню работы с учетной записью, в котором представлены подменю **Профиль** и кнопка **Выход**, для выхода из Программы с текущего устройства (рис. 11).

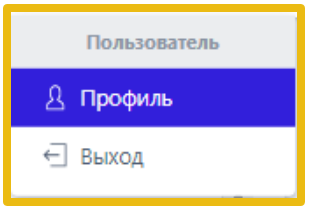


Рисунок 11 – Меню «Пользователь»

Подменю **Профиль** разделено на две информационные области: **Профиль** и **Сессии и устройства**.

Профиль – позволяет изменять пользователю имя, фамилию и адрес электронной почты для своей учетной записи, а также изменять пароль с помощью кнопки Сменить пароль. Также в профиле пользователя можно увидеть его роль и его идентификатор в Программе. Здесь же настраивается возможность получать уведомления об инцидентах на почту и настраивать двухфакторную аутентификацию (после ввода пароля при входе в учетную запись на почту будет приходить числовой код, который необходимо ввести). Аутентификационный код приходит на электронную почту, указанную в профиле.

Для сохранения и применения измененной конфигурации необходимо нажать кнопку Сохранить. При нажатии кнопки **Сменить пароль** открывается окно для смены пароля (рис. 12).

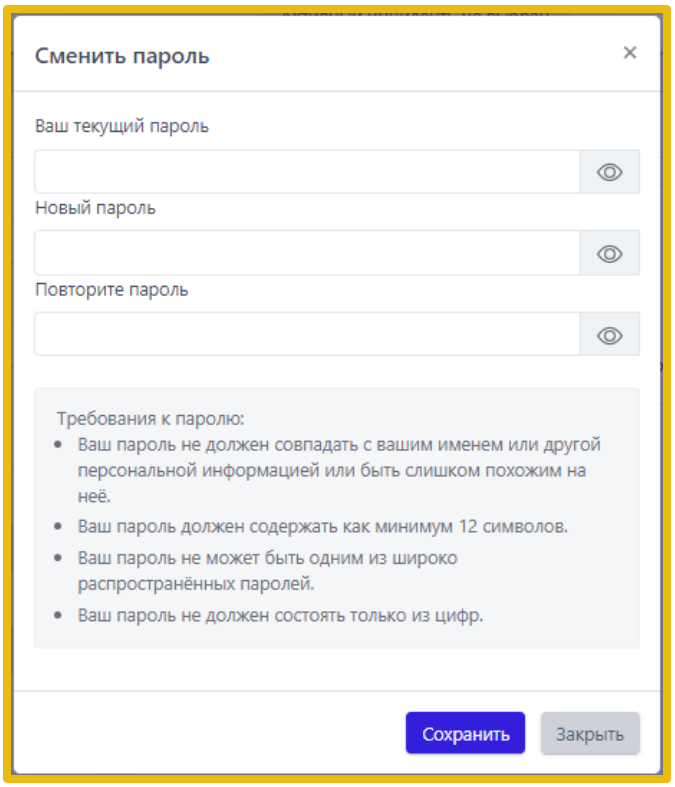


Рисунок 12 – Окно смены пароля

Введенный пароль должен соответствовать требованиям, указанным в нижней части окна:

– пароль не должен совпадать с именем пользователя или другой персональной информацией или быть слишком похожим на неё;

– пароль должен содержать как минимум 12 символов;

– пароль не может быть одним из широко распространённых паролей;

– пароль не должен состоять только из цифр.

Для смены пароля необходимо ввести старый и новый пароль с подтверждением в соответствующие поля и нажать кнопку Сохранить.

Сессии и устройства – позволяет узнавать информацию о сессиях и устройствах, с которых осуществлялся вход в Программу. В области просмотра реализована функция выхода из учетной записи текущего пользователя на всех устройствах, с которых осуществлялся вход в административный модуль Программы. Для выхода со всех устройств необходимо нажать кнопку Выйти на всех устройствах.

8.3 Главная страница

На рисунке 8 представлен раздел **Главная страница** модуля управления.

При открытии раздела **Главная страница** на правой панели отобразится страница со следующими информационными областями:

– Агенты;

– Инциденты;

– События;

– EPS;

– Динамика инцидентов;

– Критичность инцидентов;

– Динамика ключевых событий;

– Критичность ключевых событий;

– Уязвимости.

В области просмотра **Агенты** показывается состояние всех установленных агентов:

1) Общее число агентов;
2) Количество активных агентов;
3) Количество агентов, ожидающих верификацию;
4) Количество изолированных агентов.

При нажатии на числовые значения в области просмотра **Агенты** происходит переход в раздел **Агенты**, в котором можно изучить подробную информацию о выбранной категории агентов.

В области просмотра **Инциденты** показываются все зарегистрированные в Программе инциденты и открытые инциденты, по которым отсутствует решение.

При клике по числовому значению выбранной категории инцидентов происходит переход к разделу **Инциденты**, в котором представлена более подробная информация о зарегистрированных в Программе инцидентах (см. пункт 8.4.1).

В области просмотра **События** администратор может увидеть, сколько событий пришло от всех верифицированных и неизолированных агентов в последние 15 минут, а также за последний день.

Также здесь можно увидеть, какое количество пакетов с событиями находится в очереди на запись в базу данных, и тайминги проверки артефактов TI.

В области **EPS** содержится интерактивный график, показывающий загруженность модуля администрирования. Отображается количество событий за секунду, приходящее от активных агентов.

На графике имеются определенные интервалы (5 сек), отмеченные точками, при наведении на которые указателя мыши появляется всплывающее окно с отображением времени и количества событий (рис. 13).

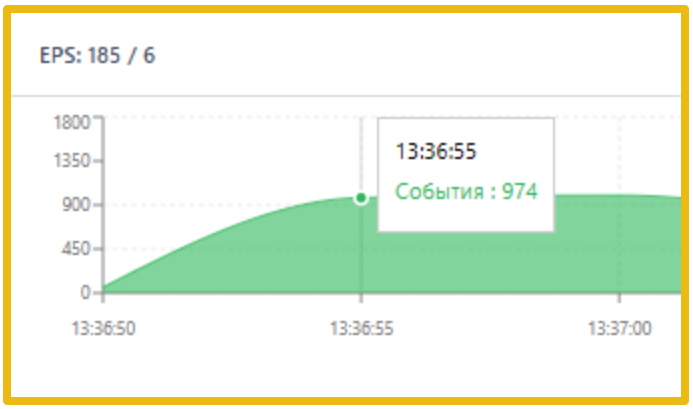
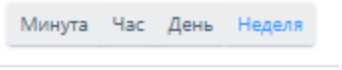


Рисунок 13 – Отображение EPS на графике с интервалом 5 сек

В области отображения EPS имеется возможность изменять интервал для отображения событий с помощью иконок 

, находящихся в правом верхнем углу.

В области **Динамика инцидентов** отображаются графики, на которых можно проследить динамику появления инцидентов по критичности за день, неделю либо за месяц.

График разделен контрольными точками на отрезки с периодичностью в один день, при наведении указателя мыши на отрезок появляется всплывающее окно, показывающее количество инцидентов. Динамику изменения инцидентов можно просмотреть за период день, неделя или месяц.

В области **Критичность инцидентов** администратор может посмотреть в виде диаграмм распределение зарегистрированных инцидентов по степени критичности (с указанием количества), за день/неделю/месяц.

В области **Динамика ключевых событий** отображаются графики, на которых можно проследить динамику появления ключевых событий по критичности за день, неделю либо за месяц.

Ключевые события здесь – это события с уровнем критичности **Средняя** или выше и события, у которых назначено действие **Блокировать**.

В области **Критичность ключевых событий** администратор может посмотреть в виде диаграмм распределение зарегистрированных ключевых событий по степени критичности (с указанием количества), за день/неделю/месяц.

Записи критичности инцидентов являются активными ссылками, при нажатии по записи или цветной колонке левой кнопкой мыши происходит переход на страницу **Инциденты**, где показаны записи по выбранной критичности.

В области **Уязвимости** показана информация о последних инцидентах с трендовыми уязвимостями, а также инфографика с количеством программ, в которых содержатся и отсутствуют уязвимости, количеством уязвимостей по степени критичности и количеством агентов, в которых содержатся и отсутствуют уязвимости.

8.4 События

В серверной части Программы обрабатываются события активности, происходящей на конечных точках с установленными на них агентами. Все обрабатываемые события можно разделить на две больших категории: обнаружения и телеметрия.

Обнаружения – это события, которые EDR с низкой и выше степенью вероятности (Низкая+ критичность события) идентифицирует как опасные или вредоносные. Обнаружения помечаются значком ⚠ в поле **Описание**.

Система обнаружения и оповещения в Программе охватывает события множества компьютерных подсистем: файловая подсистема, сетевые события, события, происходящие с процессами, реестром и т.д.

Телеметрия – все события, регистрируемые Программой, с уровнем критичности **Информация** (события, которые передаются для обработки в серверную часть Программы от клиентской части).

Для любого события или группы событий в Программе может быть создан **Инцидент**. В основном, инциденты назначаются Программой автоматически на основе обнаружений, в случае, если критичность события равняется Средней+ критичности.

Примечание

Кроме автоматического создания инцидентов в «RT Protect EDR» предусмотрен функционал создания инцидента вручную, что позволяет аналитикам проводить ретроспективные расследования, конфигурируя инциденты самостоятельно.

События всех категорий можно просмотреть в области **События**. Здесь содержатся разделы **Инциденты** и **Активность**. На страницах разделов представлена исчерпывающая информация о событиях, детектируемых на агентах и обрабатываемых на сервере, а также инцидентах, связанных с этими событиями.

Подробная информация о расследованиях и анализе событий, обнаруживаемых Программой, содержится в документе «Руководство аналитика RT Protect EDR».

8.4.1. Инциденты

На странице раздела **Инциденты** содержится информация обо всех зарегистрированных инцидентах.

Инциденты генерируются Программой в автоматическом режиме при обнаружении событий, которые могут косвенно или явно интерпретироваться как вредоносные. В инциденты попадают все события-обнаружения, регулируемые правилами индикации, установленными в Программе по умолчанию, а также правилами, представленными в области **Аналитика** (кроме событий раздела **Журналы**) (см. подраздел 8.6). Кроме автоматической генерации инцидентов в Программе предусмотрен функционал добавления событий в инциденты в ручном режиме (см. пункт 8.4.2).

Важно

Инцидент формируется на странице **Инциденты**, если уровень критичности хотя бы одного из событий этого инцидента оценивается равной или выше уровня критичности **Средняя**.

Для просмотра информации по всем инцидентам необходимо удалить настройки фильтрации, установленные по умолчанию, нажав кнопку **Сбросить фильтры**. После изменения настроек на странице **Инциденты** будут показаны все инциденты, зарегистрированные в Программе.

Работа с инцидентами

Страница раздела **Инциденты** представлена на рисунке 14. Информация об инцидентах на странице раздела представлена в табличном виде. По умолчанию в таблице отображаются все незакрытые инциденты, в том числе назначенные на текущего пользователя.

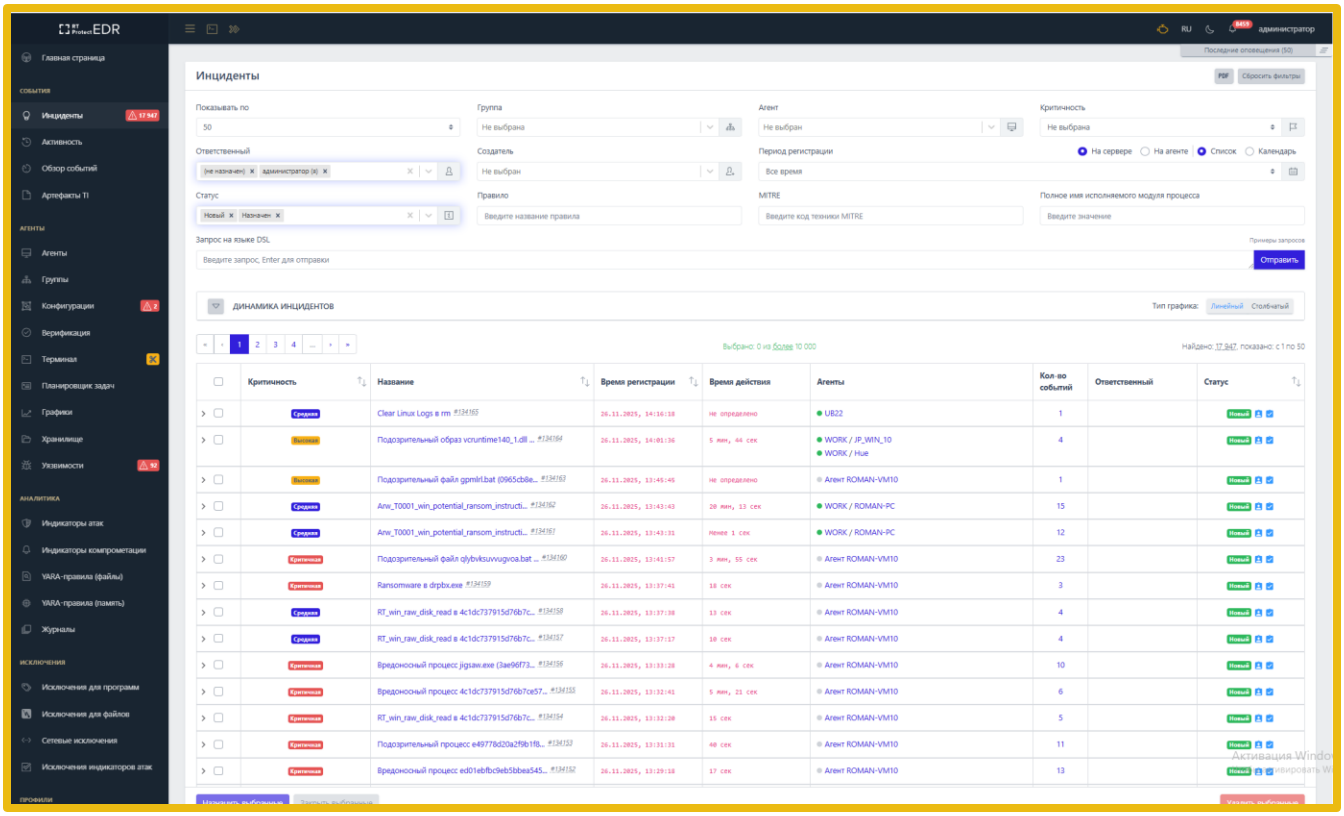


Рисунок 14 – Страница «Инциденты»

Сверху таблицы с инцидентами в поле **Динамика инцидентов** содержатся графики, на которых можно проследить динамику возникновения инцидентов в соответствии с выбранными фильтрами.

Чтобы показать график, необходимо нажать кнопку . График может быть представлен как в линейном, так и в столбчатом виде.

Чтобы переключить отображение графика, необходимо выбрать один из двух типов графика в области **Тип графика** (**Линейный** или **Столбчатый**).

В таблице инцидентов представлены следующие поля:

1) Флаг выбора инцидента ( );
2) Критичность;

3) Название;
4) Время регистрации;
5) Время действия;
6) Агенты;
7) Кол-во событий;
8) Ответственный;
9) Статус.

В поле с флагом выбора инцидентов содержится кнопка раскрытия дополнительной информации о событиях, включенных в инцидент ( ). При клике на значок снизу от строки инцидента открывается дополнительная информационная область, в которой пользователь может просмотреть данные об инциденте.

Инциденты, которые были созданы на основе правил из внешнего набора (набора, созданного на TI-платформе), помечаются в строке **Правила** значком TI. При наведении указателя мыши на данную иконку появится окно с всплывающим сообщением, представленным на рисунке 15.

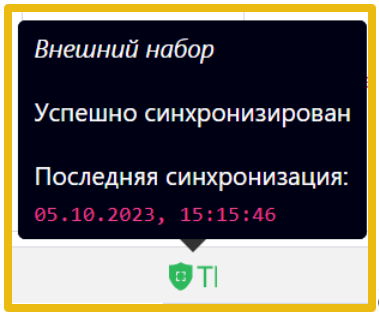


Рисунок 15 – Всплывающее сообщение с информацией о внешнем наборе

В поле дополнительной информации об инциденте в строке **Техники MITRE** представлены техники, которые покрывает данное правило.

Название техники, например, T1012 Query Registry является активной ссылкой, при нажатии по которой левой кнопкой мыши происходит переход на страницу сайта https://attack.mitre.org/techniques с полным описанием этой техники. При наведении указателя мыши на название техники появляется всплывающее окно с кратким описанием техники.

В поле **Критичность** показывается информация о степени критичности инцидента. Всего предусмотрено пять уровней критичности: **Информация** (наименее критичный уровень инцидента), **Низкий** (инциденты с критичностью **Низкий** и **Информация** могут быть созданы только вручную), **Средний**, **Высокий**, **Критичный** (наиболее критичный уровень инцидента).

В поле **Название** таблицы **Инциденты** находится имя, присвоенное инциденту и его номер. Инциденты, которые пользователи создают вручную, помечаются значком . Значок отображается рядом с названием. При нажатии ЛКМ на имени инцидента происходит переход на страницу **Инцидент**.

Для изменения названия инцидента в поле **Название** справа от имени инцидента содержится кнопка **Редактировать** ( ). Кнопка будет отображаться только для инцидента, у которого назначен ответственный за его решение пользователь. При нажатии кнопки открывается окно **Редактирование инцидента**.

Для изменения имени инцидента необходимо ввести произвольное имя в строке **Название**, после чего нажать кнопку **Сохранить** для завершения операции.

В поле **Время регистрации** отображается информация о времени регистрации инцидента.

В поле **Время действия** отображается информация о времени, в течение которого происходил инцидент.

Это время рассчитывается, как разница между временем, когда началось первое событие инцидента, и временем, когда закончилось последнее событие инцидента.

В поле **Агенты** отображается информация о группе, в которую входит агент, для которого создан инцидент и имя агента. При нажатии на имени группы или названии агента происходит переход к страницам **Группа** и **Агент**.

В поле **Кол-во событий** отображается информация о количестве событий, входящих в инцидент.

В поле **Ответственный** находится кнопка **Изменить** ( ), с помощью которой можно изменить пользователя, ответственного за решение инцидента. При нажатии кнопки **Изменить** открывается окно **Выбор ответственного по инциденту** (рис. 16).

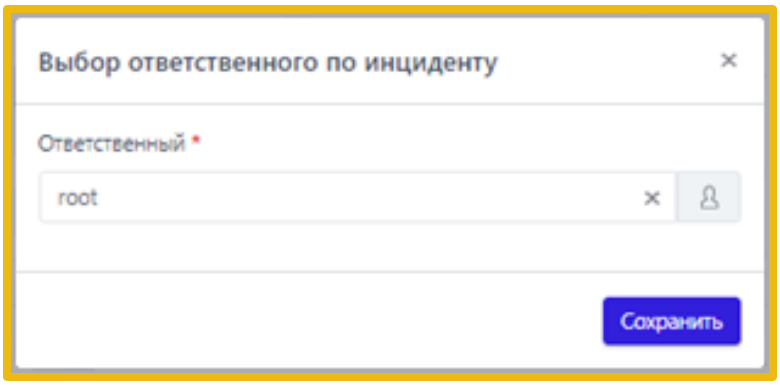


Рисунок 16 – Выбор пользователя, ответственного за решение инцидента

В случае, если ответственный за инцидент уже был назначен, то для выбора нового пользователя, ответственного за инцидент, необходимо в строке **Ответственный** выбрать пользователя из списка или ввести в ней с клавиатуры имя нового пользователя, ответственного за инцидент. Для завершения процедуры назначения ответственного пользователя следует нажать кнопку Сохранить.

В поле **Статус** отображается информация о текущем статусе инцидента. В зависимости от текущего статуса инцидента в поле будут отображаться различные кнопки, с помощью которых можно изменить некоторые параметры инцидента:

1) Закрыть инцидент – (активна при статусе **Назначен** или **Новый**);
2) Назначить инцидент (открыть повторно) – (активна при статусе **Закрыт**);

Для закрытия инцидента необходимо нажать кнопку **Закрыть инцидент** ( ) и в открывшемся окне **Закрытие инцидента** (рис. 17) нажать кнопку **Сохранить**. Закрыть инцидент можно, даже если для инцидента не назначен ответственный.

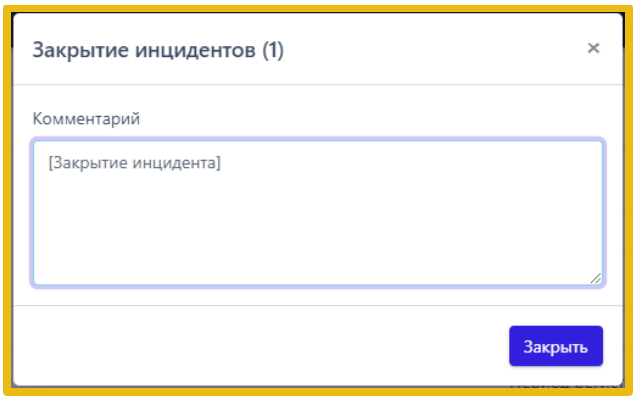


Рисунок 17 – Закрытие инцидентов

По умолчанию в окне **Закрытие инцидента** в поле **Комментарий** стоит запись **[Закрытие инцидента]**, ее можно изменить на произвольный комментарий или сохранить статус инцидента без комментария. Информация, указанная пользователем в поле **Комментарий**, отобразится на странице **Инцидент**.

Для того, чтобы назначить ответственного пользователя по новому инциденту, необходимо нажать кнопку **Назначить инцидент** () и в открывшемся окне **Назначение инцидентов** в поле **Ответственный** выбрать пользователя, ответственного за решение инцидента, после чего нажать кнопку **Сохранить**.

Кроме назначения ответственного в окне **Назначение инцидента** пользователь может ввести произвольный комментарий в поле **Комментарий**, сохранить статус инцидента без комментария или оставить комментарий по умолчанию. Информация, указанная пользователем в поле **Комментарий**, отобразится на странице **Инцидент**.

Чтобы повторно открыть инцидент, необходимо нажать кнопку **Назначить инцидент (открыть повторно)** (), после чего в открывшемся окне **Назначение инцидентов** нажать кнопку **Сохранить**, изменив или сохранив текущего пользователя в качестве ответственного за решение инцидента.

При повторном назначении можно, как и при любой другой смене статуса, добавить комментарий, который отобразится на странице **Инцидент**. После завершения операции по повторному открытию инцидента в нижней части страницы появится всплывающее окно с сообщением.

Для фильтрации инцидентов по тем или иным признакам на странице **Инциденты** содержатся следующие фильтры:

1) Показывать по;
2) Группа;
3) Агент;
4) Критичность;
5) Ответственный;
6) Создатель;
7) Период регистрации;
8) Статус;
9) Правило;
10) MITRE;

11) Полное имя исполняемого модуля процесса.

Также можно фильтровать инциденты по событиям, входящим в них, с помощью DSL-запросов. Запросы ищут совпадения по полям модели данных, принятой в Программе, и выводят результат по соответствующим инцидентам.

Принцип работы с фильтрами не отличается от работы с фильтрами в разделе **Активность**.

В поле фильтров **Правило**, **MITRE**, **Полное имя исполняемого модуля процесса,** поддерживается автоподстановка символов wildcard (*) для фильтров по агрегированным полям.

Для фильтрации в поле фильтра **Правило**, следует писать название правила без расшифровки.

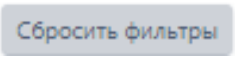
Пример:

MaliciousDomain в chrome.exe – правило с расшифровкой (MaliciousDomain – правило, по которому будут фильтроваться инциденты).

Фильтр **Период регистрации** в сравнении с фильтром **Период регистрации (на сервере)** содержит одно дополнительное значение **Всё время**, при выборе которого показываются все когда-либо зарегистрированные в Программе инциденты.

В поле фильтра **Статус** возможно выбрать следующие варианты статуса инцидента из всплывающего списка:

1) Новый;
2) Назначен;
3) Закрыт.

В поле фильтра **Ответственный** задаётся фильтрация инцидентов по пользователю, ответственному за решение инцидента. Сброс значений фильтров осуществляется с помощью кнопки 

.

Для сортировки в полях **Критичность**, **Время регистрации** и **Статус** таблицы с инцидентами используются кнопки смешанной сортировки  , сортировки по возрастанию  и сортировки по убыванию  .

В нижней части страницы **Инциденты** содержатся кнопки для выполнения следующих операций:

– назначить ответственного за инциденты;

– закрыть выбранные инциденты;

— удалить выбранные инциденты.

Чтобы назначить ответственного, необходимо выполнить следующие действия:

1) Выбрать один или несколько инцидентов с помощью кнопки выбора, отметив их флажками;
2) Нажать кнопку **Назначить выбранные**, откроется окно Назначение инцидентов;
3) В открывшемся окне выбрать ответственного и нажать кнопку **Сохранить**.

Чтобы закрыть инциденты, необходимо выполнить следующие действия:

1) Выбрать один или несколько инцидентов с помощью кнопки выбора, отметив их флажками;
2) Нажать кнопку **Закрыть выбранные**, откроется окно **Закрытие инцидентов**;
3) В открывшемся окне ввести произвольный комментарий и нажать кнопку **Отправить**.

Закрывать инциденты можно даже тогда, когда для этих инцидентов не назначены ответственные за их решение сотрудники.

Для удаления инцидентов необходимо выполнить следующие действия:

1) Выбрать один или несколько инцидентов с помощью кнопки выбора, отметив их флажками;
2) Нажать кнопку **Удалить выбранные**, откроется окно **Удаление инцидентов** (рис. 18);
3) Нажать кнопку **Начать удаление**;
4) Далее необходимо подтвердить удаление в открывшемся окне **Подтверждение действия**, нажав кнопку **Выполнить**.

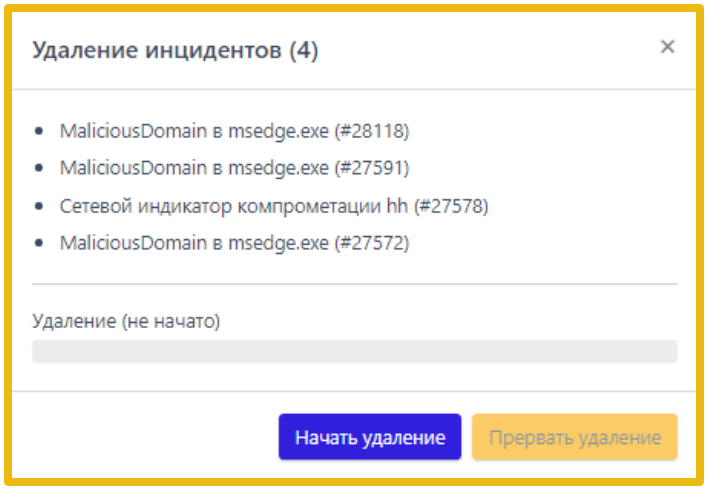


Рисунок 18 – Групповое удаление инцидентов

В процессе группового удаления инцидентов имеется возможность прервать операцию удаления, нажав по иконке Прервать удаление. Удаление инцидентов прервется на том инциденте, который не отмечен значком в списке удаляемых инцидентов.

5) Для завершения операции удаления после того, как операция была прервана, следует нажать кнопку **Закрыть**.

Администратору доступна возможность создания отчетов по инцидентам, отображаемым на странице. Чтобы сохранить отчет в формате pdf, ему необходимо нажать значок PDF в верхней части страницы с инцидентами. Отчет содержит информацию, соответствующую установленным на странице **Инциденты** фильтрам.

Инцидент

Жизненный цикл каждого инцидента подразумевает прохождение трех стадий:

– новый инцидент;

– назначенный в работу;

– закрытый инцидент.

Совет

Если инцидент не представляет больше ценности для дальнейшей работы, его можно удалить. Для этого используется кнопка **Удалить инцидент**.

В зависимости от статуса инцидента у страницы **Инцидент** функциональность может различаться. Для нового и закрытого инцидента недоступна функция редактирования инцидента). Чтобы отредактировать инцидент, необходимо назначить пользователя, ответственного за его решение.

Переход на страницу **Инцидент** выполняется при нажатии ЛКМ на имени инцидента. Для инцидента, у которого назначен ответственный за его решение пользователь, функция редактирования активна.

Страница **Инцидент** разделена на следующие области:

1) **Инцидент** (содержит основную информацию по инциденту);
2) Комментарии;
3) Дополнительная информация;

4) Обнаружения.

В области **Информация об инциденте** пользователь с соответствующими правами может назначить инцидент на того или иного аналитика для дальнейшей работы или выполнить другие действия:

– редактировать инцидент;

– закрыть инцидент;

– открыть инцидент повторно;

– удалить инцидент;

– сохранить отчет об инциденте в файл формата pdf на компьютер, с которого осуществлен доступ в модуль администрирования (кнопка PDF).

В области **Инцидент** отображаются следующие данные:

– название инцидента;

– критичность инцидента;

– ответственный за решение инцидента;

– информация о создателе инцидента (если инцидент создан вручную);

– статус инцидента;

– агент или агенты, на которых произошли события инцидента;

– время регистрации инцидента;

– время действия инцидента;

– описание.

Редактировать можно следующие параметры:

– Название;

– Ответственный;

– Критичность;

– Описание.

Примечание

Операции редактирования имени инцидента, критичности, описания, а также исключение событий из инцидента становятся доступными после назначения ответственного за инцидент.

После завершения редактирования необходимо нажать кнопку **Сохранить изменения**.

В области **Комментарии** пользователь может указать произвольный комментарий. Также комментарии указываются автоматически при переводе инцидента из одного статуса в другой, например, при назначении или закрытии инцидента.

Для добавления нового комментария следует нажать кнопку **Создать комментарий**, после чего открывается окно **Создать комментарий** (рис. 19).

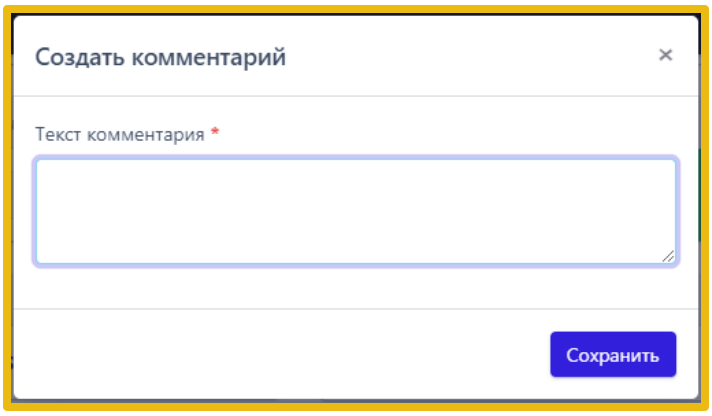


Рисунок 19 – Окно ввода комментария

Для добавления комментария к инциденту необходимо ввести в окне текст комментария и нажать кнопку **Сохранить**, после чего комментарий пользователя будет добавлен на страницу инцидента.

В области **Дополнительная информация** представлена информация по инциденту с уточнением параметров, характеризующих инцидент, таких как командная строка, правила, домены, файлы.

В строке **События** указывается общее число событий, входящих в инцидент. Число является ссылкой, которая позволяет перейти на страницу **Активность** с предустановленными настройками фильтров и соответствующим DSL-запросом.

Информация о событиях, которые были внесены в инцидент при его регистрации, представлена также в области **Обнаружения** в табличном виде.

Переход по страницам в таблице осуществляется с помощью пагинатора (см. рисунок 9).

В верхней части области **Обнаружения** отображается информация об общем количестве событий в инциденте и фильтр **Показывать по** (можно задавать следующие значения: 10, 20, 50, 100).

В таблице с обнаружениями информация распределена по следующим полям:

1) Регистрация на сервере;
2) Регистрация на агенте;
3) Группа/Имя агента;
4) Описание;
5) Процесс;
6) Информация.

Регистрация на сервере – содержит информацию о годе, месяце, дне и точном времени регистрации обнаружения на сервере по стандарту UTC.

Регистрация на агенте – содержит информацию о годе, месяце, дне и точном времени регистрации обнаружения на агенте, то есть по текущему времени, которое установлено на машине с агентом.

Группа/Имя агента – в поле отображаются группа, в которой находится агент, и название агента, имена группы и агента служат гиперссылкой для перехода к соответствующим страницам.

Описание – содержит краткое описание события, которое системой определено как обнаружение или телеметрия, событие-обнаружение помечается значком ⚠.

Процесс – содержит имя процесса, действия которого привели к обнаружению Программой, имя процесса отображается в виде ссылки для перехода к странице **Процессы** (см. пункт 8.4.3).

В поле **Информация** показаны следующие данные по обнаружению:

– Критичность/Действие;

– MITRE;

– Правило.

Критичность/Действие – показывает уровень угрозы, которая исходит от обнаруженного события для защищаемой ИТ-инфраструктуры, для автоматических обнаружений это средний, высокий и критический уровень, а также в поле отображается действие, предпринятое в связи с обнаружением события.

Программой предусмотрены три действия: блокировать, детектировать и продолжение наблюдения. В последнем случае поле останется пустым.

MITRE – в поле отображается идентификатор техники атаки MITRE ATT&CK, который соответствует событию, добавленному в инцидент (идентификатор назначается опционально).

Правило – в поле отображается наименование правила, в соответствии с которым событие было добавлено в инцидент.

В поле **Информация** также находится кнопка **Ложное срабатывание** ( ). Нажав на кнопку, пользователь может создать исключение для файла с помощью мастера исключений.

При нажатии ЛКМ на значок > в строке рядом с кнопкой выбора события, добавленного в инцидент, открывается дополнительная информация о выбранном обнаружении.

Обнаружения можно сортировать по критичности, при выборе определенной критичности будут отображаться все события не ниже этой критичности.

8.4.2. Активность

Страница раздела **Активность** содержит информацию по всем событиям, поступающим от агентов на сервер Программы. Основное функциональное назначение раздела **Активность** – это проведение аналитиком ретроспективного анализа событий с помощью инструментов и элементов, представленных в разделе. Такой анализ может быть особенно полезен при проактивном поиске угроз (подробно см. в документе «Руководство аналитика RT Protect EDR»).

Общая информация

Страница раздела **Активность** при настройках по умолчанию представлена на рисунке 20.

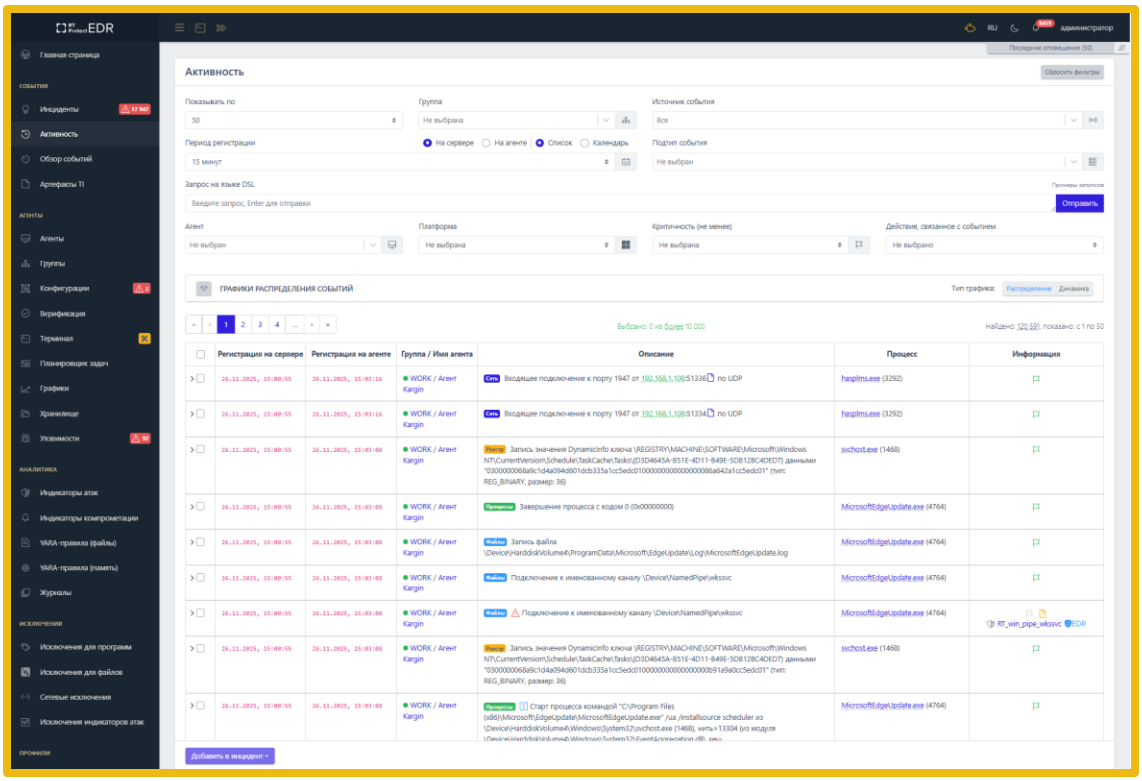


Рисунок 20 – Активность

В верхней части страницы пользователям Программы может быть показана область с диаграммами, на которых в графическом виде представлены типы и подтипы событий в соответствии с настроенными в данный момент фильтрами. Чтобы отобразить графики на странице **Активность**, необходимо нажать кнопку Показать графики ( ).

Графики распределения событий можно просматривать в круговых диаграммах, а также линейном и столбчатом виде. Для переключения между этими видами используется сочетание кнопок Динамика / Распределение (рис. 21).

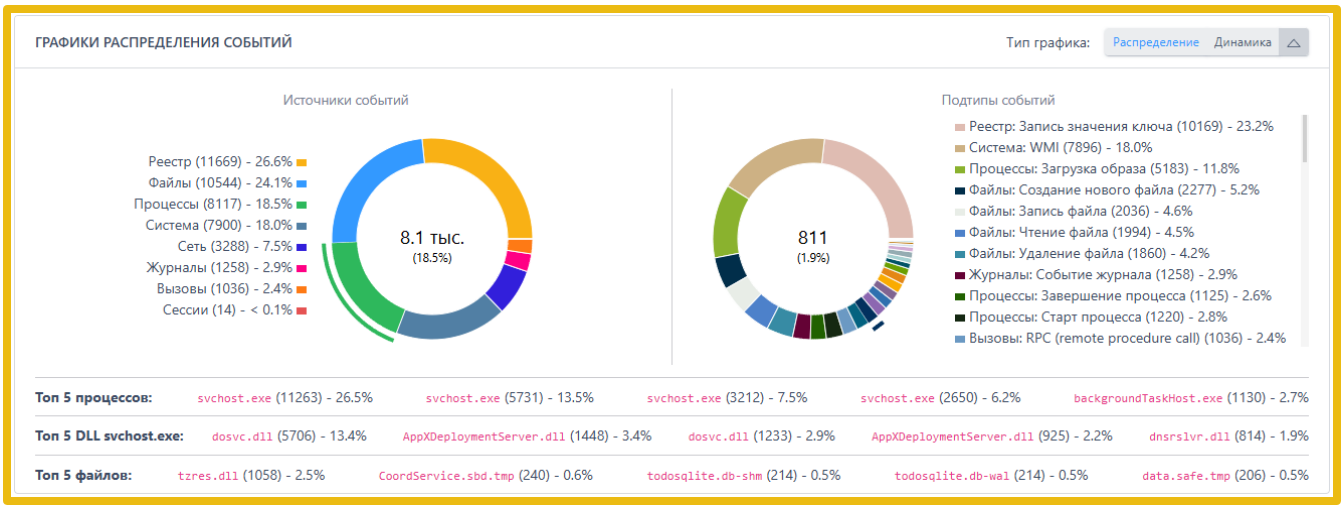


Рисунок 21 – Графики распределения событий

Ниже графиков пользователь EDR может просмотреть топ 5 наиболее часто встречающихся процессов в защищаемой инфраструктуре, топ 5 динамически загружаемых библиотек в хост-процессе **svchost.exe**, а также топ 5 файлов. Графики и диаграммы отображают информацию, задаваемую фильтрами страницы **Активность**.

Информация о событиях на странице **Активность** представлена в виде таблицы, которая включает в себя следующие поля:

1) Кнопка выбора ( );
2) Регистрация на сервере;
3) Регистрация на агенте;
4) Группа/Имя агента;
5) Описание;
6) Процесс;
7) Информация.

Для просмотра страниц с событиями используется пагинатор в верхней и нижней части таблицы с левой стороны (см. рис. 9).

По центру таблицы вверху и внизу находится строка, показывающая количество выбранных событий Выбрано: 10 из более 10000 . В верхней и нижней части таблицы с правой стороны находится строка, показывающая общее количество найденных событий (в соответствии с выбранными фильтрами) и порядковый номер отображаемых событий Найдено: 680835308, показано: с 1 по 50 .

Максимально в таблице отображается 10 000 событий. При наведении на слово более всплывает окно с подсказкой (рис. 22).

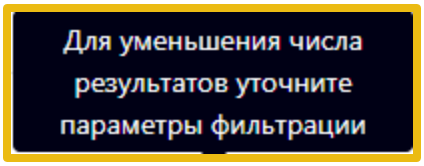
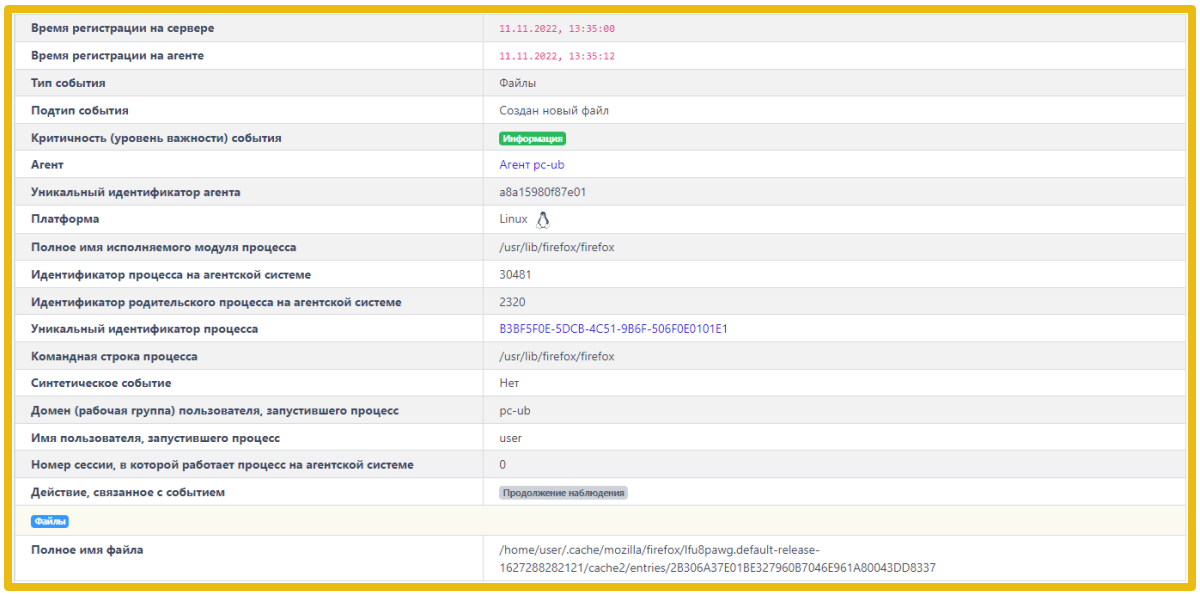


Рисунок 22 – Подсказка в таблице событий

Каждое событие содержит в себе сводную информацию, собранную в виде карточки события (рис. 23).



Время регистрации на сервере	11.11.2022, 13:35:00
Время регистрации на агенте	11.11.2022, 13:35:12
Тип события	Файлы
Подтип события	Создан новый файл
Критичность (уровень важности) события	Информация
Агент	Агент pc-ub
Уникальный идентификатор агента	a8a15980f87e01
Платформа	Linux
Полное имя исполняемого модуля процесса	/usr/lib/firefox/firefox
Идентификатор процесса на агентской системе	30481
Идентификатор родительского процесса на агентской системе	2320
Уникальный идентификатор процесса	B3BF5F0E-5DCB-4C51-9B6F-506F0E0101E1
Командная строка процесса	/usr/lib/firefox/firefox
Синтетическое событие	Нет
Домен (рабочая группа) пользователя, запустившего процесс	pc-ub
Имя пользователя, запустившего процесс	user
Номер сессии, в которой работает процесс на агентской системе	0
Действие, связанное с событием	Продолжение наблюдения
Файлы	
Полное имя файла	/home/user/.cache/mozilla/firefox/lfu8pawg.default-release-1627288282121/cache2/entries/2B306A37E01BE327960B7046E961A80043DD8337

Рисунок 23 – Карточка событий

Карточка события открывается при клике по кнопке › в поле с флагом выбора события. В зависимости от источника обнаруженной активности карточка событий будет отличаться и содержать в себе различный набор полей. К карточкам событий прикрепляется JSON-объект, который открывается при нажатии кнопки JSON справа от карточки события.

Подробная информация о модели данных событий находится в документе «Руководство аналитика RT Protect EDR». Данные событий могут использоваться аналитиком для анализа инцидентов или ретроспективного анализа, создания правил индикации и детектирования, предотвращения последствий атак и угроз для защищаемой IT-инфраструктуры.

При нажатии кнопки ▼ { слева от количества элементов в JSON-объекте структура объекта свернется и под событием отобразится только количество элементов для соответствующего JSON-объекта и кнопка раскрытия его структуры ▶ {...}.

Для возврата к первоначальному виду карточки событий необходимо нажать кнопку HTML.

Также в карточке события пользователь может выполнить типовые операции реагирования, соответствующие выбранному событию (загрузить файл в Хранилище, завершить сетевое соединение). Чтобы выполнить операции реагирования, необходимо кликнуть по кнопке **Реагирование** ().

В строках **Полное имя исполняемого файла процесса**, **Полное имя файла**, **Полное имя исполняемого модуля-инициатора операции, Полное имя файла образа** справа от имени файла или модуля содержится кнопка реагирования, которая позволяет загрузить файл в Хранилище для его дальнейшего исследования или загрузки на компьютер пользователя( ).

При нажатии ЛКМ на значении идентификаторов процесса в карточке события осуществляется переход на страницу **Процессы**. Подробная информация о странице рассматривается в подпункте 8.4.4.

При нажатии ЛКМ на значениях различных артефактов TI в строках карточки события или столбцах таблицы событий появляется всплывающее окно с информацией о проверке артефакта (хеш, IP-адрес или домен) на TI-платформе (рис. 24).

В верхней части карточки с кратким отчетом TI-платформы содержится информация о проверяемом артефакте.

Далее следует краткий отчет о том, когда объект был обнаружен, и общий вывод об опасности/безопасности артефакта (например, 

). Окно содержит кнопку **Перейти к отчету**. Обновление данных по артефакту происходит автоматически.

Для более глубокого анализа необходимо перейти на страницу с отчетом TI-платформы, нажав на кнопку **Перейти к отчету**.

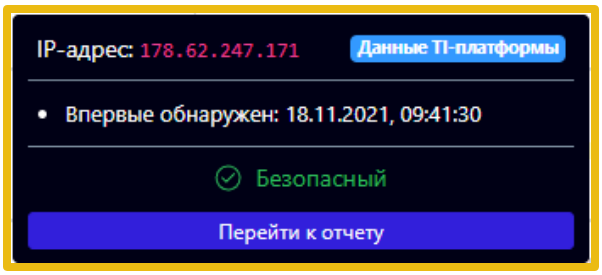


Рисунок 24 – Карточка информации о проверке объекта на TI-платформе

Проверяемые артефакты в зависимости от содержания отчета отображаются на странице **Активность** в различной цветовой гамме. Артефакты, которые TI-платформа определяет как безопасные, отмечаются зеленым цветом (192.168.80.2). Вредоносные артефакты отмечаются красным цветом (93.184.220.29). Артефакты, для которых процесс анализа выполняется в настоящее время, отображаются синим цветом (1b28cbf8a06b973a2422f4e1e400b441430c75dfe4d4c8be6f23dff824e96). Артефакты, для которых информация на TI-платформе отсутствует или не проверялась, отмечаются серым цветом (74.125.131.94). Карточка для вредоносного артефакта показана на рисунке 25.

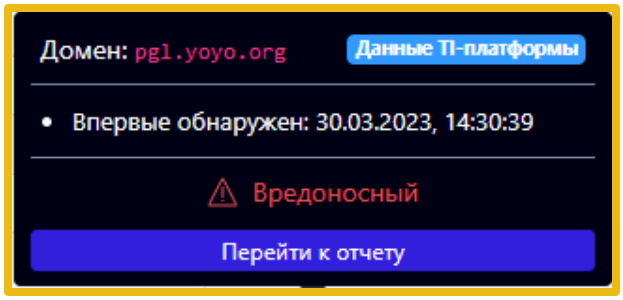


Рисунок 25 – Карточка TI-платформы для вредоносного объекта

Карточка TI-платформы для объекта, информация по которому отсутствует, представлена на рисунке 26.

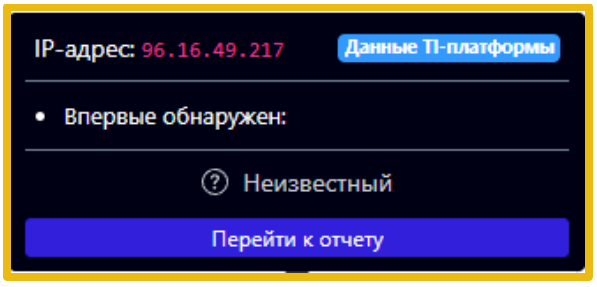


Рисунок 26 – Карточка TI-платформы для отсутствующего в базе объекта

Для локальных ip-адресов и доменов проверка на TI-платформе не выполняется (рис. 27).

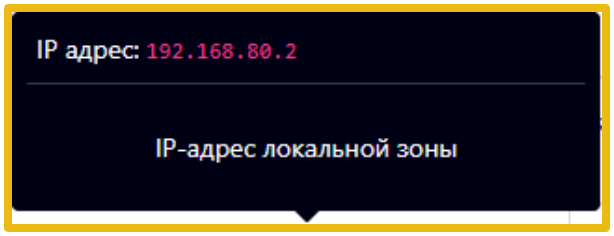


Рисунок 27 – Карточка TI-платформы для локального ip-адреса

При отсутствии в базе TI-платформы информации о выбранном артефакте или недоступности платформы пользователю выводится сообщение, представленное на рисунке 28.

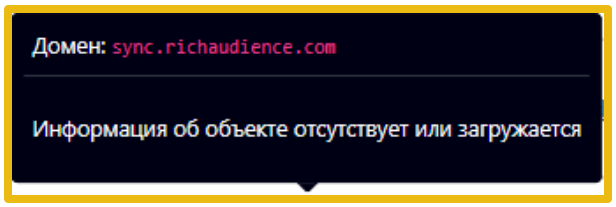


Рисунок 28 – Информация TI-платформы недоступна

В столбце **Информация** таблицы с событиями на странице **Активность** отображаются следующие данные:

1) Критичность от уровня **Информация** до уровня **Критичная**,
2) Действие (по умолчанию действие **Продолжать наблюдение** не помечается каким-либо знаком), другие действия помечаются знаками (детектировать) и (блокировать);
3) Имя правила (отображается, если в событии присутствует поле rul, то есть оно произошло в результате матчинга событий на соответствие аналитическим правилам, применяемым на агентах);
4) Кнопка **Исключить как ложное срабатывание** (– мастер исключений). С помощью мастера исключений можно в автоматизированном режиме быстро создать файловые, программные или сетевые исключения.

Фильтрация событий

Программа регистрирует множество событий, поступающих от агентов. Для уменьшения количества отображаемых событий в таблице с информацией об активности необходимо изменить параметры фильтрации.

Система фильтрации состоит из следующих полей:

1) Показывать по;
2) Группа;
3) Источник события;
4) Период регистрации;
5) Подтип события;
6) Запрос на языке DSL.
7) Агент;
8) Платформа;
9) Критичность (не менее);
10) Действие, связанное с событием.

После нажатия кнопки Сбросить фильтры все установленные параметры фильтрации сбрасываются.

Показывать по – фильтр устанавливает количество событий, которые отображаются на странице в таблице. Возможно выбрать отображение по 10, 20, 50, 100 или 500 событий. По умолчанию на странице **Активность** отображается 50 последних событий.

Группа – фильтр позволяет сортировать события по выбранной группе агентов.

Источник события – фильтр позволяет сортировать события по следующим источникам:

1) Сеть;
2) Файлы;
3) Реестр;
4) Журналы;
5) Процессы;
6) Сессии;
7) Антишифр;
8) Система;

9) Вызовы;

10) Контроль USB;

11) Статистика.

Рядом с обозначением источника события содержится цифровое значение, соответствующее типу события **t**, которое можно использовать при составлении DSL-запросов.

Период регистрации – можно выбрать период регистрации событий на сервере или агенте, интервал выбирается из списка или с помощью календаря. В таблице отображаются только те события, которые происходили в данном интервале времени.

Для задания периода регистрации событий из списка необходимо выбрать одно из следующих значений:

1) Не задан;

2) 15 минут;

3) 1 час;

4) 8 часов;

5) 1 день;

6) 1 неделя;

7) 1 месяц;

8) 3 месяца.

Для задания параметра из календаря следует установить флаг **Календарь**, как показано на рисунке 29.

Далее необходимо нажать ЛКМ на пустое поле ввода и установить в открывшемся календаре начальное и конечное значение временного интервала, после чего нажать кнопку **Выбрать** (рис. 29).

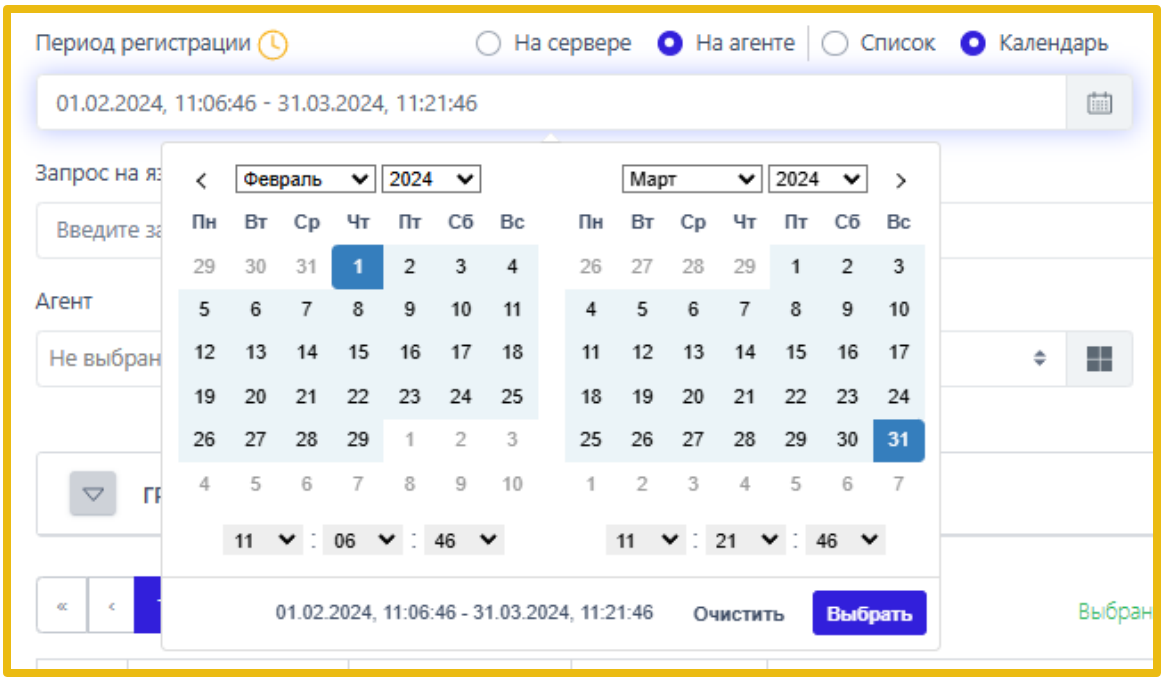


Рисунок 29 – Выбор периода регистрации события в календаре

Значение выбранного временного интервала отобразится в поле **Период регистрации**. Максимальное значение интервала, возможное для выбора – 2 месяца.

Подтип события – фильтр позволяет сортировать события по подтипу, для каждого типа событий определены свои подтипы. К примеру, для события типа **Сеть** определены следующие подтипы событий:

1) Исходящее подключение;
2) Входящее подключение;
3) Завершение сетевого подключения;
4) Отправка;
5) Прием;
6) DNS-запрос;
7) DNS-ответ;
8) Входящий DNS-запрос;
9) Исходящий DNS-ответ;
10) SSL HELLO;
11) Открытие локального порта на прием (LISTEN);
12) ICMP-сообщение;

13) Обнаружение: срабатывание сетевого исключения (устаревшее, оставлено для совместимости с ранними версиями агента).

14) Обнаружение: срабатывание индикатора компрометации;

15) Другие обнаружения.

Подробное описание событий и их подтипов содержится в документе «Руководство аналитика RT Protect EDR».

Примечание

Значения подтипов не уникальны, поэтому, если в запросе указать **st:0**, то это будет означать и подтип **Сеть: Исходящее подключение**, и **Файлы: Создан новый файл** и подтипы других типов событий. Для точности запроса необходимо указывать еще и тип события (**t**). Например, DSL-запрос **t:0 AND st:6** покажет события сети, связанные с SSL HELLO-запросами.

Запрос на языке DSL – фильтрует события в соответствии с введенным в поле фильтра запросом.

Примечание

В некоторых случаях запрос может быть составлен неэффективно, тогда Программа предупреждает об этом пользователя с помощью значка над строкой ввода ( ). При наведении курсора мыши на значок появится предупреждающий текст о желательной коррекции запроса.

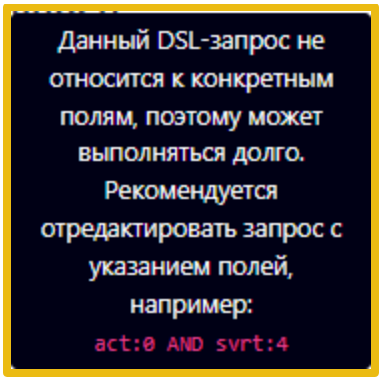


Рисунок 30 – Текст о корректировке DSL-запроса

В правой части строки фильтра над кнопкой Отправить содержатся примеры DSL-запросов (рис. 31).

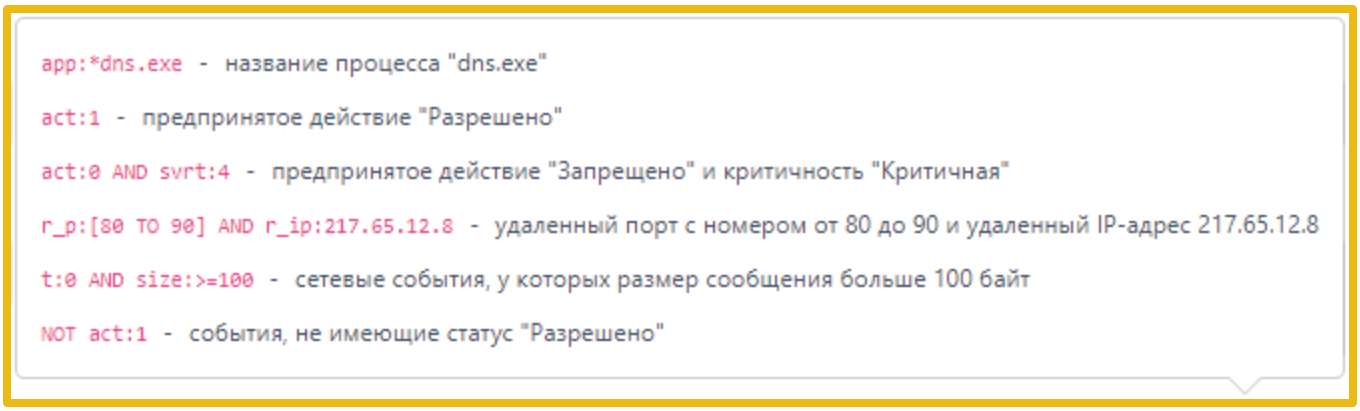


Рисунок 31 – Примеры DSL-запросов

Добавление событий в инцидент

На странице раздела **Активность** пользователь может добавить одно или несколько событий в инцидент. Для этого следует выделить их флажком в левой части таблицы, далее в нижней части страницы нажать кнопку Добавить в инцидент. Если требуется добавить событие в новый инцидент, то из списка операций, открывшегося при нажатии кнопки **Добавить в инцидент** (рис. 32), необходимо выбрать операцию **Новый**.

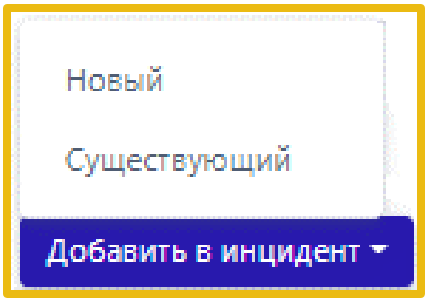


Рисунок 32 – Список операций с событиями на странице «Активность»

В результате выполнения операции откроется окно **Добавление событий в новый инцидент** (рис. 33), в котором следует заполнить поля **Название**, **Описание** и выбрать ответственного за решение инцидента в поле **Ответственный**. По умолчанию ответственным за решение инцидента назначается пользователь, добавляющий событие в новый инцидент.

Поля **Название** и **Описание** не являются обязательными для добавления события в новый инцидент.

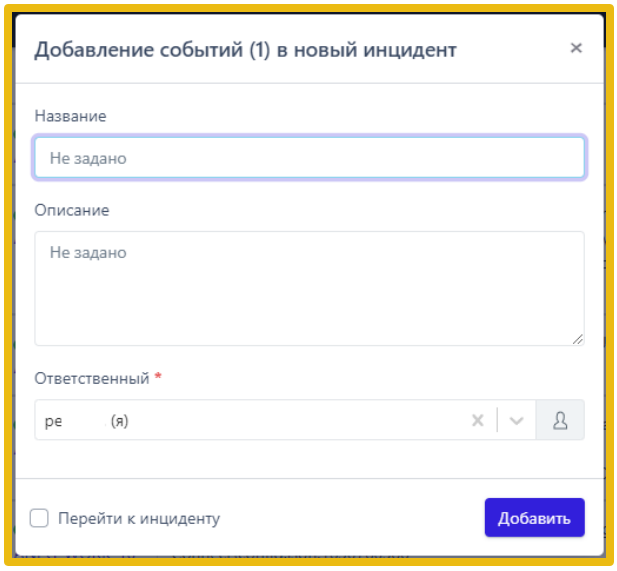


Рисунок 33 – Добавление событий в новый инцидент

В нижней части окна находится флажок **Перейти к инциденту**, при установке которого происходит автоматический переход на страницу **Инцидент** после добавления инцидента. Для завершения операции добавления события в новый инцидент необходимо нажать кнопку Добавить. Если требуется добавить событие в существующий инцидент, то из списка операций, открывшегося при нажатии кнопки **Добавить в инцидент**, следует выбрать операцию **Существующий**. В результате выполнения операции откроется окно **Добавление событий в инцидент** (рис. 34), в котором в поле **Инцидент** необходимо выбрать существующий инцидент.

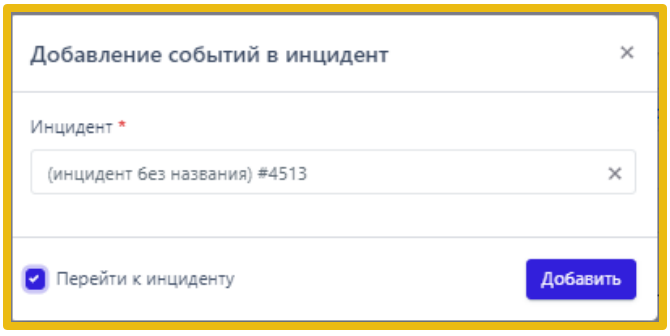


Рисунок 34 – Добавление события в существующий инцидент

В нижней части окна, также как и в окне **Добавление событий в новый инцидент**, находится флажок **Перейти к инциденту**, при установке которого после нажатия кнопки Добавить происходит автоматический переход на страницу **Инцидент** для выбранного инцидента. Если флажок **Перейти к инциденту** в окнах **Добавление событий в новый инцидент** и **Добавление событий в инцидент** не устанавливать и нажать кнопку **Добавить**, то будет выполнена выбранная операция. Пользователь при этом останется на странице **Активность**.



Примечание

Добавление событий в существующий инцидент возможно только для инцидентов, у которых назначен ответственный за их решение пользователь.

