RT Protect EDR

Руководство по установке и эксплуатации для администратора

Версия 1.0.23 от 14 октября 2024
Разработано компанией АО «РТ-Информационная безопасность»

RT Protect

Оглавление

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 по установке и эксплуатации для Администратора
Версия документа	Версия 1.0.23 (актуально для версии агента 2.0.162.2673, версии фронтенда 2.40.6, версии бекенда 1.21.1-17)
Идентификация программы	«RT Protect EDR»
Идентификация разработчика	АО «РТ-Информационная безопасность»
Уровень доверия	Оценочный уровень доверия 4 (ОУД4)
Идентификация ПЗ	Профиль защиты систем обнаружения вторжений уровня узла типа «У» четвертого класса защиты. ИТ.СОВ.У4.ПЗ. Утвержден ФСТЭК России от 3.02.2012г. Профиль защиты средств контроля подключения съемных машинных носителей информации четвертого класса защиты ИТ.СКН.П4.ПЗ (утвержден ФСТЭК России от 01.12.2014)
Идентификация ОК	«Требования к системам обнаружения вторжений, утвержденные приказом ФСТЭК России от 6 декабря 2011 г. № 638. ГОСТ Р ИСО/МЭК 15408 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий»
Ключевые слова	Система обнаружения вторжений, СОВ, ОУД4

1.2 Аннотация документа

Документ предназначен для ознакомления администраторов сервера управления 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

Термин	Описание
Нити (Threads)	Наименьшая единица обработки, исполнение которой может быть назначено ядром операционной системы. Нити исполняются внутри процесса
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
Разработчик	АО «РТ-Информационная безопасность»
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

Термин	Описание
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 злоумышленника, обладающего современным уровнем специальных знаний и значительными ресурсами, которые позволяют ему создавать угрозу опасных кибератак
AS-REP Roasting	Атака на Kerberos, применяемая для учетных записей пользователей, не требующих предварительной аутентификации
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
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

Термин	Описание
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
Kerberoasting	Тип атаки на Kerberos, при котором аутентифицированный в домене пользователь может запросить билет для доступа к сервису TGS (Ticket Granting Service). TGS зашифрован хешем пароля учетной записи, от которой запущен целевой сервис. Злоумышленник, получив таким образом TGS-билет, теперь может расшифровать его, подбирая пароль и не боясь блокировки, поскольку делает это оффлайн. При успешном исходе злоумышленник получает пароль от ассоциированной с сервисом учетной записи, которая зачастую является привилегированной

Термин	Описание
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
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
TGS	Служба выдачи разрешений на доступ к определенному сетевому ресурсу по протоколу Kerberos
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

Термин	Описание
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 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 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.

Клиентская часть Программы не содержит в своем составе заимствованных компонентов без исходного кода. Все компоненты собираются из исходного кода.

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

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

Оператор поиска угроз – выполняет проактивный поиск угроз в защищаемой Программой инфраструктуре;

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

2.2 Функциональные возможности в части СОВ

Программа обеспечивает следующие функциональные возможности в части СОВ:

– 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	Система обнаружения вторжений «RT Protect EDR» Модуль агента	1	Поставляется по сети (пакет-установщик)
	Система обнаружения вторжений «RT Protect EDR» Модуль администрирования с консолью на сервере*	1	Доступ к модулю как услуга
-01 30 01	Система обнаружения вторжений «RT Protect EDR» Формуляр	1	Поставляется в печатном виде (формат А4)
-20 01	Система обнаружения вторжений «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 и выше;

– Linux Ubuntu 18.04;

– Linux Ubuntu 20.04;

– Linux Ubuntu 22.04;

– Linux Ubuntu 24.04;

– Debian 11;

– Debian 12;

– Astra Linux SE 1.6;

– Astra Linux SE 1.7;

– Astra Linux 1.8;

– Red OS 7.3;

– ALT Linux 10.

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, защищенному с помощью SSL с применением шифрования ГОСТ.

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.

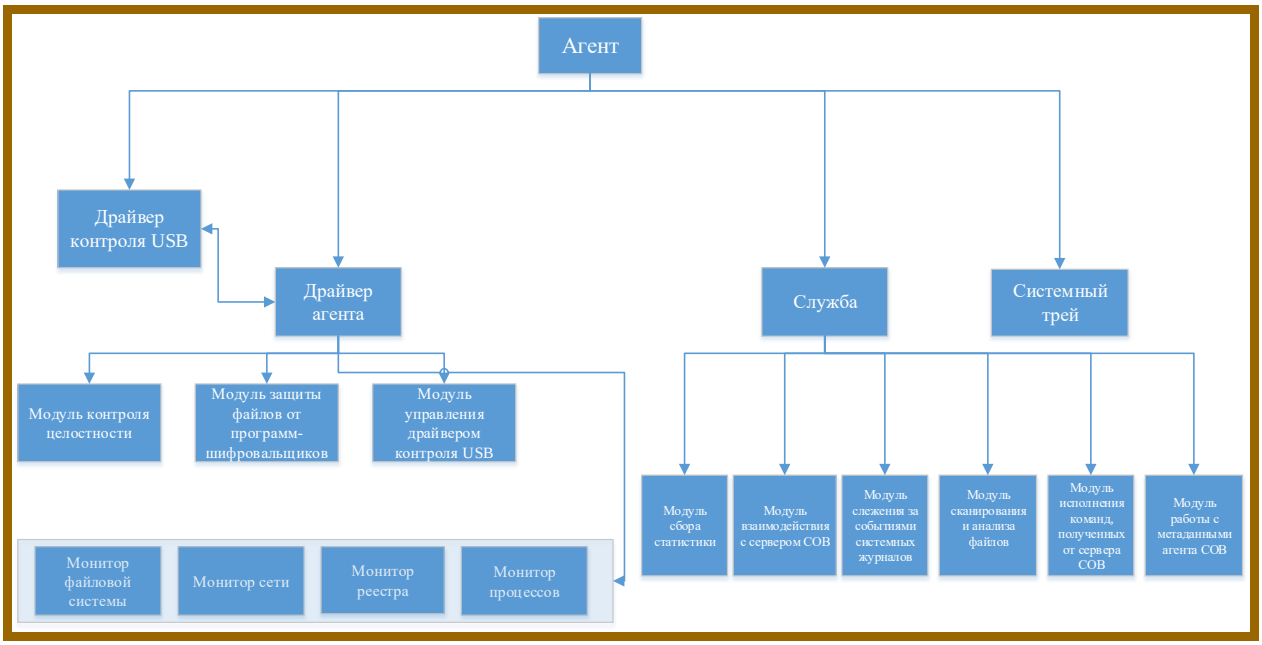


Рисунок 1 – Архитектура агента Windows

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 трех компонентов:

1) Исполняемый модуль – сервис system, запускаемый от имени суперпользователя при загрузке ОС, название сервиса и исполняемого файла avd;

2) BPF-модули – набор BPF-программ, загружаемый в ядро ОС по инициативе сервиса;

3) Модуль ядра, загружается в ядро ОС по инициативе сервиса.

Схематично архитектура агента Linux представлена на рисунке 2.

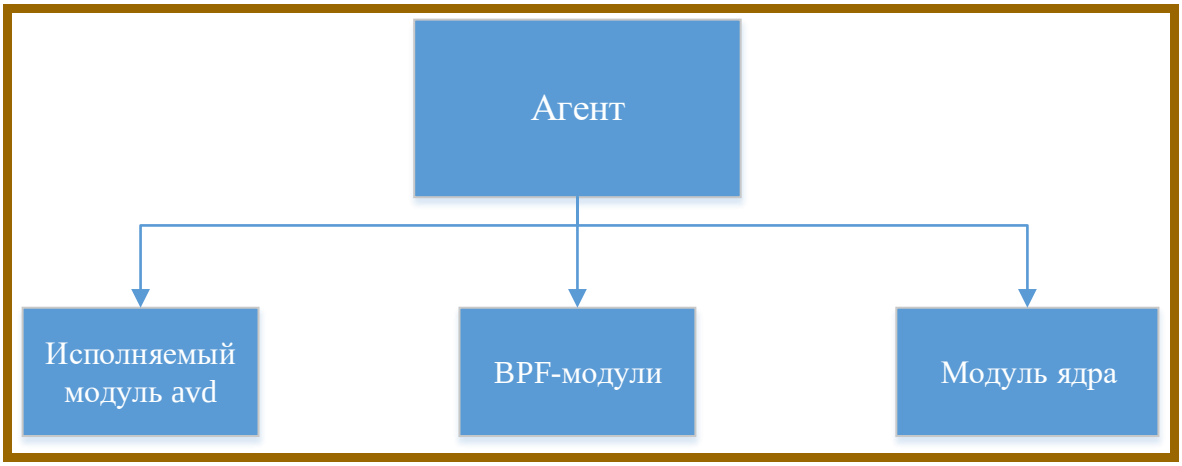


Рисунок 2 – Архитектура агента Linux

4.4 Архитектура серверной части

4.4.1. Общие сведения

Серверная часть системы включает в себя сервер сбора статистики, web-сервер управления (backend), СУБД, БД, административный модуль (frontend).

Серверная часть функционирует под управлением ОС семейства Linux.

Архитектура серверной части системы схематично представлена на рисунке 3.

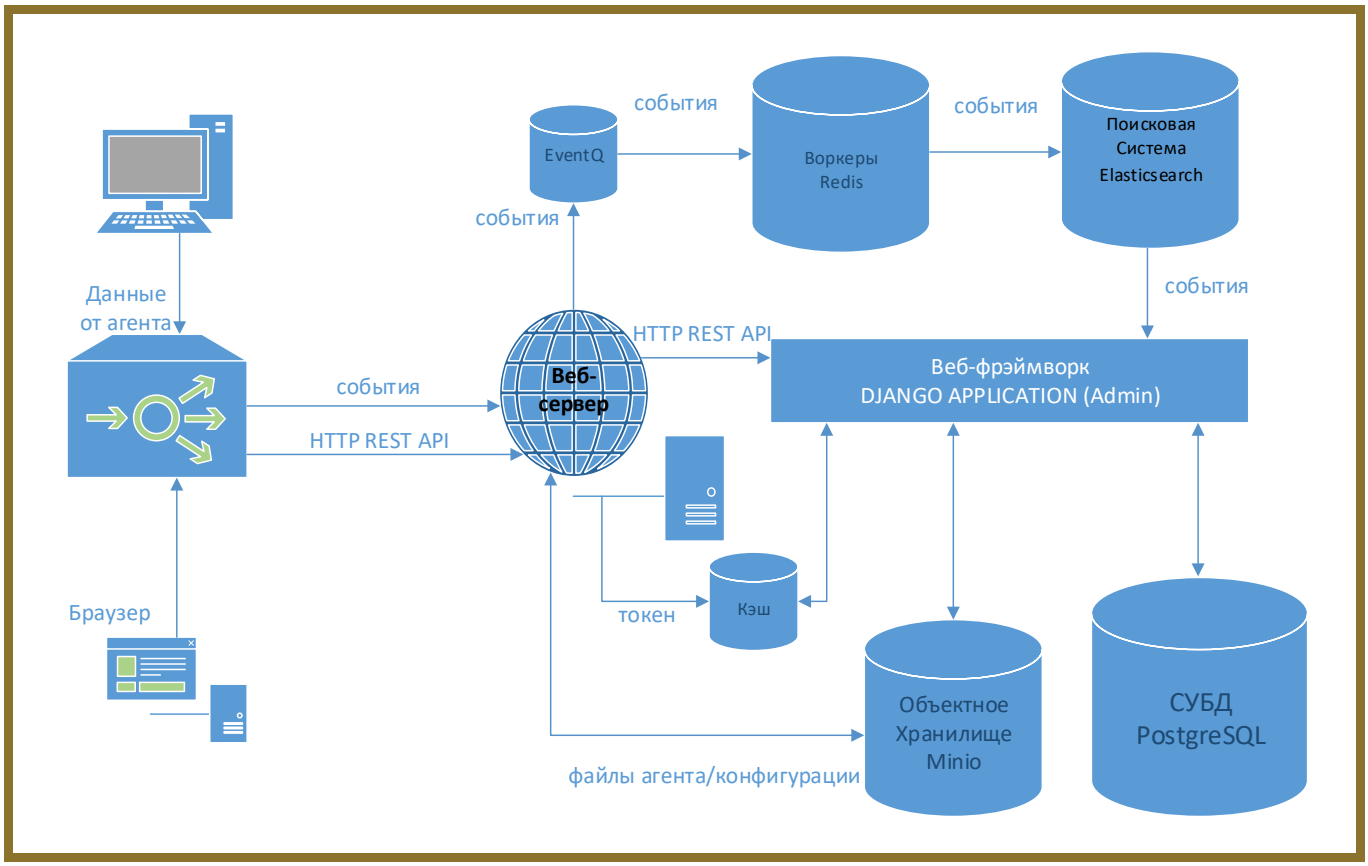


Рисунок 3 – Архитектура серверной части «RT Protect EDR»

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.

Важно

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, а также на различных версиях ОС Linux (Ubuntu 18.04, Ubuntu 20.04.5 LTS с ядром linux-5.15.0, Ubuntu 22.04, Ubuntu 24.04, Astra SE 1.6, Astra SE 1.7 _x86-64, ALT Linux 10, Red OS 7.3, Debian GNU/Linux 11 (bullseye) [Linux 5.10.0-19-amd64 x86_64], Debian GNU/Linux 12).

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.

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

Программа пригодна для функционирования на аппаратных платформах, указанных в таблице 6.

Таблица 6 – Программно-аппаратное обеспечение и среда функционирования

Характеристики	Платформа 1 (клиентская часть)		Платформа 2 (серверная часть)	
Операционная система	Windows/Linux		Linux	
	Минимальные требования	Рекомендуемые требования	Минимальные требования	Рекомендуемые требования
Процессор	Процессор частотой 2 ГГц и выше с поддержкой инструкций SSE2	Intel CoreTM I3 Duo 3.1 GHz или эквивалентный (с поддержкой SSE2)	Не менее 10 ядер частотой минимум 2,4 ГГц с возможностью работы в 20 потоков	Три сервера с конфигурацией процессора не менее 10 ядер частотой минимум 2,4 ГГц с возможностью работы в 20 потоков
Оперативная память	1 ГБ	2 ГБ	32ГБ	64 ГБ на каждом сервере
Жесткий диск (свободное пространство)	100 МБ	2ГБ	8 ТБ	Три жестких диска на каждый сервер по 8 ТБ каждый

Серверная часть Программы поддерживает работу в браузерах, представленных в таблице 7.

Таблица 7 – 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 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 (USB-носитель, CD/DVD).

Примечание

Агент EDR после установки регистрирует ETW-провайдер RT Protect EDR или VR 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) и адрес сервера. ID клиента можно увидеть на сервере управления в разделе **Лицензия/Информация о лицензии.**

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).

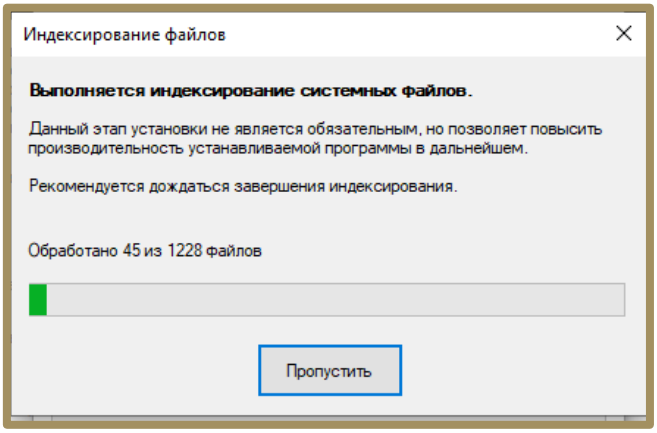


Рисунок 5 – Подтверждение установки

Примечание

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

---

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

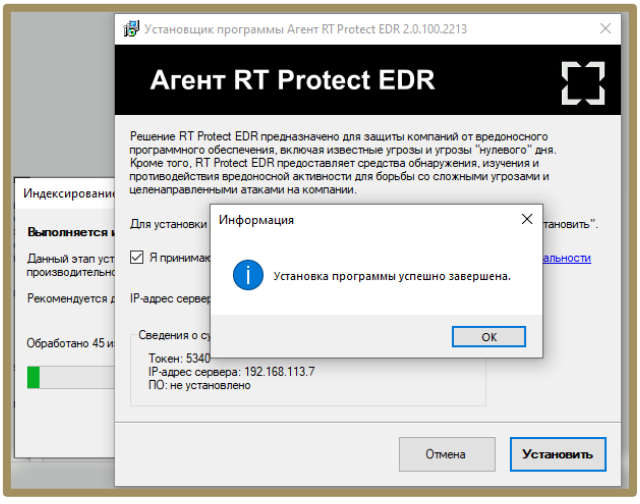


Рисунок 6 – Процесс установки

7) Нажать кнопку **ОК.**

8) После завершения всех процедур установки в правом углу экрана в системном трее появится иконка установленного агента (рис. 7).

Примечание

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

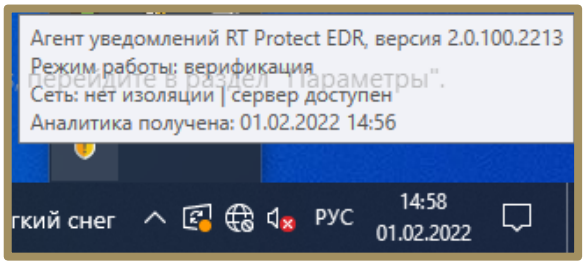


Рисунок 7 – Иконка установленного агента EDR

9) После первоначальной установки агента его необходимо верифицировать. Операция доступна только пользователям системы с ролью «Администратор». После верификации агента в трее появится сообщение, представленное на рисунке 8.

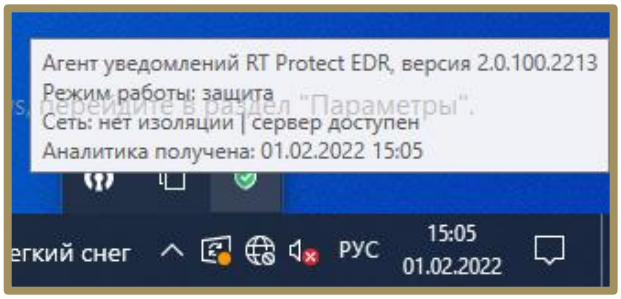


Рисунок 8 – Агент верифицирован

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
```

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 защиты»;

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

– /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;

2) Astra SE 1.7 (поддерживаемые ядра):

– 5.10.142-1-generic;

– 5.15.0-33-generic;

– 5.4.0-110-generic;

– 5.4.0-54-generic.

3) Debian 11:

– 5.10.0-19-amd64;

4) Debian 12;

5) Ubuntu 20.04:

– 5.15.0-67-generic;

– 5.15.0-69-generic;

– 5.15.0-70-generic;

– 5.15.0-71-generic;

– 5.15.0-72-generic;

– 5.4.0-137-generic;

– 5.4.0-139-generic;

– 5.4.0-148-generic.

6) Ubuntu 22.04:

– 5.19.0-41-generic

7) Ubuntu 24.04;

8) RedOs 7.3:

– 5.10.29-3.el7.x86_64

9) ALT Linux 10.

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;

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

– Red OS 7.3;

– ALT Linux 10.

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. Подробная инструкция находится по ссылке.

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)

Первая настройка

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=edr.vr-protect.ru
  ...
}
```

Вместо имени можно указать адрес сервера:

```
  server=192.168.1.1
```

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.

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
```

2. Остановить сервис, выполнив команду:

```
sudo systemctl stop avd
```

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

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

3. Запустить сервис, выполнив команду:

```
sudo systemctl start avd
```

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).

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**. Откроется окно, представленное на рисунке 9.

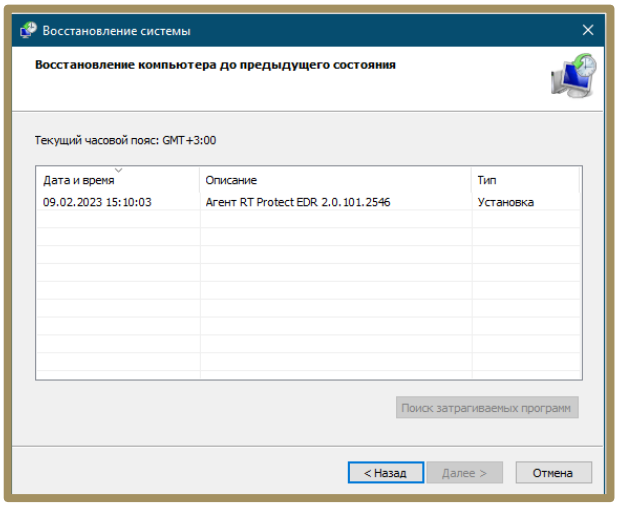


Рисунок 9 – Точка восстановления системы

5) Выбрать точку восстановления, созданную при установке агента EDR, выделив соответствующую строчку из списка. Появится окно, представленное на рисунке 10.

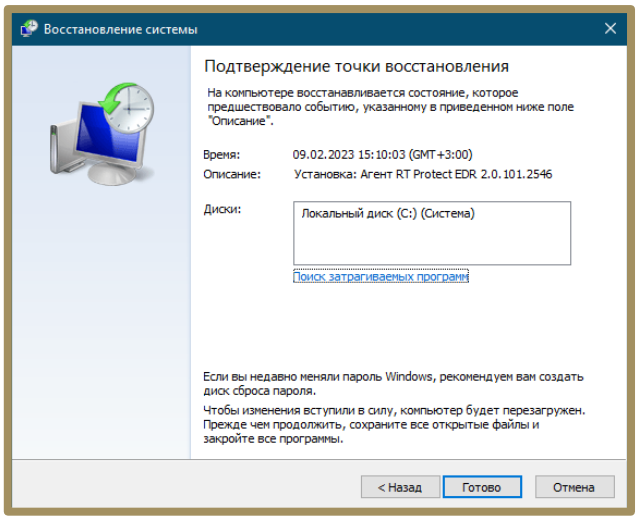


Рисунок 10 – Подтверждение точки восстановления

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/Agent_RT_Protect_EDR;

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 токен для удаления, созданный в Программе автоматически. Токен 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 (если включен режим защиты от удаления).

Выполняется это с помощью команды:

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

Где вместо password 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. Общие сведения и инструкция по установке серверной части RT Protect EDR на локальном сервере

Системные требования

Для установки серверной части Программы требуется соблюдение системных требований, указанных в пункте 5.1.

В качестве операционной системы должен выступить дистрибутив Linux Ubuntu версии 20.04 или Astra Linux SE 1.7.

Подготовка окружения

Для развертывания сервера EDR необходим АРМ с установленным на нем программным обеспечением:

– Python (не ниже версии 3.10.0) [установка]

– Ansible (не ниже версии 5.7.1) [установка]

Необходимо настроить доступ на сервер (***Docker-хост***) по SSH. Удаленному пользователю должны быть предоставлены права sudo (или root-пользователь). Для удобства использования Ansible необходимо добавить свой открытый SSH-ключ на сервере, в противном случае может потребоваться установка дополнительной утилиты **sshpass**.

Далее необходимо проверить, что с сервера есть доступ к реестру Docker-образов (http://docker.rt-protect.ru/) и есть доступ в Интернет (для установки deb-пакетов).

Создание конфигурации сервера

Чтобы создать конфигурацию сервера, необходимо клонировать репозиторий на АРМ, на котором разворачивается сервер EDR, перейдя по ссылке https://minio.rt-protect.ru/buckets/edr/browse либо по ссылке (https://gitlab.vr-protect.ru/edr-backend/edr-deploy). Далее необходимо перейти в корень репозитория **edr-deploy**. Структура каталогов представлена на рисунке 11.

Рисунок 11 – Структура каталогов репозитория edr-deploy

В каталоге **config** хранятся конфигурации серверов. Сюда необходимо добавить свою новую конфигурацию. Необходимо обратить внимание на то, что каталог **config** не отслеживается гитом (записан в ***.gitignore***) (кроме подкаталога **default**), поэтому можно без ограничений добавлять собственные конфигурации в любом количестве и не опасаться того, что чувствительные данные из них попадут в общий репозиторий.

Правильным подходом будет держать все конфигурации в одном месте – в каталоге **config** в соответствующих подкаталогах. Таким образом можно одновременно управлять несколькими конфигурациями серверов. Для удобства лучше именовать подкаталоги, например, по IP-адресу сервера или домену. Тогда структура каталога **config** со временем примет вид, как указано на рисунке 12.

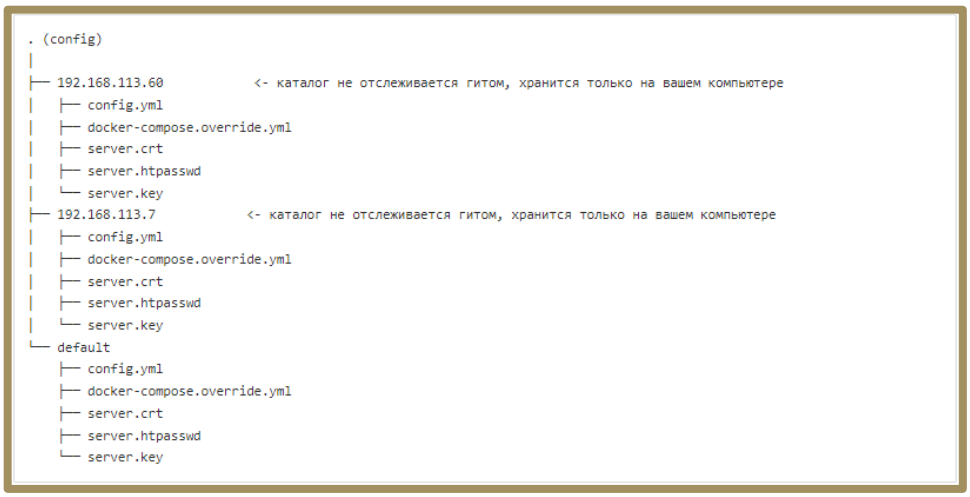


Рисунок 12 – Структура каталога config

На рисунке можно увидеть две дополнительные конфигурации (помимо конфигурации по умолчанию): для сервера 192.168.113.60 и для сервера 192.168.113.7.

Далее необходимо создать свой подкаталог в каталоге **config** и скопировать в него содержимое каталога **config/default** (рис. 13).

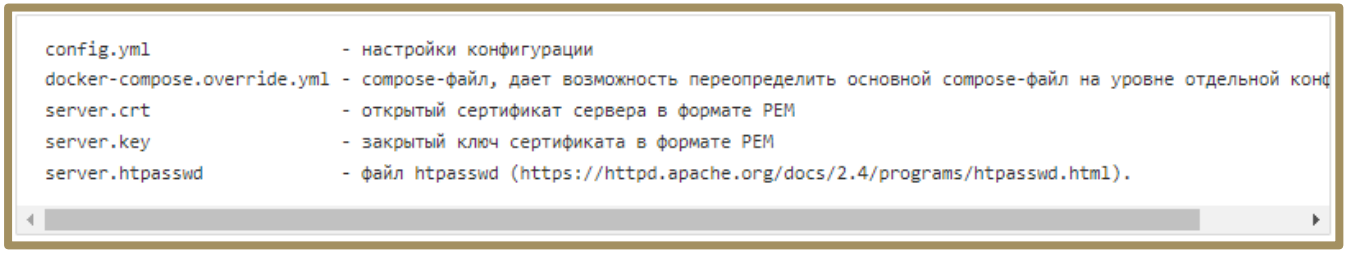


Рисунок 13 – Настройки каталога config по умолчанию

Далее необходимо настроить содержимое каждого файла так, как требуется (кроме файла **server.htpasswd**). В файле **config.yml** содержатся все доступные настройки, включая версии компонентов системы и секреты сервисов (secrets). Подробное описание файла конфигурации:

config_name – название конфигурации, должно совпадать с названием каталога, содержащего данный конфигурационный файл;

product_type – тип продукта, допустимы два значения: EDR и ARW;

allowed_hosts – внешние домены и IP-адреса, по которым агенты и пользователи из браузера будут обращаться к серверу EDR, через запятую следует указать все IP-адреса и домены, по которым будет осуществляться внешний доступ системе;

elasticsearch_hosts – закомментированная настройка, если сервер EDR должен использовать внешнюю базу Elasticsearch, то необходимо раскомментировать настройку и указать адрес подключения к Elasticsearch вместе с паролем, если он есть;

event_retention_period – срок хранения событий в базе Elasticsearch, после которого события могут быть удалены (вместе с индексами);

auto_verification – авто верификация агентов: если Agent ID есть в базе, то агент считается верифицированным;

logging_level – уровень логирования демонов (число, DEBUG = 10, INFO = 20, WARNING = 30, ERROR = 40);

config_sync_period – период (в минутах) синхронизации внешних наборов конфигураций, значение по умолчанию 2;

onfig_file_max_size – максимальный размер (в мегабайтах) файла набора конфигурации, значение по умолчанию – 100;

etw_data_stream – закомментированная настройка, устанавливающая экспорт событий ETW (winlog) в data stream, по умолчанию экспорт отключен, для включения необходимо раскомментировать и указать имя data stream;

django_email* – настройки подключения к почтовому серверу, который используется для отправки уведомлений сервером EDR;

docker_registry* – настройки подключения к реестру Docker-образов;

eventq* – настройки временного буфера для поступающих от агентов событий (сделан на очередях Redis);

cache* – настройки кеш-сервиса на Redis;

minio* – настройки объектного хранилища MinIO с S3 совместимым API, используется для хранения конфигураций (списков) агентов, а также для хранения файлов, загруженных с агентов, и дистрибутивов агента.

postgresql* – настройки базы данных PostgreSQL, которая используется как бекенд для Django-приложения;

elasticsearch – настройки базы данных elasticsearch, которая является базой данной для всех событий и инцидентов;

worker* – настройки воркеров, воркеры вычитывают события из eventq (временный буфер на Redis), совершают с событием ряд операций, после чего записывают в Elasticsearch, кроме того воркеры производят экспорт событий во внешние системы (например, в SIEM);

djangoapp_version – версия веб-приложения на Django, предоставляет API для фронтенда, взаимодействует с агентами, управляет другими компонентами системы;

djangoapp_session_token_secret_key – ключ для шифрования сессионных токенов пользователей;

webserver_version – версия веб-сервера, веб-сервер принимает запросы от агентов и от фронтенд-приложений, выполняет предобработку данных и проксирует запросы другим сервисам

loadbalancer_version – версия балансировщика разгрузки, реализованная на Nginx, сервис принимает внешние подключения по портам 80, 443;

frontend_version – версия веб-модуля администрирования;

rating* – настройки рейтинговой подсистемы;

ioa* – настройки микросервиса проверки индикаторов атак;

ti_strict_mode – настройки показа содержимого внешних наборов с TI: 0 – показывать все данные наборов, 1 – показывать все данные, кроме поля **Условие** в индикаторах атак;

agent_proxy_limit – настройки количества агентов, которые получат информацию об обновлениях от сервера за период в 10 сек;

compose_dir – путь до каталога с файлами docker-compose.yml и env;

secrets_dir – путь до файлов, содержащих секреты сервисов (пароли, токены и другую чувствительную информацию).

Несмотря на то, что **docker-compose.yml** уже есть и настроен правильно (находится в каталоге **compose-files**), может возникнуть необходимость в корректировании настроек.

Это можно сделать на уровне собственной конфигурации, отредактировав файл **docker-compose.override.yml**. Такие изменения не затронут другие конфигурации.

Файлы **server.crt** и **server.key** можно настроить (если есть сертификат, подписанный Центром Сертификации), а можно и не настраивать, если конфигурация тестовая, и доступ извне будет ограничен. В этом случае сертификат будет самоподписанным.

Важно

Файл server.htpasswd необходимо оставить без изменений, скопировав его из **config/default**.

Запуск скрипта развертывания (Ansible Playbook)

Когда все файлы конфигурации будут настроены, необходимо перейти в корень репозитория (edr-deploy). Рядом должен находиться файл edr-install.yml.

Далее необходимо выполнить в консоли команду:

```
$ ansible-playbook edr-install.yml --extra-vars "@config/192.168.113.60/config.yml" -i 192.168.113.60, -u username --ask-become-pass
```

Описание аргументов команды:

@config/192.168.113.60/config.yml – это путь до файла **config.yml** вашей конфигурации;

config/192.168.113.60 – это каталог конфигурации;

192.168.113.60 – это адрес сервера для доступа по SSH (Docker-хост);

username – это имя удаленного пользователя.

Если ваш удаленный пользователь root, то можно сократить команду до:

```
$ ansible-playbook edr-install.yml --extra-vars "@config/192.168.113.60/config.yml" -i 192.168.113.60, -u root
```

После выполнения команды начнется процесс развертывания сервера EDR. В начале может возникнуть необходимость ввода пароля для доступа по SSH. Далее необходимо ввести пароль и нажать клавишу **Enter**.

Параметры установки уже известны демону Ansible, он возьмет их из файла **config.yml**.

Когда Ansible закончит работу, необходимо подождать еще несколько минут (5-10) и перейти в окно веб-браузера.

Далее необходимо набрать адрес сервера и проверить подключение, затем выполнить вход в систему с логином и паролем **admin/admin** и поменять пароль по умолчанию.

Обновление сервера EDR

Если требуется обновить сервер EDR (например, при изменении версии компонента в **config.yml**), то необходимо выполнить команду, указанную выше, но заменить **edr-install.yml** на **edr-update.yml**. Остальную часть команды менять не нужно. Пример:

