RT Protect EDR

Руководство по установке и эксплуатации для администратора

Версия 1.0.10 от 18 сентября 2023
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 Администратора
Версия документа	Версия 1.0.7
Идентификация программы	СОВ «RT Protect EDR»
Идентификация разработчика	АО «РТ-Информационная безопасность»
Уровень доверия	Оценочный уровень доверия 3 (ОУД3), усиленный компонентами ADV_IMP.2 «Реализация функций безопасности объекта оценки (ФБО)», ADV_LLD.1 «Описательный проект нижнего уровня», ALC_FLR.1 «Базовое устранение недостатков», ALC_TAT.1 «Полностью определенные инструментальные средства разработки», AVA_VLA.3 «Умеренно стойкий» и расширенный компонентами ALC_UPI_EXT.1 «Процедуры обновления базы решающих правил» и AMA_SIA_EXT.3 «Экспертиза анализа влияния обновлений базы решающих правил на безопасность ОО». Оценочный уровень доверия 3 (ОУД3), усиленный компонентами ADV_FSP.4 «Полная функциональная спецификация», ADV_IMP.2 «Полное отображение представления реализации ФБО», ADV_TDS.3 «Базовый модульный проект», ALC_CMC.4 «Поддержка генерации, процедуры приемки и автоматизация», ALC_FLR.1 «Базовое устранение недостатков», ALC_TAT.1 «Полностью определенные инструментальные средства разработки», AVA_VAN.5 «Усиленный методический анализ», расширенный компонентами ADV_IMP_EXT.3 «Реализация ОО», ALC_FPU_EXT.1 «Процедуры обновления программного обеспечения межсетевого экрана» и AMA_SIA_EXT.3 «Анализ влияния обновлений на безопасность межсетевого экрана»

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.
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, ОУД3

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

Термин	Описание
Дерево процесса	Графическое отображение взаимосвязи процесса-родителя и дочернего процесса
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)
Нити (Threads)	Наименьшая единица обработки, исполнение которой может быть назначено ядром операционной системы. Реализация потоков выполнения и процессов в разных операционных системах отличается друг от друга, но в большинстве случаев поток выполнения находится 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
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

Термин	Описание
Хост	Электронно-вычислительная машина, являющаяся конечной точкой вычислительной сети. В узком смысле хост – это любое устройство, предоставляющее сервисы формата «клиент-сервер» в режиме сервера по каким-либо интерфейсам и уникально определённое на этих интерфейсах
Эвристический анализ	Совокупность функций антивируса, нацеленных на обнаружение неизвестных вирусным базам вредоносных программ. Термин обозначает и один из конкретных способов
Энтропия	Статистический параметр, который показывает вероятность встречаемости определённых байтов в файле
Active Directory	Иерархически организованное хранилище данных об объектах сети, обеспечивающее удобные средства для поиска и использования этих данных. Компьютер, на котором работает Active Directory, называется контроллером домена. С Active Directory связаны практически все административные задачи
Alerts	Оповещение об атаке на защищаемую инфраструктуру
Ansible	Система управления конфигурациями, написанная на языке программирования Python, с использованием декларативного языка разметки для описания конфигураций. Применяется для автоматизации настройки и развёртывания программного обеспечения
APT-атака	Термин кибербезопасности, означающий 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
CSRSS	Клиент-серверная подсистема времени выполнения
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.

Термин	Описание
Dfsrs	Утилита, которая используется для распределенной репликации файлов в ОС Windows
DismHost	Процесс обслуживания образов развертывания и управления ими. Утилита, которая используется для обслуживания образа Windows и исправления различных ошибок, связанных с файлами образов Windows
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
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
ICACLS	Утилита Windows, которая позволяет отображать или изменять списки управления доступом (Access Control Lists (ACLs) к файлам и папкам файловой системы
Imphash	Хеш импортируемых библиотек
Informational alerts	Оповещения о событиях, прямо не угрожающих безопасности инфраструктуры
Inhibit System Recovery	Техника атаки по методологии MITRE, которая предполагает отключение служб, отвечающих за восстановление операционной системы
Int	Целочисленный тип данных, один из простейших и самых распространённых типов данных в языках программирования. Служит для представления целых чисел

Термин	Описание
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
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
Parent PID Spoofing	Техника атаки, предполагающая манипуляции с токеном доступа процесса

Термин	Описание
Powershell.exe	Утилита для запуска инфраструктуры управления конфигурацией и автоматизации задач Microsoft. Инфраструктура Powershell состоит из оболочки командной строки и связанного языка сценариев
Powershell_ise.exe	Интегрированная среда сценариев (ISE) Windows PowerShell. Графическое приложение, позволяющее читать, писать, выполнять, отлаживать и тестировать сценарии и модули в среде с графическим интерфейсом
Prefetcher	Компонент операционной системы Microsoft Windows, ускоряющий процесс её начальной загрузки, а также сокращающий время запуска программ
Pwsh.exe	Новое имя утилиты Powershell.exe, начиная с версии 6
Sophos	Производитель средств информационной безопасности для настольных компьютеров, серверов, мобильных устройств, почтовых систем и сетевых шлюзов
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
Timestamp	Последовательность символов или закодированной информации, показывающей, когда произошло определённое событие. Обычно показывает дату и время
TiWorker	Штатный процесс ОС Windows, отвечающий за работу модуля поиска и инсталляции обновлений в скрытом режиме
TLSH	Вероятностный алгоритм хеширования
TrustedInstaller	Служба Windows для установки модулей, работающая по технологии Windows Resource Protection. Служба отвечает за безопасность доступа к системным файлам
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

Термин	Описание
UUID	Стандарт идентификации, используемый в создании программного обеспечения, стандартизированный Open Software Foundation (OSF) как часть DCE – среды распределённых вычислений. Основное назначение UUID – это позволить распределённым системам уникально идентифицировать информацию без центра координации
VirusTotal	Бесплатная служба, осуществляющая анализ подозрительных файлов и ссылок (URL) на предмет выявления вирусов, червей, троянов и всевозможных вредоносных программ
Web-сервер	Сервер, принимающий HTTP-запросы от клиентов, чаще всего веб-браузеров, и выдающий HTTP-ответы, как правило, вместе с HTML-страницей, изображением, файлом, медиа-потоком или другими данными
WHOIS	Сетевой протокол прикладного уровня, базирующийся на протоколе TCP. Основное применение – получение регистрационных данных о владельцах доменных имён, IP-адресов и автономных систем
Windows	Группа семейств коммерческих операционных систем корпорации Microsoft, ориентированных на управление с помощью графического интерфейса
WMI	Инструментарий управления Windows. Одна из базовых технологий для централизованного управления и слежения за работой различных частей компьютерной инфраструктуры под управлением платформы Windows

1.4 Условные обозначения

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

Таблица 3 – Условные обозначения

Обозначение	Описание
ПРОПИСНЫЕ БУКВЫ	Акронимы, аббревиатуры
«Times New Roman»	Названия документов, команд, каталогов, файлов и т.д.
Жирный шрифт	Подписи таблиц, рисунков, названия разделов, подразделов, пунктов и подпунктов, название кнопок меню модуля администрирования программы
	Обозначения кнопок меню, операций модуля администрирования программы
Times New Roman/Times New Roman	Перечисление альтернативных вариантов, путь меню, путь файла
	Информация, требующая внимания пользователя
	Информация, связанная с важными конфигурационными настройками и особенностями работы EDR
	Рекомендации и предположения, которые могут помочь в работе с EDR

2. Общие сведения

2.1 Назначение и архитектура программы

Система обнаружений вторжений «RT Protect EDR» предназначена для защиты IT-инфраструктуры пользователей продукта от действий известных и неизвестных вредоносных программ, различного рода сложных и целевых атак как внешних, так и внутренних, в том числе, из сетей международного информационного обмена.

Основными функциями программы являются управление событиями безопасности и управление информацией о безопасности.

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.

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.

Все компоненты программы обладают следующими функциональными возможностями:

– осуществляют защиту (совместно с механизмами среды функционирования) собственной программной и информационной части от вмешательства;

– допускают настройку своих параметров со стороны администратора безопасности;

– ведут журнал аудита (в том числе осуществляют регистрацию попыток изменения конфигурации, а также попыток доступа к компонентам и данным).

2.3 Функциональные возможности в части антивирусной защиты

Программа обеспечивает следующие функциональные возможности в части САВЗ:

– проверки в файловых областях носителей информации с целью обнаружения зараженных КВ объектов;

– проверка с целью обнаружения зараженных КВ объектов по команде;

– проверка с целью обнаружения зараженных КВ объектов сигнатурными методами;

– получение и установка обновлений БД ПКВ без применения средств автоматизации;

– генерация записи аудита для событий, подвергаемых аудиту;

– чтение информации из записей аудита;

– ассоциация событий аудита с идентификаторами субъектов;

– ограничение доступа к чтению записей аудита;

– поиск, сортировка, упорядочение данных аудита;

– управление уполномоченными пользователями режимом выполнения функций безопасности программы;

– управление уполномоченными пользователями параметрами настройки функций безопасности программы;

– поддержка определенных ролей для программы и их ассоциация с конкретными администраторами безопасности и пользователями ИС.

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»	1	Поставляется по сети

	Комплект эксплуатационных документов согласно ведомости ЭД		

*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 20.04.5 LTS с ядром linux-5.15.0;

– Debian GNU/Linux 11 (bullseye) [Linux 5.10.0-19-amd64 x86_64];

– ОС Linux Ubuntu 18.04;

– Astra SE 1.7_x86-64;

– Red OS 7.3.

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 клиентской части

Архитектура агента системы предполагает наличие следующих основных функциональных компонентов:

– драйвер, работающий в режиме ядра системы;

– служба, работающая в режиме пользователя.

Схематично архитектура агента представлена на рисунке 1.

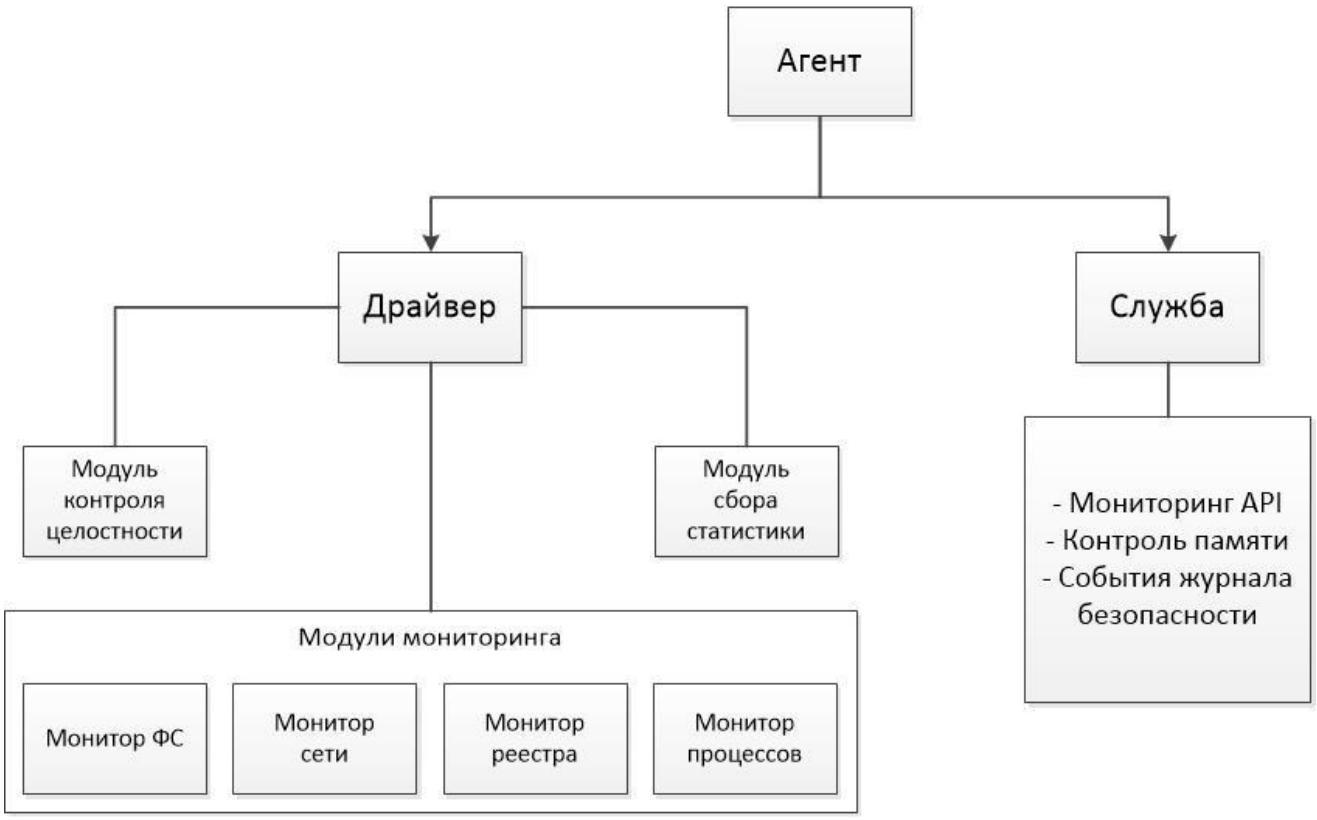


Рисунок 1 – Архитектура агента

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 серверной части

4.3.1. 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 2.