Переходы к другим страницам из таблицы с событиями

В таблице событий можно перейти на другие страницы. Клик по имени группы агента в столбце **Группа/Имя агента** позволяет перейти на страницу **Агенты**. Клик по имени агента в столбце **Группа/Имя агента** позволяет перейти на страницу **Агент**. Клик по имени процесса в столбце **Процесс** в карточке события позволяет перейти на страницу **Процессы**.

8.4.3. Проверка с помощью TI-платформы

TI-платформа сопоставляет и анализирует данные компьютерных угроз из нескольких источников в режиме реального времени для поддержки защитных действий Программы. На данный момент в Программе предусмотрена проверка следующих артефактов:

— хеш;

— глобальный ip-адрес;

— глобальное имя домена;

Проверка выполняется в нескольких источниках, в зависимости от типа артефакта, набор источников, в соответствии с которыми проверяется артефакт, может отличаться:

1) Внешние источники (например, MalwareBazaar);
2) VirusTotal;
3) Заключение аналитика;

4) YARA;

5) IOC;

6) Public TI;

7) Whois.

Вердикты TI-платформы равнозначны с аналитикой сервера EDR. Например, если вердикт TI по определённому хешу будет отмечен как вредоносный, а на сервере EDR тот же хеш будет отмечен как безопасный, то будет создан инцидент. То же самое произойдет и в обратном случае, когда сервер EDR отмечает артефакт как вредоносный, а TI-платформа как безопасный. Если правила TI-платформы и правила сервера EDR будут дублировать друг друга, то в случае обнаружения вредоносной активности создадутся два независимых инцидента. Страницы отчета TI-платформы открываются на вкладке **Общая информация**, которая содержит сводные данные из всех доступных для выбранного артефакта источников.

В верхней части страницы отчета отображается наименование и значение артефакта и вердикт TI-платформы. На левой панели отчета отображаются вкладки с наименованиями источников данных, от которых были получены сведения для вынесенного вердикта. На правой панели отчета отображается информация о выбранном артефакте. Информация представлена в табличном виде.

Поля таблицы содержат следующие данные:

1) Вердикт (безопасный/вредоносный/подозрительный);

2) Время обнаружения (когда артефакт обнаружен впервые);

3) Теги (опционально);

4) Размер файла (опционально);

5) Хеш, рассчитанный по алгоритму SHA-256;

6) Хеш, рассчитанный по алгоритму SHA-1 (опционально);

7) Хеш, рассчитанный по алгоритму MD5 (опционально);

8) Хеш, рассчитанный по алгоритму TLSH (опционально);

9) Хеш, рассчитанный по алгоритму Imphash (опционально);

10) Хеш, рассчитанный по алгоритму SSDEEP (опционально);

11) Обнаруженные имена (опционально).

Для таких данных, как значения хеш-сумм и обнаруженных имен, доступна функция копирования в буфер обмена. Для копирования в буфер обмена необходимо нажать кнопку **Скопировать в буфер обмена** ( ) в строке с выбранным значением хеш-суммы или обнаруженными именами.

Справа от таблицы с данными находится кнопка JSON . При нажатии кнопки формат отчета меняется на JSON-формат (рис. 35).



Рисунок 35 – Отчёт в JSON

Любой элемент или блок элементов в формате JSON можно скопировать, нажав кнопку . Для возврата к результатам отчета в формате HTML необходимо нажать ЛКМ на значок HTML .

8.4.4. Процессы

В Программе содержится доступный для понимания и эффективный в расследовании инструментарий для анализа поведения программ, запускаемых на машине агента, который позволяет найти информацию о запуске, работе или остановке той ли иной программы в системе агента. На странице **Процессы** пользователь может узнать общую информацию о запускаемых программах:

– какие дочерние процессы запустил родительский процесс;

– с какими файлами процесс связан (какие файлы создавал, читал, в какие вносил изменения);

– какие ключи реестра процесс создавал и в какие вносил изменения;

— с какими сетевыми соединениями и библиотеками DLL процесс взаимодействовал;

— какие точки автозапуска были созданы процессом;

— распространенность процесса в агентской сети и т.д.

Общая информация

На страницу **Процесс** переход осуществляется по ссылкам из разных полей таблиц с событиями на страницах разделов **Инцидент** и **Активность**. Ссылка представлена названием процесса или значением универсального уникального идентификатора (UUID). Ссылки в Программе отображаются синим цветом, для перехода необходимо кликнуть по выбранной ссылке. Если нажать на ссылку перехода к странице процесса, то пользователю становится доступна информация о выбранном процессе и его дерево, в графическом виде показывающее отношение родительских и дочерних процессов.

В верхней части страницы **Процессы** посередине представлено имя процесса и его идентификатор (PID), далее рядом с именем отображается состояние процесса (Запущен / Завершен), в правой части на этой же строке располагаются название группы и имя агента, на котором данный процесс был запущен. Названия группы и агента отображаются в виде гиперссылок для быстрого перехода к страницам **Группа** и **Агент**.

В центральной части находится область отображения дерева процесса, в которой можно отследить всю цепочку событий процесса, как предшествующих его возникновению, так и последующих, если таковые имеются.

В верхней части области отображения дерева процесса находится кнопка **Изменить ориентацию дерева** , с помощью которой пользователь может сменить горизонтальное отображение дерева процесса на вертикальное и наоборот.

Рядом с кнопкой изменения ориентации дерева находится кнопка **Изменить размер области дерева** . После нажатия кнопки область отображения дерева процессов увеличится или уменьшится соответственно.

Администратор может задавать временный интервал отображения дерева процессов, выбрав интервал из списка или задав его с помощью календаря.

Просмотр дерева процессов в случае отображения множества веток родительских и дочерних процессов осуществляется с помощью кнопки перемещения объектов (значок руки). Для перемещения дерева процесса необходимо навести на него курсор мыши (при наведении на область отображения дерева процессов

курсор мыши меняет свое отображение на значок руки) и, зажав ЛКМ, переместить изображение дерева. При наведении курсора мыши на имя процесса пользователю показывается командная строка этого процесса.

Для уменьшения/увеличения масштаба отображения дерева процессов с помощью колеса прокрутки мыши увеличить или уменьшить масштаб, зажав клавишу Ctrl.



Примечание

Если количество дочерних процессов для выбранного родительского процесса превышает отображаемое по умолчанию число процессов, то в верхнем правом углу окна появляется кнопка , позволяющая добавить в область отображения оставшиеся дочерние процессы.

Снизу от области отображения дерева процессов находится область с подробной информацией о выделенном в данный момент родительском или дочернем процессе.

Для вывода информации об определенном процессе необходимо нажать ЛКМ на значок под названием этого процесса, после чего от выбранного родительского процесса будут показаны его дочерние процессы. Чтобы возвратить дерево в исходное состояние, то есть убрать дочерние процессы выбранного процесса, необходимо нажать ЛКМ на значок еще раз.

Вкладки, которые включают множество элементов, могут подгружать информацию в течение некоторого времени, в этот момент рядом с именем вкладки отобразится мигающий значок (к примеру, Реестр). После завершения загрузки информации рядом с названием вкладки отобразится количество элементов, на которые так или иначе повлиял процесс, выбранный ранее (к примеру, Реестр (154)).

В таблице отображаются следующие вкладки:

1) Информация;
2) Файлы;
3) Сеть;
4) Реестр;
5) Взаимодействие процессов;
6) Загруженные DLL/SO (для процесса **%SYSTEM%** вместо загруженных DLL будут указаны загруженные модули ядра);

7) Точки автозапуска;

8) Распространенность;

9) Событие старта;

10) Правила/MITRE.

В нижней части страницы **Процесс** находятся ссылки и кнопки операций:

1) Все события процесса ;

2) Ключевые события процесса (1) ;

3) Обзор событий процесса

4) Восстановить файлы ;

5) Реагирование .

Все события процесса – при нажатии ссылки Все события процесса происходит переход к странице **Активность**, на которой будут представлены все дочерние процессы выбранного родительского процесса. Подробную информацию о работе на странице **Активность** можно узнать в пункте 8.4.2.

Ключевые события процесса – при нажатии ссылки Ключевые события процесса (1) происходит переход на страницу **Активность**, на которой отображаются важные события (события с уровнем критичности от уровня **Низкая** и выше, а также события для которых выбрано блокирующее действие), связанные с процессом. При этом отображаемые события должны подчиняться логике DSL-запроса, указанного в строке **Запрос на языке DSL** (рис. 36).

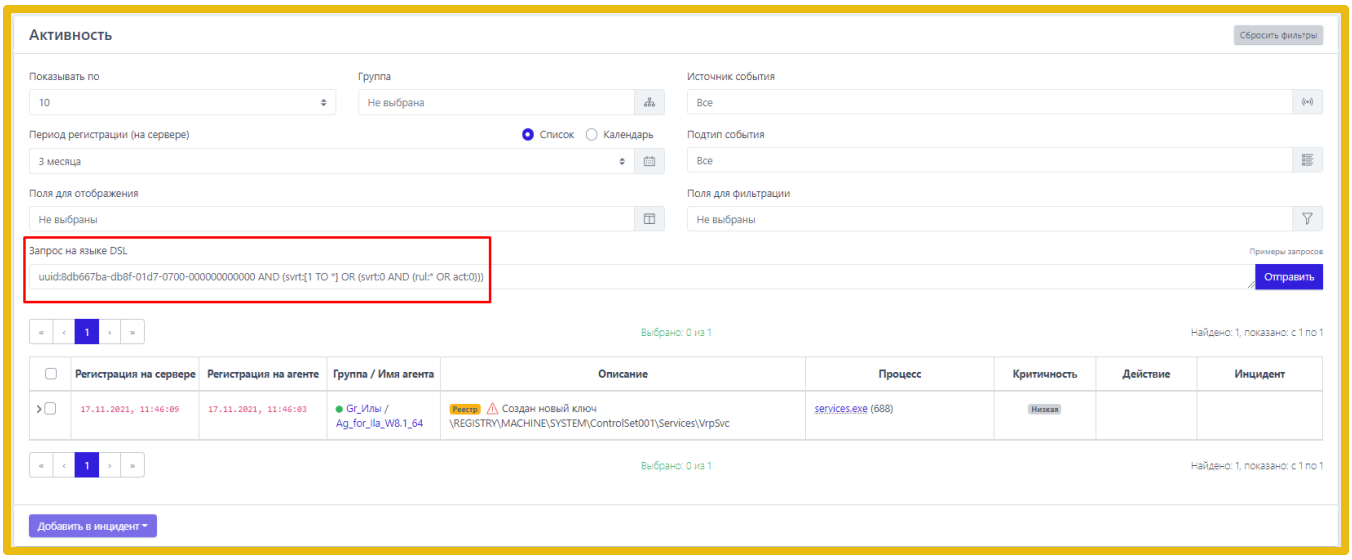


Рисунок 36 – Ключевые события процесса

Восстановить файлы – кнопка позволяет восстановить файлы, затронутые вредоносным процессом, если эти файлы были зарезервированы модулем Антишифра (функционал является устаревшим, работает только для первых и вторых версий агента).

Реагирование – кнопка позволяет выполнить операцию реагирования (завершить процесс, завершить группу процессов, сделать дамп памяти процесса, сканировать дамп памяти процесса, выполнить операцию ремедиации, то есть отката действий, сделанных вредоносным процессом или группой процессов).

Вкладка «Информация»

В таблице раздела отображается общая информация о процессе.

Для этого пользователю показаны следующие поля:

1) Исполняемый модуль;
2) Командная строка;
3) Время старта/завершения;
4) Имя пользователя (SID);
5) SHA-256;
6) Подпись;
7) Флаги исполняемого модуля;
8) Поведенческие признаки;

Исполняемый модуль – в поле отображается имя модуля исполняемого файла, инициировавшего запуск процесса. Рядом с именем находится значок операции загрузки модуля в файловое хранилище для проведения дополнительного анализа ( ).

Командная строка – в поле отображается значение командной строки, которая запустила рассматриваемый процесс.

Время старта/завершения – в поле отображается год, месяц, число и время до секунды, в которое был выполнен старт и завершение рассматриваемого процесса на агенте.

Имя пользователя (SID) – в поле отображается имя пользователя и идентификатор безопасности пользователя, от имени которого был запущен рассматриваемый процесс.

SHA-256 – в поле отображается хеш-сумма исполняемого файла, запустившего процесс. При нажатии ЛКМ на значение хеш-суммы пользователю показывается всплывающее окно с кратким отчетом TI-платформы об исполняемом файле. Рядом с хеш-суммой отображаются две кнопки.

Первая кнопка позволяет скопировать хеш в буфер обмена ( ). Вторая позволяет перейти на страницу **Процессы и модули** для выбранной хеш-суммы ( ).

Подпись – в поле отображается значение сертификата Code Signing для исполняемого файла рассматриваемого процесса.

Флаги исполняемого модуля – в поле показаны флаги, с которыми исполняется Программа, кнопка Показать все... открывает дополнительную область с флагами исполняемого модуля процесса.

Поведенческие признаки – в поле показаны поведенческие признаки Программы, кнопка Показать все... открывает дополнительную область с поведенческими признаками процесса.

Вкладка «Файлы»

В таблице вкладки **Файлы** отображается информация о файлах, с которыми связан рассматриваемый процесс (рис. 37).

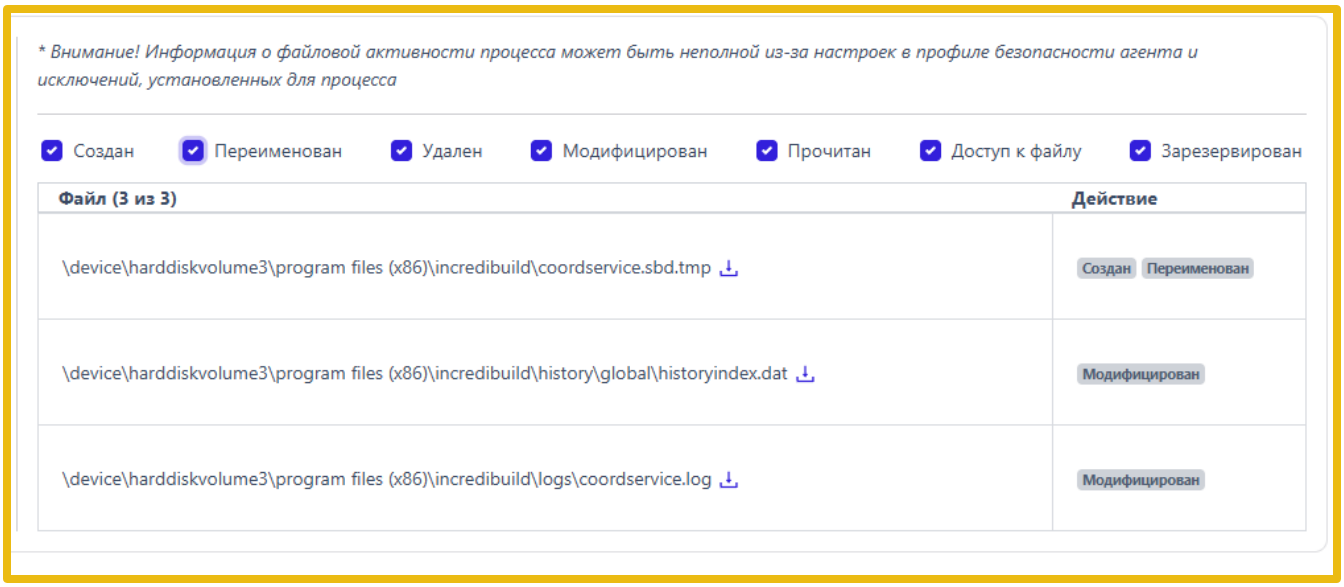


Рисунок 37 – Информация о файлах процесса

Для фильтрации файлов предусмотрена система флажков.

Файл, соответствующий выбранному параметру, при снятии флажка не будет отображаться в таблице. Рядом с абсолютным именем файла отображается кнопка загрузки файла ( ) в файловое хранилище для проведения дополнительного анализа с помощью TI-платформы или программы просмотра файлов.

Если среди действий с файлом, присутствующем в списке, было удаление, то он помечается значком . При наведении курсора мыши на значок пользователю выводится предупреждающее сообщение (рис. 38).

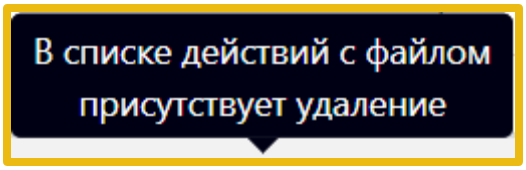


Рисунок 38 – Сообщение о присутствии в списке удаления файла

Вкладка «Сеть»

Во вкладке **Сеть** отображается информация о сетевых подключениях процесса:

1) Входящие подключения;
2) Исходящие подключения;
3) DNS-запросы;
4) SSL Hello.

Информация о сетевых подключениях представлена в табличном виде. Таблица для каждого типа подключения включает в себя различные поля, в том числе:

1) IP-адрес;
2) Имя хоста;
3) Удаленный порт;
4) Локальный порт;
5) Протокол;
6) Тип запроса.

IP-адрес – показывает сетевой адрес соответствующего сетевого подключения.

Имя хоста – в поле отображается доменное имя конечной точки, с которой осуществлялось сетевое соединение.

Удаленный порт – в поле отображается номер порта, по которому осуществлялось сетевое соединение.

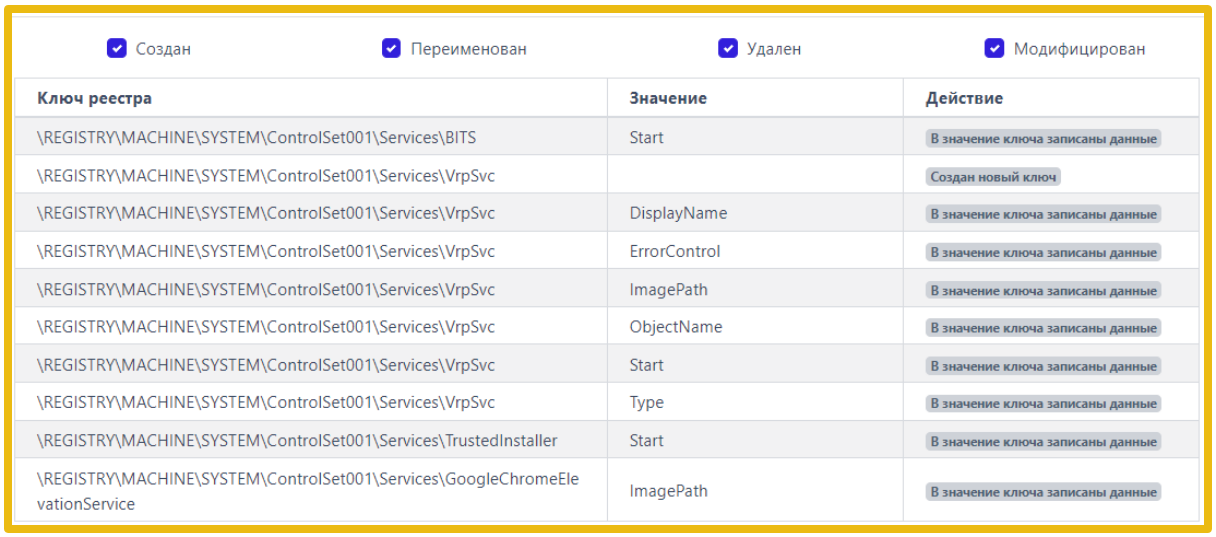
Протокол – в поле отображается сетевой протокол, по которому осуществлялось сетевое соединение.

Тип запроса – показывает типы записей о соответствии имени и служебной информации в системе доменных имён, например, A, AAAA, CNAME, MX и т.д.

Для входящего подключения кроме удаленного порта указывается еще и локальный порт.

Вкладка «Реестр»

Во вкладке **Реестр** отображается информация о ключах реестра, с которыми производил действия выбранный процесс (рис. 39).



☑ Создан ☑ Переименован ☑ Удален ☑ Модифицирован

Ключ реестра	Значение	Действие
\REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\BITS	Start	В значение ключа записаны данные
\REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\VrpSvc		Создан новый ключ
\REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\VrpSvc	DisplayName	В значение ключа записаны данные
\REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\VrpSvc	ErrorControl	В значение ключа записаны данные
\REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\VrpSvc	ImagePath	В значение ключа записаны данные
\REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\VrpSvc	ObjectName	В значение ключа записаны данные
\REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\VrpSvc	Start	В значение ключа записаны данные
\REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\VrpSvc	Type	В значение ключа записаны данные
\REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\TrustedInstaller	Start	В значение ключа записаны данные
\REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\GoogleChromeElevationService	ImagePath	В значение ключа записаны данные

Рисунок 39 – Ключи реестра, на которые действовал процесс

Информация о ключах реестра представлена в таблице, в которой присутствуют следующие столбцы:

1) **Путь ключа реестра** – в поле прописывается путь ключа реестра, с которым выбранный процесс производил те или иные действия;
2) **Значение** – в поле отображается значение, которое было внесено выбранным процессом в ключ реестра;
3) **Действие** – в поле отображается действие, которое совершил выбранный процесс с ключом реестра: это может быть внесение данных в значение ключа, удаление ключа, создание нового ключа и т.д.

Примечание

Информация о ключах реестра может быть неполной, если в профиле безопасности агента установлена опция **Фильтровать события модификации реестра**.

Вкладка «Взаимодействие процессов»

Во вкладке **Взаимодействие процессов** отображается информация о процессах, взаимодействовавших или взаимодействующих с выбранным процессом. Представлены две информационные области **Доступ к процессу** и **Доступ к нити процесса**.

Информация содержится в таблице, которая включает следующие поля:

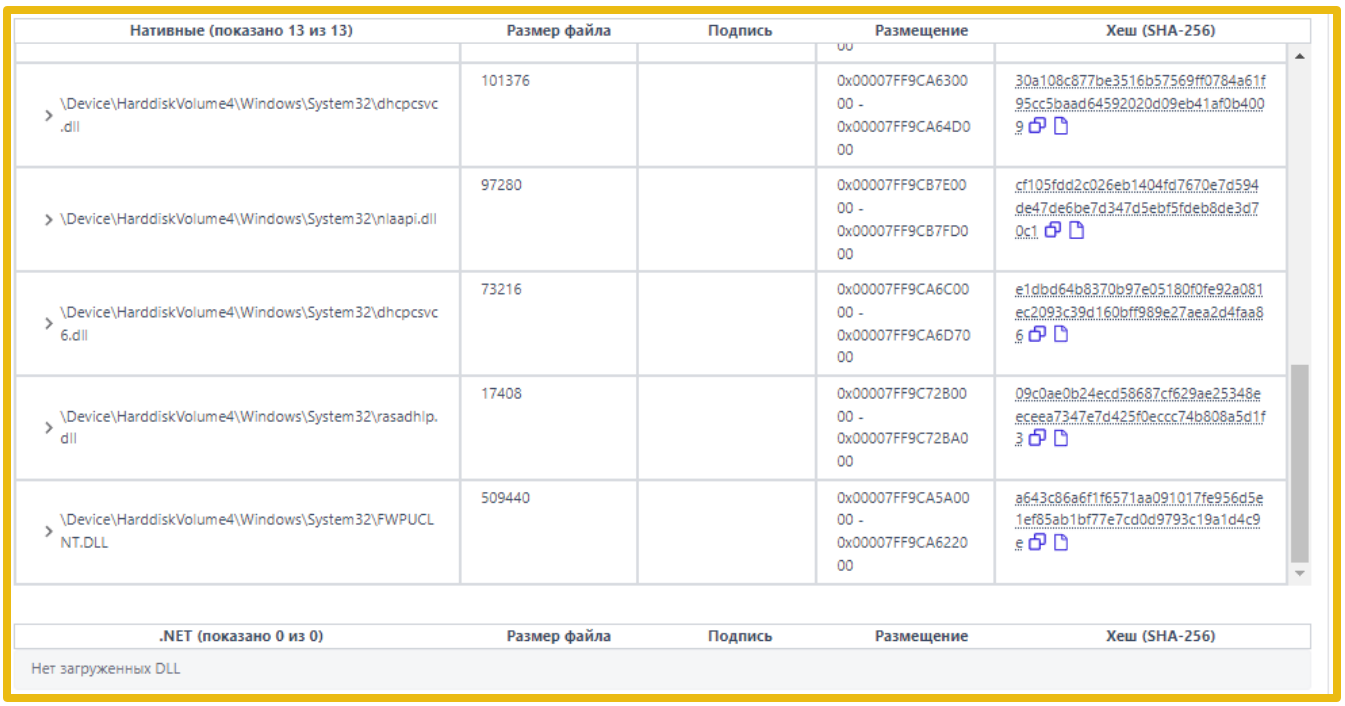
1) Имя исполняемого образа;
2) Запрошенные права;
3) Предоставленные права;
4) Кол-во событий.

В области **Доступ к процессу** показана информация о том, к каким процессам в системе выбранный процесс осуществлял доступ, какие права при предоставлении доступа он запросил, и какие права были ему предоставлены.

В области **Доступ к нити процесса** показана информация о том, к каким нитям выбранный процесс осуществлял доступ, и какие права при предоставлении доступа были запрошены и предоставлены.

Вкладка «Загруженные DLL/SO»

Во вкладке **Загруженные DLL/SO** отображается информация о нативных и .Net-библиотеках DLL, используемых выбранным процессом (рис. 40).



Нативные (показано 13 из 13)	Размер файла	Подпись	Размещение	Хеш (SHA-256)
\Device\HarddiskVolume4\Windows\System32\dhcpcsvc.dll	101376		0x00007FF9CA630000 - 0x00007FF9CA64D000	30a108c877be3516b57569ff0784a61f95cc5baad64592020d09eb41af0b4009
\Device\HarddiskVolume4\Windows\System32\nlaapi.dll	97280		0x00007FF9CB7E0000 - 0x00007FF9CB7FD000	cf105fdd2c026eb1404fd7670e7d594de47de6be7d347d5ebf5fdeb8de3d70c1
\Device\HarddiskVolume4\Windows\System32\dhcpcsvc6.dll	73216		0x00007FF9CA6C0000 - 0x00007FF9CA6D7000	e1dbd64b8370b97e05180f0fe92a081ec2093c39d160bff989e27aea2d4faa86
\Device\HarddiskVolume4\Windows\System32\rasadhlp.dll	17408		0x00007FF9C72B0000 - 0x00007FF9C72BA000	09c0ae0b24ecd58687cf629ae25348eceeea7347e7d425f0eccc74b808a5d1f3
\Device\HarddiskVolume4\Windows\System32\FWPUCLNT.DLL	509440		0x00007FF9CA5A0000 - 0x00007FF9CA622000	a643c86a6f1f6571aa091017fe956d5e1ef85ab1bf77e7cd0d9793c19a1d4c9e

.NET (показано 0 из 0)	Размер файла	Подпись	Размещение	Хеш (SHA-256)
Нет загруженных DLL				

Рисунок 40 – Список загруженных библиотек DLL

Важно

Если в профиле безопасности агента установлена опция **Исключать события загрузки известных модулей**, то в списке DLL этих модулей не будет. Подробный список известных DLL-библиотек содержится в пункте 8.8.2.

Рядом с названием библиотеки находится кнопка раскрытия (›) дополнительной информации о событии, связанном с библиотекой.

При нажатии ЛКМ на кнопку открывается карточка событий, связанная с рассматриваемыми процессом и библиотекой. Для процесса **%SYSTEM%** будет представлен список загруженных модулей ядра, дополнительная информация о которых также становится доступной при нажатии кнопки ›.

Вкладка «Точки автозапуска»

Во вкладке **Точки автозапуска** отображается информация о точках автозапуска, созданных рассматриваемым процессом в реестре.

Рядом с названием точки автозапуска в таблице находится кнопка раскрытия дополнительной информации (›), которая описывает создание точки автозапуска. При нажатии ЛКМ на кнопку › открывается карточка этого события.

Вкладка «Распространенность»

Во вкладке **Распространенность** отображается информация о распространении выбранного процесса в агентской сети (рис. 41)

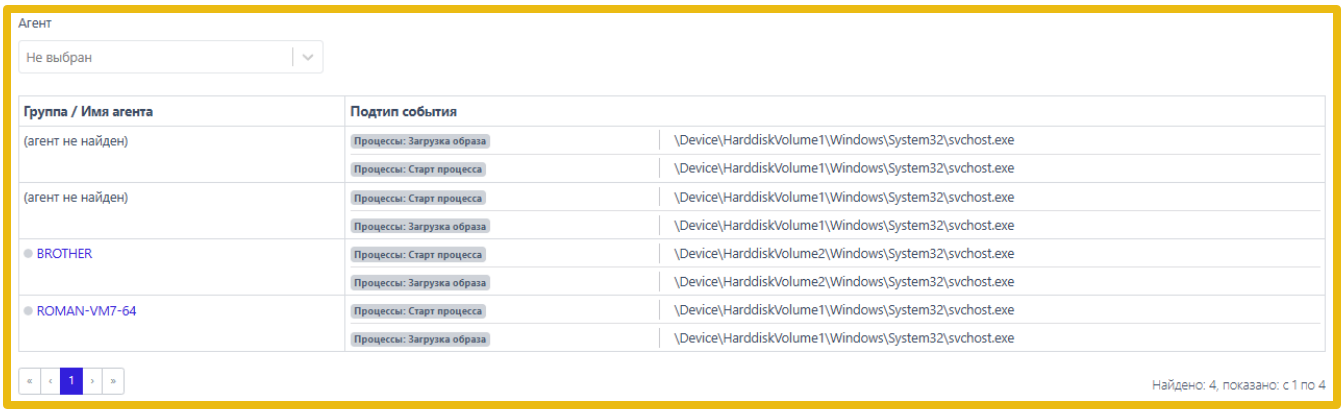


Рисунок 41 – Вкладка «Распространенность»

Вкладка «Событие старта»

Во вкладке **Событие старта** показана карточка события для старта процесса (рис. 42).

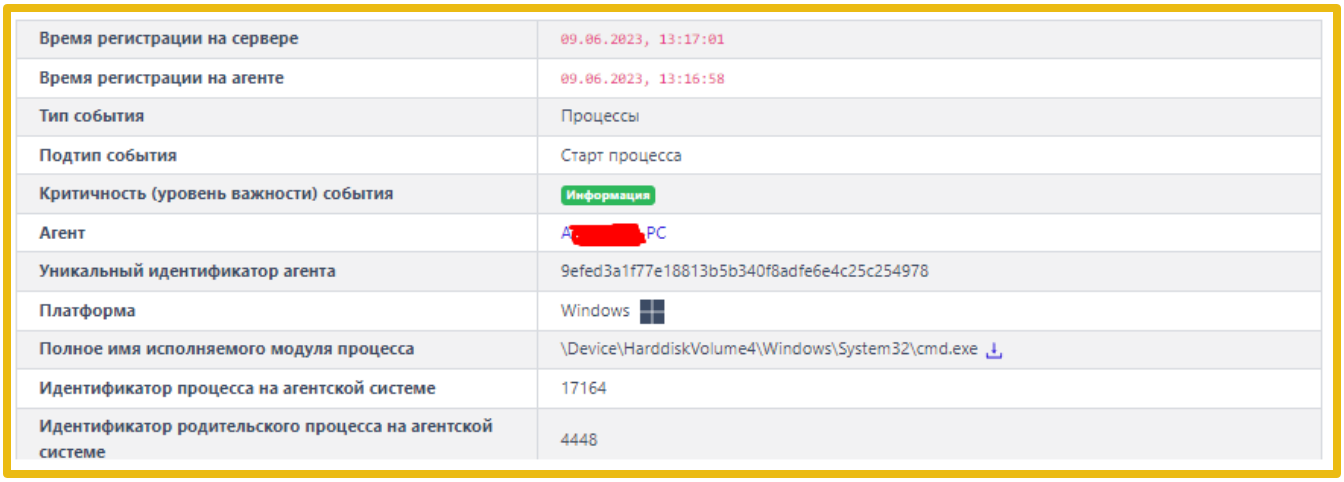


Рисунок 42 – Событие старта

Вкладка «Правила/MITRE»

Во вкладке **Правила/MITRE** содержится информация о срабатываниях действующих в EDR правил, а также техник, тактик и процедур MITRE (TTP) для выбранного процесса (рис. 43).

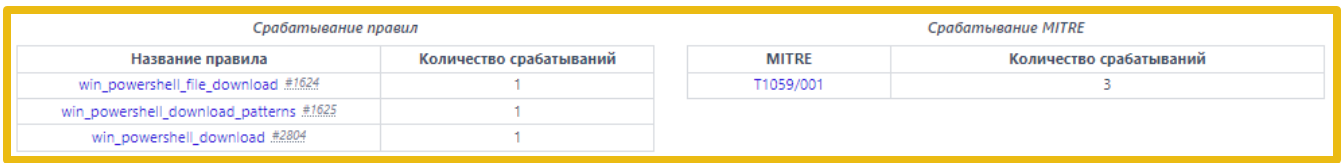


Рисунок 43 – Правила/MITRE

8.4.5. Обзор событий

Обзор событий – это инструмент создания подборок событий для представленных категорий по определенным запросам, фильтрам или сочетанию запросов и фильтров.

На странице **Обзор событий** представлены подборки событий, распределенные по следующим категориям:

1) Графики распределения событий и график динамики событий;
2) Агенты;
3) Правила;
4) Техники MITRE;
5) Исполняемые файлы;
6) Библиотеки (DLL/SO);
7) Командные строки;
8) Модули;
9) Хеши;
10) Пользователи;
11) Сессии (Локальные/Дистанционные);
12) Файлы (точки автозапуска (Файлы);
13) Реестр (точки автозапуска (Реестр);
14) Сеть;
15) Настраиваемая агрегация.

Каждая из категорий содержит определенное количество событий, которое зависит от установленных пользователем фильтров.

Фильтры, доступные на странице **Обзор событий** представлены ниже:

1) Максимальный размер агрегации;
2) Группа;
3) Источник события (тип события);
4) Период регистрации события на сервере или агенте;
5) Подтип события;

6) Фильтрация по запросу на языке DSL;
7) Агент;
8) Платформа;
9) Критичность (не менее установленной);
10) Действие, связанное с событием.

8.4.6. **Артефакты TI**

На странице **Артефакты TI** пользователь может оценить распространённость артефакта (хеш, IP-адрес или имя домена) в агентской сети, а также узнать вердикт TI-платформы по этим артефактам. Распространённость показывает, на каких конечных точках с агентами появлялся тот или иной артефакт.

Пользователь может искать нужный артефакт с помощью фильтров:

1) **Показывать по** (10, 20, 50, 100 строк в таблице);
2) **Платформа** (Windows или Linux);
3) IP-адрес;
4) Домен;
5) **Имя модуля** (требуется ввести имя модуля полностью);
6) Подпись;
7) Тип подписи;
8) Хеш модуля (SHA-256);
9) **Период регистрации на сервере** (можно выбрать в списке или календаре).

Вердикт TI-платформы открывается, если пользователь нажмет поле с артефактом. Первоначально открывается краткий отчет. Полный отчет доступен, если нажать кнопку **Перейти к отчету**.

Пользователь может просмотреть дополнительную информацию из карточки события старта процесса, которая открывается при нажатии кнопки  .

Важно

Если артефакт не проверялся алгоритмами TI, то не показывается на странице **Артефакты TI**. Такими артефактами являются артефакты, добавленные в исключения, хеши файлов, подписанных доверенной подписью, локальные ip-адреса и т.д.

Для поиска по странице по самому артефакту рядом с полем ввода артефакта имеются иконки, которые в неактивном состоянии имеют серый цвет, а при нахождении данного артефакта, например, в событиях активности подсвечиваются синим цветом (рисунок 44).

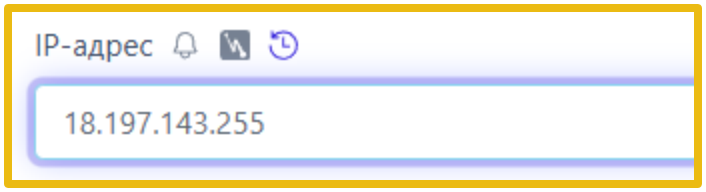


Рисунок 44 – Поиск артефакта и отображение, что он присутствует в событиях активности

Если артефакт присутствует в индикаторах компрометации или исключениях для файлов, то будут подсвечены соответствующие иконки (,).

8.5 Агенты

В области **Агенты** основной панели Программы находятся следующие разделы:

1) Агенты;
2) Группы;
3) Конфигурации
4) Верификация;
5) Терминал;
6) Планировщик задач;
7) Графики;
8) Хранилище;
9) Уязвимости.

В разделе **Агенты** представлена информация обо всех агентах, зарегистрированных в Программе. Кроме того, администратор может добавлять агентов в группы или удалять их из группы, создавать/удалять группы, вносить изменения в конфигурацию настроек защиты агентов и т.п.

В разделе **Группы** администратор может создать новую группу или удалить ее.

В разделе Конфигурации представлены конфигурации наборов, по умолчанию устанавливаемые на агентах, а также конфигурации, создаваемые и редактируемые администратором.

В разделе **Верификация** администратор может просмотреть информацию об агентах, ожидающих верификацию и верифицировать выбранного агента(ов).

В разделе **Терминал** администратор может выполнять команды для управления операционной системой, установленной на хосте выбранного агента с помощью командной строки, а также просмотреть краткую информацию об этом агенте: имя компьютера, процессор, ip-адрес и т.д.

В разделе **Планировщик задач** администратор может создавать различные задачи согласно заданному сценарию на выполнение, назначать задачи агентам, следить за статусом выполнения задач и многое другое.

В разделе **Графики** пользователь может просматривать и конфигурировать информацию об активности отдельно взятого агента в графическом виде.

В разделе **Хранилище** пользователь может работать с загруженными файлами: просматривать подозрительные или требующие исследования файлы, просматривать подробную информацию об этих файлах в отчётах TI-платформы, удалять загруженные файлы или просматривать их в программе просмотра файлов и т.д.

8.5.1. Агенты

Общая информация

Страница **Агенты** позволяет пользователю, обладающему правом управления агентами, выполнять различные действия по реагированию на определенные события, осуществлять действия по управлению агентами, а также осуществлять поиск агентов. Информация об агентах представлена на странице **Агенты** в табличном виде, поиск по ним осуществляется с помощью полей фильтрации и DSL-запросов.

Агенты, на которых есть системные или прикладные ошибки, подсвечиваются значком  . При обнаружении таких агентов желательно собрать с них логи и передать их представителям Производителя.

Поля фильтрации на странице «Агенты»

На странице **Агенты** предусмотрены следующие поля фильтрации:

1) Показывать по;
2) Группа;
3) Домен;
4) Изоляция;
5) Активность;
6) Операционная система;
7) Имя компьютера;
8) Защита агента;
9) Агент;
10) Платформа;
11) Сетевой адрес;
12) Защита от удаления;
13) Автоматическое обновление;
14) Золотой образ;
15) Поля для фильтрации (входят фильтры).

В фильтре **Поля для фильтрации** администратор может добавить дополнительные поля:

1) Опция /NO_DRIVER;
2) Проблемный;
3) Часовой пояс;
4) Конфигурация;
5) Критичность;
6) Наличие открытых инцидентов;
7) Артефакт;

8) Режим работы;

9) Наличие блокировок в рамках реагирования;

10) **Поля с наборами и профилями** (индикаторы атак, индикаторы компрометации и т.д.)

Отдельным блоком на странице выделяется строка **Настройки DSL**, которые открываются с помощью кнопки  . В настройках администратор может указать период регистрации событий на сервере, источник события и его подтип и сам запрос, в соответствии с которым будет производиться выборка из событий, произошедших на агентах.



Важно

Для применения настроек по периоду регистрации событий, источнику события, его подтипу DSL-запрос должен быть задан и отправлен.

При вводе DSL-запросов создается выборка над базой событий, из которой делается агрегация агентов, подлежащих отображению. Например, DSL-запрос «sha256:x» выводит список агентов, на которых были зафиксированы события с указанным хешем (поле **sha256** события). В поле **Совпадения по DSL** выборки по запросу пользователь может увидеть, сколько событий, соответствующих запросу, произошло на агенте. Нажимая на ссылку с количеством событий, пользователь сразу перейдет на страницу **Активность** с результатами, соответствующими выбранным фильтрам.

Показывать по – фильтр устанавливает количество агентов, которые отображаются на странице в таблице. Возможно выбрать отображение по 10, 20, 50, 100 или 500 агентов.

Группа – фильтрует агентов по названию группы, к которой они принадлежат.

Домен – фильтрует агентов по имени домена, к которому принадлежат компьютеры, на которых установлены зарегистрированные в Программе агенты.

Изоляция – при выборе одного из значений фильтров (**Все агенты/Изолирован/Не изолирован**) в таблице **Агентов** будут представлены агенты, соответствующие выбранному состоянию агента.

Активность – при выборе одного из значений фильтра (**Все агенты/Активен/Не активен**) в таблице **Агентов** будут представлены агенты, соответствующие выбранному значению активности.

Операционная система – фильтрует агентов по установленной на них операционной системе.

Имя компьютера – фильтрует агентов по именам компьютеров, на которых установлены зарегистрированные в Программе агенты.

Защита агента – фильтрует агентов в соответствии с тем, включена на них защита или нет.

Агент – фильтрует агентов по выбранному из списка имени агента. Можно выбрать только одного агента. Применяется, если нужна фильтрация по конкретному агенту.

Платформа – фильтрует агентов в соответствии с выбранной операционной системой: Windows или Linux.

Сетевой адрес – фильтрует агентов по вводимому в поле фильтра сетевому адресу.

Защита от удаления – позволяет фильтровать информацию на странице по агентам с включенной или выключенной опцией парольной защиты от удаления агента.

Автоматическое обновление – фильтрует агентов по признаку включенного или выключенного автоматического обновления.

Золотой образ – позволяет фильтровать информацию на странице по агентам с соответствующим состоянием золотого образа, доступны следующие параметры фильтрации:

– Все агенты;

– Не отслеживается;

– Соответствие;

– Имеются отличия.

Поля для фильтрации – при выборе значений в фильтре **Поля для фильтрации** на страницу дополнительно могут быть добавлены следующие фильтры: **Опция/NO_DRIVER**, **Проблемный**, **Часовой пояс**, **Конфигурация**, **Критичность**, **Наличие открытых инцидентов**, **Артефакт**, **Режим работы**, **Наличие блокировок в рамках реагирования**, **Исключения для файлов**, **Исключения для программ**, **Сетевые исключения**, **Индикаторы компрометации**, **YARA-правила (файлы)**, **YARA-правила (память)**, **Индикаторы атак**, **Исключения индикаторов атак**, **Профили Антишифра**, **Профили безопасности агента**, **Профили контроля USB**.

Опция /NO_DRIVER – позволяет фильтровать агентов в соответствии с тем, включен ли драйвер на агенте или нет (для агента с установленной опцией NO_DRIVER отсутствует возможность переводить машину с агентом в изоляцию, а также отсутствует защита, то есть правила индикации атак, срабатывание индикаторов

компрометации не приводят к завершениям процессов, запрету тех или иных действий потенциально опасных программ и т.д.).

Проблемный – фильтрует агентов по отсутствию/наличию системных или прикладных ошибок на агентах, где под системными подразумеваются ошибки драйвера, а под прикладными – ошибки службы агента.

Часовой пояс – фильтрует агентов по часовому поясу, установленному на агентах.

Конфигурация – фильтрует агентов по привязанной конфигурации, можно выбрать всех агентов и агентов, у которых заданы не все настройки конфигурации.

Критичность – фильтрует агентов по заданной для них критичности, представлены следующие степени критичности: **Низкая**, **Ниже среднего**, **Средняя**, **Высокая**, **Критичная**.

Наличие открытых инцидентов – фильтр показывает агентов с открытыми инцидентами или без инцидентов.

Артефакт – фильтрует агентов по типу и значению артефакта, доступны артефакты – SHA-256, IP-адреса и домены.

Режим работы – фильтрует агентов по одному из двух доступных режимов работы (режим ядра и eBPF).

Наличие блокировок в рамках реагирования – фильтрует агентов по факту наличия или отсутствия на агентах заблокированных файлов, сетевых соединений или запусков по командной строке.

Исключения для файлов – фильтрует агентов по названию выбранного в поле фильтра набора исключений для файлов. В таблице будут представлены только агенты, привязанные к этому набору. Подробная информация об исключениях для файлов содержится в пункте 8.7.

Исключения для программ – фильтрует агентов по названию выбранного в поле фильтра набора исключения для программ.

В таблице будут представлены только агенты, привязанные к этому набору. Подробная информация об исключениях для программ содержится в пункте 8.7.1.

Сетевые исключения – фильтрует агентов по названию выбранного в поле фильтра набора сетевых исключений. В таблице будут представлены только агенты, привязанные к этому набору.

Индикаторы компрометации – фильтрует агентов по названию выбранного в поле фильтра набора индикаторов компрометации. В таблице будут представлены только агенты, привязанные к этому набору. Подробная информация об индикаторах компрометации содержится в пункте 8.6.1.

Журналы – фильтрует агентов по названию выбранного в поле фильтра набора журналов. В таблице будут представлены только агенты, привязанные к этому набору. Подробная информация о журналах содержится в пункте 8.6.4.

YARA-правила (Файлы/Память) – фильтрует агентов по названию выбранного в поле фильтра набора файловых сигнатур. В таблице будут представлены только агенты, привязанные к этому набору.

Индикаторы атак – фильтрует агентов по названию выбранного в поле фильтра набора индикаторов атак. В таблице будут представлены только агенты, привязанные к этому набору. Подробная информация об индикаторах атак содержится в пункте 8.6.1.

Исключения индикаторов атак – фильтрует агентов по привязанным наборам с исключениями индикаторов атак.

Профили Антишифра – фильтрует агентов по названию выбранного в поле фильтра профиля Антишифра. В таблице будут представлены агенты, привязанные к этому профилю. Подробная информация о профилях Антишифра содержится в пункте 8.8.1.

Профили безопасности агента – фильтрует агентов по названию выбранного в поле фильтра профиля безопасности агента. В таблице будут представлены агенты, привязанные к этому профилю. Подробная информация о профилях защиты данных содержится в пункте 8.8.2.

Профили контроля USB – фильтрует агентов по названию выбранного в поле фильтра профиля контроля USB. В таблице будут представлены агенты, привязанные к этому профилю. Подробная информация о профилях контроля USB содержится в пункте 8.8.3.

Информация в таблице с агентами

В шапке таблицы просмотра агентов представлены следующие поля:

1) Поле выбора агентов (отмечено кнопкой выбора  и переключателем );
2) Группа/Имя агента;
3) Версия агента;

4) EPS;

5) Сетевые адреса;

6) Домен/Имя компьютера;

7) Операционная система;

8) Часовой пояс;

9) Состояние;

Поле с кнопкой выбора применяется для выбора в таблице одного или нескольких агентов. Для этого необходимо отметить флажком кнопки выбора для соответствующих агентов. Для отмены следует нажать на кнопку выбора повторно. Для выбора в таблице всех агентов, показанных на одной странице, необходимо отметить флажком верхнюю кнопку выбора в столбце поля выбора агентов.

Совет

Если требуется отметить всех агентов, показанных на всех страницах, то необходимо перевести переключатель **Выбрать все элементы** во включенное положение ( ). При этом переход на другую страницу переводит переключатель в выключенное положение.

Группа/Имя агента – содержит имя группы, которой принадлежит агент, и имя агента, на котором произошел инцидент.

Кроме того, рядом с именем агента отображается значок, указывающий на принадлежность агента платформе Windows или Linux.

Версия агента – показывает номер версии агента.

EPS – показывает среднее количество событий в секунду на агенте за отрезок времени равный 15 минутам.

Сетевые адреса – в поле отображаются ip-адреса, назначенные для всех сетевых интерфейсов компьютера, на котором установлен агент.

Имя компьютера – в поле отображается имя компьютера, на котором установлен агент.

Операционная система – в поле отображается название ОС, под управлением которой работает компьютер, на котором установлен агент.

Часовой пояс – в поле отображается часовой пояс, настроенный на компьютере, на котором установлен агент.

Состояние – в поле отображается информация о состоянии компьютера, на котором установлен агент и информация о фиксации списка программ, установленных на машине с агентом (золотого образа). **Состояние** может принимать значения **Активен/Не активен**, а также в случае изоляции АРМ с установленным на нем агентом дополнительно может быть присвоено значение **Изолирован**. Если агент не активен, то пользователю будет показано время последней активности агента. Также вне зависимости от активности отображаются данные об открытых инцидентах на агенте.

Состояние в части отслеживания золотого образа отображается в таблице иконками:

–  – соответствие золотому образу;

–  – имеются отличия в сравниваемой информации, приходящей от агента, об установленном ПО (золотым образом).

Каждая строка таблицы агентов содержит дополнительную информацию. Для просмотра этой информации необходимо нажать кнопку раскрытия › в поле с кнопкой выбора элемента таблицы **Агенты**.

Дополнительная информация об агенте представлена в табличном виде и содержит поля:

1) ID агента;
2) Имя агента;
3) Версия агента;
4) Токен агента;
5) Время установки;
6) Время последнего обновления;
7) Время последней верификации;
8) Время загрузки системы;
9) Процессор;
10) Количество ядер процессора;
11) Объем оперативной памяти (МБ);
12) События;

13) Инциденты;

14) Изоляция;

15) Защита агента;

16) Автоматическое обновление;

17) Опция /NO_Driver;

18) Золотой образ;

19) Защита от удаления;

20) Терминал;

21) Описание.

Часть полей вынесено в отдельную область **Конфигурации**, в которой показаны привязанные к агенту конфигурационные наборы:

1) Индикаторы атак.

2) Индикаторы компрометации;

3) YARA-правила (файлы);

4) YARA-правила (память);

5) Журналы;

6) Исключения для программ;

7) Исключения для файлов;

8) Сетевые исключения;

9) Исключения индикаторов атак;

10) Профиль безопасности агента;

11) Профиль Антишифра;

12) Профиль контроля USB.

ID Агента – в поле показан набор символов, идентифицирующий агента на сервере.

Имя агента – имя агента, присвоенное ему администратором во время регистрации агента в Программе.

Версия агента – в поле показана актуальная версия установленного дистрибутива агента.

Токен агента– в поле показывается часть ключа, присвоенного агенту для верификации с помощью этого ключа на сервере.

Время установки – в поле отображается информация о времени установки агента.

Время последнего обновления – в поле отображается информация о времени последнего обновления агента.

Время последней верификации – в поле отображается информация о времени последней верификации агента.

Время загрузки системы – в поле отображается информация о дате и времени последней загрузки операционной системы, под управлением которой действует агент.

Процессор – в поле отображается наименование процессора компьютера, на котором установлен агент.

Количество ядер процессора – в поле отображается количество ядер процессора компьютера, на котором установлен агент.

Объем оперативной памяти (МБ) – в поле отображается объем оперативной памяти компьютера, на котором установлен агент. Объем указан в мегабайтах.

События – в поле отображается информация о количестве событий, обнаруженных на компьютере с установленным агентом.

Информация показывается за сутки и за последние 15 минут *За сутки: 0 / За 15 мин: 0* . При нажатии ЛКМ на число событий происходит переход на страницу **Активность**.

Инциденты – в поле отображается количество инцидентов, зарегистрированных в Программе для выбранного агента за все время функционирования и количество открытых на данный момент инцидентов *Всего: 0 / Открытых: 0* . При нажатии ЛКМ на число инцидентов происходит переход на страницу **Инциденты**.

Изоляция – в поле отображается информация об изоляции компьютера с установленным агентом от остальной части вычислительной сети. Если компьютер изолирован, то значок изоляции отображается в виде закрытого замка . Если компьютер не изолирован, то значок изоляции отображается в виде открытого замка . При нажатии на значки / происходит переход на страницу **Агент** в раздел **Настройка агента**.

Защита – в поле отображается состояние включена или отключена защита агента.

Автоматическое обновление – в поле отображается информация о том включен или отключен ли параметр **Автоматическое обновление** на агенте.

Опция /NO_DRIVER – в поле отображается установлен ли агент с опцией без драйвера (имеются состояния: установлена опция, не установлена опция).

Золотой образ – в поле отображается информация о соответствии программ, установленных на агенте, зафиксированному списку (золотому образу).

Защита от удаления – в поле отображается информация о том, включена ли защита от удаления агента или нет.

Терминал – поле содержит ссылку Открыть , для работы в командной строке с компьютером, на котором установлен агент. При нажатии ссылки открывается окно онлайн-терминала для выбранного агента.

Описание – поле содержит произвольное описание агента.

Индикаторы атак – в поле отображаются названия наборов индикаторов атак, назначенных агенту. При нажатии ЛКМ на названии набора происходит переход на страницу **Наборы индикаторов атак** в разделе **Индикаторы атак**.

Индикаторы компрометации – в поле отображаются названия наборов индикаторов компрометации, назначенных агенту. При нажатии ЛКМ на названии набора происходит переход на страницу **Наборы индикаторов компрометации** в разделе **Индикаторы компрометации**.

YARA-правила – в поле отображаются названия наборов YARA-правил, назначенных агенту. При нажатии ЛКМ на названии набора происходит переход на страницу **Наборы YARA-правил** в разделе **YARA-правила**.

Журналы – в поле отображаются названия наборов журналов, назначенных агенту. При нажатии ЛКМ на названии набора происходит переход на страницу **Журналы**.

Исключения для программ – в поле отображаются названия наборов исключений для программ, назначенных агенту. При нажатии ЛКМ на названии набора происходит переход на страницу **Исключения для программ** в одноименном разделе.

Исключения для файлов – в поле отображаются названия наборов исключений для файлов, назначенных агенту. При нажатии ЛКМ на названии набора происходит переход на страницу **Исключения для файлов** в одноименном разделе.

Сетевые исключения – в поле отображаются названия наборов сетевых исключений, назначенных агенту. При нажатии ЛКМ на названии набора происходит переход на страницу **Сетевые исключения** в одноименном разделе.

Исключения индикаторов атак – в поле отображаются названия наборов исключений индикаторов атак, назначенных агенту.

При нажатии ЛКМ на названии набора происходит переход на страницу **Исключения индикаторов атак** в одноименном разделе.

Профиль Антишифра – в поле отображается название профиля Антишифра, к которому привязан агент. При нажатии ЛКМ на названии профиля происходит переход на его страницу.

Профиль безопасности агента – в поле отображается профиль безопасности, к которому привязан агент. При нажатии ЛКМ на названии профиля происходит переход на страницу этого профиля.

Профиль контроля USB – в поле отображается профиль контроля USB, к которому привязан агент. При нажатии ЛКМ на названии профиля происходит переход на страницу этого профиля.

Операции с агентами

На странице **Агенты** администратор может выполнять различные групповые действия с произвольным количеством агентов. Информация об агентах, зарегистрированных в Программе, представлена в табличном виде. Чтобы выбрать агента и применить к нему определенное действие, администратору необходимо отметить этого агента флажком ( ).

Совет

Если требуется отметить всех агентов, показанных на всех страницах, то необходимо перевести переключатель **Выбрать все элементы** во включенное положение ( ). При этом переход на другую страницу переводит переключатель в выключенное положение.

В нижней части страницы **Агенты** находится панель операций с выбранными агентами.

Пользователю Программы доступны следующие операции:

1) Добавить агентов в созданную или во вновь создаваемую группу  ;
2) Применить конфигурацию –  ;
3) Включить автоматическое обновление выбранных агентов –  ;
4) Отключить автоматическое обновление выбранных агентов –  ;
5) Включить защиту на выбранном агенте –  ;
6) Отключить защиту на выбранном агенте –  ;
7) Зафиксировать состав ПО выбранных агентов в качестве золотого образа –  ;
8) Отключить отслеживание состава ПО выбранных агентов золотому образу –  ;
9) Включить защиту от удаления для выбранных агентов –  ;
10) Выключить защиту от удаления для выбранных агентов –  ;
11) Изменить критичность для выбранных агентов –  ;
12) Выполнить команду на выбранных агентах –  (функционал старого терминала, оставлен для обратной совместимости с агентами старых версий);
13) Задать команду по реагированию для выбранных агентов –  (выполнение сценариев реагирования);
14) Исключить выбранных агентов из своих групп –  ;
15) Удалить выбранных агентов –  .
16) Принудительно синхронизировать конфигурацию агентов –  .

Добавить в группу – функция позволяет добавлять агентов в выбранную группу. Для добавления необходимо отметить флажком одного или нескольких агентов, далее нажать кнопку  , после чего выбрать операцию из списка (рис. 45).

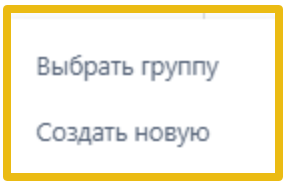
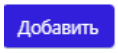


Рисунок 45 – Выбор операции с агентом

Если необходимо добавить выбранного/выбранных агента/агентов в уже созданную группу, то следует кликнуть по кнопке **Выбрать группу**, после чего в открывшемся окне выбрать нужную группу (рис. 46) и нажать кнопку  , после чего подтвердить действие.

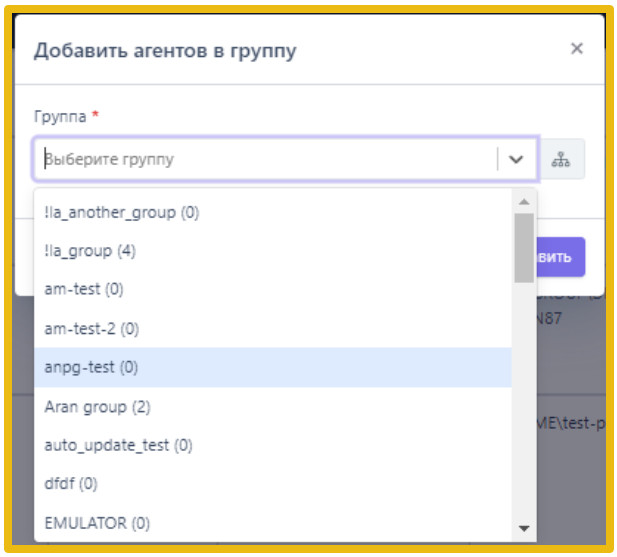


Рисунок 46 – Выбор группы из списка

Если необходимо добавить выбранных агентов во вновь создаваемую группу, то следует кликнуть по кнопке **Создать новую** (см. рис. 45), после чего в открывшемся окне ввести название в строке **Название группы** и нажать кнопку **Создать и добавить**.

Применить конфигурацию – функция позволяет привязывать наборы с конфигурациями к выбранным агентам. Для привязки к определенному набору одного или нескольких агентов необходимо отметить их флажком в столбце выбора агентов, после чего нажать кнопку применения конфигурации  . Откроется окно **Применение параметров конфигурации**, в котором следует назначить наборы с правилами, исключениями и профилями для отмеченных агентов. После завершения выбора необходимо нажать кнопку **Применить**.

По отношению к наборам, ранее привязанным к агентам, пользователь может выполнить следующие действия:

– замена наборов;

– добавление наборов (выбранные наборы будут поставлены перед ранее привязанными наборами), порядок наборов важен, так как анализаторы работают с первым одинаковым элементом из двух разных наборов, например, одному и тому же домену может быть присвоено в одном наборе действие **Разрешить**, а в другом **Блокировать**, соответственно, будет выполнено действие для домена из набора, проанализированного первым;

– удаление наборов (выбранные наборы будут удалены из списка ранее привязанных к агентам наборов).

– Администратор также может выбрать конфигурацию из шаблона, в этом случае произойдет замена ранее привязанной конфигурации наборов и профилей.

Включить/отключить автоматическое обновление выбранных агентов – по умолчанию на всех агентах включена опция автоматического обновления, чтобы ее отключить, необходимо отметить флажками нужных агентов, после чего нажать кнопку  и подтвердить действие в открывшемся окне. Для обратной операции необходимо отметить флажками агентов, для которых выключена опция автоматического обновления и нажать кнопку  , после чего подтвердить действие в открывшемся окне.

Включение/отключение защиты на выбранном агенте – защита включена по умолчанию на всех агентах, если требуется, чтобы функции защиты были отключены на агентах, то необходимо отметить их флажками, после чего нажать кнопку  и подтвердить операцию в открывшемся окне. Для обратной операции следует нажать кнопку  , после чего подтвердить выбранное действие в открывшемся окне.

Зафиксировать состав ПО выбранных агентов в качестве золотого образа – функция позволяет отслеживать изменения в программах, установленных на компьютере с агентом. При включенной опции фиксации состава ПО, EDR будет показывать администратору, какие обновления были сделаны в операционной системе, какие программы из состава золотого образа удалены и какие новые программы, не входящие в состав золотого образа, установлены на компьютере с агентом. Агенты, в составе которых имеются отличия от золотого образа, помечаются на странице **Агенты** в поле **Состояние** значком . Агенты с созданным золотым образом, состав ПО которых не менялся, будут отмечены значком .

Чтобы создать золотой образ состава ПО агентов, необходимо отметить их флагами, после чего нажать кнопку и подтвердить действие в открывшемся окне. Отключить функцию создания золотого образа можно, выбрав агентов с включенным образом и нажав кнопку **Отключить отслеживание соответствия состава ПО выбранных агентов золотому образу** (), после чего подтвердить операцию в открывшемся окне.

Включить защиту от удаления для выбранных агентов – чтобы включить защиту от удаления для выбранных агентов, необходимо отметить их флажками и нажать кнопку , после чего откроется окно ввода пароля для защиты от удаления агента. Удаление агента с компьютера, на котором он установлен, после завершения операции будет возможно только после ввода пароля. Чтобы увидеть и при необходимости скопировать пароль, необходимо перейти на страницу удаляемого агента. Пароль будет показан аналитику при наведении курсора на значок .

Отключить защиту от удаления для выбранных агентов – чтобы отключить защиту от удаления для выбранных агентов, необходимо отметить их флажками и нажать кнопку , после чего подтвердить операцию в открывшемся окне. Требование о вводе пароля при удалении агента будет снято.

Изменить критичность на выбранных агентах – чтобы изменить критичность на агентах, необходимо отметить флажком одного или нескольких агентов, после чего нажать кнопку . Откроется окно **Изменение критичности агентов**, в котором следует выбрать необходимую критичность, после чего нажать кнопку **Применить**. Операция требует подтверждающего действия, для завершения необходимо нажать кнопку **Подтвердить** в открывшемся окне.

Критичность влияет на управление уязвимостями, если агенту присвоен статус критичный и на нем обнаружена трендовая уязвимость, то для нее будет создан инцидент, отображаемый на странице с уязвимостями.

Выполнить команду на выбранных агентах – необходимо отметить флажком одного или нескольких агентов, после чего задать и выполнить команду для этих агентов. Это действие можно произвести нажатием кнопки  (следует обратить внимание, что функционал считается устаревшим и оставлен для совместимости с ранними версиями агента), после чего будет открыто окно, представленное на рисунке 47.

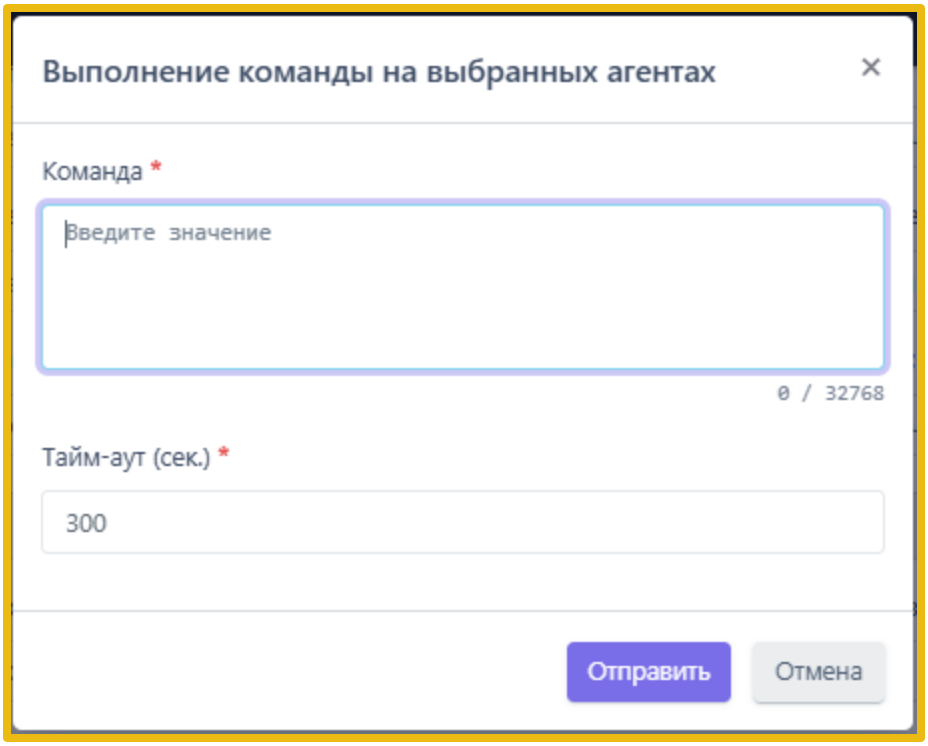


Рисунок 47 – Окно ввода команд

После ввода команды необходимо нажать кнопку **Отправить**. Список команд аналогичен командам, описанным в разделе 8.5.6.