```
$ ansible-playbook edr-update.yml --extra-vars "@config/192.168.113.60/config.yml" -i 192.168.113.60, -u username --ask-become-pass
```

5.3 Роли

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

– аналитик;

– администратор;

– оператор поиска угроз (threat hunter).

Аналитик – сотрудник отдела информационной безопасности (далее ИБ) или Центра обеспечения безопасности (SOC-центр), который выполняет функцию экспертной оценки угроз, возникающих в отношении защищаемой IT-инфраструктуры. Аналитик является пользователем серверной части Программы.

Аналитик с помощью доступного для него функционала расследует события, которые потенциально могут нарушить работу защищаемых устройств или защищаемой сети в целом. Это работа с инцидентами, ретроспективный анализ событий, работа с правилами, регулирующими индикацию атак и т.д.

В случае обнаружения вредоносной программы или атаки на инфраструктуру защищаемого объекта, аналитик может оперативно отреагировать, изолировав зараженный вредоносным файлом хост или заблокировав действие опасной программы, а также использовать другие доступные способы, чтобы решить проблему нарушения безопасности.

Администратор – уполномоченный сотрудник организации Заказчика или SOC-центра. Администратор устанавливает серверный и агентский модули, а также настраивает Программу в соответствии с настоящим документом для его корректной и полнофункциональной работы.

В круг типовых задач администратора входит:

– поддержание администрируемой системы в рамках выбранной политики безопасности;

– обеспечение должного уровня конфиденциальности и целостности данных;

– подготовка и сохранение резервных копий данных, их периодическая проверка и уничтожение;

– создание и поддержание в актуальном состоянии пользовательских учётных записей;

– ответственность за информационную безопасность в компании;

– отслеживание информации об уязвимостях системы и своевременное принятие мер;

– периодическое практическое тестирование защищенности системы;

– документирование своей работы;

– устранение неполадок в системе.

В круг типовых задач аналитика входят:

– реагирование на предупреждения Программы;

– анализ предупреждений Программы;

– регистрация инцидента ИБ, проведение внутреннего расследования;

– предотвращение развития инцидента ИБ;

– устранение инцидента ИБ;

– восстановление безопасности после инцидента ИБ;

– формирование рекомендаций по результатам инцидента ИБ по повышению уровня ИБ.

Оператор поиска угроз (threat hunter) – сотрудник отдела ИБ или SOC-центра, который с помощью запросов на странице **Активность** может провести исследование активности агентов с целью обнаружения артефактов вредоносной активности или признаков направленной атаки на защищаемую инфраструктуру. Например, отчеты о выявленных атаках любого вендора содержат артефакты, связанные с этими атаками (имена файлов, хеши, ip-адреса, доменные имена, некоторые специфичные действия процессов).

Полученные данные используются для пополнения базы индикаторов компрометации и индикаторов атак.

В типовой круг задач оператора поиска угроз входят:

– просмотр и анализ активности процессов, зарегистрированных в агентской сети;

– просмотр и анализ произошедших инцидентов.

5.4 Особенности работы Программы с антивирусными средствами сторонних производителей

5.4.1. 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>/*.

5.4.2. Особенности выполнения действия блокирования для антивирусных решений.

В некоторых случаях к заблокированному модулю процесса может обращаться антивирусное средство. Для того, чтобы это было возможно, в Программе предусмотрено внутреннее исключение, которое создает событие для подобного обращения. То есть, если событие блокирования возникает в контексте антивирусного процесса (такие процессы отмечаются в системе флагом AVEngine), то блокирующее действие переопределяется на **Продолжать наблюдение** и критичность события сбрасывается на уровень **Информация**, при этом в причине события указывается **Исключение для программ**. Такая логика характерна для всех аналитических правил, кроме файловых исключений.

6. Интерфейс Программы

6.1 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, для открытия окна авторизации необходимо в строке браузера ввести имя сервера или его ip-адрес. После ввода в строке браузера корректных данных откроется окно авторизации (рис. 14).

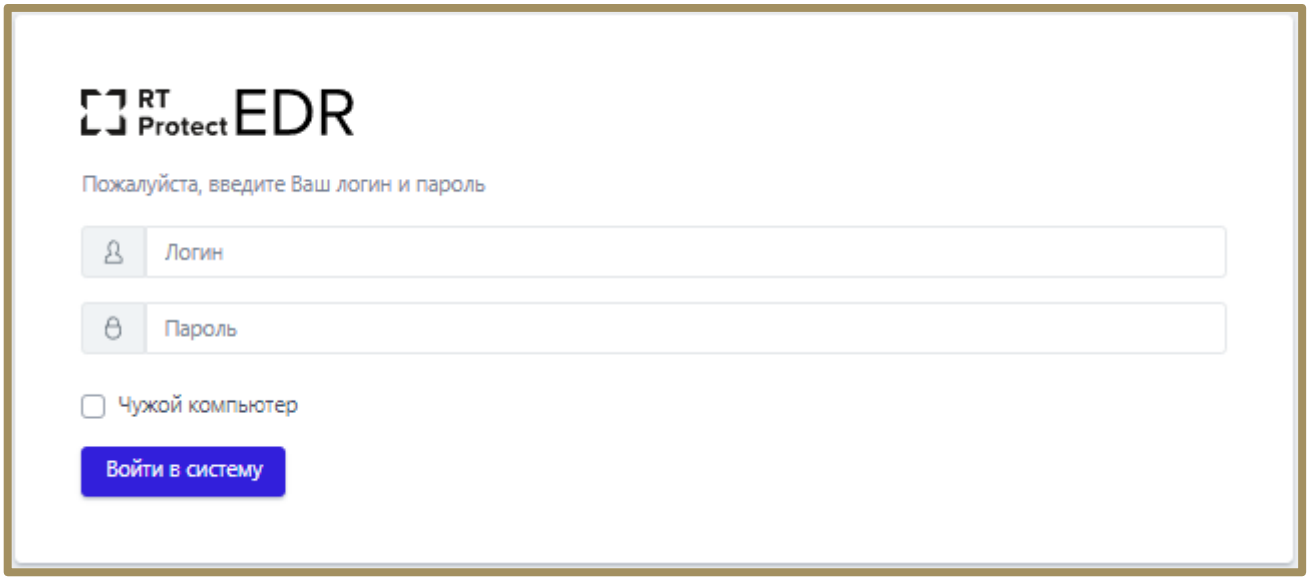


Рисунок 14 – Окно авторизации

После ввода в окне авторизации пароля и логина администратора открывается основное окно Программы (рис. 15).

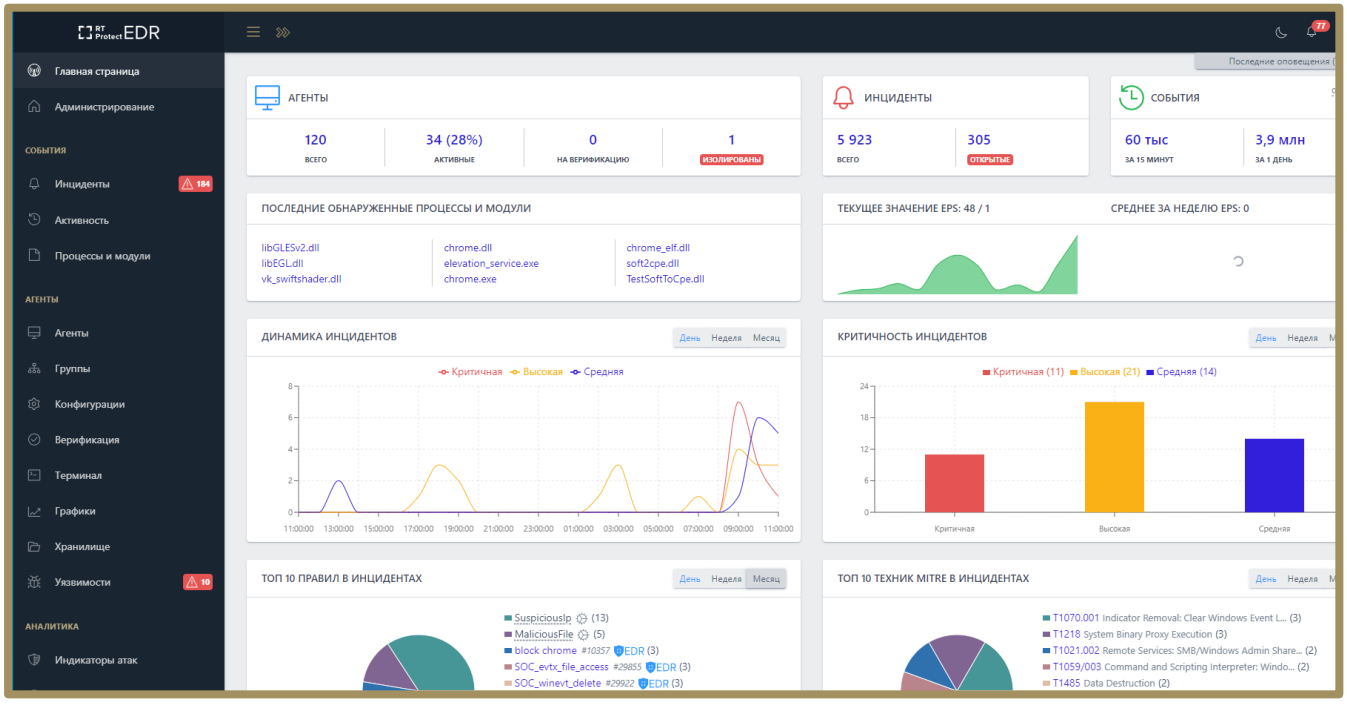


Рисунок 15 – Основное окно Программы

Если в течение 12 часов пользователь выполнил 20 или более неудачных попыток входа, то его учетная запись будет заблокирована. В этом случае разблокировать такого пользователя сможет только администратор (подробнее см. подраздел 6.4).

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 защиты данных на агентах;

– просмотр действий пользователей;

– просмотр параметров работы Программы.

В левой части основного окна Программы (см. рис. 15) находится вертикальная панель управления, доступная администратору для выполнения различных настроек и просмотра информации по разделам.

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 – 

.

6.2 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 **Скрыть/показать панель разделов** () левая панель с разделами Программы становится скрытой. Для возврата первоначального вида необходимо повторно нажать на кнопку  .

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** ().

6.2.1. 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. 16).

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

Рисунок 16 – 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. 16). 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 приходят в режиме реального времени. При появлении нового оповещения в верхней части основного окна Программы появляется сообщение (рис. 17).

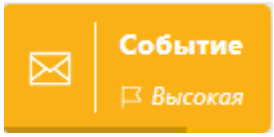


Рисунок 17 – Всплывающее окно с оповещением о событии

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. Также в строке с названием находится идентификационный номер инцидента.

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).

6.2.2. 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. 18).

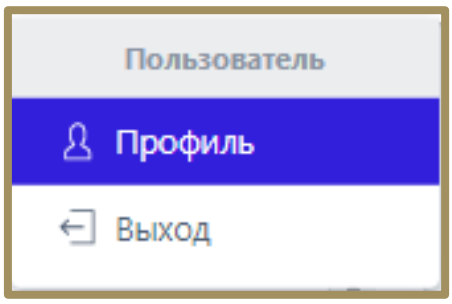


Рисунок 18 – Меню «Пользователь»

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 (администратор или аналитик) 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. 19).

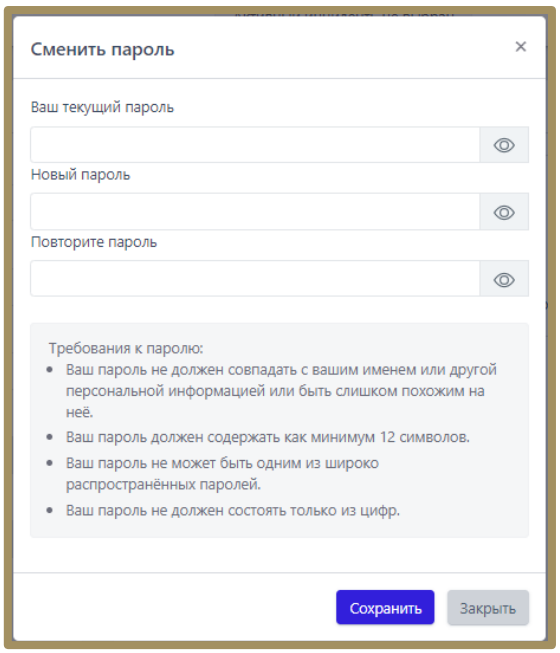


Рисунок 19 – Окно смены пароля

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.

6.3 Главная страница

На рисунке 15 представлен раздел **Главная страница** модуля управления.

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

– **Агенты;**

– **Инфраструктура;**

– **Инциденты;**

– **Последние обнаруженные процессы и модули;**

– **Текущее значение EPS и среднее за неделю EPS;**

– **Динамика инцидентов;**

– **Распределение инцидентов по критичности;**

– **Топ 10 правил в инцидентах;**

– **Топ 10 техник MITRE ATT&CK в инцидентах;**

– **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 **Список агентов**, 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 нажатии левой кнопкой мыши (далее ЛКМ) по числовому значению выбранной категории инцидентов происходит переход к разделу **Инциденты**, в котором представлена более подробная информация о зарегистрированных в Программе инцидентах (см. пункт 6.5.1).

В области просмотра **События** администратор может увидеть, сколько событий пришло от всех верифицированных и не изолированных 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.

В области просмотра **Последние обнаруженные процессы и модули** показываются последние программы, обнаруженные в защищаемой инфраструктуре.

При наведении указателя мыши на имя процесса появляется всплывающее окно с описанием полного пути до места обнаружения процесса/модуля (рис. 20).

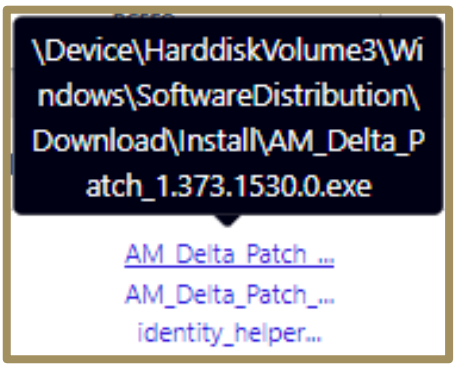


Рисунок 20 – Путь до обнаруженного процесса

Имя процесса или модуля является активной ссылкой, при нажатии на нее происходит переход на страницу активности, на которой показаны события, связанные с выбранной программой.

В области **Текущее значение 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 текущей даты, времени и количества событий (рис. 21).

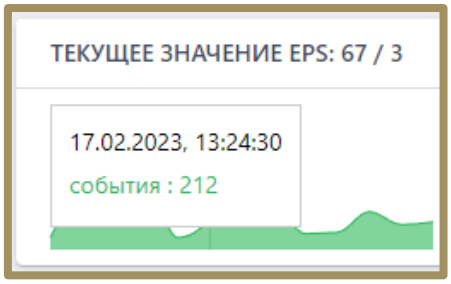


Рисунок 21 – Отображение EPS на графике с интервалом 5 сек

В области **Среднее за неделю EPS** отображается график и среднее за неделю количество событий в секунду для активных агентов.

На графике имеются определенные интервалы (1 день), отмеченные точками, при наведении на которые указателя мыши, появляется всплывающее окно с отображением текущей даты, времени и количества событий (рис. 22).

Рисунок 22 – Отображение среднего за неделю EPS на графике в интервале 1 день

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.

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 **Топ 10 правил в инцидентах** в виде круговой диаграммы показаны десять правил, которые наиболее часто срабатывают при создании инцидентов. Некоторые правила могут содержать ссылки на наборы в виде значков (EDR) или значки, обозначающие удаленные наборы, а также наборы, полученные от TI-платформы (, TI).

Можно изменить период, за который учитываются эти диаграммы, изменив настройки на День/Неделя/Месяц. Имя правила в списке правил является активной ссылкой, если это не встроенное правило, при нажатии по ссылке происходит переход на страницу с правилом. При наведении указателя мыши на правило появляется всплывающее окно с отображением имени правила и категорией правила (Индикатор компрометации, Индикатор атак).

В области **ТОП 10 ТЕХНИК MITRE ATT&CK В ИНЦИДЕНТАХ** в виде круговой диаграммы отображается 10 основных техник MITRE, на которые ссылаются инциденты.

Диаграмму можно отображать за периоды в **День/Неделю/Месяц**. Имена техник являются активными ссылками, при нажатии происходит переход на сайт https://attack.mitre.org, на котором можно ознакомиться с описанием данной техники.

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.

6.4 Администрирование

В разделе **Администрирование** администратор может просматривать информацию о пользователях, создавать и удалять учетные записи пользователей, а также изменять параметры учетных записей пользователей.

6.4.1. Общая информация о списке пользователей

В разделе **Администрирование** показана информация обо всех зарегистрированных в Программе пользователях.

Данные о пользователях представлены в табличном виде (рисунок 23).

Таблица содержит следующие поля:

1) Имя пользователя;

2) Последнее время входа;

3) Имя;

4) Фамилия;

5) Email;

6) Роль;

7) Статус;

8) Управление.

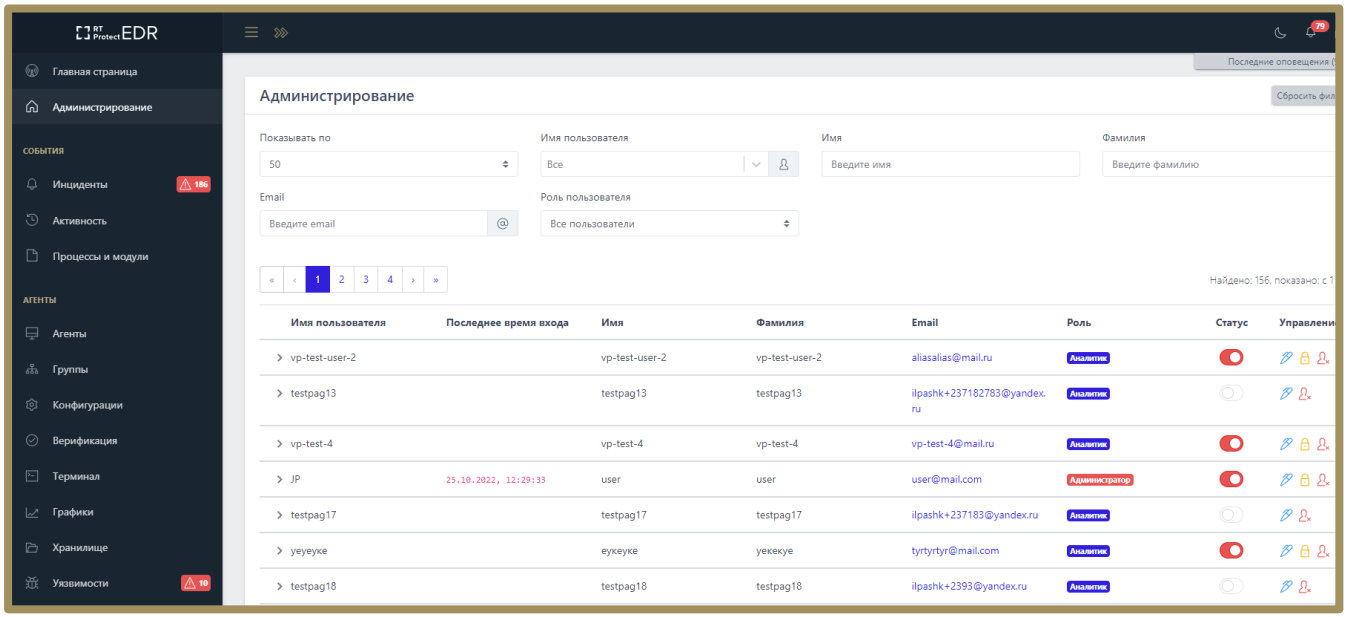


Рисунок 23 – Раздел «Администрирование»

Имя пользователя – содержит логин, под которым пользователь зарегистрирован в Программе.

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.

Email – электронный почтовый адрес, указанный пользователем при регистрации.

Роль – функциональная роль пользователя (предусмотрены 3 роли: **Администратор, Аналитик, Оператор поиска угроз**).

Статус и **Управление** – в указанных полях содержатся кнопки для изменения параметров учетных записей пользователей.

В верхней части окна над таблицей содержатся строки для поиска пользователей по параметрам фильтрации:

– **Показывать по;**

– **Имя пользователя** (логин);

– **Имя;**

– **Фамилия;**

– **Email;**

– **Роль пользователя.**

Каждая строка таблицы содержит дополнительную информацию о сессиях пользователя, для ее просмотра необходимо нажать ЛКМ на значок ›. В случае, если у пользователя были активные сессии, они будут показаны ниже строки. По умолчанию отображается только последняя сессия (рис. 24).

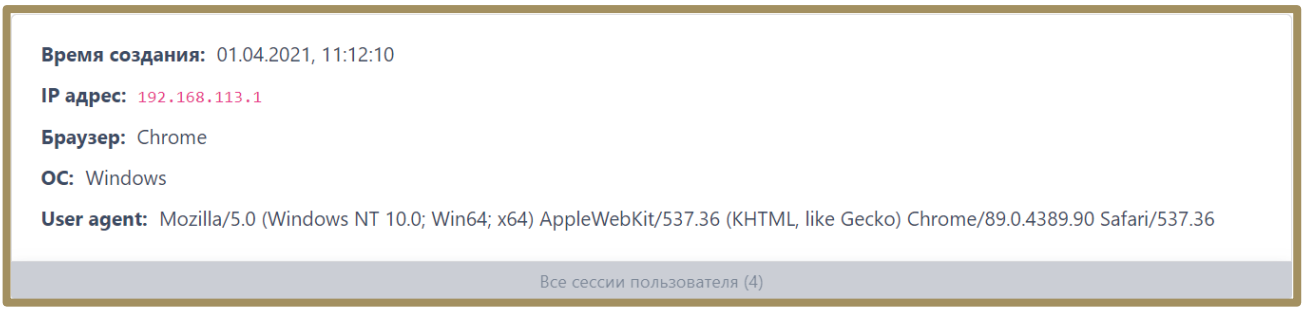


Рисунок 24 – Информация о сессиях пользователя

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 наименование браузера, с помощью которого выполняется взаимодействие с агентом.

6.4.2. 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** 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, адрес электронной почты, а также роль выбранного пользователя.

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. 25). Пароль должен соответствовать правилам, указанным в пункте 6.4.3.

Рисунок 25 – 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.

При нажатии кнопки **Удалить пользователя** открывается окно, в котором для удаления учетной записи выбранного пользователя следует нажать кнопку **Выполнить.**

6.4.3. 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;**

– **Роль.**

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.

6.4.4. 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. 26). Такое же сообщение выводится во всех полях, требующих ввода информации.

Рисунок 26 – 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. 27).

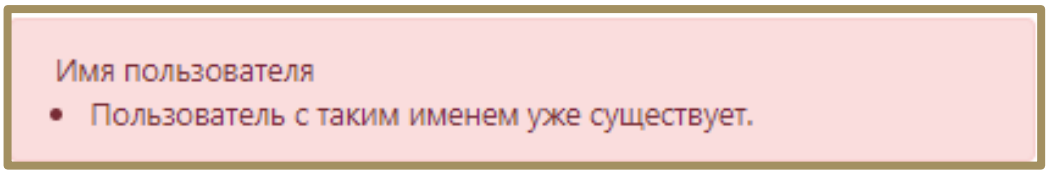


Рисунок 27 – Сообщение о совпадении имени пользователя

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. 28).

Рисунок 28 – Сообщение о неправильном адресе электронной почты

Если введенный пароль не соответствует одному или нескольким указанным в пункте 6.4.3 правилам, то в нижней части окна появится сообщение, в котором будет указано нарушенное при создании пароля правил (рис. 29).

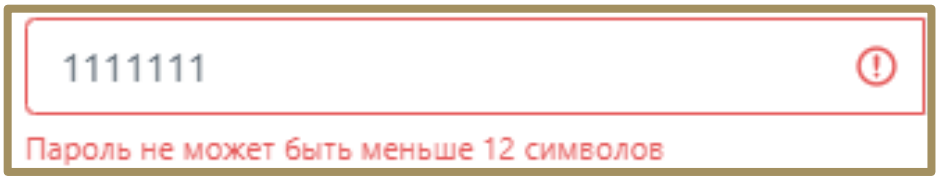


Рисунок 29 – Предупреждающее сообщение при вводе некорректного пароля

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. 30).

Рисунок 30 – 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. 31).

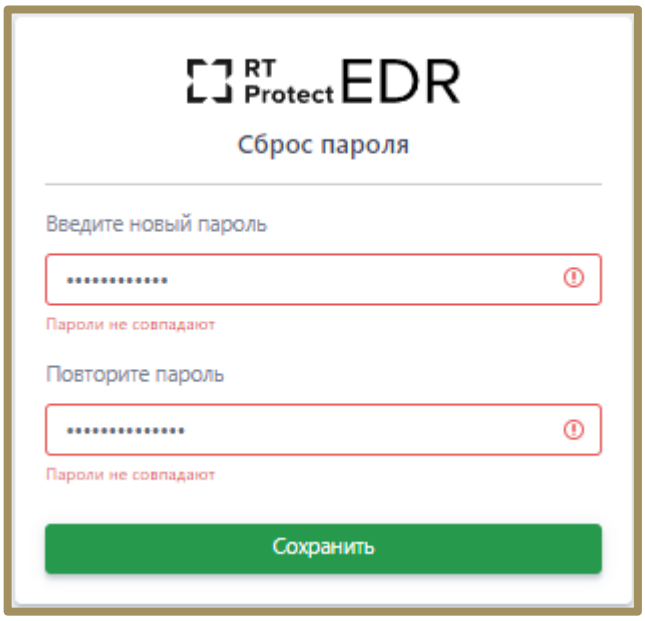


Рисунок 31 – Ввод некорректных значений при сбросе пароля

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 12 часов пользователь Программы выполнит 20 или более неудачных попыток входа, то его учетная запись будет заблокирована. В этом случае разблокировать такого пользователя сможет только администратор Программы.

6.5 События

В серверной части Программы обрабатываются события активности, происходящей на конечных точках с установленными на них агентами. Все обрабатываемые события можно разделить на три больших категории: обнаружения (в устоявшейся международной терминологии – **alerts**), информационные обнаружения (**informational alerts**) и телеметрия.

Обнаружения – это события, которые EDR со средней и выше степенью вероятности (средняя+ критичность события) идентифицирует как опасные или вредоносные. На страницах с отображаемыми событиями обнаружения помечаются значком ⚠ в полях **Описание** или **Название**. Система обнаружения и оповещения в Программе охватывает события множества компьютерных подсистем: файловая подсистема, сетевые события, события, происходящие с процессами, реестром и т.д.

Информационные обнаружения – это события, имеющие низкий уровень критичности, то есть события, представляющие маловероятную угрозу, но при этом изредка требующие внимания аналитика информационной безопасности. Такие события в некоторых случаях могут представлять опасность для защищаемой ИТ-инфраструктуры или являться признаком того, что на агенте проявляется активность, связанная с развитием атаки. Информационные обнаружения (informational alerts) не настолько явно говорят нам о том, что в защищаемой системе присутствует вредоносная активность или объект, но в то

же время достаточно важны, чтобы выделить их в отдельную категорию событий.

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.

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».

6.5.1. 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** (см. подраздел 6.7). Кроме автоматической генерации инцидентов в Программе предусмотрен функционал добавления событий в инциденты в ручном режиме (см. пункт 6.5.2).

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 32. 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.

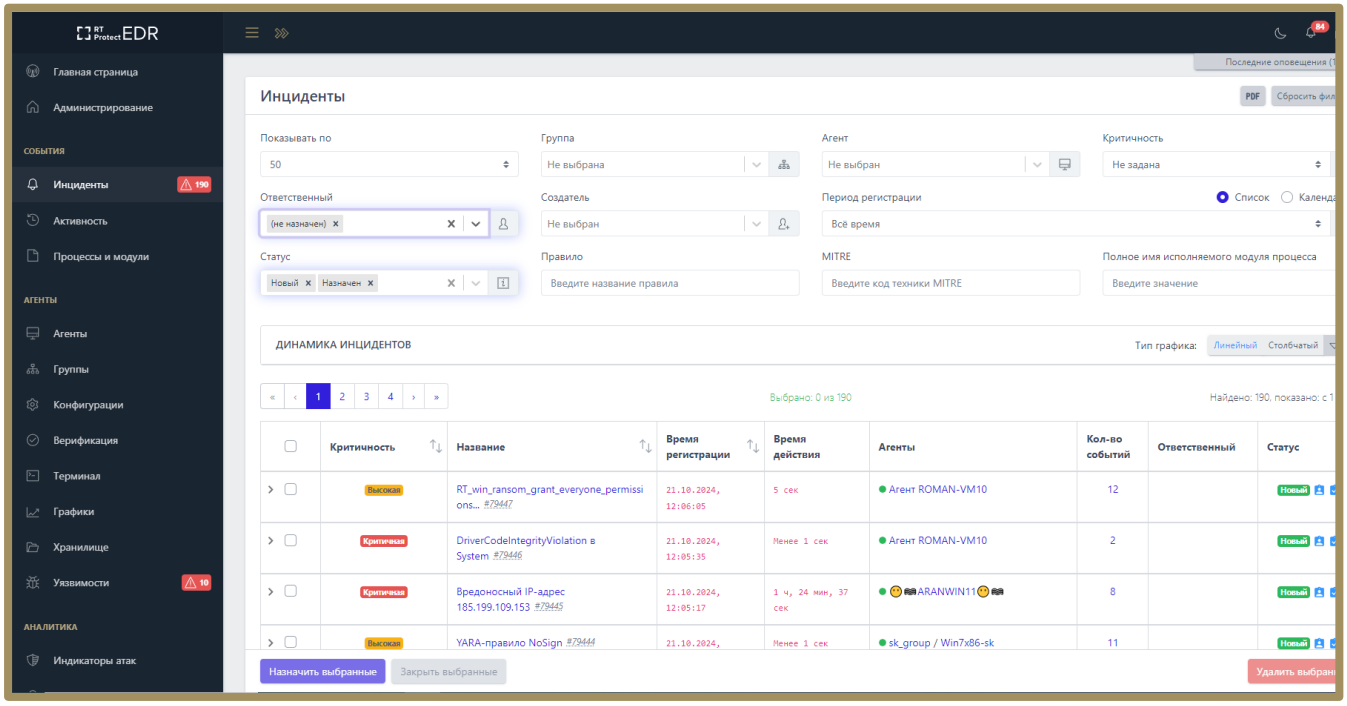


Рисунок 32 – Страница «Инциденты»

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) Кнопка 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 кнопкой выбора инцидентов содержится кнопка раскрытия дополнительной информации о событиях, включенных в инцидент ( ). При нажатии ЛКМ 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 33.

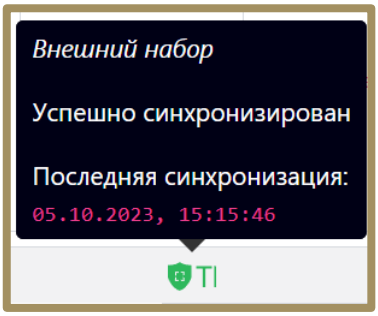


Рисунок 33 – Всплывающее сообщение с информацией о внешнем наборе

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**, **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. 34).

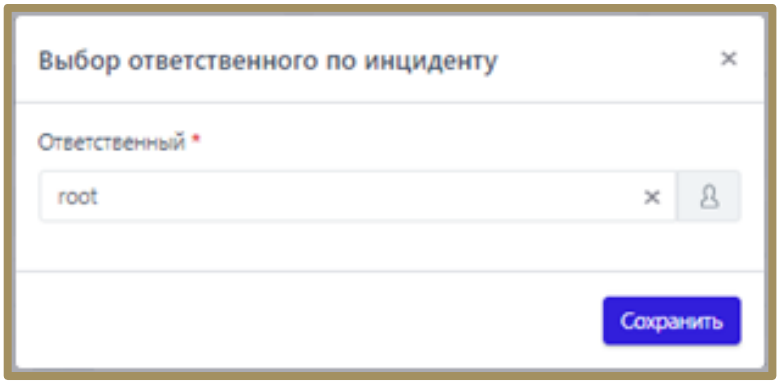


Рисунок 34 – Выбор пользователя, ответственного за решение инцидента