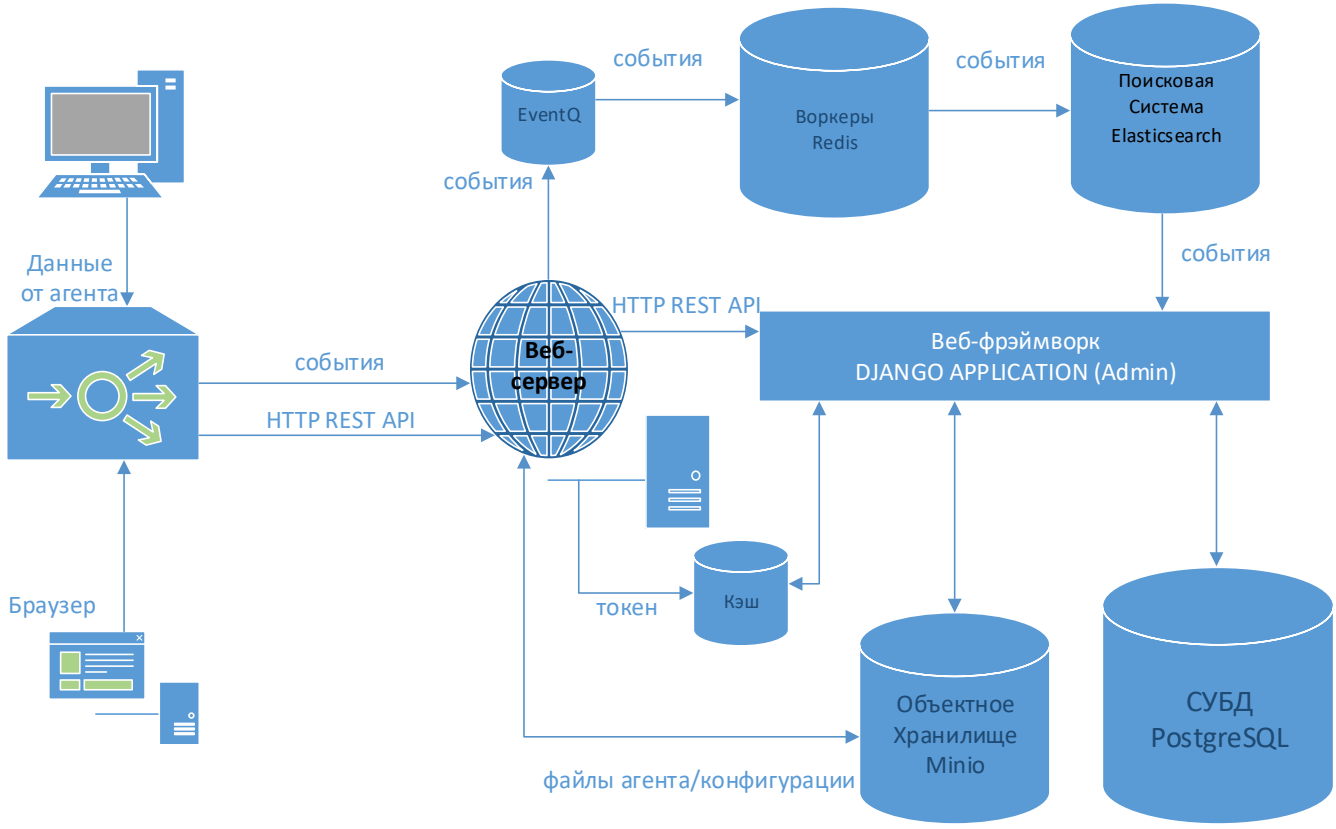


Рисунок 2 – Архитектура серверной части «RT Protect EDR»

4.3.2. 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 «RT Protect EDR» в Клиентской части (агент) работает на 64-х разрядной платформе Windows 7, 8, 8.1, 10, 11, на серверных версиях Win_Server_2008_R2x64, Win_Server_2012_R2x64, Win_Server_2016_x64, Win_Server_2019_x64, а также на различных версиях ОС Linux (Ubuntu 18.04, Ubuntu 20.04.5 LTS с ядром linux-5.15.0, Astra SE 1.7 _x86-64, Red OS 7.3, Debian GNU/Linux 11 (bullseye) [Linux 5.10.0-19-amd64 x86_64]). 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

Характеристики	Платформа 1 (клиентская часть)		Платформа 2 (серверная часть)	
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

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 3.

Рисунок 3 – 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 **Создать точку восстановления.**

5) Нажать кнопку **Установить,** после чего появится окно **Индексирование файлов** (рис. 4).

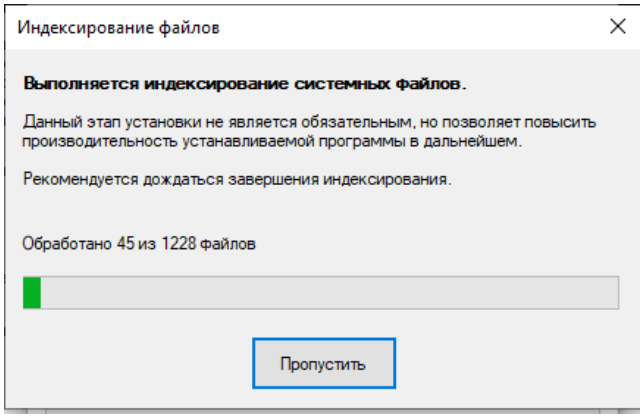


Рисунок 4 – Подтверждение установки

6) После окончания процесса установки появится информационное окно (рис. 5).

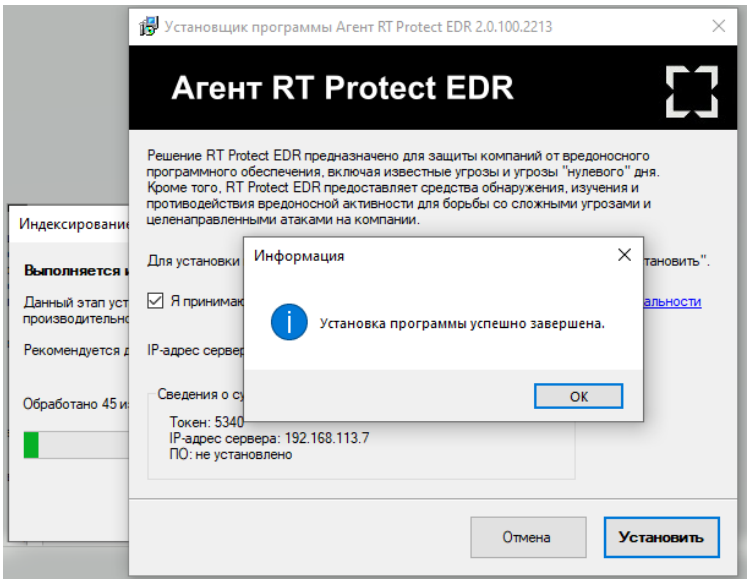


Рисунок 5 – Процесс установки

7) Нажать кнопку **ОК.**

8) После завершения всех процедур установки в правом углу экрана в системном трее появится иконка установленного агента (рис. 6).

Примечание

После завершения установки на диске С в папке Program Files создается папка **ИБ Реформ\Агент RT Protect EDR\.**

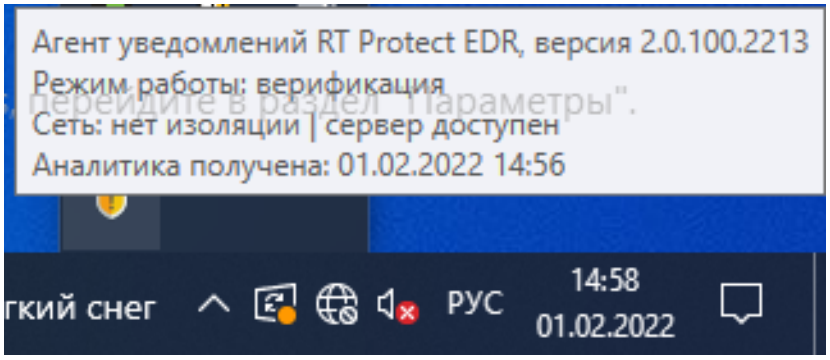


Рисунок 6 – Иконка установленного антивируса

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 7.

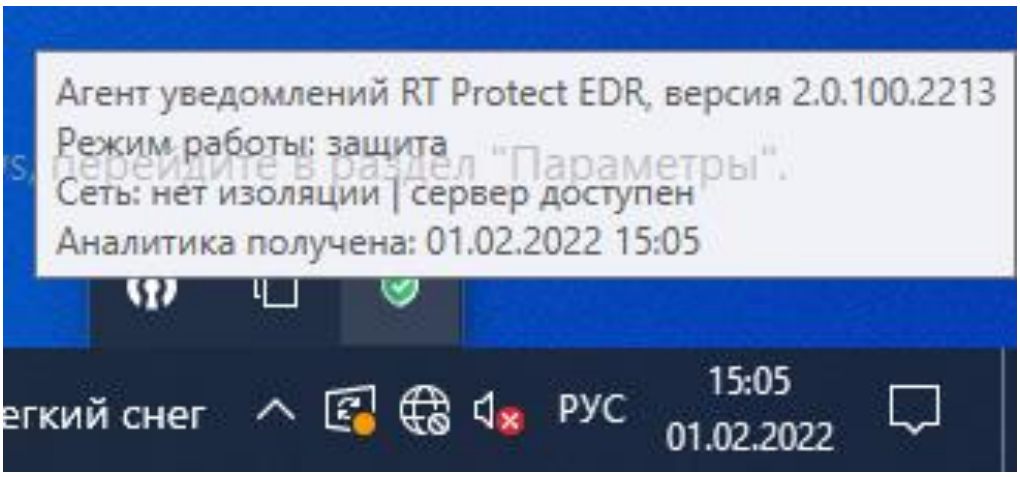


Рисунок 7 – Агент верифицирован

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
```

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 1.7 (поддерживаемые ядра):

– 5.10.142-1-generic;

– 5.15.0-33-generic;

– 5.4.0-110-generic;

– 5.4.0-54-generic.

2) Debian 11:

– 5.10.0-19-amd64;

3) Ubuntu 18.04:

– 4.15.0-163-generic

4) 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.

5) Ubuntu 22.04:

– 5.19.0-41-generic

6) RedOs 7.3:

– 5.10.29-3.el7.x86_64

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 18.04;

– Ubuntu 20.04;

– Debian GNU/Linux 11;

– Astra SE 1.7 _x86-64.

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

– Red OS 7.3.

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
```

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

```
sudo dnf install jansson-2.14-1.e17 .x86_64
sudo dnf install libev-4.33-1.e17. x86_64
```

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
```

4) 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
```

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=...
```

Запуск

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 должен появиться в списке верификации на сервере EDR.

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

Основные файлы (исполняемый модуль сервиса, динамические библиотеки, конфигурационные файлы) сохраняются в системе по пути:

/opt/avd/

Совет

Параметры работы сервиса агента могут быть заданы через конфигурационный файл:
/opt/avd/etc/avd.conf.

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 8.

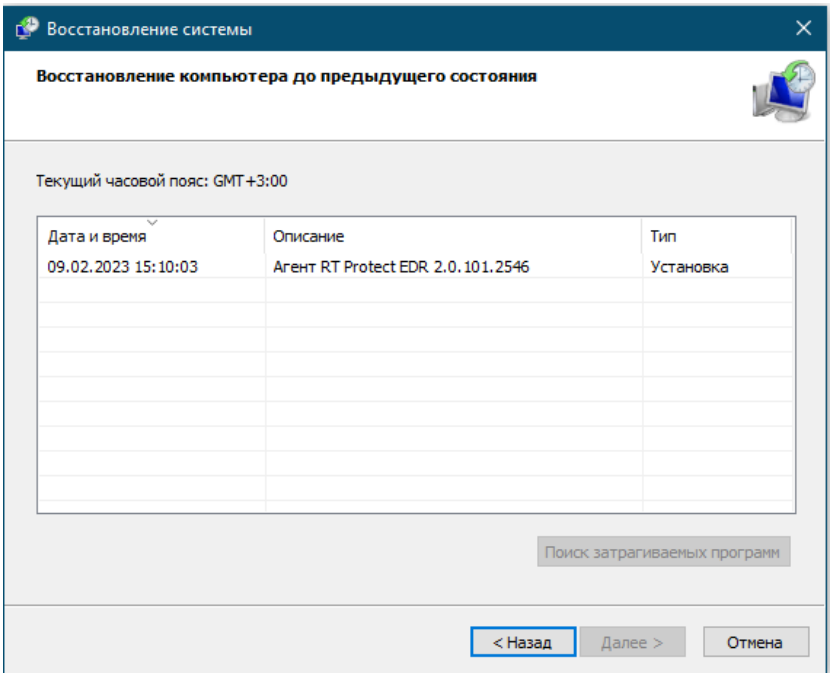


Рисунок 8 – Точка восстановления системы

5) Выбрать точку восстановления, созданную при установке агента EDR, выделив соответствующую строчку из списка. Появится окно, представленное на рисунке 9.

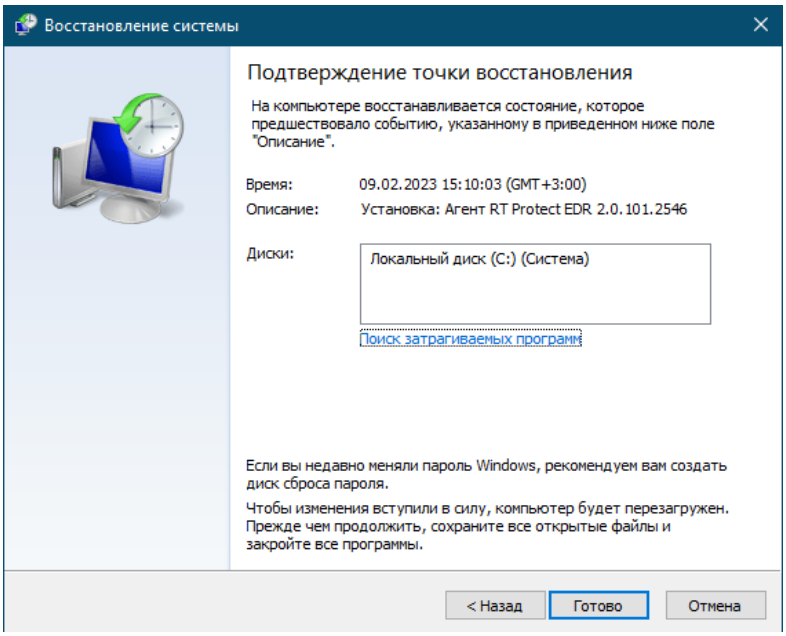


Рисунок 9 – Подтверждение точки восстановления

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/ИБ Реформ/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

Удаление Агента (в ОС Linux) с конечной точки можно произвести, набрав в терминале следующую команду:

sudo dpkg -r avd

Удаление Агента (в ОС RED OS) с конечной точки можно произвести, набрав в терминале следующую 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.

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]

С вашего компьютера должен быть доступ на сервер (***Docker-хост***) по SSH, а у удаленного пользователя 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 (https://docker.vr-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.vr-protect.ru/buckets/edr 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 10.