Исключить выбранных агентов из своих групп – функция позволяет исключать выбранных агентов из своих групп. Для выполнения операции следует выбрать агентов, принадлежащих какой-либо группе, отметив их флажком в столбце выбора, далее нажать кнопку  , после чего подтвердить действие.

После удаления агента из группы в столбце **Группа/Имя агента** перестанет отображаться название группы и останется только имя агента, для которого применялась функция **Исключить из группы**.

Удалить выбранные – функция позволяет удалять выбранных агентов из списка зарегистрированных в Программе.

Для выполнения операции необходимо выбрать агентов, которых следует удалить, отметив их флажком в столбце выбора, далее нажать кнопку  и подтвердить действие.



Примечание

Если информация о ПО, установленном на машине с агентом, не отслеживается (не отслеживается соответствие золотому образу), то в столбце **Состояние** отсутствует иконка, сигнализирующая об этом. Соответствующие сведения будут указаны при раскрытии дополнительной информации об агенте.

Для удобства идентификации агентов администратором, имеется возможность скачать в формате CSV краткую информацию об агентах, нажав по иконке  . Файл будет загружен на компьютер, с которого был произведен вход в модуль администрирования, в папку **Загрузки**.

Информация об агентах в данном файле представлена в виде списка, где по каждому агенту представлены следующие данные:

1) Имя компьютера;
2) Домен;
3) Активен/не активен агент (активен – 1, не активен – 0);
4) Причина завершения работы, которая указывается в числах согласно следующему списку:

– 0 – Агент работает в штатном режиме;

– 1 – Штатное завершение работы компьютера;

– 2 – Штатный переход компьютера в состояние сна или гибернации;

– 3 – Штатная остановка агента;

5) Версия дистрибутива агента;
6) Сетевые адреса.

В файле будет присутствовать информация о тех агентах, которые отсортированы на странице **Агенты** в зависимости от выставленных фильтров, либо будет информация обо всех агентах, если фильтры отсутствуют.

8.5.2. Агент

Страница **Агент** позволяет выполнять различные операции с агентом, выполнять сценарии реагирования, а также просматривать информацию о функционировании агента.

Для перехода на страницу **Агент** требуется кликнуть по его имени. Имя агента присутствует в нескольких разделах Программы, например, на страницах **Агенты**, **Группы**, **Терминал**.

Общая информация

Страница разделена на несколько областей:

1) Агент;
2) Управление;
3) Конфигурация;
4) Информация о системе;
5) Программное обеспечение;
6) Описание;
7) Запуски задач агента;
8) Состояние агента;
9) Графики.

Агент – в области отображается информация об основных параметрах агента, некоторые из них администратор может изменять и сохранять сделанные изменения.

Управление – в области администратор может управлять различными состояниями агента, а также открыть терминал для управления агентом. Агент управляется через консоль с помощью функционала интерпретатора PowerShell.

Конфигурации – в области отображаются все наборы конфигураций, которые прикреплены к агенту. Каждый набор можно изменить, после чего применить измененную конфигурацию. Рядом с именем набора находится кнопка перехода к набору .

Информация о системе – в области отображается информация об операционной системе и основных характеристиках компьютера, на котором установлен выбранный агент.

Программное обеспечение – в области отображается информация о программном обеспечении, установленном на агенте.

Описание – в области можно добавить описание к агенту. Для сохранения описания необходимо нажать кнопку **Сохранить**.

Запуски задач агента – в области показаны ссылки на запуски задач. Кроме того, здесь представлены время запуска задачи, триггер, по которому задача выполняется, статусы агентов и кнопка завершения выполнения запуска. Кнопка активна, если запуск активен.

Состояние агента – в области отображается информация о состоянии агента: графики загрузки центрального процессора, использование памяти агентом, а также информация о событиях, происходящих на агенте (ошибки, предупреждения и т.д.), информация о процентном соотношении для топ-5 индикаторов атак в загрузке ЦП механизмом проверки индикаторов атак, информация о количестве захешированных данных, информация о количестве просканированных данных.

Журнал агента – в области отображается информация об ошибках, возникающих на агенте, например, об ошибках применения конфигурации правил.

Графики – в области отображается информация о работе компьютера, на котором установлен агент, в графическом виде.

Важно

Для агентов, у которых установлена опция с выключением драйвера, будет отсутствовать возможность переводить агента в изоляцию и включать защиту.

Область «Агент»

В области **Агент** пользователь может выполнить следующие операции:

1) Узнать информацию о наличии на агентах прикладных или системных ошибок;
2) Изменить имя агента;
3) Установить настройку обновления дистрибутива агента (автоматическое или вручную);

4) Узнать информацию об идентификаторе агента, при необходимости скопировать его;
5) Узнать информацию о часовом поясе агента;
6) Узнать информацию об установленной версии агента;
7) Узнать информацию об активности агента;
8) Узнать наименование ОС, на которой установлен агент;
9) Узнать время установки агента;
10) Узнать время последней верификации агента;
11) Узнать время последнего обновления конфигурации агента;
12) Узнать время обновления агента;
13) Узнать информацию о пяти последних пользователях, вошедших локально или дистанционно на компьютер с установленным агентом (кроме того, показывается и время входа);
14) Просмотреть количество программ с уязвимостями;
15) Удалить агента с сервера управления (после удаления агент автоматически отправится на верификацию);
16) Просмотреть уведомление о блокировках в рамках реагирования.

Примечание

Агент теряет статус активного, если на сервер не приходит статистическая информация от агента в течение 3 минут. При этом события активности за последние 15 минут для такого агента будут доступны.

На странице пользователю могут выводиться предупреждающие сообщения, отмеченные значком . При наведении курсора мыши на значок будет выведено сообщение, например, если время на агенте не соответствует настройкам часового пояса. Кроме того, в области **Агент** может отображаться значок , сигнализирующий о наличии системных или прикладных ошибок на агенте. Системные ошибки сообщают о наличие ошибок драйвера, а прикладные о наличии ошибок службы агента.

В рамках автоматического реагирования по сценарию реагирования на агенте может присутствовать иконка  , сигнализирующая о наличии блокировок (рисунок 48).

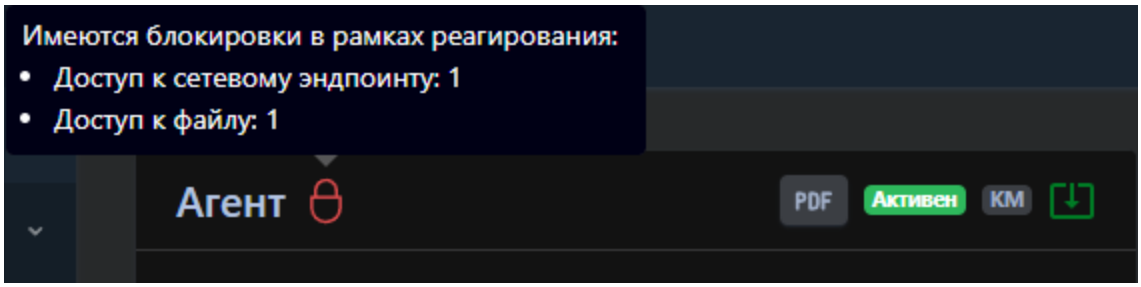


Рисунок 48 – Имеющиеся блокировки в рамках реагирования

Для получения более подробной информации о блокировках требуется с помощью терминала выполнить команду block list.

Здесь же находится кнопка для создания отчета по агенту в формате pdf (PDF). При нажатии кнопки отчет сохраняется в каталоге, установленном в настройках браузера компьютера, с которого осуществлен доступ к серверу управления. Также на странице может выводиться иконка оповещения , при наведении на которую выводится сообщение о будущем обновлении агента. Данная иконка говорит о том, что как только агент станет активным после перезагрузки, будет выполнено обновление агента.

Значок рядом с индикатором активности агента (KM) показывает, какой защитный компонент присутствует на агенте: компонент ядра или eBPF (технология в ядре Linux, позволяющая безопасно запускать программы в привилегированном контексте ядра, не изменяя его исходный код или загружая модули ядра).

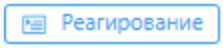
Для изменения имени выбранного агента необходимо в строке **Имя Агента** ввести новое имя, после чего нажать кнопку **Сохранить изменения** ( ).

Для всех агентов, верифицируемых в Программе, кнопка **Автоматическое обновление** ( ) включена по умолчанию. Чтобы снять автоматическое обновление, необходимо перевести кнопку в состояние **Отключено**.

Для удаления агента необходимо нажать кнопку Удалить Агента и подтвердить действие.

Область «Управление»

В области **Управление** пользователь может выполнить следующие операции:

1) Создать задачу по реагированию, выбрав из списка имеющихся сценариев реагирования (

);
2) Включить или отключить защиту на агенте;
3) Просмотреть и изменить пароль для удаления агента, установленного на конечной точке;
4) Узнать количество событий, зафиксированных агентом за сутки и за последние 15 минут;
5) Узнать количество инцидентов, зарегистрированных для агента за все время и количество открытых инцидентов, требующих внимания аналитика;
6) Открыть сессию онлайн-терминала для выбранного агента;
7) Настроить параметры получения информации о программах, установленных на агентах (золотой образ);
8) Включить или отключить на агенте защиту от удаления с компьютера, на котором он установлен;
9) Добавить агента в группу;
10) Узнать значение EPS (количество событий в секунду) для выбранного агента в текущий момент и среднее EPS за последнюю неделю.
11) Принудительно синхронизировать конфигурацию агента.

Защита агента – отключение защиты агента подразумевает, что на агенте перестают работать защитные функции драйвера агента, при этом агент может отправлять статистику, принимать новые конфигурационные наборы, обрабатывать команды терминала, кроме команд **stop и memscan**.

В поле **События** информация о количестве событий представлена в виде ссылок *За сутки: 0* и *За 15 мин: 0* . Для просмотра событий, зарегистрированных для агента за последние сутки необходимо нажать на ссылку **За сутки,** после чего откроется страница **Активность** для выбранного агента, показывающая сколько событий зарегистрировано для него за последние сутки. Для просмотра событий, зарегистрированных для агента за последние 15 минут следует нажать на ссылку **За 15 мин,** после чего для выбранного агента откроется страница **Активность**, показывающая сколько событий зарегистрировано для него за последние 15 минут. Для просмотра подробной информации о странице **Активность** необходимо перейти в пункт 8.4.2.

В поле **Инциденты** информация о количестве инцидентов представлена в виде ссылок *Всего: 8* и *Открытых: 6* . Для просмотра инцидентов, зарегистрированных для агента за все время, следует нажать на элемент **Всего**, после чего откроется страница **Инциденты** для выбранного агента, показывающая, сколько инцидентов зарегистрировано для него за все время функционирования.

Для просмотра инцидентов, открытых для выбранного агента в данный момент, необходимо нажать ссылку **Открытых**, после чего откроется страница **Инциденты** для указанного агента, показывающая информацию об открытых на текущее время инцидентах. Для просмотра подробной информации о странице **Инциденты** следует перейти в пункт 8.4.1.

В поле **Золотой образ** в разделе **Управление** администратор может просмотреть состояние золотого образа (зафиксированное состояние списка установленных программ на машине с агентом).

Состояние может быть следующим:

– Не отслеживается (список установленных программ не отслеживается агентом);

– Совпадение (список установленных программ совпадает с зафиксированным состоянием золотого образа;

– Имеются отличия (список установленных программ отличается от зафиксированного состояния золотого образа).

В поле **Золотой образ** имеется иконка , при нажатии по которой ЛКМ открывается окно выбора действий по работе с золотым образом (рис. 49).

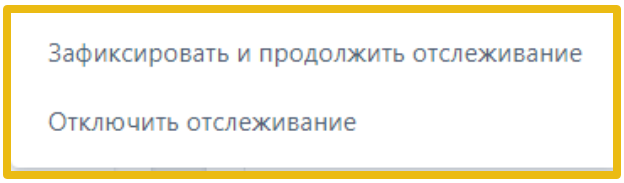
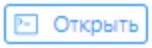


Рисунок 49 – Действия с золотым образом

В области **Программное обеспечение** в списке **Установленное ПО** программы из списка золотого образа, удаленные на агенте, будут помечены значком и зачеркиванием, а программы, вновь установленные, но не зафиксированные агентом в золотом образе, будут помечены значком .

Для фиксации списка установленных программ требуется выбрать действие **Зафиксировать и включить отслеживание**, после чего появится окно подтверждения действия фиксации золотого образа. Для фиксации далее требуется нажать кнопку **Выполнить**.

В поле **Терминал** пользователь может перейти к открытой сессии онлайн-терминала для выбранного агента, нажав кнопку 

.

В поле **Защита от удаления** администратор может включить или отключить настройку агента, позволяющую удалять агента после ввода специального пароля. Для этого необходимо перевести кнопку  во включенное или выключенное положение и подтвердить выполнение операции в открывшемся окне. После ввода пароля функция защиты от удаления будет включена, и пароль будет показан в строке **Пароль** при наведении курсора на значок  . Его можно в любое время изменить с помощью значка Редактировать ().

Пароль должен соответствовать следующим требованиям:

1) Пароль не должен совпадать с именем пользователя или другой персональной информацией или быть слишком похожей на нее;
2) Пароль должен содержать как минимум 12 символов;
3) Пароль не может быть одним из широко распространенных паролей;
4) Пароль не должен состоять только из цифр.

В поле **Группа** пользователь может просмотреть информацию о группе, к которой принадлежит агент. В случае, если агент не входит ни в одну из зарегистрированных в Программе групп, то в поле **Группа** будет указано, что агент находится не в группе.

Для добавления выбранного агента в группу следует нажать ЛКМ в поле **Выберите группу** и выбрать из появившегося списка название группы, в которую нужно добавить агента.

После выбора группы необходимо нажать кнопку **Сохранение изменения** (). Далее в открывшемся окне **Подтверждение действия** следует нажать кнопку 

, после чего в нижней части страницы появится сообщение о добавлении агента в группу.

После добавления агента в группу в поле **Группа** будет указано название группы, в которую теперь входит агент.

Для удаления агента из группы следует нажать кнопку **Исключить из группы**  . Далее в открывшемся окне **Подтверждение действия** следует нажать кнопку  .

Область «Конфигурации»

Конфигурации разделены по двум вкладкам: **Наборы** и **Профили**.

В этих вкладках администратор может выполнять следующие операции:

– применять к выбранному агенту определённый набор исключений для файлов;

– применять к выбранному агенту определённый набор исключений для программ;

– применять к выбранному агенту определённый набор сетевых исключений;

– применять к выбранному агенту определённый набор исключений для индикаторов атак;

– применять к выбранному агенту определённый набор индикаторов компрометации;

– применять к выбранному агенту определённый набор журналов;

– применять к выбранному агенту определённый набор YARA-правил для файлов;

– применять к выбранному агенту определённый набор YARA-правил для памяти;

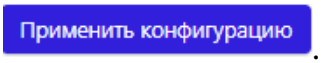
– применять к выбранному агенту определённый набор индикаторов атак;

– применять к выбранному агенту определённый профиль Антишифра;

– применять к выбранному агенту определённый профиль безопасности;

– применять к выбранному агенту определённый профиль контроля USB.

Аналитические правила и профили, описанные в конфигурационных наборах, применяются на агентах только в случае, если выбранный набор или профиль сохранен и его конфигурация применена для соответствующего агента. Для наборов и профилей указывается дата и время применения на агенте.

Для изменения конфигурации наборов необходимо в поле с наборами нажать ЛКМ на строке с названием текущего набора и из выпадающего списка выбрать набор или несколько наборов, после чего нажать кнопку  . После применения конфигурации в нижней части страницы появится сообщение о сохранении конфигурации агента.

Для применения конфигурационных наборов, прикрепленных к агенту, необходимо нажать кнопку **Перейти к набору (набор не применен)**  в строке с названием соответствующего набора.

Область «Информация о системе»

В области **Информация о системе** отображается следующая информация:

1) Имя компьютера;
2) Время загрузки системы;
3) Версия ОС;
4) Процессор;
5) Количество ядер процессора;
6) Объем оперативной памяти (МБ);
7) Жесткие диски;
8) Сетевые интерфейсы.

Имя компьютера – в поле отображается имя компьютера, на котором установлен агент.

Время загрузки системы – в поле отображается информация о дате и времени последней загрузки операционной системы, под управлением которой действует агент.

Версия ОС – в поле отображается версия операционной системы, под управлением которой работает компьютер с установленным агентом.

Процессор – в поле отображается наименование и тактовая частота процессора компьютера, на котором установлен агент.

Количество ядер процессора – в поле отображается количество ядер процессора у компьютера, на котором установлен агент.

Объем оперативной памяти (МБ) – в поле отображается объем оперативной памяти компьютера, на котором установлен агент. Объем указан в мегабайтах.

Жесткие диски – в поле отображается подробная информация о жестком диске компьютера, на котором установлен агент: название, наименование дискового накопителя, его размер, модель, производитель, а также уникальный аппаратный идентификатор жесткого диска.

Сетевые интерфейсы – в поле отображается подробная информация о сетевых интерфейсах компьютера, на котором установлен агент: тип подключения к сети, наименование сетевого адаптера, ip-адреса по четвёртой и шестой версии протоколов.

Область «Программное обеспечение»

Область содержит информацию по обновлениям системы, список установленного на агенте программного обеспечения и отдельный список установленных драйверов. Списки показывают различия между текущим состоянием системы и золотым образом системы, если включено отслеживание золотого образа. Обновление списка ПО возможно с помощью кнопки **Обновить информацию**.



Важно

Информация об установленном ПО обновляется при каждом запуске агента (старт компьютера, установка или обновление агента), но не реже 1 раза в сутки в автоматическом режиме или принудительно по запросу, путем отправки агенту команды inventory через Терминал. Информация о системе обновляется также при каждом запуске агента. Если меняется конфигурация сетевых интерфейсов или накопителей, то эта информация обновляется автоматически непосредственно в момент такого изменения.

Область «Описание»

В области **Описание** пользователь может произвольно описать характеристики, состояние, или особенности агента. Чтобы сохранить описание, пользователю необходимо нажать кнопку **Сохранить**.

Область «Запуск задач агента»

В области **Запуск задач агента** пользователь может просмотреть таблицу со списком запусков задач по данному агенту. Нажав по имени запуска можно перейти на страницу запуска задачи.

Область «Состояние агента»

В области **Состояние агента** отображаются последние 500 сообщений о событиях журнала агента, например, когда не обновляется конфигурация определенных правил.

В журнале реализован простой поиск по совпадению с запросом. Также события можно фильтровать по уровню: критическая ошибка, ошибка, предупреждение, информация и подробно.

Кроме журнала с оповещениями о состоянии агента в области отображаются графики, показывающие:

— загрузку центрального процессора службой и драйвером агента;

— использование агентом (службой и драйвером по отдельности) памяти;

— топ-5 индикаторов атак по нагрузке от общей нагрузки на ЦП механизма проверки индикаторов атак/исключений (показана в bps (базисные пункты – единица измерения доли времени ЦП, которое ИА-подсистема агента потратила на проверку конкретного индикатора атак или исключения), 10000 bps соответствует 100 процентам от нагрузки);

— количество захешированных данных в байтах;

— количество просканированных данных в байтах.

Область «Графики»

В графическом виде показана информация о работе компьютера, на котором установлен агент. На странице **Агент** отображаются графики работы за последние 15 минут.

При включенном компьютере, на котором установлен агент, в области **Графики** отображается следующая информация:

1) Загрузка ЦП;
2) Загрузка памяти;
3) Процессы;
4) Нити;
5) Описатели;
6) Загрузка диска (чтение);
7) Загрузка диска (запись);
8) Загрузка сети (передача);
9) Загрузка сети (прием);
10) Количество сетевых соединений.

Загрузка ЦП – на графике отображается загрузка центрального процессора компьютера, на котором установлен агент, в процентах от общей производительности. На оси x показано время с шагом в 3 минуты 15 секунд, а на оси y показана загрузка ЦП в процентах.

При наведении курсора на точку графика пользователю во всплывающем окне будет показан процент загрузки центрального процессора в конкретный момент времени.

Загрузка памяти – на графике отображается загрузка оперативной памяти компьютера, на котором установлен агент, в процентах от общей производительности. На оси x показано время с шагом в 3 минуты 15 секунд, а на оси y показана загрузка оперативной памяти в процентах. При наведении курсора на точку графика пользователю во всплывающем окне будет показан процент загрузки оперативной памяти в конкретный момент времени.

Процессы – на графике отображается количество активных процессов ОС, запущенных на компьютере, на котором установлен агент. На оси x показано время с шагом в 3 минуты 15 секунд, а на оси y показано число активных процессов ОС. При наведении курсора на точку графика пользователю во всплывающем окне будет показано точное количество процессов в конкретный момент времени.

Нити – на графике отображается количество активных нитей ОС, запущенных на компьютере, на котором установлен агент. На оси x показано время с шагом в 3 минуты 15 секунд, а на оси y показано число активных нитей. При наведении курсора на точку графика пользователю во всплывающем окне будет показано точное количество нитей в конкретный момент времени.

Описатели – на графике отображается количество активных описателей, работающих на компьютере, на котором установлен агент. На оси x показано время с шагом в 3 минуты 15 секунд, а на оси y показано число активных описателей.

При наведении курсора на точку графика пользователю во всплывающем окне будет показано точное количество описателей в конкретный момент времени.

Загрузка диска (чтение) – на графике отображается скорость чтения файлов с жесткого диска, на котором установлена ОС с действующим агентом.

На оси x показано время с шагом в 3 минуты 15 секунд, а на оси y показана скорость чтения с диска в килобайтах в секунду.

При наведении курсора на точку графика пользователю во всплывающем окне будет показана точная скорость загрузки диска на чтение в конкретный момент времени.

Загрузка диска (запись) – на графике отображается скорость записи файлов на жесткий диск, на котором установлена ОС с действующим агентом. На оси x показано время с шагом в 3 минуты 15 секунд, а на оси y показана скорость записи на диск в килобайтах в секунду.

При наведении курсора на точку графика пользователю во всплывающем окне будет показана точная скорость записи файлов на диск в конкретный момент времени.

Загрузка сети (передача) – на графике отображается скорость передачи файлов с компьютера, на котором установлен агент. На оси x показано время с шагом в 3 минуты 15 секунд, а на оси y показана скорость передачи в килобитах в секунду. При наведении курсора на точку графика пользователю во всплывающем окне будет показана точная скорость сетевой передачи файлов в конкретный момент времени.

Загрузка сети (прием) – на графике отображается скорость приема файлов на компьютер, на котором установлен агент. На оси x показано время с шагом в 3 минуты 15 секунд, а на оси y показана скорость приема в килобитах в секунду. При наведении курсора на точку графика пользователю во всплывающем окне будет показана точная скорость сетевой передачи файлов в конкретный момент времени.

Количество сетевых соединений – на графике отображается количество сетевых соединений между хостом, на котором установлен агент, и внешним сетевым периметром.

Возврат к нормальному режиму работы после установки агента в режиме «no_driver»

Для возврата агента, который был установлен с опцией «no_driver», к нормальному режиму работы требуется выполнить следующие действия:

1) В модуле администрирования перейти в раздел Терминал;
2) Выбрать агента, которому требуется изменить параметр;
3) Выполнить команду:

enable

4) Перейти на страницу агента и убедиться, что опция **Защита агента** включена.

Указанные выше команды можно выполнить для группы агентов на странице **Агенты** с помощью команды **Выполнить команду на выбранных агентах** ( ).

8.5.3. Группы

Общий вид страницы **Группы агентов** представлен на рисунке 50.

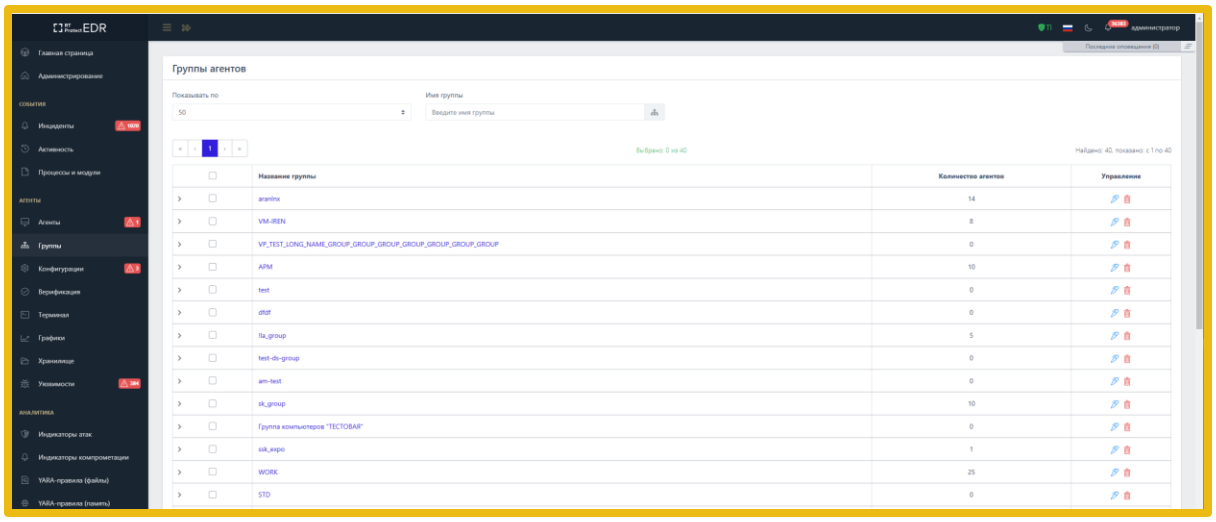


Рисунок 50 – Страница «Группы агентов»

На странице **Группы агентов** в табличном виде представлена информация о созданных группах, их именах, а также о количестве агентов, входящих в эти группы.

В таблице со списком групп отображаются следующие поля:

1) Поле выбора агентов (отмечено кнопкой выбора ☐);
2) Название группы;
3) Количество агентов;
4) Управление.

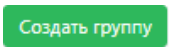
Для выбора в таблице одной или нескольких групп агентов необходимо отметить флажком кнопки выбора для соответствующих групп. Для отмены выбора следует нажать на кнопку выбора ☑ повторно.

Название группы – в поле отображается имя группы агентов. При нажатии ЛКМ на названии группы агентов происходит переход к странице **Группа** выбранной группы агентов.

Количество агентов – в поле в числовом виде отображается количество агентов в выбранной группе.

Управление – в поле отображаются кнопка изменения названия группы ( ) и кнопка для удаления группы .

При нажатии ЛКМ на значок › в поле с кнопкой выбора открывается информация об агентах, принадлежащих этой группе. Если в группе отсутствуют прикрепленные к ней агенты, то в раскрытой строке будет отображаться надпись об отсутствии агентов в выбранной группе. Если в группе есть прикрепленные агенты, то они будут отображаться в раскрытой строке.

В нижней части области **Группы** расположены кнопки операций 

и 

. Для создания новой группы агентов следует ввести её название в поле **Название группы** и нажать кнопку **Создать группу**. После этого в нижней части страницы появится сообщение о добавлении новой группы, а в таблице со списком групп появится строка с информацией о новой группе.

Для удаления группы или нескольких групп агентов необходимо выбрать их, отметив флажком в поле выбора групп, и нажать кнопку **Удалить выбранные**.

Далее в открывшемся окне **Подтверждение действия** следует нажать кнопку 

. После удаления выбранные группы агентов не будут отображаться в списке таблицы.

Имя группы является активной ссылкой, при нажатии по которой осуществляется переход на страницу **Агенты** с сортировкой агентов по соответствующей группе.

8.5.4. Конфигурации

Раздел **Конфигурации** содержит редактируемые настройки наборов и профилей для агентов Windows и Linux, которые агенты получают в момент верификации. Можно настраивать несколько наборов в одной конфигурации. Кроме того, аналитик может настраивать собственные удаляемые и редактируемые конфигурации, которые могут использоваться в качестве шаблонов, распространяемых на агентов на странице **Агенты**.

Для новых агентов автоматически назначаются конфигурации с наборами по умолчанию.

Чтобы создать новую конфигурацию, необходимо нажать кнопку **Создать конфигурацию**. Откроется окно **Создание конфигурации**, в котором необходимо задать имя конфигурации и выбрать наборы и профили. Кнопка **Создать** будет активна только в том случае, когда будут назначены все наборы и профили конфигурации.

Конфигурации можно редактировать и удалять, при этом удалить используемые при верификации конфигурации по умолчанию для Windows и Linux нельзя. Чтобы редактировать конфигурацию, необходимо нажать кнопку . Чтобы удалить конфигурацию, необходимо нажать кнопку .

Администратор может работать со списком конфигураций с помощью фильтра по имени. Конфигурации сортируются на странице по алфавиту или по числовым и символьным значениям.

8.5.5. Верификация

Общие сведения

Верификация и деверификация являются обычными действиями администрирования системы. В частности, верификацию ожидают все новые установленные агенты. Верификацию обязаны пройти и агенты, которые были перезапущены, или те агенты, которые внезапно стали получать от сервера ошибки на все другие запросы.

В запросе верификации в обязательном порядке передаются идентификатор агента (agent_id), токен агента (token), а также набор других полезных данных машины с установленным агентом (сетевое имя, версия ОС и т. д.). Для верификации агента необходимо выполнить ряд действий.

Сразу после старта программа агента должна убедиться, что сервер готов принимать от него данные (события). Необходимым условием для этого является «доверие» сервера токену (token) агента. Самым первым запросом к серверу является запрос на верификацию агента. Если сервер отвечает на запрос верификации кодом 200 (OK), то агент переходит к запросу «черных» и «белых» списков и отправке событий и статистики на сервер. В случае получения агентом ошибочного ответа на запрос о верификации, агент повторяет запрос на верификацию спустя время равное t (~2 минуты).

При первичной инициализации агентской сети на основе единого «золотого образа» в окне **Верификация** могут наблюдаться записи, отмеченные восклицательным знаком. Данные записи носят информационный характер и говорят о том, что для агента был автоматически сгенерирован новый устойчивый токен. Записи исчезнут из окна верификации в течение 5-15 минут. В окне **Верификация** останутся только агенты, которых нужно верифицировать (если включен режим верификации новых агентов, то это будет выполнено сервером автоматически, в противном случае это необходимо сделать вручную, выбрав агентов и нажав кнопку **Верифицировать выбранных**).

При манипуляциях с «золотым образом» (например, переустановке агента в нем при пересоздании) на стороне сервера могут наблюдаться дубликаты агентов, созданных из разных вариаций «золотого образа». Один из этих дублирующихся агентов будет актуальным и активным, а остальные необходимо удалить вручную, либо они будут удалены сервером автоматически по прошествии периода неактивности (по умолчанию 60 дней).

В Программе существует два случая автоверификации:

1) В первом случае агент должен быть верифицирован ранее администратором Программы. Если после этого у агента меняется токен, то он пропускается в систему уже без повторного подтверждения.
2) Во втором случае автоверификация устанавливается в настройках сервера при его развёртывании. В этом случае новый агент допускается в систему без подтверждения администратором.

При верификации агенту с сервера в первую очередь передаются наборы с исключениями и профилям, и только потом добавляются аналитические наборы (индикаторы атак, компрометации и т.д.).



Важно

По умолчанию события, возникшие на агенте до этапа верификации, не приходят на сервер.

Процедура верификации

При переходе на страницу **Верификация** администратор имеет возможность просмотреть всех неверифицированных агентов и произвести процедуру верификации. Если отсутствуют агенты, требующие верификации на сервере, то на странице отображается соответствующая запись.

При наличии агентов, требующих верификации, на странице будет представлена информация об этих агентах.

На странице представлены следующие поля фильтрации:

1) Показывать по – фильтрует агентов по количеству отображаемых на странице;
2) Сетевой адрес – фильтрует агентов по сетевым адресам;
3) Имя компьютера – фильтрует агентов по имени компьютера;
4) Домен – фильтрует агентов по имени домена.

В верхней части страницы справа находится кнопка для сброса настроек фильтрации Сбросить фильтры . При активации кнопки все настройки фильтрации сбрасываются на значения, заданные по умолчанию.

В шапке таблицы представлены следующие поля:

1) Кнопка выбора (отмечена элементом);
2) ID;
3) Сетевые адреса;
4) Домен/Имя компьютера;
5) Операционная система;
6) Часовой пояс;
7) Данные об активности (Новый / Добавлялся ранее).

Рядом с кнопкой выбора агента находится элемент , который позволяет открывать дополнительную информацию об агенте, требующем верификацию:

1) Домен (или рабочая группа)/Имя компьютера;
2) Время загрузки системы;
3) Версия ОС;
4) Процессор;
5) Количество ядер процессора;
6) Объем оперативной памяти (МБ);
7) Жесткие диски;
8) Сетевые интерфейсы;

Информация об агенте, ожидающем верификацию, при установке нового агента в системе появится в таблице. Для верификации агента необходимо отметить его флажком , после чего нажать кнопку **Верифицировать выбранных**.

Элементы навигации в таблице с агентами, требующими верификации, идентичны описанным в пункте 8.2.2 (см. рис. 9).

Перед процедурой верификации можно добавить агента в определенную группу или создать для него свою группу. Для добавления в группу перед верификацией необходимо выбрать определенную группу агентов в поле **Добавить группу**.

Для добавления во вновь созданную группу перед верификацией следует в поле **Создать новую группу** ввести название новой группы. В эту группу будет включен агент после завершения процедуры верификации.

8.5.6. Терминал

Общая информация

Терминал является консолью управления, предназначенной для задания команд определенному агенту. Формат команд аналогичен формату средства автоматизации PowerShell. Функционал является устаревшим и оставлен для совместимости с ранними версиями агента. Для замены терминала в Программе присутствует онлайн-терминал, вызываемый с помощью кнопки  на горизонтальной панели управления в верхней части окна Программы.

При переходе на страницу **Терминал** появится окно, представленное на рисунке 51.

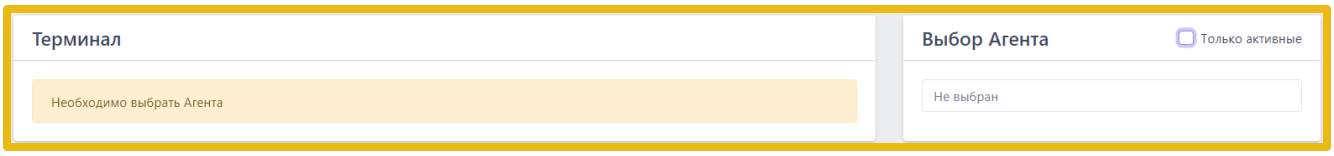
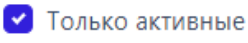


Рисунок 51 – Страница «Терминал»

В области **Выбор Агента**, находящейся в правой части, необходимо выбрать из всплывающего списка агента, для которого будут вводиться команды в терминале. Чтобы оставить в списке только активные в данный момент агенты, следует установить флажок  .

Если флажок не устанавливать, то для выбора будут доступны все агенты, но отправлять команды в терминале можно будет только активным, для неактивных агентов будет доступен только просмотр истории команд терминала.

После выбора активного агента с левой стороны страницы появится окно **Терминал**, разделённое на две области:

1) Область просмотра истории работы с терминалом;
2) Область ввода команд.

Если в списке выбрать неактивного в данный момент агента, то область ввода команд будет выделена для такого агента заливкой серого цвета, обозначающей, что ввод команд невозможен, кнопки Прервать Отправить также будут неактивны, как и область ввода **Таймаут (сек)**. По умолчанию таймаут составляет 300 секунд.

Отправка команд управления на странице «Терминал»

Для управления агентом с помощью командной строки необходимо в области ввода с прописанной в ней подсказкой **Введите команду (Enter – отправить, Ctrl-C – прервать, макс. длина 32768 символов)** ввести необходимую команду и нажать клавишу **Enter** или кнопку Отправить.

В области просмотра истории терминала отображаются ранее введённые команды и показывается текущий статус выполнения команды. Предусмотрены следующие статусы: Отправлена / Получена / Выполнена (код 0). Для просмотра основных доступных команд и описаний к ним следует ввести в окне терминала команду **help** (рис. 52).

```
Список основных команд:

cat               Читает файл с диска и отображает его в виде ASCII
clean             Удаляет зарезервированные файлы
cp                Копирует файл или директорию
enable            Включает управления защитой агента (для агентов с параметром /no_driver)
get               Загружает файл в файловое хранилище или сервер аналитики
get-eventlog      Отображает события, зарегистрированные в журнале событий, или список журналов событий
get-variable      Предоставляет доступ к переменным среды Windows
help              Отображает эту справку или справку по команде
inventory         Обновляет информацию об установленном ПО, обновлениях и драйверах агента
ipconfig          Выводит информацию о конфигурации сети
ls                Отображает списки файлов и директорий в заданной директории
mkdir             Создает директорию
mv                Перемещает файл или директорию
netstat           Отображает статистику протокола и текущих сетевых подключений TCP/IP
ps                Отображает информацию о процессах
put               Загружает файл на агент
reg               Управление реестром Windows
restart-computer  Перезагружает ОС
restore           Восстанавливает файлы процесса из каталога SHADOWCOPY
rm                Удаляет файл или директорию
shutdown          Выключает ОС
startas           Выполняет команду в активной сессии пользователя
stop              Завершает процесс
tray              Управляет значком и уведомлениями в трее
```

Рисунок 52 – Список основных команд терминала

Если требуется справка о команде из представленного списка, необходимо ввести команду, написание которой удовлетворяет синтаксису:

1) get-helphelp {<имя_командлета> | <название_раздела>};

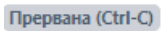
2) help {<имя_командлета> | <название_раздела>};

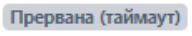
3) <имя_командлета> -?.

Снизу от области просмотра истории терминала находится кнопка перехода к результату последнего ввода команды 

.

В нижней части области **Терминал** содержится кнопка 

, ее действие дублируется с помощью нажатия сочетания клавиш Ctrl+C во время выполнения команды в терминале. С помощью кнопки или сочетания клавиш можно прервать выполнение команды. Статус команды поменяется на 

, а через единицу времени, указанную в поле **Таймаут (сек)** статус поменяется на 

.

Для установки времени ожидания ответа от агента при отправке команд в поле **Таймаут (сек)** необходимо указать нужный интервал времени в секундах. По умолчанию время ожидания составляет 30 секунд.

Для изменения агента в области **Выбор Агента** нужно нажать кнопку  в строке с названием текущего агента, после чего из выпадающего списка выбрать нового агента.

Описание команд терминала, реализованных в службе агента

Перечень команд, реализованных в службе агента:

– clean;

– drop;

– get;

– put;

– inventory;

– restore;

– startas;

– stop;

– tray;

– enable;

– команды перезапуска службы агента;

– trace;

– memscan;

– memdump;

– netlimit;

– reset-errors.

– get-log;

– remed.

Команда **clean** – удаляет зарезервированные файлы. Команда выполняется согласно синтаксису **clean** [<Максимальный возраст файлов>]. Максимальный возраст файлов (допустимые суффиксы: d – дни, h – часы, m – минуты). По умолчанию: используется значение из профиля Антишифра (10 дней).

Примеры написания команды **clean**:

clean 10h – удаляет зарезервированные файлы старше десяти часов;

clean 2d – удаляет зарезервированные файлы старше двух дней.

Команда **drop** – принудительно завершает сетевое соединение.

Команда выполняется согласно синтаксису drop [-id] <fluuid или flow> [-w admin|ti], где

– id – fluuid или flow сетевого соединения;

– w – кто завершил сетевое соединение: admin - администратор, ti - TI платформа (по умолчанию: admin).

Примеры написания команды **drop**:

drop -id c24bba95-9d6b-01da-2d12-000000000000 – Завершает сетевое соединение с уникальным идентификатором (поле fluuid в событии) c24bba95-9d6b-01da-2d12-000000000000;

drop -id 2096738 – Завершает сетевое соединение с идентификатором (поле flow в событии) 2096738.

Команда **get** – загружает файл в файловое хранилище EDR. Команда выполняется согласно синтаксису get [-f] <Полный путь до файла> [-t <ti или cloud>] [-r] [-xl], где:

-f – путь до файла;

-t – тип хранилища для загрузки файла (ti – TI-платформа, cloud – хранилище EDR, по умолчанию берется тип хранилища cloud);

-r – удаление файла после успешной загрузки (по умолчанию: файл не удаляется);

-xl – параметр разрешает загрузку файла больше 32 МБ (по умолчанию: ограничение на макс. размер загружаемого файла 32 МБ).

Пример написания команды:

get "\Device\HarddiskVolume8\Windows\SysWOW64\vmnat.exe" (загрузка файла в хранилище EDR);

get "\Device\HarddiskVolume8\Windows\SysWOW64\vmnat.exe" -t cloud (загрузка файла в хранилище EDR);

get "\Device\HarddiskVolume8\Windows\SysWOW64\vmnat.exe" -t ti (загрузка файла на TI-платформу).

Команда **inventory** – обновляет информацию об установленном ПО, обновлениях и драйверах агентов.

Команда **put** – загружает файл с сервера EDR на машину с установленным агентом. Команда выполняется согласно синтаксису put [-u] <Ссылка для загрузки> [-w <Расположение файла на агенте>] [-y] [-n <Новое имя файла>], где:

-u – это ссылка для загрузки;

-w – расположение файла на агенте (директория, в которую загружается файл, если директория не существует, то она создается, по умолчанию C:\ProgramData\РТ-Информационная безопасность\Агент RT Protect EDR\download\);

-y – перезапись существующего файла (по умолчанию перезаписи нет);

-n – новое имя файла (по умолчанию имя берется из ссылки для загрузки).

Примеры написания команды:

1) Команда загрузки файла на машину с агентом по пути C:\ProgramData\РТ-Информационная безопасность\Агент RT Protect EDR\download\first_aid_kit.exe:

put https://<адрес_сервера>/api/storage/user/object/<UUID-объекта>/first_aid_kit.exe;

2) Команда загрузки файла на машину с агентом по пути C:\Tools\file_ver_1.exe:

put https://<адрес_сервера>/api/storage/user/object/<UUID-объекта>/first_aid_kit.exe -w C:\Tools -n file_ver_1.exe.

Команда **restore** – восстанавливает зарезервированные файлы. Команда выполняется согласно синтаксису restore [-id] <UUID-процесса> [-c], где -id – это UUID процесса, а -c – аргумент для удаления созданных файлов.

Пример написания команды:

restore -id {FD547C1E-4260-40DA-9DB9-6D4A22F4FEE4}.

Команда **startas** – запускает процесс под определенным пользователем. Команда выполняется согласно синтаксису startas [-cmd] <Командная строка> [-u <Имя пользователя>] [-ws {normal | hidden | minimized | maximized}], где:

-cmd – это командная строка для запуска;

-u – имя пользователя с активной сессией (по умолчанию используется активная сессия пользователя);

-ws – стиль окна запускаемого процесса: normal (по умолчанию), hidden, minimized, maximized.

Пример написания команды:

startas calc.

Команда **stop** – завершает процесс. Команда выполняется согласно синтаксису stop [-id] <UUID процесса [-c <Статус завершения процесса>] [-w admin|ti] [-t <Тип сообщения>], где:

-id – это UUID процесса;

-c – статус завершения процесса (по умолчанию 0);

-w – кто завершил процесс: admin – администратор, ti – TI-платформа (по умолчанию admin);

-t – тип сообщения, определяет уровень уведомления о завершении процесса: info, warning, error (по умолчанию, если параметр -w установлен как admin, то -t принимает значение info, если параметр -w установлен как ti, то -t принимает значение error).

Примеры написания команды:

stop -id {FD547C1E-4260-40DA-9DB9-6D4A22F4FEE4};

stop -id {FD547C1E-4260-40DA-9DB9-6D4A22F4FEE4} -w ti;

stop -id {FD547C1E-4260-40DA-9DB9-6D4A22F4FEE4} -w admin -t error.

Формат команды для кнопки **Завершить процесс**: stop -id {FD547C1E-4260-40DA-9DB9-6D4A22F4FEE4}

Формат команды для завершения процесса по требованию TI-платформы: stop -id {FD547C1E-4260-40DA-9DB9-6D4A22F4FEE4} -w ti.

Команда **tray** – управляет значком и уведомлениями в трее.

Команда выполняется согласно синтаксису tray [<Уровень>], где:

[<Уровень>] 0 – нет значка в трее, уведомления не выводятся;

[<Уровень>] 1 – есть значок, уведомления не выводятся;

[<Уровень>] 2 – есть значок, показывать только критические уведомления;

[<Уровень>] 3 – есть значок, показывать все уведомления.

Пример написания команды:

tray;

tray 2.

Команда **enable** – включает управление защитой агента, установленного с параметром /no_driver.

Для перезапуска службы агента необходимо выполнить последовательно следующие команды в терминале агента:

– New-ItemProperty -Path HKLM:\System\CurrentControlSet\Services\Vrpsvc -Name AllowStop –PropertyType DWord -Force -Value 1

– & sc.exe control vrpsvc 128

– restart-service vrpsvc

Команда **trace** управляет трассировкой агента. Команда выполняется согласно синтаксису trace <-start или -stop> <-svc или -drv> [маска логируемых подсистем (по умолчанию трассируются все подсистемы: 0xFFFFFFFF)][уровень логирования (по умолчанию: 0xFF)][-s], где:

-start – запускает трассировку;

-stop – останавливает трассировку;

-svc – управление трассировкой службы;

-drv – управление трассировкой драйвера;

-usb – управление трассировкой USB-драйвера;

– [маска логируемых подсистем] – маска трассируемых подсистем службы или драйвера (используется в команде -start);

– [уровень логирования] – 0x5 (Verbose), 0x4 (Informational), 0x3 (Warning), 0x2 (Error), 0x1 (Critical), (используется в команде -start);

— -s – аргумент, позволяющий не удалять файл трассировки после остановки (по умолчанию файл будет удален после удачной отправки на сервер), (используется в команде -stop).

— Маски логируемых подсистем и наименования этих подсистем приведены в таблице 50.

Таблица 50 – Маски логируемых подсистем

Подсистемы	Маски
Маски логируемых подсистем для службы агента	
TRACE_SERVICE_ENGINE	0x00000001
TRACE_EVENTS	0x00000002
TRACE_METADATA_ENGINE	0x00000004
TRACE_AGENT_UPDATE	0x00000008
TRACE_FILE_SCANNER	0x00000010
TRACE_NETWORK_CONTAINMENT	0x00000020
TRACE_SESSION_MONITOR	0x00000040
TRACE_ETW_CONSUMER	0x00000080
TRACE_ETW_DOTNET_LOAD_IMAGE_MONITOR	0x00000100
TRACE_ETW_RPC_MONITOR	0x00000200
TRACE_ETW_KERBEROS_ATTACK_MONITOR	0x00000400
TRACE_ETW_SYSTEMTIME_CHANGED_MONITOR	0x00000800
TRACE_ETW_WMI_ACTIVITY_MONITOR	0x00001000
TRACE_ETW_MONITORS	0x00002000
TRACE_TERMINAL	0x00004000
TRACE_WMI_MONITOR	0x00008000
TRACE_SYSTRAY	0x00010000
TRACE_MS_GROUP_POLICY	0x00020000
TRACE_YARA	0x00040000
TRACE_ML	0x00080000
Маски логируемых подсистем для драйвера агента	
TRACE_REGISTRY_MONITOR	0x00000001
TRACE_REGISTRY_MATCHER	0x00000002
TRACE_REGISTRY_CONFIG_PARSER	0x00000004
TRACE_RESERVED1	0x00000008
TRACE_FS_MONITOR	0x00000010
TRACE_FS_MONITOR_SIGN	0x00000020
TRACE_FS_MONITOR_RULES	0x00000040
TRACE_FS_MONITOR_HASHES	0x00000080
TRACE_FS_MONITOR_SCAN	0x00000100
TRACE_FS_MONITOR_DEF_SCAN	0x00000200

Подсистемы	Маски
TRACE_RESERVED2	0x00000400
TRACE_RESERVED3	0x00000800
TRACE_ARW	0x00001000
TRACE_ARW_BLOCK_OPERATION	0x00002000
TRACE_ARW_RESERVED1	0x00004000
TRACE_ARW_RESERVED2	0x00008000
TRACE_PATH_CLASSIFY	0x00010000
Маски логируемых подсистем для USB-драйвера	
TRACE_BASE	0x00000001
TRACE_PNP	0x00000002
TRACE_AGENT_INTERACTION	0x00000004

Примеры написания команды:

1) Трассировка всех подсистем службы с уровнем логирования Verbose:

```
trace -start –svc
```

2) Трассировка подсистем службы: TRACE_SESSION_MONITOR и TRACE_WMI_MONITOR, с уровнем логирования Warning:

```
trace -start -svc 0x8040 0x3
```

3) Остановка трассировки службы:

```
trace -stop -svc
```

4) Трассировка всех подсистем драйвера с уровнем логирования Verbose:

```
trace -start -drv
```

5) Трассировка подсистем драйвера TRACE_REGISTRY_MONITOR, TRACE_REGISTRY_MATCHER, TRACE_REGISTRY_CONFIG_PARSER с уровнем логирования Error:

```
trace -start -drv 0x7 0x2
```

6) Остановка трассировки драйвера:

```
trace -stop -drv
```

Команда **memdump** – сохраняет снимок памяти указанного процесса в файл. Файл сохраняется в директорию dumps (в ProgramData\<директория агента>). Команда выполняется согласно синтаксису: memdump {[-id] <UUID процесса> | <PID>}.

Пример написания команды:

memdump 2260

memdump -id 2260

memdump {0F573999-EAA5-4529-9AE8-509EEA3DAC73}

memdump -id {0F573999-EAA5-4529-9AE8-509EEA3DAC73}

В результате выполнения команды в директории **C:\ProgramData\PT-Информационная безопасность\Агент RT Protect EDR\dumps** будет создан файл с дампом процесса.

Команда **memscan** – сканирует память указанного процесса на наличие вредоносного кода. Команда выполняется согласно синтаксису: memscan {[-id] <UUID процесса> | <PID>}, где

pid – это идентификатор процесса (вместо PID процесса можно указать его уникальный идентификатор в RT Protect EDR).

Пример написания команды:

memscan 1080

memscan -id 1080

memscan {0F573999-EAA5-4529-9AE8-509EEA3DAC73}

memscan -id {0F573999-EAA5-4529-9AE8-509EEA3DAC73}

Команда **netlimit** – ограничивает максимальную скорость отправки событий. Команда выполняется согласно синтаксису: netlimit [<Макс. скорость>], где:

<Макс. скорость> – Максимальная скорость отправки (Кбит\с), (значение 0: без ограничений скорости).

Пример написания команды:

1) Вывод текущего ограничения максимальной скорости отправки:

netlimit

2) Установка ограничения максимальной скорости отправки 5 Кбит\с:

netlimit 5

3) Снятие ограничения на максимальную скорость:

netlimit 0

Команда **reset-errors** – сбрасывает счетчики прикладных и системных ошибок на агенте, команда выполняется согласно синтаксису reset-errors [all | app | sys], где:

all – сброс всех счетчиков ошибок (выполняется по умолчанию);

app – сброс счетчика прикладных ошибок;

sys – сброс счетчика системных ошибок.

Примеры выполнения команд:

Сброс счетчиков системных и прикладных ошибок:

```
reset-errors
```

Сброс счетчика прикладных ошибок:

```
reset-errors app
```

Сброс счетчика системных ошибок:

```
reset-errors sys
```

Команда **get-log** – загружает логи агента в файловое хранилище, команда выполняется согласно синтаксису get-log <Наименование лога>, где наименование лога агента принимает следующие значения:

driver – лог драйвера;

usb – лог usb-драйвера;

service – лог службы.

Команда **remed** - Ремедиация файлов и ключей реестра.



Важно

Следует обратить внимание, что ремедиация не работает для файловой системы FAT32.

Команда выполняется согласно синтаксису:

remed <Действие> -hid <ID группы процессов> <-range <Начало/Конец>> <-files и\или -registry> или [<Максимальный возраст файлов>] Действие clean - очистить хранилище, restore - ремедиация файлов\реестра

где:

1) Параметры действия restore:

– hid – ID группы процессов;

– range – временной диапазон ремедиации;

Например: 2026-02-11T10:00:00/2026-02-11T18:00:00 или

2026-02-20T14:08:29.699050200Z/2026-02-20T25:08:10.699050200Z

— files – ремедиация файлов (По умолчанию: выключен);

— registry – ремедиация ключей\значений реестра (По умолчанию: выключен).

2) Параметры действия clean:

Максимальный возраст файлов.

Допустимые суффиксы:

— d - дни,

— h - часы,

— m - минуты, (по умолчанию используется значение из профиля Антишифра);

— all - Удалить все файлы.

Примеры выполнения команд:

1) Ремедиация файлов группы процессов HID={FD547C1E-4260-40DA-9DB9-6D4A22F4FEE4} за временной диапазон от 2026-02-11T10:00:00 до 2026-02-11T18:00:00 (локальное время агента):

```
remed restore -hid {FD547C1E-4260-40DA-9DB9-6D4A22F4FEE4} -range 2026-02-11T10:00:00/2026-02-11T18:00:00 –files
```

2) Ремедиация файлов и реестра группы процессов HID={FD547C1E-4260-40DA-9DB9-6D4A22F4FEE4} за временной диапазон от 2026-02-20T14:08:29.699050200Z до 2026-02-20T25:08:10.699050200Z (UTC время):

```
remed restore -hid {FD547C1E-4260-40DA-9DB9-6D4A22F4FEE4} -range 2026-02-20T14:08:29.699050200Z/2026-02-20T25:08:10.699050200Z -files -registry
```

3) Удаляет зарезервированные файлы старше 10 часов:

```
remed clean 10h
```

4) Удаляет все зарезервированные файлы.

Информация в области «Выбор агента»

В области **Выбор агента** пользователю доступна следующая информация об агенте:

1) Имя компьютера;
2) Версия ОС;
3) Время загрузки системы;
4) Процессор;
5) Оперативная память;
6) Сетевые адреса.

Имя компьютера – в поле отображается имя компьютера, на котором установлен агент.

Версия ОС – в поле отображается название ОС, установленной на компьютере, на котором работает агент.

Время загрузки системы – в поле отображается информация о дате и времени последней загрузки операционной системы, под управлением которой действует агент.

Процессор – в поле отображается наименование и тактовая частота процессора компьютера, на котором установлен агент.

Оперативная память – в поле отображается объем оперативной памяти компьютера, на котором установлен агент. Объем указан в мегабайтах.

Сетевые адреса – в поле отображаются ip-адреса, назначенные для всех сетевых интерфейсов компьютера, на котором установлен агент.

В нижней части области **Выбор агента** отображается состояние агента – Активен / Не активен.

8.5.7. Планировщик задач

Общие сведения

Планировщик задач – это инструмент, позволяющий управлять со стороны сервера следующими сущностями:

– Задача;

– Сценарий;

– Запуск;

— Сценарии реагирования.

Задача – это именованная сущность, объединяющая в себе сценарий, список агентов, к которым необходимо применить этот сценарий, а также атрибуты планирования – разовая в определенное время, немедленно или по запросу (on-demand), периодическая с заданным периодом выполнения и др.

Задача имеет опцию разнесения во времени (распределения на агентах во времени), чтобы избежать одновременной пиковой нагрузки на агентскую сеть.

Сценарий – это именованный список действий (actions).

В сценарии можно задавать как встроенные команды агента, например, GET, так и команды, характерные для командных интерпретаторов ОС Windows (Powershell, CMD) либо Linux (BASH, SH).

Также в сценарии можно задать определенные сценарии реагирования, которые заранее описаны разработчиком.

Применение планировщика задач дает ряд преимуществ, описанных в списке ниже:

1) Планировщик позволяет отслеживать прогресс команд, отправляемых агентам.
2) Планировщик позволяет создавать задания, которые не являются командами терминала – сетевая изоляция, выборка из базы событий и др.
3) Планировщик позволяет создавать пакетные задания, т.е. объединять несколько действий в одну сущность.
4) Планировщик позволяет настроить расписание задач и обеспечить периодическое их исполнение например, периодическое сканирование памяти процессов или каталогов диска, тем самым происходит автоматизация определенных процессов в SOC.
5) Цепочки автоматического реагирования на угрозы можно описывать в терминах задач планировщика, исполняемых по запросу (on-demand).

Описание интерфейса страниц

Общий вид страницы **Планировщик задач** зависит от выбранной вкладки, находящейся в верхней части страницы.

Выбранная вкладка подсвечивается серым цветом.

Имеются следующие вкладки:

– Сценарии;

– Задачи;

– Запуски;

Сценарии

Сценарии – это именованные списки действий которые выполняются в заданном пользователем порядке. Информация на странице **Сценарии** представлена в виде таблицы со следующими полями:

– иконка >, предназначенная для раскрытия подробностей по сценарию;

– кнопка выбора всех сценариев либо одного сценария;

– **Название** (отображается название сценария);

– **Дата создания/Автор** (отображается имя пользователя, создавшего сценарий, и дата создания сценария);

– **Последнее изменение/Пользователь** (отображается время последнего изменения сценария и пользователь, изменивший сценарий);

– **Управление** (отображаются иконки для управления сценарием).

Для фильтрации информации на странице **Планировщик задач/Сценарии** предусмотрена следующая система фильтров:

– **Показывать по** (указывается количество строчек в таблице). Имеется возможность выбрать из следующих параметров: 10, 20, 50, 100, 500;

– **Название** (указывается название сценария);

– Описание;

– **Создатель** (указывается имя пользователя, создавшего сценарий;

– Время создания (указывается время создания сценария).

Рядом с фильтрами **Название** и **Описание имеется** иконка  , при нажатии по которой ЛКМ, всплывает окно с подсказкой, представленное на рисунке 53.

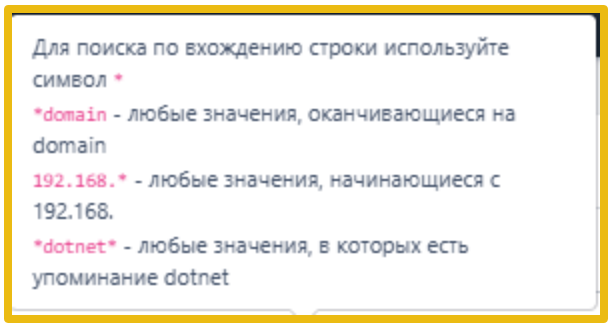


Рисунок 53 – Всплывающая подсказка по заполнению полей фильтрации

Для сброса элементов фильтрации в верхней части страницы предусмотрена иконка Сбросить фильтры .

На странице **Планировщик задач/Сценарии** имеется возможность выполнить следующие действия:

– добавить сценарий;

– включить выбранные сценарии (иконка);

– выключить выбранные сценарии ( );

– удалить выбранные сценарии;

– управлять сценариями реагирования.

– импортировать, экспортировать выбранные сценарии.

Для того, чтобы добавить новый сценарий, требуется нажать по иконке Добавить сценарий , после чего откроется окно, представленное на рисунке 54.

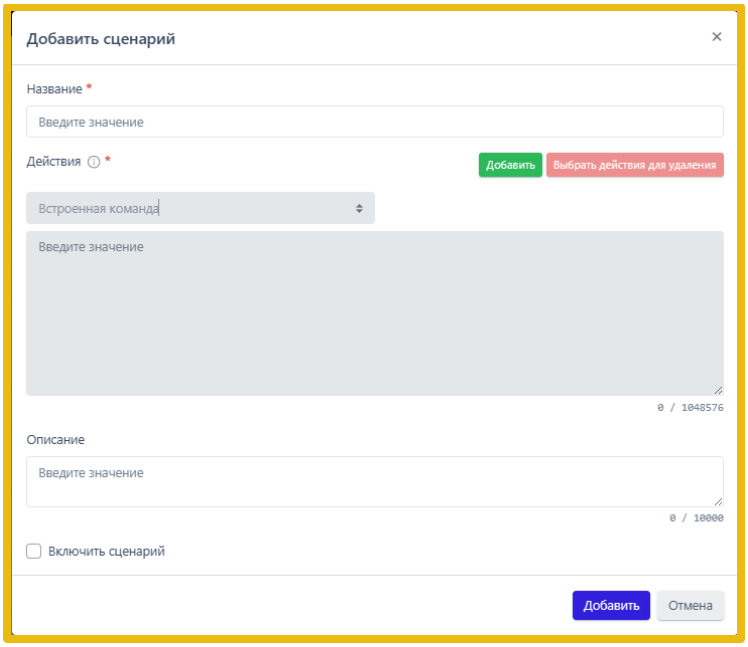


Рисунок 54 – Добавление нового сценария

В данном окне для создания сценария требуется выполнить следующие действия:

– указать название сценария;

– нажав по кнопке **Добавить** (в верхней части окна), добавить количество действий;

– для каждого действия выбрать наименование интерпретатора либо указатель встроенной команды агента;

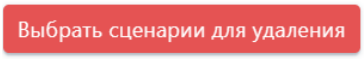
– написать команду;

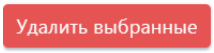
– добавить описание;

– отметить признак **Включить сценарий** (чтобы сценарий стал активным);

– нажать по иконке **Добавить**.

После выполнения перечисленных действий сценарий появится в списке сценариев.

Для удаления действия в сценарии нажать по иконке 

, после чего нажать ЛКМ по номеру сценария, который необходимо удалить (он выделится красным цветом), и нажать по иконке 

.

В поле **Управление** на странице **Планировщик задач/Сценарии** возможно с помощью иконок произвести следующие действия со сценариями:

– включить/выключить сценарий ();

– редактировать сценарий ();

– удалить сценарий ();

– закрепить сценарий за сценарием реагирования () (в этом случае действие в сценарии реагирования будет заменено на действие, выполняемое в закрепляемом сценарии).

При выполнении действий по удалению сценария либо по включению/выключению сценария появится окно подтверждения, в котором следует подтвердить действие, нажав по иконке **Подтвердить**.

При выключении сценария задача, в которой указан данный сценарий, выполняться не будет.

После выполнения действий по редактированию сценария следует нажать по иконке **Сохранить**.

Чтобы экспортировать выбранные сценарии, нажмите кнопку  . Для импорта нажмите кнопку  .

Сценарий

При нажатии по названию сценария ЛКМ открывается страница сценария, представленная на рисунке 55.

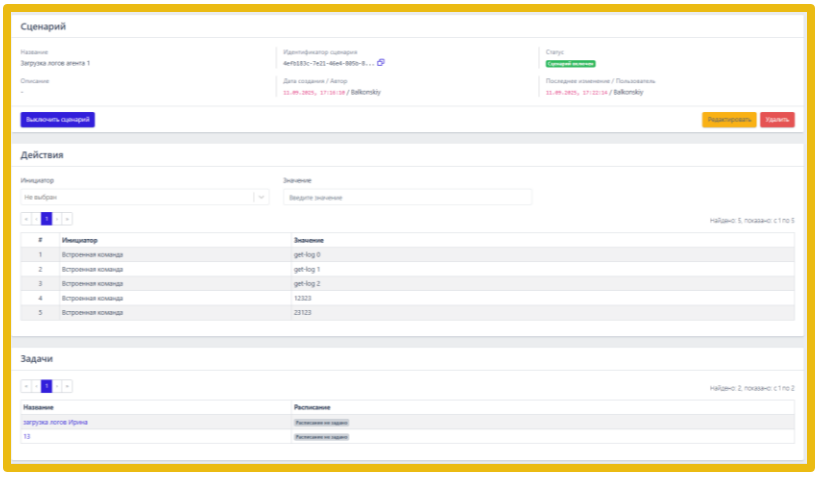


Рисунок 55 – Страница выбранного сценария

На данной странице во вкладке **Сценарий** можно просмотреть информацию о сценарии, включить сценарий, редактировать сценарий, удалить сценарий.

Во вкладке **Действия** можно просмотреть действия, которые будут выполняться в данном сценарии.

Во вкладке **Задачи** можно просмотреть задачи, у которых применяется данный сценарий.

При нажатии ЛКМ по названию задачи происходит переход на страницу данной задачи.

Задачи

Общий вид страницы **Задачи** представлен на рисунке 56.