В случае, если ответственный за инцидент уже был назначен, то для выбора нового пользователя, ответственного за инцидент, необходимо в строке **Ответственный** удалить текущего пользователя, нажав в ней кнопку . Далее выбрать пользователя из списка, нажав ЛКМ на пустую строку поля **Ответственный**, 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 или открыть инцидент повторно – (активна при статусе **Новый** и **Закрыт**);

Для закрытия инцидента необходимо нажать кнопку **Закрыть инцидент** ( ) и в открывшемся окне **Закрытие инцидента** (рис. 35) нажать кнопку **Сохранить**. Закрыть инцидент можно, даже если для инцидента не назначен ответственный.

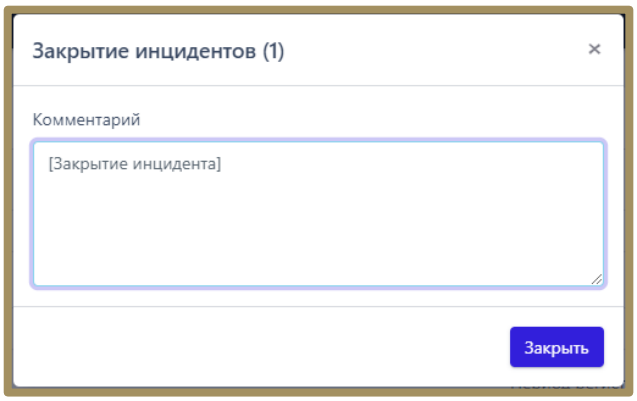


Рисунок 35 – Закрытие инцидентов

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**.

Для повторного открытия инцидента 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.

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

В поле фильтров **Правило**, **MITRE**, **Полное имя исполняемого модуля процесса,** поддерживается автоподставление 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).

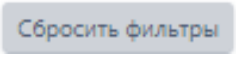
Фильтр **Период регистрации** в сравнении с фильтром **Период регистрации (на сервере)** содержит одно дополнительное значение **Всё время,** при выборе которого показываются все когда-либо зарегистрированные в Программе инциденты.

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 инциденты,** 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. 36);

3) Нажать кнопку **Начать удаление**;

4) Далее необходимо подтвердить удаление в открывшемся окне **Подтверждение действия**, нажав кнопку **Выполнить.**

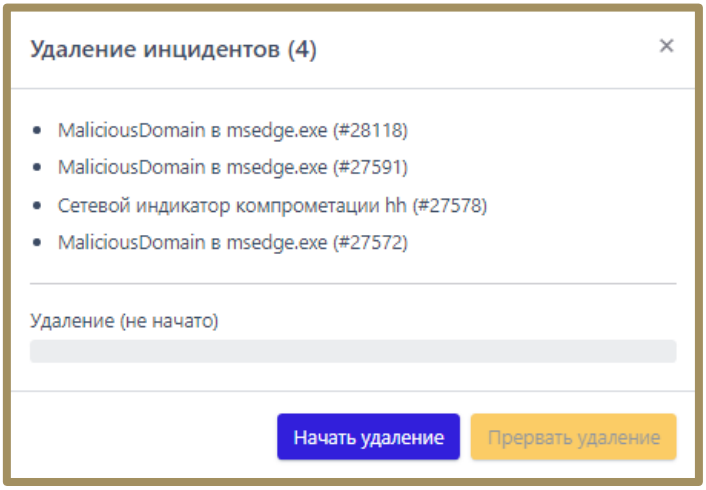


Рисунок 36 – Групповое удаление инцидентов

В процессе группового удаления инцидентов имеется возможность прервать операцию удаления, нажав по иконке 

. Удаление инцидентов прервется на том инциденте, который не отмечен значком  в списке удаляемых инцидентов.

5) Для завершения операции удаления следует нажать кнопку **Закрыть**.

Администратору доступна возможность создания отчетов по инцидентам, отображаемым на странице. Чтобы сохранить отчет в формате pdf, ему необходимо нажать значок 

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 области **Информация об инциденте**.

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) **Информация об инциденте**;

2) **Комментарии**;

3) Дополнительная информация;

4) **Обнаружения**.

В области **Информация об инциденте** пользователь 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 **Информация об инциденте** отображаются следующие данные:

– название инцидента;

– критичность инцидента;

– ответственный за решение инцидента;

– статус инцидента;

– агент, на котором 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. 37).

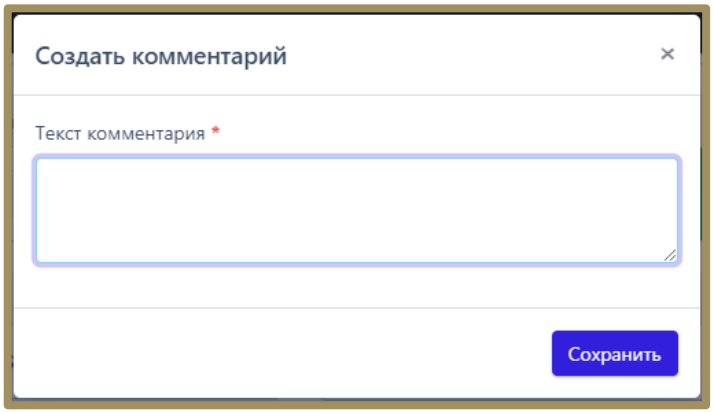


Рисунок 37 – Окно ввода комментария

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 16).

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 6.5.3).

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. Создать исключение с помощью мастера можно не для всех инцидентов.

Общий вид окна при создании исключения с помощью мастера исключений для файла представлен на рисунке 38.

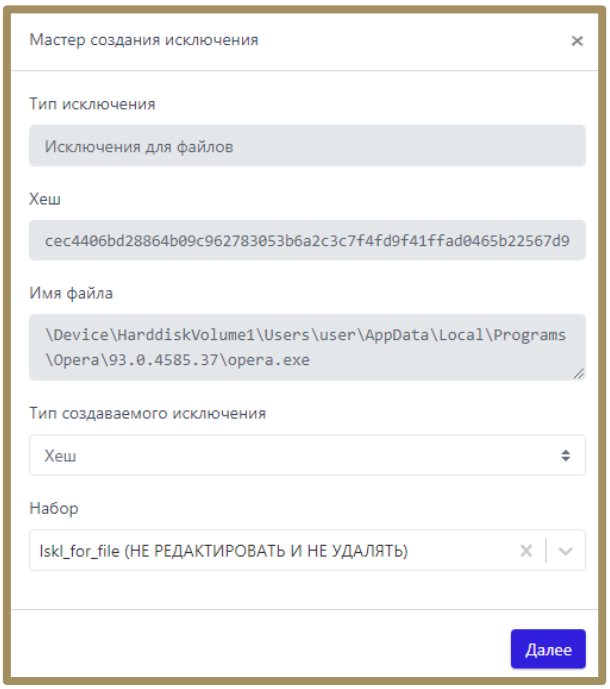


Рисунок 38 – Окно мастера создания исключений

В данном окне поля **Тип исключения**, **Хеш**, **Имя файла** устанавливаются автоматически из выбранного обнаружения, требуется определить только тип создаваемого исключения: исключение по хеш-сумме или исключение по имени файла. Также можно указать набор, в который следует добавить исключение.

Для дальнейшего создания исключения требуется нажать кнопку **Далее**, после чего произойдет переход к окну **Добавить исключение** (рис. 39).

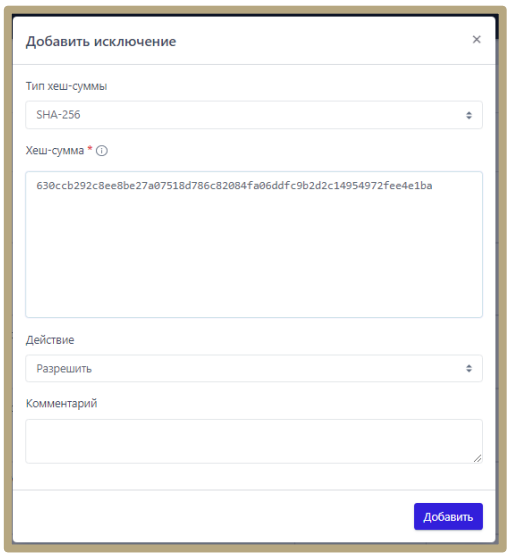


Рисунок 39 – Окно добавления исключения

Хеш-сумма заполняется автоматически из предыдущего окна. Чтобы завершить добавление исключения, требуется только определить действие (**Разрешить**/**Блокировать**) и нажать по кнопке **Добавить**.

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

6.5.2. 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 40.

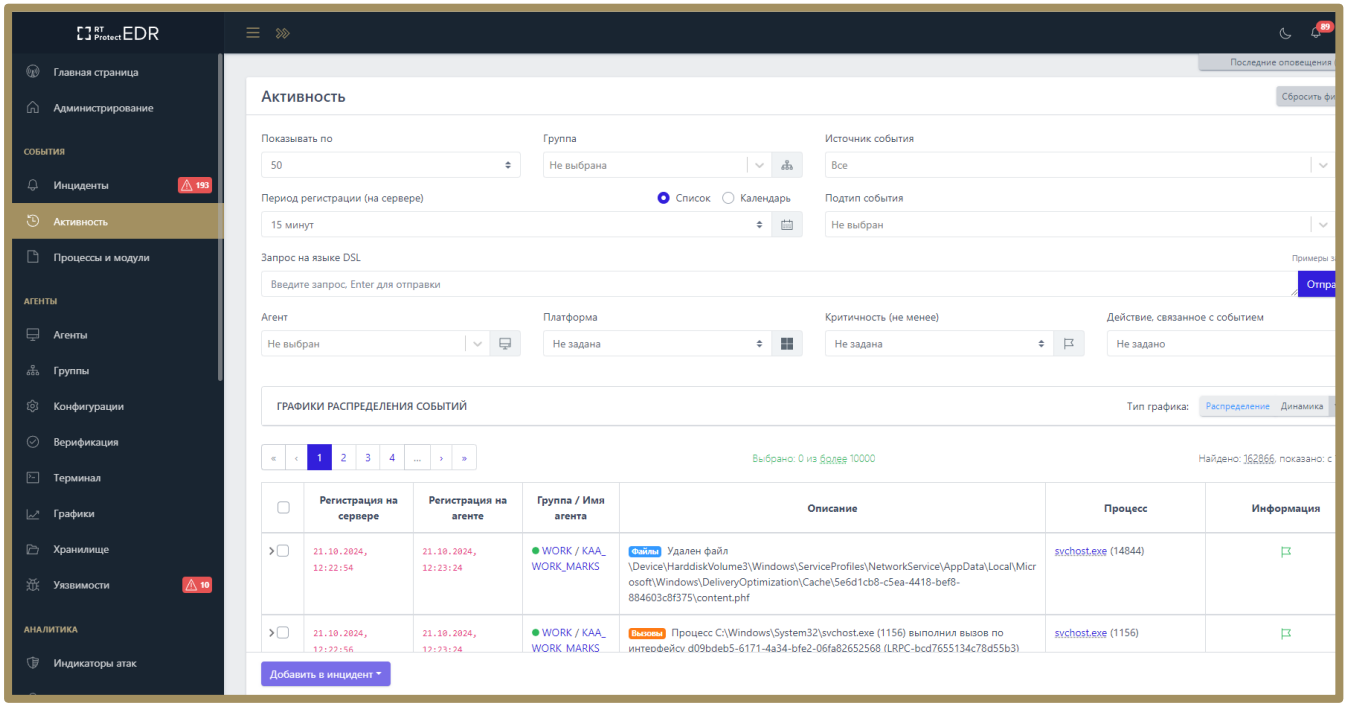


Рисунок 40 – Активность

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 показать графики, необходимо нажать кнопку  .

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. 41).

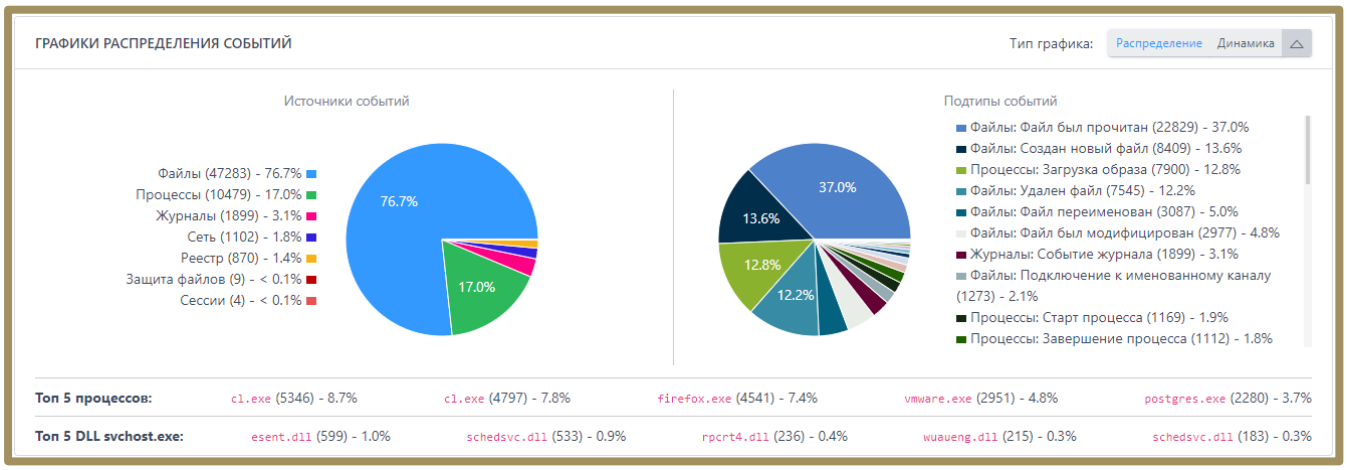


Рисунок 41 – Графики распределения событий

Ниже графиков пользователь EDR может просмотреть топ 5 наиболее часто встречающихся процессов в защищаемой инфраструктуре, а также топ 5 динамически загружаемых библиотек в хост-процессе **svchost.exe**.

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. 16).

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 фильтрацией по времени) 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. 42).

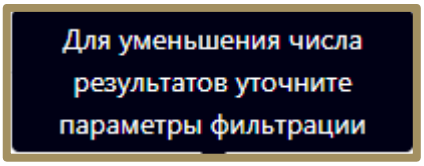
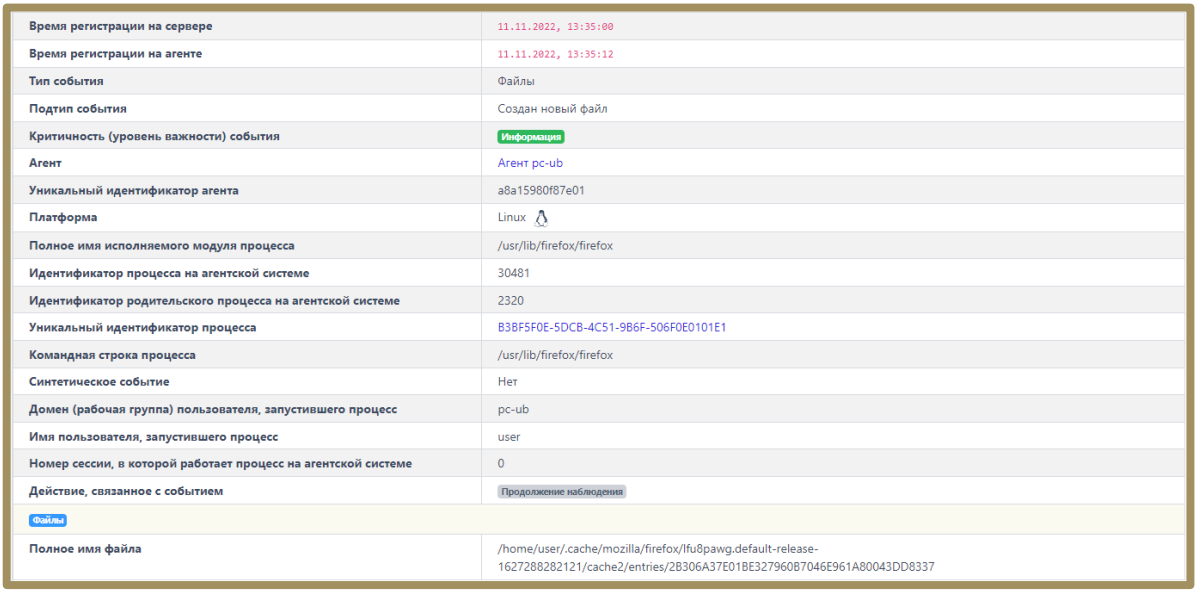


Рисунок 42 – Подсказка в таблице событий

Каждое событие содержит в себе сводную информацию, собранную в виде карточки события (рис. 43).



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 43 – Карточка событий

Карточка события открывается при нажатии ЛКМ на выбранном событии. 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».

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

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 {...}.

Некоторые поля в карточке события содержат гиперссылки для перехода к различным разделам Программы. При нажатии ЛКМ на имени агента или имени группы в строке **Агент** осуществляется переход на страницу агента или группы.

В строках **Полное имя исполняемого модуля процесса**, **Полное имя файла**, **Полное имя исполняемого модуля-инициатора операции**, **Полное имя файла образа** справа от имени файла или модуля содержится кнопка загрузки файла в файловое хранилище . При наведении курсора мыши на кнопку появится всплывающее окно с сообщением **Загрузить файл в файловое хранилище** (рис. 44).

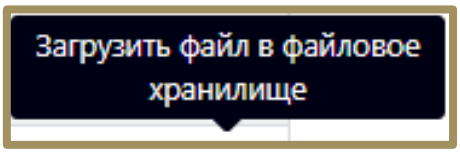


Рисунок 44 – Сообщение о загрузке файла в файловое хранилище

Если агент, на котором происходило событие, отображаемое в карточке события, в данный момент не активен, кнопка загрузки приобретёт вид . При наведении курсора мыши на кнопку появится всплывающее окно с сообщением **Загрузка файла невозможна, так как агент не активен** (рис. 45).

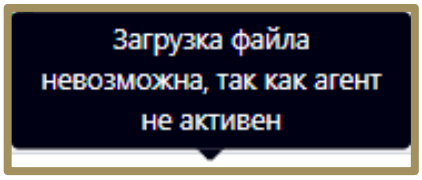


Рисунок 45 – Сообщение о том, что загрузка файла невозможна

Если агент, на котором произошло событие, активен и ссылка на скачивание файла доступна, то при нажатии кнопки отправляется запрос на загрузку файла, после чего файл загружается в хранилище.

При нажатии ЛКМ на значении идентификаторов процесса в таблице и карточках событий осуществляется переход на страницу **Процессы**. Подробная информация о странице рассматривается в подпункте 6.5.3.

При нажатии ЛКМ на значениях различных проверяемых объектов в строках карточки события или столбцах таблицы событий появляется всплывающее окно с информацией о проверке на TI-платформе объекта (рис. 46):

– ip-адрес;

– имя домена;

– хеш файла.

В верхней части карточки с кратким отчетом TI-платформы содержатся информация о проверяемом артефакте. Далее следует краткий отчет о том, когда объект был обнаружен, и общий вывод об опасности/безопасности объекта (например, Безопасный). Окно содержит кнопку **Перейти к отчету**. Обновление данных по объекту происходит автоматически.

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

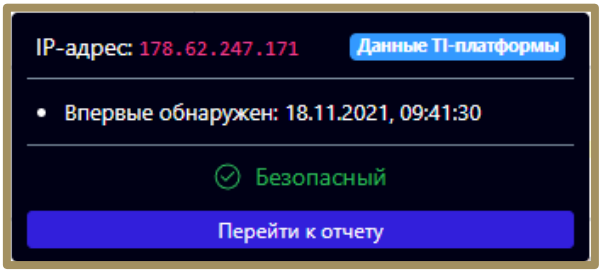


Рисунок 46 – Карточка информации о проверке объекта на TI-платформе

Проверяемые объекты в зависимости от содержания отчета отображаются на странице **Активность** в различной цветовой гамме. Объекты, которые TI-платформа определяет как безопасные, отмечаются зеленым цветом (192.168.80.2). Вредоносные объекты отмечаются красным цветом (93.184.220.29). Объекты, для которых процесс анализа выполняется в настоящее время, отображаются синим цветом (1b28cbf8a06b973a2422f4e1e400b441430c75dfe4d4c8be6f23dff824e96). Объекты, для которых информация на TI-платформе отсутствует или не проверялась, отмечаются серым цветом (74.125.131.94). Карточка для вредоносного объекта показана на рисунке 47.

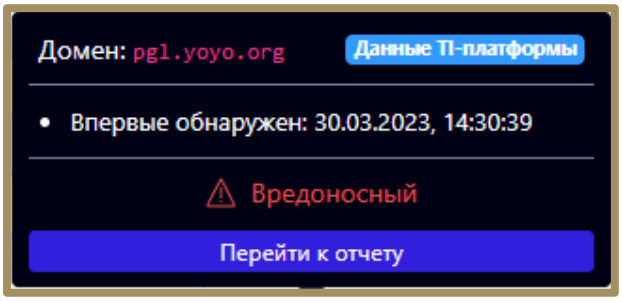


Рисунок 47 – Карточка TI-платформы для вредоносного объекта

Карточка TI-платформы для объекта, информация по которому отсутствует, представлена на рисунке 48.

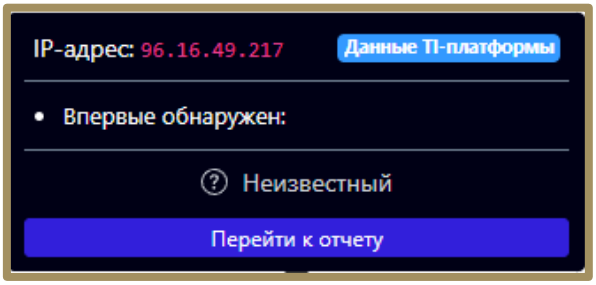


Рисунок 48 – Карточка TI-платформы для отсутствующего в базе объекта

Для локальных ip-адресов и доменов проверка на TI-платформе не выполняется (рис. 49).

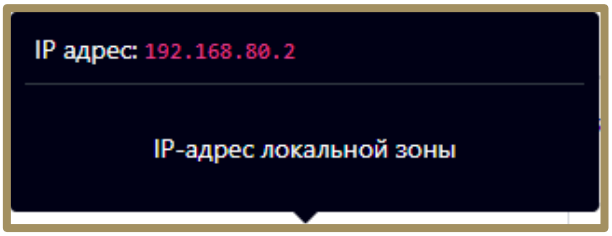


Рисунок 49 – Карточка TI-платформы для локального ip-адреса

При отсутствии в базе TI-платформы информации о выбранном артефакте или недоступности платформы пользователю выводится сообщение, представленное на рисунке 50.

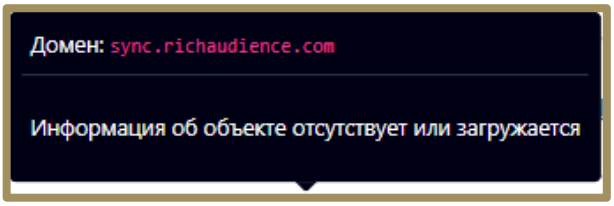


Рисунок 50 – Информация TI-платформы недоступна

В столбце **Информация** таблицы с событиями на странице **Активность** показывается соответствующая информация:

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 событие входит в инцидент), является ссылкой для перехода на страницу;

4) Инцидент (отображается имя инцидента, если событие на странице **Активность** входит в этот инцидент), имя инцидента является ссылкой и позволяет перейти на страницу **Инцидент**;

5) Кнопка **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 в представлении **По умолчанию** состоит из следующих полей:

1) **Показывать по**;

2) **Группа**;

3) **Источник события**;

4) **Период регистрации (на сервере)**;

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) Защита Файлов;

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 (на сервере) – задается параметр, который указывает на интервал времени для регистрации событий. В таблице отображаются только те события, которые происходили в данном интервале времени. Доступно задание параметра из списка или с помощью календаря.

Для задания параметра из списка необходимо установить флаг **Список**, как показано на рисунке 51. Далее выбрать из открывшегося списка 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.

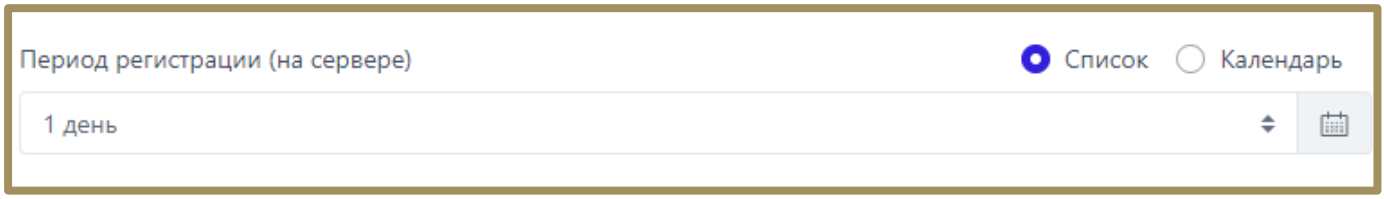


Рисунок 51 – Выбор периода регистрации события из списка

Для задания параметра из календаря следует установить флаг **Календарь**, как показано на рисунке 52. Далее необходимо нажать ЛКМ на пустое поле ввода и установить в открывшемся календаре год, месяц и дату для начального и конечного значений временного интервала, после чего нажать кнопку **Выбрать** (рис. 53).

Рисунок 52 – Выбор периода регистрации события в календаре

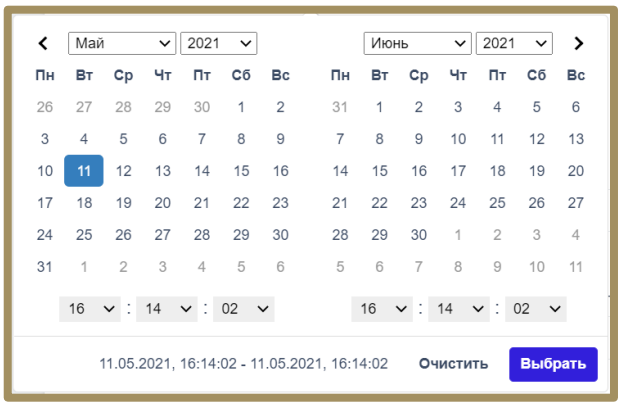


Рисунок 53 – Календарь для выбора периода регистрации событий

Значение выбранного временного интервала отобразится в поле **Период регистрации (на сервере).**

Для очистки установленного интервала необходимо нажать кнопку **Очистить.**

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) Отправка;

4) Прием;

5) DNS-запрос;

6) DNS-ответ;

7) Входящий DNS-запрос;

8) Исходящий DNS-ответ;

9) SSL HELLO;

10) Открытие локального порта на прием (LISTEN);

11) Сеть: Обнаружение: срабатывание сетевого исключения.

12) Обнаружение: срабатывание индикатора компрометации;

13) Другие обнаружения.

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.

В правой части строки фильтра над кнопкой Отправить содержатся примеры DSL-запросов (рис. 54).

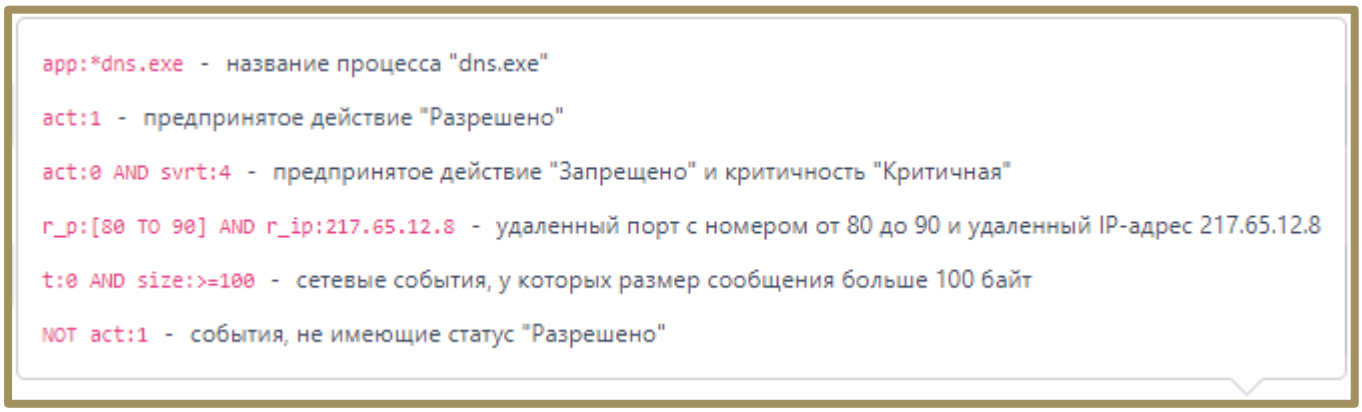


Рисунок 54 – Примеры DSL-запросов

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. 55), необходимо выбрать операцию **Новый.**

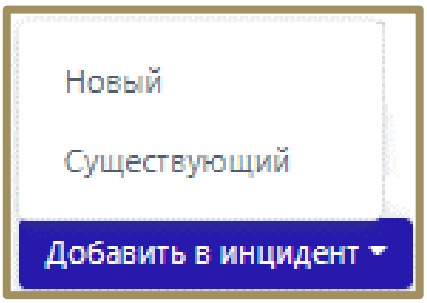


Рисунок 55 – Список операций с событиями на странице «Активность»

В результате выполнения операции откроется окно **Добавление событий в новый инцидент** (рис. 56), 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.

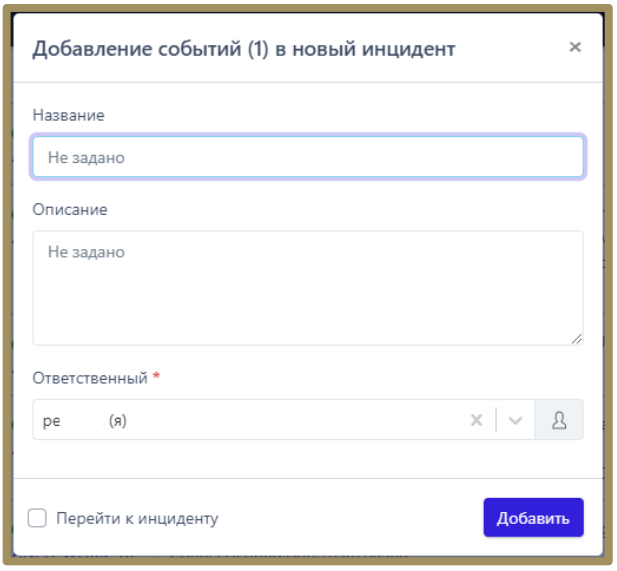


Рисунок 56 – Добавление событий в новый инцидент

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. 57), в котором в поле **Инцидент** необходимо выбрать существующий инцидент.

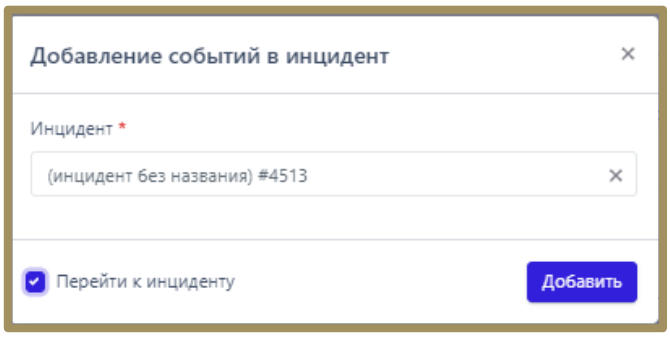


Рисунок 57 – Добавление события в существующий инцидент

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.**

Переходы к другим страницам из таблицы с событиями

В таблице событий можно перейти на другие страницы. При нажатии ЛКМ на имени группы агента в столбце **Группа/Имя агента** осуществляется переход на страницу **Группа** в раздел **Настройка Группы.** Подробная информация об этом разделе рассматривается в пункте 6.6.3. При нажатии ЛКМ на имени агента в столбце **Группа/Имя агента** осуществляется переход на страницу **Агент** в разделе **Настройка агента.** При нажатии ЛКМ на имени процесса в столбце **Процесс** в карточке события осуществляется переход на страницу **Процессы** (см. пункт 6.5.3).

6.5.3. 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);

2) Время обнаружения (когда артефакт обнаружен впервые);

3) Время загрузки файла на сервер;

4) Размер файла (опционально);

5) Хеш, рассчитанный по алгоритму SHA-256 (опционально);

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  . При нажатии кнопки формат отчета меняется на JSON-формат (рис. 58).

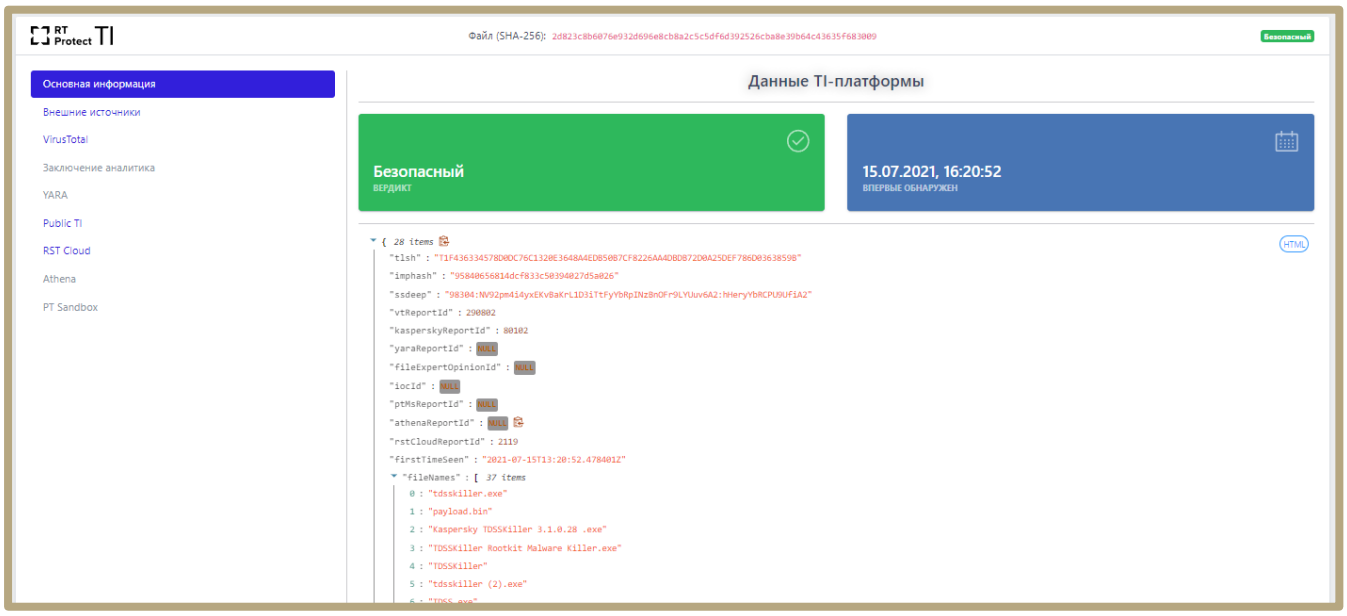


Рисунок 58 – Отчёт в JSON

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.

6.5.4. 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 **Процессы** переход осуществляется по ссылкам из разных полей таблиц с событиями на страницах разделов **Инциденты** и **Активность.** Чаще всего ссылка представлена названием процесса или значением универсального уникального идентификатора (UUID). Ссылки в Программе отображаются синим цветом, для перехода необходимо нажать ЛКМ на выбранную ссылку. 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 (рис. 59).

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**.

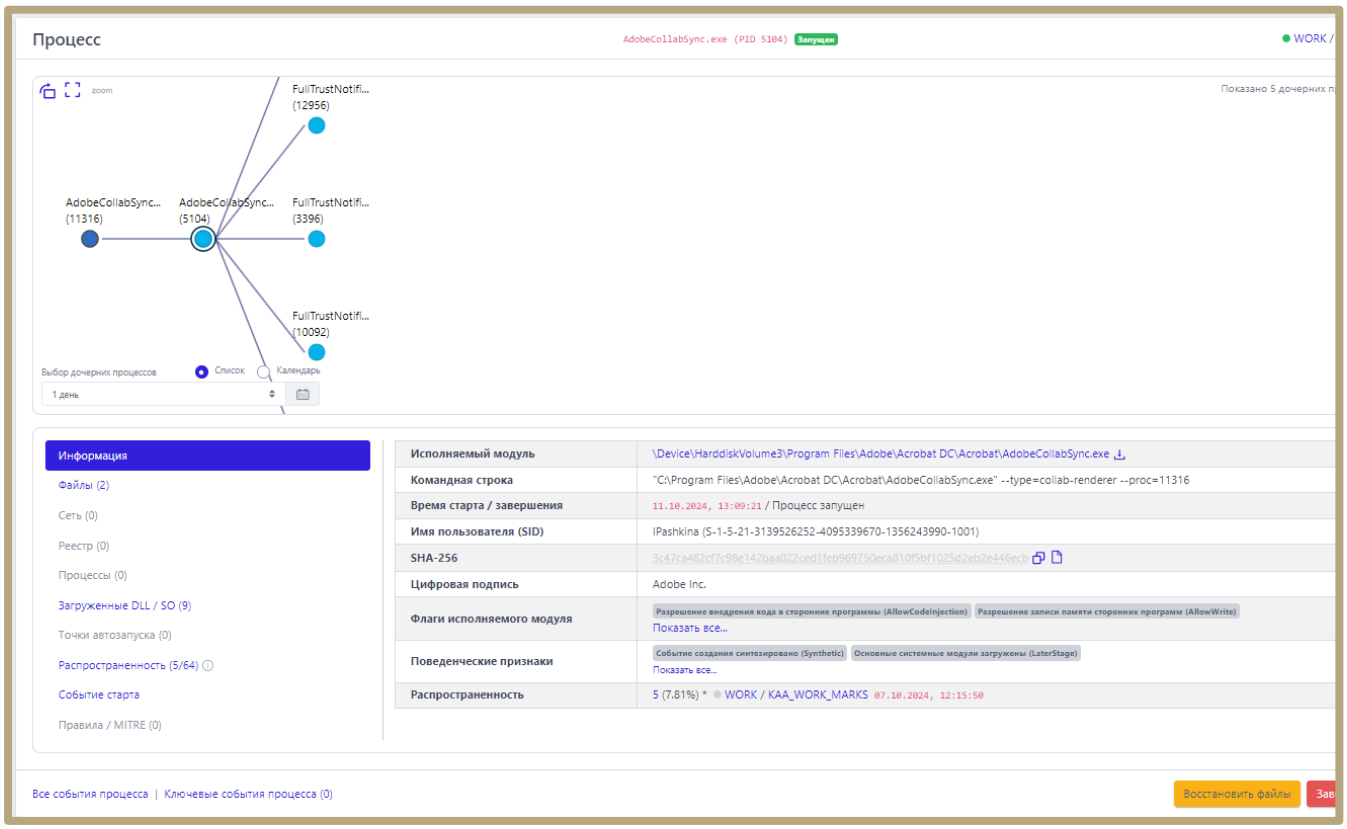


Рисунок 59 – Информация о процессе

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. Рядом с кнопкой загрузки находится информационная строка, в которой показывается общее количество выводимых в область отображения процессов (Показано 5 дочерних процессов из 80).

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. Значок изменится на , а снизу области дерева процессов отобразится таблица с

вкладками. 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, ). После завершения загрузки информации рядом с названием вкладки отобразится количество элементов, на которые так или иначе повлиял процесс, выбранный ранее (к примеру, ).

В таблице отображаются следующие вкладки:

1) Информация;

2) Файлы;

3) Сеть;

4) Реестр;

5) Процессы;

6) Загруженные DLL/SO (для процесса **%SYSTEM%** вместо загруженных DLL будут указаны загруженные модули ядра);

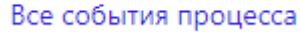
7) Точки автозапуска;

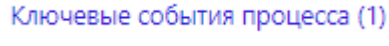
8) Распространенность;

9) Событие старта;

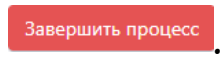
10) Правила/MITRE.

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

1)  ;

2)  ;

3)  ;

4)  .

Все события процесса – при нажатии кнопки 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 6.5.2.

Ключевые события процесса – при нажатии кнопки Ключевые события процесса (1) происходит переход на страницу **Активность,** на которой отображаются важные события (индикаторы, или события с уровнем критичности от уровня **Низкая** и выше), связанные с процессом. При этом отображаемые события должны подчиняться логике DSL-запроса, указанного в строке **Запрос на языке DSL** (рис. 60).

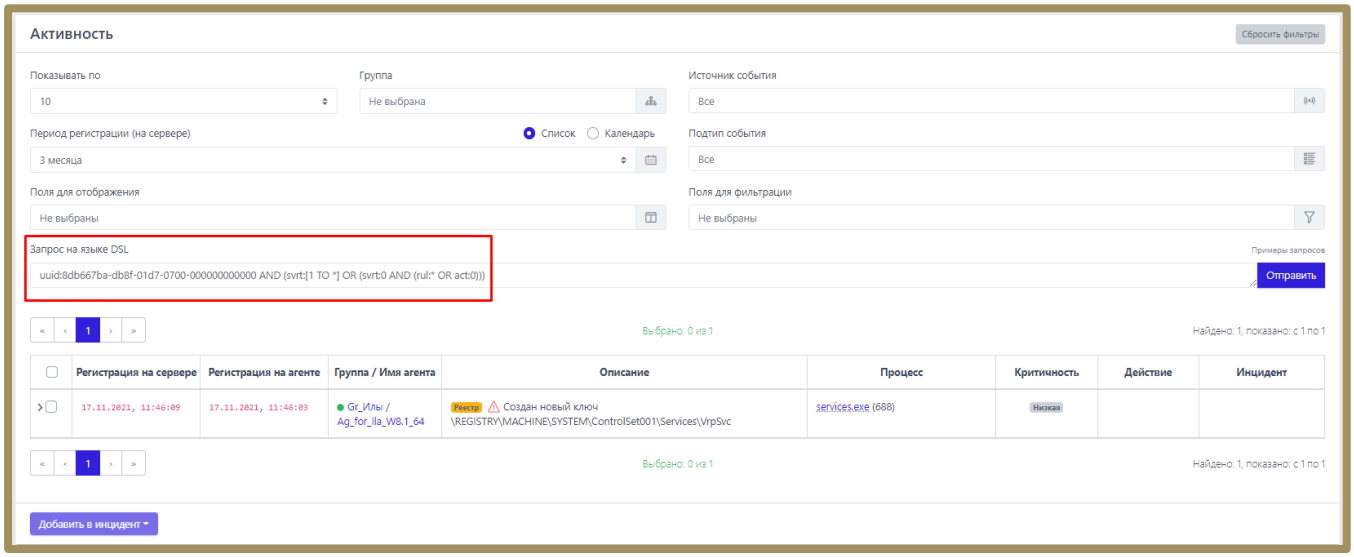


Рисунок 60 – Ключевые события процесса

Восстановить файлы – кнопка позволяет восстановить файлы, затронутые вредоносным процессом, если эти файлы были зарезервированы Программой.

Завершить процесс – кнопка позволяет быстро остановить вредоносную активность процесса. Кнопка активна, если процесс находится в состоянии Запущен.

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) Цифровая подпись;

7) Флаги исполняемого модуля;

8) Поведенческие признаки;

9) Распространенность.

Исполняемый модуль – в поле отображается имя модуля исполняемого файла, инициировавшего запуск процесса. Рядом с именем находится значок загрузки модуля в файловое хранилище для проведения дополнительного анализа (см. пункт 6.6.8).

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 ( ).

Цифровая 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.