```
. (edr-deploy)
|
├── README.md
├── compose-files
|   ├── docker-compose.external-es.yml
|   ├── docker-compose.yml
|   ├── env.external-es.j2
|   └── env.j2
├── config
|   └── default
|       ├── config.yml
|       ├── docker-compose.override.yml
|       ├── server.crt
|       ├── server.htpasswd
|       └── server.key
├── edr-install.yml
└── edr-update.yml
```

Рисунок 10 – 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 11.

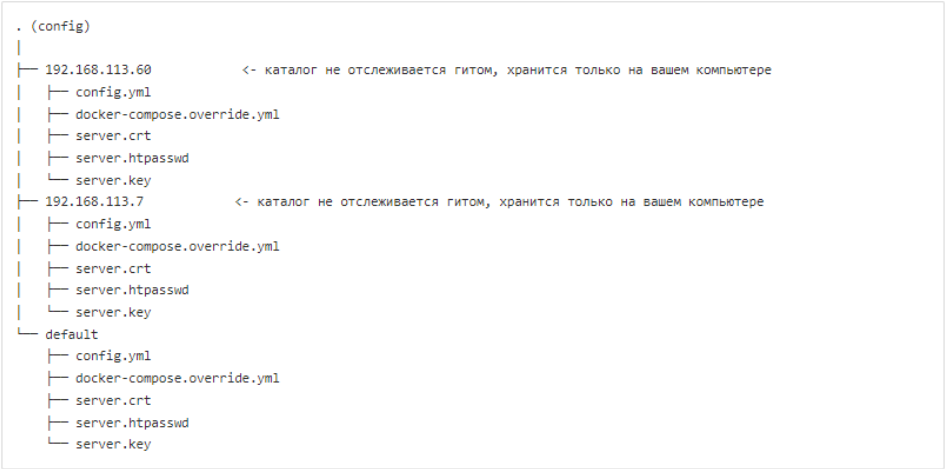


Рисунок 11 – Структура каталога config

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. 12).

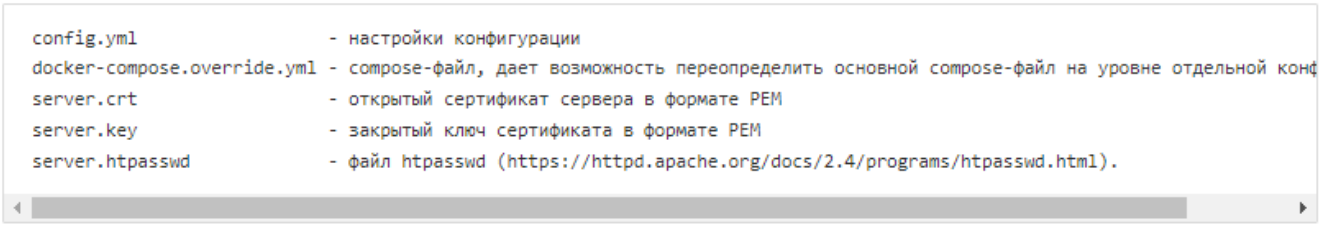


Рисунок 12 – Настройки каталога config по умолчанию

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).

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.

Примечание

Server.htpasswd нужен для предоставления внешнего доступа к Elasticsearch с использованием basic-аутентификации. Подобное не должно быть нужно в реальных проектах и несет опасность. Файл **server.htpasswd** нужен только в процессе разработки. Текущие конфигурации не разрешают внешний доступ к Elasticsearch в любом случае независимо от содержания файла **server.htpasswd**, так как порт 9200 (Elasticsearch) закрыт, и не пробрасывается на хост.

Важно

Файл server.htpasswd не нужно удалять или трогать его содержимое! Необходимо просто скопировать 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, хэши, 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.

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. 13).

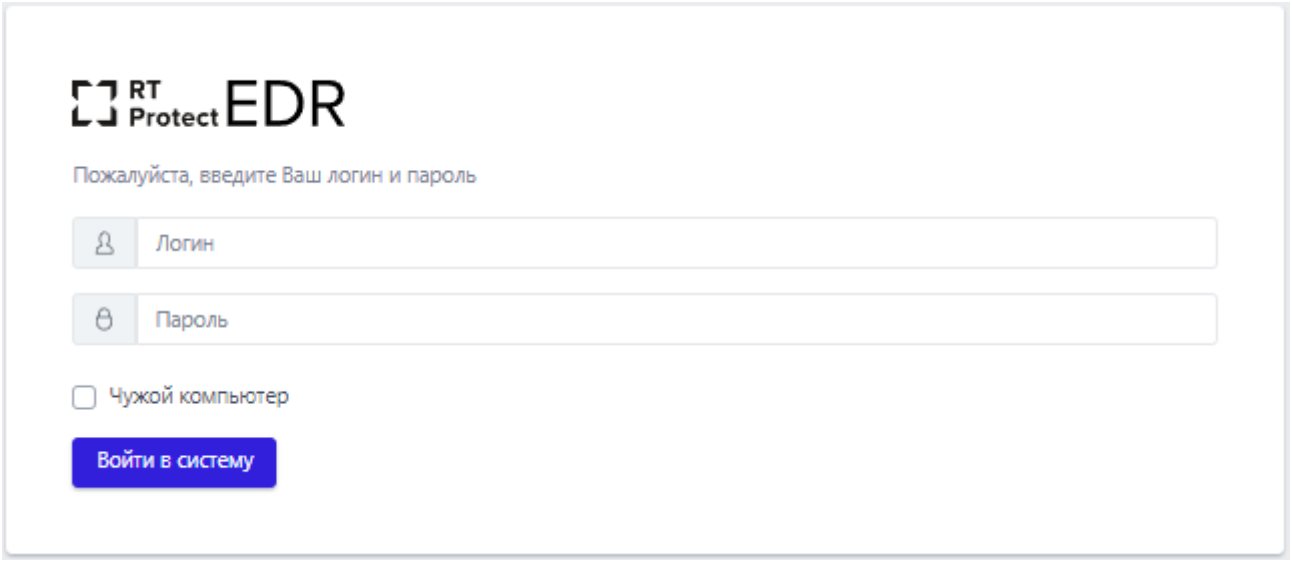


Рисунок 13 – Окно авторизации

После ввода в окне авторизации пароля и логина администратора открывается основное окно программы (рис. 14).

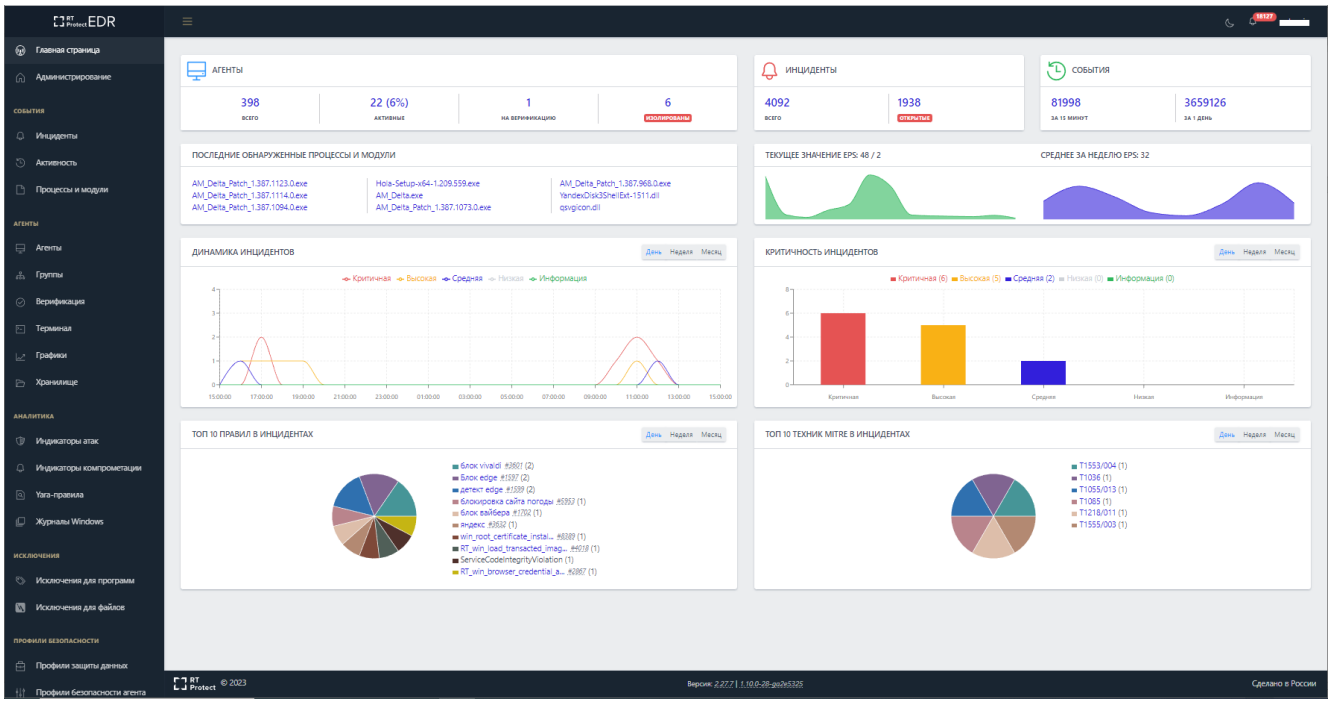


Рисунок 14 – Основное окно программы

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. 14) 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 – RT Protect © 2022.

В центре рядом с товарным знаком отображается текущая версия программы:

1) Frontend – Версия: 2.6.45;

2) Backend – 1.1.5-5-g048e161.

Справа от текущей версии программы отображается надпись о том, где «RT Protect EDR» разработана – Сделано в России.

6.2 Горизонтальная панель управления

В верхней части окна находится горизонтальная панель управления (рис. 15).

Рисунок 15 – Горизонтальная панель управления

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

При нажатии кнопки **Скрыть/показать панель разделов** ( ) основное окно программы приобретает вид, как показано на рисунке 16. Для возврата первоначального вида необходимо повторно нажать на кнопку .

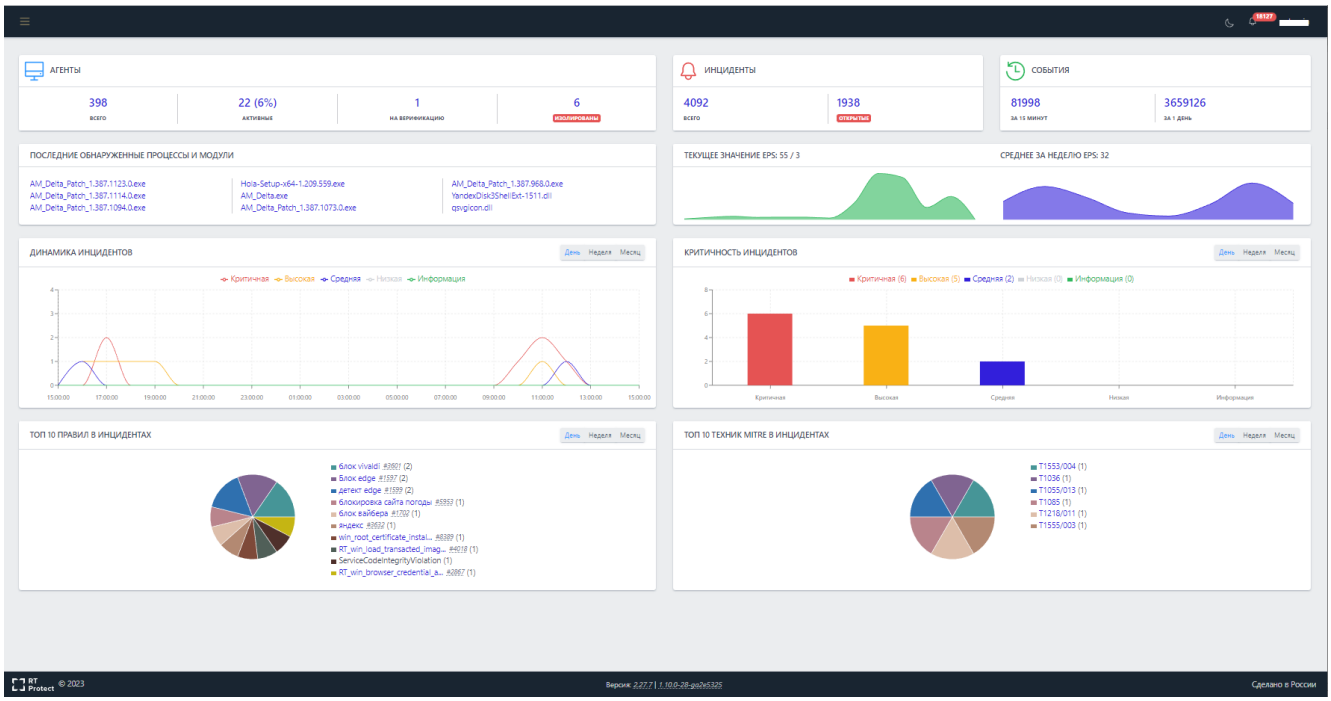


Рисунок 16 – Основное окно программы при скрытой панели разделов

При нажатии кнопки **Темная тема** () основное окно программы приобретает вид, как показано на рисунке 17. Для возврата первоначального вида необходимо нажать кнопку **Светлая тема (**  **)**.

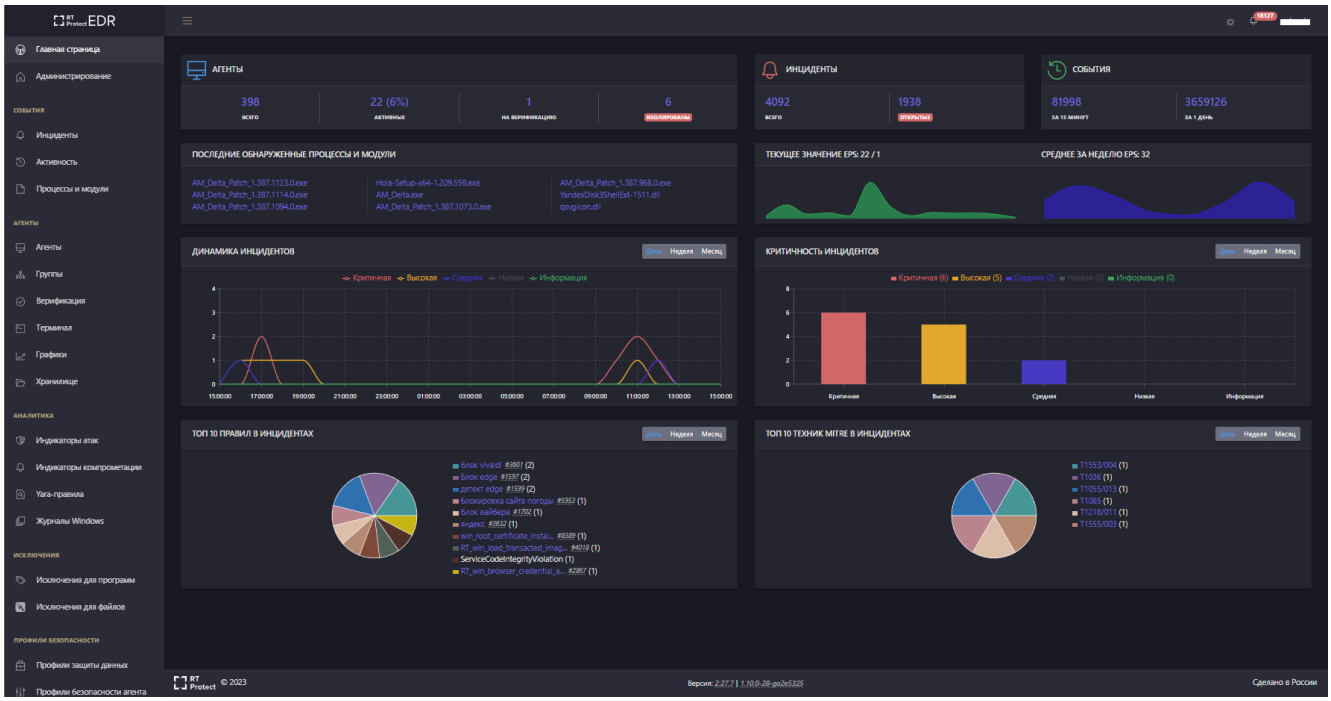


Рисунок 17 – Основное окно программы при выборе темной темы

6.2.1. Оповещения

Страница **Оповещения** является одной из основных страниц для работы аналитика безопасности, так как именно здесь аналитик может прочитать сводку с информацией об инцидентах.

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 (рис. 18).

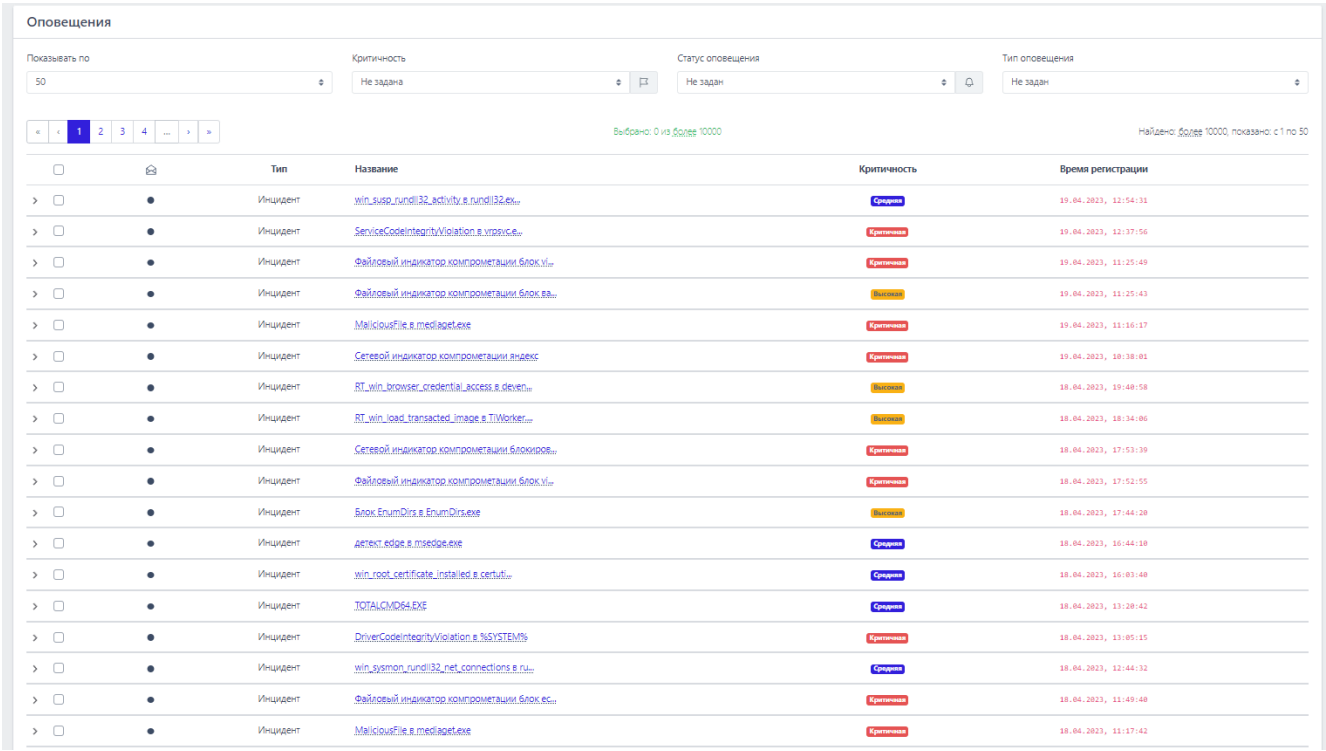


Рисунок 18 – Оповещения

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 или 100 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. 19).

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

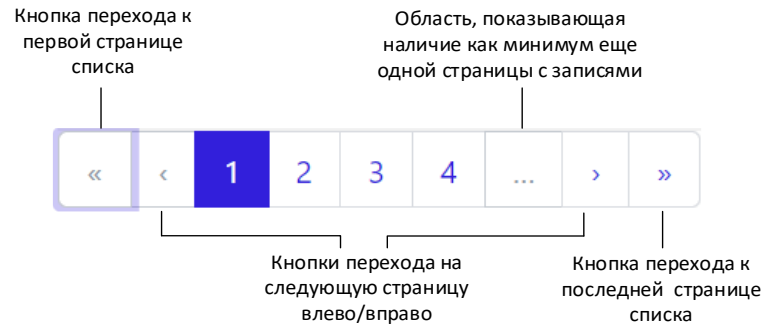


Рисунок 19 – Пагинатор

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».

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) **Не задан** – при выборе фильтра в таблице будут показаны все типы оповещений;