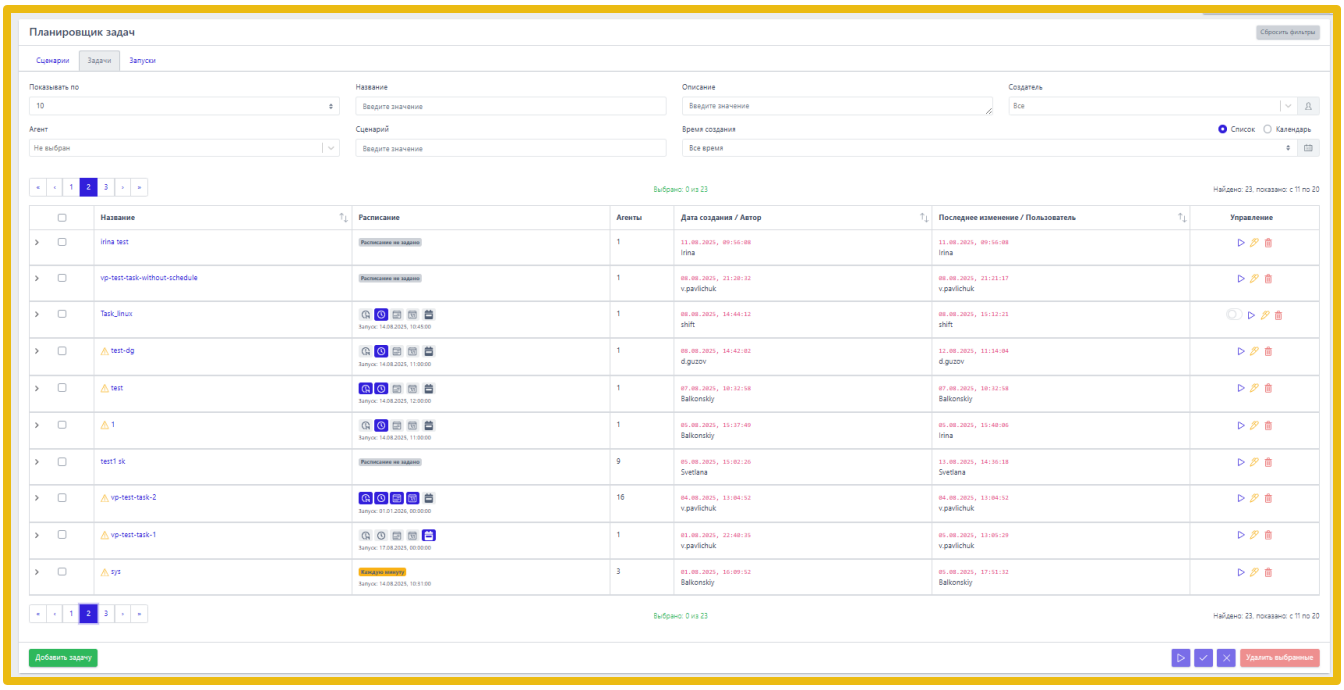


Рисунок 56 – Планировщик задач раздел Задачи

Информация на данной странице представлена в виде таблицы со следующими полями:

– иконка > для раскрытия дополнительной информации;

– кнопка выбора всех задач либо одной задачи;

– Название задачи;

– **Расписание** (в виде иконок указываются параметры созданного расписания для задачи);

– **Агенты** (указывается количество агентов, к которым привязана задача);

– **Время создания** (указывается время создания задачи);

– **Дата создания/Автор** (отображается имя пользователя, создавшего задачу и дата создания задачи);

– **Последнее изменение/Пользователь** (отображается время последнего изменения задачи и пользователь, изменивший задачу);

– **Управление** (иконки по включению/выключению, иконка запуска задачи, редактированию и удалению задачи).

Для фильтрации на странице предусмотрена следующая система фильтров:

– **Показывать по** (указывается, сколько строк отображается в таблице;

– **Название** (указывается название задачи);

– Описание;

– **Создатель** (указывается имя пользователя, создавшего задачу);

– **Агент** (указывается имя агента, которому назначена задача);

– Сценарий;

– Время создания.

На странице **Планировщик задач/Задачи** имеется возможность выполнить следующие действия:

– добавить задачу;

– запустить задачу (иконка  в области Управление при нажатии по иконке );

– запустить задачу с дополнительными параметрами (иконка  в области **Управление** при нажатии по иконке );

– включить выбранные задачи (иконка );

– запустить выполнение задачи ();

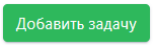
– запустить выбранные задачи ();

– выключить выбранные задачи ();

– редактировать задачу ();

– удалить задачу ();

– удалить выбранные задачи.

Для добавления задачи требуется нажать по иконке 

, после чего откроется окно, представленное на рисунке 57.

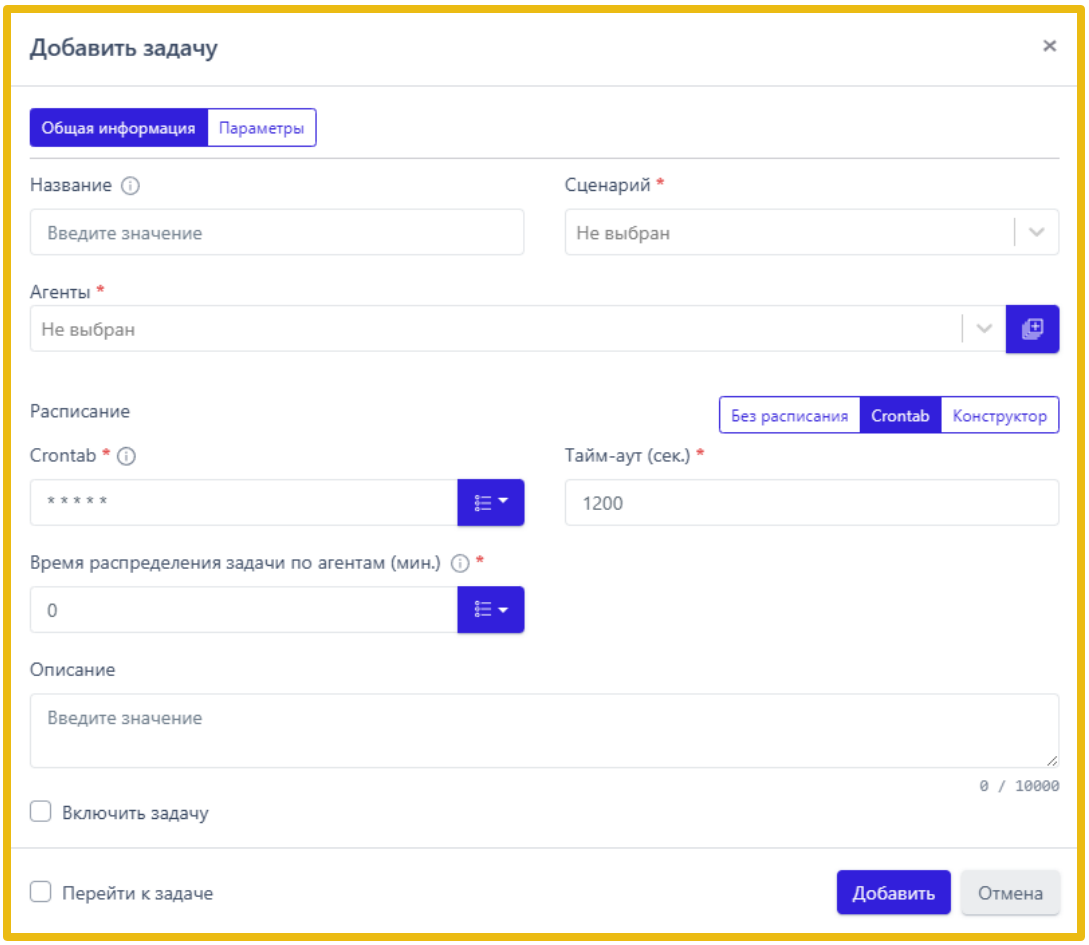


Рисунок 57 – Окно добавления задачи

Для добавления задачи в данном окне требуется выполнить следующие действия:

– добавить название задачи в поле **Название**;

– добавить агентов, на которых будет выполнена данная задача;

– добавить сценарий для задачи;

– добавить расписание выполнения задачи (подробнее о написании расписания смотри ниже);

– добавить таймаут в секундах;

– добавить время распределения задач по агентской сети;

– добавить описание к задаче;

– добавить признак включения задачи;

– нажать по иконке **Добавить**.

Добавление агентов, на которых будет выполнена задача можно произвести двумя способами:

– с помощью иконки открывающей список агентов,

– с помощью иконки  , открывающей список в котором можно указать идентификаторы агентов.

После выполнения действий, описанных выше, задача появится в списке задач.

Следует обратить внимание, что задача может быть создана и без расписания (для этого необходимо при создании задачи следует нажать ЛКМ по иконке 

).

Расписание для выполнения задачи возможно добавить двумя способами:

1) С помощью планировщика Cron, для которого также есть **Шаблоны расписания**.
2) Например, при выборе шаблона **Каждые 30 минут** в формате Cron, расписание будет иметь вид

```
*/30 * * * *
```

.

3) С помощью конструктора расписания, который отображается во вкладке **Конструктор**.

При добавлении задачи возможно указать параметры во вкладке **Параметры** (рис. 58).

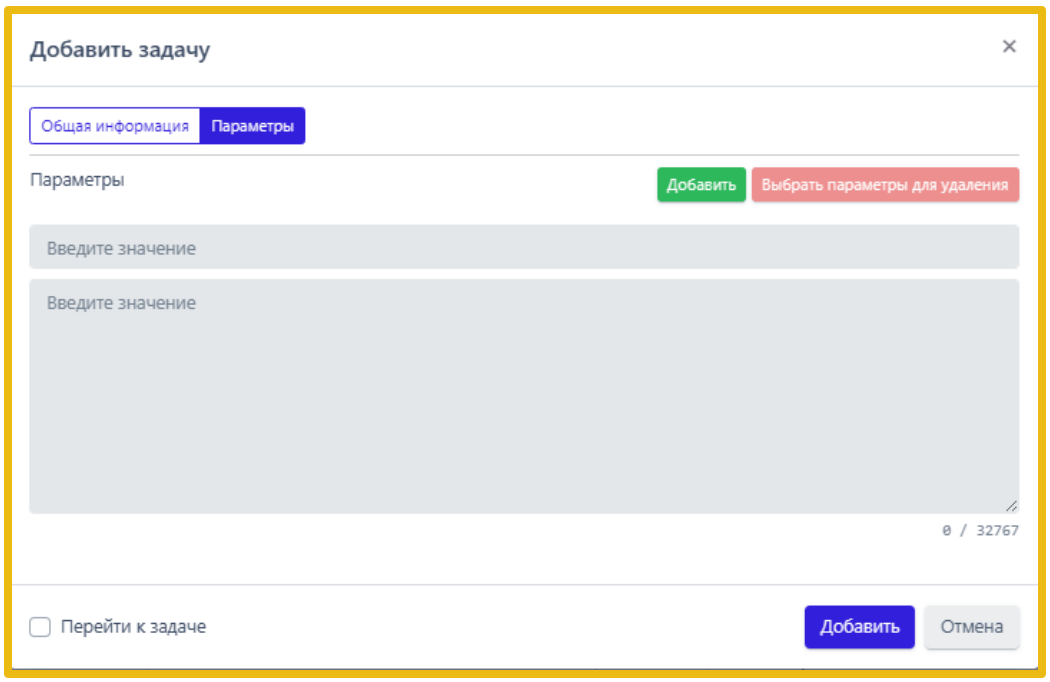


Рисунок 58 – Добавление параметров при создании задачи

При создании задачи для более чем 10 агентов следует указать время распределения задач по агентской сети в минутах.

Данная настройка необходима для исключения возможных проблем с выполнением задачи на большом количестве агентов.

В поле **Управление** страницы **Планировщик задач/Задачи** возможно с помощью иконок произвести следующие действия с задачами:

– включить/выключить задачу (/) – функционал поддерживается для задач по расписанию;

– редактировать задачу ( );

– запустить задачу ( );

– удалить задачу ( ).

При выполнении действий по удалению задачи либо по включению/выключению задачи появится окно подтверждения, в котором следует подтвердить действие, нажав по иконке **Подтвердить**.

При выключении задача выполняться не будет.

После выполнения действий по редактированию задачи следует нажать по иконке **Сохранить**.

Задача

При нажатии ЛКМ на странице **Планировщик задач** вкладка **Задачи** по имени конкретной задачи, открывается окно, представленное на рисунке 59.

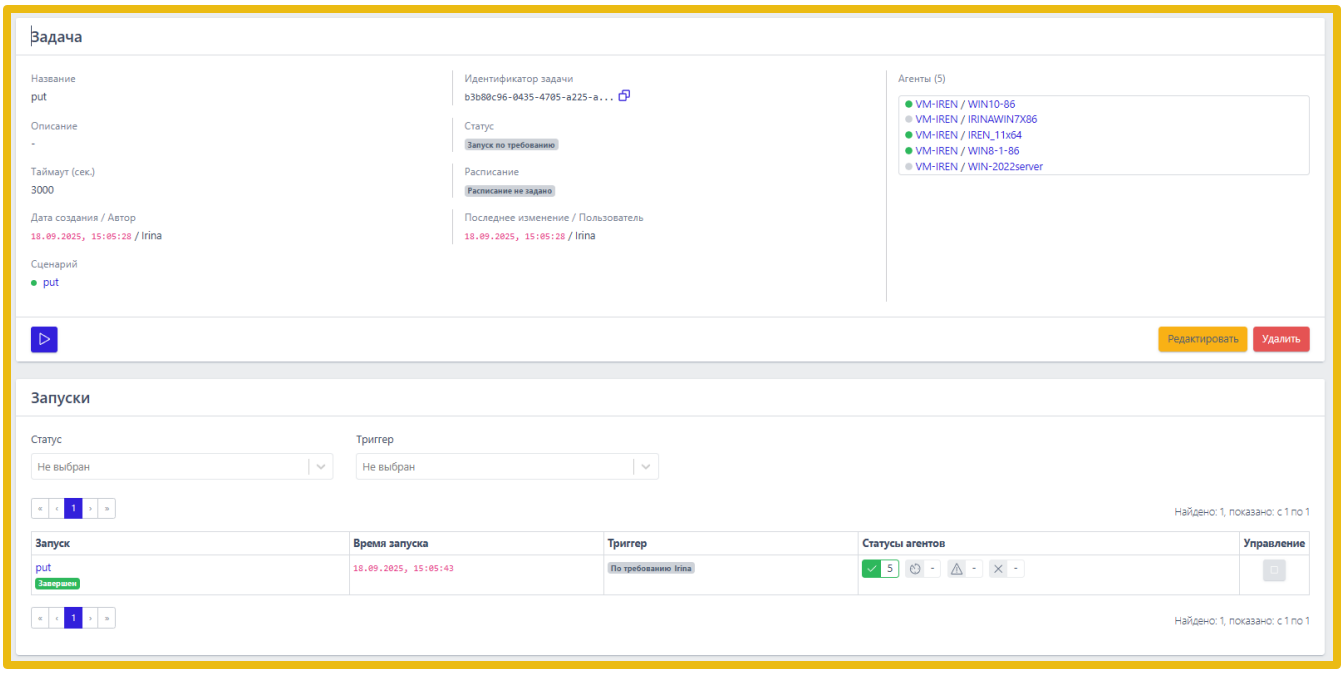


Рисунок 59 – Страница Задача

На странице **Задача** администратор может просмотреть информацию о задаче, включить/выключить задачу (для задач по расписанию), запустить задачу, редактировать задачу, удалить задачу.

На странице **Задача** администратор может просмотреть информацию по запускам данной задачи, а также завершить выполнение запуска с помощью иконки в поле **Управление**.

Запуски

Общий вид страницы **Планировщик задач/Запуски** представлен на рисунке 60.

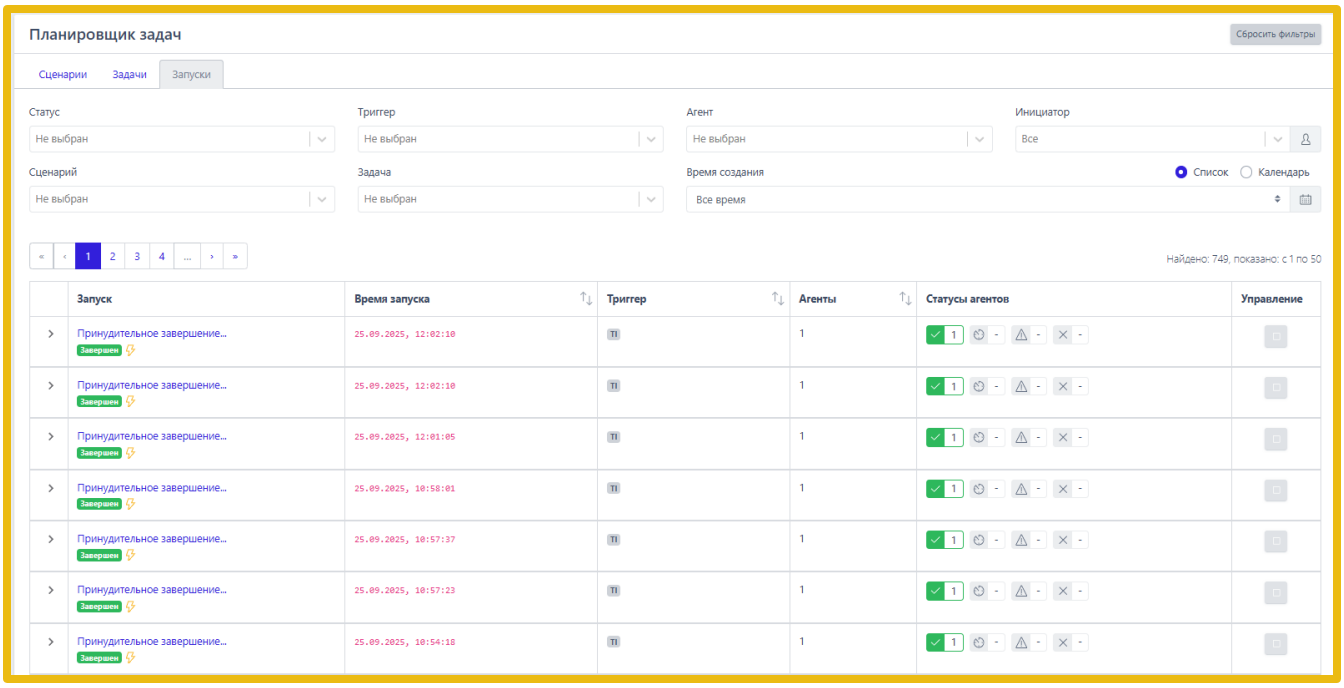


Рисунок 60 – Планировщик задач раздел Запуски

Информация на странице представлена в виде таблицы со следующими полями:

– иконка для раскрытия информации о запуске;

– Время запуска;

– **Триггер** (по требованию, TI, по расписанию, по событию, по инциденту);

– Агенты;

– **Статусы агентов** (показываются статусы выполнения запусков задач на агентах). Возможны следующие варианты: **Создан**, **Подтвержден**, **В процессе**, **Принудительно остановлен**, **Ошибка**, **Завершен**;

– **Управление** (кнопка остановки запуска задачи –).

На странице **Запуски** в поле **Запуск** может присутствовать иконка , которая указывает на то, что происходил единоразовый запуск, то есть запуск задачи, не привязанной к расписанию.

Для фильтрации информации на странице, предусмотрена система фильтров, представленная согласно следующему списку:

– Статусы;

– Триггеры;

– Агент;

– Инициатор;

– Сценарий;

– Задача;

– Время создания;

– Действия.

При нажатии по иконке > открывается окно с информацией по запуску задачи (рисунок 61).

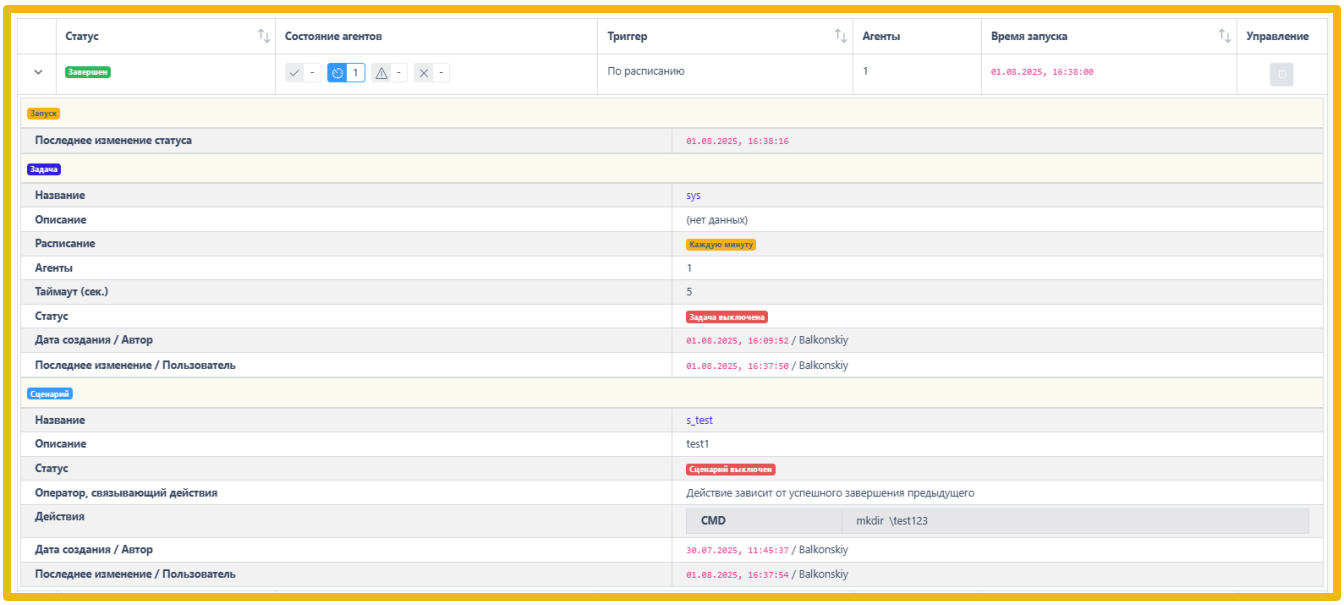


Рисунок 61 – Информация о запуске

При нажатии по имени запуска открывается страница конкретного запуска, представленная на рисунке 62.

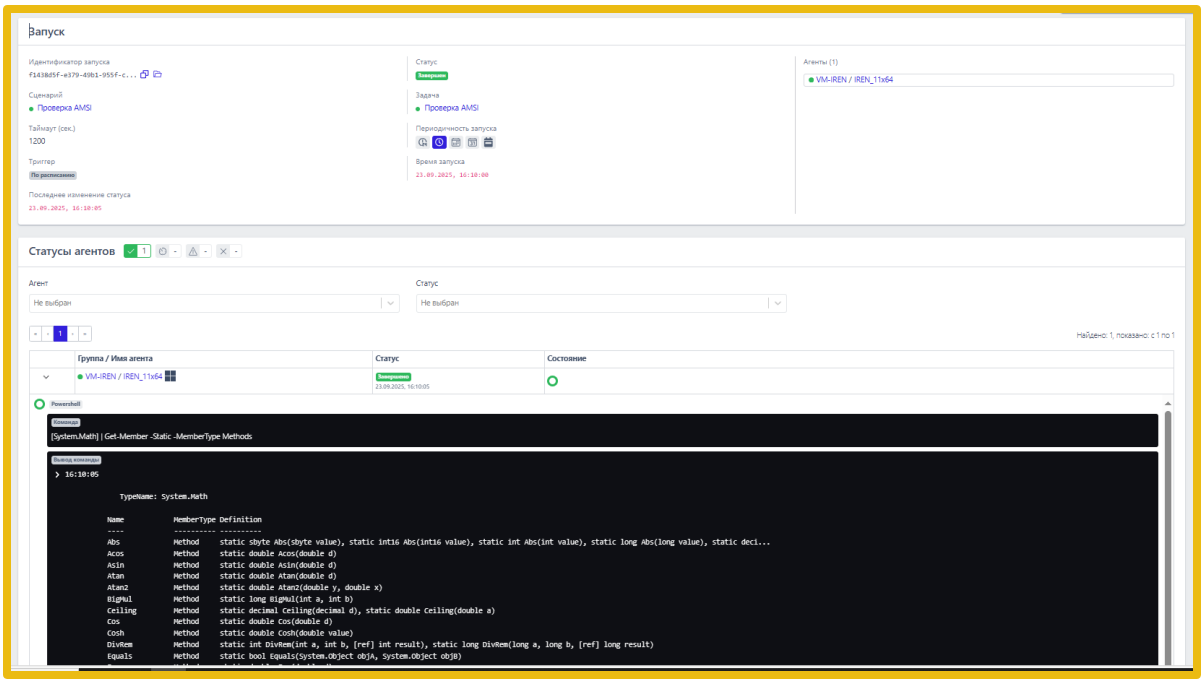


Рисунок 62 – Страница выбранного запуска

На данной странице в области **Запуск** можно просмотреть информацию о запуске с определенным идентификатором, а также в поле **Состояние** можно просмотреть состояние запусков отдельных действий в задаче данного запуска. Для запусков задач с триггером по инциденту отображаются событие, послужившее источником инцидента, а также информация об инциденте. Для запусков задач по вердикту TI отображаются параметры запуска задачи и информация о событии, в котором участвует анализируемый TI-платформой артефакт.

Сценарии реагирования

Общий список со сценариями реагирования представлен на рисунке 63.



Рисунок 63 – Сценарии реагирования

На странице представлен список предустановленных сценариев реагирования. Подробная информация о сценариях реагирования представлена в документе «Руководство аналитика RT Protect EDR».

8.5.8. Графики

На странице **Графики** пользователь может изучить информацию о работе агентов в графическом виде, а также настроить параметры отображения графиков.

По умолчанию в разделе **Графики** не содержится графических изображений.

Для добавления графика в область отображения, расположенную ниже области ДОБАВИТЬ ГРАФИК, необходимо в поле **Агент** выбрать из выпадающего списка агента, для которого будет нарисован график. Далее в поле **Выбор метрики** следует указать параметр, вывод которого нужно осуществить в графическом виде. При необходимости вывода в поле выбора **Агент** только активных в данный момент агентов следует установить флаг **Только активные**.

Далее в поле **Выбор интервала** необходимо установить период, за время которого будет отображаться график. Доступны для выбора следующие интервалы: **15 минут**, **1 час**, **8 часов**, **1 день**, **1 неделя**, **1 месяц** и **3 месяца**.

После выбора временного интервала в поле **Ширина графиков** необходимо выбрать масштаб отображения, установив флажок в кнопке выбора **50%** или **100%**. После установки всех параметров следует нажать кнопку **Добавить график**, после чего выбранный график будет добавлен в область отображения.

Область отображения графика включает в себя:

1) Сам график;
2) Поле **Агент**, в котором отображается имя агента, являющееся одновременно ссылкой для перехода к странице **Агент**;
3) Поле активности, в котором показывается, активен или не активен агент в данный момент – Не активен / Активен ;
4) Поле **Выбор агента** (при выборе нового агента в графике отобразится информация об этом агенте);
5) Поле **Выбор метрики** (при выборе новой метрики в графике отобразится информация, соответствующая этой метрике);
6) Поле **Выбора интервала** (при выборе нового интервала в графике будет отображаться информация, заданная этим интервалом времени, интервал можно выбрать в виде списка или в виде произвольного интервала, заданного в календаре).

Для удаления графика из области отображения необходимо нажать кнопку **Закрыть график** ( ) в правой верхней части области отображения графика. Для удаления всех графиков в области отображения следует нажать кнопку Удалить все графики в верхней правой части страницы.

В области график имеется возможность, указав временной интервал, перейти на страницу **Активность**, при этом будет выполнена выборка только событий для агента, зарегистрированных на сервере в интервале времени, указанном на графике (рисунок 64).

Для перехода на страницу **Активность** с событиями согласно временному интервалу из области графика, следует выполнить следующие действия:

1) Создать график, выбрав агента, интервал и метрику;
2) Нажать ЛКМ и, выделив серым тоном интервал, отпустить кнопку мыши;
3) Для перехода на страницу **Активность** с событиями, зарегистрированными на сервере согласно выбранному интервалу, необходимо нажать по иконке .

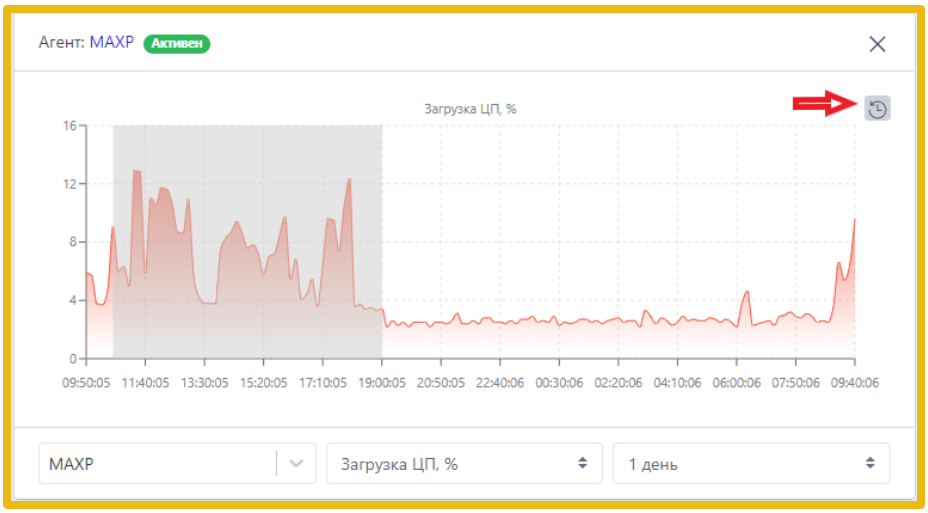


Рисунок 64 – Указание временного интервала для выборки событий из интервала на графике

8.5.9. Хранилище

Общая информация

На странице **Хранилище** отображаются все файлы, загруженные в файловое хранилище Программы (рис. 65). Администратор может как просматривать файлы, загруженные пользователями EDR с машин, на которых установлены агенты, так и загружать файлы с компьютера, на котором он выполнил вход на сервер управления.

Файлы могут загружаться пользователями для проведения анализа с помощью TI-платформы или с помощью инструмента **Просмотр файлов**.

Для переключения между таблицей с файлами, полученными от агентов, и таблицей с загруженными пользователями файлами в верхней части окна предусмотрены вкладки **Файлы с агентов** и **Загрузка файлов**.

Файлы с агентов

Общий вид страницы **Хранилище** вкладка **Файлы с агентов** представлен на рисунке 65.

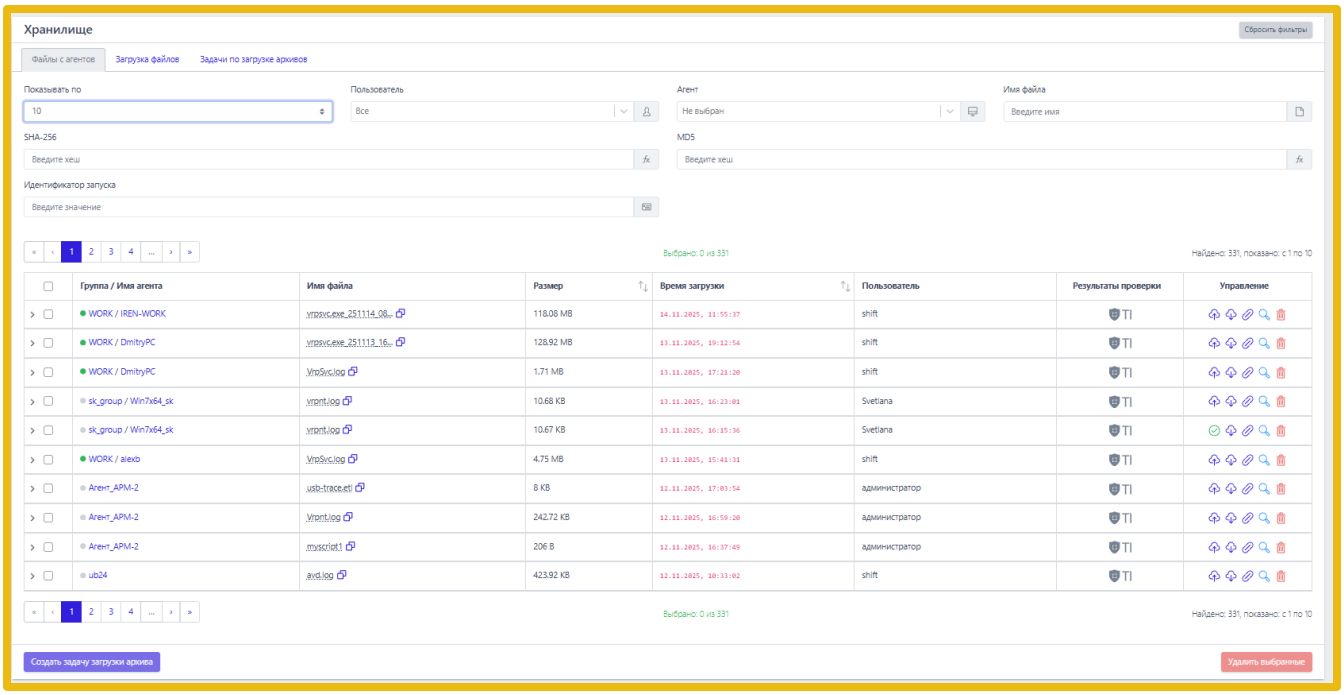


Рисунок 65 – Страница «Хранилище» вкладка «Файлы с агентов»

Информация о файлах, полученных от агента, представлена в табличном виде.

В верхней части страницы находятся следующие фильтры поиска:

1) Показывать по (устанавливает количество элементов на странице);
2) Пользователь;
3) Агент;
4) Имя файла;
5) SHA-256;
6) MD5;
7) Идентификатор запуска.

Идентификатор запуска можно увидеть на странице **Запуск** для задачи сохранения файла в хранилище.

Шапка таблицы **Файлы с агентов** состоит из следующих полей:

1) Кнопка выбора ( );
2) Группа/Имя агента;
3) Имя файла;
4) Размер;

5) Время загрузки;

6) Пользователь;

7) Результаты проверки;

8) Управление.

Группа/Имя агента – в поле указываются имя агента, с которого был загружен файл, и группа, в которую входит агент. Активные в данный момент агенты помечаются значком . В некоторых случаях, при загрузке в **Хранилище** большого файла в поле будет отображаться запись о загрузке файла вида Файл загружается... .

Для перехода к странице **Агент** необходимо нажать ЛКМ на названии агента в столбце **Группа/Имя агента**.

Для перехода к странице **Группа** следует нажать ЛКМ на названии группы агентов в столбце **Группа/Имя агента**.

Имя файла – поле содержит относительное имя файла, загруженного с агента. Для отображения полного имени файла необходимо навести курсор на значение относительного имени.

Размер – поле содержит размер файла, загруженного с агента. Размер указывается в единицах кратных байту (байтах, килобайтах и т.д.).

Время загрузки – в поле отображается время в формате UTC, в которое файл был загружен с агента на сервер.

Пользователь – в поле отображается имя пользователя, загрузившего файл.

Результаты проверки – в поле отображается кнопка отчета TI-платформы по загруженному файлу (подробная информация об отчётах платформы содержится в пункте 8.4.3). Кнопка со значком TI обозначает безопасный файл, кнопка со значком TI обозначает вредоносный файл, кнопка со значком TI обозначает подозрительный файл, кнопка со значком TI обозначает проверку файла на TI-платформе в текущий момент времени.

В случае загрузки файла, информация по которому отсутствует на TI-платформе, кнопка отчета файла отображается со значком TI. Для получения данных необходимо нажать кнопку **Перейти к отчету**.

При нажатии ЛКМ на кнопки в столбце **Результаты проверки** пользователь сможет увидеть краткий отчет о состоянии загруженного в **Хранилище** файла.

Управление – в поле отображаются кнопки операций, выполняемых с загруженным файлом.

Пользователю доступны следующие операции:

– Загрузить файл на TI-платформу ;

– Скачать файл ;

– Просмотреть файл ,

– Удалить файл ,

– Получить ссылку на скачивание .

Кнопка **Просмотреть файл** открывает окно **Просмотр файла**. Кнопка **Удалить файл** удаляет загруженный файл с сервера.

Чтобы открыть дополнительную информацию о загруженном файле, необходимо нажать ЛКМ на значок › рядом с кнопкой выбора в левой части таблицы. Снизу строки появится дополнительная таблица, в которой кроме полей **Время загрузки**, **Размер** и **Пользователь**, представленных в основной таблице, добавлены поля **Имя**, **MD5** и **SHA-256**.

Имя – поле содержит полное, абсолютное имя файла.

MD5 – поле содержит значение хеша для алгоритма md5.

SHA-256 – поле содержит значение хеша для алгоритма sha-256.

Снизу таблицы находятся кнопки Создать задачу загрузки архива и Удалить выбранные .

Для удаления одного или нескольких файлов необходимо отметить флажками соответствующие кнопки выбора для удаляемых файлов и нажать кнопку **Удалить выбранные**.

Для создания задачи по загрузке архива требуется сначала выделить кнопкой выбора из списка необходимые файлы и далее нажать по иконке, и в окне подтверждения действия вписать имя файла архива. После чего задача по загрузке архива будет отображаться во вкладке **Задачи по загрузке архивов**.

Загрузка файлов

Общий вид страницы **Хранилище** вкладки **Загрузка файлов** представлен на рисунке 66.

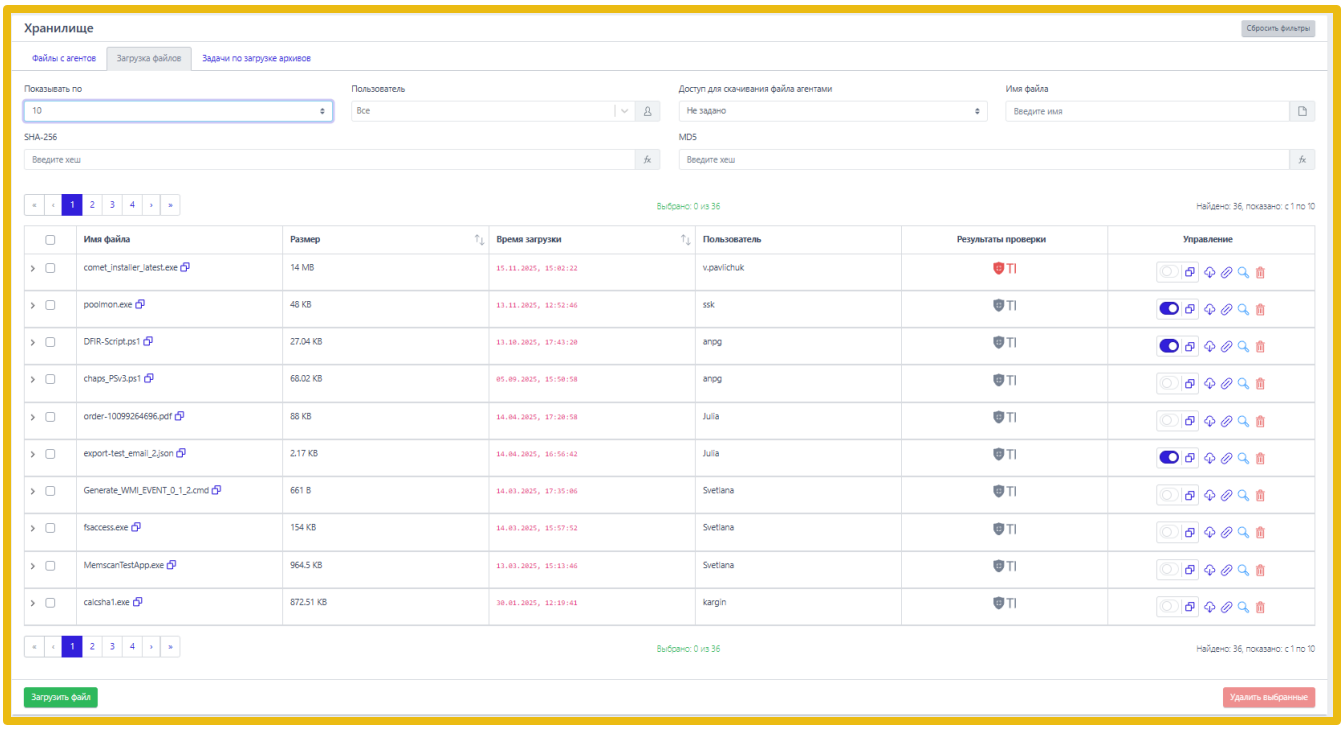


Рисунок 66 – Общий вид страницы «Хранилище» вкладка «Загрузка файлов»

В верхней части страницы **Хранилище** вкладки **Загрузка файлов** находятся следующие фильтры поиска:

1) Показывать по (устанавливает количество элементов на странице);
2) Пользователь;
3) Доступ для скачивания файла агентами (разрешен/запрещен);
4) Имя файла;
5) SHA-256;
6) MD5.

Шапка таблицы **Загрузка файлов** состоит из следующих полей:

– Кнопка выбора;

– Имя файла;

– Размер;

– Время загрузки;

– Пользователь;

– Результаты проверки;

– Управление.

В поле **Управление** можно выполнить следующие действия:

– запретить/разрешить скачивание файла агентами (/), разрешив скачивание мы создадим постоянную ссылку на скачивание файла, которую далее скопировать для дальнейшей работы с ней с помощью кнопки **Скопировать ссылку на файл** ( );

– скачать файл ( );

– получить ссылку на скачивание ( );

– просмотреть файл ( );

– удалить файл ( ).

Загрузить файл в хранилище с компьютера, с которого осуществлен вход в модуль администрирования, можно, нажав по иконке Загрузить файл .

Задачи по загрузке архивов

На странице представлены созданные задачи по загрузке архивов.

Общий вид страницы **Хранилище** вкладки **Задачи по загрузке архивов** представлен на рисунке 67.

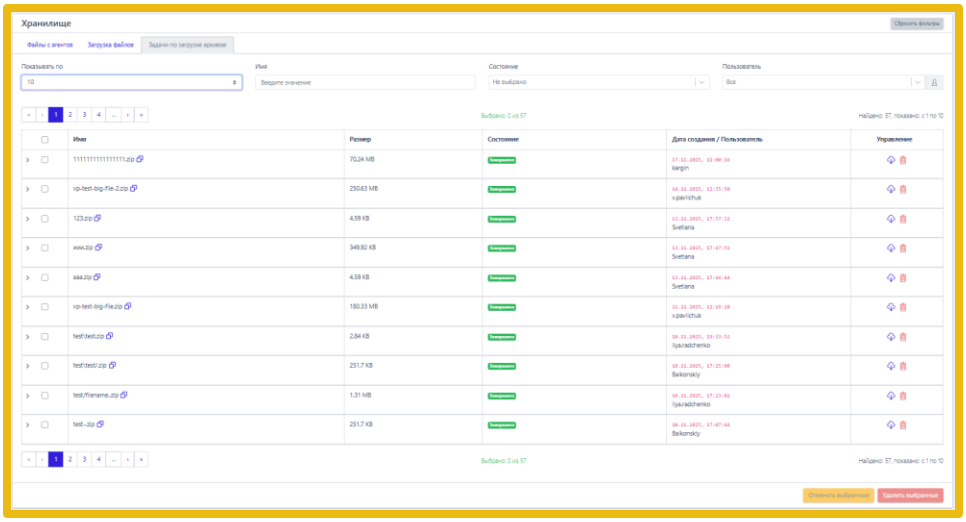


Рисунок 67 – Общий вид страницы «Хранилище» вкладка «Задача по загрузке архивов»

Информация на странице представлена в виде таблицы со следующими полями:

– Кнопка выбора;

– Имя;

– Размер;

– Состояние;

– Дата создания/Пользователь;

– Управление (Скачать архив, удалить архив).

На странице представлены следующие фильтры:

– Показывать по;

– Имя;

– Состояние;

– Пользователь.

В фильтре **Состояние** имеются следующие поля:

– Создано;

– Копирование файлов;

– Архивирование файлов;

– Отменено пользователем;

– Завершено;

– Ошибка;

– Отменено.

Просмотр файла

Функция **Просмотреть файл** используется для побайтового просмотра загруженных в хранилище файлов. Она доступна как во вкладке **Файлы с агентов**, так и на вкладке **Загрузка файлов**. Чтобы открыть окно **Просмотр файла** (рис. 68), необходимо нажать кнопку **Просмотреть файл** ( ) в разделе **Хранилище**.



Рисунок 68 – Просмотр файла

В верхней части окна **Просмотр файла** посередине отображается имя просматриваемого файла `cleanmgr.exe` . В нижней части окна **Просмотр файла** посередине отображается количество загруженных байтов Загружено (байт): 1048576 из 2790032 . В Программе предусмотрена загрузка файлов в объеме не более одного мегабайта информации, это позволяет экономить ресурсы.

Если размер файла превышает один мегабайт, то рядом с количеством загруженных байтов на странице **Просмотр файла** появляется кнопка **Загрузить ещё 1 Мб содержимого файла** (Загружено (байт): 1048576 из 2790032). После нажатия кнопки содержимое окна **Просмотр файла** обновляется (на страницу добавляется еще один мегабайт информации из загруженного файла). При наведении курсора мыши на слово **Загружено** пользователю выводится сообщение о выводе по умолчанию 1 Мб информации (рис. 69).

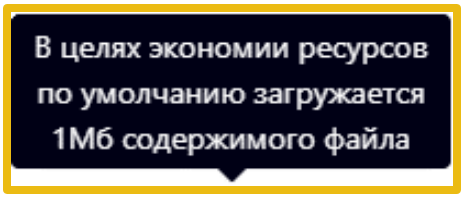


Рисунок 69 – Сообщение в окне «Просмотр файлов»

Для просмотра информации в бинарном формате следует изменить формат отображения в строке **Кодировка** с выбранной кодировки на **Нет (Binary)**.

8.5.10. **Уязвимости**

Уязвимость – это недостаток программы, используя который можно нарушить ее целостность и вызвать неправильную работу программы.

Управление уязвимостями осуществляется в разделе **Уязвимости**. Сканирование уязвимостей осуществляется TI-платформой и позволяет проверить программное обеспечение на конечных точках с установленными агентами и выявить программы, защита которых ослаблена наличием известных и эксплуатируемых уязвимостей.

Сканер способен обнаруживать уязвимости из базы NIST (National Institute of Standarts and Technology), а также из базы данных угроз ФСТЭК (БДУ ФСТЭК).



Примечание

Запрос на сканирование программы на наличие уязвимостей отправляется TI-платформе в случае обнаружения нового ПО.

Для специалиста, работающего с уязвимостями, важны такие понятия, как инциденты модуля уязвимости и критичность агента.

Под инцидентами подразумеваются сущности, возникающие в случае совпадения двух событий: на агенте присутствует программа, в которой есть «трендовая» уязвимость, а также критичность агента имеет значение «Критичная». Трендовые уязвимости определяются аналитиками на TI-платформе, а критичность агента устанавливается аналитиками RT Protect EDR. Критичным может быть агент, установленный на важном хосте: контроллер домена, сервер с важной базой данных и т.д. Трендовая уязвимость в Программе помечается соответствующим значком ( ). Обычно под трендовыми подразумеваются такие уязвимости, которые активно используются злоумышленниками в данный момент времени и поэтому требуют особого внимания к себе со стороны сотрудников информационной безопасности.

Страница **Уязвимости** содержит диаграммы, на которых можно видеть результаты сканирования обнаруженных в защищаемой инфраструктуре программ, количество выявленных уязвимостей с разбивкой по критичности, а также покрытие агентов по наличию на них уязвимостей.

Записи диаграмм Программы и Уязвимости кликабельны и позволяют перейти во вкладку Программы с соответствующей настройкой фильтрации полей.

Информация во вкладке **Инциденты** представлена в таблице, которая содержит следующие поля:

1) Инцидент (содержит название инцидента и CVE-идентификатор уязвимости);
2) Агент (показывает имя критичного агента, на котором содержится программа с трендовой уязвимостью);
3) Статус инцидента (активен, завершен автоматически или завершен вручную);
4) Программное обеспечение (название программы, в которой обнаружена трендовая уязвимость);
5) Время обнаружения;
6) Действия (содержит кнопку **Закрыть инцидент** ⊗).

Инциденты можно искать с помощью фильтров: **Статус**, **Агенты**, **Группы**. Необходимо учитывать, что результаты вывода фильтров **Агенты** и **Группы** пересекаются, то есть при выборе группы, в которой нет ранее выбранного агента, результат, выданный по этому агенту пропадет.

При желании настройки фильтров можно сбросить при помощи кнопки **Сбросить фильтры**.

Клик по имени инцидента приводит к переходу на страницу, содержащую сведения об инциденте, сведения о программе, в которой найдена трендовая уязвимость, и сведения об этой уязвимости. В области **Сведения об инциденте** содержится кнопка **Закрыть инцидент**.

При закрытии инцидента необходимо указывать причину его закрытия, это может быть изменение критичности агента, обновление программы, закрывающее уязвимость или снятие с уязвимости аналитиком TI-платформы статуса трендовой.

Информация во вкладке **Программы** представлена в таблице, которая содержит следующие поля:

1) Имя;
2) Издатель;
3) Версия;
4) Агенты;
5) Уязвимости.

Программы в таблице можно фильтровать с помощью следующих фильтров:

1) Статус;

2) Агенты;

3) Группы;

4) Имя;

5) Издатель;

6) Платформа (Windows или Linux);

7) Критичность;

8) Признак трендовой уязвимости (трендовая или обычная);

9) CVE;

10) Оценка CVSS V2 (не менее) (от 0 до 10);

11) Оценка CVSS V3 (не менее) (от 0 до 10);

12) Оценка CVSS V3.1 (не менее) (от 0 до 10);

13) Оценка CVSS V4 (не менее) (от 0 до 10).

Настройки фильтров сбрасываются с помощью кнопки **Сбросить фильтры**.

Клик по имени программы в таблице вкладки **Программы** приводит к переходу на страницу, содержащую сведения о программе, в том числе об агентах, на которых эта программа присутствует, а также сведения обо всех обнаруженных в программе уязвимостях.

Уязвимости отмечаются значками, показывающими степень критичности (– критичная, – высокая, – средняя, – ниже среднего, – низкая).

Клик по идентификатору CVE-уязвимости в таблице вкладки **Программы** показывает краткую информацию по уязвимости, нажатие кнопки **Перейти к уязвимости** позволяет выполнить переход на страницу, содержащую сведения об уязвимости, в том числе список относящихся к ней CWE и количество программ, в которых уязвимость присутствует.



Примечание

В отличие от CVE, идентификатор CWE указывает не на конкретную уязвимость, а на общую проблему или недочет в программном обеспечении.

Кроме сведений об уязвимости страница содержит критерии соответствия уязвимости, ее описание, рекомендации по устранению.

Во вкладке **Уязвимости** отображены все найденные уязвимости в защищаемой инфраструктуре.

Информация представлена в таблице со следующими полями:

1) CVE;
2) Агенты;
3) Программы;
4) Инциденты;
5) Открытые инциденты;
6) Создана.

Уязвимости можно фильтровать с помощью следующих фильтров:

1) Показывать по;
2) Критичность;
3) Агенты;
4) Группы;
5) Признак трендовой уязвимости;
6) Критичности агентов;
7) CVE;
8) Оценка по CVSS V2 (не менее);
9) Оценка по CVSS V3 (не менее);
10) Оценка по CVSS V3.1 (не менее);
11) Оценка по CVSS V4 (не менее).

Формирование отчетности на странице с уязвимостями

Аналитик может сформировать отчет о найденных на агентах уязвимостях и сохранить этот отчет на компьютер, с которого осуществляется доступ к серверу управления. Отчет формируется на странице **Управление уязвимостями** во вкладке **Программы**.

Чтобы сохранить отчет в формате csv, необходимо нажать кнопку  , после чего отчет будет доступен в папке **Загрузки** или в другой папке, указанной в настройках браузера. Для формирования отчета необходимо использовать кнопку  .

В отчете отображается полный список ПО на просканированных агентах, в котором присутствуют программы с найденными уязвимостями. Отчет формируется с учетом применяемых на странице фильтров.

Распространенность программы с уязвимостью в защищаемой инфраструктуре

Чтобы получить информацию о распространении программы с уязвимостью в защищаемой EDR инфраструктуре, аналитику необходимо перейти в раздел **Программы** страницы **Управление уязвимостями**, после чего кликнуть по имени программы. Откроется страница с разделом **Сведения о программе**, в котором в поле **Агенты с уязвимостью** можно просмотреть все хосты с установленными агентами, на которых обнаружена программа.

8.6 Аналитика

Основное назначение инструментов, представленных в области **Аналитика** – это создание условий для предотвращения простых и сложных угроз, в том числе известных и неизвестных APT-атак.

Аналитические правила позволяют выявлять аномальную активность на защищаемых конечных точках и реагировать в автоматическом или ручном режиме на эти аномалии.

Подобные возможности достигаются с помощью соотнесения событий телеметрии, получаемой от компьютеров с агентами, с внутренними настройками EDR и настройками правил индикации (индикаторы атак, индикаторы компрометации, YARA-правила).

В основу EDR заложены инструменты автоматического обнаружения и индикации, позволяющие с высокой долей вероятности выделить в событиях телеметрии, приходящих с агентов, события, потенциально или прямо указывающие на воздействия вредоносных программ или развитие APT-атак.

В систему индикации входит множество подсистем обработки событий, связанных с работой программ, файловыми событиями, событиями реестра, сетевых интерфейсов, работой подсистемы ETW-событий, и т.д.

В области **Аналитика** основной панели Программы находятся следующие разделы:

1) Индикаторы атак;

2) Индикаторы компрометации;

3) YARA-правила (файлы);

4) YARA-правила (память);

5) Журналы.

Разделы содержат наборы аналитических правил, которые могут быть созданы в модуле администрирования или получены с TI-платформы.

Наборы аналитических правил и исключений, получаемые Программой от TI, помечаются значком TI, если наборы синхронизируются, и значком TI, если синхронизации нет (скорее всего такой набор был удален на TI-платформе). Все наборы попадают в общий список и требуют назначения со стороны администратора для их применения на агентах.

Внешние наборы приходящие от TI сервиса с ошибкой, помечены иконкой TI. Эта иконка актуальна как для наборов аналитики, так и для наборов с исключениями. Для просмотра ошибок набора нужно перейти в сам набор и в поле ОШИБКИ НАБОРА нажать по иконке для раскрытия подробной информации в формате json.

Администратор может удалять несинхронизируемые наборы в EDR, при этом синхронизируемые наборы удалять и изменять не может.

Для пользователей Программы предусмотрена возможность создавать и редактировать собственные наборы для увеличения эффективности процесса обнаружения вредоносных атак и объектов.

В Программе сохранены аналитические наборы по умолчанию, которые позволяют детектировать известные и неизвестные угрозы, а также позволяют уменьшить количество ложноположительных срабатываний.

8.6.1. Индикаторы атак

Общая информация

Индикаторы атак используются в качестве инструмента динамического анализа угроз для защищаемой инфраструктуры. Индикация атак построена на основе правил как установленных в Программе по умолчанию, так и вновь создаваемых пользователями.

Важно

Если в профиле безопасности агента установлен режим «только детектирование», то действие «блокировать» для индикаторов атак, применяемых на агенте, будет переопределено на действие «детектировать».

Подробное описание структуры правил, особенностей их написания и работы с индикаторами содержится в документе «Руководство аналитика RT Protect EDR».

Наборы индикаторов атак

Страница с наборами индикаторов атак включает в себя следующие структурные элементы:

– элементы для фильтрации;

– таблица с наборами индикаторов атак;

– кнопка Добавить набор;

– кнопка Передать все наборы агентам ();

– кнопка Удалить выбранные (наборы);

– кнопка Редактировать ( );

– кнопка **Удалить** ( );

– кнопка Передать набор ( ).

В таблице с наборами индикаторов содержатся следующие поля:

– **Название** (набора);

– **Количество записей** (показывает, сколько индикаторов атак содержится в наборе);

– **Привязано агентов** (показывает, сколько агентов привязано к набору);

– Управление (содержит кнопки Редактировать, Удалить и Передать набор).

Для фильтрации информации на странице с наборами, предусмотрена система фильтров согласно следующему списку:

– **Поиск по полям набора** (поиск осуществляется по подстроке без учета регистра в полях: **Имя**, **MITRE**, **Условие**, **Описание**, **Комментарий**);

— Название набора.

Пример применения универсального фильтра представлен на рисунке 70.

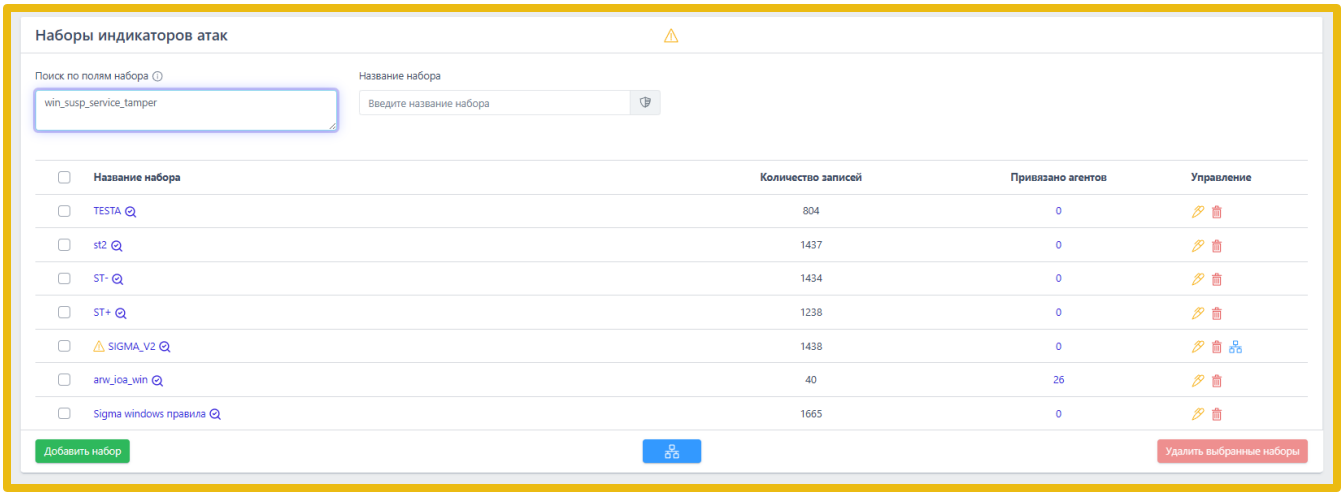


Рисунок 70 – Пример применения фильтрации по имени индикатора

На рисунке выше представлена таблица с наборами индикаторов атак, в которых присутствует заданный в фильтре текст (в данном случае имя индикатора). Названия наборов являются активной ссылкой. Кликнув, можно перейти на набор с правилами.

Рядом с названием набора присутствует иконка , нажав по которой, можно перейти непосредственно к индикатору атак, в котором присутствуют заданные в фильтре поля.

Описанные выше элементы фильтрации также применимы в разделах аналитики на страницах с наборами индикаторов компрометации и наборов с журналами, в разделах исключений с наборами исключений для программ, файлов, сетевых исключений, а также исключений индикаторов атак.

На странице пользователь может выполнить следующие операции:

— просматривать ранее созданные наборы индикаторов атак;

— добавлять новые наборы;

— редактировать название выбранного набора;

— передавать агентам изменения выбранного набора;

— удалять выбранные наборы.

— Для корректной работы наборов после каждого изменения требуется их передавать агентам с помощью соответствующих кнопок.

Для перехода к странице **Индикаторы атак** необходимо нажать ЛКМ на имени набора в поле **Название набора**.

На странице наборов представлены наборы, которые были созданы в подключаемом модуле «RT Protect TI». Эти наборы недоступны для редактирования в модуле администрирования RT Protect EDR и отмечены значком TI .

Страница «Индикаторы атак»

На странице **Индикаторы атак** содержится информация о правилах. Правила позволяют проводить динамический анализ событий, поступающих с агента. Кроме того, страница содержит инструменты конфигурирования этих правил и ссылки на MITRE ATT&CK.

Ссылки приводятся на те правила, которые описывают детектирование известных и указанных в базе знаний MITRE ATT&CK техник проникновения и атак на компьютерные сети и системы.

На странице с индикаторами атак можно выполнить следующие операции:

– просматривать информацию о ранее созданных индикаторах;

– создать новый индикатор атаки;

– выполнить поиск по имени индикатора;

– выполнить поиск по условию индикатора;

– копировать индикатор атаки из одного набора в другой;

– переместить индикатор атаки из одного набора в другой;

– экспортировать индикатор в файл;

– импортировать данные из файла;

– активировать/деактивировать индикатор атаки;

– редактировать индикатор атаки;

– удалить индикаторы атак из набора.

– Таблица индикаторов атак содержит следующие элементы:

– Имя;

– Тип;

– Критичность/Действие;

– MITRE;

– Дата создания/Автор;

– Последнее изменение/Пользователь;

– Управление.

Имя – в поле отображается значение имени индикатора.

Тип – в поле отображается тип события, на которое срабатывает индикатор атаки. События, которые могут быть отмечены как индикаторы атак:

– Сеть: Исходящее подключение;

– Сеть: Входящее подключение;

– Сеть: SSL HELLO;

– Сеть: Открытие локального порта на прием (LISTEN);

– Сеть: DNS-ответ;

– Файлы: Создан новый файл;

– Файлы: Файл переименован;

– Файлы: Удален файл;

– Файлы: Прямой доступ к диску (тому) на чтение;

– Файлы: Прямой доступ к диску (тому) на запись;

– Файлы: Создан именованный канал;

– Файлы: Доступ к файлу;

– Реестр: Создан новый ключ;

– Реестр: Удален ключ;

– Реестр: В значение ключа записаны данные;

– Реестр: Ключ переименован;

– Журналы: Событие журнала;

– Процессы: Загрузка драйвера;

– Процессы: Старт процесса;

– Процессы: Загрузка образа;

– Процессы: Доступ к процессу;

– Процессы: Создание нити в стороннем процессе;

– Процессы: Доступ к нити процесса;

– Процессы: Загрузка образа в сторонний процесс;

– Процессы: Загрузка .NET-сборки.

Критичность/Действие – в поле отображается степень критичности наступления события, описанного в индикаторе, а также действие, предпринимаемое Программой при срабатывании правила (обозначается знаками – блокировать , – детектировать).

MITRE – в поле отображается ссылка на технику атаки из базы знаний MITRE ATT&CK, на обнаружение которой настроен индикатор. Ссылка представляет собой ID техники атаки, указанный на сайте базы знаний MITRE ATT&CK.

Дата создания/Автор – в поле отображается дата и время создания правила, а также его автор.

Последнее изменение/Пользователь – в поле отображается дата и время последнего изменения правила, а также имя пользователя, выполнившего эти изменения.

Управление – содержит кнопки активации/деактивации правила в наборе, редактирования и удаления правила.

Для добавления нового индикатора атаки необходимо нажать кнопку **Добавить индикатор** в нижней части страницы.

Добавить индикатор можно двумя способами (рис. 71):

1) Создать новый индикатор;
2) Импортировать индикатор из sigma-правила.

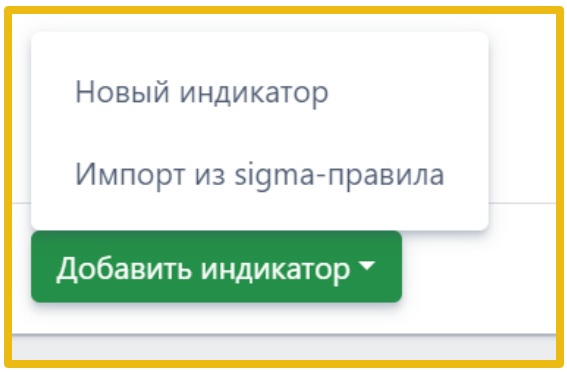
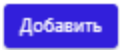


Рисунок 71 – Окно выбора способа добавления индикатора атаки

При выборе способа **Новый индикатор** откроется окно **Добавить индикатор**.

В данном окне следует прописать условия, на основании которых будет срабатывать правило.

Особенности создания индикаторов атак, их синтаксис подробно описывается в документе «Руководство аналитика RT Protect EDR». После написания условия необходимо нажать кнопку 

.

При создании индикаторов атак отдельные элементы условия будут подсвечиваться (операторы, значения полей). Написание условий подразумевает проверку синтаксиса, которая запускается или с помощью кнопки в нижней части окна раздела **Условие** (), или при сохранении индикатора атаки. Для создания индикатора и его дальнейшего применения необходимо, чтобы условие не противоречило синтаксису правил.

Для редактирования индикатора следует нажать кнопку **Редактировать**  в строке выбранного индикатора атаки и в открывшемся окне **Редактировать индикатор** внести необходимые изменения.

Для сохранения внесенных изменений необходимо нажать кнопку **Сохранить**.

В выпадающем списке **Режим** пользователь может установить режим обнаружения индикатора атаки.