Распространенность – в поле отображается, на каком количестве агентов был обнаружен процесс, кроме того просчитано процентное соотношение таких агентов к их общему количеству. Помимо этого, показан агент, на котором процесс был обнаружен впервые.

Вкладка «Файлы»

В таблице вкладки **Файлы** отображается информация о файлах, с которыми связан рассматриваемый процесс (рис. 61).

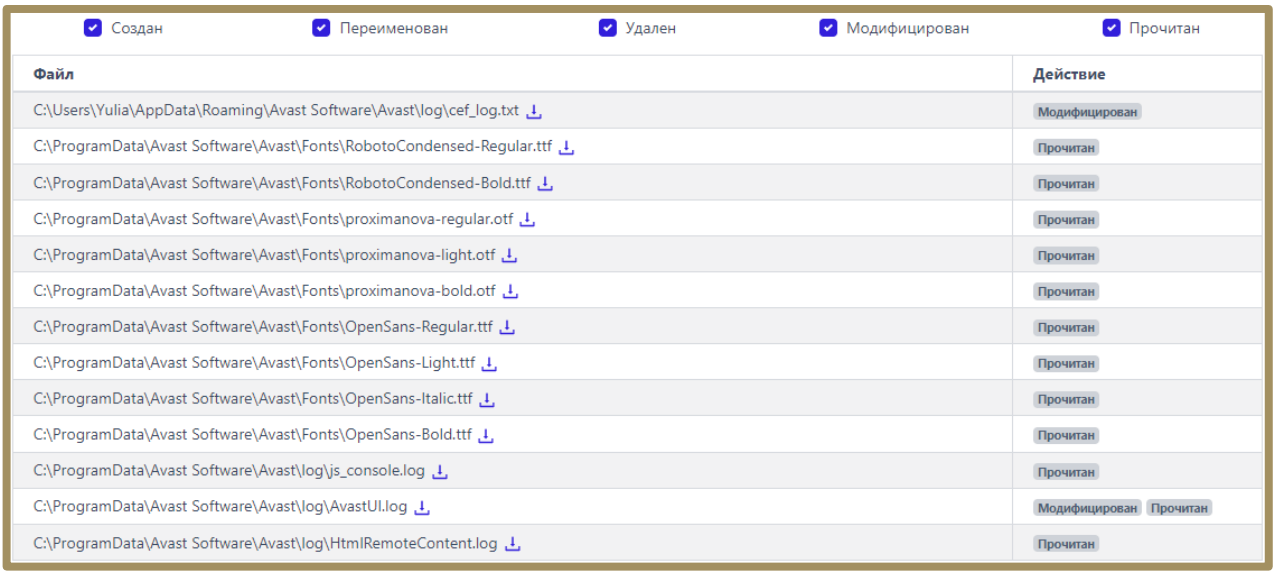


Рисунок 61 – Информация о файлах процесса

Для фильтрации файлов предусмотрена система флажков Создан Модифицирован Прочитан Переименован Удален. 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. 62).

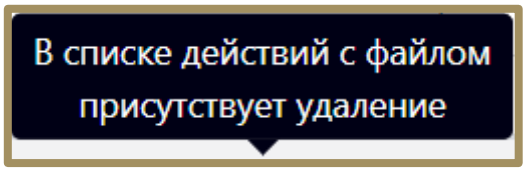


Рисунок 62 – Сообщение о присутствии в списке удаления файла

Вкладка «Сеть»

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

1) Входящие подключения;

2) Исходящие подключения;

3) DNS-запросы.

Информация о сетевых подключениях представлена в табличном виде. Таблица для каждого типа подключения включает в себя следующие поля:

1) IP-адрес;

2) Имя хоста;

3) Удаленный порт;

4) Протокол;

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.

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. 63).

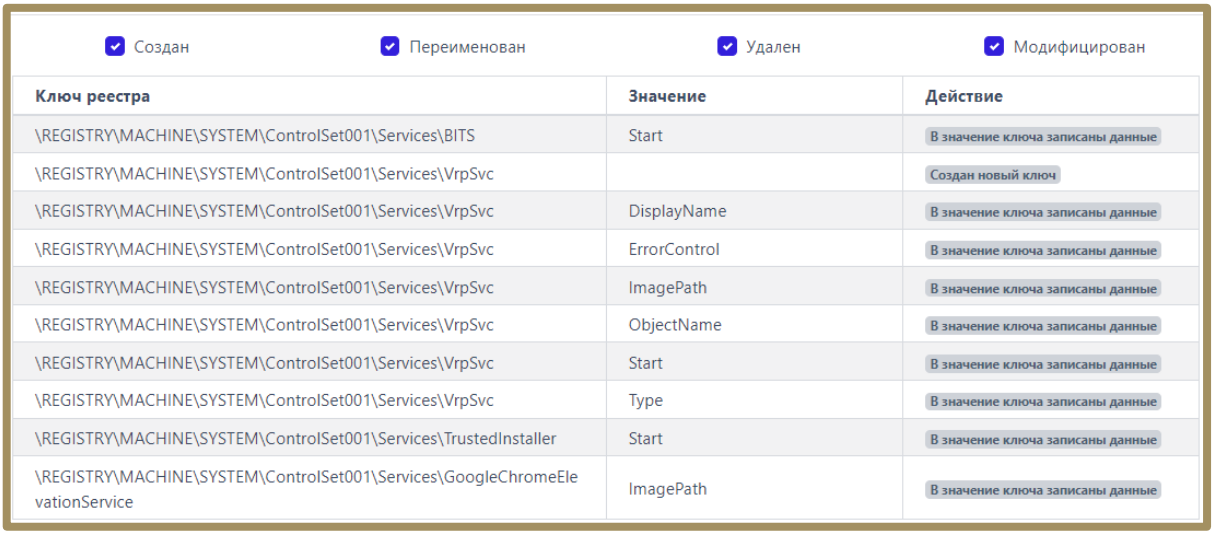


Рисунок 63 – Ключи реестра, на которые действовал процесс

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.

Вкладка «Процессы»

Во вкладке **Процессы** 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**;

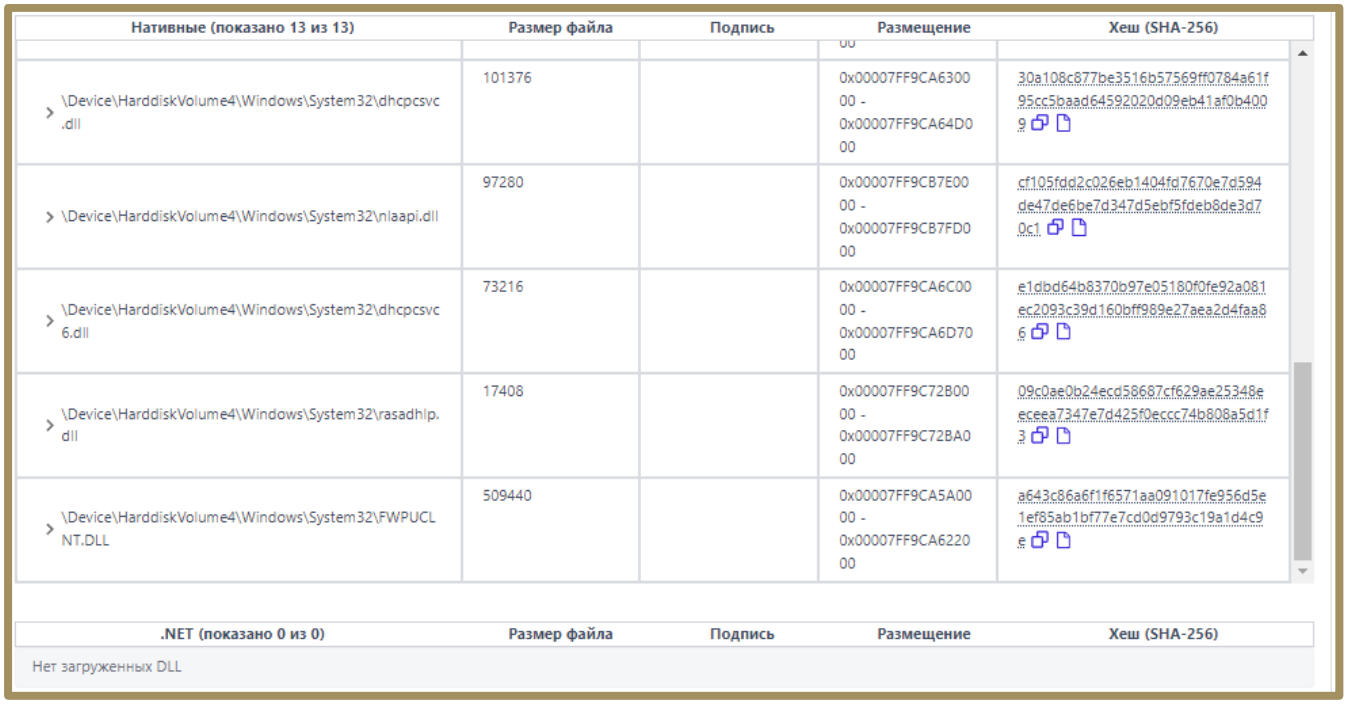
4) **Кол-во событий**.

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. 64).



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	09c0ae0b24ecd58687cf629ae25348eeceea7347e7d425f0eccc74b808a5d1f3
\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 64 – 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 6.9.2.

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 ( ), которое 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. 65)

Время первой регистрации	Группа/агент	Путь до исполняемого файла
17.11.2021, 19:40:18	WORK / MAXP_10	\Device\HarddiskVolume3\Windows\System32\cmd.exe
17.11.2021, 19:56:35	WORK / ROMAN-PC	\Device\HarddiskVolume6\Windows\System32\cmd.exe

Рисунок 65 – Вкладка «Распространенность»

Вкладка «Событие старта»

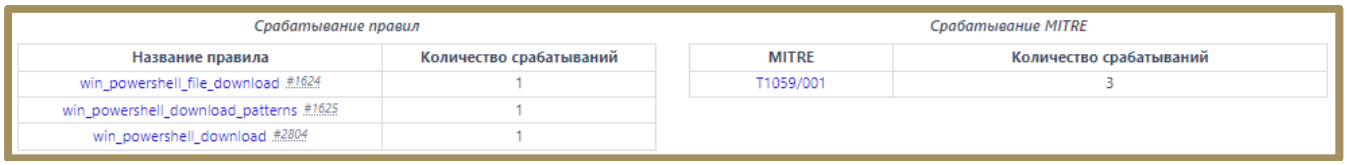
Во вкладке **Событие старта** показана карточка события для старта процесса (рис. 66).

Время регистрации на сервере	09.06.2023, 13:17:01
Время регистрации на агенте	09.06.2023, 13:16:58
Тип события	Процессы
Подтип события	Старт процесса
Критичность (уровень важности) события	Информация
Агент	A[redacted]PC
Уникальный идентификатор агента	9efed3a1f77e18813b5b340f8adfe6e4c25c254978
Платформа	Windows
Полное имя исполняемого модуля процесса	\Device\HarddiskVolume4\Windows\System32\cmd.exe
Идентификатор процесса на агентской системе	17164
Идентификатор родительского процесса на агентской системе	4448

Рисунок 66 – 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. 67).



Срабатывание правил

Название правила	Количество срабатываний
win_powershell_file_download #1624	1
win_powershell_download_patterns #1625	1
win_powershell_download #2804	1

Срабатывание MITRE

MITRE	Количество срабатываний
T1059/001	3

Рисунок 67 – Правила/MITRE

6.5.5. Процессы и модули

На странице **Процессы и модули** пользователь может оценить распространенность программы (модуля) в агентской сети, а также узнать вердикт TI-платформы по этой программе. Распространённость программы показывает, на каких агентах появлялся файл с определенной хеш-суммой.

Пользователь может искать нужную программу с помощью фильтров:

1) **Показывать по** (10, 20, 50, 100 строк в таблице);

2) **Платформа** (Windows или Linux);

3) **Имя модуля** (требуется ввести имя модуля полностью);

4) **Подпись**;

5) **Тип подписи**;

6) **Хеш модуля (SHA-256)**;

7) **Период регистрации на сервере** (можно выбрать в списке или календаре).

Вердикт TI-платформы открывается, если пользователь нажмет поле с хеш-суммой. 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 ›.

В таблице с основной информацией о программе отображаются следующие поля:

1) Время регистрации старта процесса на сервере;

2) Время регистрации старта процесса на агенте;

3) На каком агенте программа была обнаружена впервые;

4) Хеш программы;

5) Имя файла (имя программы);

6) Электронная подпись;

7) Число агентов, на которых была обнаружена программа;

8) Распространение программы (в процентах от общего числа агентов).

6.6 Агенты

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

1) Агенты;

2) Группы;

3) Верификация;

4) Терминал;

5) Графики;

6) Хранилище;

7) 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 **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 **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.

6.6.1. Агенты

Общая информация

На странице **Агенты** в табличном виде представлена информация об агентах, зарегистрированных в Программе, и поля фильтрации для поиска и сортировки агентов по значениям фильтров.

Работа с таблицей просмотра агентов и фильтрами, отображение общего количества элементов в таблице, отображение выбранных элементов идентичны описанным в разделах **Активность** и **Инциденты** (см. пункты 6.5.1 и 6.5.2).

Страница **Агенты** представлена на рисунке 68.

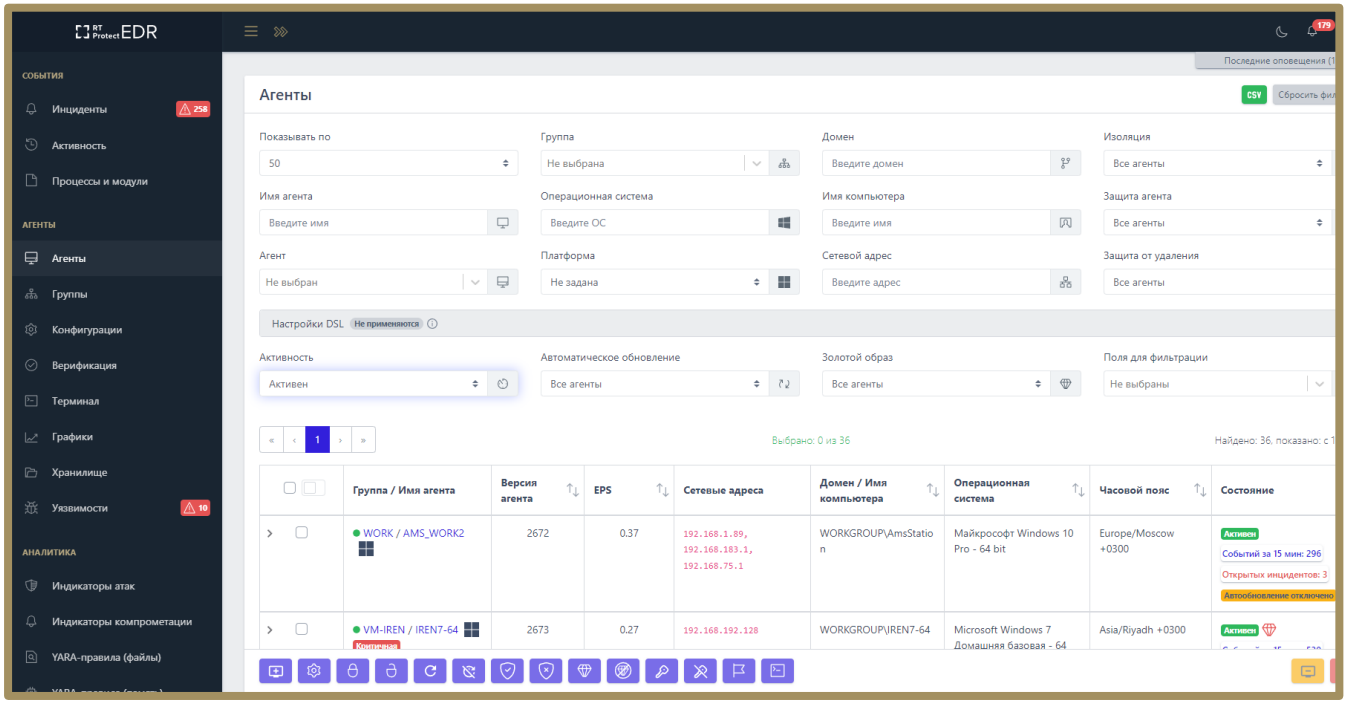


Рисунок 68 – Страница «Агенты»

Поля фильтрации на странице «Агенты»

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

1) **Показывать по;**

2) **Группа;**

3) **Домен;**

4) **Изоляция;**

5) **Имя агента;**

6) **Операционная система;**

7) **Имя компьютера;**

8) **Защита агента;**

9) **Агент;**

10) **Платформа;**

11) **Сетевой адрес;**

12) **Защита от удаления;**

13) **Активность;**

14) **Автоматическое обновление;**

15) **Золотой образ;**

16) **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) **Настройки;**

5) **Поля с конфигурациями** (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.

При вводе DSL-запросов создается выборка над базой событий, из которой делается агрегация агентов, подлежащих отображению. Например, DSL-запрос «sha256:x» выводит список агентов, имеющих события с указанным хешем x (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 соответствующей фильтрацией по имени агента, DSL-запросом, а также трехмесячным периодом регистрации события.

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

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

Имя агента – фильтрует агентов по имени, которое было присвоено им при регистрации в Программе.

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

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

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

Часовой пояс – фильтрует агентов по определенному часовому поясу в различных форматах часовых поясов: EST, GMT, UTC и др.

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

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

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

Настройки – при выборе одного из значений фильтра (**Не задано**/**Есть нестандартные**/**Только стандартные**) в таблице **Агентов** будут представлены агенты, соответствующие выбранному значению.

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

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

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

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

Период регистрации (на сервере) – фильтрует агентов в соответствии с указанным периодом времени (15 минут, 1 час, 8 часов, 1 день, 1 неделя, 1 месяц, 3 месяца) событий, происходивших на тех или иных агентах. Можно выбрать период фильтрации в календаре.

Поля для фильтрации – при выборе значений в фильтре **Поля для фильтрации** на страницу дополнительно могут быть добавлены следующие фильтры: **Исключения для файлов**, **Исключения для программ**, **Индикаторы компрометации**, **Журналы Windows**, **YARA-правила**, **Индикаторы атак**, **Профили защиты данных**, **Профили безопасности агента**.

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 6.8.

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 6.8.1.

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 6.7.1.

Журналы Windows – фильтрует агентов по названию выбранного в поле фильтра набора журналов Windows. В таблице будут представлены только

агенты, привязанные к этому набору. Подробная информация о журналах Windows содержится в пункте 6.7.4.

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. Подробная информация о **YARA-правилах** и соответствующих им файловых сигнатурах содержится в пункте 6.7.3.

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 6.7.1.

Профили защиты данных – фильтрует агентов по названию выбранного в поле фильтра профиля защиты данных.

В таблице будут представлены только агенты, привязанные к этому профилю. Подробная информация о профилях защиты данных содержится в пункте 6.9.1.

Профили безопасности агента – фильтрует агентов по названию выбранного в поле фильтра профиля безопасности агента. В таблице будут представлены только агенты, привязанные к этому профилю. Подробная информация о профилях защиты данных содержится в пункте 6.9.2.

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.). Защиту агента при выключенном драйвере также, как и изоляцию, невозможно включить.

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.

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

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;
3) Версия;
4) Токен;
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;

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 Windows;

6) Исключения для программ;

7) Исключения для файлов;

8) Сетевые исключения;

9) Исключения для индикаторов атак;

10) Профиль безопасности агента;

11) Профиль защиты данных;

12) Профиль контроля USB.

ID Агента – в поле показан набор символов, идентифицирующий агента на сервере.

Имя – имя агента, присвоенное ему администратором во время регистрации агента в Программе.

Версия – в поле показана актуальная версия установленного дистрибутива агента.

Токен – в поле показывается часть ключа, присвоенного агенту для верификации с помощью этого ключа на сервере.

Верификация – в поле отображается информация о том, верифицирован или не верифицирован агент.

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 

. 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 кнопку перехода к терминалу , для работы в командной строке с компьютером, на котором установлен агент. При нажатии кнопки происходит переход на страницу **Терминал**.

Описание – поле содержит произвольное описание агента.

Индикаторы атак – в поле отображается название набора индикаторов атак, к которому привязан агент. При нажатии ЛКМ на названии набора происходит переход на страницу **Наборы индикаторов атак** в разделе **Индикаторы атак**.

Индикаторы компрометации – в поле отображается название набора индикаторов компрометации, к которому привязан агент. При нажатии ЛКМ на названии набора происходит переход на страницу **Наборы индикаторов компрометации** в разделе **Индикаторы компрометации**.

YARA-правила – в поле отображается название набора YARA-правил, к которому привязан агент. При нажатии ЛКМ на названии набора происходит переход на страницу **Наборы YARA-правил** в разделе **YARA-правила**.

Журналы Windows – в поле отображается название набора журналов Windows, к которому привязан агент. При нажатии ЛКМ на названии набора происходит переход на страницу **Журналы Windows**.

Исключения для программ – в поле отображается название набора исключений для программ, к которому привязан агент. При нажатии ЛКМ на названии набора происходит переход на страницу **Исключения для программ** в одноименном разделе.

Исключения для файлов – в поле отображается название набора исключений для файлов, к которому привязан агент. При нажатии ЛКМ на названии набора происходит переход на страницу **Исключения для файлов** в одноименном разделе.

Профиль защиты данных – в поле отображается название профиля защиты данных, к которому привязан агент. При нажатии ЛКМ на названии профиля происходит переход на страницу профиля.

Профиль безопасности агента – в поле отображается профиль безопасности, к которому привязан агент. При нажатии ЛКМ на названии профиля происходит переход на страницу этого профиля.

Операции с агентами

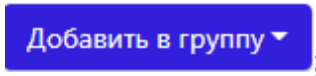
На странице **Агенты** администратор может выполнять различные групповые действия с произвольным количеством агентов. Информация об

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) 

;

2) Применить конфигурацию –  ;

3) Изолировать выбранных агентов –  ;

4) Отменить изоляцию выбранных агентов –  ;

5) Включить автоматическое обновление выбранных агентов –  ;

6) Отключить автоматическое обновление выбранных агентов –  ;

7) Включить защиту на выбранном агенте –  ;

8) Отключить защиту на выбранном агенте –  ;

9) Зафиксировать состав ПО выбранных агентов в качестве золотого образа –  ;

10) Отключить отслеживание состава ПО выбранных агентов золотому образу –  ;

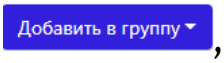
11) Включить защиту от удаления для выбранных агентов –  ;

12) Выключить защиту от удаления для выбранных агентов –  ;

13) Выполнить команду на выбранных агентах –  ;

14) Исключить выбранных агентов из своих групп –  ;

15) Удалить выбранных 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. 69).

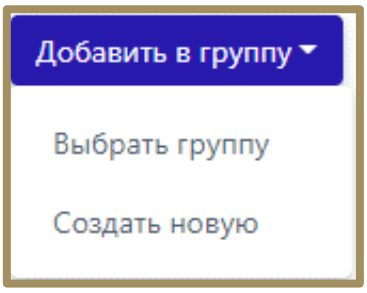
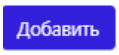


Рисунок 69 – Выбор операции с агентом

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. 70) и нажать кнопку  , после чего подтвердить действие.

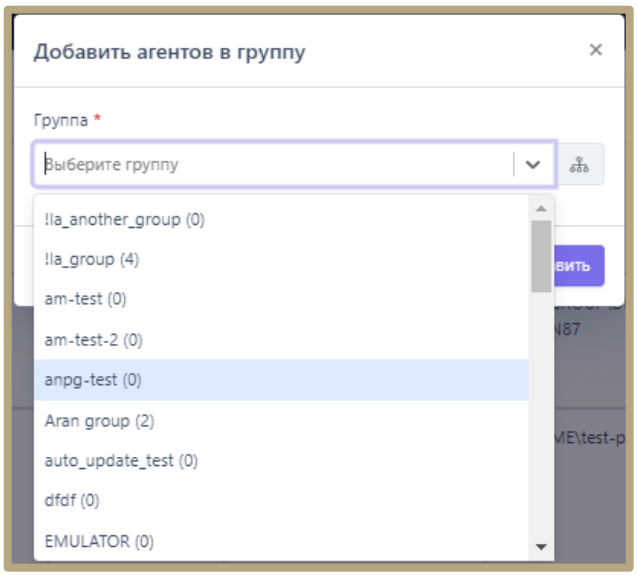


Рисунок 70 – Выбор группы из списка

Если необходимо добавить выбранных агентов во вновь создаваемую группу, то следует кликнуть по кнопке **Создать новую** (см. рис. 69), после чего в открывшемся окне ввести название в строке **Название группы** и нажать кнопку Создать.

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 **Выбор наборов**, в котором можно назначить наборы с правилами, исключениями и профилями для отмеченных агентов.

После завершения выбора необходимо нажать кнопку **Сохранить**.

После завершения операции для отмеченных агентов в столбце **Конфигурация** будут показаны новые привязанные наборы, информация о примененных наборах по умолчанию не отображается, за исключением случая, когда все наборы, примененные для агента, являются наборами по умолчанию.

Изолировать/отменить изоляцию агентов – чтобы изолировать одного или нескольких агентов, необходимо отметить их флажками, после чего нажать

кнопку  , далее ввести комментарий в открывшемся окне **Переход к изоляции агентов** и нажать кнопку **Отправить.** Для отмены изоляции необходимо отметить изолированных агентов флажками, после чего нажать кнопку  . Далее подтвердить действия в открывшемся окне, нажав кнопку **Выполнить.**

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 токена 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 (токен удаления), необходимо перейти на страницу удаляемого агента. Токен 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.

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  , после чего будет открыто окно, представленное на рисунке 71.

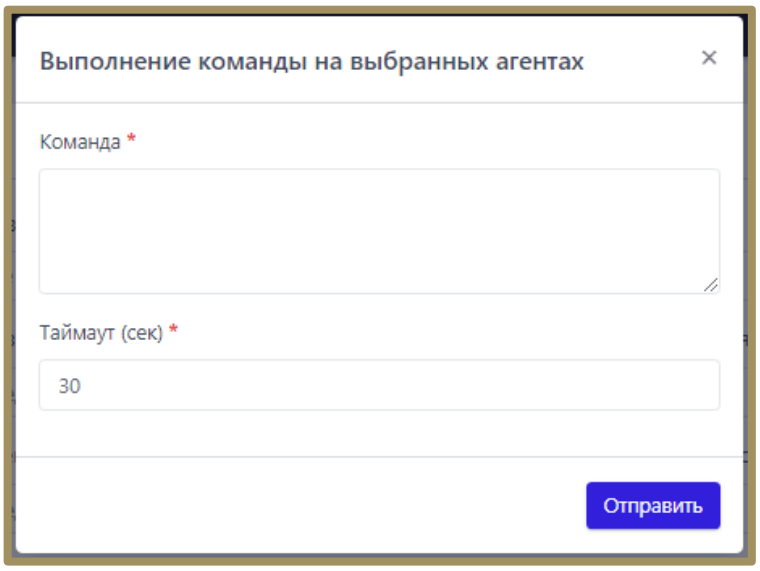


Рисунок 71 – Окно ввода команд

После ввода команды необходимо нажать кнопку **Отправить**. Список команд аналогичен командам, описанным в разделе 6.6.6.

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 CSV. 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.

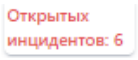
В файле будет присутствовать информация о тех агентах, которые отсортированы на странице **Агенты** в зависимости от выставленных фильтров, либо будет информация обо всех агентах, если фильтры отсутствуют.

Переходы к другим страницам из таблицы с агентами

Часть элементов в таблице выполняет функцию гиперссылки к другим страницам. Для перехода к странице выбранного агента необходимо нажать ЛКМ на названии агента в столбце **Группа/Имя агента**. Для перехода к странице выбранной группы следует нажать ЛКМ на названии группы агентов в столбце **Группа/Имя агента**.

При наличии событий для определенного агента в поле **Состояние** будет отображаться ссылка на события за последние пятнадцать минут 

. Для перехода к странице **Активность** и просмотра событий необходимо нажать ЛКМ на ссылку. Подробную информацию о странице **Активность** можно просмотреть в пункте 6.5.2.

При наличии инцидентов для определенного агента в поле **Состояние** будет отображаться количество инцидентов. Для перехода к странице **Инциденты** для просмотра этих событий следует нажать ЛКМ на ссылку 

. Подробную информацию о странице **Инциденты** можно просмотреть в пункте 6.5.1.