2) **Инцидент** – при выборе фильтра в таблице будут показаны оповещения об инцидентах.

Ниже строки с фильтрами находится строка с элементами навигации в таблицах (см. рис. 19). 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. В нижней части страницы во всплывающем окне появляется сообщение **Оповещения отмечены как прочитанные** (рис. 20).

Рисунок 20 – Сообщение о прочитанных оповещениях

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**. При нажатии кнопки Прочитать все появляется окно, представленное на рисунке 21.

После нажатия кнопки Выполнить все оповещения, показанные пользователю, будут отмечены как прочитанные, после чего в нижней части основного окна программы появится подтверждающее сообщение (см. рис. 20).

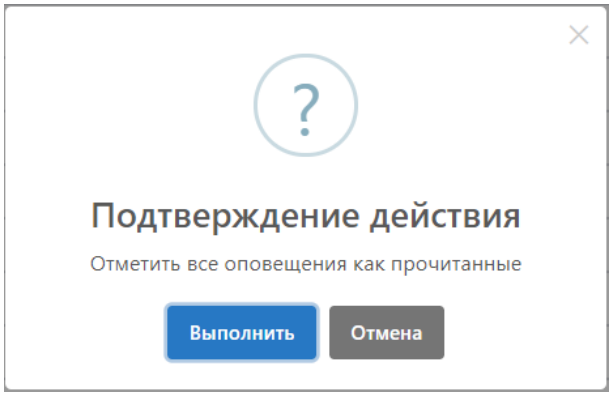


Рисунок 21 – Отметить все оповещения как прочитанные

Оповещения приходят в режиме реального времени. При появлении нового оповещения в верхней части основного окна программы появляется сообщение (рис. 22).

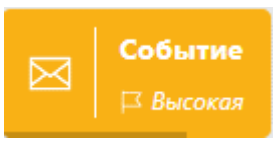


Рисунок 22 – Всплывающее окно с оповещением о событии

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

При выборе типа оповещения **Инцидент** в дополнительной информации отображаются только поля **Название (при создании)** и **Описание (при создании)** (рис. 23).

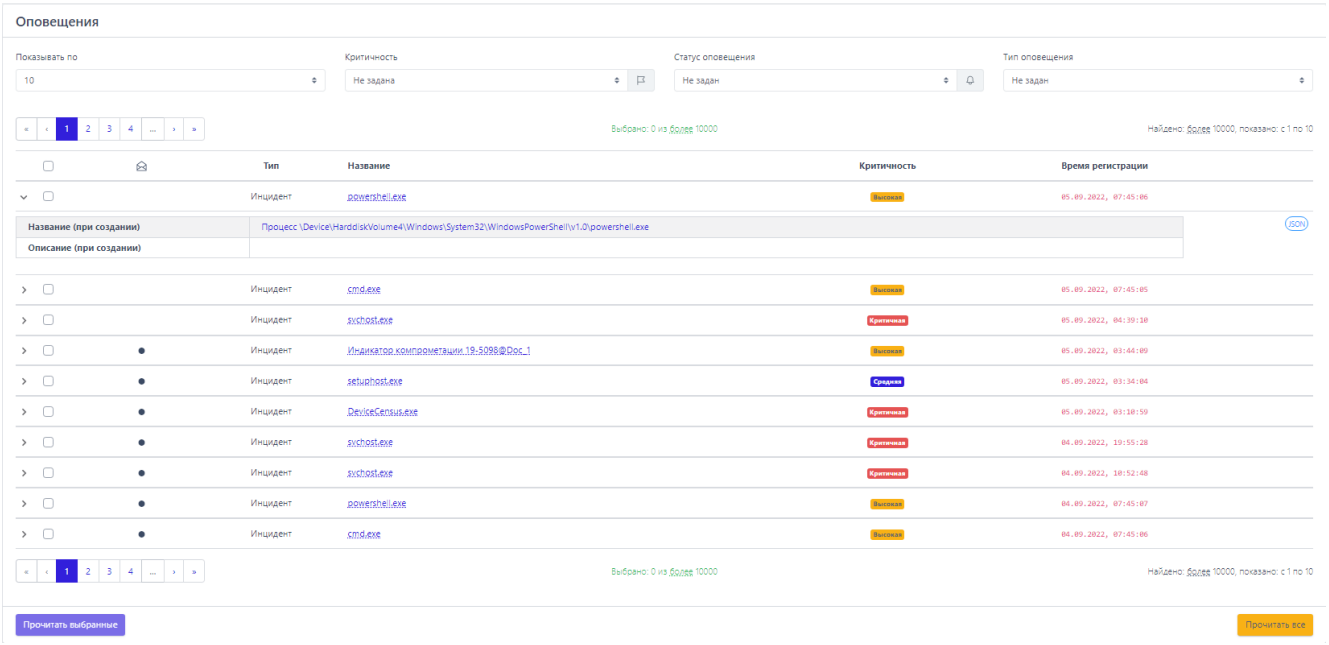


Рисунок 23 – Дополнительная информация в оповещении (инцидент)

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.

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. 24).

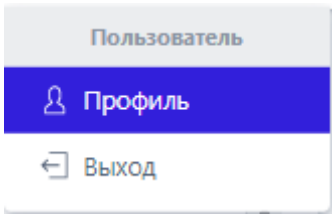


Рисунок 24 – Меню «Пользователь»

Подменю **Профиль** разделено на две информационные области: **Профиль** и **Сессии и устройства** (рис. 25).

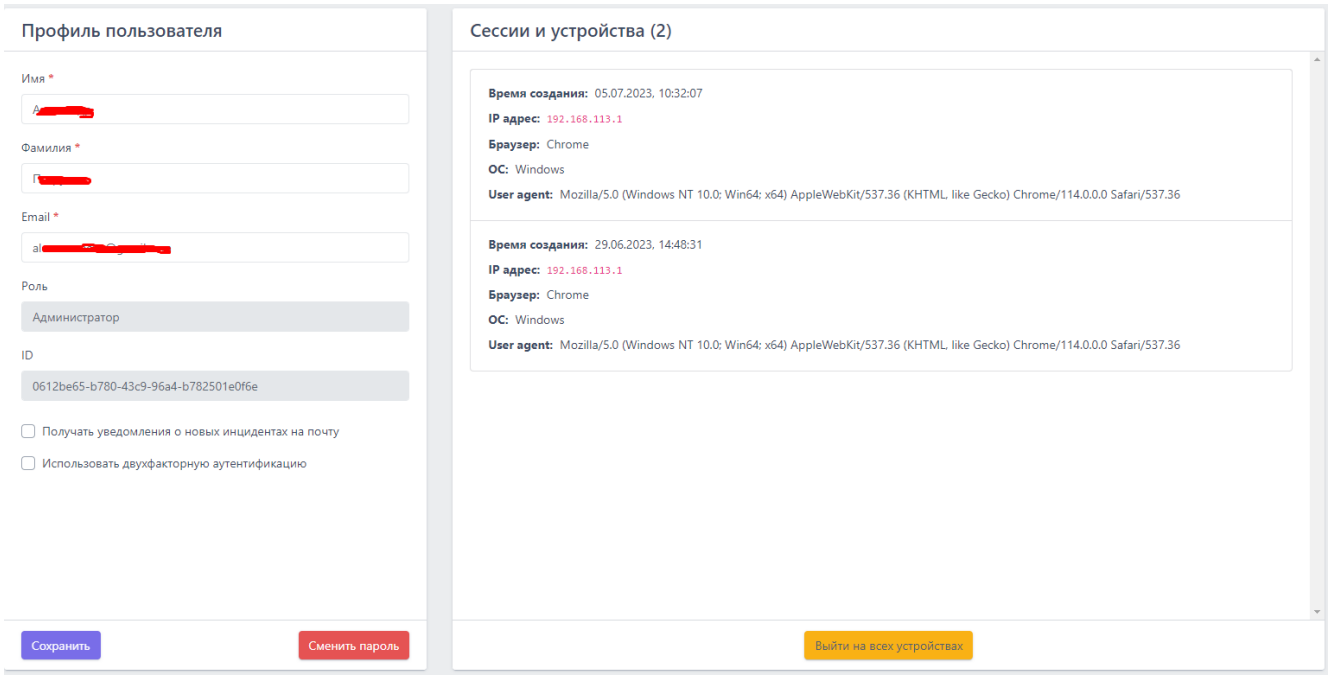


Рисунок 25 – Подменю «Профиль»

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. 26).

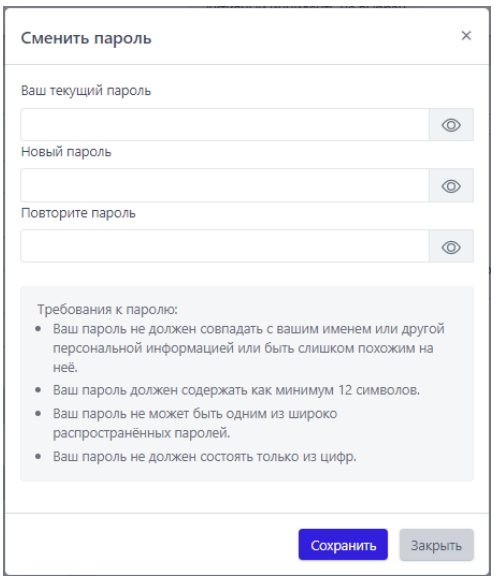


Рисунок 26 – Окно смены пароля

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 14 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**.

В области просмотра **Агенты** показывается состояние всех установленных агентов (рис. 27):

1) Общее число агентов;

2) Количество активных агентов;

3) Количество агентов, ожидающих верификацию;

4) Количество изолированных агентов.

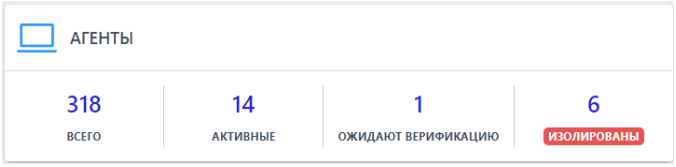


Рисунок 27 – Область информации «Агенты»

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 в поле слева и открытые инциденты, по которым отсутствует решение в поле справа (рис. 28). 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).

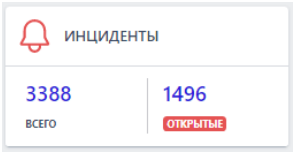


Рисунок 28 – Область информации «Инциденты»

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 (рис. 29).

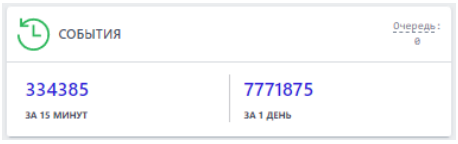


Рисунок 29 – Область информации «События»

В области просмотра **Последние обнаруженные процессы и модули** показываются последние программы, обнаруженные в защищаемой инфраструктуре (рис. 30).

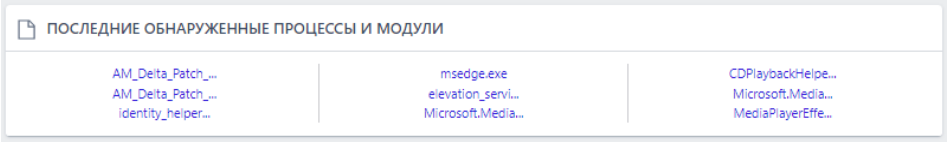


Рисунок 30 – Область информации «Последние обнаруженные процессы и модули»

При наведении указателя мыши на имя процесса появляется всплывающее окно с описанием полного пути до места обнаружения процесса/модуля (рис. 31).

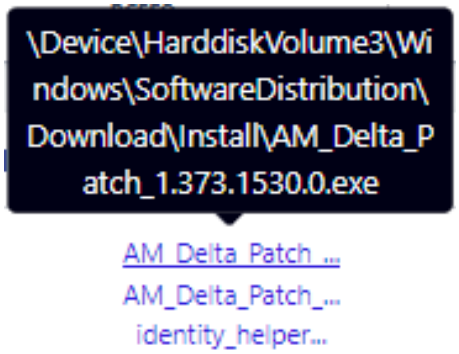


Рисунок 31 – Путь до обнаруженного процесса

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

В области **Текущее значение EPS** содержится интерактивный график, показывающий загруженность модуля администрирования (рис. 32). Отображается количество событий за секунду, приходящее от активных агентов.

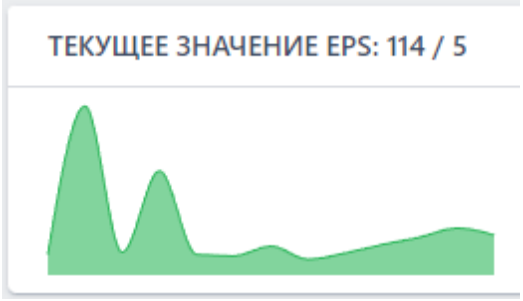


Рисунок 32 – Отображение текущего EPS на графике

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. 33).