Доступны следующие режимы:

1) Обычный (без определенных условий);
2) Без генерации обнаружения (инцидент создаваться не будет, но событие будет отображено на странице **Активность**);
3) Однократная генерация обнаружения (будет создан только один инцидент, даже если событие, которое сгенерировало инцидент, произойдет неоднократно).

Для копирования или перемещения индикатора из одного набора в другой необходимо отметить индикатор флажком и нажать кнопку  , после чего в открывшемся окне **Выбор набора** определить набор, в который следует скопировать или переместить выбранный элемент. Для перемещения индикатора следует поставить флажок **Переместить и удалить выбранные элементы из текущего набора**. Для завершения операции необходимо нажать кнопку **Выбрать**.

Чтобы экспортировать индикаторы атак в файл, необходимо нажать кнопку  . Далее выбрать один из двух предложенных форматов экспорта файла (csv, json). Файл сохранится в директории **Загрузки**. Экспортируется выбранный набор целиком. Чтобы импортировать индикаторы атак из файла в выбранный набор, необходимо нажать кнопку  , после чего выбрать файл с импортируемыми индикаторами и нажать кнопку **Открыть**.

Для активации/деактивации правила необходимо нажать кнопку / или нажать соответствующий элемент ( ) снизу таблицы индикаторов атак.

Для удаления индикатора атаки необходимо выбрать его с помощью кнопки выбора, установив флажок, после чего нажать кнопку **Удалить выбранные**. Для завершения операции ее необходимо подтвердить в открывшемся окне **Подтверждение действия**.

При выборе способа добавления индикатора **Импорт из sigma-правила**, открывается окно, представленное на рисунке 72.

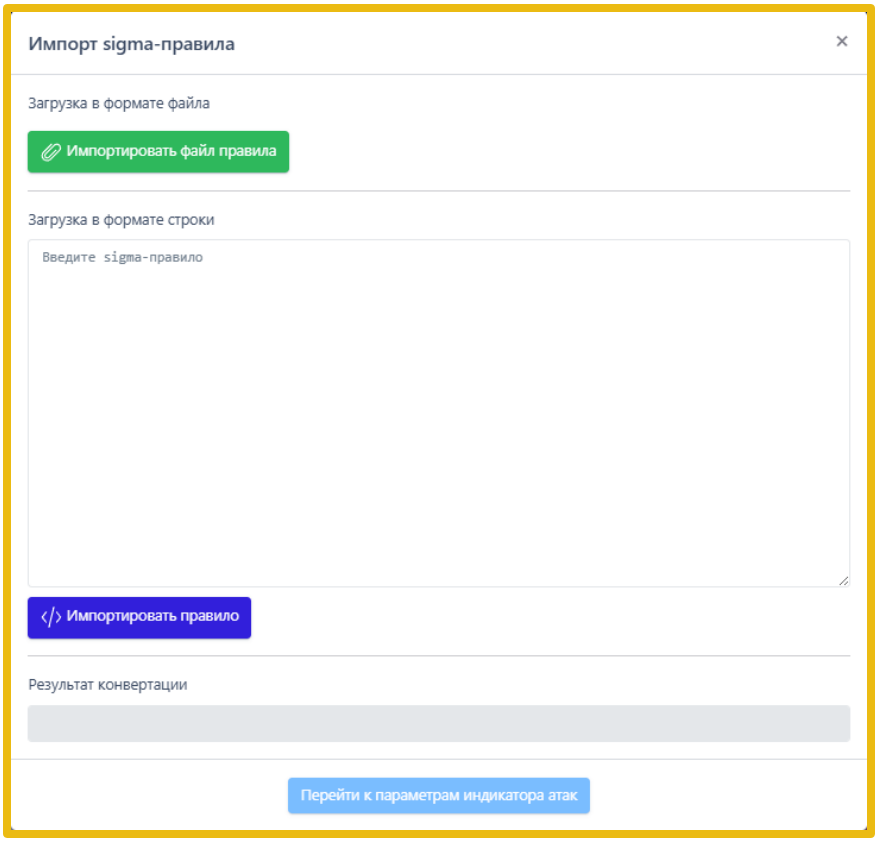
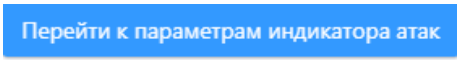


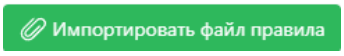
Рисунок 72 – Окно добавления индикатора с помощью импорта из sigma-правила

Sigma-правило, на основании которого будет создан индикатор атак, может быть добавлено в формате файла, либо в формате строки.

Для создания индикатора на основе Sigma-правила следует перейти на сайт https://github.com/SigmaHQ/sigma/tree/master/rules/windows и, выбрав одно из правил, нажать по иконке Импортировать правило.

При удачной конвертации правила, в поле **Результат конвертации** появится запись **Успешная конвертация**. Далее для редактирования индикатора на основе sigma-правила следует нажать по иконке 

. Откроется окно **Добавить индикатор** с информацией из того sigma-правила, на основании которого создан индикатор. Дальнейшие действия редактирования и сохранения индикатора атак аналогичны действиям, описанным в данном разделе выше.

Кроме указанной выше процедуры можно воспользоваться импортом yml-файла с правилом, скачав его по ссылке с sigma-правилами и загрузив в формате файла с помощью кнопки 

.

Ретроспективный анализ индикаторов атак

Ретроспективный анализ правила позволяет проверять срабатывания вновь создаваемых правил на массиве событий, сохраненных в системе. Подразумевается, что значительное количество срабатываний правила будет говорить о том, что оно нуждается в доработке. События, используемые коррелятором, хранятся не более 30 дней, поэтому при выборе периода проверки необходимо это учитывать.

Ретроспективный анализ индикаторов атак доступен во вкладке **Проверка** на странице **Редактировать индикатор.** Для того, чтобы проверить правило, необходимо выбрать период проверки и нажать кнопку **Запустить проверку.**

В случае, если будет достигнуто 500 и более срабатываний правила, проверка будет приостановлена, так как считается, что такое количество срабатываний свидетельствует о необходимости редактирования правила.

8.6.2. Индикаторы компрометации

Индикаторы компрометации, обрабатываемые Программой, подразделяются на сетевые и файловые. Особенностью работы с файловыми индикаторами является то, что все файлы, находящиеся на конечных точках с установленным на них агентом, проверяются только по имени файла.

По умолчанию файловая аналитика (подсчет хешей, матчинг индикаторов и др.) производится только для исполняемых файлов и только при их запуске или загрузке, если исполняемый файл – это динамически загружаемая библиотека. Опция профиля безопасности агента позволяет дополнительно указать расширения

файлов (помимо исполняемых), для которых также требуется включить файловый анализ, который будет производиться в режиме реального времени при доступе к этим файлам.

При обращении к файлу, хеш-сумма которого совпадает с хеш-суммой, указанной в индикаторе компрометации, обращение блокируется, а в модуле администрирования формируется (или дополняется) инцидент, объединяющий в себе все события, соответствующие индикатору. Эти события могут иметь разный тип в зависимости от выполняемой операции: открытие файла, чтение, удаление, а также могут относиться к разным процессам в системе. Таким образом блокируются все операции с файлом, изолируя его «по месту», без перемещения в карантин.

Запуск исполняемого файла или файла с потенциально активным содержимым, хеш которого присутствует в перечне индикаторов компрометации, будет блокироваться монитором файловой системы на самом раннем этапе запуска, когда системный объект **процесс** для него еще не сформирован.

Общая информация

На странице **Наборы индикаторов компрометации** в разделе **Индикаторы компрометации** содержится информация об объектах (или артефактах), которые являются источником компрометации.

Обнаружение событий, связанных с описанными в наборах компрометации артефактами, вызывает определенное действие, зафиксированное в наборе. Таким действием может быть блокирование или детектирование вызываемого артефактом процесса.

Важно

Если в профиле безопасности агента установлен режим «только детектирование», то действие «блокировать» для индикаторов компрометации, применяемых на агенте, будет переопределено на действие «детектировать».

Подробная информация об особенностях аналитической работы с индикаторами компрометации и методах обнаружения известных и неизвестных угроз содержится в документе «Руководство аналитика RT Protect EDR».

Наборы индикаторов компрометации

Информация на странице **Наборы индикаторов компрометации** представлена в табличном виде. Если на странице присутствует хотя бы один неприменённый набор индикаторов компрометации, то в верхней части таблицы появится значок предупреждения .

При наведении на значок курсора мыши возникнет запись **Не все наборы были применены**.

Строка для такого набора также будет помечена предупреждающим значком с всплывающей надписью **Набор не применен**, в поле **Управление** для такого набора появится кнопка **Передать набор** ( ), а в середине нижней части страницы появляется кнопка **Передать все наборы агентам** ( ).

В шапке таблицы представлены следующие поля: кнопка выбора (отмечена элементом), **Название набора**, **Количество записей**, **Привязано агентов**, **Управление**.

Название набора – в поле отображается название набора индикаторов компрометации, при нажатии ЛКМ на название набора происходит переход к странице **Индикаторы компрометации**.

Количество записей – в поле отображается количество индикаторов, сохраненных в наборе.

Привязано агентов – в поле отображается количество привязанных к набору агентов. При нажатии ЛКМ на число агентов происходит переход к странице **Агенты**, на которой в таблице будут показаны привязанные к набору агенты.

Управление – в поле отображаются кнопки операций с набором индикаторов компрометации: **Редактировать** , **Удалить** и **Передать набор** .

Редактировать – при нажатии кнопки открывается окно **Редактировать набор**. В поле **Имя** отображается название набора, для его изменения необходимо ввести в строке с именем набора новое имя и нажать кнопку Сохранить.

Удалить – при нажатии кнопки открывается окно **Подтверждение действия**. Далее для удаления набора необходимо нажать кнопку Выполнить.

Передать набор – кнопка отображается в поле **Управление** при условии, что в наборе индикаторов компрометации были изменения.

При нажатии кнопки открывается окно **Подтверждение действия**. Далее для передачи набора агентам необходимо нажать кнопку **Подтвердить**.

В нижней части страницы **Наборы индикаторов компрометации** находятся кнопки Добавить набор и Удалить выбранные наборы.

Для добавления нового набора индикаторов компрометации необходимо нажать кнопку **Добавить набор**, после чего в открывшемся окне **Добавить набор** в строке **Имя** ввести название нового набора.

Если к новому набору требуется добавить индикаторы из наборов, созданных и сохраненных в Программе ранее, то в поле **Базовый набор** следует выбрать из выпадающего списка набор, который станет основой для нового набора.

Добавление базового набора является опциональным условием. Если в окне **Добавить набор** не ввести значение имени нового набора, то кнопка **Добавить** не будет активна. Для завершения операции добавления необходимо нажать кнопку **Добавить**.

Для удаления одного или нескольких наборов индикаторов компрометации следует отметить флажками соответствующие им кнопки выбора , после чего нажать кнопку **Удалить выбранные наборы.** В открывшемся окне **Подтверждение действия** необходимо нажать кнопку **Подтвердить**.

Страница «Индикаторы компрометации»

Переход на страницу с таблицей **Индикаторы компрометации** происходит при нажатии ЛКМ на названии набора в таблице **Наборы индикаторов компрометации**.

На странице **Индикаторы компрометации** пользователь может выполнять следующие действия:

– просматривать информацию об индикаторах, входящих в выбранный набор;

– создавать новые индикаторы компрометации;

– изменять индикаторы компрометации, входящие в выбранный набор;

– экспортировать индикаторы в файлы различных форматов;

– импортировать данные из файла в набор индикаторов;

– копировать/перемещать индикаторы выбранного набора в другие наборы индикаторов компрометации;

– сохранять набор с добавленными индикаторами компрометации;

– активировать/деактивировать выбранные индикаторы компрометации.

– удалять из набора выбранные индикаторы компрометации.

В верхней части области **Индикаторы компрометации** отображается имя набора и фильтр **Показывать по** (возможно задавать значения 10, 20, 50, 100 или 500 элементов).

После добавления или изменения индикаторов сверху таблицы появится значок ⚠ с предупреждающим сообщением **Набор не применен**. Сообщение появляется при наведении курсора мыши на предупреждающий значок.

Шапка таблицы с индикаторами содержит следующие поля:

1) Кнопка выбора (отмечена элементом ▢);
2) Имя индикатора;
3) Тип артефакта;
4) Артефакт;
5) Действие;
6) Комментарий;
7) Дата создания/Автор;
8) Последнее изменение/Пользователь;
9) Управление.

Имя индикатора – поле содержит произвольное название индикатора, заданное пользователем.

Тип артефакта – поле содержит тип объекта, являющегося индикатором компрометации.

Каждый индикатор компрометации основывается на определенном типе артефакта. Тип артефакта задается при создании или изменении индикатора компрометации.

В Программе предусмотрено несколько типов артефактов:

1) **Файл** – при выборе данного типа при создании или редактировании индикатора компрометации появляются дополнительно поле с обязательным именем файла, а также опциональные поля **Артефакт (хеш файла SHA-256)** и **Артефакт (размер файла)**;
2) **SHA-256** – в качестве индикатора компрометации в поле **Артефакт** будет выбрано значение хеша, рассчитанного по алгоритму sha-256, для объекта, при обнаружении которого Программа создаст инцидент;

3) **SHA-1** – в качестве индикатора компрометации в поле **Артефакт** будет выбрано значение хеша, рассчитанного по алгоритму sha-1, для объекта, при обнаружении которого Программа создаст инцидент;
4) **MD5** – в качестве индикатора компрометации в поле **Артефакт** будет выбрано значение хеша, рассчитанного по алгоритму MD5, для объекта, при обнаружении которого Программа создаст инцидент;
5) **IP-адрес** – в качестве индикатора компрометации в поле **Артефакт** будет выбран IP-адрес сетевого соединения, при взаимодействии с которым Программа создаст инцидент;
6) **Доменное имя** – в качестве индикатора компрометации в поле **Артефакт** будет выбрано имя домена, например, mail.ru, при взаимодействии с которым Программа создаст инцидент;



Важно

Домен и IP-адрес могут быть написаны вместе с портом (<IP/домен>:<порт>). Порт в контексте сетевых коммуникаций – это виртуальное «окно», через которое проходят данные для определенной Программы или службы. Каждый порт имеет свой уникальный номер.

7) **URL** – в качестве индикатора компрометации будет выбран унифицированный указатель ресурса в сети Интернет, при взаимодействии с которым Программа создаст инцидент;
8) **Сетевая сигнатура** – в качестве индикатора компрометации в поле **Артефакт** будет выбрана сетевая сигнатура, при обнаружении которой Программа создаст инцидент.

Артефакт – в поле отображается наименование артефакта. Название артефакта должно соответствовать выбранному типу артефакта, то есть, если указать тип артефакта **Доменное имя**, то название артефакта должно соответствовать правилам написания доменных имен, к примеру, **example.com**. Дополнительно поле содержит элемент , позволяющий скопировать в буфер обмена имя артефакта.

Действие – в поле отображается действие, которое должна осуществить Программа при обнаружении события, связанного с выбранным индикатором компрометации.

В качестве ответа на вредоносную или потенциально вредоносную активность предусмотрены следующие действия:

— Блокировать – в этом случае активность будет запрещена;

— Детектировать – в этом случае активность будет разрешена, но Программа уведомит пользователя об обнаружении детектируемого события, создав инцидент.

Комментарий – в поле отображается произвольный комментарий к выбранному индикатору компрометации. Поле **Комментарий** заполняется при необходимости во время редактирования или добавления нового индикатора.

Файловые индикаторы компрометации содержат флаг **Блокировка действует и в контексте критических системных процессов**, подробная информация о флаге и критических системных процессах содержится в документе «Руководство аналитика RT Protect EDR».

Дата создания/Автор – в поле отображается дата и время создания правила, а также его автор.

Последнее изменение/Пользователь – в поле отображается дата и время последнего изменения правила, а также имя пользователя, выполнившего эти изменения.

Управление – в поле отображаются кнопки **Редактировать** , **Удалить** а также кнопка активации/деактивации соответствующего индикатора (/). Для редактирования индикатора компрометации следует нажать кнопку **Редактировать**. В открывшемся окне **Редактировать индикатор** необходимо изменить одно или несколько полей, требующих изменения или корректировки, и нажать кнопку **Сохранить**. Поля формы **Редактировать индикатор** идентичны полям таблицы индикаторов, описанным выше.

Для удаления индикатора компрометации необходимо нажать кнопку **Удалить** . В открывшемся окне **Подтверждение действия** следует нажать кнопку Выполнить.

В нижней части таблицы индикаторов находятся кнопки операций с индикаторами:

1) Добавить индикатор;
2) Передать набор агентам – ;
3) Копировать/переместить выбранные элементы в другой набор – ;
4) Экспортировать набор в файл – ;
5) Импортировать данные из файла в набор (поддерживаемые форматы: csv, json) – ;
6) Активировать/деактивировать индикатор или индикаторы ;
7) Удалить индикатор или индикаторы Удалить выбранные.

Для добавления индикатора в области **Индикаторы компрометации** необходимо нажать кнопку Добавить индикатор.

Далее в открывшемся окне **Добавить индикатор** (рис. 73) следует заполнить поля, соответствующие полям, указанным в шапке таблицы индикаторов, после чего нажать кнопку Добавить.

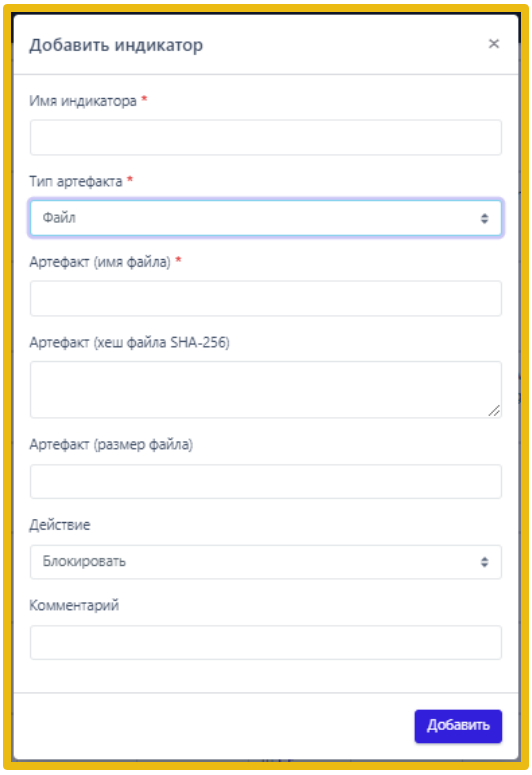


Рисунок 73 – Окно «Добавить индикатор» с типом артефакта «Файл»

Для передачи агентам любого изменения в индикаторах необходимо нажать кнопку **Передать набор агентам**. Кнопка не будет отображаться на странице до внесения следующих изменений в набор.

Для копирования или перемещения индикаторов из одного набора в другой следует отметить флажками кнопки выбора для индикатора или индикаторов, которые нужно скопировать/переместить в другой набор.

После выбора индикаторов следует нажать кнопку **Копировать/Переместить выбранные элементы в другой набор**.

В открывшемся окне **Выбор набора** необходимо в поле **Набор** выбрать из выпадающего списка набор индикаторов компрометации.

В этот набор будут скопированы выбранные ранее индикаторы. Если необходимо их переместить с удалением из набора-донора, то следует установить флажок **Переместить и удалить выбранные элементы из текущего набора**.

Для завершения операции нужно нажать кнопку Выбрать. Для отмены операции следует нажать кнопку закрытия окна ×.

Для экспорта набора в файл следует нажать кнопку **Экспортировать набор в файл**. Далее в открывшемся списке необходимо выбрать файловый формат, в котором будут сохранены данные из набора. После выбора формата созданный файл в указанном формате будет сохранен в папку, в которую настроена загрузка файлов в операционной системе (например, папка **Загрузки**).

Для импорта данных из файла с индикаторами следует нажать кнопку – **Импортировать данные из файла в набор, поддерживаемые форматы: csv, json**. После нажатия кнопки открывается окно файлового менеджера, в котором необходимо выбрать импортируемый файл, после чего импортировать данные из файла в выбранный набор индикаторов компрометации. После завершения операции импорта индикаторы компрометации из импортируемого файла добавятся в выбранный набор индикаторов компрометации.

8.6.3. YARA-правила (файлы)

Общая информация

Правила, указанные в разделе **YARA-правила (файлы)**, используются в качестве инструмента анализа угроз для защищаемой инфраструктуры в части анализа вредоносных файловых сигнатур.

В Программе предусмотрены YARA-правила в наборе по умолчанию, а также инструментарий для создания новых правил.

Важно

YARA-правила работают на агенте только в том случае, если в профиле безопасности выбранного агента установлен режим глубокого сканирования, включающий в себя YARA-правила, то есть выбраны режимы **YARA-правила** или **ML и YARA-правила**.

Подробное описание структуры правил, особенностей их написания и работы с YARA-правилами содержится в документе «Руководство аналитика RT Protect EDR».

Наборы YARA-правил (файлы)

Страница с наборами YARA-правил для файлов включает в себя следующие структурные элементы:

— элементы фильтрации;

— таблица с наборами YARA-правил;

— кнопка Добавить набор;

— кнопка Передать все наборы агентам;

— кнопка Удалить выбранные наборы.

Для добавления нового набора необходимо нажать кнопку **Добавить набор**, после чего в окне **Добавить набор** ввести название нового набора YARA-правил. На этом этапе можно добавить YARA-правила из базового набора в новый. Для завершения операции необходимо нажать кнопку **Добавить**.

После любого изменения набора для его корректной работы требуется передать изменения агентам, для этого необходимо нажать кнопку **Передать набор** () или **Передать все наборы агентам** ().

Для удаления набора необходимо нажать кнопку **Удалить** () или **Удалить выбранные наборы**.

Для фильтрации на странице **Наборы Yara-правил (файлы)** имеется система фильтров, представленная в следующем списке:

— **Имя правила** (необходимо ввести полное имя правила);

— Название набора.

При нажатии ЛКМ на имени набора открывается страница **YARA-правила (файлы)** для выбранного набора (рис. 74).

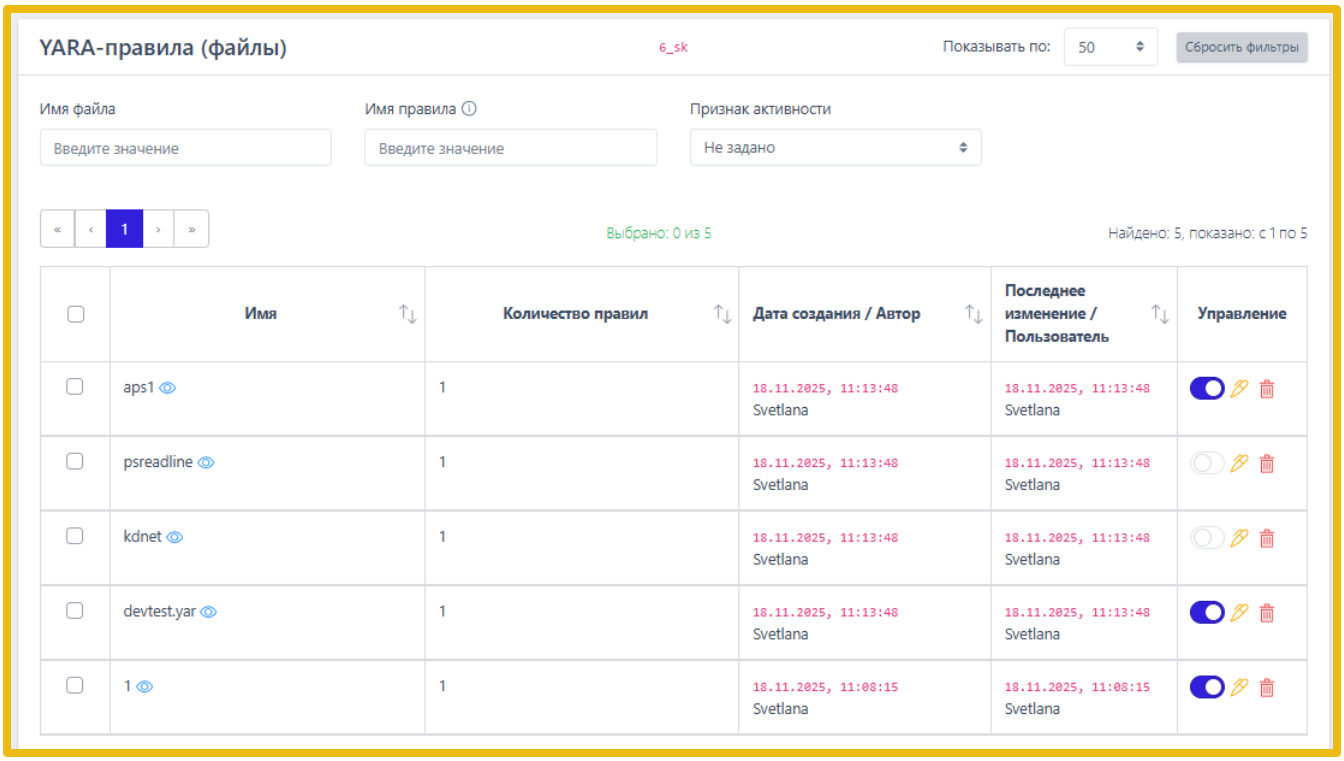


Рисунок 74 – YARA-правила (файлы)

Страница «YARA-правила (файлы)»

На странице **YARA-правила (файлы)** можно выполнять следующие операции:

– просматривать правила из выбранного набора;

– добавлять новые правила в выбранный набор;

– применять наборы после изменения правил;

– копировать/перемещать выбранные правила в другой набор;

– экспортировать выбранный набор в файл;

– импортировать данные из файла в выбранный набор правил;

– активировать или деактивировать правило;

– редактировать выбранное правило;

– удалить выбранное правило из набора.

Для добавления нового правила необходимо нажать кнопку **Добавить правила**, после чего необходимо выбрать операцию **Новый файл** (для добавления одного файла в режиме набора текста или загрузки с хоста администратора) или **Загрузить файлы** (для добавления одного или нескольких файлов путём загрузки с хоста администратора).

После выбора операции **Новый файл** откроется окно **Добавить YARA-правила**, в котором необходимо добавить имя YARA-файла и написать правило или несколько правил в соответствии с синтаксисом YARA. Администратор может добавить файл в формате .yar с помощью кнопки **Загрузить файл** ( ).

Подробная информация о синтаксисе YARA содержится в документе «Руководство аналитика RT Protect EDR» и официальной документации YARA. Пример правила YARA приведен на рисунке 75.

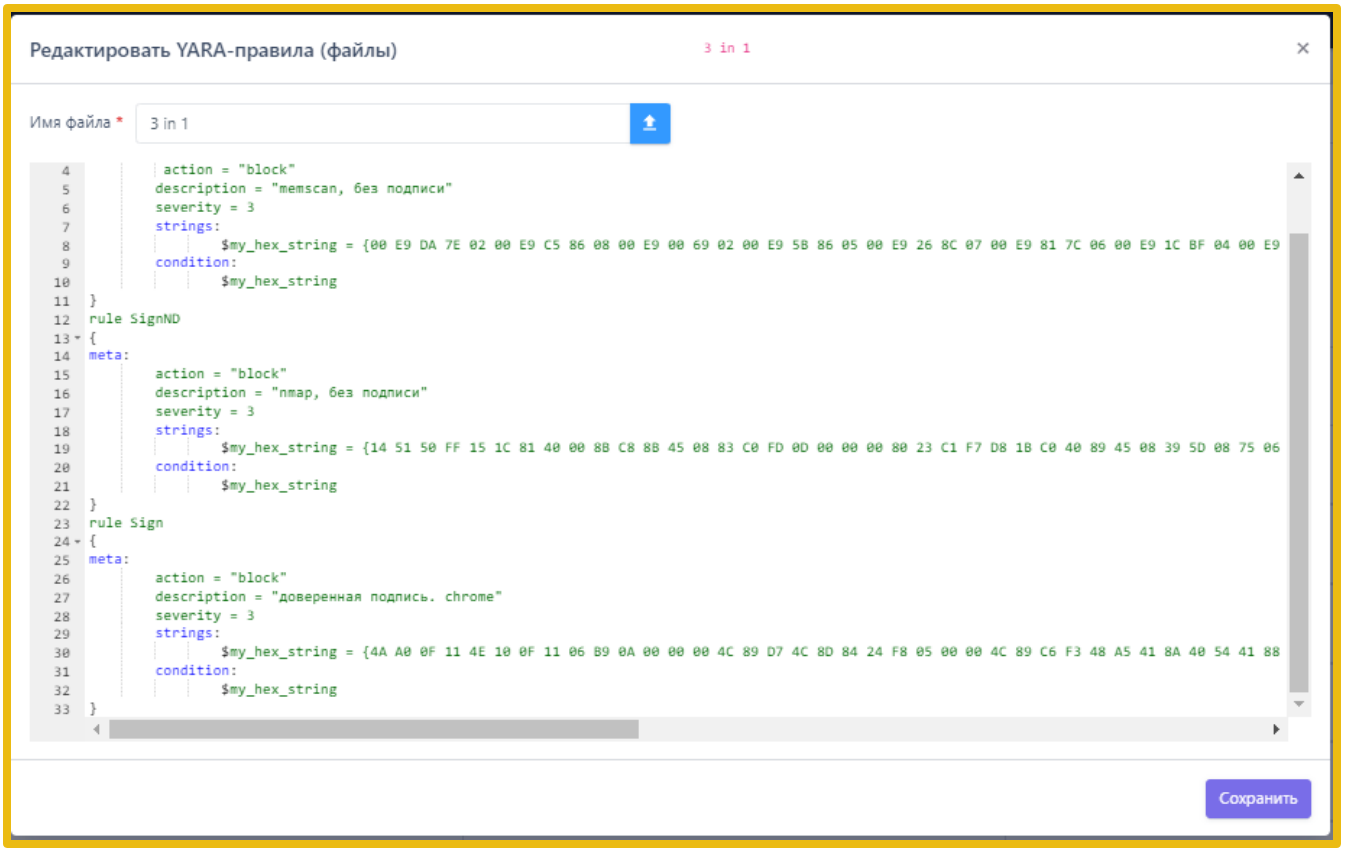


Рисунок 75 – Пример правила YARA

Для корректной работы после любых изменений в наборе необходимо нажать кнопку **Передать набор агентам** ( ).

При выборе операции **Загрузить файлы** откроется окно **Загрузить файлы YARA**, в котором необходимо нажать кнопку **Выбрать файлы**, после чего в Проводнике выбрать один или несколько файлов с расширением .yar или .yara. Для завершения операции необходимо нажать кнопку **Загрузить файлы на сервер**.

Для копирования или перемещения правила из одного набора в другой необходимо выбрать нужные элементы и нажать кнопку **Копировать/Переместить выбранные элементы в другой набор** ( ).

Далее выбрать набор, в который будет копироваться выбранный элемент. Если необходимо переместить элемент, то следует в окне **Выбор набора** установить флажок **Переместить и удалить выбранные элементы из текущего набора**. Для завершения операции необходимо нажать кнопку **Выбрать**.

Для экспорта набора в файл следует нажать кнопку **Экспортировать набор в файл**  (формат JSON). Набор будет сохранен в папке **Загрузки** в соответствующем формате.

Для импорта правил из файла требуется нажать кнопку **Импортировать данные из файла в набор, поддерживаемые форматы: JSON** ().

Далее выбрать на компьютере файл соответствующего формата, содержащий нужные правила, и нажать кнопку **Открыть**.

Чтобы активировать или деактивировать правило из выбранного набора, необходимо нажать кнопку  / или выполнить активацию/деактивацию с помощью кнопок **Активировать выбранные элементы/Деактивировать выбранные элементы** ().

Для удаления правил из набора необходимо отметить флажками правила, которые требуется удалить и нажать кнопку **Удалить выбранные** или удалить правила по отдельности с помощью кнопки **Удалить** ().

Для редактирования правила следует нажать кнопку **Редактировать** ( ), после чего внести изменения в открывшемся окне с правилом. После внесения изменений в правило необходимо нажать кнопку **Сохранить**.

На странице предусмотрена фильтрация YARA-правил по имени, а также фильтрация файлов по имени файла в соответствующих строках. При этом необходимо помнить, что поиск по имени правил требует ввода полного имени правила.

8.6.4. YARA-правила (память)

Правила, указанные в разделе **YARA-правила (память)**, используются в качестве инструмента анализа угроз для защищаемой инфраструктуры в части анализа памяти процесса на наличие вредоносных сигнатур. В Программе предусмотрены YARA-правила в наборе по умолчанию, а также инструментарий для создания новых правил.

Наборы YARA-правил (память)

Страница с наборами YARA-правил для памяти включает в себя те же структурные элементы, что и страница **Наборы YARA-правил (файлы)**:

— таблица с наборами YARA-правил;

— кнопка **Добавить набор**;

— кнопка **Передать все наборы агентам**;

— кнопка **Удалить выбранные наборы**.

Для добавления нового набора необходимо нажать кнопку **Добавить набор**, после чего в окне **Добавить набор** ввести название нового набора YARA-правил. На этом этапе можно добавить YARA-правила из базового набора в новый. Для завершения операции необходимо нажать кнопку **Добавить**.

После любого изменения набора для корректной его работы требуется применять сделанные изменения, для этого необходимо нажать кнопку **Передать набор** () или **Передать все наборы агентам** ().

Для удаления набора необходимо нажать кнопку **Удалить** () или **Удалить выбранные наборы**.

Для фильтрации на странице **Наборы Yara-правил (память)** имеется фильтр по имени правила, входящего в набор.

При нажатии ЛКМ на имени набора открывается страница **YARA-правила (память)** для выбранного набора.

Страница «YARA-правила (память)»

На странице **YARA-правила (память)** можно выполнять следующие операции:

— просматривать правила из выбранного набора;

— добавлять новые правила в выбранный набор;

— применять наборы после изменения правил;

— копировать/перемещать выбранные правила в другой набор;

— экспортировать выбранный набор в файл;

— импортировать данные из файла в выбранный набор правил;

— активировать или деактивировать правило;

— редактировать выбранное правило;

— удалить выбранное правило из набора.

Для добавления нового правила необходимо нажать кнопку **Добавить правила**, после чего необходимо выбрать операцию **Новый файл** (для добавления одного файла в режиме набора текста или загрузки с хоста администратора) или **Загрузить файлы** (для добавления одного или нескольких файлов путём загрузки с хоста администратора). После выбора операции **Новый файл** откроется окно **Добавить YARA-правила**, в котором необходимо добавить имя YARA-файла и написать правило или несколько правил в соответствии с синтаксисом YARA. Администратор может добавить файл в формате .yar с помощью кнопки **Загрузить файл** ().

Для корректной работы после любых изменений в наборе необходимо нажать кнопку **Передать набор агентам** ().

При выборе операции **Загрузить файлы** откроется окно **Загрузить файлы YARA**, в котором необходимо нажать кнопку **Выбрать файлы**, после чего в открывшемся окне выбрать один или несколько файлов с расширением .yar или .yara. Для завершения операции необходимо нажать кнопку **Загрузить файлы на сервер**.

Для копирования или перемещения правила из одного набора в другой следует выбрать нужные элементы и нажать кнопку **Копировать/Переместить выбранные элементы в другой набор** (). Далее выбрать набор, в который будет копироваться выбранный элемент. Если необходимо переместить элемент, то следует в окне **Выбор набора** установить флажок **Переместить и удалить выбранные элементы из текущего набора**. Для завершения операции необходимо нажать кнопку **Выбрать**.

Для экспорта набора в файл следует нажать кнопку **Экспортировать набор в файл**  (формат JSON). Набор будет сохранен в папке **Загрузки** в соответствующем формате.

Для импорта правил из файла требуется нажать кнопку **Импортировать данные из файла в набор, поддерживаемые форматы: JSON** ().

Далее выбрать на компьютере файл соответствующего формата, содержащий нужные правила, и нажать кнопку **Открыть**.

Чтобы активировать или деактивировать правило из выбранного набора, необходимо нажать кнопку  или выполнить активацию/деактивацию с помощью кнопок **Активировать выбранные элементы/Деактивировать выбранные элементы** ().

Для удаления правил из набора необходимо отметить флажками правила, которые требуется удалить и нажать кнопку **Удалить выбранные** или удалить правила по отдельности с помощью кнопки **Удалить** ( ).

Для редактирования правила следует нажать кнопку **Редактировать** ( ), после чего внести изменения в открывшемся окне с правилом. После внесения изменений в правило необходимо нажать кнопку **Сохранить**.

На странице предусмотрена фильтрация YARA-правил по имени, а также фильтрация файлов по имени файла в соответствующих строках. При этом необходимо помнить, что поиск по имени правил требует ввода полного имени правила с учетом регистра. Также в качестве фильтра можно выставить признак активности для поиска активных или неактивных правил.

8.6.5. Журналы

Общая информация

На странице **Наборы журналов** содержатся наборы с правилами детектирования подсистемы трассировки событий для Windows (ETW). События, генерируемые подсистемой ETW, собираются агентом и доставляются на сервер, если агенту назначены наборы с соответствующими правилами.

Правила – это по сути подписки на определенные ETW-провайдеры, которые можно создавать с помощью удобного интерфейса раздела **Журналы** Программы. Информация о собранных ETW-событиях может быть использована при написании индикаторов атак (в данный момент функционал не поддерживается.

Наборы журналов

Страница **Наборы журналов** содержит следующие структурные элементы:

– элементы фильтрации;

– таблица с наборами журналов;

– кнопка **Добавить набор**;

– кнопка **Передать все наборы агентам** ();

– кнопка **Удалить выбранные наборы**.

Чтобы добавить новый набор с журналами, необходимо нажать кнопку **Добавить набор**, после чего ввести название нового набора.

На этом этапе можно добавить к новому набору журналы из ранее сохраненных наборов. Для этого нужно выбрать соответствующий набор в строке **Базовый набор**. Для завершения операции необходимо нажать кнопку **Добавить**.

Для редактирования названий наборов применяется кнопка **Редактировать** ( ).

Чтобы удалить набор/наборы требуется отметить нужные наборы флажками и нажать кнопку **Удалить выбранные наборы** или удалить их по отдельности с помощью кнопки **Удалить** ( ).

Для перехода к странице **Журналы** необходимо нажать ЛКМ на имени набора журналов в поле **Название набора**.

Страница «Журналы»

На странице **Журналы** в табличном виде отображается информация об определенном наборе правил для событий журналов.

Пользователь может выполнить на странице следующие операции:

- добавить новое правило или несколько правил для журналов;
- редактировать или удалить существующее правило/правила;
- экспорт/импорт файла с набором;
- копировать элементы одного набора или весь набор в другой набор.

В таблице **Журналы** отображаются следующие поля:

1) Поля кнопки выбора ( );
2) Имя журнала;
3) Ключевые слова (любые);
4) Ключевые слова (все);
5) Уровень;
6) Фильтр кодов событий;
7) Дополнительные параметры;
8) Дата создания/Автор;
9) Последнее изменение/Пользователь;
10) Управление.

Имя журнала – в поле отображается имя провайдера событий подсистемы ETW или имя лога для агентов Linux.

Ключевые слова (любые) – в поле отображается информация о любых ключевых словах, на основе которых будут обнаруживаться события выбранного ETW-провайдера. То есть используется совпадение по любому из представленных в списке ключевому слову.

Ключевые слова (все) – в поле отображается информация обо всех ключевых словах, на основе которых будут обнаруживаться события выбранного ETW-провайдера. То есть используется совпадение по всем ключевым словам одновременно.

В Программе доступна настройка детектирования событий по ключевым словам для определенных провайдеров ETW, поэтому для многих правил в поле будет отображаться надпись Не заданы.

Уровень – в поле отображается уровень детектируемого события, заданный пользователем. Уровень добавляется при создании или редактировании правил для журналов. Доступны следующие уровни событий: **Подробно**, **Информация**, **Предупреждение**, **Ошибка** и **Критическая ошибка**.

Фильтр кодов событий – в поле прописываются коды событий, согласно которым будут фильтроваться события выбранного провайдера. Правила записи кодов событий отображается при наведении курсора на значок ⓘ в окне добавления журнала (рис. 76).

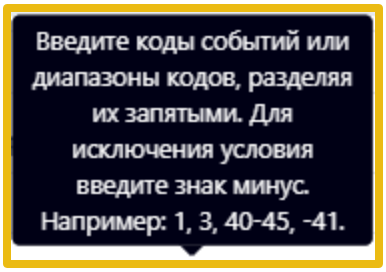


Рисунок 76 – Правила записи кодов событий

Дополнительные параметры – в поле отображается информация о дополнительных параметрах детектирования ETW-событий. Доступны для выбора следующие параметры:

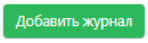
1) SID пользователя;
2) ID терминальной сессии;
3) Стек вызовов;

4) Исключить события с нулевым значением KEYWORD;

5) Порядковый номер процесса;

6) Ключ события;

7) Исключить события от приватных процессов.

Чтобы добавить нового провайдера событий подсистемы ETW, в соответствии с настройками которого будут обнаруживаться события на агенте, необходимо в нижней части страницы нажать кнопку 

. Пользователю доступно два режима добавления журнала:

– по GUID;

– по имени канала.

– Для режима **GUID** обязательными к заполнению являются поля **Имя провайдера** и **GUID провайдера**. Для режима **Имя канала** обязательным для заполнения является поле **Имя канала**.

Для копирования или перемещения журнала из одного набора в другой необходимо выбрать нужные элементы и нажать кнопку **Копировать/Переместить выбранные элементы в другой набор** (). Далее выбрать набор, в который будет копироваться выбранный элемент. Если необходимо переместить элемент, то следует в окне **Выбор набора** установить флажок **Переместить и удалить выбранные элементы из текущего набора**. Для завершения операции необходимо нажать кнопку **Выбрать**.

Для экспорта набора с журналами в файл следует нажать кнопку **Экспортировать набор в файл** (). Далее выбрать формат, в котором будет экспортироваться набор (CSV или JSON). Набор будет сохранен в папке **Загрузки** в выбранном формате.

Для импорта журналов из файла требуется нажать кнопку **Импортировать данные из файла в набор, поддерживаемые форматы: CSV, JSON** (). Далее выбрать на компьютере файл соответствующего формата, содержащий нужные журналы, и нажать кнопку **Открыть**.

Чтобы активировать или деактивировать журналы из выбранного набора, необходимо нажать кнопку  или выполнить активацию/деактивацию с помощью кнопок **Активировать выбранные элементы/Деактивировать выбранные элементы** ()

Для удаления журналов из набора необходимо отметить флажками журналы, которые требуется удалить, и нажать кнопку **Удалить выбранные** или удалить журналы по отдельности с помощью кнопки **Удалить** ().

8.7 Исключения

В области **Исключения** содержатся следующие разделы:

— Исключения для файлов;

— Исключения для программ;

— Сетевые исключения;

— Исключения индикаторов атак.

С помощью этих разделов выполняется настройка файловых, программных и других исключений, которые позволяют переопределить работу файлов, определить особенности выполнения программ, переопределить сетевые блокировки, а также блокировать работу индикаторов атак. Кроме того, исключения позволяют блокировать исполнение файлов или создание сетевых подключений без создания инцидентов в программе.

8.7.1. Исключения для программ

Общая информация

На странице **Наборы исключений для программ** содержится список программ, исполнение которых должно соответствовать тем или иным настройкам безопасности. Для этого в Программе предусмотрена система флагов, устанавливающих параметры безопасности для исполняемых файлов. Исключающие флаги определяют, какие аналитические проверки необходимо выключить для указанного исполняемого файла и, соответственно, порождаемого им процесса, какие события необходимо выключить для того или иного процесса, какие установить разрешения выбранному процессу, а также определить дополнительные особенности поведения программы.

В список исключений для программ можно вносить исполняемые файлы без настройки для них каких-либо определенных условий, задаваемых флагами.

Наличие этой возможности позволяет администратору настроить Программу для уменьшения количества ложных срабатываний, а в случае необходимости, заблокировать ту или иную программу в целях обеспечения безопасности.

Наборы исключений для программ

Страница **Наборы исключений для программ** включает в себя следующие структурные элементы:

— элементы фильтрации;

— таблица с наборами исключений для программ;

— кнопка **Добавить набор**;

— кнопка **Передать все наборы агентам**;

— кнопка **Удалить выбранные наборы**.

Чтобы добавить новый набор с исключениями для программ, необходимо нажать кнопку **Добавить набор**, после чего ввести название нового набора.

На этом этапе можно добавить к новому набору исключения для программ из ранее сохраненных наборов. Для этого нужно выбрать соответствующий набор в строке **Базовый набор**. Для завершения операции необходимо нажать кнопку **Добавить**.

Для редактирования названий наборов применяется кнопка **Редактировать** ( ).

Чтобы удалить набор/наборы требуется отметить нужные наборы флажками и нажать кнопку **Удалить выбранные наборы** или удалить их по отдельности с помощью кнопки **Удалить** ( ).

Для перехода к странице **Исключения для программ** необходимо нажать ЛКМ на имени набора в поле **Название набора**.

Для осуществления поиска по наборам необходимо использовать фильтры **Поиск по полям набора** и Название. В фильтре **Поиск по полям набора** поиск осуществляется по подстроке без учета регистра в полях: **Значение**, **Издатель ЭП**, **Правила**, **Комментарий**.

Страница «Исключения для программ»

На странице **Исключения для программ** можно выполнять следующие операции:

— просматривать исключения для программ в выбранном наборе;

— добавлять новое исключение по имени файла;

— добавлять новое исключение по хешу;

— добавлять новое исключение по командной строке;

— применять изменения в наборе исключений;

— копировать/перемещать выбранные исключения из одного набора в другой;

— экспортировать набор с исключениями в файл;

— импортировать исключения из файла в набор;

— активировать/деактивировать исключения в наборе;

— редактировать исключение;

— удалять выбранные исключения.

Для добавления в набор нового исключения для программы необходимо нажать кнопку **Добавить исключение** и в открывшемся списке выбрать тип добавляемого исключения: **Файл**, **Хеш** или **Командная строка**. Далее в открывшемся окне **Добавить исключение** следует установить параметры, в соответствии с которыми будет функционировать программа, внесенная в список исключений.

В зависимости от выбора типа исключения (**Файл**, **Хеш** или **Командная строка**) окно **Добавить исключение** будет содержать поля с различными параметрами.

Для типа исключений **Файл** необходимо определить следующие параметры: **Файлы**, **Флаги**, **Издатель ЭП**, **Правила**, **Комментарий**.

Для типа исключений **Хеш** следует определить следующие параметры: **Тип хеш-суммы**, **Хеш-сумма**, **Флаги**, **Издатель ЭП**, **Правила**, **Комментарий**.

Для типа исключений **Командная строка** необходимо определить следующие параметры: **Командная строка прародителя**, **Командная строка родителя**, **Командная строка процесса**, **Флаги**, **Издатель ЭП**, **Правила**, **Комментарий**.

Файл – в поле прописываются имена исполняемых файлов, которые необходимо добавить в исключения. Имена файлов после добавления исключения будут отображаться в таблице **Исключения для программ** в поле **Значение**, а в поле **Тип** будет указан тип исключения.

Тип хеш-суммы – в поле устанавливается тип хеш-суммы исполняемого файла. В Программе предусмотрены следующие типы хеш-сумм для добавления файлов в исключения: **SHA-256**, **SHA-1** и **MD5**. Тип хеш-суммы после добавления исключения отображается в таблице **Исключения для программ** в поле **Тип**.

Хеш-сумма – в поле прописываются значения хеш-сумм для исполняемых файлов, которые необходимо добавить в исключения. После добавления исключения значение хеш-суммы отображается в таблице **Исключения для программ** в поле **Значение.**

Командная строка прародителя – в поле прописывается значение командной строки для процесса, являющегося прародителем по отношению к процессу, для которого добавлено исключение.

Командная строка родителя – в поле прописывается значение командной строки для процесса, являющегося родителем по отношению к процессу, для которого добавлено исключение.

Командная строка процесса – в поле прописывается значение командной строки процесса, для которого назначено исключение. После добавления исключения значение командной строки отображается в таблице **Исключения для программ** в поле **Значение**.

В поле ввода командных строк допускается задание значения произвольной командной строки с помощью символа *.

Флаги – в поле определяются условия, согласно которым будут исполняться файлы, добавленные в список исключений для программ. В EDR предусмотрены следующие флаги:

1) Запрет принудительного подавления событий;
2) Разрешение внедрения кода в сторонние программы;
3) Разрешение записи памяти сторонних программ;
4) Разрешение чтения памяти сторонних программ и управления ими;
5) Компонент имеет 32-х битную и 64-х битную версию;
6) Подтверждение по электронной подписи;
7) Разрешение прямого доступа к диску для записи;
8) Разрешение прямого доступа к диску для чтения;
9) Право взаимодействия с критическими системными программами;
10) Антивирусный компонент;
11) Исключение из телеметрии сетевых событий;
12) Исключение из телеметрии файловых событий;
13) Исключение из телеметрии событий реестра Windows;
14) Исключение из телеметрии событий поведения;
15) Исключение всей телеметрии;
16) Исключение анализа файловой активности;
17) Исключение анализа входящей сетевой активности;

18) Исключение анализа исходящей сетевой активности;

19) Исключение матчинга индикаторов атак.

Все установленные для добавляемого исключения флаги будут отображаться в таблице **Исключения для программ** в поле **Флаги**.

Издатель ЭП – в поле прописывается имя издателя электронной подписи для исполняемого файла. После добавления исключения имя издателя отобразится в таблице **Исключения для программ** в поле **Издатель ЭП**.

Правила – в поле администратором или аналитиком прописывается название правила, на срабатывание которого пишется исключение, например, CmdLineTampering или Ransomware.



Важно

При добавлении исключения в поле **Издатель ЭП** и **Правила** может быть указано несколько издателей, а также несколько правил, которые разделены символом ;

Комментарий – в поле прописывается произвольный комментарий. Для добавления новой программы-исключения по имени файла или хеш-сумме комментарий не является обязательным параметром.

Комментарий после добавления исключения будет отображаться в таблице **Исключения для программ** в поле **Комментарий**.

Для завершения операции добавления исключения для программы необходимо после ввода информации в окне **Добавить исключение** нажать кнопку **Добавить**.

Процедура удаления исключений для файлов идентична процедуре удаления индикаторов компрометации.

Для внесения изменений в исключение для программы необходимо нажать кнопку **Редактировать** в соответствующей строке таблицы **Исключения для программ** и в открывшемся окне **Редактировать исключение** изменить необходимую информацию.

В зависимости от типа исключения, которое можно увидеть в поле **Тип** в таблице **Исключения для программ**, окно **Редактировать исключение** будет содержать разный набор полей, соответствующий набору полей окна **Добавить исключение**.

Для завершения редактирования необходимо нажать кнопку Сохранить после внесения изменений в редактируемый элемент. Чтобы отменить изменения, следует нажать кнопку закрытия окна ✕.

Для копирования или перемещения исключения из одного набора в другой необходимо выбрать нужные элементы и нажать кнопку **Копировать/Переместить выбранные элементы в другой набор** ( ). Далее выбрать набор, в который будет копироваться выбранный элемент. Если необходимо переместить элемент, то следует в окне **Выбор набора** установить флажок **Переместить и удалить выбранные элементы из текущего набора**. Для завершения операции необходимо нажать кнопку **Выбрать**.

Для экспорта набора с исключениями в файл следует нажать кнопку **Экспортировать набор в файл** ( ).

Далее выбрать формат, в котором будет экспортироваться набор (csv или json). Набор будет сохранен в папке **Загрузки** в выбранном формате.

Для импорта исключений из файла требуется нажать кнопку **Импортировать данные из файла в набор, поддерживаемые форматы: CSV, JSON** ( ). Далее выбрать на компьютере файл соответствующего формата, содержащий нужные правила, и нажать кнопку **Открыть**.

Чтобы активировать или деактивировать исключение из выбранного набора, необходимо нажать кнопку / или выполнить активацию/деактивацию с помощью кнопок **Активировать выбранные элементы/Деактивировать выбранные элементы** ( )

Для удаления исключений из набора необходимо отметить флажками исключения, которые требуется удалить, и нажать кнопку **Удалить выбранные** или удалить исключения по отдельности с помощью кнопки **Удалить** ( ).

8.7.2. Исключения для файлов

Общая информация

На странице **Наборы исключений для файлов** содержится список наборов с именами файлов или хеш-суммами файлов, которые добавлены в список исключений. Для таких файлов в Программе предусмотрены следующие действия: **Разрешить**, **Блокировать** и **Продолжение наблюдения**.

Наличие этой возможности позволяет администратору настроить Программу для уменьшения количества ложных срабатываний, а в случае необходимости, заблокировать тот или иной файл в целях обеспечения безопасности без создания при этом инцидента в Программе.

Наборы исключений для файлов

Страница **Наборы исключений для файлов** включает в себя следующие структурные элементы:

– таблица с наборами исключений для файлов;

– кнопка **Добавить набор**;

– кнопка **Передать все наборы агентам**;

– кнопка **Удалить выбранные наборы**.

Чтобы добавить новый набор с исключениями для файлов, необходимо нажать кнопку **Добавить набор**, после чего ввести название нового набора.

На этом этапе можно добавить к новому набору исключения для файлов из ранее сохраненных наборов. Для этого нужно выбрать соответствующий набор в строке **Базовый набор**. Для завершения операции необходимо нажать кнопку **Добавить**.

Для редактирования названий наборов применяется кнопка **Редактировать** ( ).

Чтобы удалить набор/наборы требуется отметить нужные наборы флажками и нажать кнопку **Удалить выбранные наборы** или удалить их по отдельности с помощью кнопки **Удалить** ( ).

Для перехода к странице **Исключения для файлов** необходимо нажать ЛКМ на имени набора в поле **Название набора**.

Страница «Исключения для файлов»

На странице **Исключения для файлов** можно выполнять следующие операции:

– просматривать исключения для файлов в выбранном наборе;

– добавлять новое исключение по имени файла;

– добавлять новое исключение по хешу;

– применять изменения в наборе исключений;

– копировать/перемещать выбранные исключения из одного набора в другой;

– экспортировать набор с исключениями в файл;

– импортировать исключения из файла в набор;

– активировать/деактивировать исключения в наборе;

– редактировать исключение;

– удалять выбранные исключения.

Для добавления исключения в выбранный набор необходимо нажать кнопку **Добавить исключение** и выбрать тип добавляемого исключения: **Файл** или **Хеш**. Далее в открывшемся окне **Добавить исключение** следует заполнить поля с параметрами исключения. В зависимости от выбора типа исключения окно **Добавить исключение** будет содержать поля с различными параметрами.

Для типа **Файл** необходимо определить следующие параметры: **Файл**, **Действие** и **Комментарий**.

Для типа **Хеш** следует определить следующие параметры: **Тип хеш-суммы**, **Хеш-сумма**, **Действие** и **Комментарий**.

Файл – в поле прописывается имя файла, которого необходимо добавить в исключения. Имена файлов после добавления исключения будут отображаться в таблице **Исключения для файлов** в поле **Значение**, а в поле **Тип** прописывается тип исключения. Поле является обязательным для заполнения, на что указывает значок звездочки (*).

Действие – в поле устанавливается действие в случае обнаружения файла с указанным именем или хеш-суммой. Предусмотрены следующие действия: **Разрешить**, **Блокировать** и **Продолжение наблюдения**. Выбранное действие после добавления исключения будет отображаться в таблице **Исключения для файлов** в поле **Действие.**

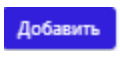
Комментарий – в поле прописывается произвольный комментарий. Для добавления нового файла-исключения по имени файла или хеш-сумме комментарий не является обязательным параметром. Комментарий после добавления исключения будет отображаться в таблице **Исключения для файлов** в поле **Комментарий**.

Тип хеш-суммы – в поле устанавливается тип хеш-суммы файла. В Программе предусмотрены следующие типы хеш-сумм для добавления файлов в исключения: **SHA-256**, **SHA-1** и **MD5**. Тип хеш-суммы после добавления исключения отображается в таблице **Исключения для файлов** в поле **Тип**.

Хеш-сумма – в поле прописываются значения хеш-сумм для файлов, которые необходимо добавить в исключения. После добавления исключения значение хеш-суммы отображается в таблице **Исключения для файлов** в поле **Значение**. Поле является обязательным для заполнения.

Для всех типов (хеш или файл) можно установить флажок **Не отправлять события**, что позволит сократить количество отправляемых на сервер событий, исключив соответствующие события выбранного типа из потока событий. Необходимо отметить, что комбинация включенного действия **Продолжение наблюдения** и отключенной опции **Не отправлять события** является недопустимой. Кроме того, для действия **Блокировать** становится активной опция **Блокировка действует и в контексте критических системных процессов**. При создании блокирующего исключения для файла возможно написать такое исключение, при срабатывании которого будет блокироваться критический системный процесс, что крайне опасно и может привести к блокировке всей работы и установке ОС в состояние «Синего экрана». При установке галочки в поле **Блокировка действует и в контексте критического системного процесса** необходимо осознавать, что описанное выше состояние допустимо и может произойти на хосте, для которого будет применяться данное блокирующее исключение. Для ОС Windows критическими системными считаются следующие процессы:

1) Процесс System (ядро ОС);
2) Процесс с ненулевым уровнем защиты (PPL, Windows 8.1+);
3) Trustlet-процесс Windows 10+ (https://learn.microsoft.com/en-us/windows/win32/procthread/isolated-user-mode--ium--processes)
4) Процессы: csrss.exe, smss.exe, lsass.exe, services.exe, wininit.exe, winlogon.exe, logonui.exe, lsm.exe, sppsvc.exe (идентифицируются по полному пути);
5) Библиотека lsm.dll (идентифицируется по полному пути) внутри хост-процесса (svchost.exe).

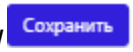
Чтобы завершить операцию **Добавить исключение**, после ввода параметров в окне **Добавить исключение** следует нажать кнопку 

.

В поле **Значение** таблицы с исключениями для файлов отображается элемент , который позволяет скопировать значение исключения в буфер обмена.

Для внесения изменений в исключение для файла необходимо нажать кнопку **Редактировать** в соответствующей строке таблицы **Исключения для файлов** и в открывшемся окне **Редактировать исключение** изменить необходимую информацию.

В зависимости от типа исключения, которое можно увидеть в поле **Тип** в таблице **Исключения для файлов**, окно **Редактировать исключение** будет содержать разный набор полей, соответствующий окну **Добавить исключение**.

Для сохранения внесенных изменений необходимо нажать кнопку 

. Для отмены изменений следует нажать кнопку **Закрыть окно** – .

Для копирования или перемещения исключения из одного набора в другой необходимо выбрать нужные элементы и нажать кнопку **Копировать/Переместить выбранные элементы в другой набор** ().

Далее выбрать набор, в который будет копироваться выбранный элемент. Если необходимо переместить элемент, то следует в окне **Выбор набора** установить флажок **Переместить и удалить выбранные элементы из текущего набора**. Для завершения операции необходимо нажать кнопку **Выбрать**.

Для экспорта набора с исключениями в файл следует нажать кнопку **Экспортировать набор в файл** ().

Далее выбрать формат, в котором будет экспортироваться набор (csv или json). Набор будет сохранен в папке **Загрузки** в выбранном формате.

Для импорта исключений из файла требуется нажать кнопку **Импортировать данные из файла в набор, поддерживаемые форматы: CSV, JSON** (). Далее выбрать на компьютере файл соответствующего формата, содержащий нужные правила, и нажать кнопку **Открыть**.

Чтобы активировать или деактивировать исключение из выбранного набора, необходимо нажать кнопку  или выполнить активацию/деактивацию с помощью кнопок **Активировать выбранные элементы/Деактивировать выбранные элементы** ()

Для удаления исключений из набора необходимо отметить флажками исключения, которые требуется удалить, и нажать кнопку **Удалить выбранные** или удалить исключения по отдельности с помощью кнопки **Удалить** ().

8.7.3. Сетевые исключения

Общая информация

На странице **Наборы сетевых исключений** представлены имена наборов исключений, в которых указываются IP-адреса и доменные имена в качестве идентификаторов при создании исключений. Предусмотрены следующие действия при создании сетевых исключений для взаимодействия с IP-адресами, URL-адресами и доменными именами: **Блокировать**, **Разрешить (всегда)**, **Продолжение наблюдения**, **Разрешить (кроме изоляции)**.

При создании сетевого исключения, действия, которые следует прописать в соответствующем поле, имеют следующий смысл:

— **Блокировать** (означает, что взаимодействие конечной точки, на которой установлен агент, с указанным в исключении IP-адресом, URL-адресом или доменным именем блокируется, при этом (в отличие от действия **Блокировать** в других индикаторах), не создается событий с критичностью, которые необходимы для создания инцидента, то есть будут создаваться события с критичностью **Низкая**;

— **Разрешить (всегда)** (означает, что взаимодействие конечной точки, на которой установлен агент, с указанным в исключении IP-адресом или доменным именем разрешается, при этом функциональность сохраняется даже тогда, когда агент изолирован);

— **Продолжение наблюдения** (означает, что взаимодействие конечной точки, на которой установлен агент, с указанным в исключении IP-адресом или доменным именем разрешается, при этом связанные с артефактом события отправляться не будут);

— **Разрешить (кроме изоляции)** (означает, что взаимодействие конечной точки, на которой установлен агент, с указанным в исключении IP-адресом или доменным именем разрешается, кроме того случая, когда конечная точка, на которой установлен агент, находится в режиме изоляции.

Использование сетевых исключений позволяет подавлять сетевые срабатывания TI-платформы или индикаторов и снижать количество анализируемой системой информации, то есть считается, что домены и ip-адреса из белого списка не нужно анализировать, это позволяет снизить нагрузку на систему.

Наборы сетевых исключений

Страница **Наборы сетевых исключений** включает в себя следующие структурные элементы:

— таблица с наборами сетевых исключений;

— кнопка **Добавить набор**;

— кнопка **Передать все наборы агентам**;

— кнопка **Удалить выбранные наборы**.

Чтобы добавить новый набор с сетевыми исключениями, необходимо нажать кнопку **Добавить набор**, после чего ввести название нового набора. На этом этапе можно добавить к новому набору исключения для файлов из ранее сохраненных наборов.

Для этого нужно выбрать соответствующий набор в строке **Базовый набор**. Для завершения операции необходимо нажать кнопку **Добавить**.

Для редактирования названий наборов применяется кнопка **Редактировать** ( ).

Чтобы удалить набор/наборы, требуется отметить нужные наборы флажками и нажать кнопку **Удалить выбранные наборы** или удалить их по отдельности с помощью кнопки **Удалить** ( ).

Для перехода к странице **Сетевые исключения** необходимо нажать ЛКМ на имени набора в поле **Название набора**.

Страница «Сетевые исключения»

На странице **Сетевые исключения** можно выполнять следующие операции:

— просматривать сетевые исключения в выбранном наборе;

— добавлять новое исключение по IP-адресу, IP-адресу и порту (так реализован на данный момент URL в Программе), доменному имени или доменному имени и порту;

— применять изменения в наборе исключений;

— копировать/перемещать выбранные исключения из одного набора в другой;

— экспортировать набор с исключениями в файл;

— импортировать исключения из файла в набор;

— активировать/деактивировать исключения в наборе;

— редактировать исключение;

— удалять выбранные исключения.

Для добавления исключения в выбранный набор необходимо нажать кнопку **Добавить исключение**, после чего откроется одноименное окно. Далее в открывшемся окне **Добавить исключение** следует заполнить поля с параметрами исключения.

Поле, отмеченное значком звездочки (*), является обязательным для заполнения. При добавлении исключения необходимо обратить внимание на флаг **Не отправлять события**, который позволяет включить или отключить функцию отправки событий, связанных с указанным артефактом. При этом в комбинациях, предусмотренных для артефактов и флага **Не отправлять события** есть недопустимая комбинация: действие **Продолжение наблюдения** и отключенная опция **Не отправлять события**.



Важно

Домен и IP-адрес могут быть написаны вместе с портом (<IP/домен>:<порт>)

Чтобы завершить операцию добавления исключения, после ввода параметров в окне **Добавить исключение** следует нажать кнопку Добавить. В одном исключении можно написать несколько доменов, URL или IP-адресов, каждое новое значение следует писать в новую строку.

В поле **Значение** таблицы с сетевыми исключениями отображается элемент , который позволяет скопировать IP-адрес, URL-адрес или доменное имя в буфер обмена.

Для внесения изменений в исключение необходимо нажать кнопку **Редактировать** в соответствующей строке таблицы **Сетевых исключений** и в открывшемся окне **Редактировать исключение** изменить необходимую информацию. Для сохранения внесенных изменений необходимо нажать кнопку Сохранить. Для отмены изменений следует нажать кнопку **Закрыть окно** – .

Для копирования или перемещения исключения из одного набора в другой необходимо выбрать нужные элементы и нажать кнопку **Копировать/Переместить выбранные элементы в другой набор** ( ).