Если к агенту привязан конфигурационный набор не по умолчанию, то в поле **Конфигурация** отобразится ссылка с названием этого набора. При нажатии ссылки выполняется переход к странице, соответствующей конфигурации набора. Например, при нажатии ЛКМ на названии набора YARA-правил произойдет переход к странице данного набора в разделе **YARA-правила**.

6.6.2. Агент

Для перехода на страницу **Агент** требуется кликнуть по имени агента. 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) Конфигурации;

4) Информация о системе;

5) Программное обеспечение;

6) Описание;

7) Журнал агента;

8) 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**.

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) Изменить имя агента;

2) Установить настройку обновления дистрибутива агента (автоматическое или вручную);

3) Узнать информацию об идентификаторе агента, при необходимости скопировать его;

4) Узнать информацию о часовом поясе агента;

5) Узнать информацию об установленной версии агента;

6) Узнать информацию об активности агента;

7) Узнать наименование ОС, на которой установлен агент;

8) Узнать время установки агента;

9) Узнать время последней верификации агента;

10) Узнать время последнего обновления конфигурации агента;

11) Узнать время обновления агента;

12) Узнать информацию о пяти последних пользователях, вошедших локально или дистанционно на компьютер с установленным агентом (кроме того, показывается и время входа);

13) Просмотреть количество программ с уязвимостями;

14) Удалить агента с сервера управления (после удаления агент автоматически отправится на верификацию).

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 (рис. 72).

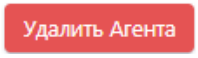
Рисунок 72 – Предупреждение о несоответствии настройкам часового пояса

Здесь же находится кнопка для создания отчета по агенту в формате pdf (PDF). При нажатии кнопки отчет сохраняется в папке **Загрузки** компьютера, с которого осуществлен доступ на сервер 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.

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 

и подтвердить действие.

Область «Управление»

В области **Управление** пользователь может выполнить следующие операции:

1) Изолировать агента или снять с него изоляцию;

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) Перейти на страницу **Терминал** выбранного агента;

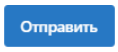
7) Настроить параметры получения информации о программах, установленных на агентах (золотой образ);

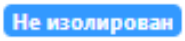
8) Включить или отключить на агенте защиту от удаления с компьютера, на котором он установлен;

9) Просмотреть или скопировать в буфер обмена токен сгенерированный автоматически при установке агента с включенной опцией парольной защиты от удаления;

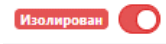
10) Добавить агента в группу;

11) Узнать значение EPS (количество событий в секунду) для выбранного агента в текущий момент и среднее EPS за последнюю неделю.

Изоляция – чтобы изолировать компьютер, на котором установлен агент, от остальной части вычислительной сети и оставить только ограниченную связь между машиной, на которой установлен агент, и сервером, необходимо в поле **Изоляция** нажать кнопку **Включить изоляцию** . Далее в открывшемся окне **Переход к изоляции** следует ввести комментарий для выбранного агента. Информация о технических аспектах процесса сетевой изоляции агента рассмотрена более подробно в документе «Руководство Аналитика RT Protect EDR» в пункте 10.6.1 «Изоляция Агента/ Описание механизма реализации функции сетевой изоляции со стороны агента». После ввода комментария в окне и нажатия кнопки 

режим 

будет изменен на режим 

. Изоляция агента происходит в течение 10 секунд, после чего статус агента в области **Управление** поменяется на 

. На машине агента в этот момент в области уведомлений пользователю придет сообщение о том, что сеть агента изолирована.

Для возврата в штатный режим необходимо нажать кнопку **Отменить изоляцию**  . Далее в открывшемся окне **Подтверждение действия** следует нажать кнопку 

, после чего в нижней части страницы появится сообщение об отправке команды на отмену изоляции. Для отмены операции необходимо нажать кнопку 

или кнопку закрытия окна  .

Отмена изоляции агента происходит в течение 10 секунд. За это время статус агента в области **Управление** поменяется на 

, после чего

агенту будет возвращен статус Не изолирован, а на машине агента в области уведомлений появится сообщение, что изоляция сети отменена.

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 **get** и **stop**.

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 6.5.2.

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 6.5.1.

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. 73).

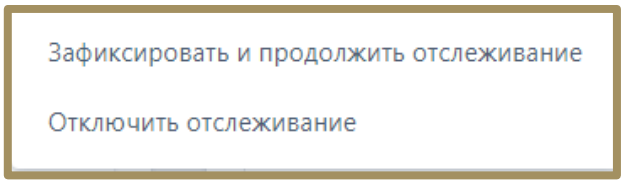


Рисунок 73 – Действия с золотым образом

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 **Консоль управления** пользователь может перейти к странице **Терминал** для выбранного агента, нажав кнопку Открыть. Для просмотра подробной информации о странице **Терминал** необходимо перейти в пункт 6.6.6.

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. Пароль вводится в окне, представленном на рисунке 74.

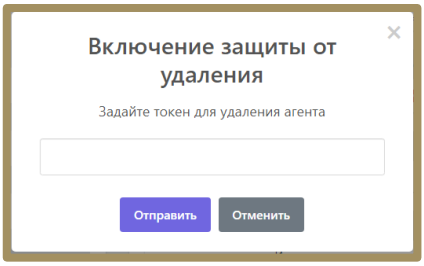


Рисунок 74 – Окно ввода пароля при включении функции защиты агента от удаления

После ввода пароля функция защиты от удаления будет включена, и пароль будет показан в строке **Токен удаления** при наведении курсора на значок . Его можно в любое время изменить с помощью значка . Нажатие на значок открывает окно **Изменение токена удаления**. Длина пароля (токена) не должна быть меньше шести символов.

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

добавления  . 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 Windows;

– применять к выбранному агенту определённый набор YARA-правил для файлов;

– применять к выбранному агенту определённый набор YARA-правил для памяти;

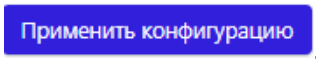
– применять к выбранному агенту определённый набор индикаторов атак;

– применять к выбранному агенту определённый профиль защиты данных;

– 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**.

Область «Описание»

В области **Описание** пользователь может произвольно описать характеристики, состояние, или особенности агента. Чтобы сохранить описание, пользователю необходимо нажать кнопку **Сохранить**.

Область «Журнал агента»

В области **Журнал 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.

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).

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.

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** ( ).

6.6.3. Группы

Общий вид страницы **Группы агентов** представлен на рисунке 75.

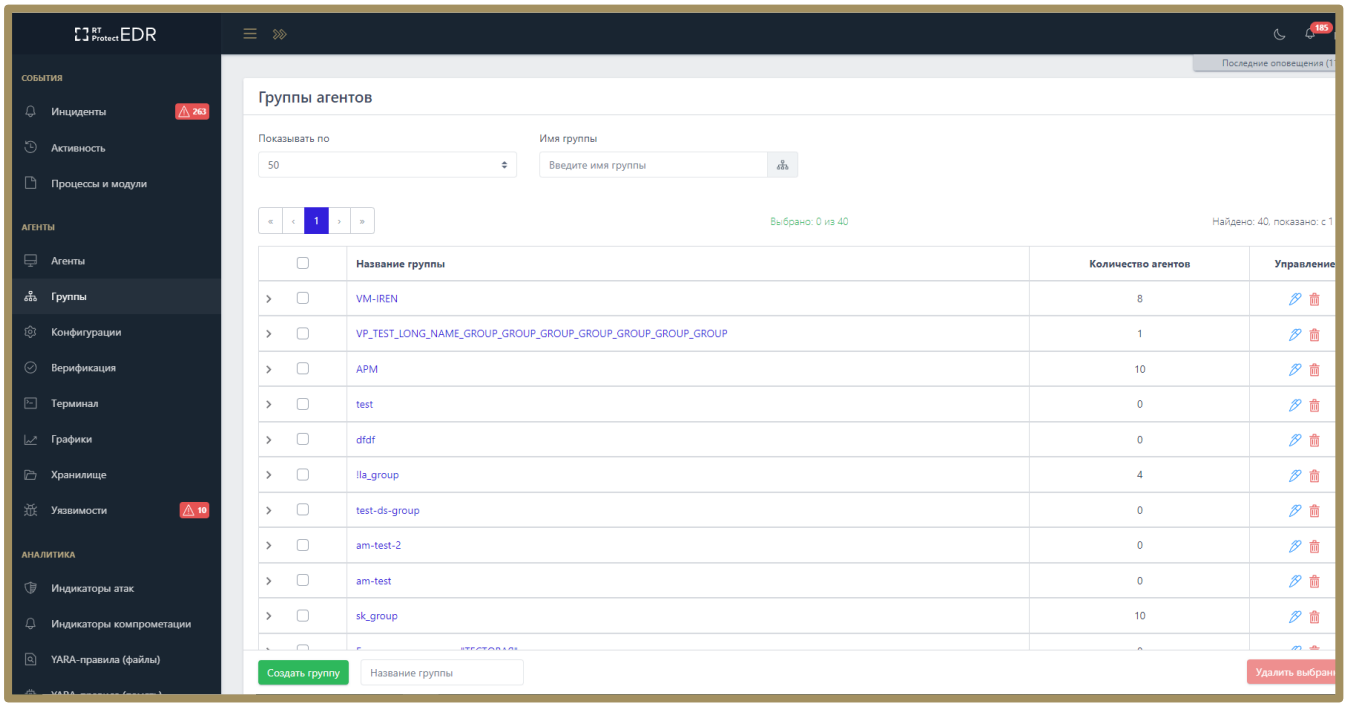


Рисунок 75 – Страница «Группы агентов»

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 Создать группу и Удалить выбранные. 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.

6.6.4. Конфигурации

Раздел **Конфигурации** содержит настройки наборов и профилей для агентов Windows и Linux, которые агенты получают в момент верификации.

Чтобы назначить выбранные конфигурации, необходимо нажать кнопку **Сохранить**.

6.6.5. 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).

Возможна ситуация, когда в списке агентов, ожидающих верификацию, появится агент, ранее верифицированный на сервере. Так происходит при восстановлении системы, на которой установлен агент, из снимка виртуальной машины. Эта ситуация не является критической и нужно повторно верифицировать агента.

Примечание

Сервер может работать только с агентами, «вручную» верифицированными администратором системы. При этом сервер на отдельной странице интерфейса всегда отображает список агентов, ожидающих верификации. Администратор может в любой момент верифицировать агента, и тот получит на свой очередной запрос верификации ответ с кодом 200 (OK).

Процедура верификации

При переходе на страницу **Верификация** администратор имеет возможность просмотреть всех не верифицированных агентов и произвести процедуру верификации. Если отсутствуют агенты, требующие верификации на сервере, то на странице отображается соответствующая запись (рис. 76).

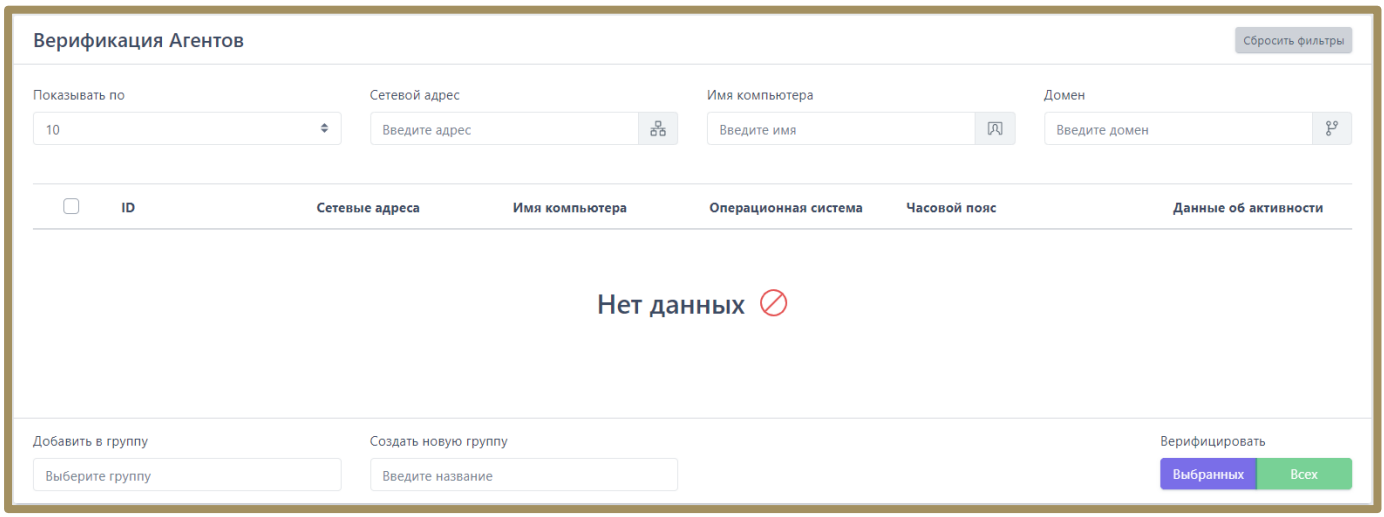


Рисунок 76 – Страница «Верификация» (нет верифицируемых агентов)

На рисунке 76 в таблице для отображаемых агентов отсутствуют агенты на верификацию, и в связи с этим присутствует надпись **Нет данных** ⊘.

При наличии агентов, требующих верификации, на странице будет представлена информация об этих агентах (рис. 77).

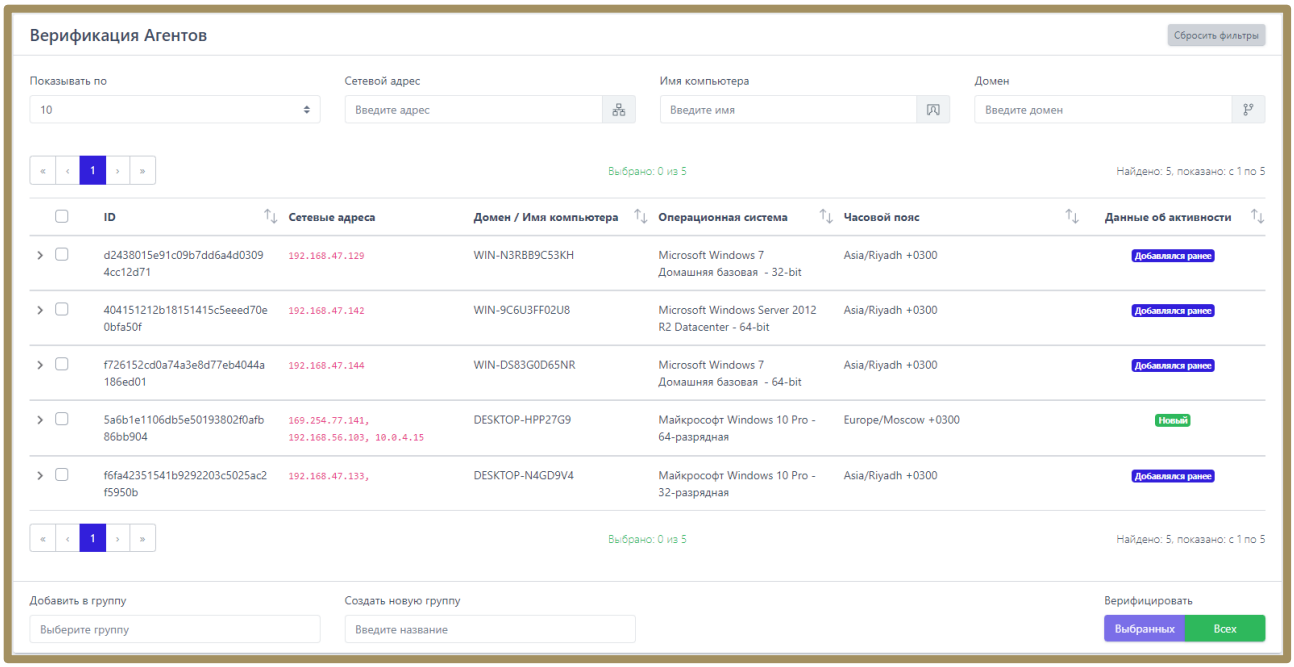


Рисунок 77 – Страница «Верификация» (есть верифицируемые агенты)

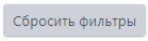
На странице представлены следующие поля фильтрации:

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 

. 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;

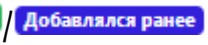
3) Сетевые адреса;

4) Домен/Имя компьютера;

5) Операционная система;

6) Часовой пояс;

7) Данные об активности (

/ 

).

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 6.2.1 (см. рис. 16).

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.

6.6.6. Терминал

Общая информация

Терминал является консолью управления, предназначенной для задания команд определенному агенту. Формат команд аналогичен формату средства автоматизации PowerShell. При переходе на страницу **Терминал** появится окно, представленное на рисунке 78.

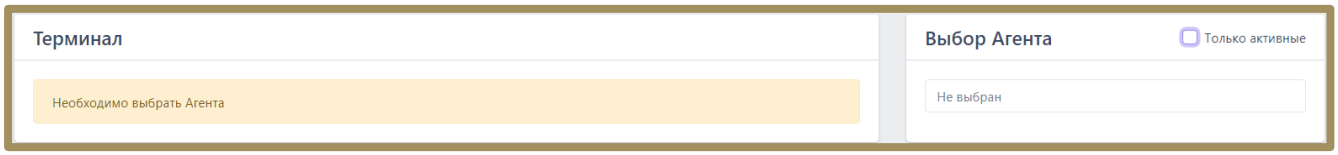


Рисунок 78 – Страница «Терминал»

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 Только активные .

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. 79).

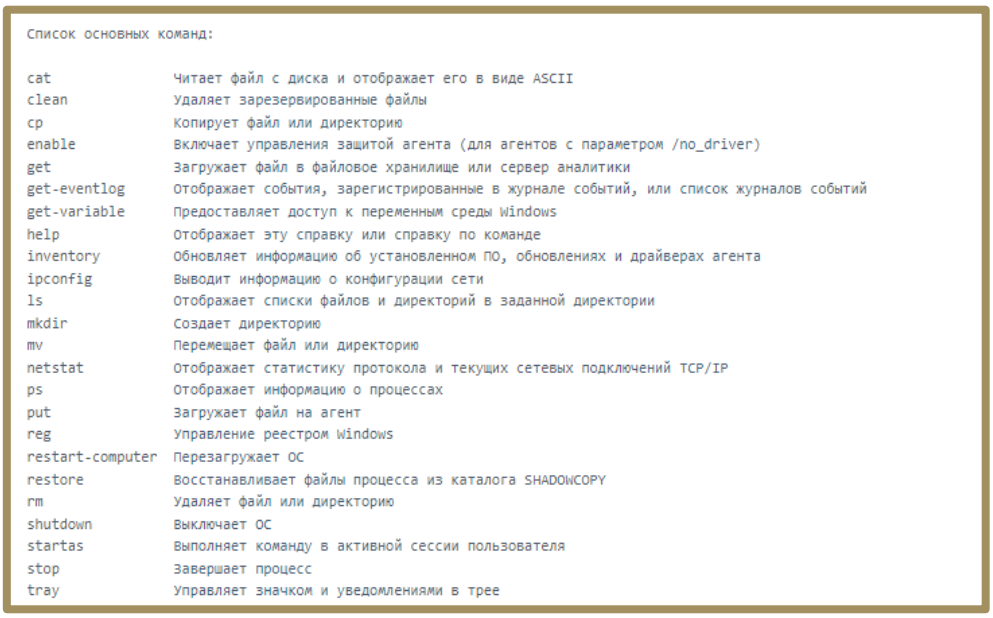


Рисунок 79 – Список основных команд терминала

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 Перейти вниз .

В нижней части области **Терминал** содержится кнопка Прервать, 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 Прервана (Ctrl-C), а через единицу времени, указанную в поле **Таймаут (сек)** статус поменяется на Прервана (таймаут).

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;

– off;

– enable;

– перезапуск службы агента;

– trace;

– memscan;

– memdump;

– netlimit.

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 защиты данных агента (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>], где:

-f – путь до файла;

-t – тип хранилища для загрузки файла (ti – TI-платформа, cloud – хранилище EDR, по умолчанию берется тип хранилища cloud).

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://192.168.113.7/api/storage/user/object/894a2551-1e14-4e38-9f44-432428017c06/first_aid_kit.exe;

2) Команда загрузки файла на машину с агентом по пути C:\Tools\file_ver_1.exe:

put https://192.168.113.7/api/storage/user/object/894a2551-1e14-4e38-9f44-432428017c06/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 управления параметром **off** – для изменения параметра off необходимо в терминале агента ввести след. команду:

New-ItemProperty -Path HKLM:\System\CurrentControlSet\Services\Vrpnt\Parameters -Name off -PropertyType DWord -Force -Value <Новое значение параметра off>.

Пример написания команды:

New-ItemProperty -Path HKLM:\System\CurrentControlSet\Services\Vrpnt\Parameters -Name off -PropertyType DWord -Force -Value 0x1F.

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;

[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 8.

Таблица 8 – 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
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

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

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.

6.6.7. 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 будет отображаться информация об этом агенте);

5) Поле **Выбор метрики** (при выборе новой метрики в графике будет отображаться информация, соответствующая этой метрике);

6) Поле **Выбора интервала** (при выборе нового интервала в графике будет отображаться информация, заданная этим интервалом времени).

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 80).

Для перехода на страницу **Активность** с событиями согласно временного интервала 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, нажать по иконке  .

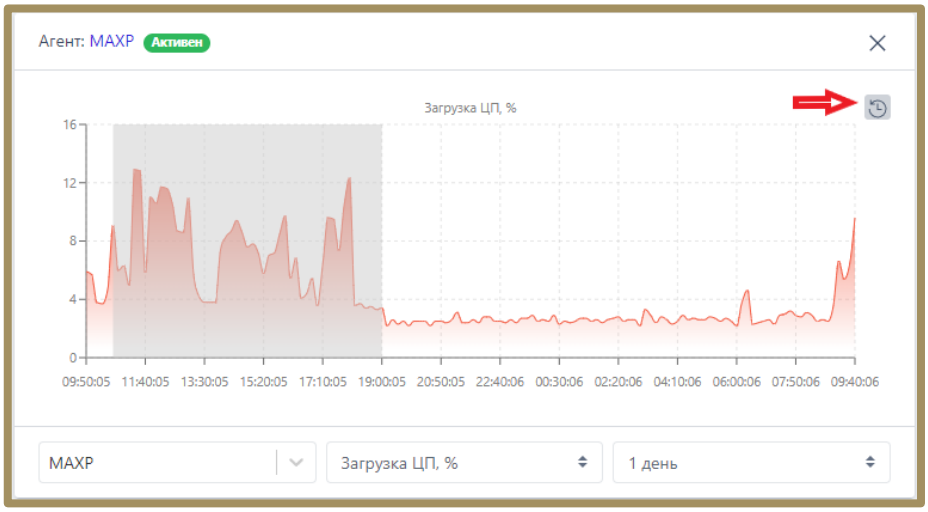


Рисунок 80 – Указание временного интервала для выборки событий из интервала на графике

6.6.8. Хранилище

Общая информация

На странице **Хранилище** отображаются все файлы, загруженные в файловое хранилище Программы (рис. 81). 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 в модуль администрирования. 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**.

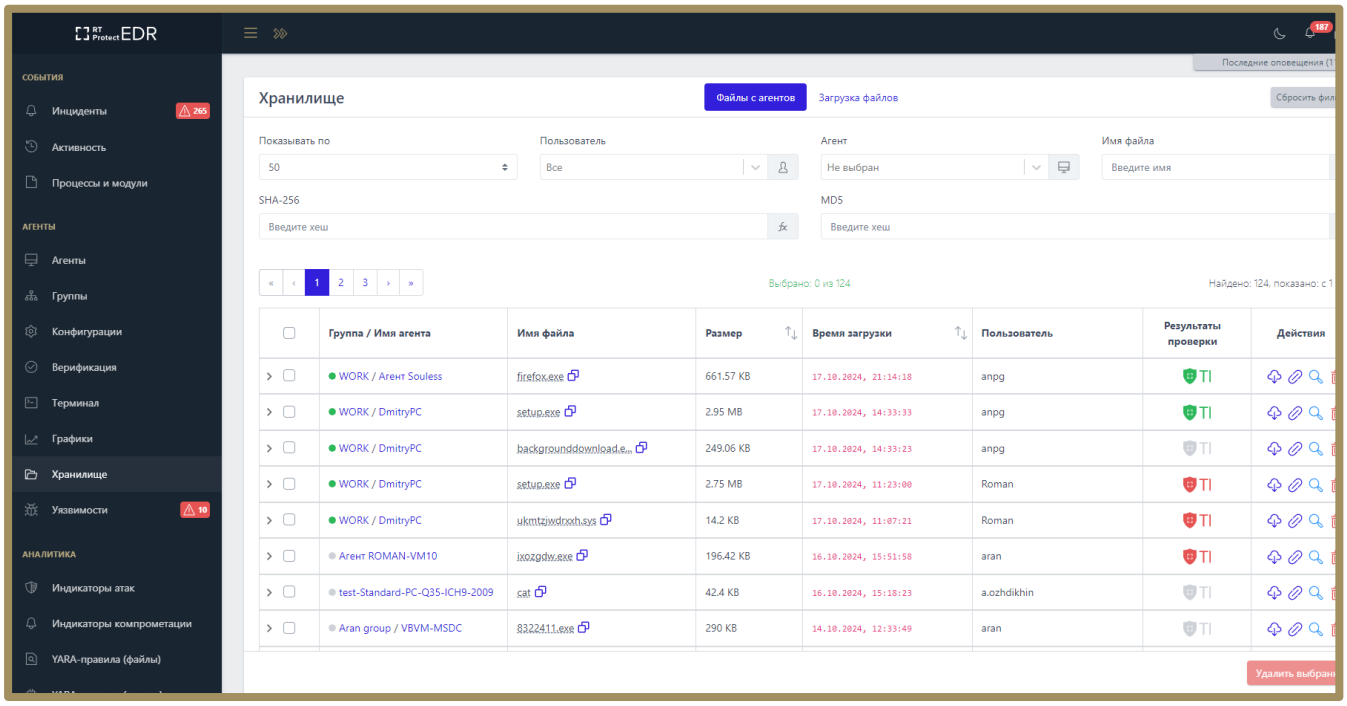


Рисунок 81 – Страница «Хранилище»

Информация о файлах, полученных от агента, представлена в табличном виде. Навигация (см. рисунок 16) и сортировка в таблице выполняются с помощью элементов, описанных ранее (см. пункт 6.5.2).

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.

Во вкладке **Загрузка файлов** присутствует тот же набор фильтров, за исключением фильтра **Агент**.

Шапка таблицы с загруженными файлами состоит из следующих полей:

1) Кнопка выбора (отмечена элементом ▢);

2) Группа/Имя агента;

3) Имя файла;

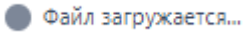
4) Размер;

5) Время загрузки;

6) Пользователь;

7) Действия.

Поля таблицы на вкладках **Файлы с агентов** и **Загрузка файлов** не отличаются.

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 

.

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 6.5.3). Кнопка со значком  обозначает безопасный файл, кнопка со значком  обозначает вредоносный файл, кнопка со значком  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 . 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.

Действие – в поле отображаются кнопки операций, выполняемых с загруженным файлом. Пользователю доступны операции **Просмотреть файл** и **Удалить файл**  , **Скачать файл**  , **Получить ссылку на скачивание**  .

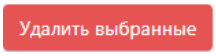
Кнопка **Просмотреть файл** открывает окно **Просмотр файла**. Кнопка **Удалить файл** удаляет загруженный файл с сервера.

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 находится кнопка 

. Для удаления одного или нескольких файлов необходимо отметить флажками соответствующие кнопки выбора для удаляемых файлов и нажать кнопку **Удалить выбранные**.

Загрузить файл в хранилище с компьютера, с которого осуществлен вход в модуль администрирования, можно во вкладке **Загрузка файлов**. Для этого необходимо нажать кнопку **Загрузить файл** внизу страницы и в открывшемся окне файлового проводника выбрать загружаемый элемент.

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. 82), необходимо нажать кнопку **Просмотреть файл** (🔍) в разделе **Хранилище**.

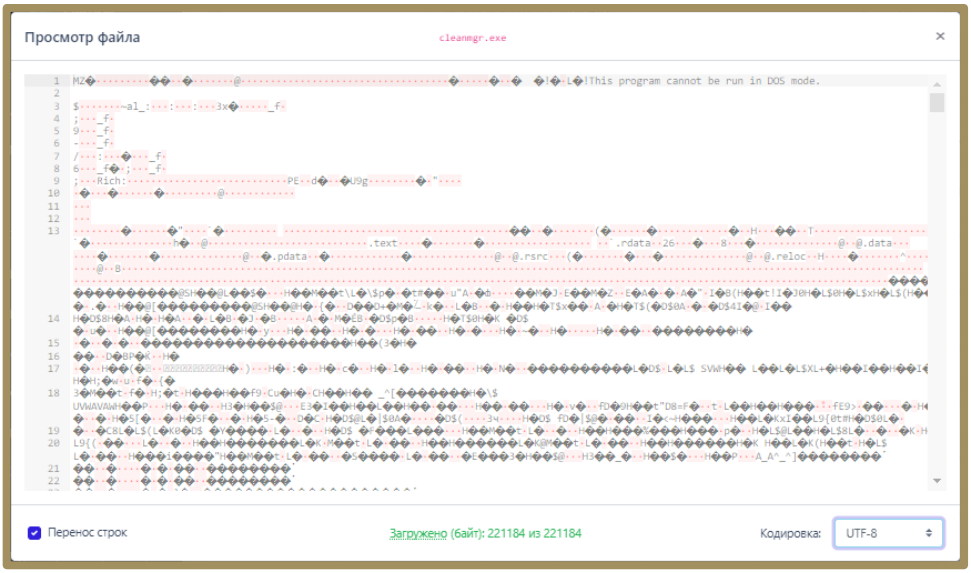


Рисунок 82 – Просмотр файла

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. 83).

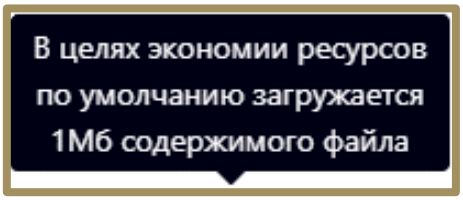


Рисунок 83 – Сообщение в окне «Просмотр файлов»

Для просмотра информации в бинарном формате следует изменить формат отображения в строке **Кодировка** с выбранной кодировки на **Нет (Binary)**.

6.6.9. 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**, **Агент**, **Группа**. 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) Агент;

3) Платформа (Windows или Linux);

4) Имя;

5) Издатель;

6) Критичность (не менее);

7) Признак трендовой уязвимости (трендовая или обычная);

8) Группа агентов;

9) Оценка CVSS (от 0 до 10);

10) Значение CVE.

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** приводит к переходу 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.

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.

6.7 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 (YARA-правила, индикаторы компрометации, индикаторы атак).

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 Windows.

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.

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.

6.7.1. 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 (рис. 84) включает в себя следующие структурные элементы:

– таблица с наборами индикаторов атак;

– кнопка **Добавить набор**;

– кнопка **Применить набор**;

– кнопка **Удалить выбранные наборы**.

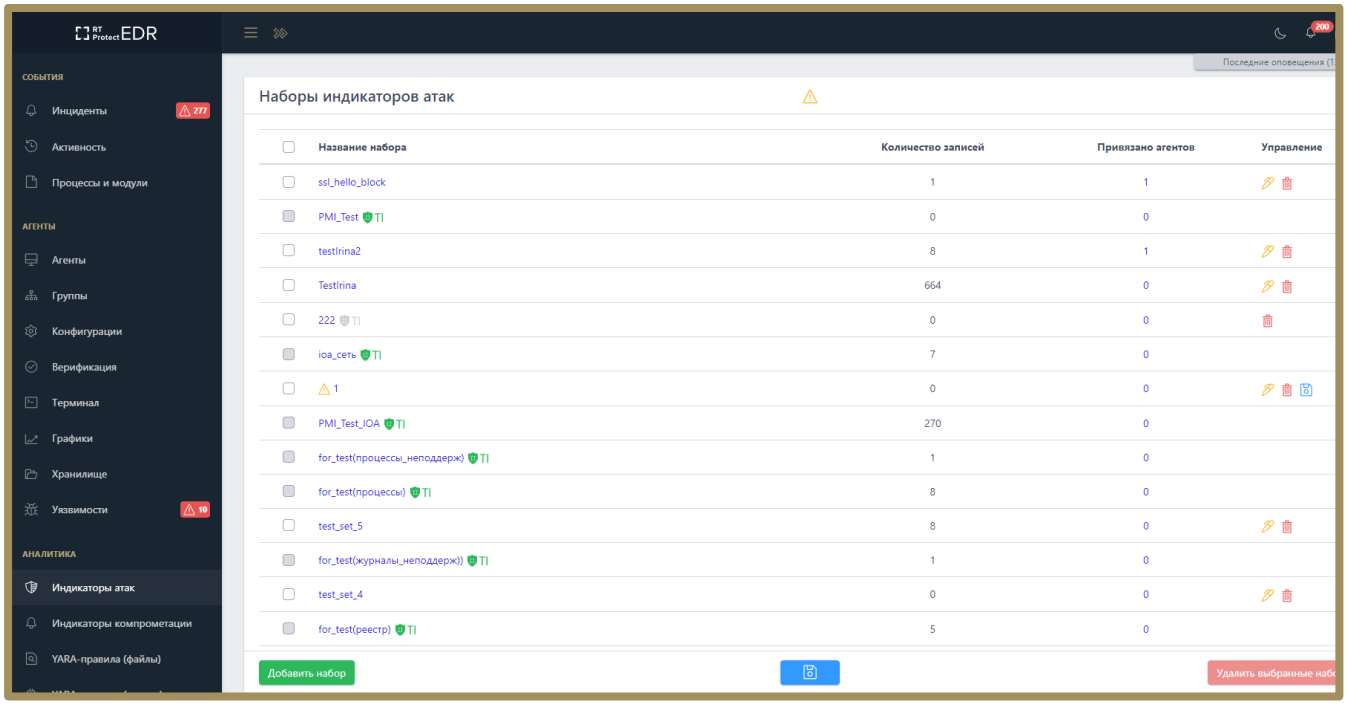


Рисунок 84 – Наборы индикаторов атак

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 **Применить**).

На странице пользователь может выполнить следующие операции:

– просматривать ранее созданные наборы индикаторов атак;