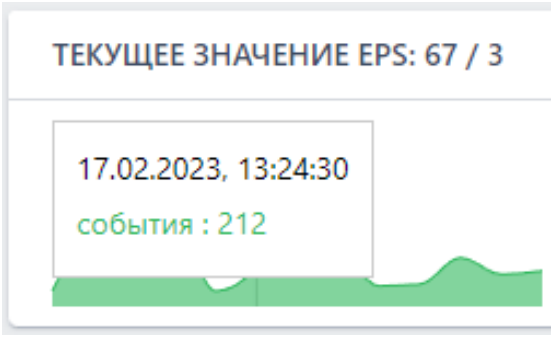


Рисунок 33 – Отображение EPS на графике с интервалом 5 сек

В области **Среднее за неделю EPS** отображается график и среднее за неделю количество событий в секунду для активных агентов (рис. 34).

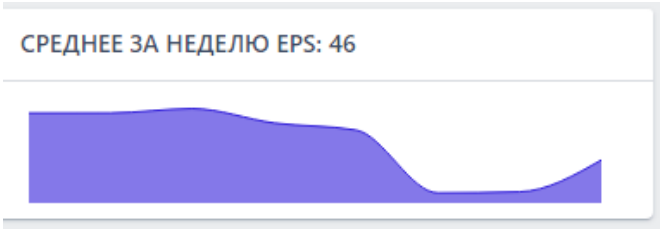


Рисунок 34 – Отображение среднего за неделю EPS на графике

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. 35).

Рисунок 35 – Отображение среднего за неделю EPS на графике в интервале 1 день

В области **Динамика инцидентов** (рис. 36) отображаются графики, на которых можно проследить динамику появления инцидентов по критичности за день, неделю либо за месяц.

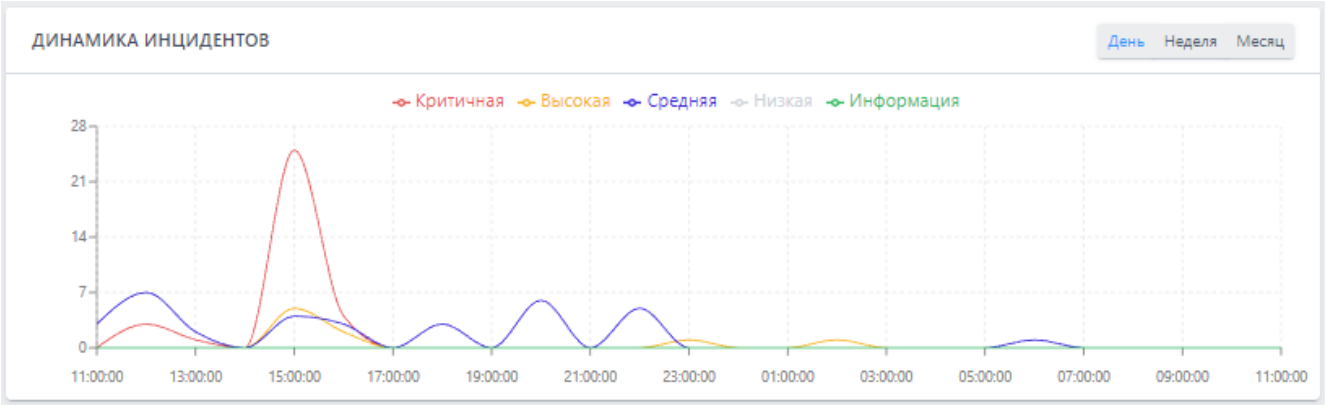


Рисунок 36 – Отображение динамики инцидентов по критичности с периодом 1 неделя

График разделен контрольными точками на отрезки с периодичностью в один день, при наведении указателя мыши на отрезок появляется всплывающее окно, показывающее количество инцидентов (рисунок 37).

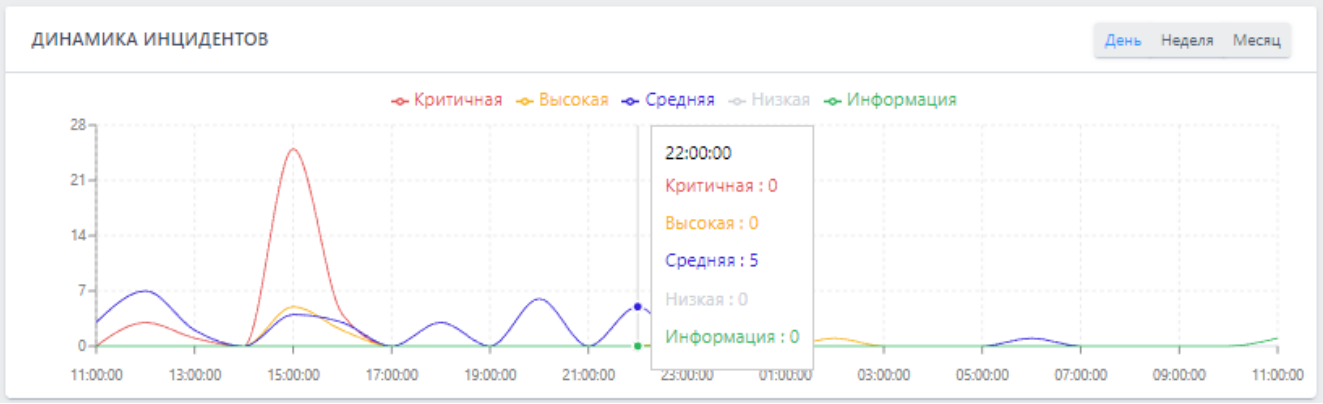


Рисунок 37 – Отображение количества инцидентов в определенный день

Динамику изменения инцидентов можно просмотреть за период день, неделя или месяц.

В области **Критичность инцидентов** (рис. 38) администратор может посмотреть в виде диаграмм распределение зарегистрированных инцидентов по степени критичности (с указанием количества), за день/неделю/месяц.

Рисунок 38 – Диаграмма распределения инцидентов по критичности

Записи критичности инцидентов являются активными ссылками, при нажатии по записи 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 (рисунок 39).

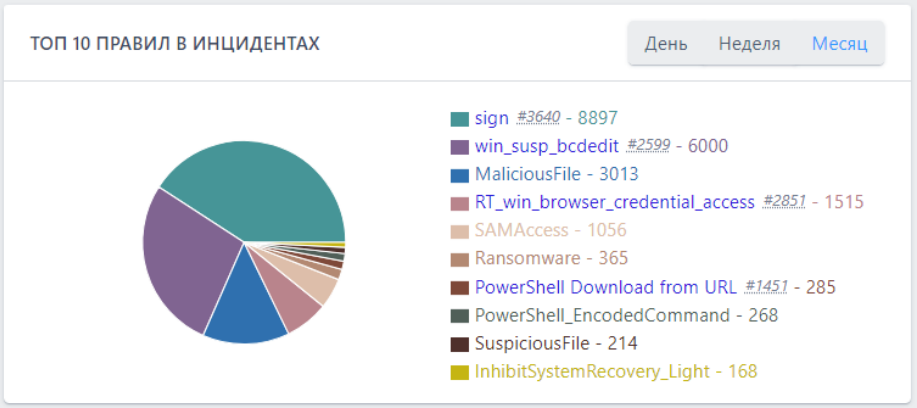


Рисунок 39 – Диаграмма отображения десяти основных правил при регистрации инцидентов

Можно изменить период, за который учитываются эти диаграммы, изменив настройки на День/Неделя/Месяц. Имя правила в списке правил является активной ссылкой, при нажатии по которой 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 (рисунок 40).

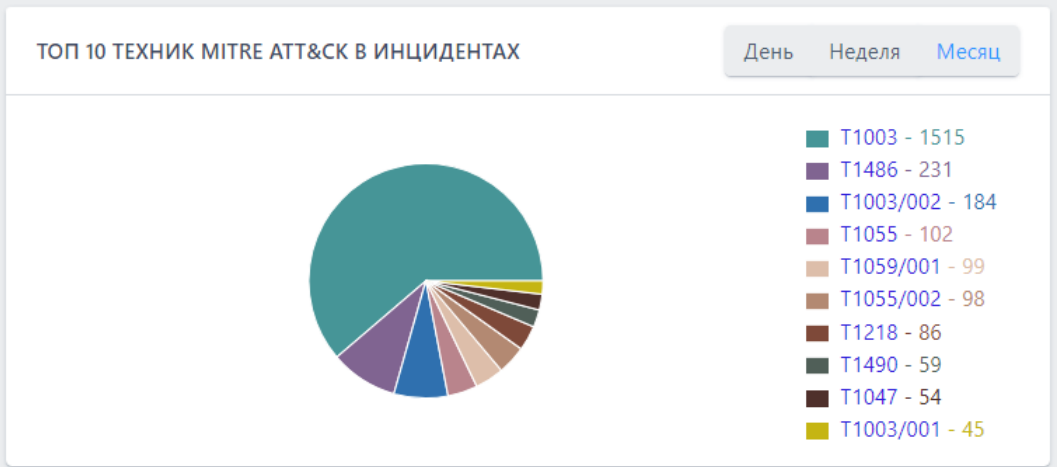


Рисунок 40 – Диаграмма отображения основных техник в инцидентах

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.

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.

Таблица содержит следующие поля:

1) Имя пользователя;

2) Последнее время входа;

3) Имя;

4) Фамилия;

5) Email;

6) Роль;

7) Статус;

8) Управление.

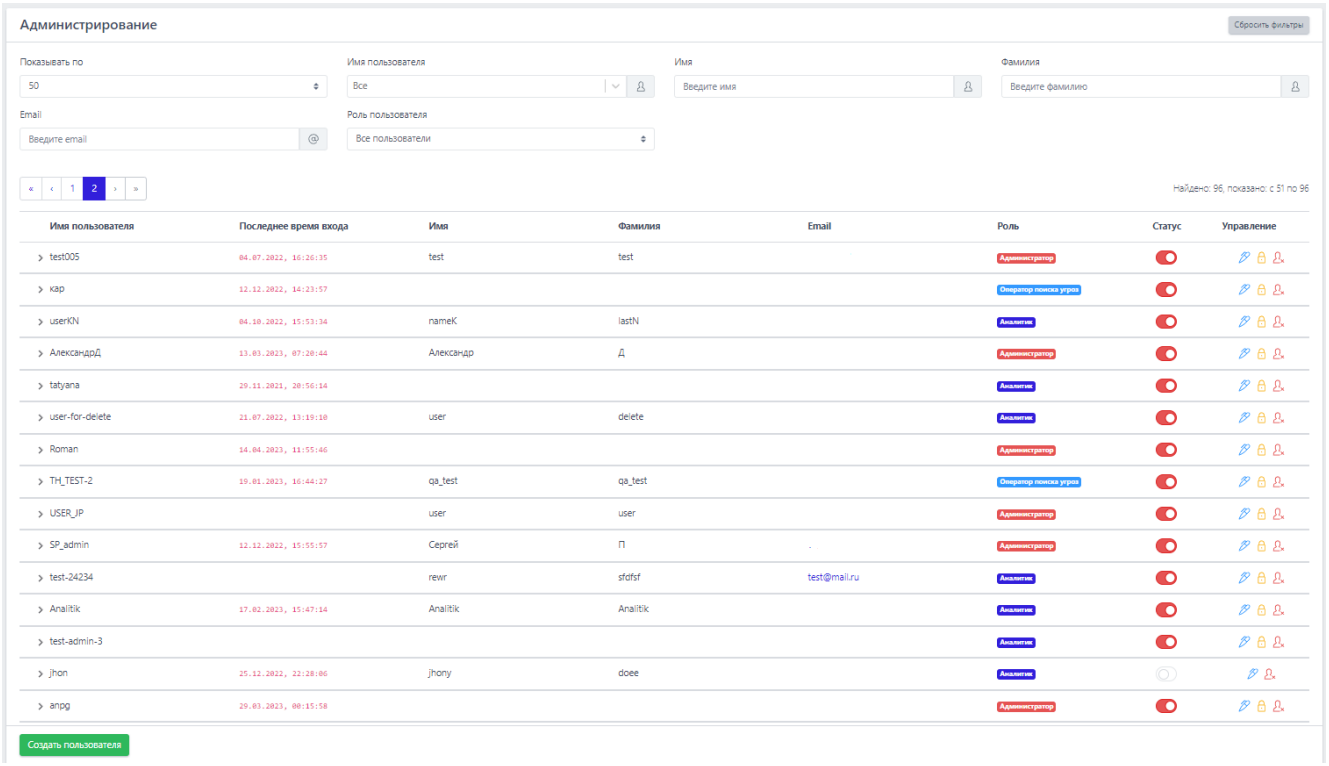


Рисунок 41 – Раздел «Администрирование»

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. 42).

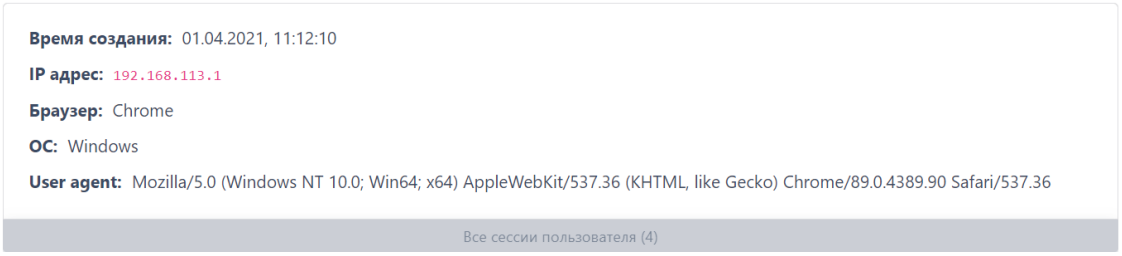


Рисунок 42 – Информация о сессиях пользователя

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: С**татус** 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 (рис. 43).

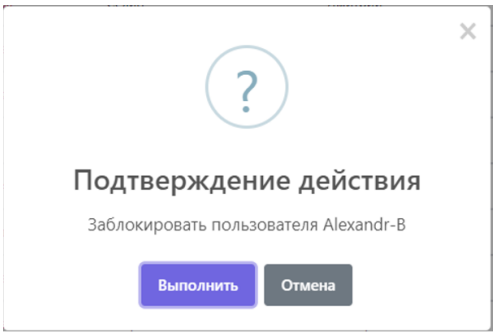


Рисунок 43 – Окно подтверждения блокирования пользователя

После подтверждения операции в нижней части основного окна программы появляется сообщение **Пользователь разблокирован/заблокирован** (рис. 44).

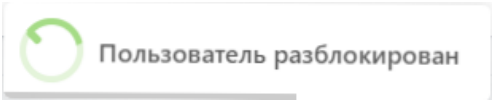


Рисунок 44 – Сообщение о разблокировании пользователя

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 (рис. 45).

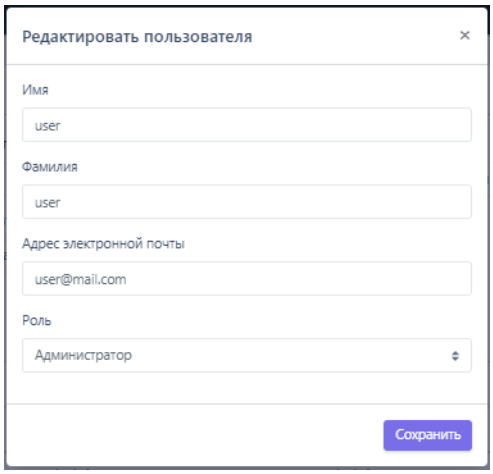


Рисунок 45 – Окно редактирования пользователя

Опция изменения роли пользователя не применяется по отношению к собственной учетной записи.

Для сохранения и применения измененных параметров необходимо нажать кнопку **Сохранить**. После сохранения изменений в нижней части страницы во всплывающем окне появляется сообщение **Данные пользователя сохранены** (рис. 46).

Рисунок 46 – Сообщение о сохранении данных пользователя

При нажатии кнопки **Сбросить пароль** открывается окно, в котором для сброса текущего пароля выбранному пользователю следует нажать кнопку **Выполнить** (рис. 47). Для отмены сброса пароля необходимо нажать кнопку **Отмена** или закрыть окно.