Далее выбрать набор, в который будет копироваться выбранный элемент. Если необходимо переместить элемент, то в окне **Выбор набора** следует установить флажок **Переместить и удалить выбранные элементы из текущего набора**. Для завершения операции необходимо нажать кнопку **Выбрать**.

Для экспорта набора с исключениями в файл требуется нажать кнопку **Экспортировать набор в файл** ( ). Далее выбрать формат, в котором будет экспортироваться набор (csv или json). Набор будет сохранен в папке **Загрузки** в выбранном формате.

Для импорта исключений из файла следует нажать кнопку **Импортировать данные из файла в набор, поддерживаемые форматы: CSV, JSON** ( ). Далее выбрать на компьютере файл соответствующего формата, содержащий нужные правила, и нажать кнопку **Открыть**.

Чтобы активировать или деактивировать исключение из выбранного набора, необходимо нажать кнопку / или выполнить активацию/деактивацию с помощью кнопок **Активировать выбранные элементы/Деактивировать выбранные элементы** ( )

Для удаления исключений из набора необходимо отметить флажками исключения, которые требуется удалить, и нажать кнопку **Удалить выбранные** или удалить исключения по отдельности с помощью кнопки **Удалить** ( ).

При добавлении/редактировании исключения, если в поле, обязательном для заполнения, было введено не валидное значение, появляется надпись о некорректно введенном значении (IP-адреса или доменного имени) и исключение не будет создано. Данное утверждение представлено на рисунке 77.

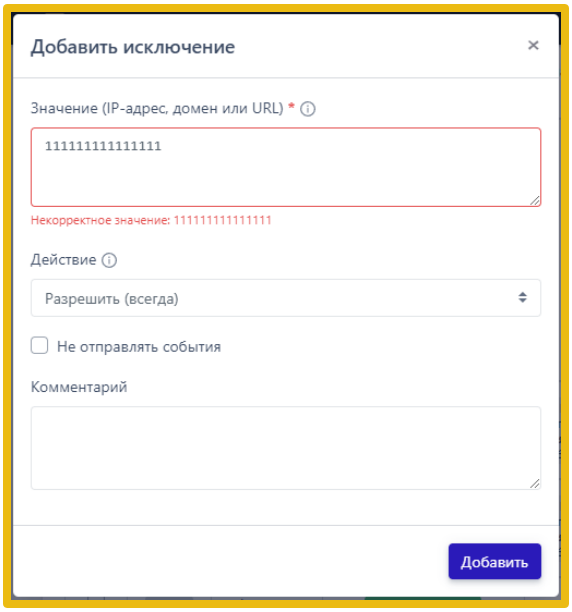


Рисунок 77 – Ввод некорректных параметров при добавлении исключения

8.7.4. Исключения индикаторов атак

Общая информация

Исключения индикаторов атак – это программные элементы, позволяющие переопределить логику индикаторов атак, то есть исключить блокирующее или детектирующее действие при совпадении с условием исключения.

Исключение работает по имени и типу индикатора, к условию которого добавляется условие исключения, поэтому важно указывать правильные имя и тип индикатора атак.

В Программе предусмотрена возможность исключать группу индикаторов атак подстановкой символа *, например, soc_indicator* будет применяться для всех правил, в имени которых содержится часть soc_indicator. Также возможна подстановка символа ?, обозначающего один любой символ.

Кроме того, в Программе предусмотрена возможность создавать универсальные по типу исключения для индикаторов атак, которые будут действовать для всех типов индикаторов атак.

Наборы исключений индикаторов атак

Страница **Наборы исключений индикаторов атак** включает в себя следующие структурные элементы:

– элементы фильтрации;

– таблица с наборами исключений для индикаторов атак;

– кнопка Добавить набор;

– кнопка Передать все наборы агентам;

– кнопка Удалить выбранные наборы.

Чтобы добавить новый набор с исключениями для индикаторов атак, необходимо нажать кнопку **Добавить набор**, после чего ввести название нового набора. На этом этапе можно добавить к новому набору исключения из ранее сохраненных наборов. Для этого нужно выбрать соответствующий набор в строке **Базовый набор**. Чтобы завершить операцию, необходимо нажать кнопку **Добавить**.

Для редактирования названий наборов применяется кнопка **Редактировать** ( ).

Чтобы удалить набор/наборы, требуется отметить нужные наборы флажками и нажать кнопку **Удалить выбранные наборы** или удалить их по отдельности с помощью кнопки **Удалить** ( ).

Для перехода к странице **Исключения индикаторов атак** необходимо нажать ЛКМ на имени набора в поле **Название набора**.

Страница «Исключения индикаторов атак»

На странице **Исключения индикаторов атак** можно выполнять следующие операции:

– просматривать исключения индикаторов атак в выбранном наборе;

– добавлять новое исключение индикатора атак;

– применять изменения в наборе исключений;

– копировать/перемещать выбранные исключения из одного набора в другой;

– экспортировать набор с исключениями в файл;

– импортировать исключения из файла в набор;

– активировать/деактивировать исключения в наборе;

– редактировать исключение;

– удалять выбранные исключения.

Для добавления исключения в выбранный набор необходимо нажать кнопку **Добавить исключение**, после чего откроется одноименное окно. Далее в открывшемся окне **Добавить исключение** следует заполнить поля с параметрами исключения. Поле, отмеченное значком звездочки (*), является обязательным для заполнения. Добавить условие исключения индикатора атак можно как вручную, так и с помощью конструктора. Также, как и для индикаторов атак, в исключениях для них доступна функция проверки синтаксиса.

Чтобы завершить операцию добавления исключения, после ввода параметров в окне **Добавить исключение** следует нажать кнопку Добавить.

Для внесения изменений в исключение необходимо нажать кнопку **Редактировать** в соответствующей строке таблицы **Исключений индикаторов атак** и в открывшемся окне **Редактировать исключение** изменить необходимую информацию. Для сохранения внесенных изменений необходимо нажать кнопку Сохранить. Для отмены изменений следует нажать кнопку **Закрыть окно** – .

Для копирования или перемещения исключения из одного набора в другой необходимо выбрать нужные элементы и нажать кнопку **Копировать/Переместить выбранные элементы в другой набор** ( ). Далее выбрать набор, в который будет копироваться выбранный элемент.

Если необходимо переместить элемент, то следует в окне **Выбор набора** установить флажок **Переместить и удалить выбранные элементы из текущего набора**. Для завершения операции необходимо нажать кнопку **Выбрать**.

Для экспорта набора с исключениями в файл следует нажать кнопку **Экспортировать набор в файл** ( ). Далее выбрать формат, в котором будет экспортироваться набор (csv или json). Набор будет сохранен в папке **Загрузки** в выбранном формате.

Для импорта исключений из файла требуется нажать кнопку **Импортировать данные из файла в набор, поддерживаемые форматы: CSV, JSON** ( ). Далее выбрать на компьютере файл соответствующего формата, содержащий нужные правила, и нажать кнопку **Открыть**.

Чтобы активировать или деактивировать исключение из выбранного набора, необходимо нажать кнопку / или выполнить активацию/деактивацию с помощью кнопок **Активировать выбранные элементы/Деактивировать выбранные элементы** ( )

Для удаления исключений из набора необходимо отметить флажками исключения, которые требуется удалить, и нажать кнопку **Удалить выбранные** или удалить исключения по отдельности с помощью кнопки **Удалить** ( ).

8.8 Профили

В области **Профили** администратор Программы может настраивать профили агента. Настройка профилей позволяет управлять Антишифром, управлять модулем контроля USB, оптимизировать количество событий, поступающих от агента, настраивать работу AMSI, и т.д. При изменении настроек профиля можно воспользоваться кнопкой отмены изменений ( ). При нажатии кнопки все ранее сделанные изменения в этом профиле будут отменены, при этом необходимо учитывать, что переход на другую страницу после внесения изменений сохраняет их, отменить эти изменения с помощью кнопки будет уже нельзя.

8.8.1. Профиль Антишифра

В современном цифровом мире киберугрозы становятся все более изощренными и опасными. Одной из самых серьезных проблем для организаций и частных пользователей являются ransomware-атаки, или атаки шифровальщиков. Эти вредоносные программы шифруют данные на устройствах жертв, требуя выкуп за их расшифровку. В таких условиях необходимо использовать специализированные решения, такие как модули противодействия шифровальщикам, которые способны предотвратить или минимизировать ущерб от ransomware-атак.

Модуль Антишифра прежде всего направлен на защиту от угроз нулевого дня, выполняя перехват и эвристический анализ файловой активности каждого процесса в системе в режиме реального времени.

Это позволяет выявлять характерные для шифровальщиков паттерны поведения, после чего блокировать их действия.



Важно

Режим «только детектирование» не распространяется на работу модуля Антишифр.

Модуль защиты от шифровальщиков (Антишифр) является важной частью RT Protect EDR: он останавливает работу шифровальщиков на компьютерах с установленным агентом Windows в режиме реального времени, позволяя защищать все каталоги системы от шифрования. Данное утверждение справедливо для третьих версий агентов и выше. Модуль Антишифра можно включать как с активным модулем ремедиации, так и без него (модуль ремедиации появляется в версиях программы 4.0, соответственно для третьих версий и ниже описания, касающиеся модуля ремедиации, неактуальны).



Важно

Антишифр работает только в агентах Windows.

Антишифр позволяет настраивать модуль ремедиации (модуль выполняет функции отката действий, выполненных вредоносной программой на определенный период времени, но не более, чем на 72 часа). Под настройками модуля понимается возможность включения тестового режима работы модуля, сохранения

данных для восстановления реестра, возможность отправлять события создания резервной копии для операций резервирования файлов, возможность установить максимальное время хранения резервных копий, максимального размера резервируемых файлов и возможность установить процент доступного для заполнения резервными копиями дискового пространства.

Управление модулем Антишифра осуществляется с помощью профилей.

– экспортировать настройки профиля Антишифра в файл формата TXT;

– импортировать настройки из ранее экспортированного профиля Антишифра (поддерживаются файлы в формате TXT).

Информация о профилях Антишифра представлена в табличном виде. В таблице отображаются следующие поля:

– Название профиля;

– Привязано агентов;

– **Управление** (здесь находятся кнопки редактирования, удаления и сохранения профилей – ).

Чтобы создать новый профиль Антишифра, необходимо нажать кнопку Добавить профиль и в открывшемся окне ввести название нового профиля, после чего нажать кнопку Добавить (рис. 78).

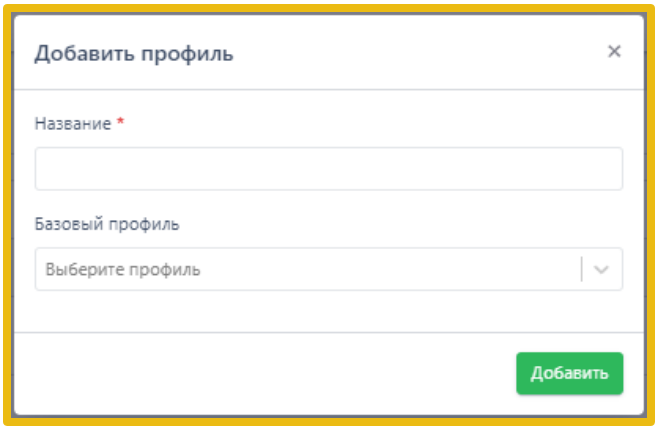


Рисунок 78 – Добавление профиля Антишифра

Если новый профиль Антишифра требуется создать на основе ранее сохраненного, то в поле выбора **Базовый профиль** следует назначить из выпадающего списка один из существующих профилей Антишифра и нажать кнопку Добавить.

С помощью кнопки **Редактировать** ( ) можно изменить название профиля (рис. 79).

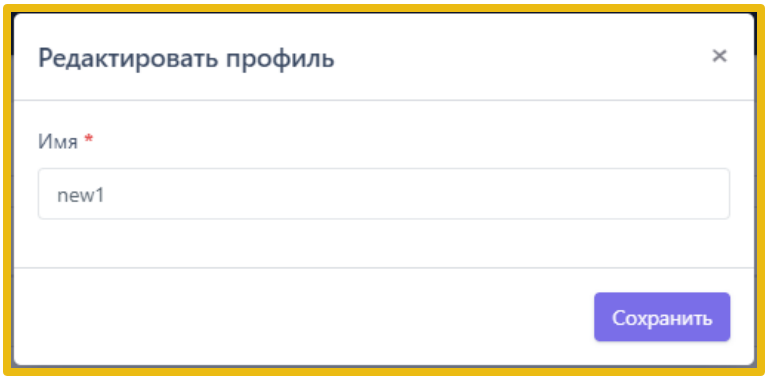


Рисунок 79 – Редактирование названия профиля Антишифра

Значок рядом с названием профиля или сверху страницы сообщает пользователю о том, что один или несколько профилей Антишифра не применены, для корректной работы их необходимо передать агентам с помощью кнопки **Передать все профили агентам** ( ).

Для удаления профиля или нескольких профилей Антишифра необходимо отметить их флажками и нажать кнопку **Удалить выбранные**.

Если требуется установить параметры защиты данных, отличающиеся от параметров существующих профилей Антишифра, то следует нажать название профиля, после чего откроется страница **Профиль Антишифра**.

Тестовый режим ремедиации – позволяет переключаться между тестовым и основным режимом работы. Тестовый режим отличается от основного режима тем, что реальная резервная копия файла не создаётся, при этом все остальные механизмы, такие как протоколирование изменений, связанные с именами файлов и реестра, отправка событий о занятости внутреннего хранилища, а также отправка событий об успешном резервировании файла осуществляется, хотя резервирования как такового в этом случае не происходит. Нужно это для того, чтобы оценить, какие файлы и в каком количестве будут резервироваться, какими процессами они вызываются. На основе этой аналитики можно для определённых доверенных

процессов отключить резервирование. Это похоже на работу режима **Только детектирование** в **Профиле безопасности агента**. Основные различия между тестовым и штатным режимом работы модуля ремедиации приведены в таблице 51.

Таблица 51 – Различия между тестовым и штатным режимом ремедиации

Опция	Штатный режим	Тестовый режим
Реальные копии файлов/реестра	Создаются	Не создаются
Резервирование имен/каталогов	Да	Да (модуль считает, сколько файлов и какого суммарного объема он бы сохранил, но данные на диск не пишет))
Фильтрация по размеру файла	Да	Да
Отправка событий	Да	Да
Завершение процессов-шифровальщиков	Да	Нет
Расход дискового пространства	Да	Минимальный
Назначение	Защита	Оценка нагрузки и настройка политик

Флаг **Защита при нехватке свободного места** запрещает любые изменения файлов, если на диске недостаточно места для их резервного копирования. Это не дает шифровальщикам уничтожить оригиналы данных, когда создать резервную копию невозможно.

Существует тип атаки, когда вредонос сначала выделяет всё свободное место на диске, чтобы установленная система резервирования не могла создать резервную копию, после чего начинает шифровать файлы «поверх» оригиналов. Если опция включена, модуль ремедиации заблокирует любую попытку изменения файла, если на диске нет места для его резервной копии. Данные останутся в безопасности.

Флаг **Резервирование альтернативных потоков данных (ADS)** включает резервирование дополнительных метаданных и потоков NTFS (Alternate Data Streams). Если отключено, резервируется только основное содержимое файла. В файловых системах вроде NTFS у одного файла может быть несколько независимых наборов данных. Обычный пользователь видит через Проводник только основной поток. Альтернативные потоки скрыты и явно не отображаются, но в них тоже хранятся данные, которые необходимы приложениям для нормальной работы. Эта опция заставляет систему резервировать все потоки, которые есть у файла.

Флаг **Резервирование прав доступа файлов** определяет необходимость сохранения оригинальных прав доступа к файлам. Опция отвечает за сохранение дескрипторов безопасности (то есть прав доступа) при попытке их поменять. Злоумышленники часто удаляют дескриптор безопасности у файлов и операционная система сама блокирует пользователю доступ к его же собственным файлам. При включенной опции модуль ремедиации сохраняет оригинальную копию прав доступа и при необходимости восстанавливает их.

Флаг **Сохранять данные для восстановления реестра Windows** – опция управляет механизмом создания резервных копий ключей реестра Windows перед внесением в него изменений. Это позволяет откатить нежелательные или вредоносные изменения, возвращая параметры системы в рабочее состояние в случае их повреждения.

Флаг **Отправлять события "Создана резервная копия" для операции резервирования файлов** определяет необходимость отправки на сервер события **Антишифр: Создана резервная копия**. Если флаг снят, то такие события отправляться не будут. На странице **Активность** всегда можно будет увидеть, какие файлы можно восстановить при ремедиации и в рамках каких процессов они создавались. Важный нюанс: для изменений в реестре такие события на сервер не отправляются, они фиксируются только для файлов.

Поле **Максимальное время хранения резервных копий (в часах)** Определяет максимальное время хранения резервных копий файлов и данных реестра Windows. По истечении этого срока устаревшие данные удаляются. Важно: если выделенное под хранилище место закончится раньше, старые копии будут удалены принудительно для освобождения пространства. Допустимое значение: от 1 до 72 часов. По истечении этого времени, резервные копии файлов и реестра, которые были созданы раньше, будут удалены. В целом рекомендованное значение максимального времени хранения резервных копий желательно устанавливать в диапазоне от 12 до 16 часов. Необходимо также помнить, что чем более длительный срок для востановления копий мы указываем, тем меньше вероятность успешного восстановления копий, которые были зарезервированы в первую очередь. Вероятность полного восстановления копий, которые были зарезервированы 70 часов назад, ниже, чем вероятность полного восстановления копий, которые были зарезервированы 5 часов назад.

Поле **Максимальный размер резервируемого файла (МБ)** определяет максимальный размер резервируемого файла в мегабайтах. Если размер резервируемого файла будет превышать размер указанного

значения, то такой файл резервироваться не будет. Значение является 32 битным, беззнаковым числом. При нулевом значении ограничения на размер не осуществляются.

Поле **Квота доступного дискового пространства (%)** определяет размер дискового пространства, которое предоставляется модулю ремедиации для хранения резервных копий и служебной информации. Это значение задаётся в процентном соотношении от размера раздела, на котором включено резервирование. Важно помнить, что значение будет рассчитываться и применяться для каждого раздела отдельно. Значение задаётся в диапазоне от 1 до 30. Квотирование и ремедиация недоступны для FAT и FAT32, а также в разделах USB-накопителей.

Как работает ремедиация?

Ремедиация – это процесс восстановления затронутых шифровальщиком файлов и ключей/значений реестра в программе RT Protect EDR.

Модуль ремедиации работает по принципу «сначала зарезервируй, а потом дай изменить». Он прозрачно создаёт резервные копии файлов и ключей реестра Windows перед тем, как их кто-то изменит или удалит. Если потом окажется, что изменения сделал шифровальщик/вредонос, оператор EDR может вернуть систему к исходному состоянию — восстановить зашифрованные/удалённые файлы и повреждённые ветки реестра.

Главное правило работы модуля ремедиации – если процесс из одного узла пытается изменить или удалить файл, который создал другой узел, то модуль ремедиации сразу делает резервную копию этого файла. Копия изменяемого файла для этого узла будет сделана единожды, сколько бы раз узел в этот файл не писал.

Все журналы и резервные копии хранятся локально, на том томе, где происходили изменения. Данные не уходят в облако или по сети. Например, при удалении файла с диска D, резервная копия сохранится на ээтом же диске.При этом само хранилище резервных копий защищено драйвером агента. Его нельзя прочитать, изменить или удалить. Шифровальщик не сможет получить доступ к резервным копиям в ходе атаки, и если он попытается это сделать, то драйвер заблокирует операцию.

Для пользователя ремедиация производится в две фазы:

1) Автоматическая защита/резервирование в фоне;
2) Ручное восстановление по требованию при расследовании инцидента.

После того как администратор включил модуль и подсистему Ремедиации в профиле Антишифра и передал его агентам, на конечной точке начинает работать фоновая защита:

– при любой попытке изменить/удалить защищаемый файл агент сначала передает его оригинал в локальное хранилище резервных копий и только затем разрешает операцию, то же самое происходит для ключей реестра перед их изменением;

– каждое такое резервирование может порождать в EDR событие «Антишифр: Создана резервная копия файла», аналитик может увидеть эти события на странице **Активность** и понять, что объект защищён и его можно восстановить.

– резервные копии хранятся ограниченное время и в пределах квоты диска.

Когда инцидент обнаружен, например, видны массовые модификации файлов или сработало правило по шифровальщику, аналитик инициирует восстановление.

Чтобы восстановить файлы и ключи реестра, можно воспользоваться тремя инструментами:

1) Сценарий реагирования на странице **Процесс**;
2) Нативная команда **remed** в онлайн-терминале;
3) Запуск задачи в Планировщике задач.

Во всех случаях прежде всего необходимо определить любой процесс из вредоносной группы для которой планируется сделать ремедиацию. Необходимо помнить, что изменения всегда отменяются для всех процессов группы целиком . Проще всего найти процесс из вредоносной группы в событиях **Инцидента**. Здесь можно сразу перейти на страницу **Процесс**, кликнув по имени процесса из вредоносной группы, и воспользоваться первым в списке инструментом – дефолтным сценарием реагирования, который активируется кнопкой **Реагирование.** Но сначала нужно выбрать соответствующую вредоносную группу процессов (на странице **Процесс** идентификатор группы обозначается иконкой ). После нажатия кнопки Реагирование необходимо выбрать операцию ремедиации. Откроется окно, в котором автоматически будет установлен **hid** логической группы, которая объединяет несколько совместно работающих процессов и время, в течение которого была активной группа процессов (если работа группы была завершена), в противном случае (если время не установлено), то его необходимо выставить вручную, используя календарь (но не более, чем на 72 часа назад или на время, установленное в профиле Антишифра).

Важно

При необходимости можно сделать корректировку времени. Для чего это нужно? Представьте ситуацию: легитимный процесс работал 3 дня, а заразился из-за уязвимости всего 10 минут назад.

Если откатить работу за все три дня , то можно потерять значительный объем данных, восстановленных из сильно устаревших копий, поэтому лучше сузить диапазон вручную, чтобы отменить только операции, который произвел шифровальщик после заражения.

После выбора временного диапазона пользователю останется только определить, какие операции следует отменить (операции с файлами вместе с ключами реестра, файлами или ключами реестра по отдельности) и нажать кнопку **Отправить**.

На странице агента в области **Запуски задач агента** в то же время создается запуск, по которому можно отследить вывод команды: наименование команды, сколько операций сделал модуль ремедиации. Тут речь идёт не о количестве восстановленных файлов и ключей реестра, а именно об отменённых изменениях. Под операцией подразумевается, например, создание файла, переименование файла, восстановление файла из резервной копии. Если шифровальщик зашифрует 1 файл, 8 только переименует, а один создаст, то в сообщении будет фигурировать, что отменено именно 10 операций. Аналогичным образом будут отображаться операции с реестром (рис. 80).

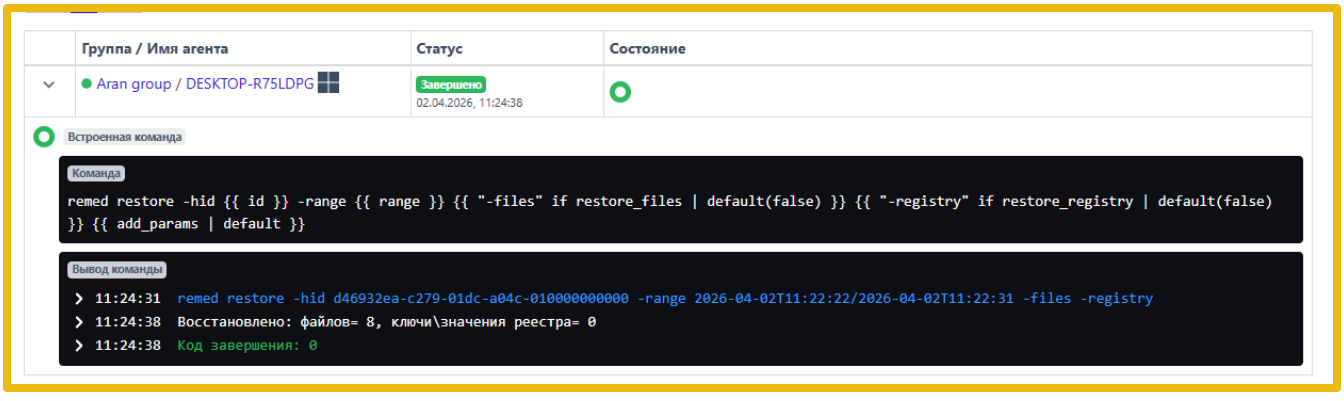


Рисунок 80 – Вывод запуска задачи на агенте

То есть ремедиация подразумевает, что созданные вредоносом файлы и ключи реестра будут удалены, переименованные файлы и ключи реестра получат исходное имя и место расположения, а удалённые или зашифрованные восстановятся к первоначальному виду из резервной копии.

При работе с командой в онлайн-терминале и создании сценария в планировщике задач алгоритм действия такой же – определить hid группы процессов, совершавшей вредоносные действия, указать временной период, на который будет выполнена ремедиация, определить, какие операции будут отменены (операции с файлами, реестром или и то, и другое), после чего написать соответствующую команду и выполнить её, а для сценария в планировщике задач необходимо создать задачу, после чего также запустить её.

8.8.2. Профили безопасности агента

На странице **Профили безопасности агента** администратор может создавать и редактировать профили, с помощью которых для верифицированных агентов устанавливаются параметры безопасности.

В соответствии с этими параметрами будут формироваться события и инциденты, присылаемые агентом в модуль администрирования.

Набор инструментов для работы с профилями не отличается от набора инструментов для настроек профилей защиты данных или создания и редактирования наборов индикаторов компрометации, атак и т.д.

Администратор может выполнить следующие операции на странице **Профили безопасности агента**:

1) Добавить новый профиль безопасности;
2) Сохранить изменения в профиле и передать изменения агентам, которым назначен выбранный профиль;
3) Редактировать название профиля безопасности;
4) Удалить один или несколько профилей безопасности.

Чтобы изменить параметры безопасности, администратору необходимо выбрать профиль безопасности агента и настроить его в соответствии с требованиями организации-заказчика.

Профиль безопасности агента

На странице **Профиль безопасности агента** аналитик может настроить параметры, в соответствии с которыми будут обнаруживаться события на агентах. Такая предварительная настройка позволит управлять нагрузкой на систему.

Настройки профиля безопасности агента подразделяются на следующие группы:

– параметры оптимизации потока событий;

– фильтрация WMI-событий;

– общие настройки безопасности;

– параметры безопасности монитора процессов;

– настройки AMSI;

– параметры безопасности файлового монитора;

– настройки противодействия сетевым атакам;

– настройки безопасности сетевого монитора;

В нижней части страницы находятся кнопки применения настроек, экспорта и импорта профиля безопасности (). Экспорт и импорт файла осуществляется в формате txt.

В области **Оптимизация потока событий** аналитик может управлять отправкой с агентов следующих событий:

1) Исключать файловые события ранней стадии запуска процессов;
2) Фильтровать файловые события;
3) Исключать файловые события префетчера;
4) Исключать события чтения исполняемых файлов, связанные с их исполнением;
5) Исключать события чтения исполняемых файлов;
6) Исключать события чтения любых файлов;
7) Исключать файловые события процесса-создателя файла;
8) Исключать события изменения параметров безопасности файлов;
9) Исключать события доступа к процессам и нитям;
10) Исключать события загрузки известных модулей;
11) Исключать события установки сетевых соединений для протокола DNS;

12) Исключать события завершения сетевых соединений;

13) Фильтровать события модификации реестра;

14) Исключать события RPC-вызовов;

15) Исключать события со статусом «Разрешено» (кроме ключевых);

16) Исключать все события со статусом «Разрешено»;

17) Оптимизировать поток файловых событий;

18) Оптимизировать поток сетевых событий;

19) Оптимизировать поток событий межпроцессного взаимодействия;

20) Оптимизировать поток событий реестра.

Установив или сняв определенные флаги, аналитик может увеличить или уменьшить количество событий, присылаемых агентом в модуль администрирования. Это позволяет снизить информационный шум или, наоборот, увеличить отображаемую активность, чтобы изучить ее в полном объеме.

После настроек оптимизации потока событий пользователь может также настроить фильтрацию по WMI-событиям. Для WMI доступны три способа фильтрации:

1) По вызову метода;

2) По созданию процесса;

3) По ключевым словам, указанным в профиле безопасности.

В добавление к вышеуказанным методам фильтрации в профиле добавлена опция для отключения генерации событий WMI. Для этого необходимо выбрать пункт фильтрации **Не отправлять события**.

Ключевые слова задаются аналитиком по принципу включения/исключения подстрок, то есть можно задать, какие слова должны содержать строки WMI-запросов, или можно задать, какие слова при фильтрации событий, поступающих от WMI, строки запросов содержать не должны.

С помощью общих настроек безопасности аналитик может установить режим «только детектирование», который позволяет отключить противодействие угрозам в режиме реального времени, то есть действия, которые могут нанести вред защищаемой инфраструктуре не будут блокироваться, но при этом не будет и ложноположительных срабатываний, которые могут привести к запрету на запуск какой-либо полезной программы, действия которой EDR может посчитать нелегитимными в соответствии со своими внутренними правилами или правилами, созданными пользователями Программы.

Важно

Режим «только детектирование» не распространяется на работу блокирующих исключений, то есть действие «блокировать», установленное по отношению к исключениям для программ, файлов или сетевых исключений будет исполняться, несмотря на выбор этого режима.

Кроме того, в общих настройках доступна опция **Принудительное подавление событий процессов при превышении лимита**.

В области **Настройки безопасности монитора процессов** администратор может настроить реакции Программы на события определенного типа:

– создание нити в стороннем процессе (кроме авторизованных программ Windows);

– доступ к стороннему процессу/нити (кроме авторизованных программ Windows.

Доступны следующие реакции:

1) Разрешить;

2) Блокировать только для неподписанных программ;

3) Блокировать.

При выборе реакции **Блокировать** события соответствующего типа будут отображаться в разделе **Инциденты**, а их активность будет блокироваться Программой. Кроме того, для событий создания нити в стороннем процессе и доступа к стороннему процессу/нити возможно настроить уровень важности, который соответствует уровню критичности события (от уровня **Информация** до уровня **Критичный**).

Для безопасности файлового монитора в Программе предусмотрена настройка реакции на прямой доступ к жесткому диску (кроме авторизованных программ Windows), а также выбор режима глубокого сканирования файлов.

Аналитик может выбрать для профиля безопасности одну из следующих реакций на события прямого доступа к жесткому диску:

– Блокировать;

– Блокировать запись;

– Блокировать запись только для неподписанных программ;

— Разрешить.



Примечание

Список программ с доверенными подписями содержит проверенное общеупотребительное ПО.

Также в настройках безопасности файлового монитора можно установить флаги **Подсчитывать хеш SHA-1**, **Подсчитывать хеш MD5** и **Подсчитывать хеш Imphash**. По умолчанию эти функции отключены, так как создают существенную нагрузку на файловый монитор и на работу ОС соответственно.

В случае выбора режима «только детектирование» изменение настроек безопасности монитора процессов и файлового монитора будет заблокировано, за исключением выбора режима глубокого сканирования файлов. Доступно четыре режима глубокого сканирования файлов:

1) Не сканировать;
2) **ML** (сканирование с помощью машинного обучения);
3) **YARA-правила** (сканирование на основе YARA-правил, созданных в разделе с аналитикой);
4) **ML и YARA-правила** (сканирование и с помощью машинного обучения, и с помощью YARA-правил).

В наборе **По умолчанию** устанавливается режим **Не сканировать**, чтобы снизить нагрузку на файловый монитор. Кроме того, пользователь может задать расширения файлов с потенциально активным содержимым. Это позволит расширить набор обрабатываемых сканером файлов, то есть добавить к базовым PE-файлам, которые обрабатываются по умолчанию, файлы с указанными здесь расширениями, например, PDF, PS1, PSM1, TXT и т.д. Нежелательно указывать здесь расширения для PE-файлов, например, EXE, так как эти файлы сканируются Программой по умолчанию.



Примечание

Ввод нескольких значений в поле **Расширения файлов с потенциально активным содержимым** осуществляется через разделитель |, а в поле **IP-адреса клиентов, DNS-запросы которых не обрабатываются и исключаются из телеметрии** осуществляется через разделитель ;.

Если включен режим глубокого сканирования, то активируется опция сканирования исполняемых файлов. Администратор может выбрать проверять все исполняемые файлы, сканировать файлы без электронной подписи или сканировать файлы без доверенной электронной подписи.



Совет

Не рекомендуется включать глубокое сканирование в случае совместной работы с антивирусами сторонних вендоров. Это создает значительную нагрузку на файловую систему.

Кроме указанных выше настроек в Программе предусмотрены настройки безопасности сетевого монитора. Настройки безопасности сетевого монитора включаются и отключаются флагами **Активная защита от сканирования сетевых портов, Запретить входящие сетевые подключения, Отправлять события ICMP**. Также в настройках безопасности сетевого монитора находится поле **IP-адреса клиентов, DNS-запросы которых не обрабатываются и исключаются из телеметрии**.

Чтобы логика настроек применялась на агентах, для которых установлен профиль безопасности, после его изменения необходимо нажать кнопку **Передать профиль агентам** ( ).

В некоторых случаях профиль безопасности может иметь некорректный или устаревший формат, его можно исправить, нажав кнопку **Восстановить по умолчанию** или **Актуализировать профиль**. Актуализация профиля необходима, если в профиле безопасности появляются новые параметры со значениями по умолчанию.

Подробное описание опций профиля безопасности агента

Оптимизация потока событий

Исключать файловые события ранней стадии запуска процессов.

Ранней стадией запуска процессов считается период разворачивания процесса с момента его старта и до момента начала загрузки им критических системных библиотек (например, ntdll, kernel32 и т.п. в Windows). Если данная опция выставлена, то в обозначенный период файловые события процессов отправляться не будут. Считается, что в этот период работает только код системного загрузчика процессов, а его файловые события нерелевантны в контексте ИБ.

Фильтровать файловые события.

Если данная опция выставлена, то из потока исключаются следующие файловые события:

– Windows:

1) операции чтения для файлов desktop.ini, *.mui, *.manifest, *.icm со стороны любых процессов;
2) операции чтения для файлов tzres.dll, stdole2.tlb, sortdefault.nls, hosts, *.ttf в системном каталоге (подкаталоге) со стороны любых процессов;
3) операции чтения/записи файлов в каталогах (подкаталогах) c:\users\<username>\appdata\{local|locallow|roaming}со стороны процессов браузеров;
4) операции с именованными каналами mojo.*, crashpad_*, wkssvc со стороны процессов браузеров.

Исключать файловые события префетчера.

Префетчер – это компонент ОС, ускоряющий запуск процессов за счет предподготовки определенных данных. Если данная опция выставлена, то файловые события префетчера отправляться не будут. Поскольку префетчер – это доверенный системный компонент, работающий на начальном этапе разворачивания процессов, его файловые события нерелевантны в контексте ИБ.

Исключать события чтения исполняемых файлов, связанные с их исполнением.

Для загрузки исполняемых файлов ОС производит их чтение с диска. Агент может отличить обычное чтение файлов (в т.ч. исполняемых), которое может выполнять любой процесс, от чтения с целью исполнения их кода, которое выполняет сама система, что является менее значимым в контексте ИБ. Поэтому предусмотрена опция, позволяющая полностью исключить из потока подобные файловые события.

Исключать события чтения исполняемых файлов.

Система или процессы могут производить чтение исполняемых файлов для тех или иных целей, например, доступ к ресурсам (исполняемые файлы Windows в формате PE) или получение файловых метаданных. Данная опция позволяет исключить из потока такие файловые события.

Исключать события чтения любых файлов.

Данная опция позволяет безусловно исключить из потока любые события чтения любых файлов. Поскольку события чтения файлов являются одними из самых массовых, исключение их из потока существенно (кратно) сокращает событийный трафик, однако может сократить возможности аналитика по расследованию инцидентов ИБ.

Исключать файловые события процесса-создателя файла.

Если тот или иной процесс создает новый файл на диске, то он в дальнейшем, как правило, записывает в него какие-то данные. Сам факт создания нового файла в большинстве случаев уже является достаточным в контексте ИБ, поэтому дальнейшую файловую активность процесса-создателя файла в отношении созданного им файла можно исключить, установив данную опцию.

Исключать события изменения параметров безопасности файлов.

Данная опция позволяет исключить из потока события изменения параметров безопасности файлов: изменение владельца, основной группы владельца файла, списка избирательного управления доступом (DACL), системного списка управления доступом (SACL) и уровень целостности файла (MIC/Integrity level).

Исключать события доступа к процессам и нитям.

Данная опция позволяет безусловно исключить из потока любые события межпроцессного взаимодействия. Поскольку события межпроцессного взаимодействия являются достаточно частыми, исключение их из потока существенно сокращает событийный трафик, однако может сократить возможности аналитика по расследованию инцидентов ИБ.

Исключать события загрузки известных модулей.

Данная опция позволяет исключать из потока события загрузки «известных» исполняемых модулей. Поскольку события загрузки исполняемых модулей множатся событиями старта процессов, данная оптимизация позволяет существенно сократить поток событий.

К «известным» модулям относятся следующие модули:

– модули, подписанные Microsoft Windows или Microsoft Corporation;

– модули, чьи хеши или имена файлов внесены в файловые исключения, назначенные агенту, со статусом «Разрешено»;

– следующие модули Windows:

1) %systemdisk%\windows\system32\shcore.dll;
2) %systemdisk%\windows\system32\sechost.dll;
3) %systemdisk%\windows\system32\rpcrt4.dll;
4) %systemdisk%\windows\system32\combase.dll;
5) %systemdisk%\windows\system32\ntdll.dll;

6) %systemdisk%\windows\system32\wow64.dll;
7) %systemdisk%\windows\system32\wow64win.dll;
8) %systemdisk%\windows\system32\wow64cpu.dll;
9) %systemdisk%\windows\system32\kernel32.dll;
10) %systemdisk%\windows\system32\kernelbase.dll;
11) %systemdisk%\windows\system32\advapi32.dll;
12) %systemdisk%\windows\system32\msvcrt.dll;
13) %systemdisk%\windows\system32\ucrtbase.dll;
14) %systemdisk%\windows\system32\gdi32.dll;
15) %systemdisk%\windows\system32\user32.dll;
16) %systemdisk%\windows\system32\win32u.dll;
17) %systemdisk%\windows\system32\comdlg32.dll;
18) %systemdisk%\windows\WinSxS*\comdlg32.dll;
19) %systemdisk%\windows\system32\comctl32.dll;
20) %systemdisk%\windows\WinSxS*\comctl32.dll;
21) %systemdisk%\windows\system32\shell32.dll;
22) %systemdisk%\windows\system32\shlwapi.dll;
23) %systemdisk%\windows\system32\oleaut32.dll;
24) %systemdisk%\windows\system32\version.dll;
25) %systemdisk%\windows\system32\imm32.dll;
26) "%systemdisk%\windows\system32\winmm.dll";
27) "%systemdisk%\windows\system32\ws2_32.dll";
28) "%systemdisk%\windows\system32\mswsock.dll";
29) "%systemdisk%\windows\system32\setupapi.dll";
30) "%systemdisk%\windows\system32\dwmapi.dll";
31) "%systemdisk%\windows\system32\winspool.drv";
32) "%systemdisk%\windows\system32\msctf.dll";
33) "%systemdisk%\windows\system32\uxtheme.dll";

34) "%systemdisk%\windows\system32\userenv.dll";

35) "%systemdisk%\windows\system32\msimg32.dll";

36) "%systemdisk%\windows\system32\usp10.dll";

37) "%systemdisk%\windows\system32\lpk.dll";

38) "%systemdisk%\windows\system32\mscoree.dll";

39) "%systemdisk%\windows\system32\bcrypt.dll";

40) "%systemdisk%\windows\system32\sspicli.dll";

41) "%systemdisk%\windows\system32\sxs.dll";

42) "%systemdisk%\windows\system32\windows.storage.dll";

43) "%systemdisk%\windows\system32\wininet.dll";

44) "%systemdisk%\windows\system32\ole32.dll";

Для ОС семейства Linux точный путь до каждого модуля индивидуален для конкретной ОС (Ubuntu, RedOs, Debian и т. д.).

Ниже представлен перечень модулей (слева) и пример пути для ОС Ubuntu 20.04 (справа).

1) libcap – /usr/lib/x86_64-linux-gnu/libcap-ng.so.*;
2) libpcre – /usr/lib/x86_64-linux-gnu/libpcre.so.*;
3) libpthread – /usr/lib/x86_64-linux-gnu/libpthread-*.so;
4) librt – /usr/lib/x86_64-linux-gnu/librt-*.so;
5) libcrypt – /usr/lib/x86_64-linux-gnu/libcrypt.so.*;
6) libcrypto – /usr/lib/x86_64-linux-gnu/libcrypto.so.*;
7) libdl – /usr/lib/x86_64-linux-gnu/libdl-*.so;
8) libgcc – /usr/lib/x86_64-linux-gnu/libgcc_s.so.*;
9) libm – /usr/lib/x86_64-linux-gnu/libm.so;
10) libc – /usr/lib/x86_64-linux-gnu/libc-*.so, /usr/lib/x86_64-linux-gnu/libc.so;
11) libstdc++ – /usr/lib/x86_64-linux-gnu/libstdc++.so.*;
12) libz – /usr/lib/x86_64-linux-gnu/libz.so.*;
13) libzstd – /usr/lib/x86_64-linux-gnu/libzstd.so.*;
14) libselinux – /usr/lib/x86_64-linux-gnu/libselinux.so.*.

Исключать события установки сетевых соединений для протокола DNS.

Данная опция управляет отправкой событий входящих и исходящих подключений к UDP-порту 53 (протокол DNS).

Как правило, сами события подключения к DNS-серверу имеют малую практическую ценность, поэтому для сокращения трафика могут исключаться из потока.

Исключать события завершения сетевых соединений.

Данная опция управляет отправкой событий завершения соединений. Данные события являются парными для событий установки входящих и исходящих соединений и, таким образом, могут создавать большой поток, поэтому для сокращения трафика могут исключаться из потока.

Фильтровать события модификации реестра.

Данная опция управляет режимом отправки событий модификации значений реестра Windows. Если опция установлена, то отправляются только события модификации релевантных с точки зрения ИБ значений реестра (точки автозапуска, настройки безопасности, опции групповых политик и др. – конкретный перечень может меняться от версии к версии агента), что сокращает поток событий без существенного ухудшения защитных свойств системы.

Если опция не установлена, то отправляются все без исключения события модификации значений реестра.

Исключать события RPC-вызовов.

Опция позволяет исключить из потока события источника **Вызовы: RPC**.

Исключать события со статусом "Разрешено" (кроме ключевых).

Статус «Разрешено» назначается событиям в результате действия исключений (заданных аналитиком или встроенных в агент). Данная опция позволяет исключать из потока те из событий со статусом «Разрешено», у которых нет ассоциированного с ними правила.

Исключать все события со статусом "Разрешено".

Данная опция подразумевает безусловное исключение из потока всех событий со статусом «Разрешено» (вне зависимости от наличия или отсутствия ассоциированного с ними правила).

Оптимизировать поток файловых событий.

Оптимизация потока файловых событий заключается в «сворачивании» нескольких одинаковых (в рамках одного процесса) событий в одно.

Оптимизировать поток сетевых событий.

Оптимизация потока сетевых событий заключается в «сворачивании» нескольких одинаковых (в рамках одного процесса) событий в одно.

Оптимизировать поток событий межпроцессного взаимодействия.

Оптимизация потока событий межпроцессного взаимодействия заключается в «сворачивании» нескольких одинаковых (в рамках одного процесса) событий в одно.

Оптимизировать поток событий реестра.

Оптимизация потока событий реестра заключается в «сворачивании» нескольких одинаковых (в рамках одного процесса) событий в одно.

Фильтрация WMI-событий.

Данная опция позволяет выбрать один из режимов фильтрации WMI-событий Windows:

1) Создание процесса – будут доступны только события создания процессов посредством WMI (вызов метода Create объекта класса Win32_Process);
2) Вызов метода – будут доступны только события вызовов методов классов;
3) По ключевым словам – будут доступны события WMI, удовлетворяющие условиям наличия/отсутствия подстрок, перечисленных в соответствующих полях ниже;
4) Не отправлять события – WMI-события полностью исключаются из потока.

В любых режимах фильтрации внутренняя аналитика, направленная на выявление техник закрепления в системе Windows посредством WMI, продолжает работать.

Общие настройки безопасности

Режим «только детектирование» (противодействие угрозам в режиме реального времени на агенте отключено).

Если режим «только детектирование» включен, то все блокирующие реакции, заданные для индикаторов компрометации и атак, а также YARA-правил переопределяются агентом на «детектирование». В этом случае в поле «Причина предпринятого действия» события делается соответствующая пометка, которая

позволяет понять, что то или иное событие не заблокировано из-за включенного режима «только-детектирование», но будет блокироваться в «боевом» режиме.

Такой режим работы агента может использоваться в двух сценариях:

— начальный период развертывания EDR, когда аналитиками изучается профиль событий новой информационной системы и подавляются ложные срабатывания;

— демонстрационный режим, позволяющий наблюдать этапы развития атаки и оценивать возможности агента по детектированию/реагированию на каждом этапе (в «боевом» режиме атака была бы заблокирована на раннем этапе).

Режим «только детектирование» не распространяется на блокирующие действия, предписанные сетевыми и файловыми исключениями.

Принудительно подавлять события процессов при превышении лимита.

Данная опция включает/отключает механизм принудительного ограничения потока событий процессов. Если процесс в течение 10 минут генерирует более 100 тысяч событий, то передача на сервер его событий с критичностью **Информация** прекращается на 1 час (события с более высокой критичностью продолжат передаваться). Передача событий процесса возобновляется при назначении ему исключений или их изменении, а также по истечении периода ограничения.

Кроме того, предусматривается возможность запрещения принудительного подавления событий с помощью флага **Запрет принудительного подавления событий** исключений для программ.



Важно

Необходимо помнить о возможности исключения телеметрии основных источников (процессы, файлы, сеть, реестр) или аналитической активности (файловые и сетевые исключения, а также индикаторы атак) путем указания соответствующего флага в разделе **Исключения для программ**

Настройки безопасности монитора процессов

Реакция на создание нити в стороннем процессе (кроме авторизованных программ Windows).

Данная опция управляет политикой агента для Windows в отношении внедрения кода одним процессом в другой (сторонний).

Указанная здесь критичность будет использована при формировании агентом события внедрения кода. Повышение уровня критичности выше «Низкой» заставит сервер EDR создавать инциденты ИБ при попытке внедрения кода. Действие определяет автоматизированную реакцию на внедрение кода со стороны агента. Логика опции не распространяется на программы, у которых есть право внедрения кода в сторонние процессы, заданное с помощью исключений для программ, а также на системные компоненты и некоторый набор легитимного ПО.

Реакция на доступ к стороннему процессу/нити (кроме авторизованных программ Windows).

Данная опция управляет политикой агента для Windows в отношении доступа одного процесса к другому процессу (стороннему) или его нити (потоку).

Указанная здесь критичность будет использована при формировании агентом события доступа. Повышение уровня критичности выше «Низкой» заставит сервер EDR создавать инциденты ИБ при попытке доступа. Действие определяет автоматизированную реакцию на доступ со стороны агента.

Логика опции не распространяется на программы, у которых есть право доступа к сторонним процессам/нитям, заданное с помощью исключений для программ, а также на системные компоненты и некоторый набор легитимного ПО.

Настройки Antimalware Scan Interface Windows (AMSI)

Настраивать AMSI можно в области **Настройка Antimalware Scan Interface Windows (AMSI)**. Администратор может включать/отключать работу AMSI, ограничивать размер содержимого в событиях AMSI, выбирать политику резервирования бесфайлового содержимого, ограничивать максимальное использование диска для хранения резервных копий содержимого AMSI.

Разрешить работу AMSI.

Включение механизма AMSI позволяет EDR проверять запускаемые скрипты (JavaScript, VBScript), командные сценарии (powershell, wscript, cscript), макросы Office VBA и исполняемые модули (в том числе бесфайловые), загружаемые в процессы. Механизмы AMSI поддерживаются, начиная с Windows 10. Когда AMSI включен, EDR генерирует соответствующие события, проверяет артефакты по наборам ИК, YARA-правилам и TI-платформе (если настроена соответствующая интеграция).

Ограничение размера содержимого в событиях AMSI.

Содержимое AMSI – это текст или двоичные данные, являющиеся объектом контроля. Текстовое содержимое может быть включено в событие EDR в непосредственном виде для удобства анализа. Данная опция ограничивает максимальный размер текстового содержимого, включаемого в событие (но не более 32766 символов). Ограничение в 0 символов отключает отправку содержимого. Если содержимое ограничивается по размеру (т.е. отправляется частично), то оно становится предметом резервирования, согласно установленной политике резервирования AMSI-содержимого.

Политика резервирования AMSI-содержимого.

Зачастую ВПО использует бесфайловые (fileless) техники атак или же вредоносное содержимое удаляется для сокрытия следов атаки. Резервирование заключается в сохранении на диск содержимого (объектов контроля) для обеспечения возможности его последующей загрузки по требованию на сервер EDR с целью углубленного анализа. Предусматриваются следующие опции резервирования:

– резервирование отключено.

– резервирование бесфайлового (fileless) содержимого.

– резервирование любого содержимого.

По умолчанию резервируется только бесфайловое (fileless) содержимое. Если текстовое содержимое целиком включено в событие, то оно не резервируется. Если содержимое зарезервировано, то в событие включается ссылка, позволяющая загрузить его на сервер EDR.

Органичение использования диска для хранения резервных копий содержимого AMSI.

Данная опция позволяет ограничить объем дискового пространства для хранения резервных копий содержимого (объектов контроля) AMS Минимальное ограничение – 1 Мб, максимальное – 100 Мб. По умолчанию действует ограничение в 10 Мб. При достижении установленного ограничения старые резервные копии будут удаляться для высвобождения места для хранения более новых.

Политика YARA-сканирования AMSI-содержимого.

Данная опция управляет механизмом сканирования AMSI-содержимого движком YARA. Сканирование производится по набору YARA-правил для файлов, назначенному агенту. При срабатывании YARA-правил в поток событий добавляется обнаружение «Файл классифицирован как вредоносный (YARA-правила)». Предусматриваются следующие политики сканирования:

– сканирование отключено.

— сканирование бесфайлового (fileless) содержимого.

— сканирование любого содержимого.

По умолчанию сканирование отключено. Сканирование бесфайлового содержимого позволяет находить вредоносные сигнатуры в памяти. Сканирование содержимого, имеющего ассоциированный файл, также может быть полезно, поскольку в уведомлениях AMSI содержимое деобфусцировано, что дает больше возможностей по написанию универсальных YARA-правил.

Настройки безопасности файлового монитора

Реакция на прямой доступ к жесткому диску (кроме авторизованных программ Windows).

Данная опция управляет политикой агента для Windows в отношении прямого доступа того или иного процесса к жесткому диску для его чтения или записи. Указанная здесь критичность будет использована при формировании агентом события доступа. Повышение уровня критичности выше «Низкой» заставит сервер EDR создавать инциденты ИБ при попытке доступа. Действие определяет автоматизированную реакцию на доступ со стороны агента. Логика опции не распространяется на программы, у которых есть право доступа к жесткому диску, заданное с помощью исключений для программ, а также на системные компоненты и некоторый набор легитимного ПО.

Подсчитывать хеш SHA-1.

По умолчанию агент при обработке файлов с потенциально активным содержимым подсчитывает хеш SHA256. Данная опция заставляет его подсчитывать еще и хеш SHA-1, а также проводить матчинг файловых индикаторов компрометации и исключений соответствующего типа. Дополнительные вычислительные операции требуют процессорного времени и могут замедлить работу системы.

Подсчитывать хеш MD5.

По умолчанию агент при обработке файлов с потенциально активным содержимым подсчитывает хеш SHA256. Данная опция заставляет его подсчитывать еще и хеш MD5, а также проводить матчинг файловых индикаторов компрометации и исключений соответствующего типа. Дополнительные вычислительные операции требуют процессорного времени и могут замедлить работу системы.

Подсчитывать хеш Imphash.

Опция включает подсчет хеша Imphash для PE-файлов. Метод import hashing (Imphash) заключается в вычислении хеш-значений на основе имён библиотек и импортируемых функций с учетом порядка их расположения внутри исполняемого файла. Этот хеш может использоваться для быстрой группировки и идентификации связанных образцов вредоносного ПО. Существуют различные модификации подсчета хеша Imphash, формирующие различные значения хеша для одного и того же файла. Агент для подсчета использует алгоритм, аналогичный YARA. Дополнительные вычислительные операции требуют процессорного времени и могут замедлить работу системы.

Режим глубокого сканирования файлов.

Обязательная часть анализа со стороны агента для всех файлов с потенциально активным содержимым включает в себя подсчет хеш-сумм, матчинг индикаторов компрометации и файловых исключений.

Для файлов формата PE (Windows Portable Executable) дополнительно производится разбор электронной подписи и метаинформации о файле. Глубокое сканирование подразумевает дополнительные проверки – YARA-правила и/или статический анализ на основе машинного обучения (ML), способный выявить характерные признаки вредоносного файла с использованием технологий искусственного интеллекта. Следует иметь ввиду, что сканирование с использованием ML может давать большое количество ложных срабатываний. YARA-правила являются эффективным средством сигнатурного анализа и позволяют выявить известные угрозы. При выборе данной опции для сканирования будет использован набор YARA-правил, назначенный агенту. Большое количество YARA-правил может замедлить работу системы.

Глубокое сканирование исполняемых файлов.

Для исполняемых файлов дополнительно доступно управление режимом глубокого сканирования, исходя из их электронной подписи (ЭП):

Все. Глубокое сканирование производится для любых исполняемых файлов вне зависимости от их ЭП. Данный режим глубокого сканирования исполняемых файлов может замедлить работу систему;

Без ЭП. Глубокое сканирование исключается для подписанных исполняемых файлов;

Без доверенной ЭП. Глубокое сканирование исключается только для подписанных доверенной ЭП исполняемых файлов, остальные файлы будут сканироваться (даже если они подписаны). Конкретный

перечень доверенных издателей может меняться и доступен в актуальной документации. К доверенным издателям относятся такие вендоры как Microsoft, Google, Apple, Intel и т.п.

Не обрабатывать файлы *.ni.dll (нативные образы .NET Framework).

Файлы нативных образов .NET Framework создаются в результате предкомпиляции утилитой NGEN управляемых (managed) образов для ускорения работы .NET-приложений. При каждой перекомпиляции меняется хеш-сумма нативного образа – даже несмотря на то, что исходный управляемый образ не изменялся. Это приводит к многочисленным проверкам по сути одного и того же файла (хеш меняется из-за изменения метаданных) и «засорению» кеша (cash trashing) модуля мониторинга файловой активности агента, что в конечном итоге оказывает негативный эффект на производительность агента в целом.

Кроме того, многочисленные вариации хеш-сумм одного и того же файла отправляются для проверки на TI-платформу и учитываются в подсистеме мониторинга распространения, что тоже создает избыточную нагрузку на эти модули.

Данная опция отключает обработку со стороны агента нативных образов .NET Framework: подсчет хешей, матчинг исключений и индикаторов, и отправку соответствующих событий в поток.

Расширения файлов с потенциально активным содержимым

По умолчанию файловая аналитика (подсчет хешей, матчинг индикаторов и др.) производится только для исполняемых файлов и только при их запуске (или загрузке, если исполняемый файл – это динамически загружаемая библиотека).

Данная опция позволяет дополнительно указать расширения файлов (помимо исполняемых), для которых также требуется включить файловый анализ, который будет производиться в режиме реального времени при доступе к ним.

Настройки противодействия сетевым атакам

Активное противодействие сканированию портов.

Данная опция включает режим эмуляции открытых TCP-портов, таким образом, что при сканировании все TCP-порты выглядят открытыми. Это существенно затрудняет для злоумышленника идентификацию работающих сетевых сервисов, снижает вероятность атаки на них и осложняет горизонтальное распространение в сети.

Противодействие сетевым атакам на контроллеры доменов

Данная опция включает сетевые защитные механизмы агента в отношении контроллеров доменов Windows в инфраструктуре.

IP-адреса контроллеров доменов.

Список IP-адресов контроллеров доменов, действующих в инфраструктуре. Разделитель значений – символ ;. Максимальная длина 255 символов.

Реакция на атаку DCSync.

Данная опция определяет реакцию агента на потенциальную сетевую атаку DCSync в отношении контроллеров доменов:

– детектирование;

– детектирование и блокирование.

Настройки безопасности сетевого монитора

Запретить входящие сетевые подключения.

При включении данной опции все входящие TCP-подключения будут отвергаться. Если агент не выполняет роль сервера в информационной системе, то в целях безопасности все входящие подключения к нему можно запретить.

Отправлять события ICMP.

При включении данной опции в поток событий будут включаться события сетевого взаимодействия по протоколу ICMP.

IP-адреса клиентов, DNS-запросы которых не обрабатываются и исключаются из телеметрии.

Список IP-адресов, для которых DNS-запросы (исходящие клиентские и входящие серверные) и соответствующие ответы на них не обрабатываются и безвозвратно исключаются из телеметрии.

8.8.3. Профили контроля USB

Профили контроля USB позволяют управлять различными устройствами, присоединяемыми к конечным точкам посредством USB-интерфейса. Контроль осуществляется как над отдельными устройствами, так и над их классами:

1) Накопители;
2) Медиа-устройства;
3) Принтеры;
4) Сканеры;
5) Беспроводные устройства и т.д.

Под управлением понимается задание различных разрешений для выбранных устройств, например, на чтение, запись, запуск и т.д. При этом в потоке событий будут формироваться события, связанные в том числе с нарушением разрешающей политики, например, пользователь попытается запустить программу с USB-накопителя при наличии соответствующего запрета на запуск, что приведет к формированию события на странице **Активность** или на странице **Инциденты**, если выбрана соответствующая критичность (**Средняя** или выше) для этого события.

Доступны следующие типы событий:

1) Устройство USB подключено;
2) Устройство USB отключено;
3) Зафиксирована запрещенная попытка чтения;
4) Зафиксирована запрещенная попытка записи;
5) Зафиксирована запрещенная попытка выполнения управляющего запроса;
6) Зафиксирована запрещенная попытка запуска исполняемого файла;
7) Статистика чтения/записи данных.

В настоящий момент контроль USB-устройств осуществляется только для агентов Windows.

Страница «Профили контроля USB»

На странице **Профили контроля USB** отображается таблица с профилями со следующими столбцами:

1) Кнопка выбора элемента;
2) Название профиля;
3) **Привязано агентов** (показывает, сколько агентов работает с этим профилем);
4) **Управление** (содержит кнопки управления профилем).

На странице можно выполнить следующие операции:

1) Добавлять профили контроля USB;
2) Передать агентам все профили, созданные и сохраненные на странице, а также отдельный профиль;
3) Редактировать название профиля;
4) Удалить профиль.

Чтобы добавить профиль, необходимо нажать по иконке Добавить профиль.

Откроется окно, представленное на рисунке 81.

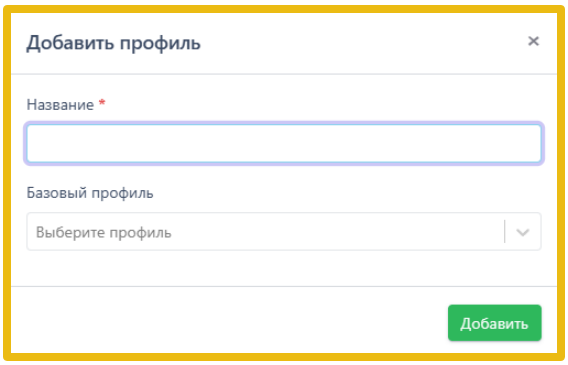


Рисунок 81 – Окно добавления профиля

Обязательной для заполнения является строка **Название**. Можно добавить любой из ранее созданных профилей в качестве базового профиля, но это действие является необязательным.

Для редактирования имени профиля необходимо нажать на странице **Профили контроля USB** по иконке в строчке напротив профиля, имя которого требуется изменить, после чего откроется окно редактирования имени профиля, представленное на рисунке 82.

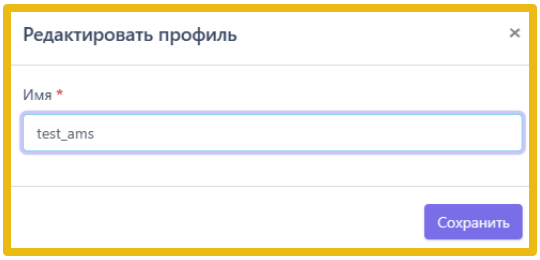


Рисунок 82 – Редактирование имени профиля

После изменения имени профиля требуется нажать по иконке **Сохранить**, после чего профиль с данным именем появится в списке профилей.

Для удаления профиля необходимо нажать кнопку или воспользоваться групповым удалением, выделив соответствующие профили и нажав кнопку **Удалить выбранные профили**.

Страница «Профиль контроля USB»

Страница **Профиль контроля USB** разделена на две основные области:

1) Базовые настройки;
2) Конфигурации контроля USB-устройств.

Базовой настройкой является то, включена ли подсистема контроля USB-устройств или нет. Включение выключение осуществляется с помощью кнопок / .

В области конфигурации контроля USB-устройств по умолчанию представлены общие универсальные конфигурации устройств (рис. 83).

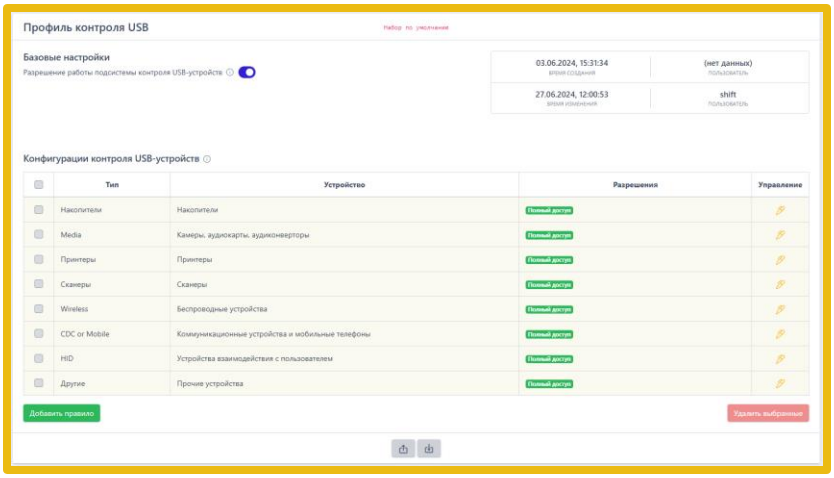


Рисунок 83 – Профиль контроля USB – Набор по умолчанию

Пользователь может добавить уникальную конфигурацию, нажав кнопку **Добавить правило**. Откроется окно **Создание правила контроля устройства USB** (рис. 84).

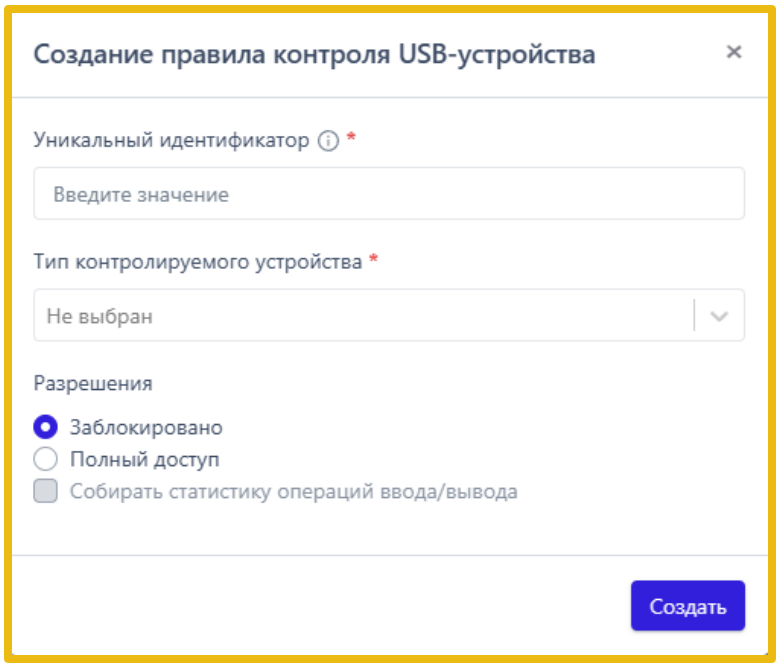


Рисунок 84 – Создание правила контроля USB-устройств

Здесь нужно ввести информацию об уникальном идентификаторе устройства в формате VID_PID_MI_SERIAL (VID – идентификатор производителя, PID – идентификатор продукта, MI – номер интерфейса, SERIAL – серийный номер устройства) или группы устройств в формате VID_PID_MI, эту информацию об устройствах можно узнать на странице **Активность** в событиях типа **Контроль USB.**

Далее следует выбрать тип контролируемого устройства и добавить необходимые разрешения, по умолчанию устройство будет заблокировано.