– добавлять новые наборы;

– редактировать название выбранного набора;

– применить изменения выбранного набора;

– удалять выбранные наборы.

Для корректной работы наборов после каждого изменения требуется их применять 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. 85):

1) Создать новый индикатор;

2) Импортировать индикатор из sigma-правила.

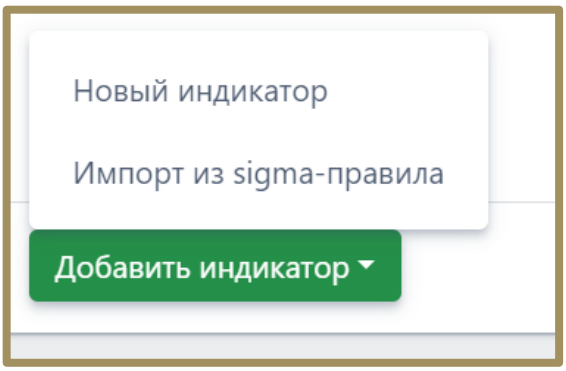


Рисунок 85 – Окно выбора способа добавления индикатора атаки

При выборе способа **Новый индикатор** откроется окно **Добавить индикатор**.

В данном окне следует прописать условия, на основании которых будет срабатывать правило. Особенности написания индикаторов атак, их синтаксис подробно описывается в документе «Руководство аналитика RT Protect EDR». После написания условия необходимо нажать кнопку Добавить.

При написании 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 (</>), 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 86.

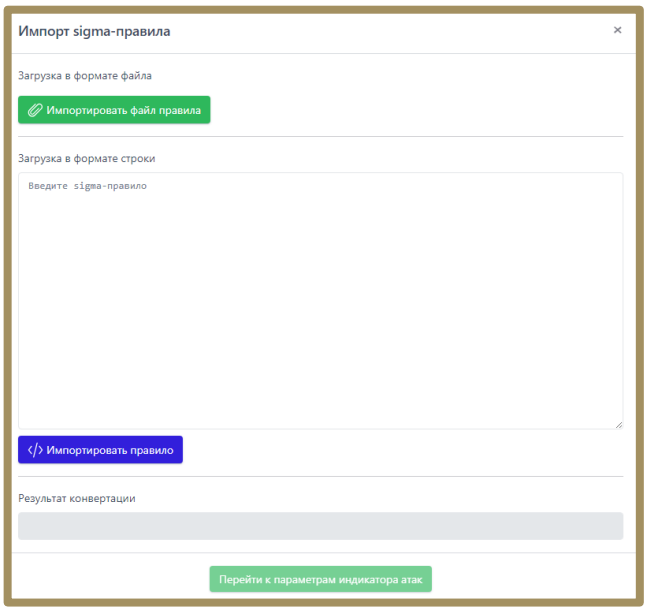
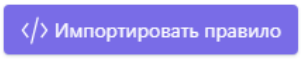
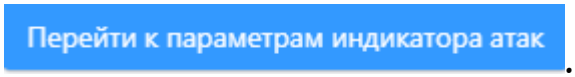


Рисунок 86 – Окно добавления индикатора с помощью импорта из sigma-правила

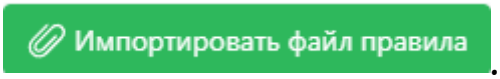
Sigma-правило, на основании которого будет создан индикатор атак, может быть добавлено в формате файла, либо в формате строки.

Для создания индикатора на основе Sigma-правила следует перейти на сайт https://github.com/SigmaHQ/sigma/blob/master/rules/windows и, выбрав одно из правил, нажать по иконке 

.

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 редактированию и сохранению 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 

.

6.7.2. 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

Страница **Наборы индикаторов компрометации** представлена на рисунке 87.

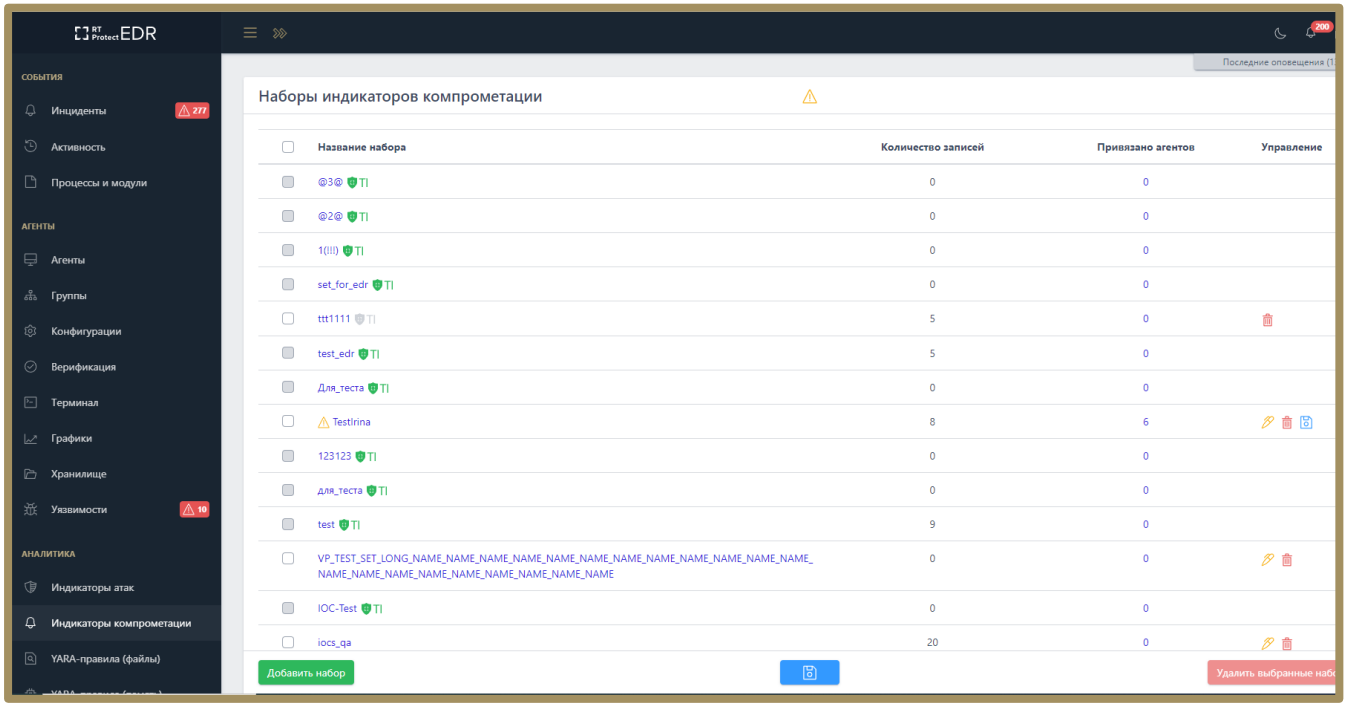


Рисунок 87 – Наборы индикаторов компрометации

Информация на странице представлена в табличном виде. Если на странице присутствует хотя бы один непримененный 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 **Применить** , а в середине нижней части страницы появляется кнопка **Применить все наборы** .

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 **Применить** .

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.

Применить – кнопка отображается в поле **Управление** при условии, что набор индикаторов компрометации не применен. При нажатии кнопки **Применить** открывается окно **Подтверждение действия**. Далее для применения набора необходимо нажать кнопку Выполнить.

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 Выполнить.

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) Действие;

5) Комментарий;

6) Дата создания/Автор;

7) Последнее изменение/Пользователь;

8) Активность;

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.

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) Применить набор – ;

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. 88) следует заполнить поля, соответствующие полям, указанным в шапке таблицы индикаторов, после чего нажать кнопку Добавить.

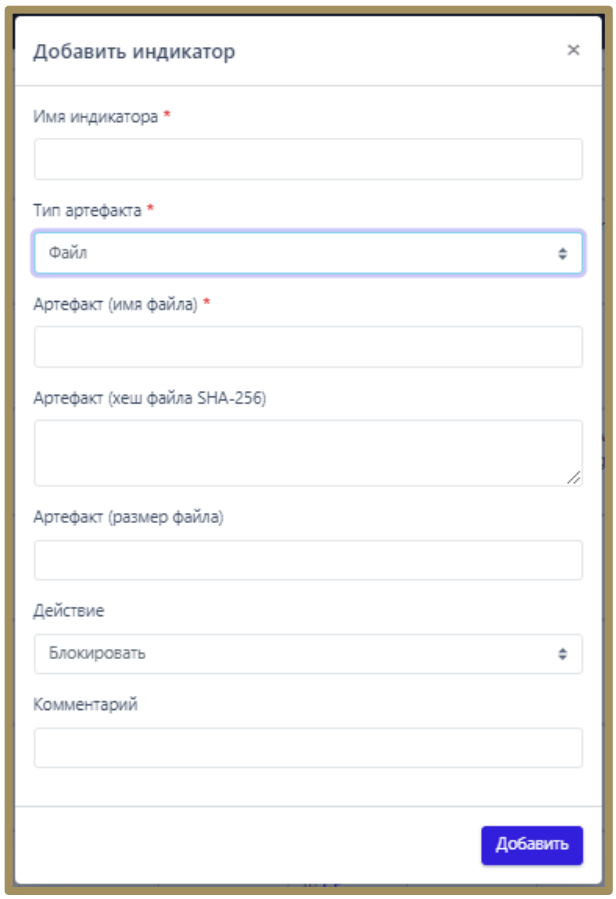


Рисунок 88 – Окно «Добавить индикатор» с типом артефакта «Файл»

Для применения любого изменения в индикаторах набора необходимо нажать кнопку **Применить набор**. 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.

6.7.3. 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 (рис. 89) включает в себя следующие структурные элементы:

– таблица с наборами YARA-правил;

– кнопка **Добавить набор**;

– кнопка **Применить набор**;

– кнопка **Удалить выбранные наборы**.

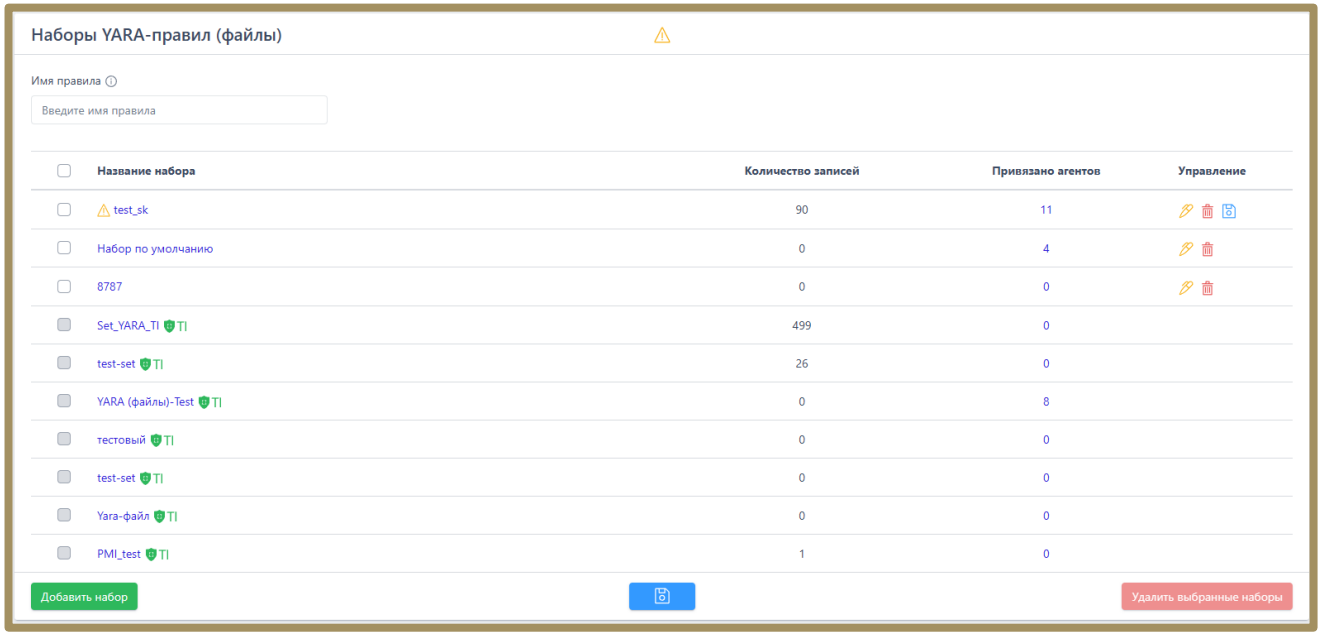


Рисунок 89 – Наборы YARA-правил (файлы)

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 **Применить** ( ) или **Применить все наборы** ( ).

Для удаления набора необходимо нажать кнопку **Удалить** ( ) или **Удалить выбранные наборы.**

Для фильтрации на странице **Наборы Yara-правил (файлы)** имеется фильтр по имени правила входящего в набор.

При нажатии ЛКМ на имени набора открывается страница **YARA-правила (файлы)** для выбранного набора (рис. 90).

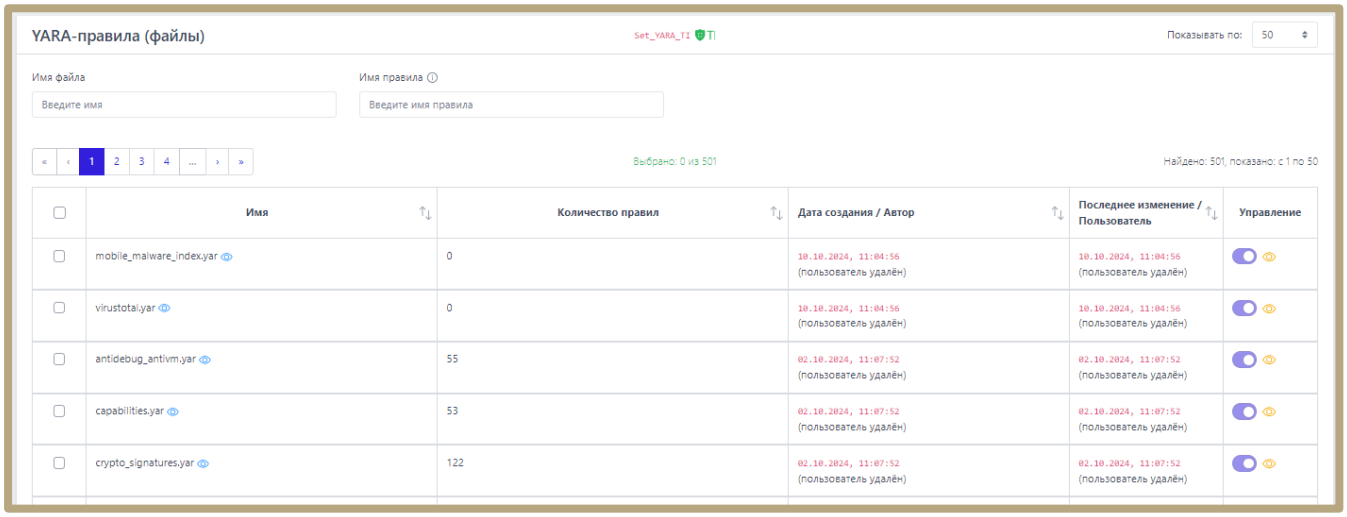


Рисунок 90 – YARA-правила (файлы)

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 91.

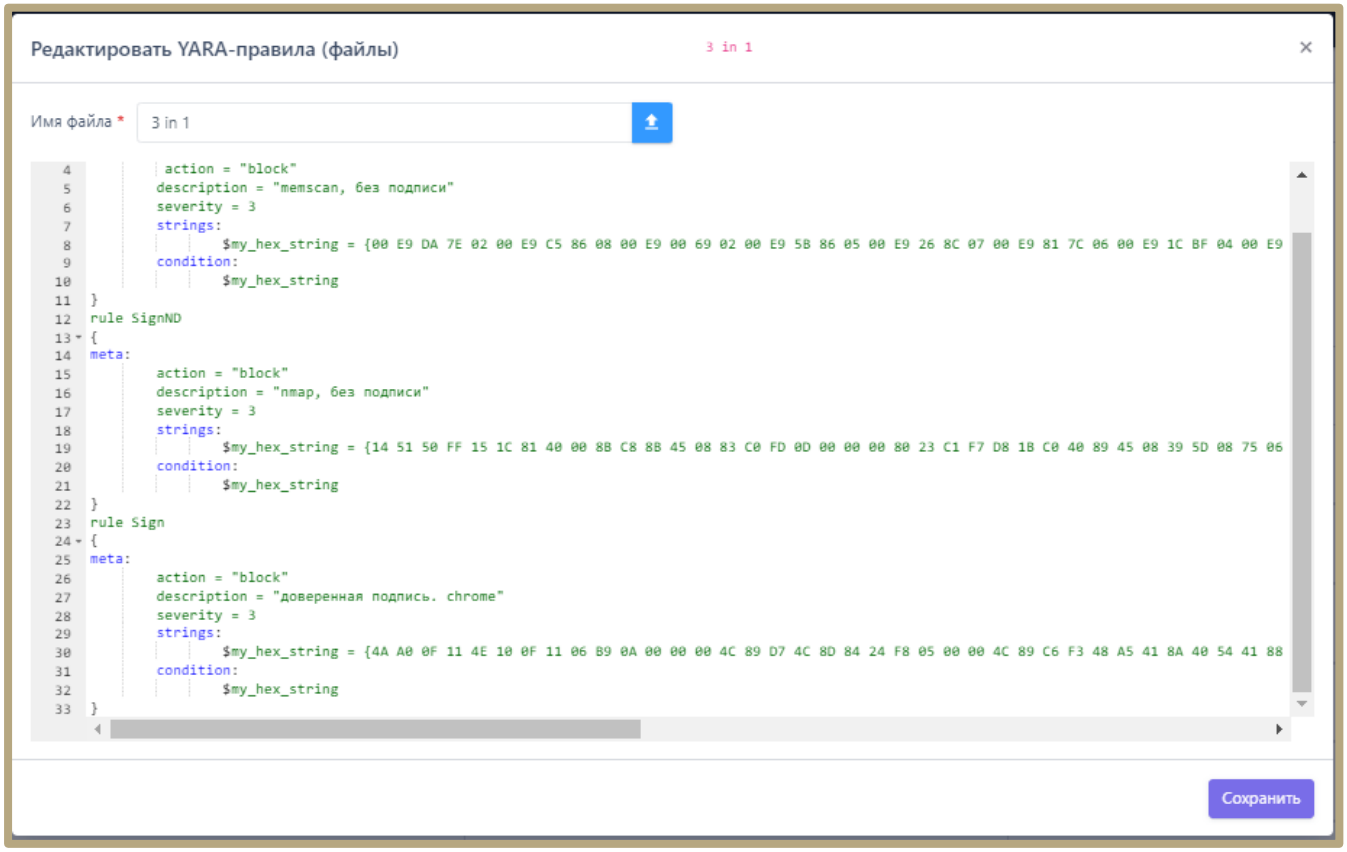


Рисунок 91 – Пример правила YARA

Для корректной работы после любых изменений в наборе необходимо нажать кнопку **Применить набор** ( ).

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. 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.

6.7.4. 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 **Применить набор**;

– 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 **Применить** ( ) или **Применить все наборы** ( ).

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 **Применить набор** ( ).

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. 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.

6.7.5. Журналы Windows

Общая информация

На странице **Наборы журналов Windows** 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 Windows** Программы. Информация о собранных ETW-событиях может быть использована при написании индикаторов атак (в данный момент функционал не поддерживается.

Наборы журналов Windows

Страница **Наборы журналов Windows** содержит следующие структурные элементы (рис. 92):

– таблица с наборами журналов Windows;

– кнопка **Добавить набор;**

– кнопка **Применить все наборы;**

– кнопка **Удалить выбранные наборы.**

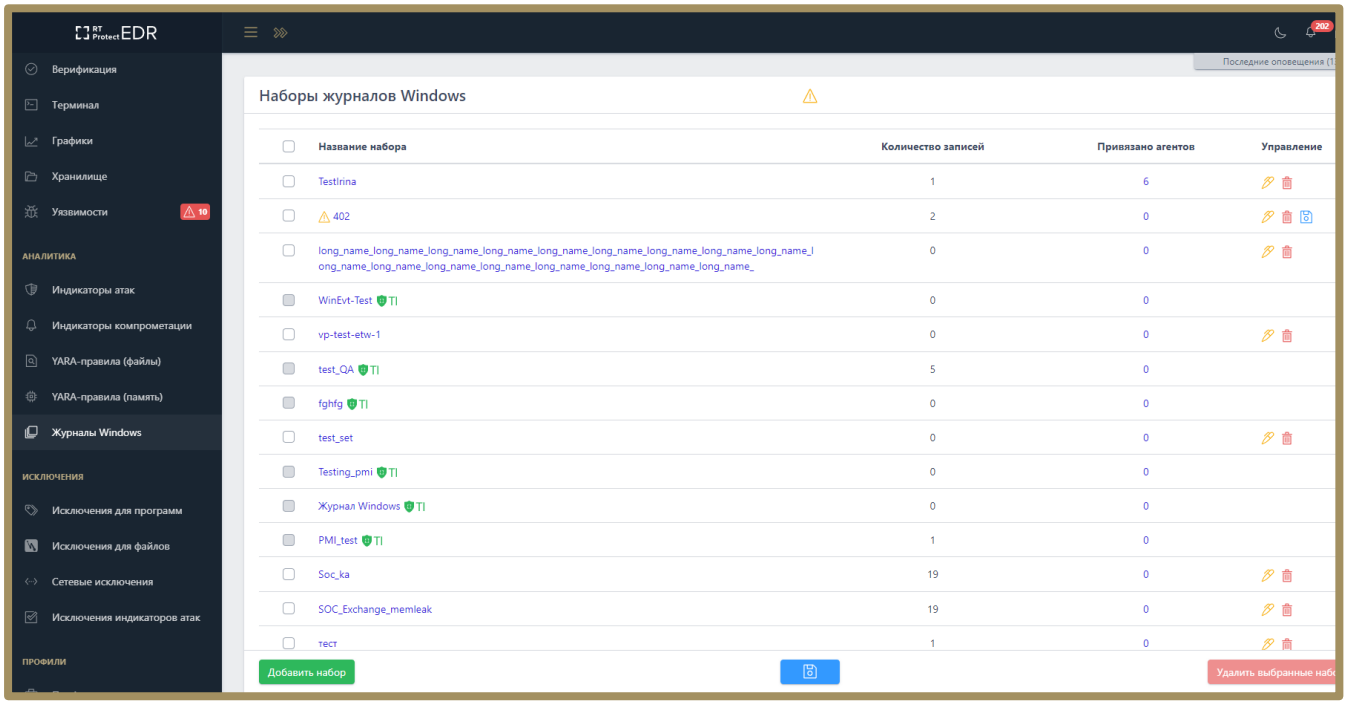


Рисунок 92 – Наборы журналов Windows

Чтобы добавить новый набор с журналами Windows, 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 Windows** необходимо нажать ЛКМ на имени набора журнала Windows в поле **Название набора**.

Страница «Журналы Windows»

На странице **Журналы Windows** в табличном виде отображается информация об определенном наборе правил для ETW-событий.

Пользователь может выполнить на странице следующие операции:

– добавить новое правило или несколько правил для журналов Windows;

– редактировать или удалить существующее правило/правила;

– экспорт/импорт файла с набором;

– копировать элементы одного набора или весь набор в другой набор.

В таблице **Журналы Windows** отображаются следующие поля:

1) Поля кнопки выбора ( );

2) Имя провайдера;

3) Ключевые слова (любые);

4) Ключевые слова (все);

5) Уровень;

6) Включение/исключение кодов событий;

7) Дополнительные параметры;

8) Последнее изменение/Пользователь;

9) Управление.

Имя провайдера – в поле отображается имя провайдера событий подсистемы ETW.

Ключевые слова (любые) – в поле отображается информация о любых ключевых словах, на основе которых будут обнаруживаться события выбранного ETW-провайдера. В Программе доступна настройка детектирования событий по ключевым словам для определенных провайдеров ETW, поэтому для многих правил в поле будет отображаться надпись Не заданы.

Ключевые слова (все) – в поле отображается информация обо всех ключевых словах, на основе которых будут обнаруживаться события выбранного ETW-провайдера. 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 Windows. 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. 93).

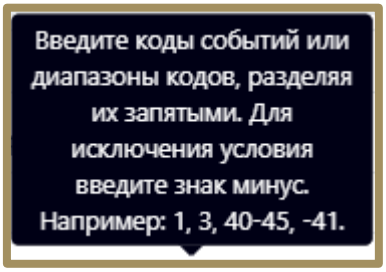


Рисунок 93 – Правила записи кодов событий

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) Группа провайдеров;

6) Порядковый номер процесса;

7) Ключ события;

8) 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 Добавить журнал. Пользователю доступно два режима добавления журнала Windows:

– 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** ().

6.8 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 и программных исключений, которые позволяют разрешить работу файлов и программ или запретить операции с ними без создания инцидентов, а также

6.8.1. Исключения для программ

Общая информация

На странице **Наборы исключений для программ** (рис. 94) 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 проверки необходимо выключить для указанного исполняемого файла и, соответственно, порождаемого им процесса.

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.

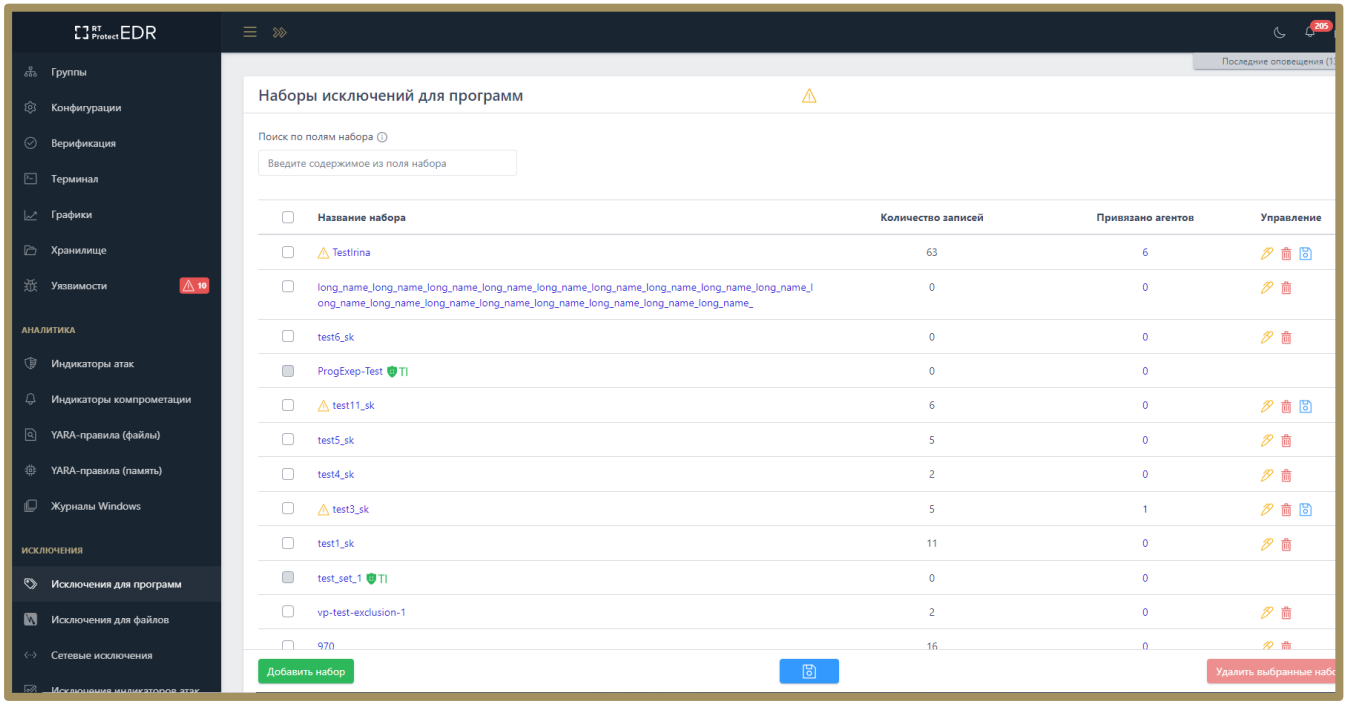


Рисунок 94 – Наборы исключений для программ

Наборы исключений для программ

Страница **Наборы исключений для программ** включает в себя следующие структурные элементы:

– таблица с наборами исключений для программ;

– кнопка **Добавить набор;**

– кнопка **Применить все наборы.**

– 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**.

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**.

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** ( ).

6.8.2. 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 предусмотрено два действия: **Разрешить** или **Блокировать**.

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.

Наборы исключений для файлов

Страница **Наборы исключений для файлов** включает в себя следующие структурные элементы (рис. 95):

– таблица с наборами исключений для файлов;

– кнопка **Добавить набор**;

– кнопка **Применить набор**;

– кнопка **Удалить выбранные наборы**.

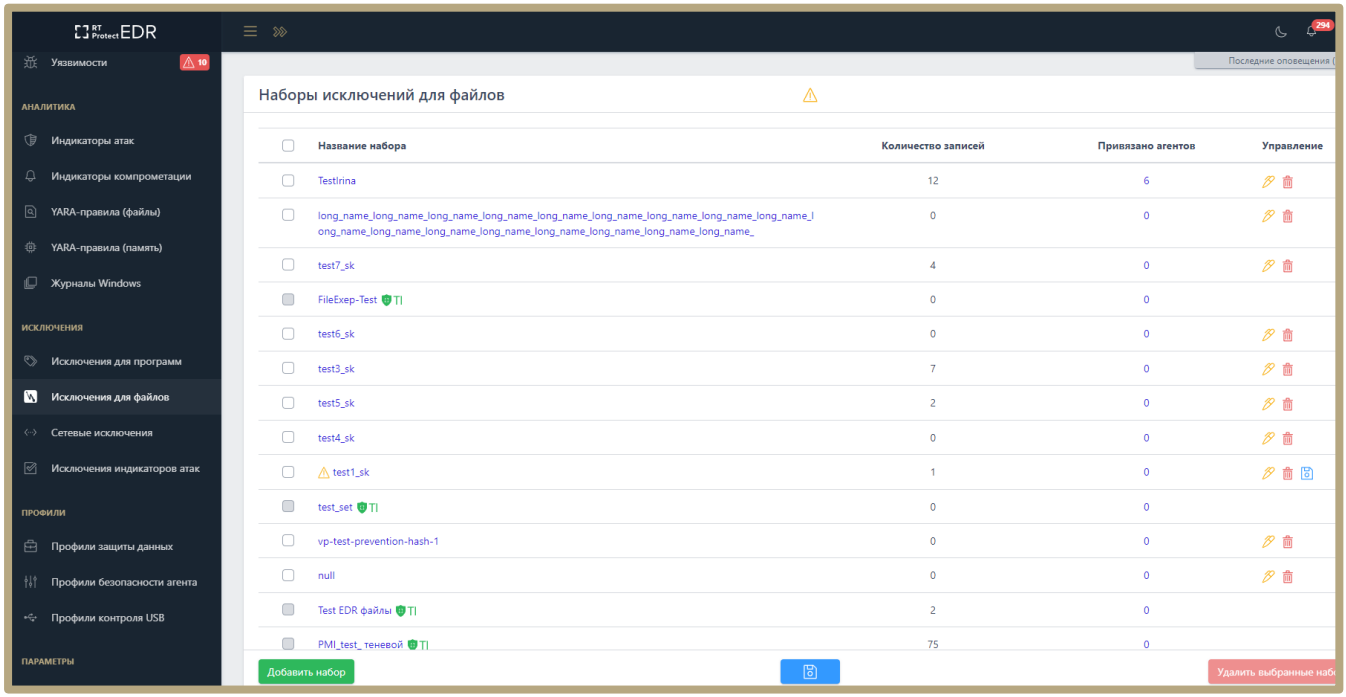


Рисунок 95 – Наборы исключений для файлов

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. Предусмотрено два действия: **Разрешить** или **Блокировать**. 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 И**сключения 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.

Чтобы завершить операцию **Добавить исключение**, после ввода параметров в окне **Добавить исключение** следует нажать кнопку Добавить.

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 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** ().

6.8.3. 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 машины, 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 машины, на которой установлен агент, с указанным в исключении IP-адресом, URL-адресом или доменным именем разрешается, при этом функциональность сохраняется даже тогда, когда агент изолирован);

– **Продолжение наблюдения** (означает, что взаимодействие машины, на которой установлен агент, с указанным в исключении IP-адресом, URL-адресом или доменным именем разрешается, при этом связанные с артефактом события отправляться не будут);

– **Разрешить (кроме изоляции)** (означает, что взаимодействие машины, на которой установлен агент, с указанным в исключении IP-адресом или доменным именем разрешается, кроме того случая, когда машина, на которой установлен агент, находится в режиме изоляции.

Использование сетевых исключений позволяет подавлять сетевые срабатывания TI-портала 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 (рис. 96):

– таблица с наборами сетевых исключений;

– кнопка **Добавить набор**;

– кнопка **Применить набор**;

– кнопка **Удалить выбранные наборы**.

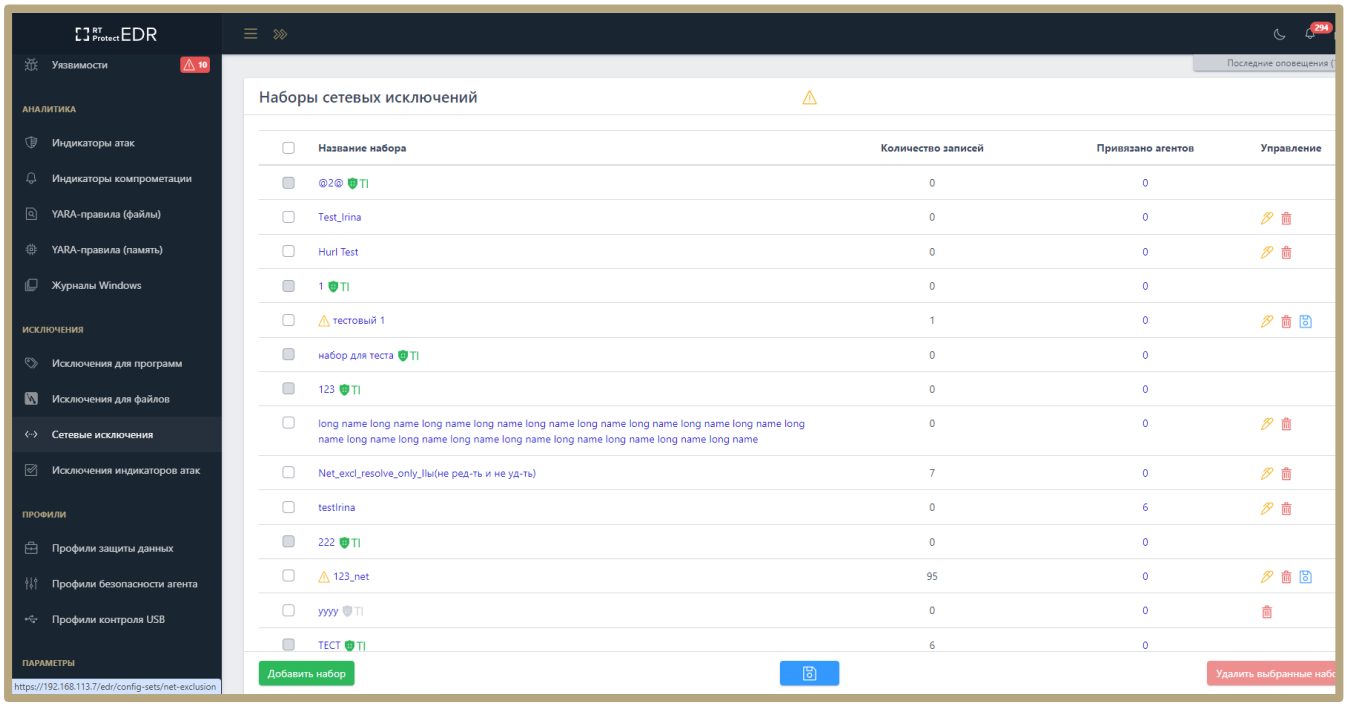


Рисунок 96 – Страница «Наборы сетевых исключений»

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, URL-адресу или доменному имени;

– 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 недопустимые комбинации: действие **Блокировать** и включенная опция **Не отправлять события**, 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 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** ( ).

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 97.

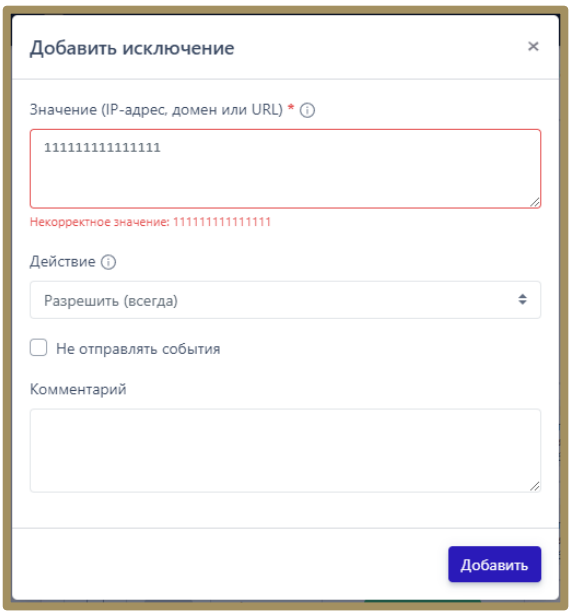


Рисунок 97 – Ввод некорректных параметров при добавлении исключения

6.8.4. 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 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 (рис. 96):

– таблица с наборами исключений для индикаторов атак;

– кнопка **Добавить набор;**

– кнопка **Применить набор;**

– кнопка **Удалить выбранные наборы.**

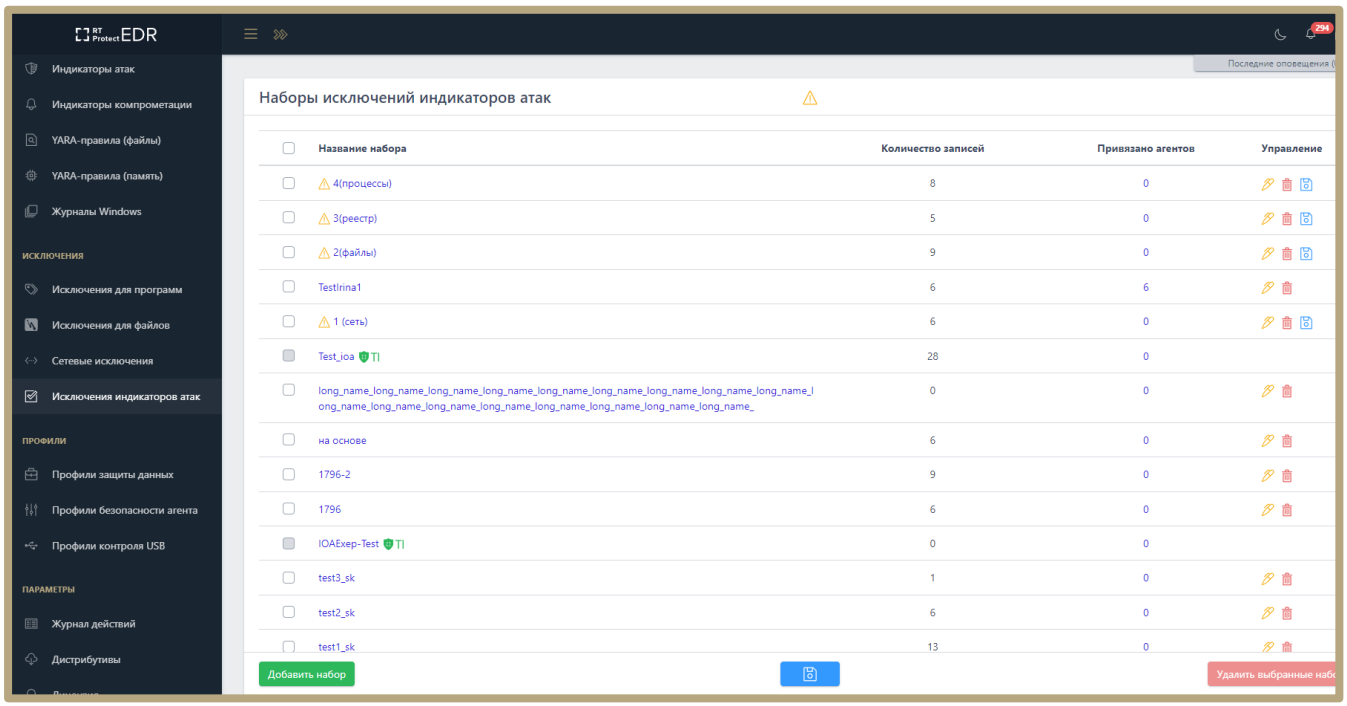


Рисунок 98 – Страница «Наборы исключений индикаторов атак»

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** ().

6.9 Профили

В области **Профили** администратор Программы может настраивать профили агента. Настройка профилей позволяет оптимизировать количество событий, поступающих от агента, изменять реакцию на инциденты, управлять системой резервирования каталогов и т.д.

6.9.1. Профили защиты данных

На странице **Профили защиты данных** администратору доступны следующие возможности:

1) Отключить\Включить работу модуля Anti-ransomware;

2) Настроить список защищаемых каталогов;

3) Настроить резервирование данных;

4) Экспортировать настройки профиля защиты в файл;

5) Импортировать настройки из ранее экспортированного профиля защиты (поддерживаются файлы в формате txt).

Модуль Anti-ransomware включен на всех агентах по умолчанию, для этого каждому новому верифицированному агенту назначается набор настроек **Профиль по умолчанию** (рис. 99).

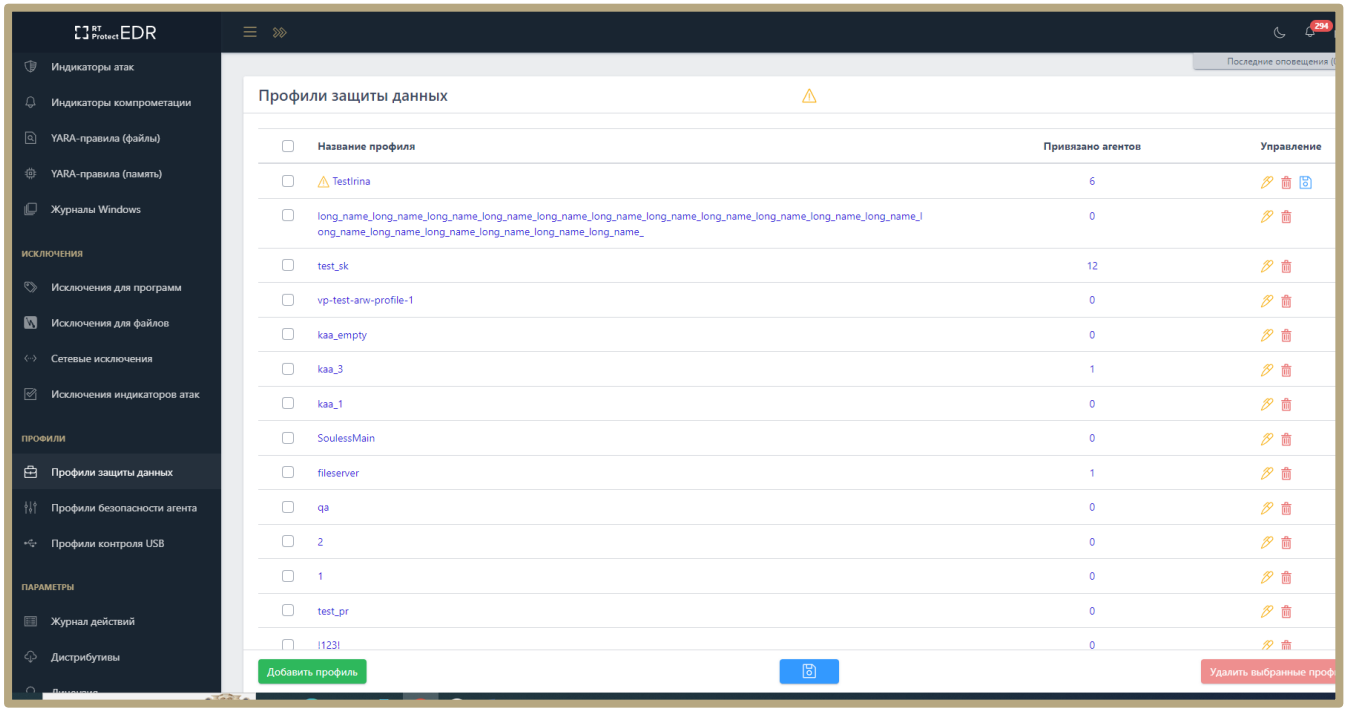


Рисунок 99 – Страница «Профили защиты данных»

Информация о профилях представлена в табличном виде.

В таблице отображаются следующие поля:

1) **Название профиля;**

2) **Привязано агентов;**

3) **Управление** (здесь находятся кнопки редактирования, удаления и сохранения профилей –).

Администратор может добавить новый профиль защиты с настройками, отличающимися от настроек профиля по умолчанию. Для этого необходимо нажать кнопку Добавить профиль и в открывшемся окне ввести название нового профиля, после чего нажать кнопку Добавить (рис. 100).

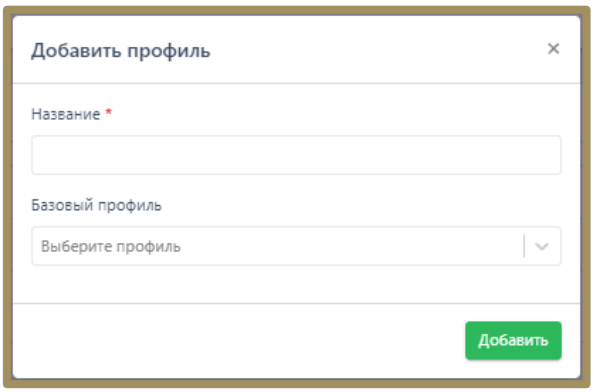


Рисунок 100 – Добавление профиля защиты

Если новый профиль защиты данных требуется создать на основе ранее сохраненного, то в поле выбора **Базовый профиль** следует назначить из выпадающего списка один из существующих профилей защиты и нажать кнопку Добавить.

С помощью кнопки **Редактировать** ( ) можно изменить название профиля (рис. 101).

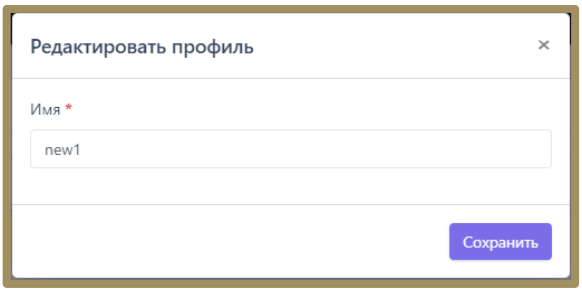


Рисунок 101 – Редактирование названия профиля защиты данных

Значок рядом с названием профиля или сверху страницы сообщает пользователю о том, что один или несколько профилей защиты данных не сохранены, для корректной работы их необходимо сохранить с помощью кнопки .

Для удаления профиля или нескольких профилей защиты данных необходимо отметить их флажками и нажать кнопку Удалить выбранные профили, после чего подтвердить действие в открывшемся окне.

Если требуется установить параметры защиты данных, отличающиеся от параметров существующих профилей защиты, то следует нажать название профиля, после чего откроется страница **Профиль защиты данных**.

Страница «Профиль защиты данных»

В любом профиле защиты данных можно выделить три области настроек (рис. 102):

1) Базовые настройки;

2) Настройки резервирования;

3) Список защищаемых каталогов.

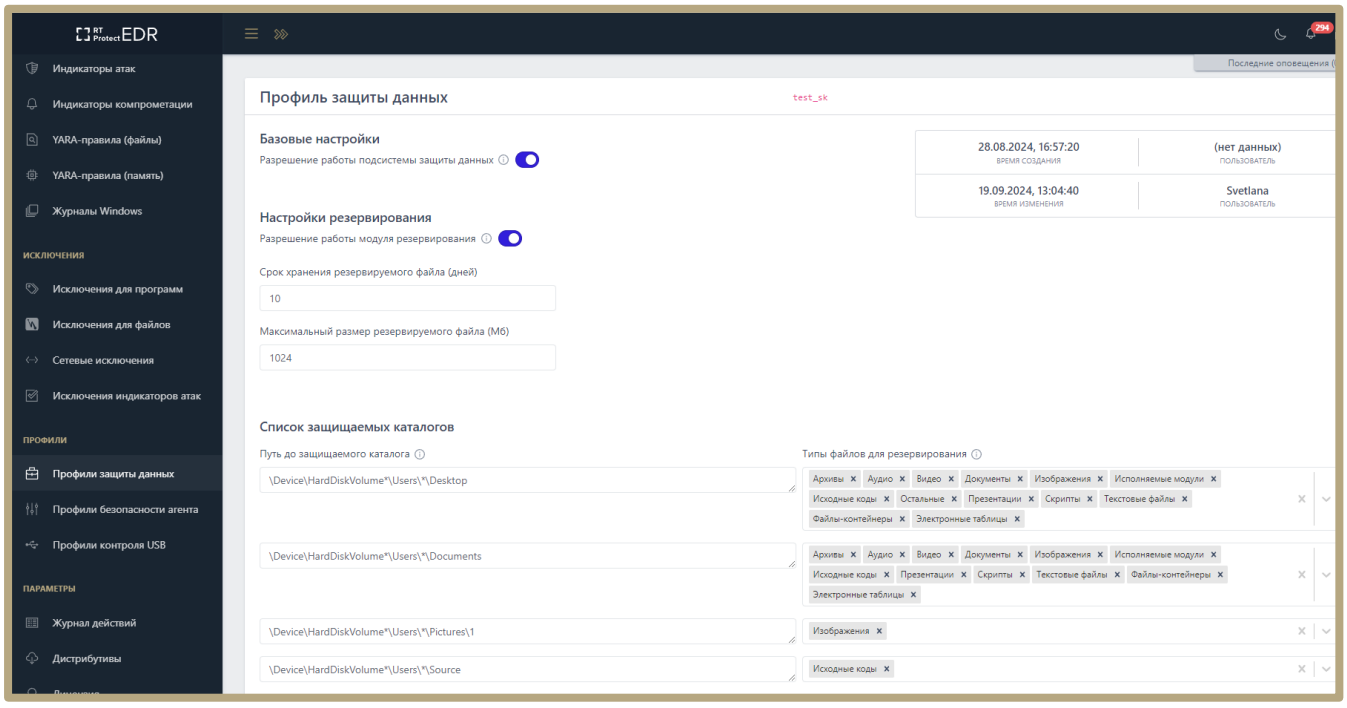


Рисунок 102 – Страница «Профиль защиты данных»

В верхней части страницы отображается информация о пользователе, создавшем профиль и времени, когда профиль был создан, а также информация

о пользователе, сделавшем в профиле последние изменения, и времени внесения этих изменений.

В области **Базовые настройки** профиля администратор может включить или выключить Anti-ransomware-модуль. Эта настройка задается кнопкой  в строке **Разрешение работы подсистемы защиты данных**.

В области **Настройки резервирования** администратор может выполнить следующие операции:

1) Разрешить или запретить работу модуля резервирования файлов (кнопка );

2) Установить срок хранения резервируемого файла в днях;

3) Установить максимальный размер резервируемых файлов в мегабайтах.

В области **Список защищаемых каталогов** администратор может настроить каталоги и типы файлов, которые необходимо резервировать.

Для добавления защищаемого каталога необходимо использовать кнопку **Добавить каталог** в нижней части страницы. В каждом каталоге может быть свой набор резервируемых файлов.

Типы резервируемых файлов

Резервирование поддерживает следующие типы файлов:

1) Архивы;

2) Аудио;

3) Базы данных;

4) Видео;

5) Документы;

6) Изображения;

7) Исполняемые модули;

8) Исходные коды;

9) Презентации;

10) Скрипты;

11) Текстовые файлы;

12) Файлы-контейнеры;

13) Электронные таблицы;

14) Остальные.

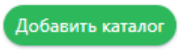
Также на странице профиля предусмотрена функция выбора сразу всех файлов для защищаемого каталога.

Каждому типу файла соответствуют определенные расширения файлов. Информация о поддерживаемых расширениях по типу файла может быть показана администратору при нажатии кнопки ⓘ в строке **Типы файлов для резервирования**.

Настройка защищаемых каталогов

Если для определенного каталога не выбран ни один из типов резервируемых файлов, то резервирование для такого каталога поддерживаться не будет.

Администратор может настроить профиль защиты данных таким образом, чтобы защищать только определенные файлы в определенных каталогах, тем самым снижая нагрузку на систему.