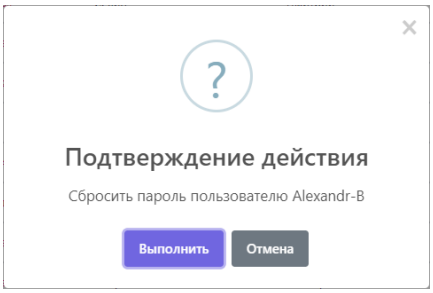


Рисунок 47 – Окно подтверждения сброса пароля

После выполнения команды в нижней части основного окна программы появляется сообщение **Отправлена ссылка на сброс пароля** (рис. 48).

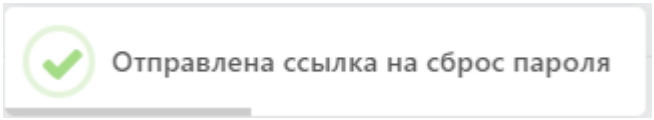


Рисунок 48 – Отправка ссылки на сброс пароля

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

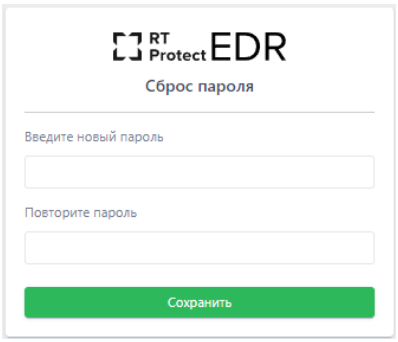


Рисунок 49 – Окно восстановления пароля пользователя

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** (рис. 50). Для отмены удаления учетной записи необходимо нажать кнопку **Отмена** или закрыть окно.

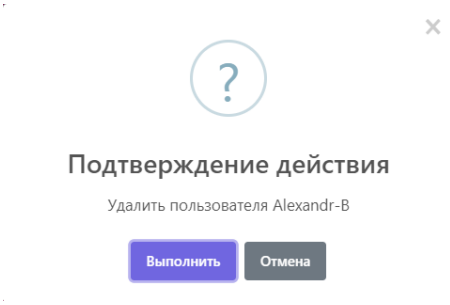


Рисунок 50 – Окно подтверждения удаления пользователя

После удаления учетной записи пользователя в нижней части основного окна программы появляется сообщение (рис. 51).

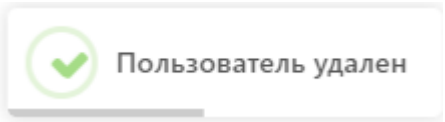


Рисунок 51 – Сообщение об удалении пользователя

6.4.3. Создание учетной записи пользователя

В нижней части панели администрирования находится кнопка **Создать пользователя**. При нажатии кнопки открывается окно **Создать пользователя** (рис. 52).

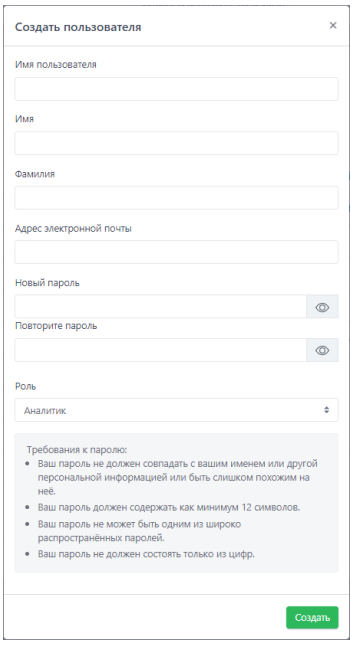


Рисунок 52 – Окно создания нового пользователя

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

Рисунок 53 – 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. 54).

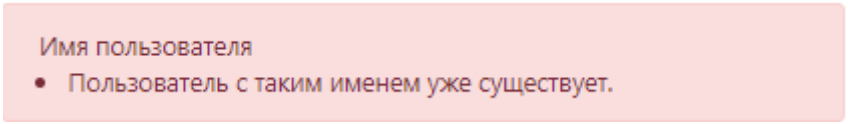


Рисунок 54 – Сообщение о совпадении имени пользователя

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. 55).

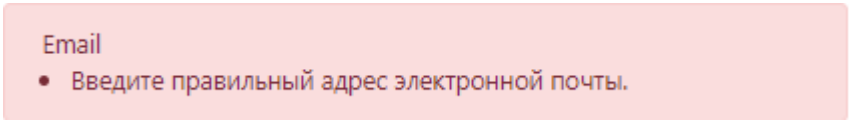


Рисунок 55 – Сообщение о неправильном адресе электронной почты

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 указан список нарушенных при создании пароля правил (рис. 56).

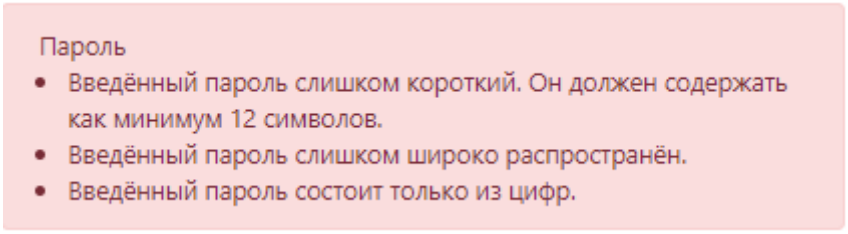


Рисунок 56 – Предупреждающее сообщение при вводе некорректного пароля

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. 57).

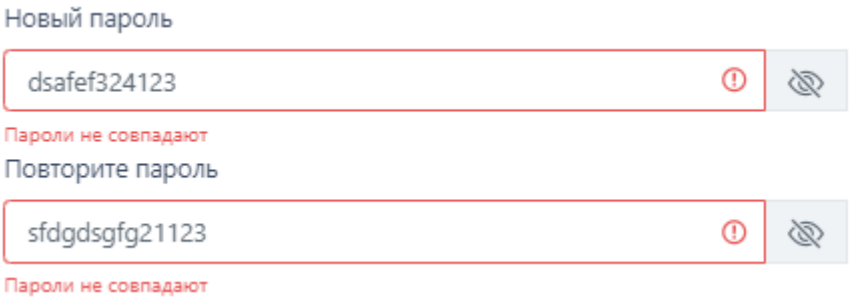


Рисунок 57 – Сообщение о несовпадении паролей

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. 58).

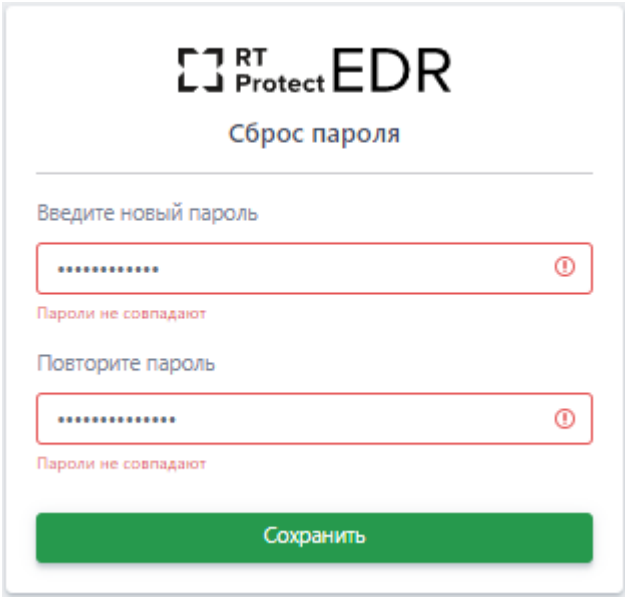


Рисунок 58 – Ввод некорректных значений при сбросе пароля

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-индикаторы,

регулируемые правилами индикации, установленными в программе по умолчанию, а также правилами, представленными в области **Аналитика** (см. подраздел 0). 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 59. 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.

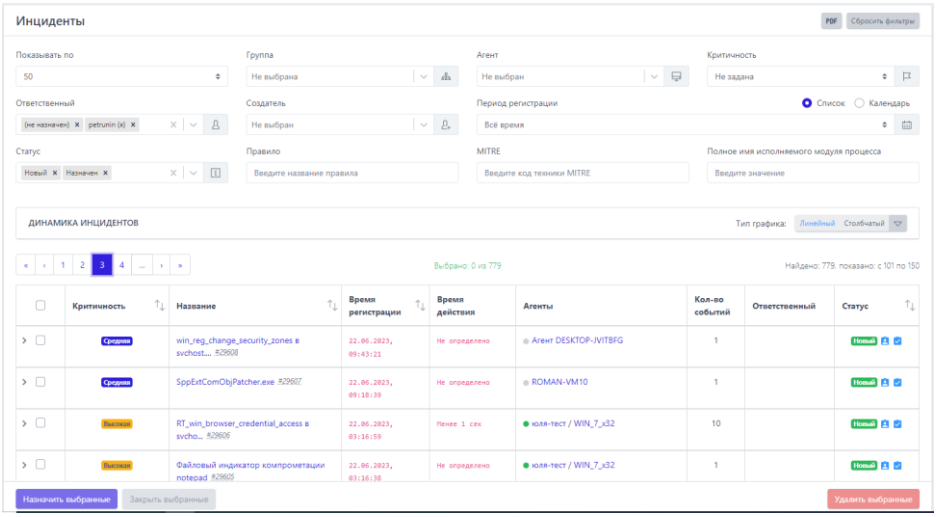


Рисунок 59 – Страница «Инциденты»

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 обнаружениях, включённых в инцидент (рис. 60).

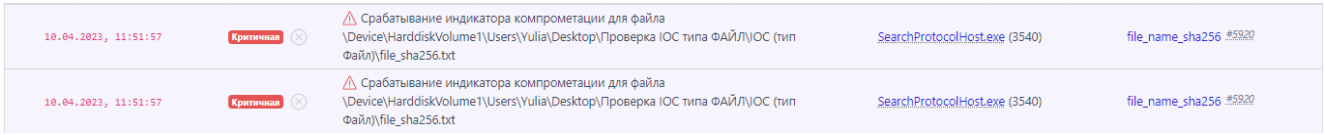


Рисунок 60 – Информация о событиях на странице «Инциденты»

Некоторые инциденты содержат десятки или сотни событий, поэтому в информации об обнаружениях пользователю показаны до двадцати последних событий инцидента.

Если необходимо просмотреть все обнаружения в инциденте, содержащем более двадцати событий, то следует перейти на страницу **Инцидент**, кликнув по имени инцидента или нажав строку **Просмотреть все** (рис. 61).

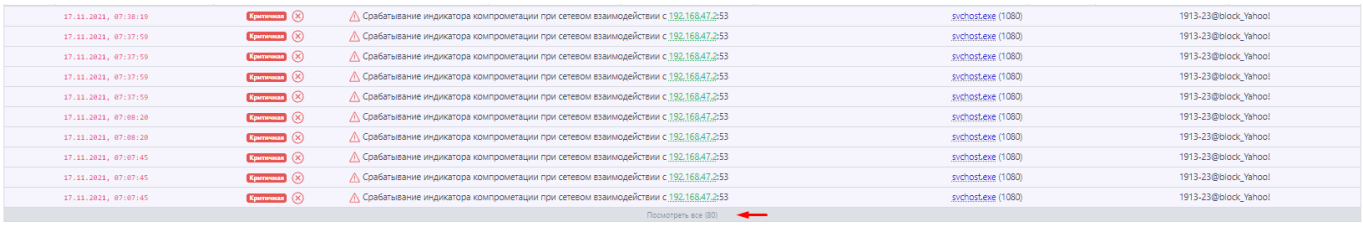


Рисунок 61 – Просмотр всех событий инцидента

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** (рис. 62).

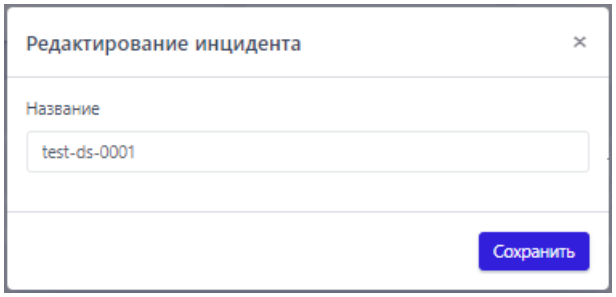


Рисунок 62 – Редактирование инцидента

Для изменения имени инцидента необходимо ввести произвольное имя в строке **Название**, после чего нажать кнопку **Сохранить** для завершения операции. После завершения операции в нижней части страницы отобразится всплывающее окно с сообщением (рис. 63).

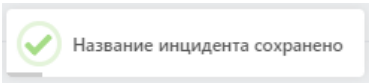