Возможно установить следующие разрешения:

1) Блокировка;
2) На чтение;
3) На чтение и запись;
4) На запуск программ;
5) На получение статистики операций ввода/вывода.

Здесь же можно настроить критичность для некоторых событий с USB-устройством:

1) Устройство USB подключено;
2) Устройство USB отключено;
3) Зафиксирована запрещенная попытка записи;

4) Зафиксирована запрещенная попытка запуска исполняемого файла (только для накопителей).

При выборе критичности от уровня **Средняя** и выше в программе будет создан инцидент, который отобразится на странице **Инциденты**.

Для завершения операции по добавлению правила необходимо нажать кнопку **Создать**.

Уникальные конфигурации, в отличие от универсальных (они выделяются желтым цветом на странице), можно удалять, для этого в строке с конфигурацией присутствует кнопка или можно воспользоваться групповым удалением, выделив нужные правила и нажав кнопку **Удалить выбранные**.

Для редактирования любых конфигураций в каждой из них присутствует кнопка .

Для передачи изменений в профиле агентам требуется нажать по иконке , после чего откроется окно подтверждения действия, представленное на рисунке 85.

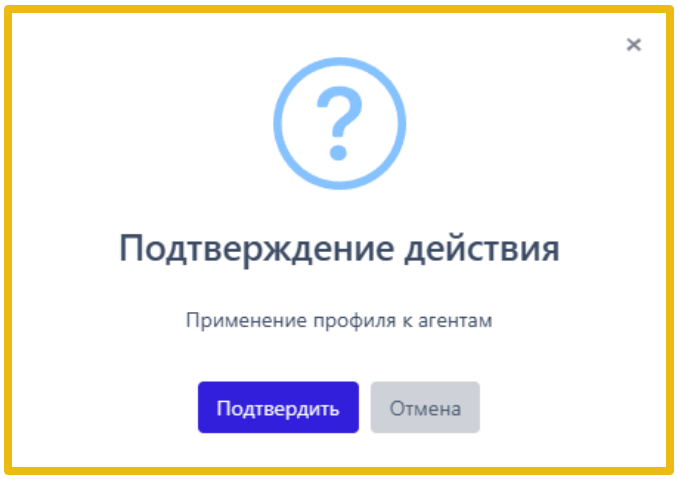


Рисунок 85 – Подтверждение действия применения профиля

После того, как пользователь нажмет по иконке **Подтвердить**, профиль будет применяться для назначенного агента.

Для применения всех профилей, имеющихся на странице **Профили**, возможно нажать по иконке .

На странице профиля имеется возможность для импорта/экспорта данных из профиля в формате txt:

– – экспортировать профиль в файл формата txt;

–  – импортировать данные из файла в профиль (формат txt).

Конфигурации в профиле можно активировать и деактивировать по отдельности или группой. Для выполнения операций по отдельности используются кнопки **Деактивировать/Активировать** ( /). Каждая операция требует подтверждения. Для активации/деактивации группы конфигураций необходимо отметить их флагом () и нажать кнопку группового применения **Активировать выбранные элементы** () или **Деактивировать выбранные элементы** ().

Быстрое создание конфигураций контроля USB на странице «Активность»

Для событий, источником которых является модуль контроля USB, конфигурационное правило может быть добавлено с помощью мастера создания правил для USB-устройств на странице **Активность**.

Для этого в каждой строке события, источником которого является **Контроль USB**, присутствует кнопка  . Нажатие кнопки открывает окно **Мастер создания правил для USB-устройств** с предзаполненными полями **Уникальный идентификатор** (VID_PID_MI_SERIAL), **Тип устройства** и полем **Профиль**, в котором можно выбрать профиль для сохранения правила.

При нажатии кнопки **Далее** открывается окно **Создание правила контроля USB-устройства**, в котором необходимо установить разрешения для выбранного устройства. Для завершения операции необходимо нажать кнопку **Создать**, после чего новая конфигурация появится на странице выбранного профиля контроля USB.

8.9 Параметры

8.9.1. Пользователи и роли

В разделе **Пользователи и роли** вкладки **Пользователи**, администратор может просматривать информацию о пользователях, создавать и удалять учетные записи пользователей, а также изменять параметры учетных записей пользователей.

Во вкладке **Роли** администратор может создавать группы ролей, назначать определенных пользователей в группы, назначать определенные права согласно определяемой роли.

Во вкладке **Блокировки** показаны пользователи, заблокированные ранее, и у администратора имеется возможность снять блокировку для пользователя.

Общая информация о списке пользователей

Во вкладке **Пользователи** показана информация обо всех зарегистрированных в Программе пользователях. Данные о пользователях представлены в табличном виде.

Таблица содержит следующие поля:

1) Имя пользователя;
2) Последнее время входа;
3) Имя;
4) Фамилия;
5) Адрес электронной почты;
6) Статус;
7) Управление.

Имя пользователя – содержит логин, под которым пользователь зарегистрирован в Программе. Если пользователь является LDAP-пользователем, то помечается значком  . При этом LDAP-пользователь может быть связан с пользователем EDR. Такой пользователь сможет войти как под учетной записью, созданной в разделе **Пользователи**, так и с учетными данными LDAP-пользователя.

Последнее время входа – содержит дату и время последнего входа пользователя.

Имя – содержит имя, которое пользователь указал при регистрации.

Фамилия – содержит фамилию, которую пользователь указал при регистрации.

Адрес электронной почты – электронный почтовый адрес, указанный пользователем при регистрации.

Статус и **Управление** – в указанных полях содержатся кнопки для изменения параметров учетных записей пользователей. В поле **Статус** администратор может блокировать/разблокировать пользователя Программы.

В поле **Управление** доступны операции редактирования данных пользователя, сброса пароля пользователя, привязки пользователя к пользователю LDAP, а также удаления пользователя.

В верхней части окна над таблицей содержатся строки для поиска пользователей по параметрам фильтрации:

– Показывать по;

– Имя пользователя (логин);

– Имя;

– Фамилия;

– Адрес электронной почты;

– LDAP-пользователи;

– Права.

Каждая строка таблицы содержит дополнительную информацию о **Роли** пользователя, а также сессиях пользователя, для ее просмотра необходимо нажать ЛКМ на значок ›. В случае, если у пользователя были активные сессии, они будут показаны в строках ниже. По умолчанию отображается только последняя сессия (рис. 86).

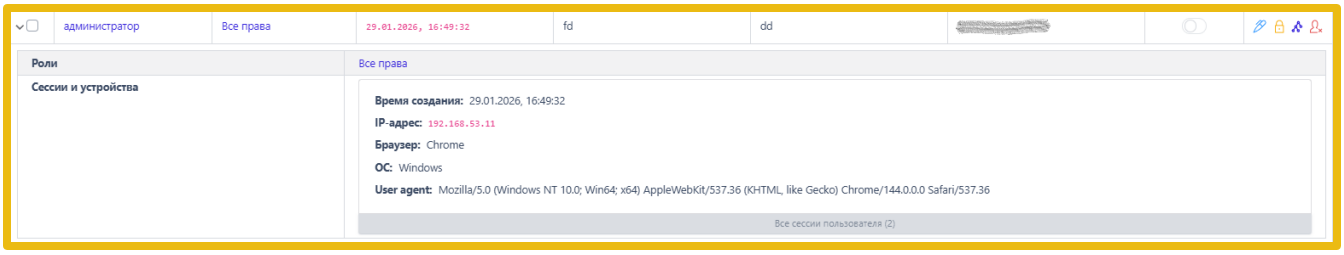


Рисунок 86 – Информация о пользователе

Для раскрытия данных по всем сессиям следует нажать кнопку **Все сессии пользователя**. В окне сессии отображается информация по следующим параметрам: **Время создания**, **IP адрес**, **Браузер**, **ОС** и **User agent**.

Время создания – дата и время входа в учетную запись пользователя для выбранной сессии.

IP адрес – ip-адрес устройства, с которого был выполнен вход пользователя для выбранной сессии.

Браузер – браузер, из которого был выполнен вход в Программу для выбранной сессии.

ОС – операционная система, под управлением которой выполнялся запуск браузера для входа в Программу.

User agent – в поле отображается строка, которая идентифицирует браузер, его версию, операционную систему, язык и т.д., то есть по сути показано наименование браузера, с помощью которого выполняется взаимодействие с агентом.

Изменение параметров учетных записей пользователей

Два поля таблицы с учетными записями пользователей содержат дополнительные кнопки для управления параметрами учетных записей: **Статус** и **Управление**.

Примечание

Кнопки управления и блокирования/разблокирования активны только для пользователей, вошедших в Программу под учетной записью администратора.

В поле **Статус** находятся кнопки **Заблокировать/Разблокировать пользователя** , с помощью которых администратор может временно запретить или разрешить тому или иному пользователю работать с Программой. Опция блокирования неприменима по отношению к своей учетной записи.

Процесс блокирования пользователя защищен от случайных нажатий необходимостью подтверждать действие блокирования/разблокирования в отдельном окне.

После подтверждения операции в нижней части основного окна Программы появляется сообщение **Пользователь разблокирован/заблокирован**.

В поле **Управление** находятся кнопки **Редактировать пользователя** (), **Сбросить пароль** (), **Привязать LDAP-пользователя** () и **Удалить пользователя** ().

Для заблокированного пользователя активны будут только кнопки удаления пользователя и редактирования.

При нажатии кнопки **Редактировать пользователя** открывается окно, в котором можно изменить имя и фамилию пользователя, а также адрес электронной почты.

Опция изменения роли пользователя не применяется по отношению к собственной учетной записи. Для сохранения и применения измененных параметров необходимо нажать кнопку **Сохранить**.

При нажатии кнопки **Сбросить пароль** открывается окно, в котором для сброса текущего пароля выбранному пользователю следует нажать кнопку **Выполнить**

Ссылка на сброс пароля отправляется пользователю на указанный при регистрации адрес электронной почты. Далее пользователь переходит по отправленной ссылке, после чего вводит новый пароль и подтверждение пароля в окне **Сброс пароля** (рис. 87). Пароль должен соответствовать правилам добавления пароля.



Рисунок 87 – Окно восстановления пароля пользователя

После ввода значений нового пароля и его подтверждения необходимо нажать кнопку Сохранить. После завершения операции сброса пароля пользователь сможет войти в свою учетную запись с новым паролем.

Для привязки LDAP-пользователя к пользователю EDR администратору необходимо нажать кнопку **Привязать LDAP-пользователя** ( ) и в открывшемся окне ввести логин LDAP-пользователя, которого необходимо привязать к пользователю EDR.

При нажатии кнопки **Удалить пользователя** ( ) открывается окно, в котором для удаления учетной записи выбранного пользователя следует нажать кнопку **Выполнить**.

Чтобы добавить роль для одного или нескольких пользователей, необходимо отметить этих пользователей флагом ( ), после чего нажать кнопку **Добавить пользователей в роль** ( ). Откроется окно, в котором необходимо определить роль для выбранных пользователей и нажать кнопку Добавить.

Чтобы исключить пользователей из роли, необходимо отметить этих пользователей флагом ( ), после чего нажать кнопку **Исключить пользователей из роли** . Откроется окно, в котором необходимо выбрать роль, из которой следует исключить пользователей, после чего нажать кнопку **Применить**.

Чтобы переназначить роли пользователям, необходимо выбрать этих пользователей ( ), после чего нажать кнопку **Переназначить роли пользователям** ( ). Откроется одноименное окно, в котором необходимо выбрать одну или несколько ролей. Выбранные роли заменят текущую роль или роли пользователя.

Создание учетной записи пользователя

В нижней части панели администрирования находится кнопка **Создать пользователя**. При нажатии кнопки открывается окно **Создать пользователя**.

Для добавления пользователя необходимо заполнить в окне **Создать пользователя** следующие поля:

– Имя пользователя;

– Адрес электронной почты;

– Имя;

– Фамилия;

– Новый пароль;

– Повторите пароль;

– Роли.

Для завершения регистрации нового пользователя следует заполнить все поля ввода. В поле ввода **Адрес электронной почты** необходимо ввести адрес электронной почты вида login@domain. Для того, чтобы отобразить/скрыть символы, вводимые в поля **Новый пароль** и **Повторите пароль** следует нажать кнопки / .

В нижней части окна **Создать пользователя** приведены правила формирования пароля:

– пароль не должен совпадать с именем пользователя или другой персональной информацией или быть слишком похожим на неё;

– пароль должен содержать как минимум 12 символов;

– пароль не может быть одним из широко распространённых паролей;

— пароль не должен состоять только из цифр.

Для подтверждения значений, установленных для новой учетной записи пользователя, необходимо нажать кнопку Создать.

Важно

Срок действия пароля устанавливается при разворачивании сервера в файле конфигурации.

Сообщения администратору при вводе некорректных значений

При вводе администратором некорректных данных в полях окон **Редактировать пользователя** и **Создать пользователя** Программа выводит сообщения об ошибках.

Если пользователь оставляет в указанных выше окнах хотя бы одно пустое поле ввода, то выводится сообщение (рис. 88). Такое же сообщение выводится во всех полях, требующих ввода информации.



Рисунок 88 – Сообщение о пустом поле ввода

При написании в поле ввода **Имя пользователя** значения имени пользователя, идентичного уже сохраненному в Программе, выводится сообщение о том, что пользователь с таким именем уже существует (рис. 89).

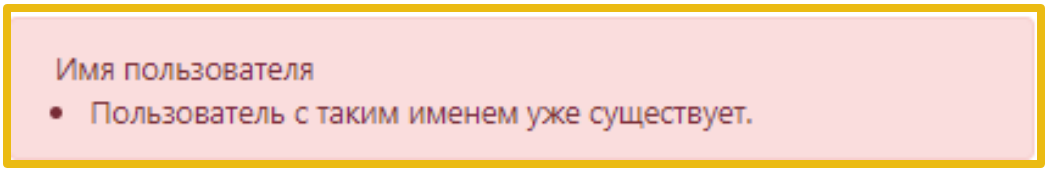


Рисунок 89 – Сообщение о совпадении имени пользователя

При вводе пользователем некорректного адреса электронной почты в поле ввода **Email** в нижней части окна **Редактировать пользователя** или **Создать пользователя** выводится сообщение о необходимости ввода правильного адреса электронной почты (рис. 90).



Рисунок 90 – Сообщение о неправильном адресе электронной почты

Если введенный пароль не соответствует одному или нескольким указанным в пункте 0 правилам, то в нижней части окна появится сообщение, в котором будет указано нарушенное при создании пароля правил (рис. 91).

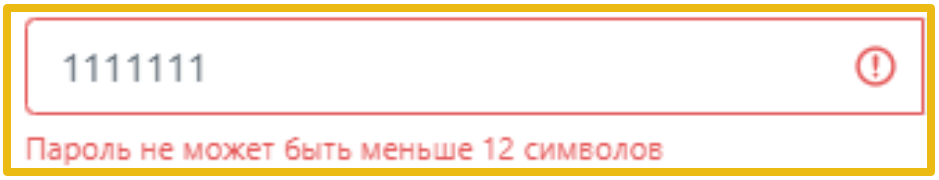


Рисунок 91 – Предупреждающее сообщение при вводе некорректного пароля

При вводе отличных друг от друга значений в поля **Новый пароль** и **Повторите пароль** в нижней части полей ввода появится сообщение о несовпадении введенных паролей (рис. 92).



Рисунок 92 – Сообщение о несовпадении паролей

При восстановлении пароля по ссылке, отправленной администратором, после ввода пользователем некорректных значений в поля **Введите новый пароль** и **Повторите пароль** в окне **Сброс пароля** будут отображаться сообщения, идентичные указанным выше (рис. 93).

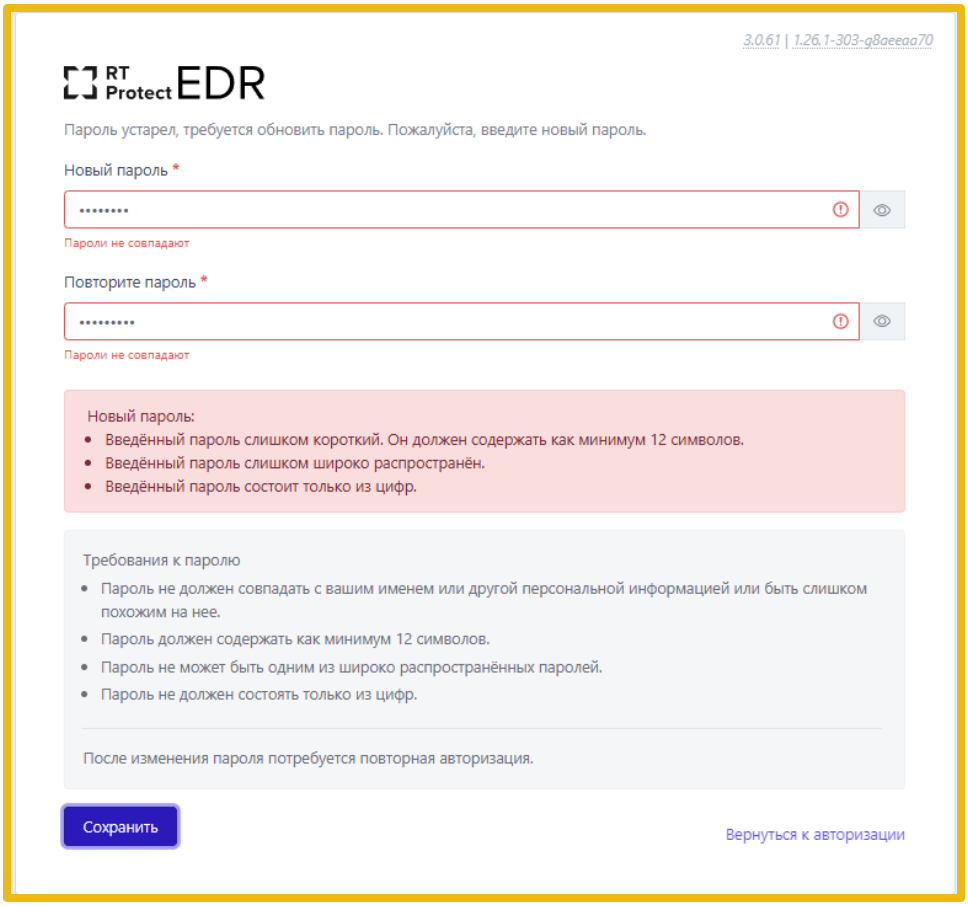


Рисунок 93 – Ввод некорректных значений при сбросе пароля

Сообщения об ошибках, которые выдает Программа при вводе некорректных значений пароля, будут идентичны тем, которые могут возникнуть при вводе пароля и его подтверждения в окне **Создать пользователя.**

Важно

Если в течение 5 минут пользователь Программы выполнит 4 или более неудачных попыток входа, то его учетная запись будет заблокирована. В этом случае разблокировать такого пользователя сможет только администратор Программы или пользователь будет разблокирован автоматически после завершения периода 24-х часовой блокировки.

Разблокировать пользователей

Чтобы разблокировать заблокированных ранее пользователей (выполнить групповую операцию разблокирования) необходимо перейти во вкладку **Блокировки** страницы **Пользователи и роли**.

В представленном на странице списке выделить пользователей, которых необходимо разблокировать (), и нажать кнопку **Разблокировать выбранных пользователей**, после чего подтвердить выполняемую операцию.

Для поиска по странице можно использовать следующие фильтры:

1) Имя пользователя (логин пользователя);
2) IP-адрес.

8.9.2. Журнал безопасности

На странице **Журнал безопасности** в табличном виде представлена информация о действиях пользователей. События таблицы можно фильтровать по количеству отображаемых событий (фильтр **Показывать по**), имени пользователя (фильтр **Пользователь**), критичности события (фильтр **Критичность**), периоду регистрации, а также выполнять поиск по типу события.

Все возможные действия пользователей, отображаемые в таблице, разделены на типы и подтипы.

Для типа действия **Авторизация пользователя** предусмотрены следующие подтипы:

- вход в систему;
- выход из системы;
- выход из системы на всех устройствах.

Для типа действия **Работа с пользователем** предусмотрены следующие подтипы:

- создание нового пользователя;
- редактирование пользователя;
- изменение пароля пользователя;
- удаление пользователя из системы;
- блокировка пользователя;
- разблокировка пользователя;
- запрос на изменение пароля пользователя;
- запрос ссылки для сброса пароля;
- сброс пароля пользователя;
- создание роли;

– редактирование роли;

– удаление роли;

– назначить роль пользователям;

– отозвать роль пользователям.

Для типа действия **Работа с агентом** предусмотрены следующие подтипы:

– верификация агентов;

– отмена верификации агента;

– редактирование агента;

– потеря связи с агентом;

– изменение состава ПО на агенте;

– добавление агентов в группу;

– удаление агентов из группы;

– отправка команды агенту;

– отправка команды группе агентов;

– загрузка нового дистрибутива агента на сервер;

– удаление дистрибутива агента с сервера;

– сетевая изоляция агентов;

– снятие сетевой изоляции агентов;

– включение функции защиты агентов;

– выключение функции защиты агентов;

– включение автоматического обновления агентов;

– выключение автоматического обновления агентов;

– включение сопоставления с золотым образом;

– выключение сопоставления с золотым образом;

– включение парольной защиты от удаления агентов;

– выключение парольной защиты от удаления агентов;

– изменение критичности у агентов;

Для типа действия **Конфигурация** предусмотрены следующие подтипы:

– создание нового набора;

– удаление набора;

– добавление новых данных в набор;

– удаление данных из набора;

– импорт данных в набор;

– редактирование данных в наборе;

– копирование данных между наборами;

– перемещение данных между наборами;

– активация элементов в наборе;

– деактивация элементов в наборе;

– передача набора агентам;

– передача профиля агентам;

– применение конфигурации наборов к агентам;

– применение конфигурации профилей к агентам;

– применение конфигурации к агентам;

– создание начальной конфигурации;

– редактирование конфигурации;

– удаление конфигурации;

– синхронизация наборов аналитики с TI.

Для типа действия **Работа с файлами агента** предусмотрены следующие подтипы:

– загрузка файла агента на сервер;

– удаление файла агента с сервера;

– загрузка файла пользователя на сервер;

– удаление файла пользователя с сервера;

– создание задачи для группового скачивания файлов;

– отмена задачи для группового скачивания файлов;

– удаление файла группового скачивания с сервера.

Для типа действия **Работа с инцидентом** предусмотрены следующие подтипы:

– создание инцидента;

– смена ответственного за инцидент;

– редактирование инцидента;

– закрытие инцидента;

– назначение инцидента;

– удаление инцидента;

– добавление событий в инцидент;

– исключение событий из инцидента;

– создание инцидента в рамках обнаружения.

Для типа действия **Действие с лицензией** предусмотрен следующий подтип:

– установка новой лицензии на сервере.

Для типа действия **LDAP** предусмотрены следующие подтипы:

– создание конфигурации LDAP;

– изменение конфигурации LDAP;

– удаление конфигурации LDAP;

– активация конфигурации LDAP;

– деактивация конфигурации LDAP;

– изменение пароля привязанного пользователя LDAP;

– добавление пользователя LDAP;

– привязка пользователя LDAP;

– удаление пользователя LDAP;

– добавление сетевого адреса LDAP;

– изменение сетевого адреса LDAP;

– удаление сетевого адреса LDAP.

Для типа действий **Планировщик задач** предусмотрены следующие подтипы:

– добавление сценария;

– редактирование сценария;

– удаление сценария;

– активация сценария;

– деактивация сценария;

– добавление задачи;

– редактирование задачи;

– удаление задачи;

– запуск задачи;

– завершение выполнения задачи;

Для типа действий **TI** предусмотрены следующие подтипы:

– создание конфигурации TI;

– изменение конфигурации TI;

– удаление конфигурации TI;

– активация конфигурации TI;

– деактивация конфигурации TI;

– изменение API-ключа конфигурации TI.

Для типа действий **SIEM** предусмотрены следующие подтипы:

– создание конфигурации экспорта событий;

– изменение конфигурации экспорта событий;

– удаление конфигурации экспорта событий;

– активация экспорта событий;

– деактивация экспорта событий;

– изменение настроек конфигурации экспорта событий.

Для типа действий **Журнал безопасности** предусмотрены следующие подтипы:

– изменение конфигурации журнала безопасности.

Для типа действий **Действие с лицензией** предусмотрены следующие подтипы:

– установка новой лицензии на сервере.

Для типа действий **Сервисы** предусмотрены следующие подтипы:

– состояние сервисов.

Для типа действий **Экспорт событий безопасности** предусмотрены следующие подтипы:

– создание конфигурации webhook-экспорта событий журнала безопасности;

– изменение конфигурации webhook-экспорта событий журнала безопасности;

– удаление конфигурации webhook-экспорта событий журнала безопасности;

– активация webhook-экспорта событий журнала безопасности;

– деактивация webhook-экспорта событий журнала безопасности;

– сброс очереди экспортируемых событий журнала безопасности.

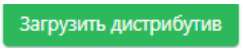
Уполномоченный пользователь может управлять событиями, отображаемыми в журнале безопасности. Для изменения списка отображаемых событий пользователю необходимо нажать кнопку **Редактировать конфигурацию** (), после чего определить, какие подтипы событий, регистрируемых в Программе, будут доступны для журналирования. Часть событий не поддерживаются, но оставлены для обратной совместимости с ранними версиями агента, это события назначения агентам различных типов конфигураций (назначение агентам профиля безопасности, набора индикаторов атак, набора индикаторов компрометации и т.д.)

Пользователь может указывать максимальный период хранения событий журнала безопасности в днях. По умолчанию это значение устанавливается на 30 дней.

8.9.3. **Дистрибутивы**

На странице **Дистрибутивы** отображается информация о дистрибутиве агента:

1) Имя (содержит название дистрибутива агента);
2) Версия;
3) Дата изменения;
4) Размер (показывает размер файла дистрибутива агента);
5) Платформа (показывает название ОС, на которую устанавливается дистрибутив агента);
6) Архитектура (показывает разрядность ОС, на которую устанавливается дистрибутив агента);
7) Управление (содержит кнопки скачивания и удаления дистрибутива ).

На странице отображается кнопка загрузки дистрибутива агента 

, при нажатии которой происходит загрузка установочного дистрибутива агента в модуль администрирования.

Если у агента установлен флаг **Автоматическое обновление**, то модуль агента обновится автоматически после загрузки новой версии установочного модуля на сервер.

Если флаг **Автоматическое обновление** не установлен, то администратору необходимо обновить дистрибутивы на машинах с агентами вручную или с помощью сторонних средств (см. пункт 5.2.1).

С помощью элемента › рядом с названием дистрибутива агента можно просмотреть дополнительную информацию:

1) Минимальная версия целевой платформы;
2) Описание (содержит описание изменений дистрибутива по сравнению с предшествующей версией);
3) MD5 (содержит 32-х символьное значение хеша для дистрибутива агента, рассчитанного по алгоритму MD5).
4) Кнопка лога изменений дистрибутива фронтенда и бекенда (Показать CHANGELOG).

При нажатии кнопки **Скачать дистрибутив** ( ) происходит загрузка дистрибутива агента в формате установщика в директорию на компьютере, с которого осуществляется доступ к модулю администрирования.

На странице **Дистрибутивы** для фильтрации информации, имеется система фильтров, которая представлена следующими фильтрами:

– Показывать по (изменяется количество записей в таблице);

– Имя (данные фильтруются по имени агента);

– Версия (данные фильтруются по номеру версии дистрибутива агента);

– Платформа (данные фильтруются по имени целевой платформы: версии Linux, Windows).

При нажатии кнопки Сбросить фильтры происходит сброс выставленных фильтров.

8.9.4. **Лицензирование**

Использование Программы заказчиками возможно при покупке лицензии. В интерфейсе предусмотрен раздел, в котором администратор может загрузить файл лицензии при первоначальном доступе к серверу администрирования или при продлении лицензии.

Кроме загрузки лицензии как файла, в Программе предусмотрена возможность ввести номер лицензии в окне загрузки в формате строки.

Параметры, указанные в лицензии, такие как срок действия и количество подключаемых модулей и агентов, указываются в договоре на поставку продукта по предварительному согласованию с Заказчиком Программы.

Лицензия может быть выпущена на любое количество агентов и сроки, оговоренные с Заказчиком в договоре на поставку.

Доступ к лицензиям (просмотр/загрузка) возможен для пользователя с ролью администратор.

На данный момент в Программе предусмотрено подключение следующих модулей:

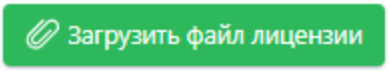
– Модуль Антишифра;

– Сканер уязвимостей;

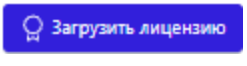
– Модуль контроля USB.

На странице **Лицензия** администратор Программы может увидеть следующую информацию:

1) Название компании, осуществившей покупку лицензии;
2) Серийный номер лицензии;
3) ID клиента (уникальный идентификационный номер);
4) Статус (действующая или недействующая);
5) Дата начала действия лицензии;
6) Дата окончания действия лицензии;
7) Максимальное количество агентов;
8) Текущее количество агентов;
9) Подключенные компоненты (компоненты, подключенные в модуле администрирования при загрузке лицензии (сканер уязвимостей, модуль защиты данных, модуль контроля USB)).

Файл лицензии загружается при нажатии кнопки 

, после чего открывается окно файлового менеджера, в котором администратор сможет выбрать лицензионный файл и загрузить его на сервер.

Если требуется ввести лицензию в формате строки, то после указания номера лицензии в поле ввода **Загрузка в формате строки** необходимо нажать кнопку 

.

Если лицензия активная и компонент в ней не подключен, то компонент недоступен.

Если лицензия отсутствует?

В случае использования модуля администрирования при отсутствии лицензии на следующих страницах не отображается информация о детектируемых событиях:

1) Главная страница;
2) Инциденты;
3) Активность.

Для корректной работы необходимо загрузить файл лицензии на сервер.

Если лицензия отсутствует, то компонент считается недоступным.

Если срок действия лицензии истек?

При окончании действия лицензии на сервере при работе с агентами возникают следующие ограничения:

1) Не происходит обновления агентов;
2) Отключается возможность добавлять новые профили безопасности агента и профили Антишифра, при этом старые профили продолжают работать и их можно редактировать;
3) Отключается возможность добавлять новые индикаторы компрометации или атак, YARA-правила, исключения и провайдеры журналов Windows, старые продолжают работать и их можно редактировать;
4) Отключается возможность скачивания и загрузки файлов на агента и с агента;
5) Отключается возможность добавлять пользователей и менять их имена, при этом возможность менять пароли остается;
6) Кнопки загрузки файлов с агентов становятся недоступными и в тултипе выводится пояснение "Загрузка файла невозможна, так как срок действия лицензии истек";
7) Если в лицензии подключен компонент **Уязвимости**, то соответствующий функционал недоступен, как если бы компонента в лицензии не было (выводится предупреждение об этом на экране **Уязвимости**, а также на экране **Лицензия**).

Если превышено допустимое количество агентов по лицензии?

При превышении количества агентов по лицензии вновь добавляемые агенты верифицировать нельзя.

Если текущее число зарегистрированных агентов превышает максимальное количество, установленное для заказчика по заключенному договору между заказчиком и производителем Программы, то в модуле администрирования отобразится сообщение о превышении максимального количества лицензионных агентов (рис. 94).

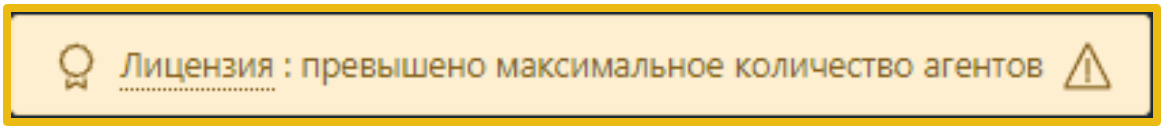


Рисунок 94 – Сообщение о превышении числа агентов

В этом случае заказчику необходимо заключить новый договор для того, чтобы количество агентов не превышало максимальное количество агентов, доступных заказчику согласно действующему договору, или удалить агентов, превышающих доступный для организации лимит.

Модульность лицензии

Для использования продукта могут быть сгенерированы по запросу и договоренности с Заказчиком следующие виды лицензий:

– Полная лицензия (подключены все имеющиеся модули);

– Ограниченная лицензия (подключен один или несколько модулей).

Если компонент не подключен в лицензии, то соответствующий функционал недоступен (в интерфейсе в сайдбаре видно, что компонент есть, например, **Уязвимости**, выводится пояснение, что необходимо подключить этот модуль).

Даже если компонент подключен, но срок действия лицензии истек, то функционал тоже недоступен (в интерфейсе в сайдбаре видно, что компонент есть, например, **Уязвимости**, выводится пояснение, что необходимо продлить лицензию);

— Если лицензия отсутствует, то и функционал подключаемых компонентов недоступен (аналогично в сайдбаре видно, что компонент есть, однако необходимо купить лицензию с этим модулем).

8.9.1. **Интеграции**

Интеграции – это инструмент администратора Программы для настройки взаимодействия между EDR, TI-платформой, LDAP-сервером и SIEM.

TI-платформа – это централизованная платформа, предназначенная для приема, агрегации, анализа, хранения и распределения данных разведки о киберугрозах. EDR осуществляет взаимодействие с ней для усиления аналитических возможностей Программы.

От настроек интеграции зависит, какие артефакты будет проверять TI-платформа, будут ли обнаруживаться уязвимости в Программе, какое количество артефактов будет обрабатываться в одном запросе и т.д.

LDAP (Lightweight Directory Access Protocol) — это протокол, то есть набор правил, для доступа к службам каталогов. Настройка интеграции EDR с LDAP-сервером позволяет создать связь между ними, чтобы пользователи, созданные в службе каталогов, могли заходить под своими учетными записями в модуль управления EDR.

SIEM (Security Information and Event Management) — это класс программного обеспечения и услуг, предназначенный для анализа, сбора, агрегации и корреляции в реальном времени событий безопасности и данных из различных источников в ИТ-инфраструктуре организации.

На странице **Интеграции** показана информация с настройками параметров взаимодействии EDR с TI-платформой, LDAP и SIEM (рисунок 95).

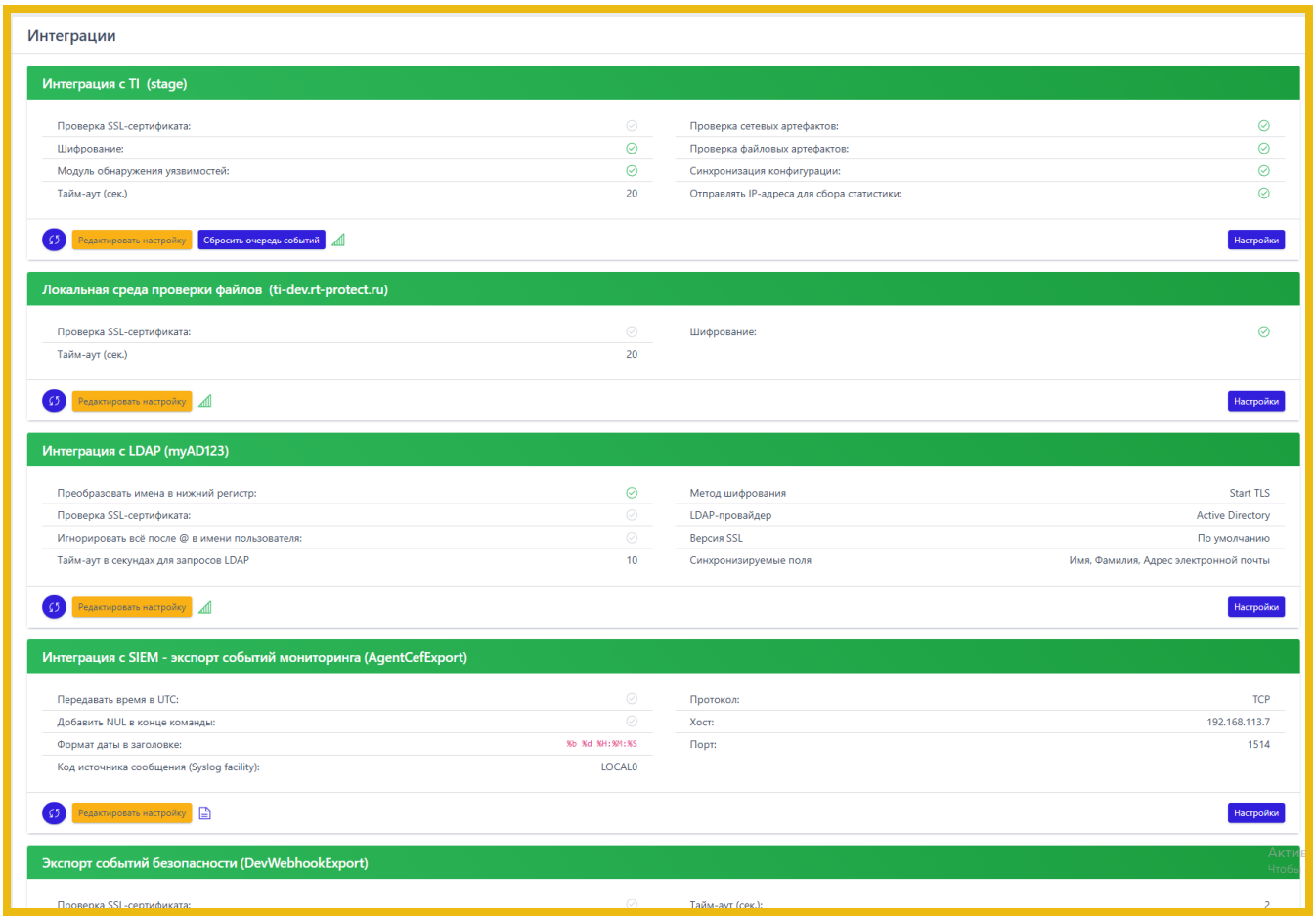


Рисунок 95 – Общий вид страницы Интеграции

Администратор сервера может просматривать настройки интеграций на данной странице, редактировать настройки, а также добавлять новые профили с настройками интеграций.

На странице имеются следующие области с информацией об интеграциях:

– Интеграция с TI;

– Интеграция с LDAP

– Интеграция с SIEM.

Интеграция с TI

В области **Интеграция с TI** администратор может настроить взаимодействие между сервером EDR и сервером TI. На странице в области **Интеграция с TI** показаны настройки интеграции, которые активны на данный момент.

Для редактирования настроек интеграции необходимо нажать ЛКМ по кнопке Редактировать настройку, после чего откроется окно редактирования, представленное на рисунке 96.

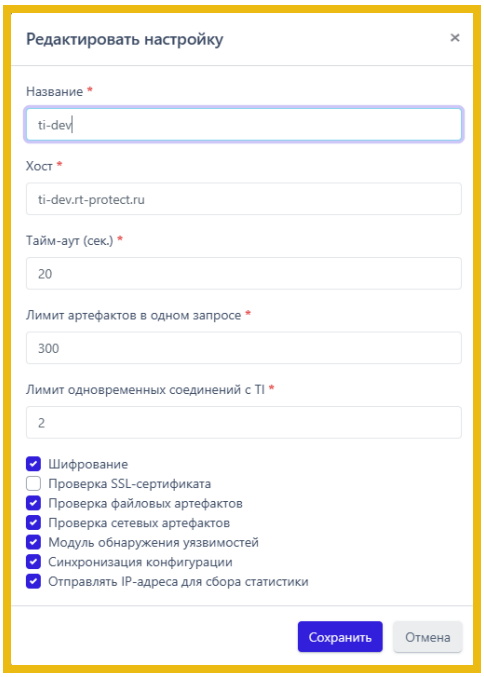


Рисунок 96 – Окно редактирования настроек интеграции с TI

После редактирования настроек следует нажать по иконке **Сохранить**.

В области **Интеграция с TI** для перехода на страницу со списком профилей с настройками следует нажать по иконке Настройки.

Страница со списками профилей настроек представлена на рисунке 97.

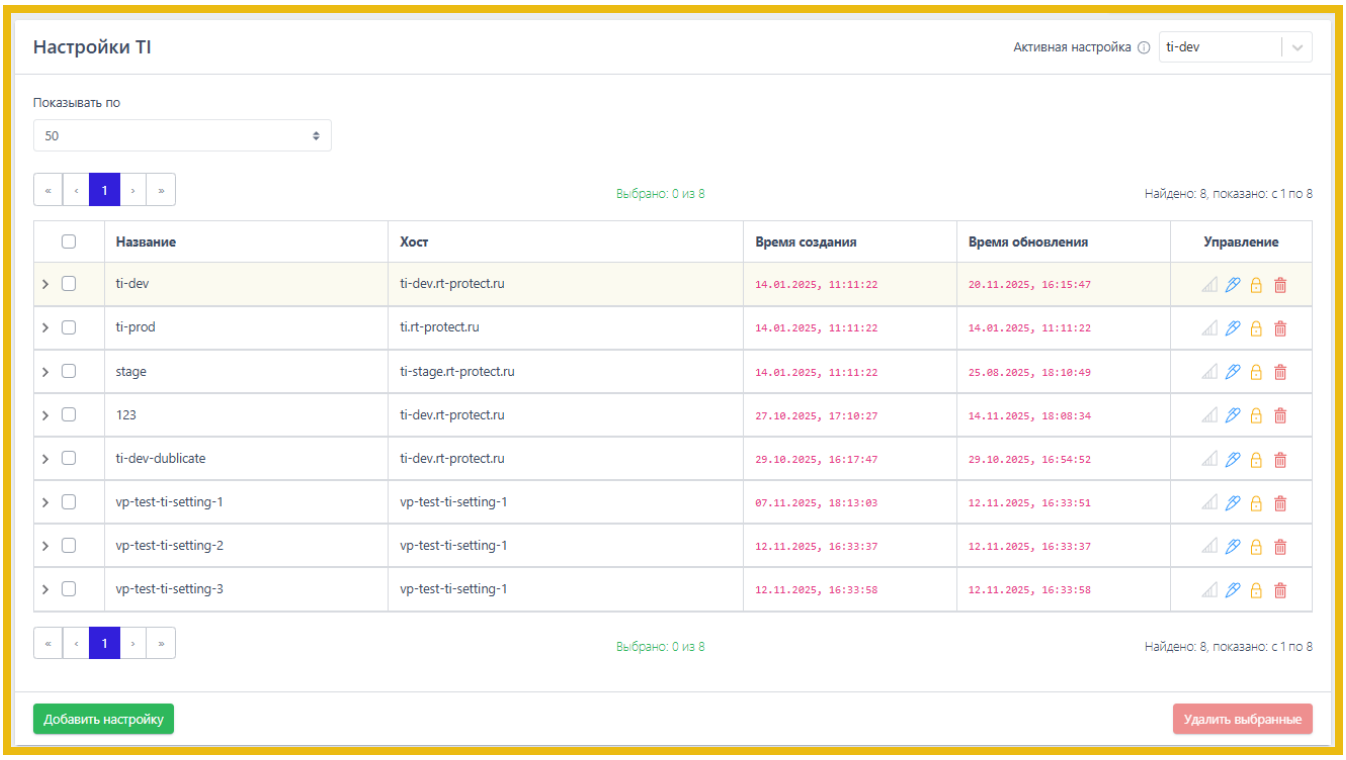


Рисунок 97 – Список профилей с настройками интеграции с TI

Информация на данной странице представлена в виде таблицы со следующими областями:

– кнопка выбора;

– иконка, раскрывающая информацию по параметрам настройки (›);

– название профиля настройки;

– имя хоста TI, с которым производится интеграция;

– время создания профиля с настройками;

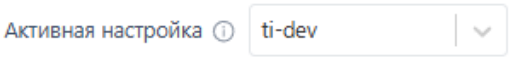
– время обновления профиля с настройками;

– управление (проверка соединения между TI и EDR ( ), редактирование настройки ( ), изменение API-ключа настройки TI ( ), удаление настройки ( )).

Важно

Следует обратить внимание на следующие моменты: сделать активными сразу две настройки нельзя, при деактивации (выключении настройки) с TI, взаимодействие с сервером EDR будет отключено, что повлияет на аналитические возможности сервера EDR.

Выбор активной настройки осуществляется администратором в строке **Активная настройка** (



).

Важно

В случае отсутствия активной настройки интеграция будет отключена.

На странице можно добавить настройку, нажав по иконке 

.

Параметры для заполнения при добавлении новой настройки аналогичны параметрам, указанным в окне редактирования настройки, за исключением поля API-ключ.

Для добавления настройки необходимо нажать кнопку **Настройки** и далее нажать кнопку **Добавить настройку**. Откроется окно **Добавить настройку** (рис. 98).

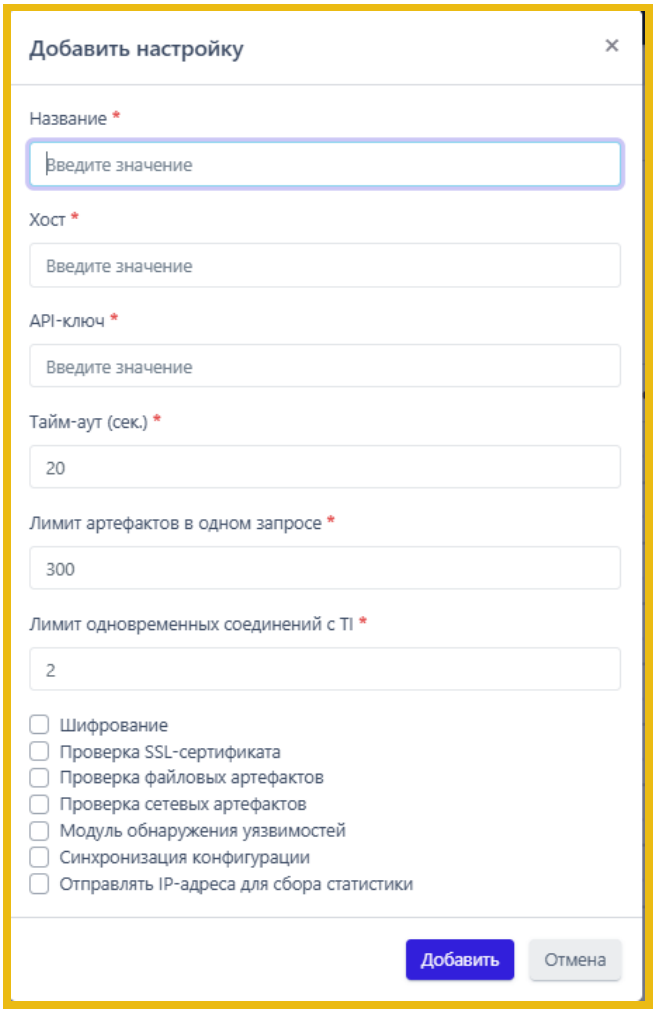


Рисунок 98 – Окно добавления настройки интеграции между TI-платформой и EDR

Название – в поле указывается название настройки интеграции.

Хост – в поле указывается имя хоста TI платформы (домен).

API-ключ – в поле указывается API-ключ. API-ключ — это уникальная строка символов (токен), которая используется для аутентификации запроса к API. API-ключ выдается производителем TI-платформы при наличии интеграции между TI-платформой и EDR.

Тайм-аут – (в секундах) ограничивает время ожидания ответа от сервера TI. Сервер TI должен ответить за это время или быстрее.

Лимит артефактов в одном запросе – определяет, сколько артефактов отправляется из EDR на TI-платформу в одном пакете.

Лимит одновременных соединений с TI – определяет лимит одновременных соединений между EDR и TI-платформой. Оптимальное значение лимита – 2 соединения.

Шифрование – опция включает или отключает шифрование при передаче запросов-ответов между EDR и TI-платформой.

Проверка SSL-сертификата – опция включает и выключает процесс проверки подлинности и валидности SSL-сертификата. Сертификат — это цифровой «паспорт» сайта. SSL – это криптографический протокол, который обеспечивает безопасную передачу данных между браузером и сервером. Проверка возможна только в том случае, если сертификат TI-платформы выпущен авторизованным центром сертификации, который может удостоверить данный сертификат, иначе эту проверку следует отключить (для самоподписанных сертификатов).

Проверка файловых и сетевых артефактов – опции включают и выключают проверку в EDR файловых артефактов (хеши SHA-256) или сетевых артефактов (IP-адреса и домены).

Модуль обнаружения уязвимостей – опция включает/отключает модуль обнаружения уязвимостей в EDR.

Синхронизация конфигурации – опция включает/отключает синхронизацию между EDR и TI-платформой внешних наборов аналитики, то есть при включенной синхронизации изменения в наборах TI-платформы приведут к изменениям внешних наборов аналитики EDR, и наоборот, при выключенной синхронизации таких изменений во внешних наборах EDR происходить не будет.

Отправлять IP-адреса для сбора статистики – опция включает или отключает отправку IP-адресов для сбора статистики. Суть этой опции в том, что если EDR отсылает пару артефактов IP-адрес+домен, то проверяется только домен (и только по нему может быть сформирован инцидент при соответствующем вердикте), а IP-адрес отбрасывается и не анализируется, но IP-адреса могут быть отправлены и сохранены в активности TI-платформы для дальнейшего разбора. Поэтому включение опции сохраняет такие IP-адреса на TI-платформе, что позволяет в дальнейшем аналитику платформы их проанализировать.

При необходимости конфигурацию настроек или несколько таких конфигураций можно удалить, используя кнопки **Удалить настройку** ( ) или **Удалить выбранные**.

Локальная среда проверки файлов

Интеграция с TI для анализа файлов позволяет EDR отправлять файлы на TI-платформу для их дальнейшей проверки с помощью песочницы. Настройки за небольшим исключением повторяют настройки интеграции с TI для отправки артефактов.

Чтобы настроить интеграцию с TI-платформой для анализа файлов, необходимо выполнить следующие действия:

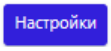
1) Определить название для интеграции;
2) Задать актуальное значение хоста TI-платформы (IP-адрес или имя хоста);
3) Задать актуальное значение API-ключа;
4) Определить тайм-аут;
5) Включить или отключить шифрование;
6) Включить или выключить проверку SSL-сертификата.

Интеграция с LDAP

В области **Интеграция с LDAP** администратор может настроить взаимодействие между серверами EDR и LDAP-сервером. С помощью иконки Редактировать настройку можно редактировать текущую настройку. Окно заполнения параметров при редактировании представлено на рисунке 99.



Рисунок 99 – Редактирование настроек

Для просмотра профилей созданных настроек требуется нажать по иконке 

.

Информация на странице **Настройки LDAP** представлена в виде таблицы со следующими полями:

1) Кнопка раскрытия информации по настройке;
2) Кнопка выбора;
3) Название LDAP-сервера;
4) DN;
5) Метод шифрования;
6) Сетевые адреса LDAP;
7) Время создания;
8) Время обновления;
9) Управление.



Примечание

Активная в данный момент настройка выделяется светло-желтым цветом .

Настройки, в которых не указаны сетевые адреса, нельзя выбрать из списка в строке **Активная настройка**.

В поле **Управление** с помощью иконок возможно выполнить следующие действия:

– проверить соединение с LDAP (нажать по иконке , дождаться ответа, успешное подключение будет отмечено иконкой , неуспешное);

– редактировать настройку (нажав по иконке);

– настроить сетевой адрес и порт LDAP-сервера (нажав по иконке);

– изменить пароль LDAP-сервера (нажав по иконке);

– удалить настройку интеграции с LDAP-сервером (нажав по иконке).

Для настройки интеграции с LDAP необходимо выполнить следующие действия:

1) Определить название LDAP-сервера.
2) Определить **имя LDAP-атрибута**, которое соответствует имени пользователя. Настройка Имя LDAP-атрибута, которое соответствует имени пользователя может принимать разные значения в зависимости от типа LDAP-провайдера и корпоративных стандартов. В качестве примеров можно привести sAMAccountName (логин для входа в домен Windows (короткое имя), самый частый вариант для корпоративных сетей Windows), uid (уникальный идентификатор пользователя, используется в OpenLDAP, FreeIPA), userPrincipalName (полное имя пользователя в формате email). То есть правильно для Active directory выбирать атрибут sAMAccountName или userPrincipalName, а для OpenLDAP и FreeIPA атрибут uid.
3) Определить базу, используемую для поиска пользователей. Это корневая папка или начальная точка в дереве LDAP-каталога, с которой начинается поиск пользователей. Типичным вариантом базы будет CN=Users, DC=mycompany, DC=local (стандартное расположение в AD). В OpenLDAP и FreeIPA также используется понятие Base DN (база для поиска) и атрибут для имени пользователя, однако, в отличие от AD, в OpenLDAP и FreeIPA обычно используются другие атрибуты и структура каталога.
4) Определить базу, используемую для поиска групп (DN группы для ограничения доступа). Настройка, которая указывает системе, где именно в LDAP-каталоге искать группы для проверки членства пользователей и назначения прав доступа.

5) Определить DN. DN (Distinguished Name) — это строка, которая однозначно идентифицирует запись в LDAP-каталоге. Она строится путем соединения относительных имен самой записи и всех ее родительских записей вплоть до корня дерева. DN состоит из одной или нескольких пар атрибут=значение, разделенных запятыми. Движение идет от самой конкретной записи к корню дерева. DN читается справа налево, от корня (самого общего) к записи (самой конкретной). Чем дальше слева оказывается элемент, тем он "ниже" в иерархии. В случае с интеграцией с EDR DN– это логин сервисного пользователя, у которого есть необходимые права на поиск информации о других пользователях, группах и политиках. Программа устанавливает сессию от этого пользователя и начинает проверку по установленному тайм-ауту – функция синхронизации. Ее смысл в том, чтобы актуализировать данные и сессии пользователей. Например, пользователь был заблокирован/удален на стороне LDAP-сервера (при этом у него активная сессия в EDR, следовательно нужно закрыть его сессию на стороне EDR).
6) Определить тайм-аут в секундах для запросов LDAP. Если установить значение 0, то тайм-аут будет отсутствовать.
7) Установить фильтрацию пользователей LDAP. Фильтры LDAP используются для поиска записей в каталоге, которые соответствуют определенным критериям. Они следуют стандарту, описанному в RFC 4515. Базовый формат: (атрибут=значение). Например, (cn=*) – ищет все записи, у которых вообще существует атрибут cn (Common Name), независимо от его значения.
8) Выбрать метод шифрования. Используется для защиты запросов к каталогам. Без шифрования злоумышленник может перехватить логины и пароли. Можно выбрать Start TLS, Simple TLS или Plain.

Примечание

StartTLS – это команда «давай шифровать», которая позволяет преобразовать существующее незашифрованное сетевое соединение в безопасное, используя протокол TLS.

Simple TLS – это метод установления защищенного соединения, при котором TLS-шифрование запускается в самом начале сессии, до какой-либо аутентификации.

Plain – это метод аутентификации, при котором клиент отправляет серверу свои учетные данные (логин и пароль) в открытом, незашифрованном виде. Использование Plain-аутентификации делает инфраструктуру уязвимой для некоторых типов атак.

9) Выбрать LDAP-провайдера. Это может быть служба каталогов Active Directory, OpenLDAP или FreeIPA.
10) Определить LDAP-атрибут для email. Если поле останется пустым, то синхронизации данных не будет. По умолчанию используется атрибут mail.
11) Определить LDAP-атрибут для имени. Если поле останется пустым, то синхронизации данных не будет. По умолчанию используется атрибут givenName.
12) Определить LDAP-атрибут для фамилии. Если поле останется пустым, то синхронизации данных не будет. По умолчанию используется атрибут sn.
13) Определить LDAP-атрибут для роли. Заполняется, если в LDAP есть атрибут, несущий информацию о роли пользователя. Если оставить поле пустым, то синхронизация не выполняется.
14) Установить или снять флаги для следующих компонентов: Включить проверку SSL-сертификата, Преобразовать имена в нижний регистр, Игнорировать всё после @ в имени пользователя. Проверка SSL-сертификата возможна только в том случае, если сертификат LDAP-сервера выпущен авторизованным центром сертификации, который может удостоверить данный сертификат, иначе эту проверку следует отключить (для самоподписанных сертификатов). Если включена опция Игнорировать всё после @ в имени пользователя, то EDR игнорирует всё после первой @ в имени пользователя LDAP, отправленном пользователем при входе. Если используется userPrincipalName в Active Directory, то следует отключить эту опцию, так как userPrincipalName содержит @.

15) Нажать кнопку **Добавить**.

16) **После добавления сервера на страницу Настройки LDAP необходимо добавить адрес и порт**, по которому будет происходить взаимодействие между сервером LDAP и EDR (рис. 100). Обычно значение порта равно 389.

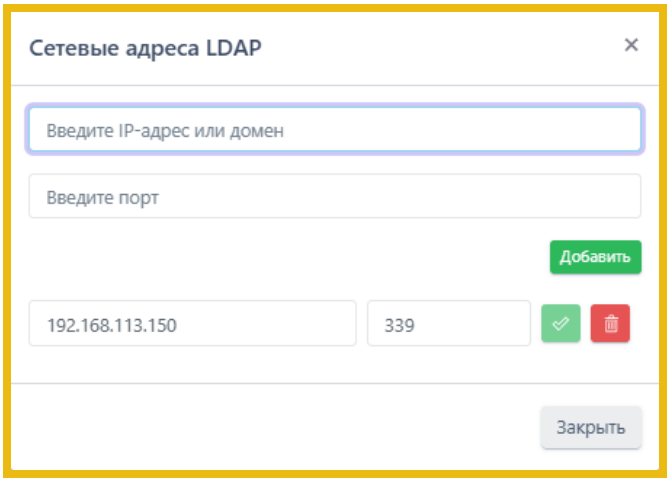


Рисунок 100 – Окно ввода сетевых адресов LDAP

При необходимости конфигурацию настроек или несколько таких конфигураций можно удалить, используя кнопки **Удалить настройку** ( ) или **Удалить выбранные**.

Как применяется LDAP-интеграция?

Общие сведения

При активной интеграции LDAP-пользователи могут входить в веб-интерфейс EDR по доменным учётным данным через отдельную форму входа **LDAP**, без хранения их паролей в EDR. В этом случае проверка пароля выполняется на стороне сервера LDAP.

Состояния учётных записей

В EDR учётная запись пользователя может находиться в одном из трёх состояний:

– локальный пользователь EDR (без связи с LDAP) создаётся администратором, вход только по локальному паролю EDR;

— локальный пользователь EDR, связанный с пользователем LDAP (может входить как по локальному паролю, так и через форму LDAP).

— пользователь LDAP (учётная запись, созданная автоматически при первом входе через форму LDAP).

Процесс входа через LDAP

При входе через форму **LDAP** система выполняет следующие шаги:

1) Поиск пользователя в службе каталогов по заданной базе поиска и фильтру;
2) Проверка введённого пароля путём подключения (bind) к LDAP под учётными данными этого пользователя. Если пароль неверен, то во входе будет отказано.
3) Если проверка пройдена и пользователь ещё не зарегистрирован в EDR, то учётная запись создаётся автоматически.
4) Если учётная запись в EDR заблокирована, то во входе будет отказано.

Какие пользователи могут войти

Возможность входа определяется параметрами интеграции LDAP. Пользователь должен одновременно удовлетворять всем условиям фильтра поиска (таблица 52).

Таблица 52 – Параметры интеграции LDAP

Параметр настройки	Влияние на круг пользователей
База поиска (base)	Каталог (поддерево), в котором ищется пользователь. Войти могут только объекты, находящиеся в этой базе.
Атрибут имени (uid)	Атрибут, по которому логин сопоставляется с записью LDAP (например, sAMAccountName, uid, userPrincipalName).
Фильтр пользователей (user_filter)	Необязательный дополнительный фильтр (RFC 4515). Позволяет ограничить вход, например, по типу или статусу учётной записи. Если не задан — не ограничивает.
База групп (group_base)	Необязательное ограничение по членству в группе. Если задано — войти смогут только члены указанной группы. Если не задано — ограничения по группе нет.



Примечание

Если фильтр пользователей и база групп не заданы, войти сможет любая учётная запись из базы поиска, прошедшая проверку пароля. Для ограничения доступа используйте фильтр пользователей и/или базу групп.

Автоматическое создание учётной записи

Предварительно создавать локальную учётную запись в EDR не требуется. При первом успешном входе пользователя LDAP его учётная запись в EDR создаётся автоматически. Локальный пароль для такой учётной записи не задаётся (вход выполняется только через форму LDAP).

Из службы каталогов при этом могут синхронизироваться атрибуты пользователя (имя, фамилия, адрес электронной почты) — в соответствии с настройками сопоставления атрибутов.

Назначение ролей и прав доступа

Роль (права доступа) автоматически не назначается. Учётная запись, созданная при первом входе через LDAP, не имеет ни одной группы прав, то есть не обладает никакими полномочиями в системе.

Практические следствия:

— пользователь успешно войдёт в систему, но без назначенной роли не сможет просматривать данные и выполнять действия;

— полноценный доступ появляется только после того, как администратор вручную назначит учётной записи одну или несколько ролей (групп прав);

— встроенные роли (например, «Аналитик L1») предоставляются только при явном назначении и не выдаются по умолчанию;

Рекомендация. После настройки интеграции LDAP заранее определите политику назначения ролей и назначайте права новым пользователям сразу после их первого входа.

Настройка доступа пользователей из нескольких OU

Одновременно в EDR активна только одна конфигурация LDAP с единственной базой поиска. При этом поиск пользователя выполняется рекурсивно — по указанной базе и всем вложенным в неё организационным подразделениям (OU). Поэтому доступ пользователей из разных OU обеспечивается не несколькими

настройками, а выбором общей базы поиска, охватывающей нужные подразделения, и (при необходимости) дополнительным фильтром.

Ограничения. Несколько активных конфигураций LDAP или несколько баз поиска не поддерживаются, поэтому необходимо использовать общую базу. Несколько адресов серверов в одной настройке служат для отказоустойчивости одного каталога, а не для подключения разных OU. Членство в OU или группе LDAP само по себе прав в EDR не даёт, роль назначается администратором вручную.

Интеграция с SIEM (экспорт событий мониторинга)

В области **Интеграция с SIEM (экспорт событий мониторинга)** уполномоченный пользователь может настроить взаимодействие между сервером EDR и SIEM. На странице показаны настройки интеграции, которые активны на данный момент.

Для редактирования настроек интеграции необходимо нажать ЛКМ по кнопке 

, после чего откроется окно редактирования, представленное на рисунке 101.

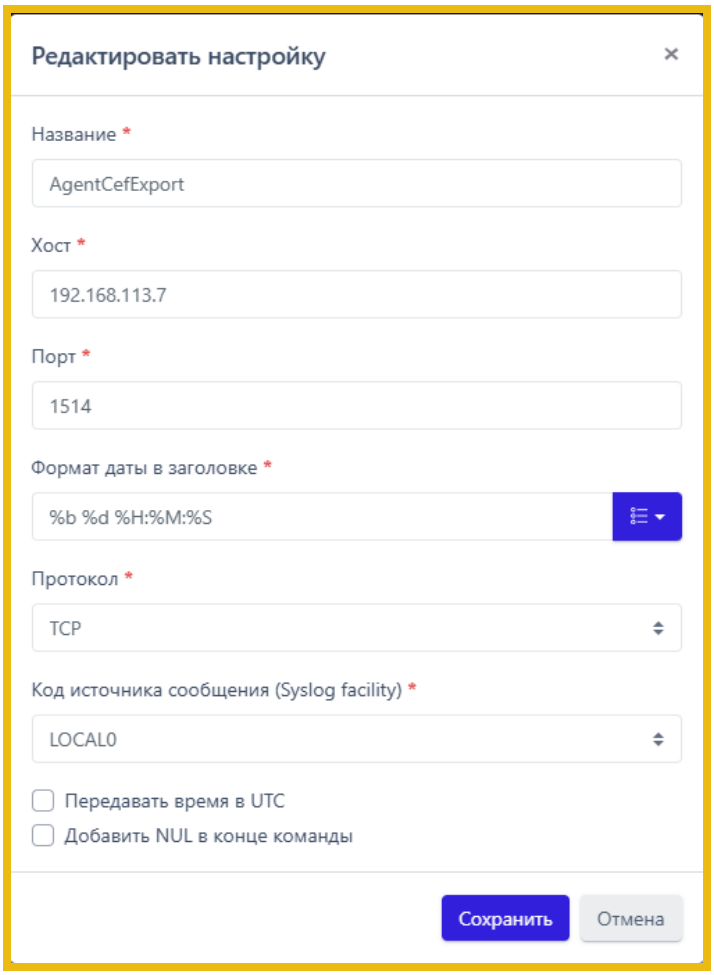


Рисунок 101 – Окно редактирования настроек интеграции с TI

После редактирования настроек следует нажать по иконке **Сохранить**.