Для добавления каталога в список защищаемых необходимо нажать кнопку 

, далее выбрать типы файлов, которые необходимо резервировать для указанного каталога и применить его, нажав по иконке ().

Примечание

Новые защищаемые каталоги добавляются с именем по умолчанию **Protected Folder**, поэтому если в профиль требуется добавить два или более каталога, требуется изменять названия добавляемых каталогов.

Путь защищаемого каталога должен соответствовать требованиям, полный список которых можно просмотреть, нажав кнопку в строке **Путь до защищаемого каталога**. В списке представлены не только требования, но и примеры правильных и неправильных путей.

Важно

При написании пути до защищаемого каталога следует обратить внимание, что символ * после HardDiskVolume в пути типа: \Device\HardDiskVolume*\Users*\Documents обозначает, что будут защищаться все диски, если вместо символа * указать конкретный номер, обозначающий жесткий диск, то защищаться будут именно каталоги, находящиеся на данном диске, например, HardDiskVolume1.

Если требуется удалить каталог из профиля защиты данных, то в строке с выбранным каталогом необходимо нажать кнопку .

Для корректного применения на агенте измененных настроек профиля защиты данных должны соблюдаться следующие условия:

– профиль защиты данных применен (кнопка в нижней части страницы);

– подсистема защиты данных включена ;

– модуль резервирования включен ;

– конфигурация профиля защиты данных применена для агента.

Профиль защиты данных можно экспортировать в txt-файл и импортировать из него. Для этого используются кнопки экспорта () и импорта ().

Как работает резервирование?

После назначения для агента конфигурации с профилем защиты, в котором предусмотрено резервирование данных в одном или нескольких каталогах, администратор сможет восстановить эти данные в случае их шифрования или удаления программой-вымогателем.

Если вирус-шифровальщик проник на конечную точку с установленным агентом и зашифровал данные в защищаемом каталоге, то для восстановления этих данных пользователю необходимо определить процесс, выполнивший шифрование данных и на странице **Процесс** нажать кнопку **Восстановить файлы** и подтвердить выбранную операцию.

Для восстановления файлов также может использоваться команда терминала. Пользователю необходимо выполнить следующие действия:

1) Определить **uuid** процесса, выполнившего шифрование данных;

2) Открыть страницу **Терминал**;

3) Выбрать агента, данные которого были зашифрованы вирусом-шифровальщиком;

4) Выполнить в терминале команду **restore** с указанием **uuid** процесса, зашифровавшего данные на агенте.

Важно

Программа позволяет восстанавливать только выбранные типы файлов, указанные в защищаемых каталогах. Список защищаемых каталогов формируется в профиле защиты данных агента, при этом должны быть включены подсистема защиты данных и модуль резервирования.

Если места на диске машины, на которой установлен агент, будет недостаточно для резервирования файлов, то модификацию и удаление файлов в пределах списка защищаемых каталогов все равно произвести будет невозможно.

6.9.2. 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 (рис. 103).

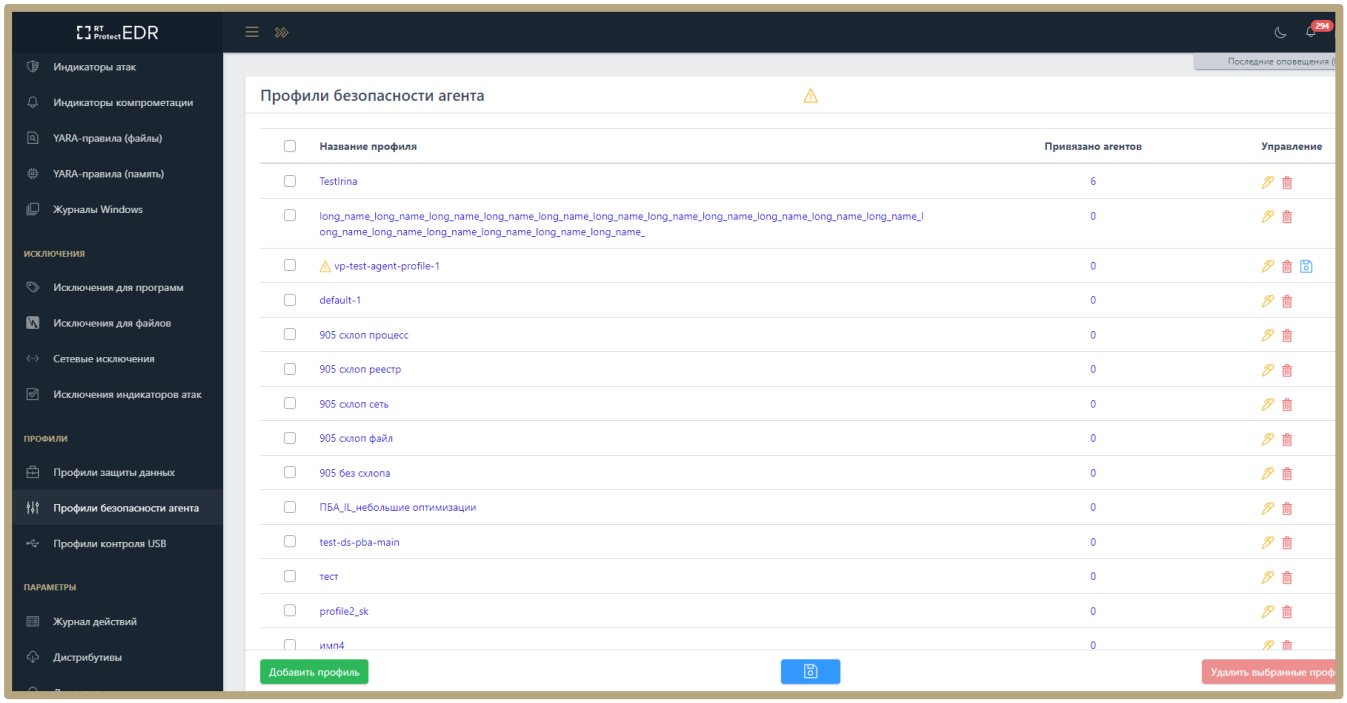


Рисунок 103 – Профили безопасности агента

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 применить изменения для агентов, 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** администратор 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;

– общие настройки безопасности.

– параметры безопасности монитора процессов;

– параметры безопасности файлового монитора;

– настройки безопасности сетевого монитора;

– настройки безопасности монитора реестра.

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 доступа к процессам и нитям;

9) Исключать события загрузки известных модулей;

10) Исключать события со статусом «Разрешено» (кроме ключевых);

11) Исключать все события со статусом «Разрешено»;

12) Исключать события RPC-вызовов;

13) Фильтровать события модификации реестра;

14) Оптимизировать представление стека вызовов в событиях;

15) Принудительное подавление событий процессов при превышении лимита.

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.

Кроме того, в области с оптимизацией потока событий находится раздел с настройками событий, получаемых от инструментария управления (WMI). 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 или созданными аналитиками правилами.

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.

В области **Настройки безопасности монитора процессов** аналитик 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**). Также аналитик может поставить флаг **Оптимизировать поток событий межпроцессного взаимодействия**, чтобы сократить количество отображаемых на сервере управления событий, связанных с обменом данными между потоками различных процессов.

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. Администратор 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.

Также в настройках безопасности файлового монитора можно установить флаги **Подсчитывать хеш SHA-1** и **Подсчитывать хеш MD5**. По умолчанию эти функции отключены, так как создают существенную нагрузку на файловый монитор.

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 и т.д.

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.

Кроме указанных выше настроек в Программе предусмотрены настройки безопасности сетевого монитора и монитора реестра. Настройки безопасности сетевого монитора включаются и отключаются флагами **Оптимизировать поток**

сетевых событий, Активное противодействие сканированию портов и **Запретить все входящие подключения,** а настройки монитора реестра флагом **Оптимизировать поток событий реестра.**

Чтобы логика настроек применялась на агентах, для которых установлен профиль безопасности, после его изменения необходимо нажать кнопку **Применить профиль** ().

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.

6.9.3. 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 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 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).

Исключать события RPC-вызовов.

Опция позволяет исключить из потока события источника **Вызовы: RPC**.

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.

Оптимизировать представление стека вызовов в событиях.

Данная опция управляет способом представления стэка вызовов в событиях. Если опция задана, то стэк вызовов передается и отображается в компактной форме, где несколько последовательных одинаковых модулей

«сворачиваются» в один, а информация о смещениях полностью исключается из стэка вызовов. Такое минималистическое представление позволяет сократить размер передаваемых агентом данных, в то же время оставляя аналитику достаточно возможностей для определения инициатора того или иного события, посредством анализа стека вызовов. Если опция не задана, то стэк вызовов передается и отображается в полном виде – без сокращений.

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.

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 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).

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.

Оптимизировать поток событий межпроцессного взаимодействия.

Оптимизация потока событий межпроцессного взаимодействия заключается в «сворачивании» нескольких одинаковых (в рамках одного процесса) событий в одно.

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.

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.

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.

Оптимизировать поток файловых событий.

Оптимизация потока файловых событий заключается в «сворачивании» нескольких одинаковых (в рамках одного процесса) событий в одно.

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 безопасности сетевого монитора

Оптимизировать поток сетевых событий.

Оптимизация потока сетевых событий заключается в «сворачивании» нескольких одинаковых (в рамках одного процесса) событий в одно.

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.

Запретить все входящие 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.

Настройки безопасности монитора реестра

Оптимизировать поток событий реестра.

Оптимизация потока событий реестра заключается в «сворачивании» нескольких одинаковых (в рамках одного процесса) событий в одно.

6.9.4. 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.**

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 кода;

7) Статистика чтения/записи данных.

Страница «Профили контроля USB»

Страница «Профили контроля USB» представлена на рисунке 104.

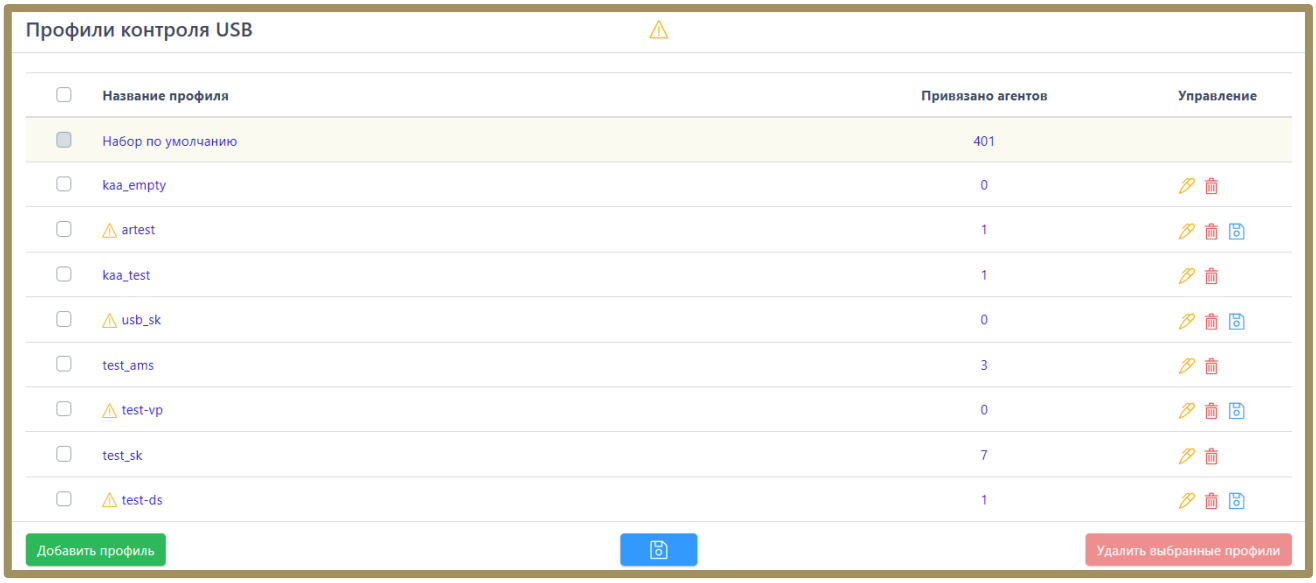


Рисунок 104 – Профили контроля USB

На странице 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) Применить 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 105.

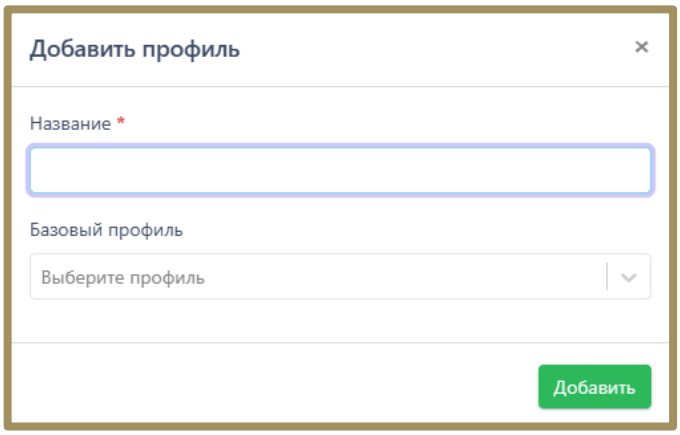


Рисунок 105 – Окно добавления профиля

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 106.

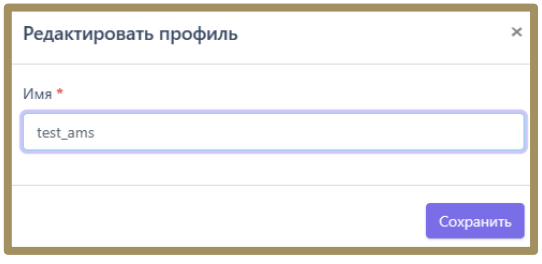


Рисунок 106 – Редактирование имени профиля

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 (смотри рисунок 107).

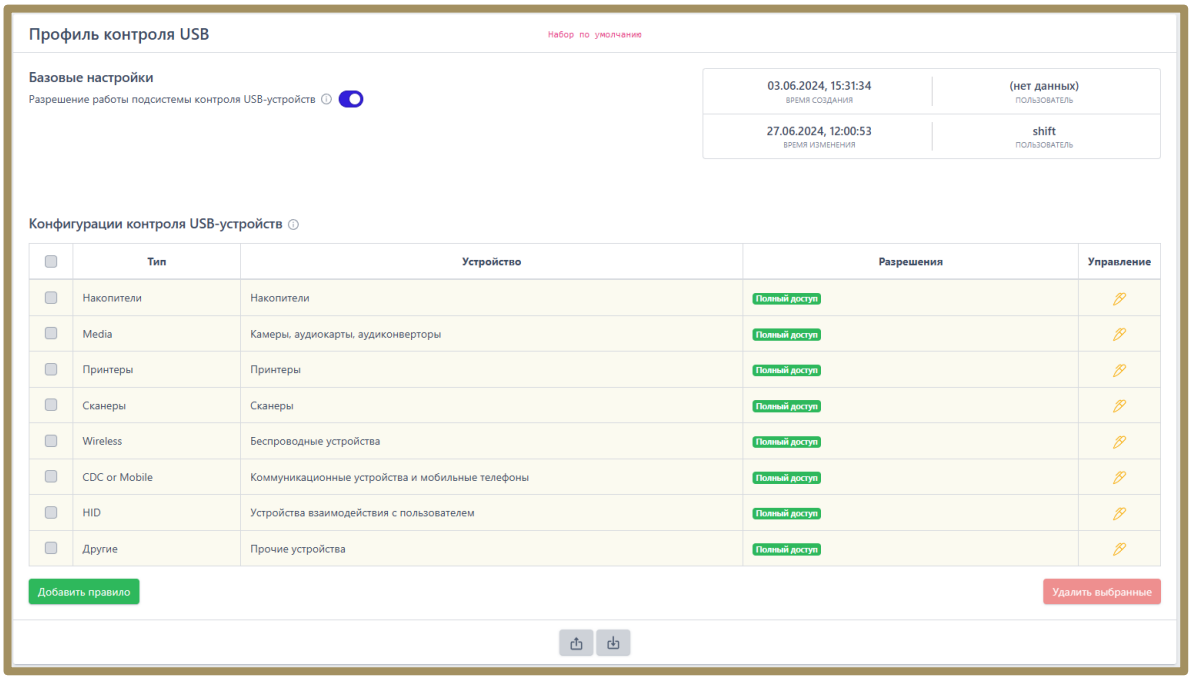


Рисунок 107 – Профиль контроля USB – Набор по умолчанию

Пользователь может добавить уникальную конфигурацию, нажав кнопку **Добавить правило**. Откроется окно **Создание правила контроля устройства USB** (см. рисунок 108).

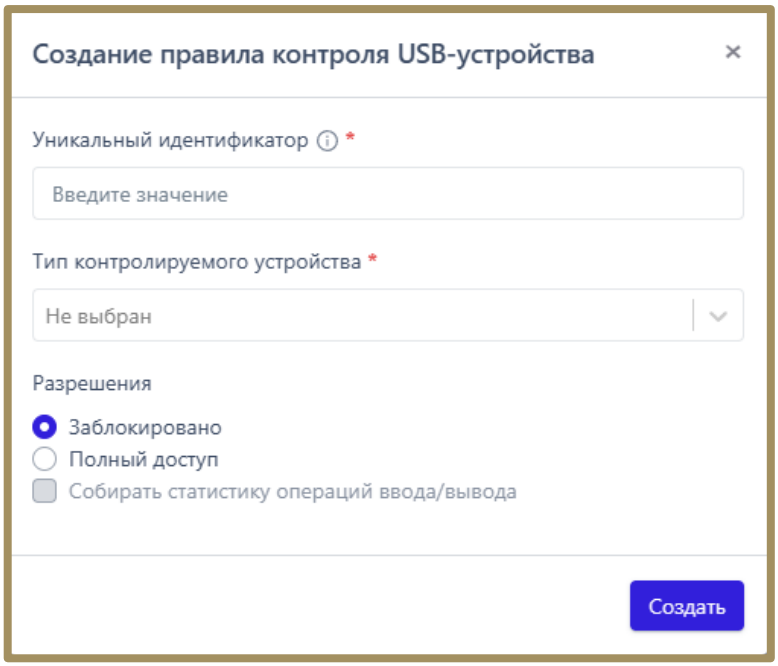


Рисунок 108 – Создание правила контроля USB-устройств

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.

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 сохранения изменений и последующего применения профиля требуется нажать по иконке , после чего откроется окно подтверждения действия, представленное на рисунке 109.

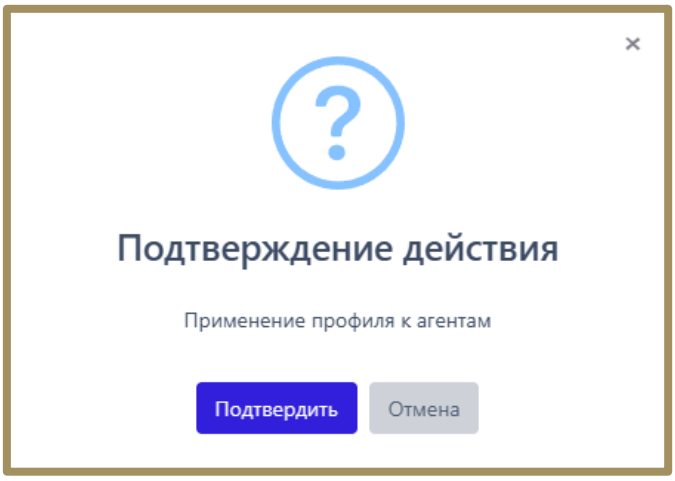


Рисунок 109 – Подтверждение действия применения профиля

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.

6.10 Параметры

В области **Параметры** основной панели Программы находятся следующие разделы: **Журнал действий, Дистрибутивы** и **Лицензирование**.

Разделы содержат параметры настройки Программы, лицензию, последнюю версию агента, журнал событий, связанных с инцидентами безопасности, учетными записями пользователей и действиями с агентами.

6.10.1. Журнал действий

На странице **Журнал действий пользователей** в табличном виде представлена информация о действиях пользователей: аналитиков и администраторов (рис. 110).

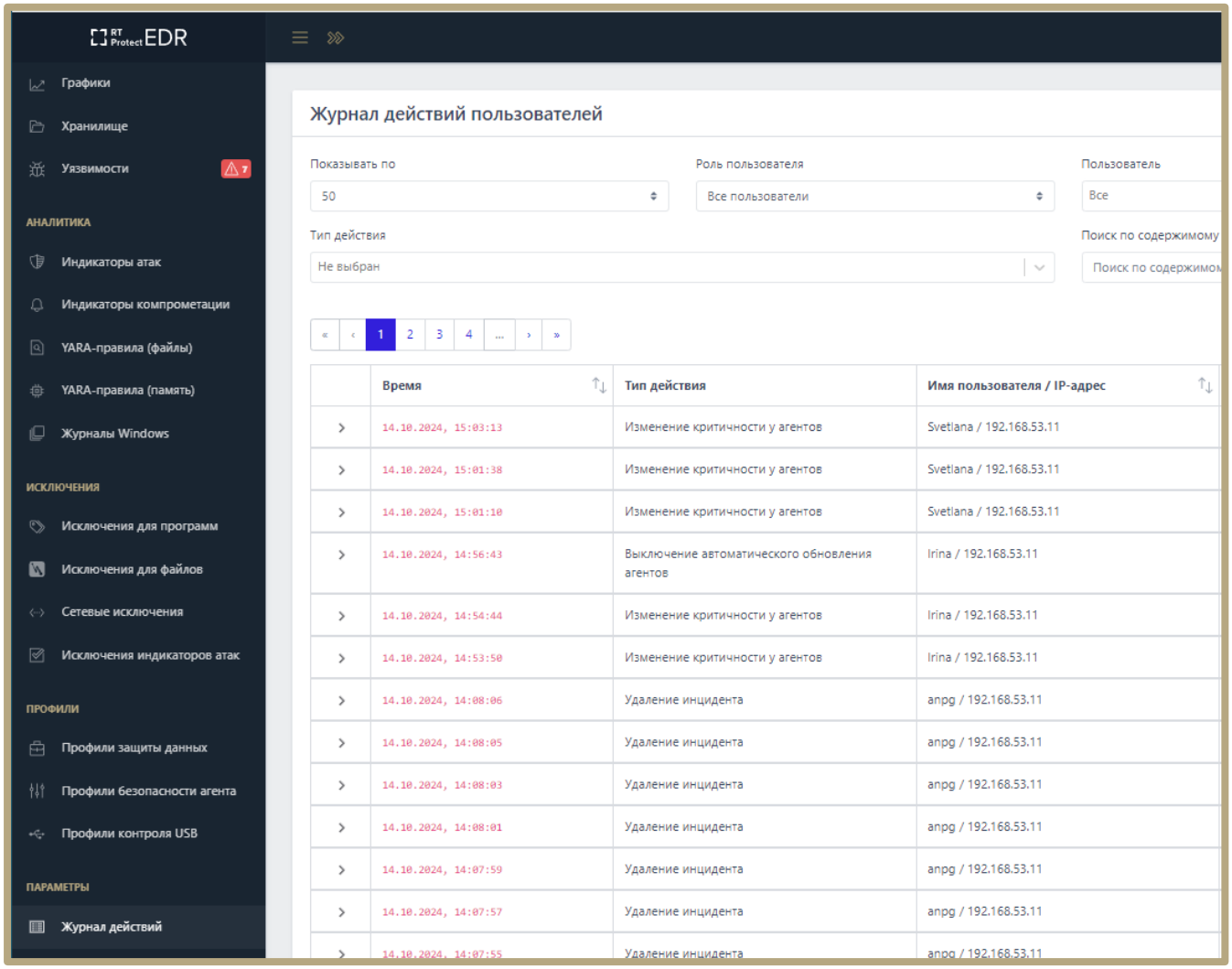


Рисунок 110 – Журнал действий

События таблицы можно фильтровать по количеству отображаемых событий (фильтр **Показывать по**), имени пользователя (фильтр **Имя пользователя**), роли пользователя (фильтр **Роль**), типу действия, совершенного пользователем (фильтр **Тип пользователя**), а также выполнять поиск по содержимому действия.

В фильтре **Поиск по содержимому действия** можно вводить поля, содержащиеся в описании действия в JSON-формате.

Все возможные действия пользователей, отображаемые в таблице, разделены на типы и подтипы:

Авторизация пользователя:

1) Вход в систему;

2) Выход из системы;

3) Выход из системы на всех устройствах.

Работа с пользователем:

1) Создание нового пользователя;

2) Изменение пароля пользователя;

3) Удаление пользователя из системы;

4) Блокировка пользователя;

5) Разблокировка пользователя;

6) Запрос ссылки для сброса пароля;

7) Сброс пароля пользователя.

Работа с агентом:

1) Отмена верификации агента;

2) Добавление агентов в группу;

3) Удаление агентов из группы;

4) Верификация агентов;

5) Отправка команды агенту;

6) Отправка команды группе агентов;

7) Загрузка нового дистрибутива агента на сервер;

8) Удаление дистрибутива агента с сервера;

9) Сетевая изоляция агентов;

10) Функции защиты агента выключены;

11) Выключение автоматического обновления агентов;

12) Снятие сетевой изоляции агентов;

13) Функции защиты агента включены;

14) Включение автоматического обновления агентов;

15) Назначение агентам набора исключений для файлов;

16) Назначение агентам набора исключений для программ;

17) Назначение агентам набора индикаторов компрометации;

18) Назначение агентам набора журналов Windows;

19) Назначение агентам набора YARA-правил (файлы);

20) Назначение агентам набора YARA-правил (память);

21) Назначение агентам набора индикаторов атак;

22) Назначение агентам профиля защиты данных;

23) Назначение агентам профиля безопасности.

Конфигурация:

1) Создание нового набора;

2) Удаление набора;

3) Добавление новых данных в набор;

4) Удаление данных из набора;

5) Импорт данных в набор;

6) Редактирование данных в наборе;

7) Копирование данных между наборами;

8) Перемещение данных между наборами.

Работа с файлами агента:

1) Загрузка файла агента на сервер;

2) Удаление файла агента с сервера.

Работа с инцидентом:

1) Создание инцидента;

2) Смена ответственного за инцидент;

3) Закрытие инцидента;

4) Назначение инцидента;

5) Добавление событий в инцидент;

6) Удаление событий из инцидента.

Действие с лицензией:

1) Установка новой лицензии на сервере.

В левой части таблицы с действиями пользователей находится кнопка раскрытия дополнительной информации о выбранном действии – ›. В зависимости от типа действия информация, раскрываемая при нажатии кнопки ›, может отличаться.

При выборе любого типа действия в разделе **Работа с пользователем** в раскрывающейся области пользователю будет показана дополнительная таблица с данными пользователя, с которым производились действия (рис. 111):

1) Имя пользователя (логин);

2) Email;

3) Имя и фамилия, указанные при регистрации;

4) Состояние активности пользователя на момент совершения с ним действий.

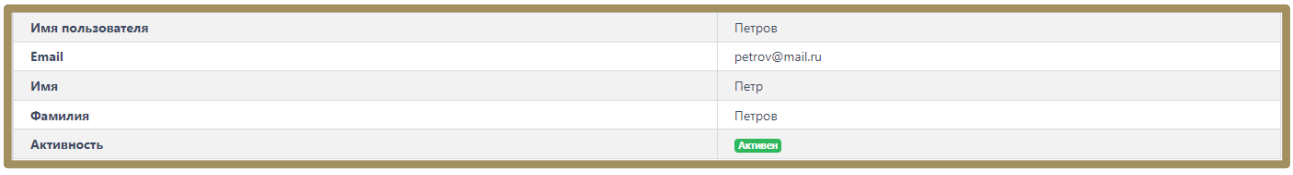


Рисунок 111 – Информация о пользователе, с которым совершались действия

При выборе типа действия **Отмена верификации агента** в разделе **Работа с агентом** в раскрывающейся области будет показана таблица с ID и именем агента, верификация которого была отменена (рис. 112).

Имя агента	TANYA-VM10
ID агента	82fe52ad3d2919609c32b526f84a685b03

Рисунок 112 – Отмена верификации агента

При выборе типов действия **Добавление агентов в группу/Удаление агентов из группы** в разделе **Работа с агентом** в раскрывающейся области будет показана таблица с именем группы, в которую добавляется или из которой удаляется агент, а также именем добавляемого/удаляемого агента.

При нажатии ЛКМ на имени группы можно перейти к странице **Группа**. При нажатии ЛКМ на имени агента происходит переход к странице **Агент**.

При выборе типов действия **Верификация Агентов/Сетевая изоляция агентов/Функции защиты агента выключены/Выключение автоматического обновления агентов/Снятие сетевой изоляции агентов/Функции защиты агента включены/Включение автоматического обновления агентов** в разделе **Работа с агентом** в раскрывающейся области будет показана таблица с именем агента, его ID и группой верифицируемого агента (рис. 113).

Имя агента	ID агента	Группа
agent_Win_7x64	f726152cd0a74a3e8d77eb4044a186ed01	юля-тест

Рисунок 113 – Информация о верифицируемом Агенте

При выборе типа действия **Отправка команды агенту** в разделе **Работа с агентом** в раскрывающейся области будет показана таблица с текстом отправленной команды, именем агента, на которого была отправлена команда,

а также временем отправки команды. При нажатии ЛКМ на имени агента происходит переход к странице **Агент**.

При выборе типа действия **Загрузка нового дистрибутива агента на сервер** в разделе **Работа с агентом** в раскрывающейся области будет показана таблица с именем и версией загружаемого на сервер агента, временем загрузки, размером дистрибутива, платформой (то есть ОС) агента, архитектурой агента, минимальной версией целевой платформы, описанием загружаемого дистрибутива и его хешем, рассчитанным по алгоритму MD5.

При выборе в разделе **Работа с агентом** типов действия **Назначение агентам набора для файлов/для программ/индикаторов компрометации/журналов Windows/YARA-правил/индикаторов атак** в раскрывающейся области будет показана таблица с названием набора и количеством агентов, к которым привязан соответствующий набор (см. рис. 114).

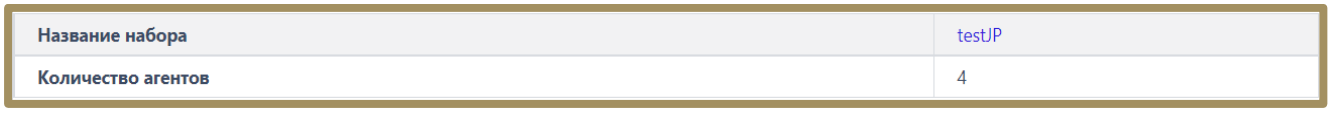


Рисунок 114 – Информация о привязанных к агенту наборах

Для перехода к разделу Программы, соответствующему указанному в таблице набору, необходимо кликнуть по имени набора.

При выборе в разделе **Конфигурация** типов действия **Создание нового набора/Удаление набора** в раскрывающейся области будет показана таблица с названием и типом создаваемого набора.