Рисунок 63 – Сообщение об изменении названия инцидента

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. 64).

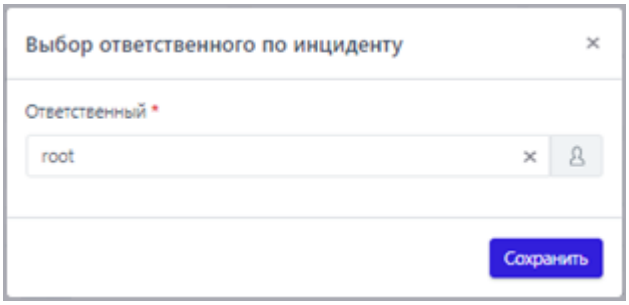


Рисунок 64 – Выбор пользователя, ответственного за решение инцидента

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, после чего в нижней части страницы отобразится всплывающее окно с сообщением (рис. 65).

Рисунок 65 – Сообщение о назначении ответственного по инциденту

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. 66) нажать кнопку **Сохранить**. Закрыть инцидент можно, даже если для инцидента не назначен ответственный.

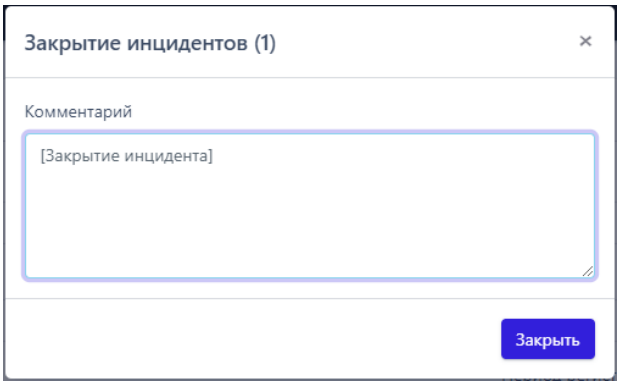


Рисунок 66 – Закрытие инцидентов

После выполнения операции в нижней части страницы появится всплывающее окно с сообщением (рис. 67).

Рисунок 67 – Сообщение о закрытии инцидента

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** (рис. 68) в поле **Ответственный** выбрать пользователя, ответственного за решение инцидента, после чего нажать кнопку **Сохранить**.

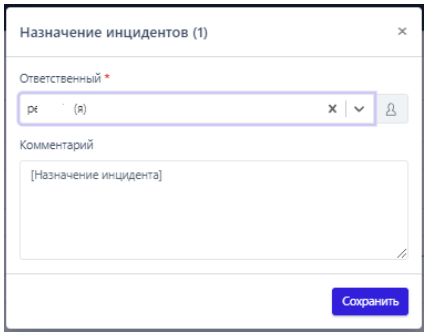


Рисунок 68 – Окно «Назначение инцидентов»

После завершения операции по назначению ответственного за решение инцидента в нижней части страницы появится окно с сообщением (рис. 69).

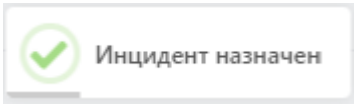


Рисунок 69 – Сообщение о назначении ответственного за инцидент

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** (см. рис. 68) 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** (см. рис. 68). После завершения операции по повторному открытию инцидента в нижней части страницы появится всплывающее окно с сообщением (см. рис. 69).

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**. 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 Сбросить фильтры.

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

Дополнительная область с событиями инцидента (рис. 70) содержит следующие показатели:

1) Время регистрации события инцидента;

2) Критичность инцидента/Действие, предпринятое программой;

3) Краткая сводка об инциденте;

4) Процесс, работа которого привела к созданию инцидента;

5) Идентификатор техники MITRE (опционально);

6) Сведения о правиле или исключении, на основе которого сформирован инцидент.

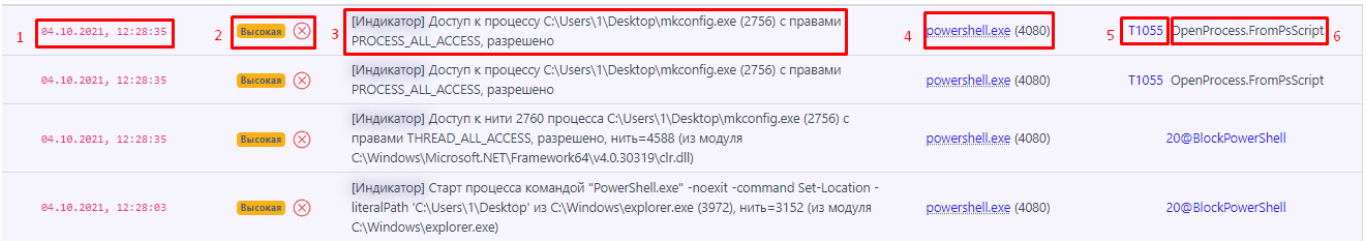


Рисунок 70 – Поля дополнительной области инцидента

Поле **Время** содержит информацию о времени обнаружения события, включённого в инцидент.

В поле **Критичность/Действие** отображается информация о степени критичности обнаружения, являющегося составной частью инцидента. Предусмотрено пять степеней критичности событий:

– Информация;

– Низкая;

– Средняя;

– Высокая;

– Критичная.

Рядом с критичностью события отображается значок действия, связанного с событием. В программе предусмотрено три вида действий, предпринимаемых в ответ на возникновение какого-либо события:

1) Блокировать (с указанием причины блокирования и правила, в соответствии с которым оно было выполнено) – обозначается значком ⊗;

2) Детектировать (с указанием причины обнаружения и правила, в соответствии с которым было детектировано событие) – обозначается значком ⊘;

3) Продолжать наблюдение (в этом случае поле будет пустым, это связано с тем, что событие не подпадает под действие какого-либо регулирующего правила).

Информация о правиле и причине, в соответствии с которыми было разрешено или запрещено действие, отображается при наведении курсора на иконку ⊘ или ⊗. В качестве примера можно рассмотреть, как выглядит сообщение о запрете действия при обнаружении вредоносного файла (см. рис. 71).

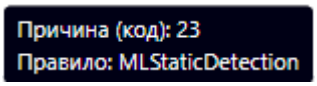


Рисунок 71 – Сообщение о причине запрета действия

В поле с названием обнаружения показана краткая информация о сути события, детектированного системой как вредоносное, опасное или требующее внимание пользователя.