В области **Интеграция с SIEM** для перехода на страницу со списком профилей с настройками следует нажать по иконке Настройки.

Страница со списками профилей настроек представлена на рисунке 102.

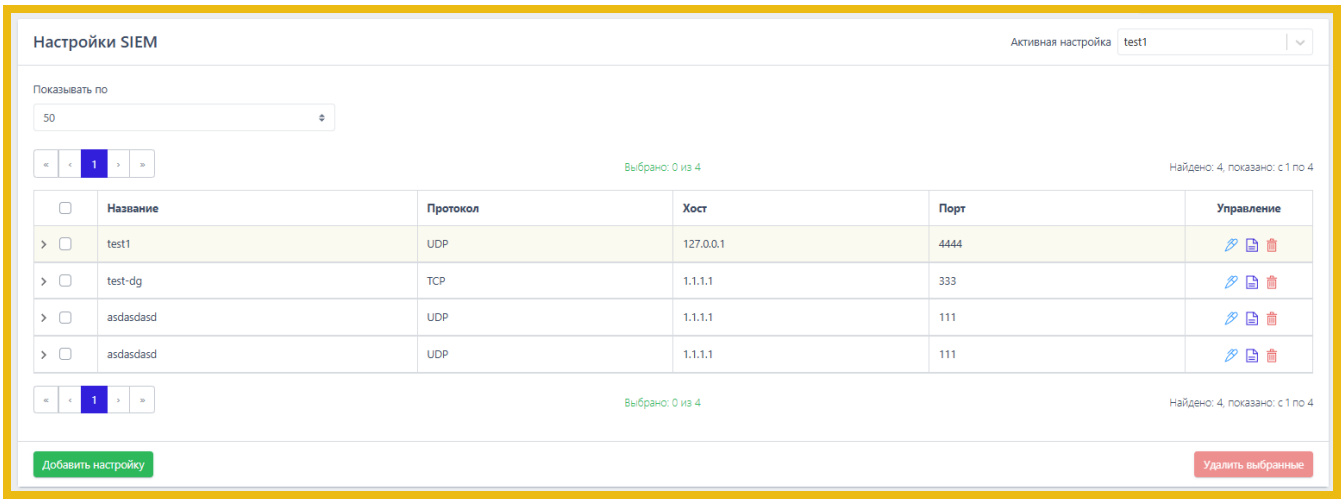


Рисунок 102 – Список профилей с настройками интеграции с SIEM

Информация на данной странице представлена в виде таблицы со следующими областями:

– кнопка выбора;

– иконка, раскрывающая информацию по параметрам настройки ( );

– название профиля настройки;

– протокол;

– хост;

– порт;

– управление (редактирование настройки ( ), редактирование файла конфигурации экспорта событий ( ), удаление настройки ( )).

Выбор активной настройки осуществляется администратором в строке **Активная настройка** (Активная настройка active-config).

На странице можно добавить настройку, нажав по иконке Добавить настройку (рис. 103).

Параметры для заполнения при добавлении новой настройки аналогичны параметрам, указанным в окне редактирования настройки.

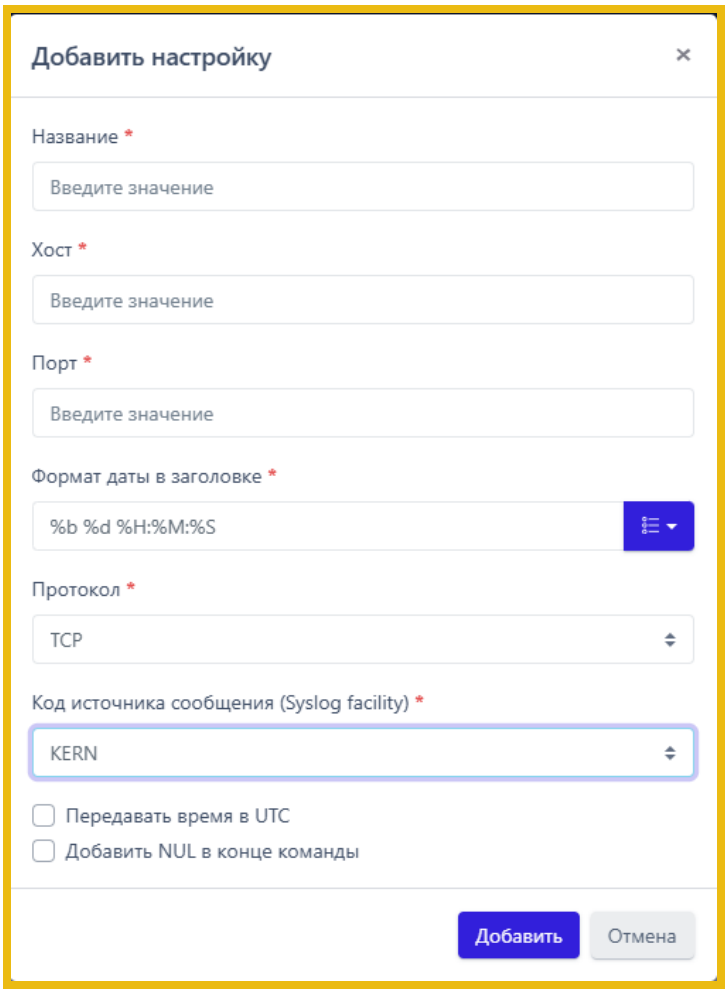


Рисунок 103 – Окно добавления настройки интеграции между TI-платформой и EDR

Название – в поле указывается название настройки интеграции.

Хост – в поле указывается имя хоста SIEM-системы (домен).

Порт – в поле указывается порт для соединения между EDR и SIEM (обычно 514).

Формат даты в заголовке – устанавливает различные форматы дат для заголовка, можно выбрать из нескольких шаблонов (кнопка).

Протокол – можно выбрать один из представленных в списке протоколов (TCP или UDP).

Код источника сообщения (Syslog facility) – Facility — это один из стандартных параметров протокола syslog (RFC 3164/5424). Он указывает, какая часть системы или какой тип приложения сгенерировал лог-сообщение.

В SIEM-системах facility используется для:

1) Фильтрации и маршрутизации событий (например, все сообщения от DAEMON направить в отдельный поток).
2) Нормализации — чтобы понимать, к какой категории относится событие, даже если текст сообщения не содержит явной метки.
3) Приоритизации — некоторые facility по умолчанию считаются более важными, например, KERN.

Опции передачи времени в UTC и добавления NUL в конце команды (опция предназначена для обхода проблемы парсинга многострочных сообщений в реализации протокола Syslog TCP).

После добавления настройки необходимо в поле **Управление** отредактировать файл конфигурации экспорта событий ( ). Файл конфигурации экспорта событий или CEF-файл – это файл в текстовом формате для обмена данными о событиях.

Для понимания, как редактировать CEF-файл, разберем примерную конфигурацию (рис. 104):



```
{
    "cef": {
        "version": 0,
        "device": {
            "vendor": "RT-IB",
            "product": "EDR",
            "version": "1.0"
        },
        "severity": {
            "NORMAL": 1,
            "GUARDED": 3,
            "ELEVATED": 6,
            "HIGH": 8,
            "SEVERE": 10
        }
    },
    "query": {
        "bool": {
            "filter": [
                { "terms":  { "t": [0, 1, 2] }},
                { "terms": { "svrt": [3, 4]}}
            ],
            "must": [
                { "query_string": {
                    "query": "sha256:*",
                    "default_operator": "AND"
                }}
            ]
        }
    },
    "mapping": {
        "default": {
            "app": "filePath"
        },
        "process": {
            "app": "cs2"
        }
    }
}
```

Рисунок 104 – Пример конфигурации CEF-файла

Конфигурация определяет следующие настройки:

1) Обязательные параметры заголовка CEF;
2) Сопоставление уровней критичности (severity);
3) Фильтрацию событий в Elasticsearch;
4) Маппинг полей внутренней модели событий в модель CEF (под маппингом полей подразумевается процесс установления соответствия между полями модели данных из EDR и полями CEF-модели).

Примечание

Подробное описание полей модели данных RT Protect EDR содержится в разделе 7.

Ознакомиться со стандартом CEF, списком полей и их обозначением можно по следующей ссылке:

https://1275.ru/wp-content/uploads/2024/12/cef-implementation-standard-27.pdf

---

1. Блок cef.

Блок cef содержит параметры, необходимые для формирования обязательной части CEF-заголовка (рис. 105).

```
"cef": {
    "version": 0,
    "device": {
        "vendor": "RT-IB",
        "product": "EDR",
        "version": "1.0"
    },
    "severity": {
        "NORMAL": 1,
        "GUARDED": 3,
        "ELEVATED": 6,
        "HIGH": 8,
        "SEVERE": 10
    }
}
```

Рисунок 105 – Обязательная часть CEF-заголовка

version – версия формата CEF, обычно используется значение 0 (актуальная версия формата), формат заголовка – CEF:Version|Device Vendor|Device Product|Device Version|Signature ID|Name|Severity|.

device – описывает источник события в виде:

1) vendor – производитель решения;
2) product – название продукта;
3) version – версия продукта.

severity – маппинг уровней критичности из внутренней модели событий в шкалу CEF (от 0 до 10):

4) Normal (Информация) – 1;
5) Guarded (Низкая) – 3
6) Elevated (Средняя) – 6;
7) High (Высокая) – 8;
8) Severe (Критичная) – 10.

Маппинг позволяет привести внутреннюю модель критичности к стандартной шкале CEF (во внутренней модели существует только 5 уровней критичности, представленные в списке выше), что в свою очередь позволяет внешним SIEM-системам корректно обрабатывать события.

2. Блок query.

Блок описывает запрос к Elasticsearch, по которому отбираются события для экспорта в SIEM:

```
"query": {
    "bool": {
        "filter": [
            { "terms":  { "t": [0, 1, 2] }},
            { "terms": { "svrt": [3, 4]}}
        ],
        "must": [
            { "query_string": {
                "query": "sha256:*",
                "default_operator": "AND"
            }}
        ]
    }
}
```

Рисунок 106 – Пример написания блока query

Блок позволяет определить критерии выборки событий, экспортировать только релевантные события. Блок использует синтаксис Elasticsearch Query DSL. В приведенном выше примере **filter** – фильтрация по типам событий (**t**) и уровням критичности (**svrt**); **must** – обязательное условие наличия поля **sha256**.

3. Блок mapping.

Блок mapping определяет сопоставление полей внутренней модели EDR-событий полям CEF. Общая структура представлена на рисунке 107.



Рисунок 107 – Общая структура блока mapping

default – базовый маппинг, применяемый ко всем событиям, формат базового маппинга – "поле_внутренней_модели":"поле_CEF", например, "app":"filePath", это означает, что внутреннее поле **app** (полное имя исполняемого файла процесса) будет записано в CEF-поле **filePath.** Если событие имеет конкретный тип (например, **process**), используется соответствующий блок маппинга. Он перекрывает значения из default-маппинга только для указанных полей. Правила приоритета – сначала применяется default, если же для типа события определен отдельный блок, то его значения являются более приоритетными, но только для указанных полей, а остальные поля берутся из default-маппинга. Доступные значения типов событий представлены в таблице 53.

Таблица 53 – Наименования событий

Тип события	Обозначение
network	Сеть

filesystem	Файлы
registry	Реестр
etw	Журналы
process	Процессы
system	Система
session	Сессии
calls	Вызовы
antiransomware	Антишифр
usb	Контроль USB

Экспорт событий безопасности

Экспорт через Webhook – современный, легковесный метод доставки событий безопасности в SIEM. При настройке важно корректно задать тайм-аут, SSL-политику и дату начала, чтобы избежать потерь или дублирования событий.

Для корректной работы экспорта необходимо добавить настройку экспорта событий безопасности. После нажатия кнопки **Настройки** откроется страница **Экспорт событий безопасности**, на которой необходимо нажать кнопку **Добавить настройку**. После этого откроется окно **Добавить настройку**, в котором необходимо добавить обязательные настройки (рис. 108).

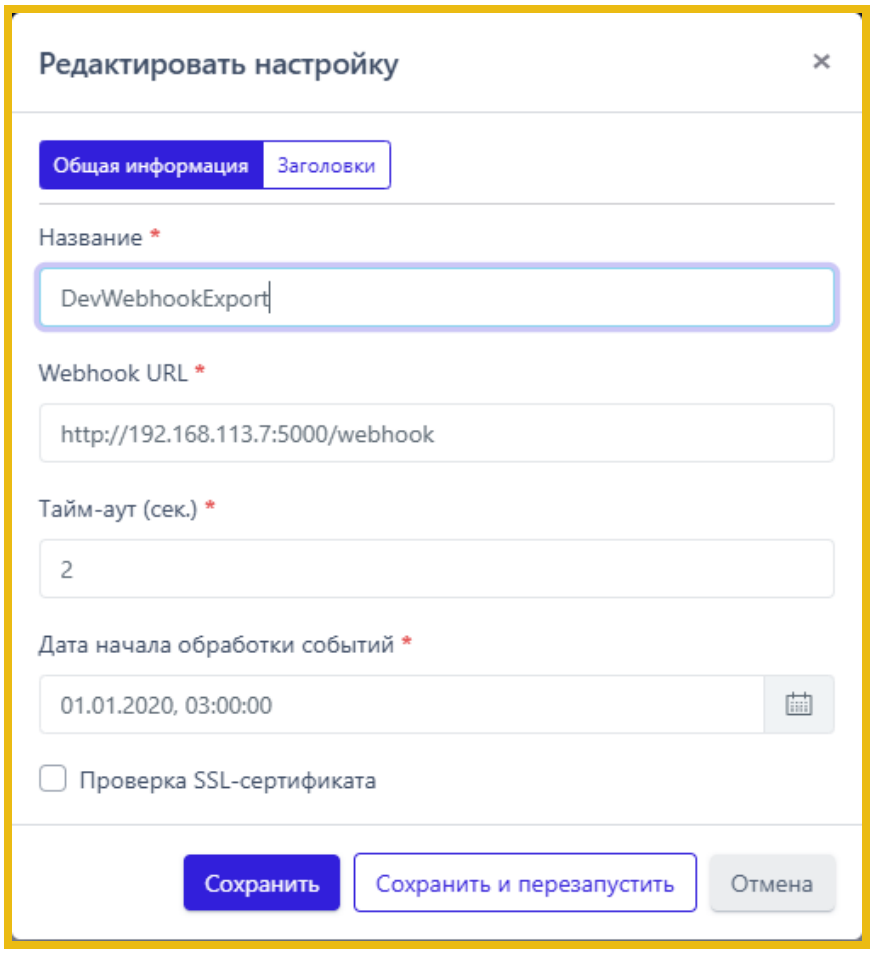


Рисунок 108 – Настройки экспорта событий безопасности

Название – в строке прописывается произвольное название интеграции между EDR и SIEM.

Webhook URL – в строке прописывается конечная точка со стороны SIEM, которая принимает HTTP-запросы от EDR-сервера.

Тайм-аут – временной период, в течение которого должна выполняться отправка событий безопасности.

Дата начала обработки событий – время, с которого будут передаваться события.

Флаг **Проверка SSL-сертификата** – проверяется валидность сертификата SIEM, если флаг установлен.

Для интеграции с SIEM также необходимо настроить заголовки.

Заголовки — это метаданные, которые передаются вместе с HTTP-запросом от EDR к SIEM. Они располагаются в начале HTTP-сообщения до тела (payload) и содержат служебную информацию о запросе: формат данных, способ кодировки, аутентификацию, тип соединения и др. Без заголовков SIEM не сможет правильно интерпретировать пришедшие события.

Заголовки решают следующие задачи:

1) Идентификация формата данных – SIEM должен знать, как парсить тело запроса (JSON, XML, plain text);
2) Аутентификация и авторизация – подтверждение, что запрос действительно от легитимного источника;
3) Управление соединением – контроль таймаутов, сжатия, кэширования;
4) Отладка и трассировка – уникальные идентификаторы запросов для поиска проблем.

Основные заголовки, используемые при экспорте событий в SIEM представлены в таблице 54.

Таблица 54 – Примеры заголовков

Заголовок	Пример значения	Назначение
Content-Type	application/json	Указывает формат тела запроса. SIEM ожидает JSON – будет парсить как JSON; если text/plain – обработает как строку.
Authorization	Bearer eyJhbGci… или Basic dXNlcjpwYXNz	Передаёт учётные данные или токен для доступа к webhook URL. Без него SIEM может отклонить запрос.
User-Agent	SecurityAudit/1.0	Идентифицирует программное обеспечение источника (удобно для логирования и фильтрации).
X-Event-ID	a1b2-c3d4-5678	Уникальный идентификатор события, чтобы SIEM мог обнаружить дубликаты.
X-Timestamp	2026-04-30T12:34:56Z	Временная метка события на источнике (если не включена в тело).
X-Forwarded-For	10.0.0.5	Оригинальный IP-адрес, если запрос идёт через прокси.
Content-Encoding	gzip	Если тело сжато (например, для уменьшения трафика).
Accept	application/json	Что ожидает источник в ответе от SIEM (не всегда используется).
Connection	keep-alive	Указывает, переиспользовать ли TCP-соединение для нескольких событий.

После добавления и сохранения настроек после заполнения формы необходимо нажать кнопку **Добавить**.

8.9.2. Настройки

В разделе отображаются настройки Elasticsearch. В контексте RT Protect EDR Elasticsearch – это платформа для поиска и анализа событий, отправляемых с агентов серверу.

На странице **Настройки** отображаются следующие характеристики Elasticsearch:

1) Состояние БД;
2) Период хранения данных БД в днях;
3) Количество свободной памяти в кластере БД в процентах;
4) Количество свободного места на дисках в кластере БД.

БД может принимать следующие состояния:

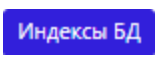
1) Все данные доступны;
2) Имеются нераспределенные реплики/шарды;
3) Часть данных недоступна.

Состояние **Все данные доступны** означает, что кластер Elasticsearch находится в идеальном рабочем состоянии и может гарантировать полную целостность и доступность данных (все шарды активны и распределены, кластер в зеленом состоянии, данные доступны для всех операций).

Кластер представляет собой одну или несколько нод (серверов), объединенных в одно целое. Нода – это один экземпляр Elasticsearch (часть кластера). Шарды – это неделимые части индекса, основные единицы хранения данных в Elasticsearch. Они служат для горизонтального масштабирования и повышения производительности. Реплики – это точные копии первичных шардов. Они обеспечивают отказоустойчивость и повышают производительность чтения данных.

Состояние **Имеются нераспределенные реплики/шарды** говорит о том, что в кластере Elasticsearch есть шарды или реплики, которые не могут быть размещены на каких-либо узлах в соответствии с политикой распределения кластера.

Состояние **Часть данных недоступна** говорит о том, что часть шардов недоступна, а соответствующие данные потеряны и поиск с записью для этих данных невозможны.

Нажатие кнопки 

открывает одноименную страницу, на которой можно просмотреть информацию об индексах и их состояниях. Индекс можно фильтровать по состоянию и статусу (закрыт, активен).

9. Машинное обучение в Программе

9.1 Классификация на сервере

В RT Protect EDR реализован статический анализ инцидентов на основе ИИ. Модель состоит из encoder-трансформера на основе RoBERTa и полносвязной нейронной сети, на вход которой поступают исходные данные инцидентов информационной безопасности (рис. 109). Данная архитектура модели выбрана в связи с большим количеством текстовых признаков, присущих инцидентам. Модель представляет собой отдельный модуль, взаимодействие с которым происходит с помощью API-вызовов. Входным параметром данного модуля является текст, содержащий в себе один или несколько JSON объектов. Дальнейшие преобразования включают в себя проверку на валидность переданных объектов, нормализацию JSON, агрегацию нескольких JSON в один (в случае, если на вход модуля поступило несколько связанных объектов), фильтрацию полей и приведение их названий к общему виду, а также обогащение с помощью RT Protect TI и дополнительной информации из источника данных Elastic, не вошедшей в исходные JSON-объекты. К признакам, используемым для работы модели машинного обучения, относятся: сработавшее правило, название организации, имя пользователя, командная строка процесса (а также родительского и прародительского процессов), имя модуля-инициатора, путь к модулю-инициатору, путь к запущенному приложению, результаты проверок индикаторов компрометации (sha256, md5, IP-адреса, домены, url), информация о локальном/удалённом хосте, IP-адреса задействованных хостов, описание данных хостов, изменения реестра Windows. Все перечисленные значения опциональны, что позволяет классифицировать различные инциденты информационной безопасности, которые, из-за своей специфики, могут иметь лишь те или иные признаки.

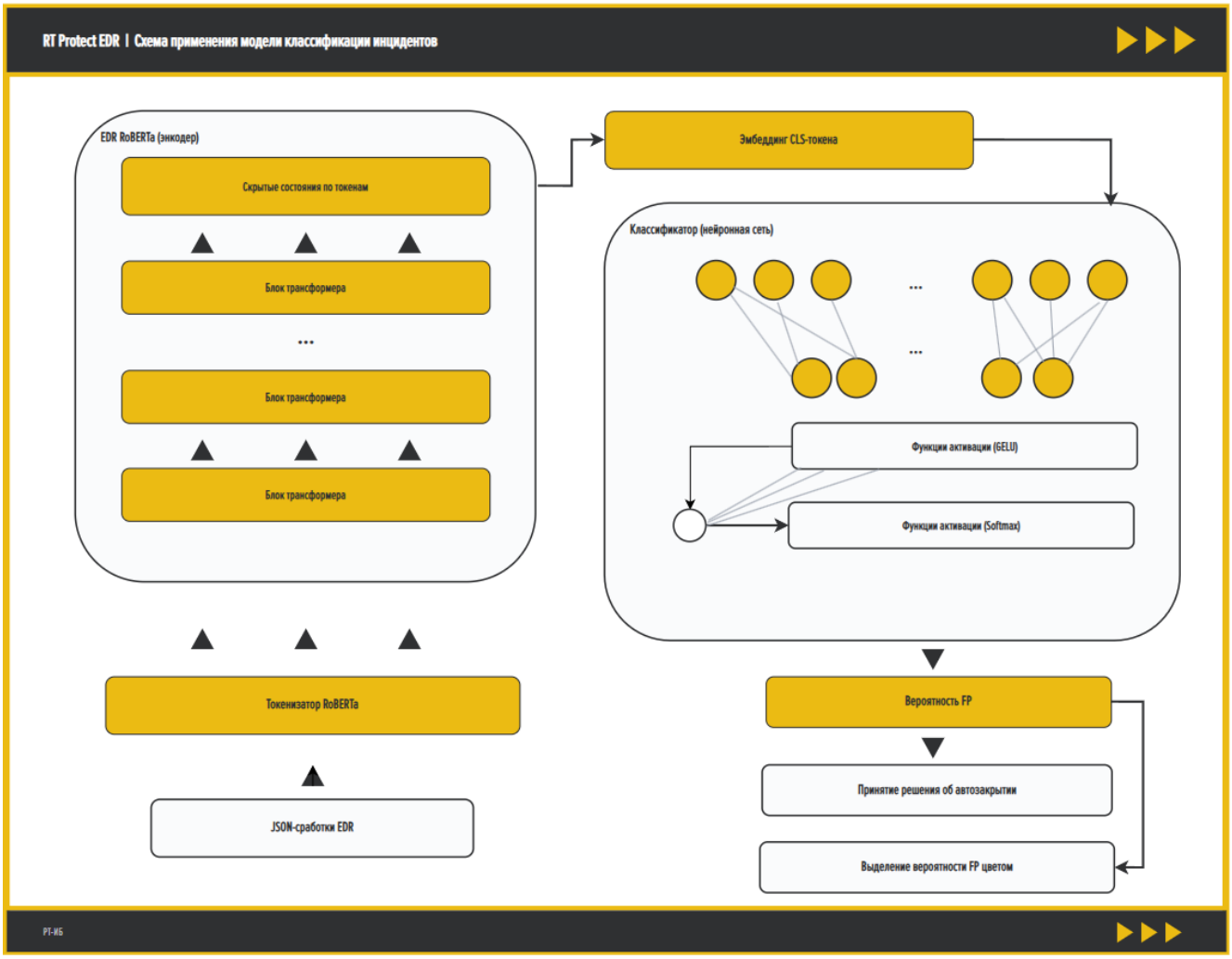


Рисунок 109 – Схема применения модели классификации инцидентов

После данного этапа происходит классификация инцидента. В качестве результата выдается значение в диапазоне [0;1], соответствующее вероятности того, что инцидент является ложноположительным срабатыванием, а также идентификатор autoClose, определяющий, можно ли автоматически закрыть данный инцидент. Модель содержит в себе несколько порогов срабатывания, которые уточняются при переобучении модели. Первая группа порогов содержит один порог (приблизительно от 0.9 до 0.95), который говорит о том, что инцидент является ложным срабатыванием правила и должен быть автозакрыт. Второй тип порогов (примерно 0.3, 0.5 и 0.7) используется для сопоставления инциденту цветовой метки («Красный», «Оранжевый», «Жёлтый» или «Зелёный»), отражающей серьёзность инцидента. Вердикт модели передается как ответ API-вызова, который обрабатывается SOAR-системой для автоматического закрытия инцидента или добавления цветовой метки, использующейся для составления приоритета обработки инцидентов аналитиками первой линии.

Сама модель представляет собой конфигурационные файлы в формате safetensors и json, которые содержат в себе веса признаков модели, словарь токенизатора модели, а также пороговые значения вынесения вердиктов автозакрытия и соответствия цветовым меткам. Эти файлы формируются в результате обучения модели в тестовой лаборатории в автоматическом режиме с помощью Airflow, что позволяет модели оставаться актуальной с течением времени.

Обучение модели производится на языке python с использованием библиотек scikit-learn, pytorch и transformers. В качестве обучающих выборок используется собственные наборы данных. Первый из них это набор данных для обучения без учителя, используемый для получения качественного численного представления посредством моделей, основанных на BERT-архитектуре, а второй уже является набором данных для обучения с учителем RoBERTa-подходом с целью оптимизации классификатора над признаками, полученными из Bert-модели.

9.2 Классификация на агенте

В RT Protect EDR реализован статический анализ исполняемых файлов на основе ИИ. В частности, применяется модель логистической регрессии, на вход которой поступают статические признаки исполняемых файлов. Данный тип модели выбран ввиду ее быстродействия и минимальных требований к вычислительным ресурсам, поскольку она работает в синхронном режиме на агентских компьютерах.

Далее будет описана схема применения модели классификации ПО, применяемая в агенте RT Protect EDR (рис. 110).

Для отслеживания запуска файлов на исполнение драйвер агента в обработчике открытия файлов анализирует флаги открытия файла.

При наличии запрашиваемого доступа «на исполнение» (FILE_EXECUTE), модуль минифильтра драйвера открывает секцию файла (для его последующего чтения в службе) и передает задачу на анализ файла службе агента посредством специального порта взаимодействия (CommunicationPort). Служба, получив задание на анализ файла, передает управление в модуль сбора признаков исполняемого файла. К признакам, необходимым для модели машинного обучения, относятся: физический и виртуальный размер файла (в байтах), флаги из заголовков исполняемого файла (PE-headers), наличие оверлея, имя секции, содержащей

точку входа программы, энтропия файла, количество url-строк, количество строк-путей, количество сигнатур ‘MZ’, количество экспортируемых и импортируемых функций, имена секций и др.

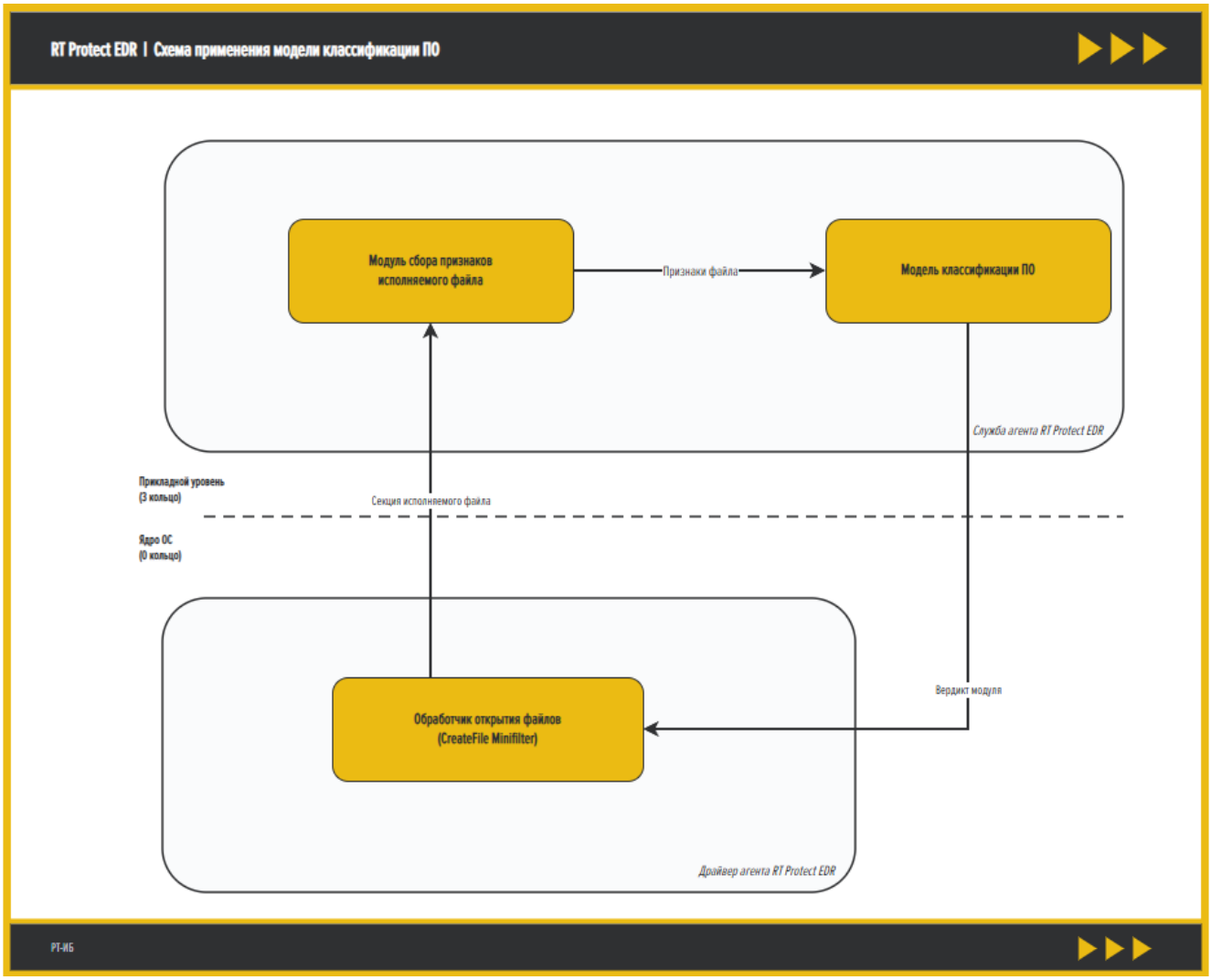


Рисунок 110 – Схема применения модели классификации ПО

После сбора перечисленных признаков вызывается функция классификации файла. На вход она принимает собранные признаки. В качестве результата выдает значение в диапазоне [0;1], соответствующее вероятности того, что файл является вредоносным. Модель содержит в себе 2 порога срабатывания, которые уточняются от версии к версии модели. Первый более низкий порог (приблизительно от 0.8 до 0.9) говорит о том, что файл подозрительный, второй (ближе к 1) – файл вредоносный. Вердикт модели передается обратно в драйвер, который на его основе выполняет предписываемые действия: пропустить, отправить предупреждение (alert) или заблокировать запуск файла с уведомлением.

Сама модель представляет собой конфигурационный файл в формате json, который содержит в себе веса признаков, а также пороговые значения вынесения вердикта. Этот файл формируется в результате обучения модели в тестовой лаборатории, а затем загружается на сервер EDR. В свою очередь сервер EDR рассылает конфигурационный файл модели по агентам.

Обучение модели производится на языке python с использованием библиотеки scikit-learn. В качестве обучающих выборок используются наборы: sophos/SOREL-20M (https://github.com/sophos/SOREL-20M), bodmas (https://github.com/whyisyoung/BODMAS), Malware Dataset IDN (https://ieee-dataport.org/documents/malware-dataset-idn), а также собственный набор файлов, собранных в тестовой лаборатории.

9.3 Список компонентов, используемых в модели ИИ

Полный список сторонних компонентов, используемых в модели машинного обучения, приведен в таблице 55.

Таблица 55 – Сторонние компоненты

№ п/п	Наименование стороннего компонента	Правообладатель	Сведения о документах, подтверждающих наличие оснований на использование компонента	Лицензии	Вид лицензии
1	scikit-learn	The scikit-learn developers	https://github.com/scikit-learn/scikit-learn?tab=BSD-3-Clause-1-ov-file#readme	BSD 3-Clause	Свободная лицензия
2	pytorch	Facebook, Inc, Idiap Research Institute, Deepmind Technologies, NEC Laboratories America, NYU	https://github.com/pytorch/pytorch/blob/main/LICENSE	BSD-Style	Свободная лицензия
3	pandas	AQR Capital Management, LLC, Lambda Foundry, Inc. and PyData Development Team, Open source contributors	https://github.com/pandas-dev/pandas/blob/main/LICENSE	BSD 3-Clause	Свободная лицензия
4	numpy	NumPy Developers	https://github.com/numpy/numpy/blob/main/LICENSE.txt	numpy	Свободная лицензия

№ п/п	Наименование стороннего компонента	Правообладатель	Сведения о документах, подтверждающих наличие оснований на использование компонента	Лицензии	Вид лицензии
5	transformers	The Hugging Face team	https://github.com/huggingface/transformers/blob/main/LICENSE	Apache License 2.0	Свободная лицензия
6	fastapi	Sebastián Ramírez	https://github.com/fastapi/fastapi/blob/master/LICENSE	MIT	Свободная лицензия
7	uvicorn	Encode OSS Ltd.	https://github.com/encode/uvicorn?tab=BSD-3-Clause-1-ov-file	BSD 3-Clause	Свободная лицензия
8	joblib	The joblib developers	https://github.com/joblib/joblib/blob/main/LICENSE.txt	BSD 3-Clause	Свободная лицензия

10. Проверка Программы

10.1 Проверка доступности агента

Проверка доступности агента осуществляется на странице **Агенты** раздела **Список агентов**. Для активных в данный момент агентов в поле **Группа/Имя агента** применяется обозначение с помощью значка ●, при наведении на который появляется запись **Активен**.

10.2 Контроль целостности исполняемых файлов и файлов конфигурации

Каждый компонент Программы содержит ЭЦП. Проверка ЭЦП компонентов агента осуществляется серверной частью автоматически.

11. Сообщения администратору

11.1 Общие сведения

Диалоговые окна, используемые для оповещения, различаются в зависимости от категории информации, которая в них содержится.

Предусмотрены следующие категории информации:

1) Ошибка;
2) Обнаружение;
3) Предупреждение;
4) Успешно.

Сообщения администратору выводятся в виде диалоговых окон.

11.2 Сообщения об ошибках

Можно выделить два типа сообщений об ошибках:

1) Общие сообщения – общий обработчик срабатывает, когда ошибка не обработана специально;
2) Специфичные сообщения – выводятся в конкретных местах приложения и содержат детальное описание ошибки.

11.2.1. Общие сообщения

Общие сообщения – универсальные сообщения, которые выводятся в тех ситуациях, когда общий обработчик срабатывает, когда ошибка не обработана специально. Эти сообщения используются почти всегда.

Из-за технологий, используемых в приложении фронтенда, общие сообщения бывают двух типов:

1) Экран ошибки;
2) Всплывающее сообщение об ошибке.

Пример сообщения в виде экрана ошибки представлен на рисунке 111.

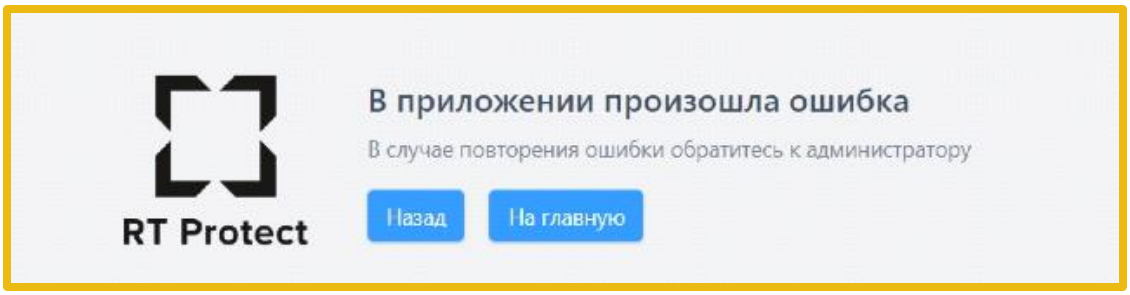


Рисунок 111 – Сообщение об ошибке типа «Экран ошибки»

Такие сообщения выводятся в том случае, если ошибка возникла внутри приложения, в логике работы одного из его компонентов.

Пример сообщения типа «Всплывающее сообщение об ошибке» показан на рисунке 112.

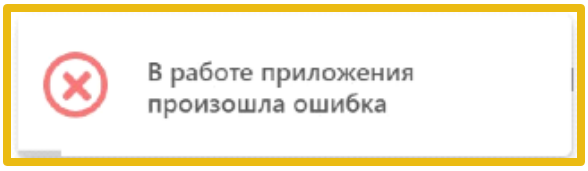


Рисунок 112 – Всплывающее сообщение об ошибке

Такие сообщения выводятся в том случае, если ошибка возникла в результате взаимодействия компонентов приложения с внешними ресурсами (например, сервером). Таких ошибок большинство.

Причины общих сообщений: отсутствие связи с сервером, CORS, и любые другие.

Действия по устранению: обновить страницу, проверить связь с сервером, сообщить администратору.

11.2.2. Специфичные сообщения

Ниже приведен список специфичных сообщений, разделенных по соответствующим страницам модуля администрирования.

Страница «Пользователи»

1) Ошибка при удалении пользователя (выводимое сообщение «Ошибка при удалении пользователя» представлено на рисунке 113).

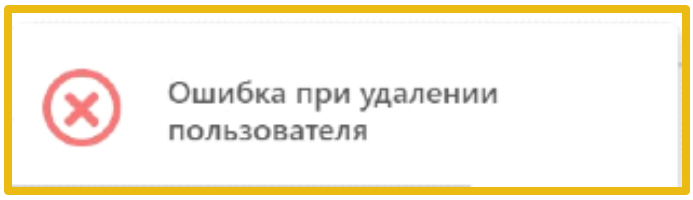


Рисунок 113 – Ошибка при удалении пользователя

Возможная причина: некорректный ответ сервера.

Возможные действия по устранению: убедиться в наличии связи с сервером, перезагрузить страницу, повторить действие.

2) Ошибка при блокировании пользователя (выводимое сообщение «Ошибка при блокировании пользователя» представлено на рисунке 114).

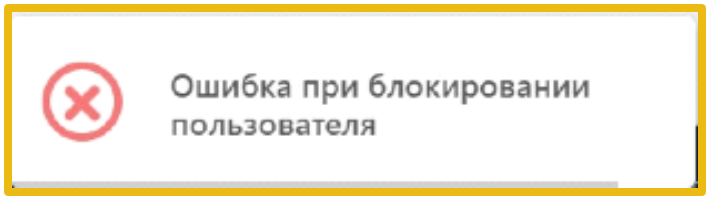


Рисунок 114 – Ошибка при блокировании пользователя

Возможная причина: некорректный ответ сервера

Возможные действия по устранению: убедиться в наличии связи с сервером, перезагрузить страницу, повторить действие.

3) Ошибка при разблокировании пользователя (выводимое сообщение «Ошибка при разблокировании пользователя» представлено на рисунке 115).

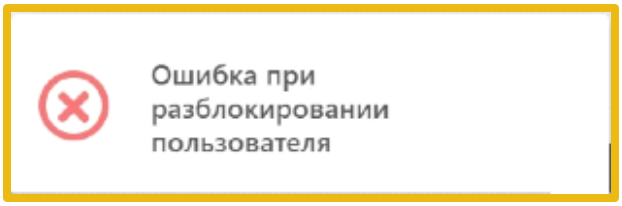


Рисунок 115 – Ошибка при разблокировании пользователя

Возможная причина: некорректный ответ сервера

Возможные действия по устранению: убедиться в наличии связи с сервером, перезагрузить страницу, повторить действие

4) Ошибка сброса пароля (выводимое сообщение «Ошибка сброса пароля» представлено на рисунке 116).

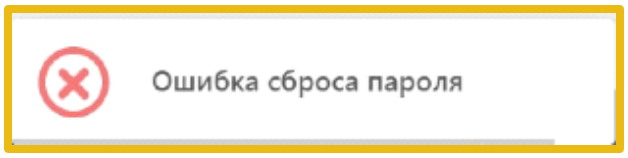


Рисунок 116 – Ошибка сброса пароля

Возможная причина: некорректный ответ сервера.

Возможные действия по устранению: убедиться в наличии связи с сервером, перезагрузить страницу, повторить действие.

Страница «Графики».

Выводимое сообщение «Ошибка при загрузке данных» представлено на рисунке 117.

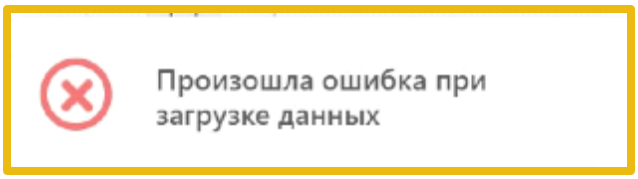


Рисунок 117 – Ошибка при загрузке данных

Возможная причина: некорректный ответ сервера.

Возможные действия по устранению: убедиться в наличии связи с сервером, перезагрузить страницу, повторить действие.

Страница «Настройка Агента».

1) Превышена максимальная длина комментария.

Выводимое сообщение «Превышена максимальная длина комментария» представлено на рисунке 118.

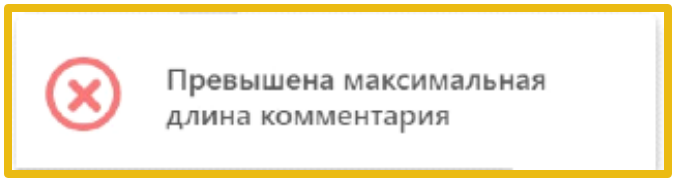


Рисунок 118 – Превышена максимальная длина комментария

Возможная причина: превышена длина комментария, некорректный ответ сервера.

Возможные действия по устранению: комментарий не должен быть длиннее 255 символов, убедиться в наличии связи с сервером, перезагрузить страницу, повторить действие.

2) Ошибка при отправке команды на переход к изоляции.

Выводимое сообщение «Ошибка при отправке команды на переход к изоляции» представлено на рисунке 119.

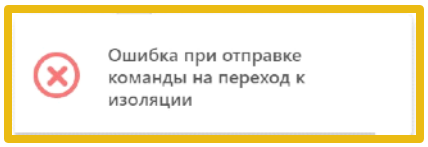


Рисунок 119 – Ошибка при отправке команды на переход к изоляции

Возможная причина: некорректный ответ сервера.

Возможные действия по устранению: убедиться в наличии связи с сервером, перезагрузить страницу, повторить действие.

3) Ошибка при отправке команды на отмену изоляции.

Выводимое сообщение «Ошибка при отправке команды на отмену изоляции» представлено на рисунке 120.

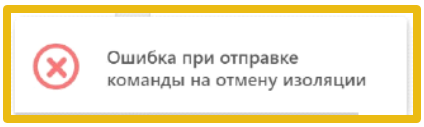


Рисунок 120 – Ошибка при отправке команды на отмену изоляции

Возможная причина: некорректный ответ сервера.

Возможные действия по устранению: убедиться в наличии связи с сервером, перезагрузить страницу, повторить действие.

Страница «Агенты»

Выводимое сообщение «Ошибка при удалении агентов» представлено на рисунке 121.

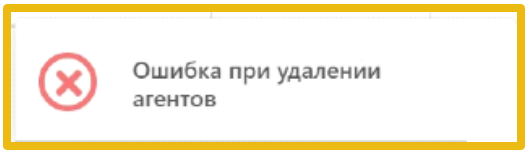


Рисунок 121 – Ошибка при удалении агентов

Возможная причина: некорректный ответ сервера.

Возможные действия по устранению: убедиться в наличии связи с сервером, перезагрузить страницу, повторить действие.

Страница «Настройка группы».

1) Ошибка при создании группы.

Выводимое сообщение «Ошибка при создании группы» представлено на рисунке 122.

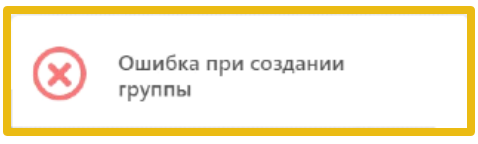


Рисунок 122 – Ошибка при создании группы

Возможная причина: некорректный ответ сервера.

Возможные действия по устранению: убедиться в наличии связи с сервером, перезагрузить страницу, повторить действие.

2) Ошибка при сохранении данных группы.

Выводимое сообщение «Ошибка при сохранении данных группы» представлено на рисунке 123.

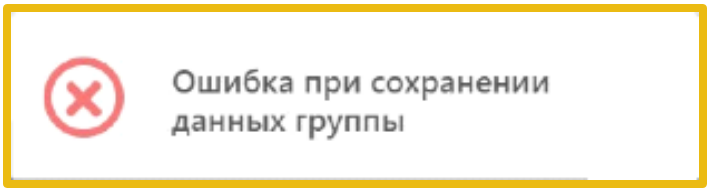


Рисунок 123 – Ошибка при сохранении данных группы

Возможная причина: некорректный ответ сервера.

Возможные действия по устранению: убедиться в наличии связи с сервером, перезагрузить страницу, повторить действие.

3) Ошибка при удалении группы.

Выводимое сообщение «Ошибка при удалении группы» представлено на рисунке 124.

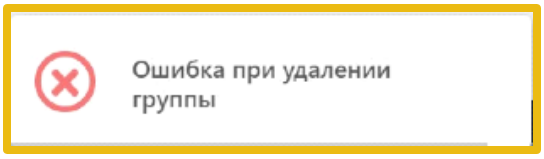


Рисунок 124 – Ошибка при удалении группы

Возможная причина: некорректный ответ сервера.

Возможные действия по устранению: убедиться в наличии связи с сервером, перезагрузить страницу, повторить действие.

4) Ошибка при исключении агентов из группы.

Выводимое сообщение «Ошибка при исключении агентов из группы» представлено на рисунке 125.

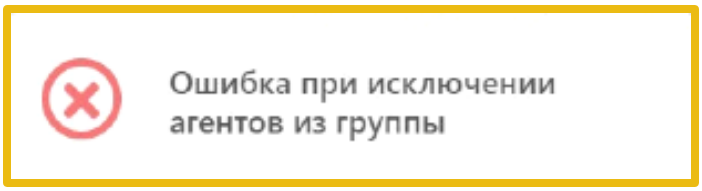


Рисунок 125 – Ошибка при исключении агентов из группы

Возможная причина: некорректный ответ сервера.

Возможные действия по устранению: убедиться в наличии связи с сервером, перезагрузить страницу, повторить действие.

Страница «Список агентов».

1) Группа с таким именем уже есть.

Выводимое сообщение «Группа с таким именем уже есть» представлено на рисунке 126.

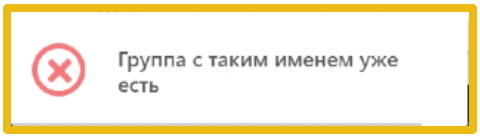


Рисунок 126 – Группа с таким именем уже есть

Возможная причина: группа с таким именем уже есть, некорректный ответ сервера.

Возможные действия по устранению: использовать уникальное имя группы, убедиться в наличии связи с сервером, перезагрузить страницу, повторить действие.

2) Ошибка при добавлении группы.

Выводимое сообщение «Ошибка при добавлении группы» представлено на рисунке 127.

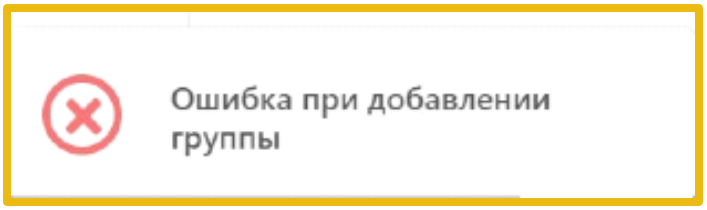


Рисунок 127 – Ошибка при добавлении группы

Возможная причина: некорректный ответ сервера.

Возможные действия по устранению: убедиться в наличии связи с сервером, перезагрузить страницу, повторить действие.

Страница «Хранилище».

1) Ошибка при удалении файла.

Выводимое сообщение «Ошибка при удалении файла» представлено на рисунке 128.

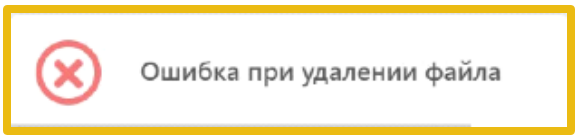


Рисунок 128 – Ошибка при удалении файла

Возможная причина: некорректный ответ сервера.

Возможные действия по устранению: убедиться в наличии связи с сервером, перезагрузить страницу, повторить действие.

Страница «Инцидента».

1) Ошибка при закрытии инцидента.

Выводимое сообщение «Ошибка при закрытии инцидента» представлено на рисунке 129.

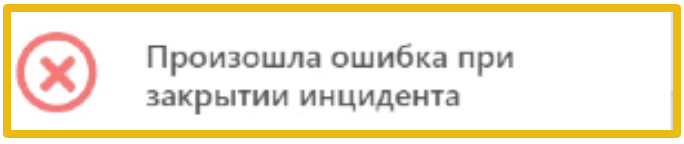


Рисунок 129 – Ошибка при закрытии инцидента

Возможная причина: некорректный ответ сервера.

Возможные действия по устранению: убедиться в наличии связи с сервером, перезагрузить страницу, повторить действие.

Страницы разделов «Аналитика» и «Профили безопасности».

1) Ошибка неверный формат файла.

Выводимое сообщение «Неверный формат данных» представлено на рисунке 130.

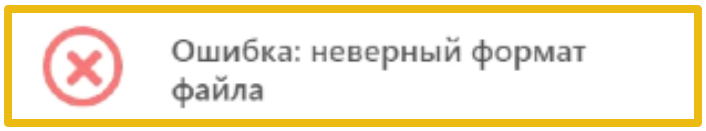


Рисунок 130 – Неверный формат файла

Возможная причина: неверный формат импортируемого файла, некорректный ответ сервера.

Возможные действия по устранению: убедиться, что файл имеет корректный формат, убедиться в наличии связи с сервером, перезагрузить страницу, повторить действие.

Страницы «Индикаторы атак» и «YARA-правила».

1) Ошибка в правиле.

Выводимое сообщение «Ошибка в правиле YARA» представлено на рисунке 131.

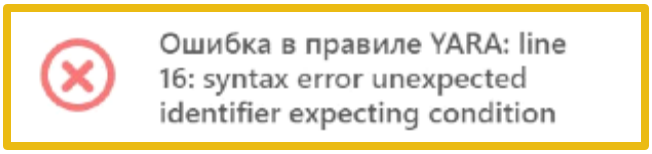


Рисунок 131 – Ошибка в правиле YARA

Возможная причина: неверное написание YARA-правила, некорректный ответ сервера.

Возможные действия по устранению: убедиться в правильности написания YARA-правила, убедиться в наличии связи с сервером, перезагрузить страницу, повторить действие.

Страница «Лицензия»

1) Кодировка файла лицензии не UTF-8.

Выводимое сообщение «Ошибка кодировки файла лицензии» представлено на рисунке 132.

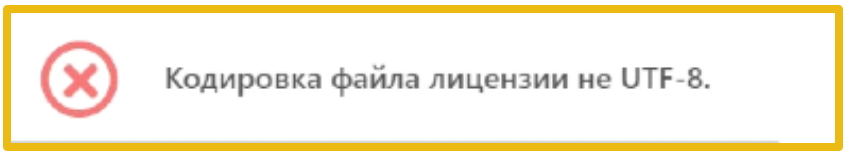


Рисунок 132 – Кодировка файла лицензии

Возможная причина: неверный формат файла лицензии, некорректный ответ сервера.

Возможные действия по устранению: убедиться в соответствии формата файла лицензии, убедиться в наличии связи с сервером, перезагрузить страницу, повторить действие.

2) Ошибка в файле лицензии.

Выводимое сообщение «Ошибка в файле лицензии» представлено на рисунке 133.

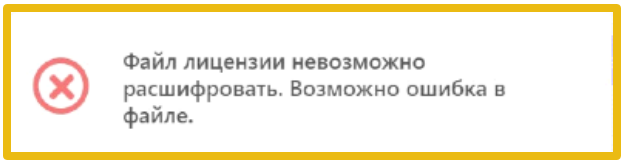


Рисунок 133 – Ошибка в файле лицензии

Возможная причина: файл был отредактирован или поврежден, некорректный ответ сервера.

Возможные действия по устранению: убедиться в целостности файла, убедиться в наличии связи с сервером, перезагрузить страницу, повторить действие.

Страница «Дистрибутивы»

1) Недопустимый формат или расширение.

Выводимое сообщение ошибки «Недопустимый формат или расширение» представлено на рисунке 134.

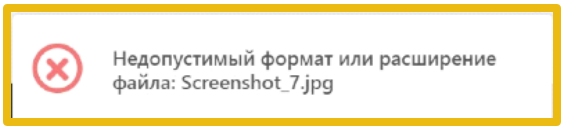


Рисунок 134 – Недопустимый формат или расширение

Возможная причина: неверный формат файла, некорректный ответ сервера.

Возможные действия по устранению: убедиться в корректности формата файла лицензии, убедиться в наличии связи с сервером, перезагрузить страницу, повторить действие.

2) Ошибка загрузки дистрибутива.

Выводимое сообщение ошибки «Дистрибутив уже существует» представлено на рисунке 135.

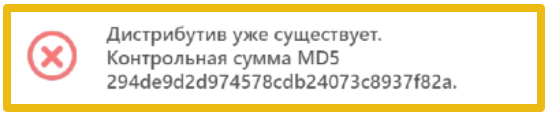


Рисунок 135 – Дистрибутив уже существует

Возможная причина: дистрибутив уже загружен, некорректный ответ сервера.

Возможные действия по устранению: убедиться в том, что данный дистрибутив не загружен, убедиться в наличии связи с сервером, перезагрузить страницу, повторить действие.

3) Проверка связи с сервером.

Приложение проверяет связь с сервером автоматически при загрузке.

Результат проверки отображается (или не отображается) в заголовке страницы по центру.

Если соединение есть, то сообщение не отображается. Если соединения нет, то отображается оповещение об этом (рис. 136).

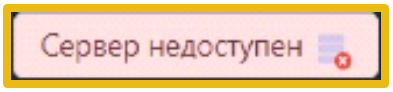


Рисунок 136 – Ошибка соединения с сервером

12. Процедура обновления программного обеспечения

12.1 Общие сведения

Определены три типа обновлений Программы:

1) Первый тип – обновление баз данных, необходимых для реализации функций безопасности (обновление БД ПКВ);
2) Второй тип – обновление, направленное на устранение уязвимостей (критическое обновление);
3) Третий тип – обновление, направленное на добавление и/или совершенствование реализации функций безопасности, а также расширение числа поддерживаемых программных и аппаратных платформ (обновление версии Программы).

Этапы жизненного цикла обновлений Программы от выпуска до применения представлены в таблице 56.

Заказчик может получить обновление третьего типа следующими способами:

1) Приобрести новый комплект поставки Программы («медиа-пак»), содержащий обновление и эксплуатационную документацию в печатном виде, согласно комплекту поставки, обратившись к дистрибьюторам АО «РТ-ИБ».
2) Загрузить обновление и комплект измененной эксплуатационной документации (включая эксплуатационный бюллетень) в электронном виде с сервера предприятия-изготовителя.

При получении обновления третьего типа и комплекта измененной эксплуатационной документации в электронном виде Заказчик должен осуществить следующие действия: после загрузки файлов обновления и комплекта измененной эксплуатационной документации произвести проверку целостности загруженных файлов путем сверки контрольных сумм с указанными в документации, хранящейся на сервере предприятия-изготовителя.

Таблица 56 – Жизненный цикл обновлений Программы

	1 тип	2 тип	3 тип
Выпуск	Регулярно в соответствии с установленной изготовителем процедурой, вплоть до окончания срока поддержки Программы	По необходимости (при выявлении уязвимостей)	По усмотрению изготовителя
Публикация	Непосредственно после выпуска	Непосредственно после выпуска	По прохождении инспекционного контроля
Инспекционный контроль	1 раз в год (полный пакет обновлений)	После выпуска в срок, предусмотренный изготовителем	После выпуска в срок, предусмотренный изготовителем
Уведомление	Реализовано в Программе	По электронной почте зарегистрированным пользователям, на сайте изготовителя – в срок не позднее 5 суток после публикации	По электронной почте зарегистрированным пользователям, на сайте изготовителя – в срок не позднее 5 суток после получения сертификата
Получение и применение	В соответствии с эксплуатационной документацией	Заказчик должен загрузить и применить обновление незамедлительно после получения уведомления	По усмотрению потребителя

Уведомления о выпуске обновлений 2 и 3 типов рассылаются по адресам электронной почты, указанным при заказе Программы, а также подписчикам рассылки (подписаться на рассылку можно по ссылке):

– info@rt-ib.ru – техническая поддержка;

– https://rt-ib.ru – адрес сайта.

Предусмотрен следующий способ предоставления обновлений потребителям:

1) Размещение новой версии Программы на сервере предприятия-изготовителя;
2) Автоматическое обновление БД ПКВ с сервера предприятия-изготовителя;
3) Обновление БД ПКВ с использованием локального сервера обновлений.

Предусмотрены следующие способы уведомления потребителей о выпуске обновлений:

1) Публикация о наличии обновлений Программы, устраняющих найденные уязвимости на официальном сайте предприятия-изготовителя https://rt-ib.ru;
2) Уведомление потребителя о выходе обновлений электронным письмом.

3) Получение потребителем информации о выходе обновлений через службу технической поддержки предприятия-изготовителя или по электронной почте (info@rt-ib.ru).

Для установочных файлов новой версии Программы, а также для пакетов обновлений, в разделах официальных сайтов и репозиториев публикуются КС, рассчитанные с использованием поддерживаемых операционными системами Windows и Linux средств проверки контроля целостности.

Перед установкой новой версии Программы или пакетов обновлений необходимо осуществить вычисление КС загруженных файлов и проверить их соответствие эталонным.

12.2 Обновление агента

Обновление дистрибутива агента выполняется администратором автоматически или вручную. По умолчанию верифицированные агенты обновляются автоматически, для этого в разделе **Настройка агента** установлен флаг **Автоматическое обновление**.

На стороне рабочей станции обновление агента выполняется «бесшовно» (без необходимости перезагрузки и в фоновом для рабочей станции режиме). Также обновляются решающие правила.

В случае ручного обновления дистрибутива агента следует снять флаг и загрузить необходимый дистрибутив на странице раздела **Дистрибутивы** (см. пункт 8.9.3), после чего перенести дистрибутив на защищаемый узел и установить агента, следуя инструкции установщика.

12.3 Оповещение покупателя об обновлении

Разработчик ведет учет покупателей Программы. Выполняется регистрация следующей информации:

1) Наименование организации;
2) Адрес организации;
3) Номер знака соответствия,
4) Контактная информация (содержит электронный почтовый адрес лица, обеспечивающего администрирование Программы).

Уведомление пользователей о выпуске обновления Программы выполняется с использованием рассылки электронных почтовых сообщений с адреса электронной почты info@rt-ib.ru. Предприятие-изготовитель направляет документ «release notes» в адрес организаций, оплативших техническую поддержку.

Документ содержит описание обновления, процедур получения и контроля целостности обновления, процедур тестирования, установки, применения и верификации.

12.4 Доставка и контроль целостности обновления программного обеспечения на стороне покупателя

Обновления программного обеспечения, успешно прошедшие контроль влияния на безопасность Программы, публикуются в закрытой части сервера предприятия-производителя. Доступ пользователей к закрытой части сервера осуществляется с использованием учетной записи и пароля, указанного в электронном почтовом сообщении, уведомляющем о наличии обновления. При публикации обновления программного обеспечения публикуется его контрольная сумма. После получения обновления пользователь имеет возможность проверить его целостность с использованием механизма контрольного суммирования.

13. Действия после сбоя и ошибки

13.1 Общие сведения

Большинство ошибок можно разделить на следующие типы:

1) Ошибки конфигурации:

– некорректные настройки параметров безопасности;

– некорректная установка компонентов Программы;

– некорректные действия со стороны пользователя/администратора;

– критические ошибки.

2) Ошибки оборудования:

– выход из строя аппаратных средств, на которых установлена Программа;

– выход из строя сервера (или компонентов на сервере) с которыми взаимодействуют компоненты Программы, установленные на оборудовании пользователя;

– перебои питания со стороны клиентской или серверной части.

Для устранения ошибки требуется переконфигурировать Программу либо восстановить её из ранее сделанной резервной копии, либо восстановить Программу с установочного носителя согласно рекомендациям настоящего руководства.

13.2 Инструкция по удалению агента в случае блокировки ОС

В некоторых случаях на агенте могут возникнуть ситуации, когда работа операционной системы не может быть продолжена в штатном режиме. В таком случае может потребоваться удаление агента. Чтобы удалить агента с компьютера в случае невозможности штатного удаления необходимо выполнить следующие шаги:

1) Перезагрузить компьютер и выполнить вход в безопасном режиме (для Windows 10 удерживать клавишу Shift при перезагрузке, для Windows 7 удерживать клавишу F8 при загрузке ОС);
2) Удалить ключ реестра HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Vrpnt с помощью утилиты regedit.exe;
3) Перезагрузить систему и удалить агента с помощью приложения «Установка и удаление программ».

13.3 Установка и применение обновления программного обеспечения

Обновление программного обеспечения происходит аналогично установке программного обеспечения. В клиентской части по умолчанию обновление происходит автоматически. Подробнее процедуры установки и применения программного обеспечения описаны в разделе 5.

13.4 Контроль установки обновления

Критерием правильности установки обновления программного обеспечения является доступность интерфейса Программы и отображение информации о новой версии Программы (см. подраздел 8.1).

14. Перечень сокращений

Основные сокращения, указанные в документе, представлены в таблице 57.

Таблица 57 – Перечень сокращений

Сокращение	Расшифровка
АРМ	Автоматизированное рабочее место
ЗБ	Задание по безопасности
ИС	Информационная система
ИТ	Информационная технология
КС	Контрольная сумма
ЛКМ	Левая кнопка мыши
ОО	Объект оценки
ОС	Операционная система
ОУД	Оценочный уровень доверия
ПЗ	Профиль защиты
ПКВ	Признаки компьютерных вирусов
ПКМ	Правая кнопка мыши
ПО	Программное обеспечение
САВЗ	Система антивирусной защиты
СОВ	Система обнаружения вторжений
УЗ	Учетная запись
УК	Управление конфигурацией
ФСТЭК	Федеральная служба по техническому и экспортному контролю
ЦП	Центральный процессор
ЭД	Эксплуатационная документация
ЭЦП	Электронная цифровая подпись
API	Application Programming Interface
APT	Advanced Persistent Threat (постоянная серьезная угроза)
BTF	BPF Type Format
CORS	Cross-Origin Resource Sharing (совместное использование ресурсов между разными источниками)
DSL	Domain-Specific Language
eBPF	Extended Berkeley Packet Filter
EDR	Endpoint Detection and Response
EPS	Events Per Second
ID	Identifier (идентификатор)
IT	Information Technology (информационные технологии)
IOA	Indicators of Attack

IOC	Indicator of Compromise
NSRL	National Software Reference Library (Национальная справочная библиотека программного обеспечения)
NTFS	New Technology File System (технологически новая файловая система)
PID	Process Identifier (идентификатор процесса)
PPID	Parent Process Identifier (идентификатор родительского процесса)
RPC	Remote Procedure Call (удалённый вызов процедур)
SID	Security Identifier (идентификатор безопасности)
SOAR	Security Orchestration, Automation and Response
TI	Threat Intelligence
VPN	Virtual Private Network

Цитирование документа допускается только со ссылкой на настоящее руководство. Руководство не может быть полностью или частично воспроизведено, тиражировано или распространено без разрешения АО «РТ-ИБ».