При выборе в разделе **Конфигурация** типов действия **Добавление новых данных в набор/Удаление данных из набора/Редактирование данных в наборе** в раскрывающейся области будет показана таблица с именем элемента, названием набора, типом набора, создателем элемента, пользователем, сделавшим последнее изменение в элементе.

При выборе в разделе **Конфигурация** типов действия **Импорт данных в набор** в раскрывающейся области будет показана таблица с названием набора, типом набора и количеством добавляемых элементов.

При выборе в разделе **Конфигурация** типов действия **Копирование данных между наборами/Перемещение данных между наборами** в раскрывающейся области будет показана таблица с именем копируемого элемента, названием набора, из которого копировали или перемещали элемент, названием набора, в который копировали или перемещали элемент, типом набора, создателем копируемого/перемещаемого элемента и пользователем, сделавшим последнее изменение в элементе.

При выборе в разделе **Работа с файлами агента** типа действия **Загрузка файла агента на сервер** в раскрывающейся области будет показана таблица с именем и размером загруженного файла, хеш-суммами, рассчитанными по алгоритмам MD5 и SHA-256, а также ID пользователя, загрузившего файл на сервер (рис. 115).

Имя файла	C:\Windows\System32\smss.exe
Размер	68 KB
MD5	437eee7b4b19a9ed01452b31adb17433
SHA-256	f9bb1d0bb4d7d3de73538e456056d9b5ba75dbbeeb2c53821c0196123d9cf7e5
ID пользователя	198f2855-889c-4c86-8d43-14ad66b0567a

Рисунок 115 – Информация о скачанных файлах

При выборе в разделе **Работа с файлами агента** и типа действия **Удаление файла агента с сервера** в раскрывающейся области будет показана таблица с именем удаленного файла и ID пользователя, удалившего файл (рис. 116).

Имя файла	C:\Windows\System32\smss.exe
ID агента	fd521338bc60194f7fe2d7de97933f397e

Рисунок 116 – Информация об удаленных файлах

При выборе в разделе **Работа с инцидентом** типа действия **Создание инцидента** в раскрывающейся области будет показана таблица с названием и описанием инцидента, присвоенными ему при создании (рис. 117).

Название (при создании)	Тестовый #5208
Описание (при создании)	Тестовый инцидент

Рисунок 117 – Информация о создании инцидента

При выборе в разделе **Работа с инцидентом** типов действия **Смена ответственного за инцидент/Закрытие инцидента/Назначение инцидента** в раскрывающейся области будет показана таблица с названием инцидента и именем пользователя, ответственного за решение этого инцидента. Для перехода к странице **Инцидент** необходимо кликнуть по имени инцидента, указанному в таблице.

При выборе в разделе **Работа с инцидентом** и типа действия **Смена ответственного за инцидент** в раскрывающейся области будет показана таблица с названием инцидента и именем пользователя, назначенного взамен предыдущего ответственного за решение инцидента (рис. 118). Для перехода к странице **Инцидент** следует кликнуть по имени инцидента, указанному в таблице.

Название	Процесс C:\Program Files (x86)\Kaspersky... #5444
Новый ответственный	anpg

Рисунок 118 – Информация о новом ответственном за инцидент

При выборе в разделе **Работа с инцидентом** типов действия **Закрытие инцидента/Назначение инцидента** в раскрывающейся области будет показана таблица с названием инцидента и именем пользователя, ответственного за

решение инцидента (рис. 119). Для перехода к странице **Инцидент** необходимо кликнуть по названию инцидента, указанному в таблице.

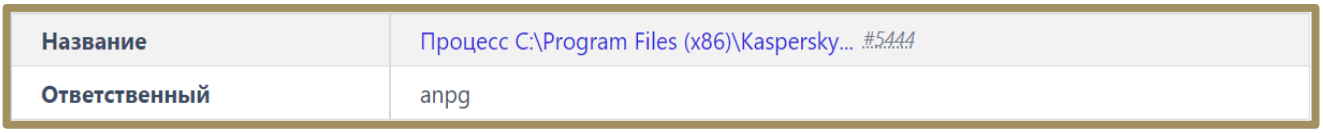


Рисунок 119 – Информация об ответственном за инцидент

При выборе в разделе **Действие с лицензией** типа действия **Установка новой лицензии на сервере** в раскрывающейся области будет показана таблица с названием компании, которой принадлежит лицензия, серийным номером лицензии, датой начала и окончания действия лицензии, максимальным возможным количеством агентов, текущим количеством агентов и комментарием к лицензии.

6.10.2. Дистрибутивы

На странице **Дистрибутивы** отображается информация о дистрибутиве агента (рис. 120):

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 /).

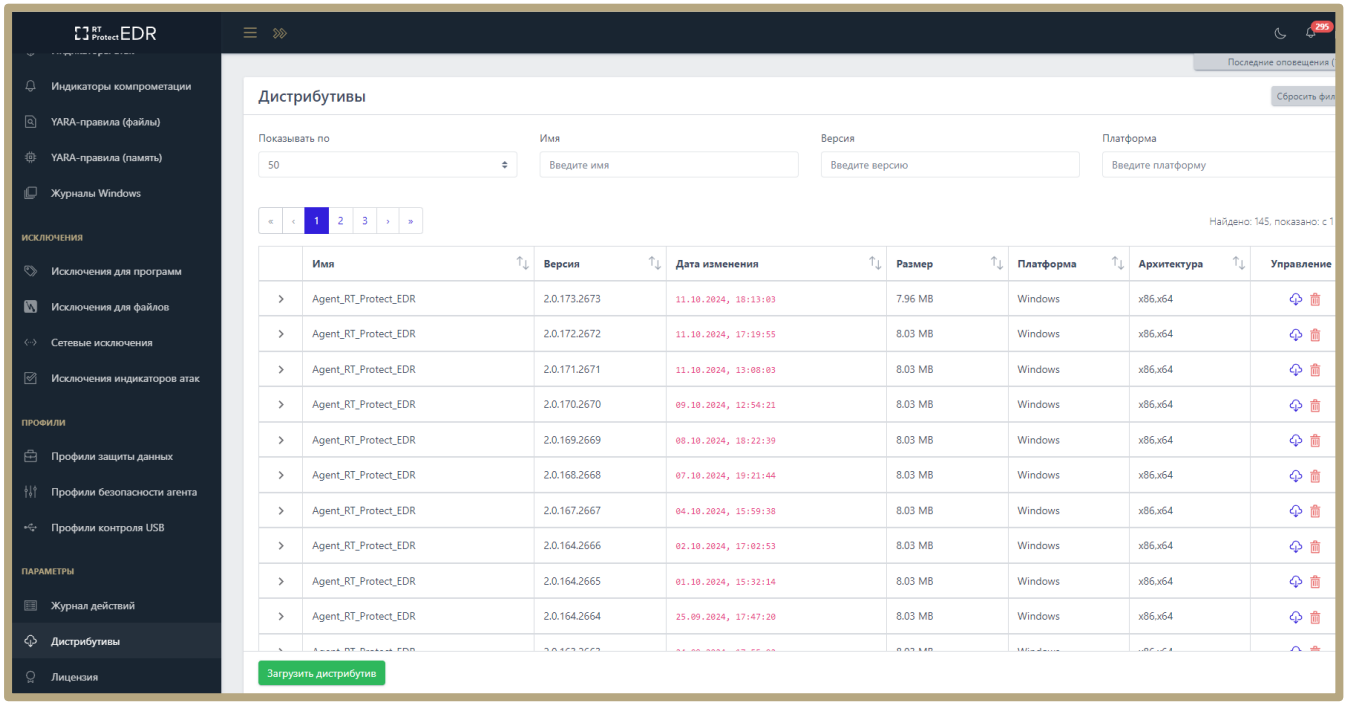


Рисунок 120 – Дистрибутивы

На странице отображается кнопка загрузки дистрибутива агента Загрузить дистрибутив, 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 служб Active Directory (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.

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.

6.10.3. 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 (рис. 121).

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 защиты данных;

– Сканер уязвимостей;

– Модуль контроля USB.

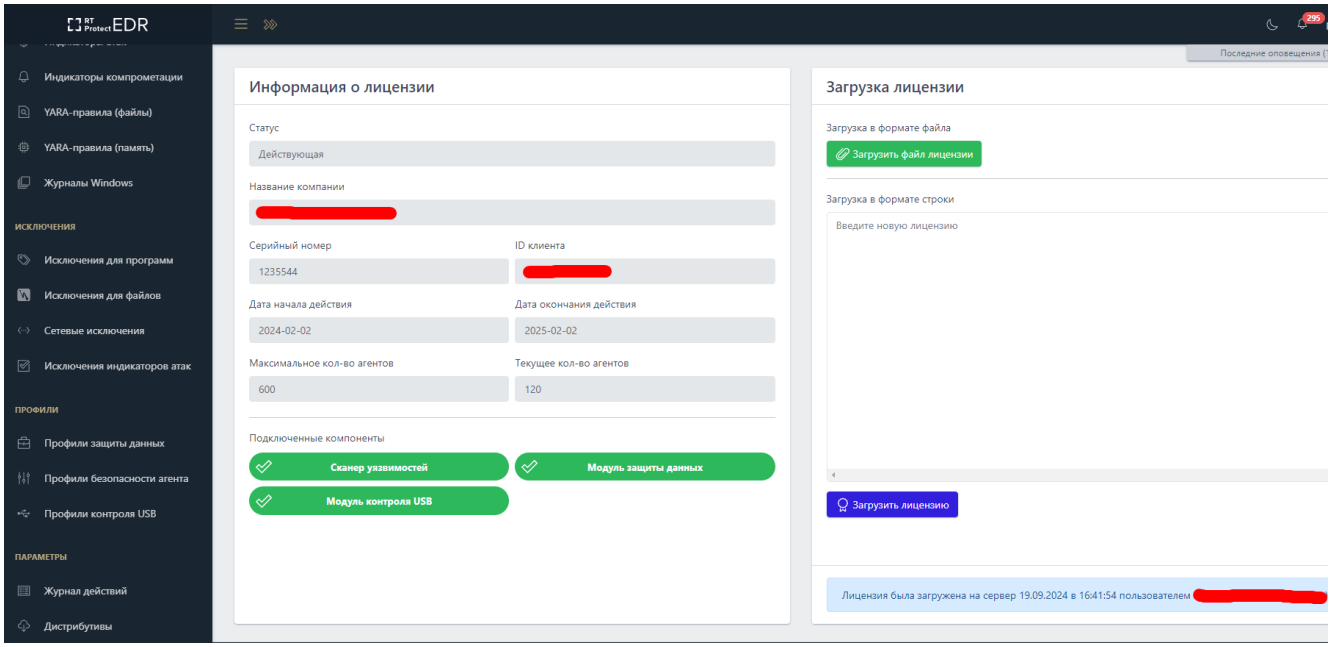


Рисунок 121 – Раздел «Лицензия»

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);

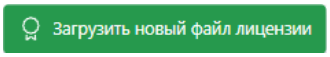
5) Дата начала действия лицензии;

6) Дата окончания действия лицензии;

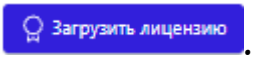
7) Максимальное количество агентов;

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 защиты данных, 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. 122).

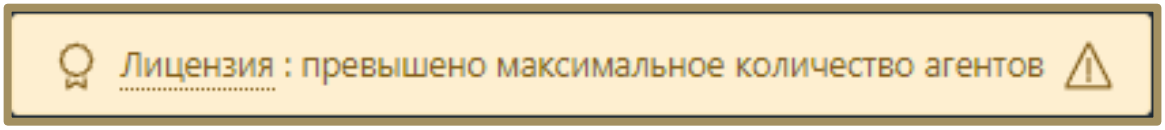


Рисунок 122 – Сообщение о превышении числа агентов

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).

Примечание

1) 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);

2) 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);

3) Если лицензия отсутствует, то и функционал подключаемых компонентов недоступен (аналогично, в сайдбаре видно, что компонент есть, просто необходимо купить лицензию с этим модулем).

6.11 Особенности работы Программы с антивирусными средствами сторонних производителей

6.11.1. 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 будем называть 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

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

6.11.2. Особенности выполнения действия блокирования для антивирусных решений.

В некоторых случаях к заблокированному модулю процесса может обращаться антивирусное средство. Для того, чтобы это было возможно, в Программе предусмотрено внутреннее исключение, которое создает событие для подобного обращения. То есть, если событие блокирования возникает в контексте антивирусного процесса (такие процессы отмечаются в системе флагом AVEngine), то блокирующее действие переопределяется на **Продолжать наблюдение** и критичность события сбрасывается на уровень **Информация**, при этом в причине события указывается **Исключение для программ**. Такая логика характерна для всех аналитических правил, кроме файловых исключений.

7. Машинное обучение в Программе

7.1 Классификация на сервере

В RT Protect EDR реализован статистический 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. 123). 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.

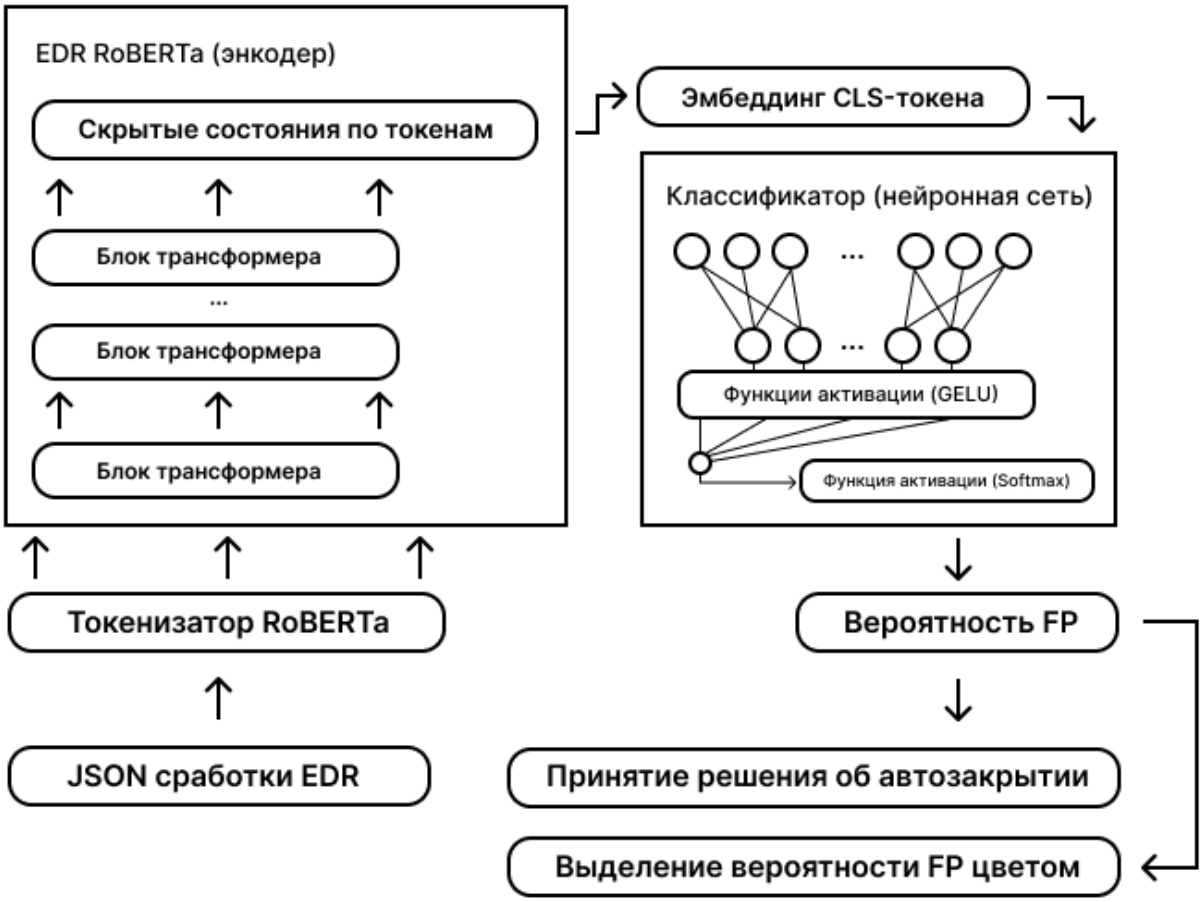


Рисунок 123 – Схема применения модели классификации инцидентов

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 содержит 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.

7.2 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. 124).

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 оверелея, 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.

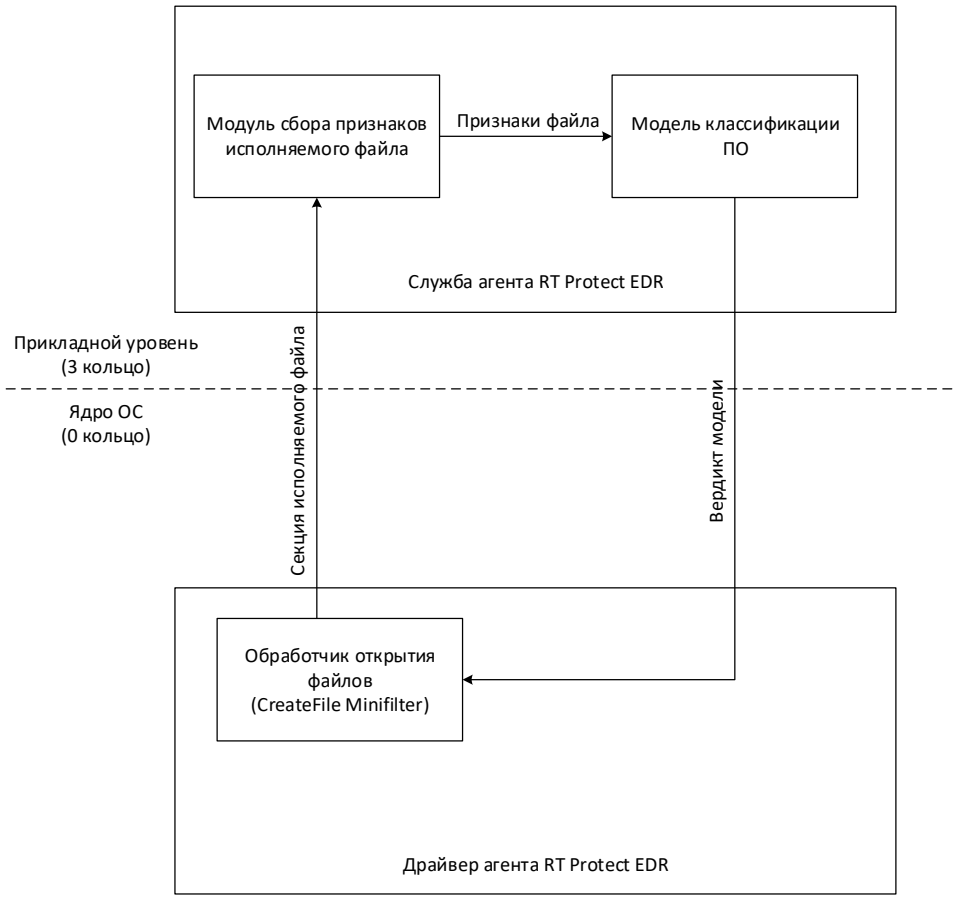


Рисунок 124 – Схема применения модели классификации ПО

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. Это 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 sklearn. В качестве обучающих выборок используется 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.

7.3 Список компонентов, используемых в модели ИИ

Полный список сторонних компонентов, используемых в модели машинного обучения, приведен в таблице 9.

Таблица 9 – Сторонние компоненты

№ п/п	Наименование стороннего компонента	Правообладатель	Сведения о документах, подтверждающих наличие оснований на использование компонента	Лицензии	Видлицензии
1	scikit-le	The scikit-learn developers		BSD 3-C	Свобод

	arn			License	наялицензия
2	pytorch	Facebook, Inc, Idiap Research Institute, Deepmind Technologies, NEC Laboratories America, NYU	https://github.com/pytorch/pytorch/blob/main/LICENSE	BSD-Style	Своднаялицензия
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	BSD3-Clause	Своднаяли

					ценз ия
4	numpy			numpy	Свободная лицензия
5	transformers	The Hugging Face team	https github	Apache License 2.0	Свободная лицензия

					ия
6	fastapi	Sebastián Ramírez	https://github.com/tiangolo/fastapi	MIT	Свободная лицензия
7	uvicorn	Encode OSS Ltd.	https://github.com/encode/uvicorn	BSD-3-Clause	Свободная лицензия
8	joblib		ht	BSD	Сво

				3-Clause	бодная лицензия

8. Проверка Программы

8.1 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.**

8.2 Контроль целостности исполняемых файлов и файлов конфигурации

Каждый компонент Программы содержит ЭЦП. Проверка ЭЦП компонентов агента осуществляется серверной частью автоматически.

9. Сообщения администратору

9.1 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.

9.2 Сообщения об ошибках

Можно выделить два типа сообщений об ошибках:

1) Общие сообщения – выводятся в приложении в том случае, если возникшая ошибка не была обработана специальным образом, и использовался общий обработчик;

2) Специфичные сообщения – выводятся в конкретных местах приложения и содержат детальное описание ошибки.

9.2.1. Общие сообщения

Общие сообщения – универсальные сообщения, которые выводятся в тех ситуациях, когда ошибка была обработана особенным образом. 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 125.

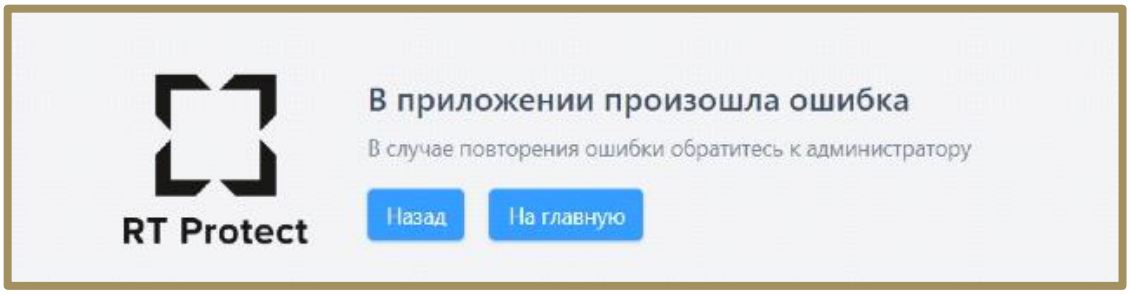


Рисунок 125 – Сообщение об ошибке типа «Экран ошибки»

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 126.

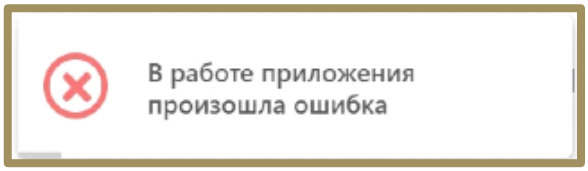


Рисунок 126 – Всплывающее сообщение об ошибке

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.

9.2.2. Специфичные сообщения

Ниже приведен список специфичных сообщений, разделенных по соответствующим страницам модуля администрирования.

Страница «Администрирование»

1) Ошибка при удалении пользователя (выводимое сообщение «Ошибка при удалении пользователя» представлено на рисунке 127).

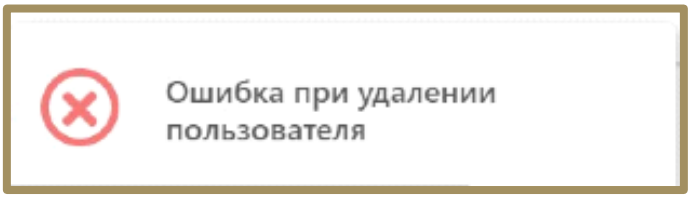


Рисунок 127 – Ошибка при удалении пользователя

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 128).

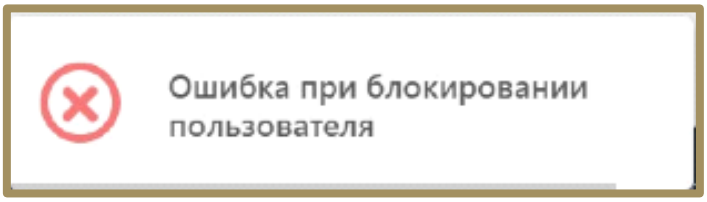


Рисунок 128 – Ошибка при блокировании пользователя

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 129).

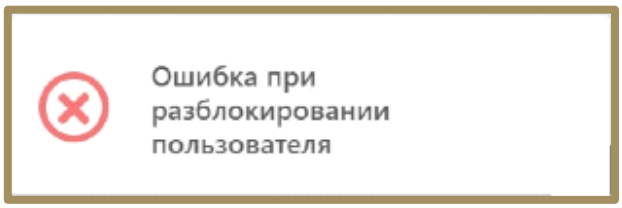


Рисунок 129 – Ошибка при разблокировании пользователя

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 130).

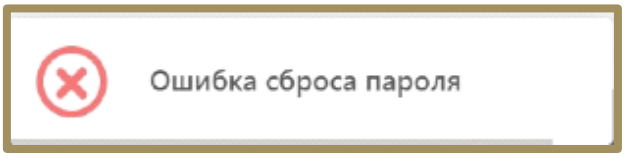


Рисунок 130 – Ошибка сброса пароля

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 131.

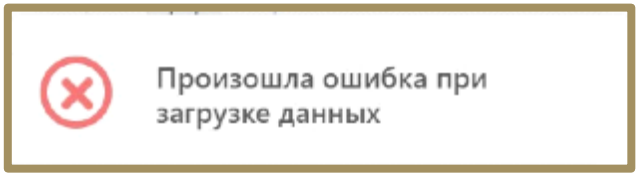


Рисунок 131 – Ошибка при загрузке данных

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 132.

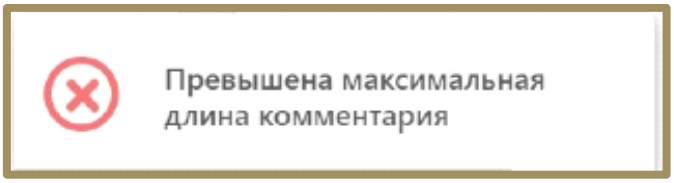


Рисунок 132 – Превышена максимальная длина комментария

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 133.

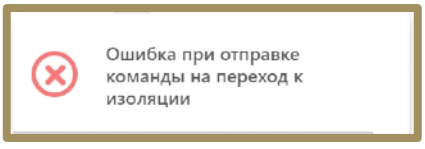


Рисунок 133 – Ошибка при отправке команды на переход к изоляции

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 134.

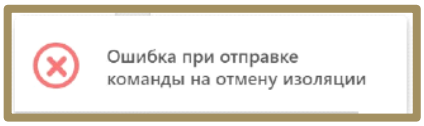


Рисунок 134 – Ошибка при отправке команды на отмену изоляции

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 135.

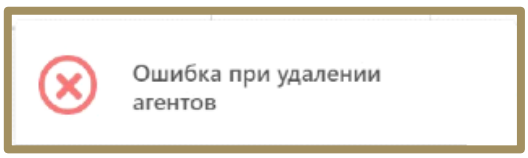


Рисунок 135 – Ошибка при удалении агентов

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 136.

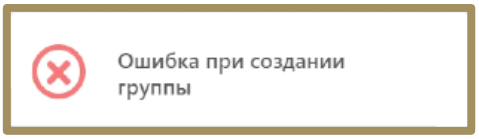


Рисунок 136 – Ошибка при создании группы

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 137.

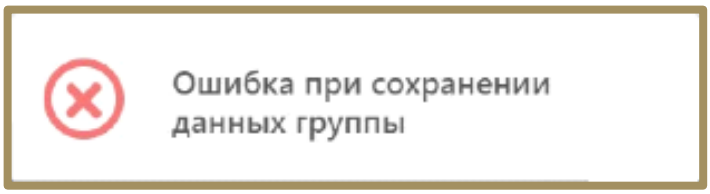


Рисунок 137 – Ошибка при сохранении данных группы

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 138.

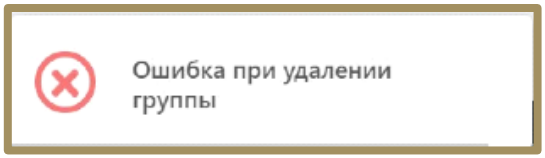


Рисунок 138 – Ошибка при удалении группы

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 139.

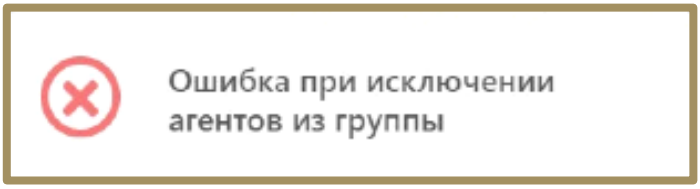


Рисунок 139 – Ошибка при исключении агентов из группы

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 140.

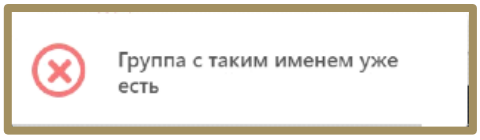


Рисунок 140 – Группа с таким именем уже есть

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 141.

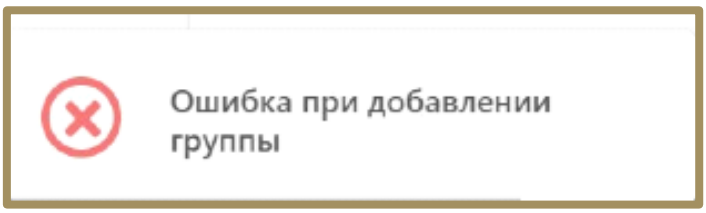


Рисунок 141 – Ошибка при добавлении группы

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 142.

Рисунок 142 – 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 143.

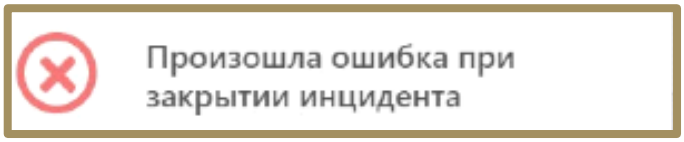


Рисунок 143 – Ошибка при закрытии инцидента

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 144.

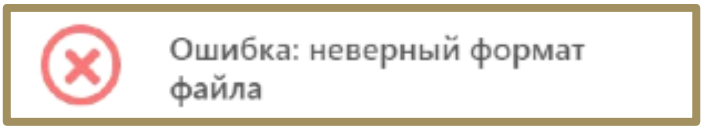


Рисунок 144 – Не верный формат файла

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 145.

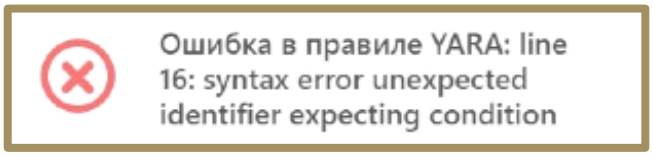


Рисунок 145 – Ошибка в правиле YARA

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 146.

Рисунок 146 – 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 147.

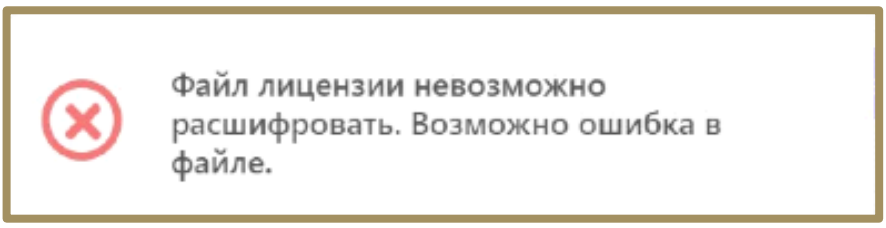


Рисунок 147 – Ошибка в файле лицензии

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 148.

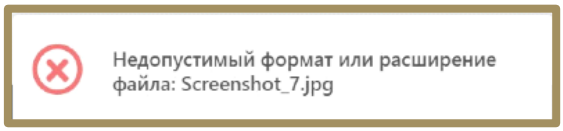


Рисунок 148 – Недопустимый формат или расширение

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 149.

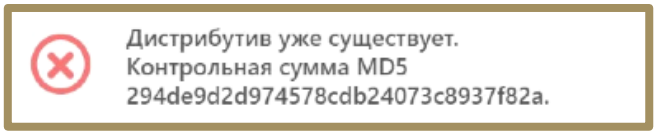


Рисунок 149 – Дистрибутив уже существует

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. 150).

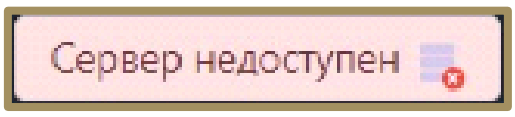


Рисунок 150 – Ошибка соединения с сервером

10. Процедура обновления программного обеспечения

10.1 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 10.

Потребитель 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-Информационная безопасность».

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 потребитель 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 10 – 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	Потребитель 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;

– www.rt-protect.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-разработчика www.rt-protect.ru;

2) Уведомление потребителя о выходе обновлений электронным письмом.

3) Получение потребителем информации о выходе обновлений через службу технической поддержки предприятия-разработчика 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 средств проверки контроля целостности.

Перед установкой новой версии Программы или пакетов обновлений необходимо осуществить вычисление КС загруженных файлов и проверить их соответствие эталонным.

10.2 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 "безшовно" (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 6.10.2), после чего перенести дистрибутив на защищаемый узел и установить агента, следуя инструкции установщика.

10.3 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. Разработчик 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.

10.4 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.

11. Действия после сбоя и ошибки

11.1 Общие сведения

Большинство ошибок можно разделить на следующие типы:

1) Ошибки конфигурации:

– некорректные настройки параметров безопасности;

– некорректная установка компонентов Программы;

– некорректные действие 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.

11.2 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».

11.3 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.

11.4 Контроль установки обновления

Критерием правильности установки обновления программного обеспечения является доступность интерфейса Программы и отображение информации о новой версии Программы (см. подраздел 6.1).

12. Перечень сокращений

Основные сокращения, указанные в документе, представлены в таблице 11.

Таблица 11 – Перечень сокращений

АРМ	Автоматизированное рабочее место
ЗБ	Задание по безопасности
ИС	Информационная система
ИТ	Информационная технология
ЛКМ	Левая кнопка мыши
ОО	Объект оценки
ОС	Операционная система
ОУД	Оценочный уровень доверия
ПЗ	Профиль защиты
ПКМ	Правая кнопка мыши
ПО	Программное обеспечение
САВЗ	Система антивирусной защиты
СОВ	Система обнаружения вторжений
УК	Управление конфигурацией
ФСТЭК	Федеральная служба по техническому и экспортному контролю
ЦП	Центральный процессор
APT	Advanced Persistent Threat (постоянная серьезная угроза)
CORS	Cross-Origin Resource Sharing (совместное использование ресурсов между разными источниками)
EPS	Events Per Second
ID	Identifier (идентификатор)
IT	Information Technology (информационные технологии)
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)
TGS	Ticket Granting Server (служба выдачи билетов)

Цитирование документа допускается только со ссылкой на настоящее руководство. Руководство не может быть полностью или частично воспроизведено, тиражировано или распространено без разрешения АО «РТ-Информационная безопасность».