В поле с именем процесса содержится ссылка в виде имени на модуль исполняемого файла процесса. Ссылка позволяет быстро перейти к странице **Процессы** и при необходимости завершить процесс или расследовать особенности его выполнения (см. пункт 6.5.3).

В поле с идентификатором **MITRE** отображается ссылка на идентификатор техники атаки из базы знаний MITRE ATT&CK, на которую указывает событие, включенное в инцидент. Информация в поле добавляется опционально.

В поле с обозначением имени правила указывается информация о правиле, в соответствии с которым программа выполнила действие для события, добавленного в инцидент.

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. 72);

3) Нажать кнопку **Начать удаление**;

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

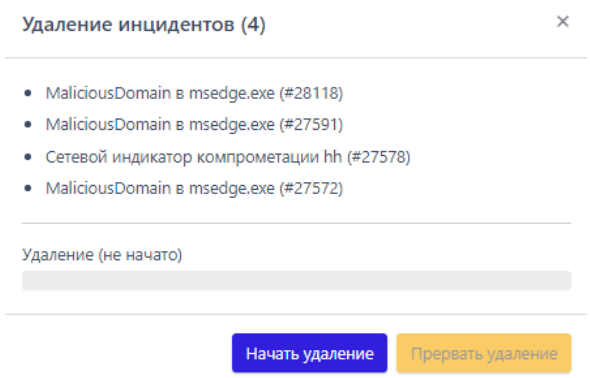


Рисунок 72 – Групповое удаление инцидентов

В процессе группового удаления инцидентов имеется возможность прервать операцию удаления, нажав по иконке Прервать удаление. Удаление инцидентов прервется на том инциденте, который не отмечен значком в списке удаляемых инцидентов. Процесс прерывания операции показан на рисунке 73.

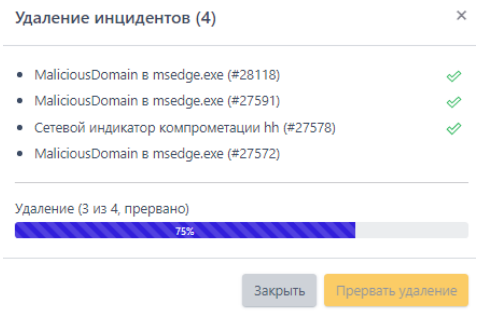


Рисунок 73 – Прерывание удаления инцидентов

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 PDF в верхней части страницы с инцидентами. Отчет содержит информацию, соответствующую установленным на странице **Инциденты** фильтрам.

Инцидент

Жизненный цикл каждого инцидента подразумевает прохождение трех стадий:

– новый инцидент;

– назначенный в работу;

– закрытый инцидент.

Совет

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

В зависимости от статуса инцидента у страницы **Инцидент** функциональность может различаться. Для нового и закрытого инцидента недоступна функция редактирования инцидента (рис. 74). Чтобы отредактировать инцидент, необходимо назначить пользователя, ответственного за его решение.

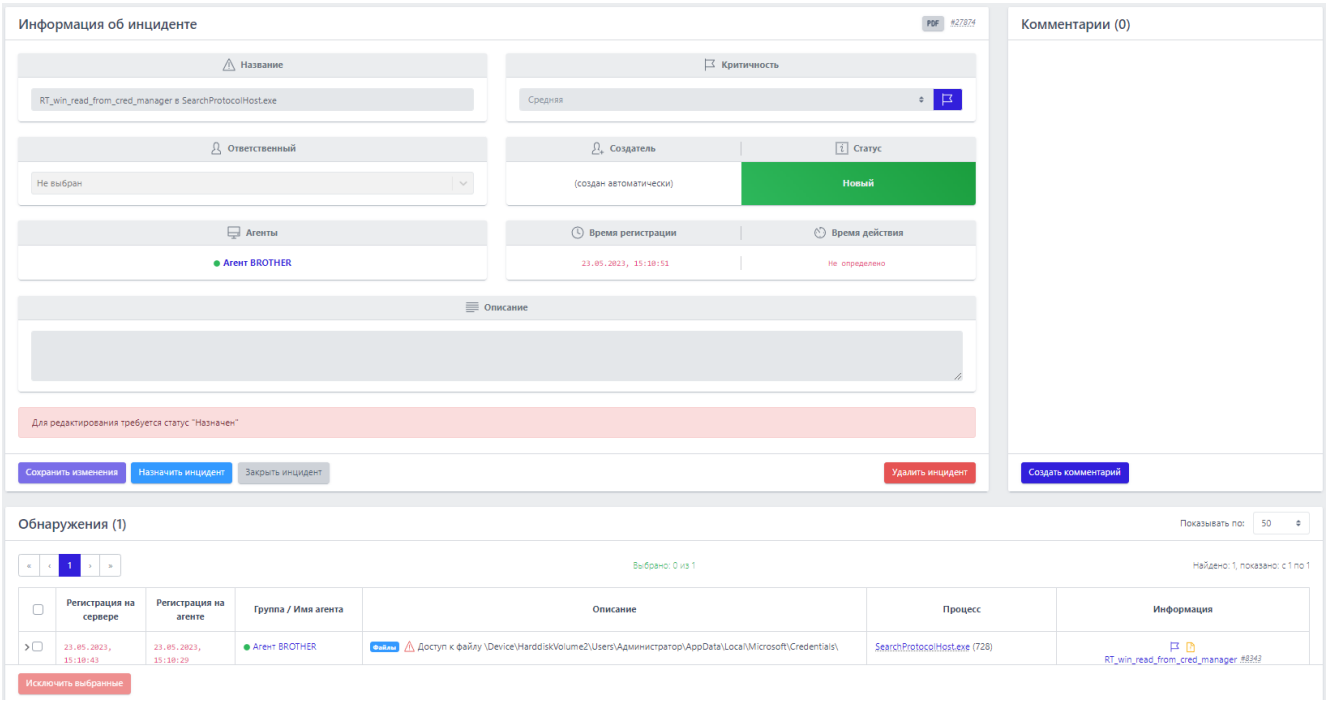


Рисунок 74 – Страница «Инцидент» (статус «Новый»)

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) **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 (рис. 75). Также комментарии указываются автоматически при переводе инцидента из одного статуса в другой, например, при назначении или закрытии инцидента.

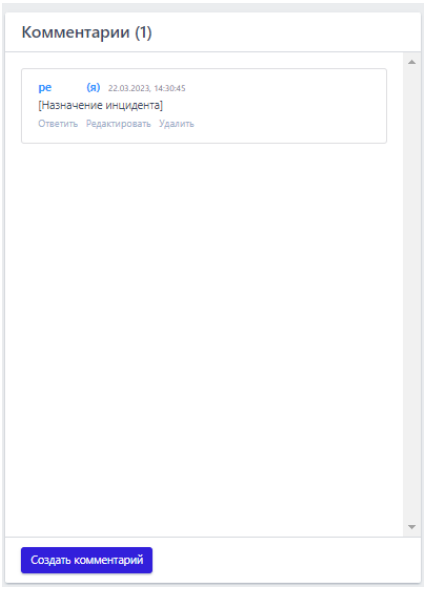


Рисунок 75 – Комментарии

Для добавления нового комментария следует нажать кнопку **Создать комментарий,** после чего открывается окно **Новый комментарий** (рис. 76).

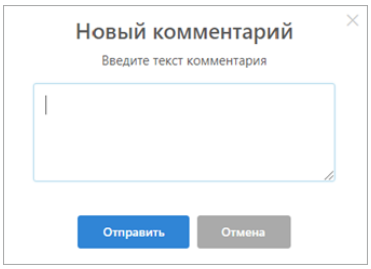


Рисунок 76 – Окно ввода комментария

Для добавления комментария к инциденту необходимо ввести в окне **Новый комментарий** текст комментария и нажать кнопку **Отправить,** после чего комментарий пользователя будет добавлен на страницу инцидента (рис. 77).

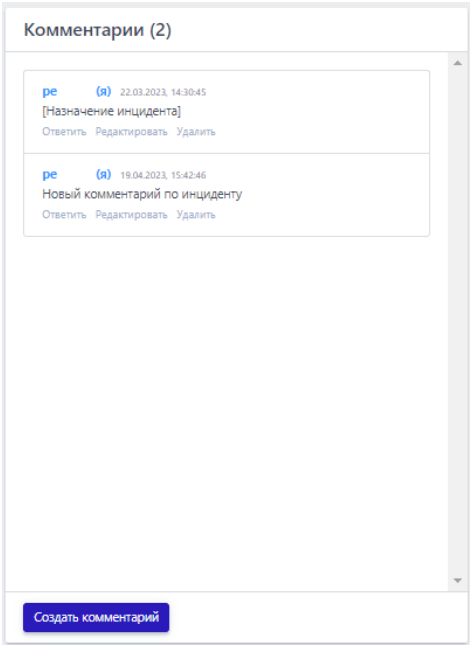


Рисунок 77 – Комментарии (добавление комментария)

Для отмены ввода комментария следует в окне **Новый комментарий** нажать кнопку **Отмена** или **Закрыть окно** ( ).

Информация о событиях, которые были внесены в инцидент при его регистрации, представлена в области **Обнаружения** в табличном виде (рис. 78). Переход по страницам в таблице осуществляется с помощью пагинатора (см. рисунок 19).

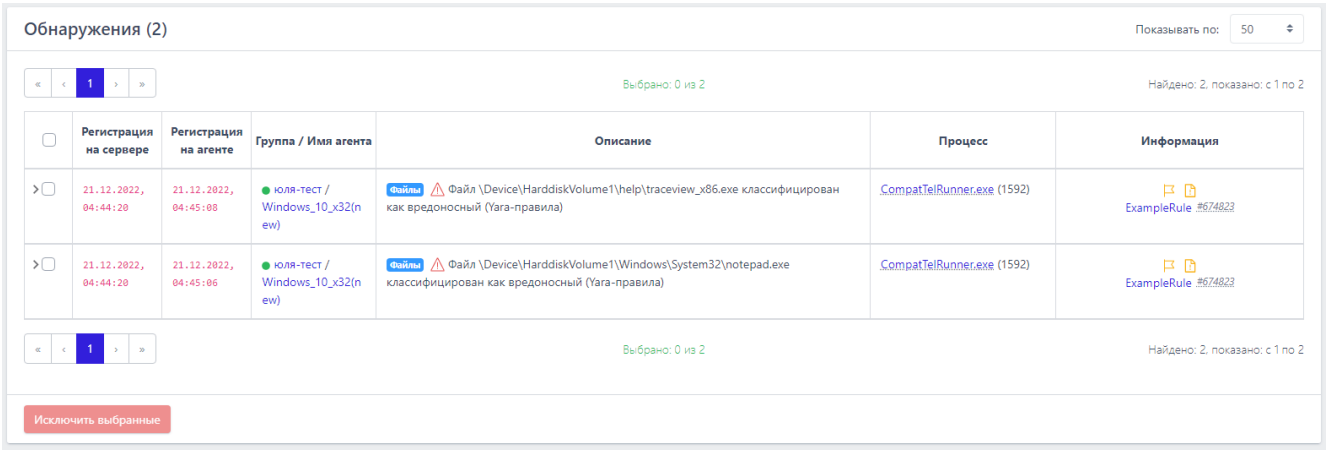


Рисунок 78 – Область «Обнаружения»

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 79.

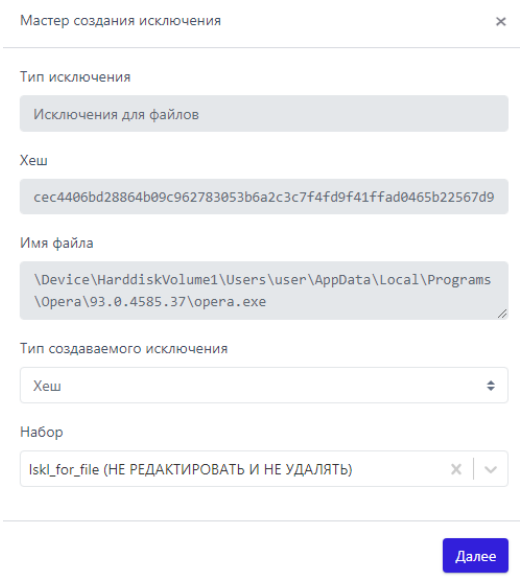


Рисунок 79 – Окно мастера создания исключений

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 добавления исключения (рис. 80).

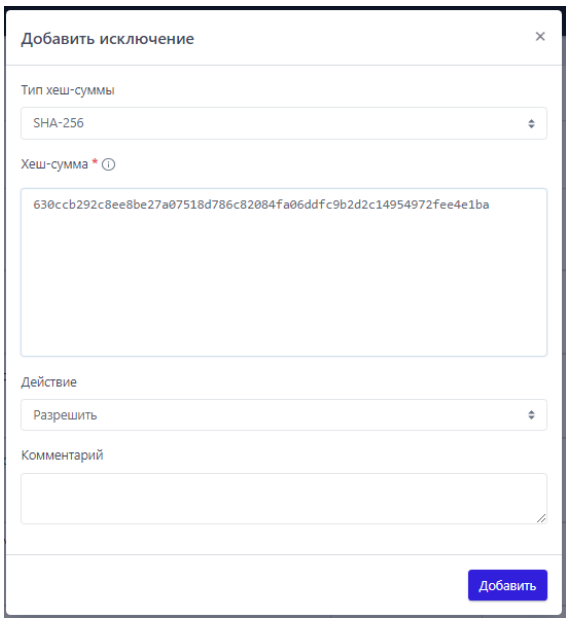


Рисунок 80 – Окно добавления исключения

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 (рис. 81).

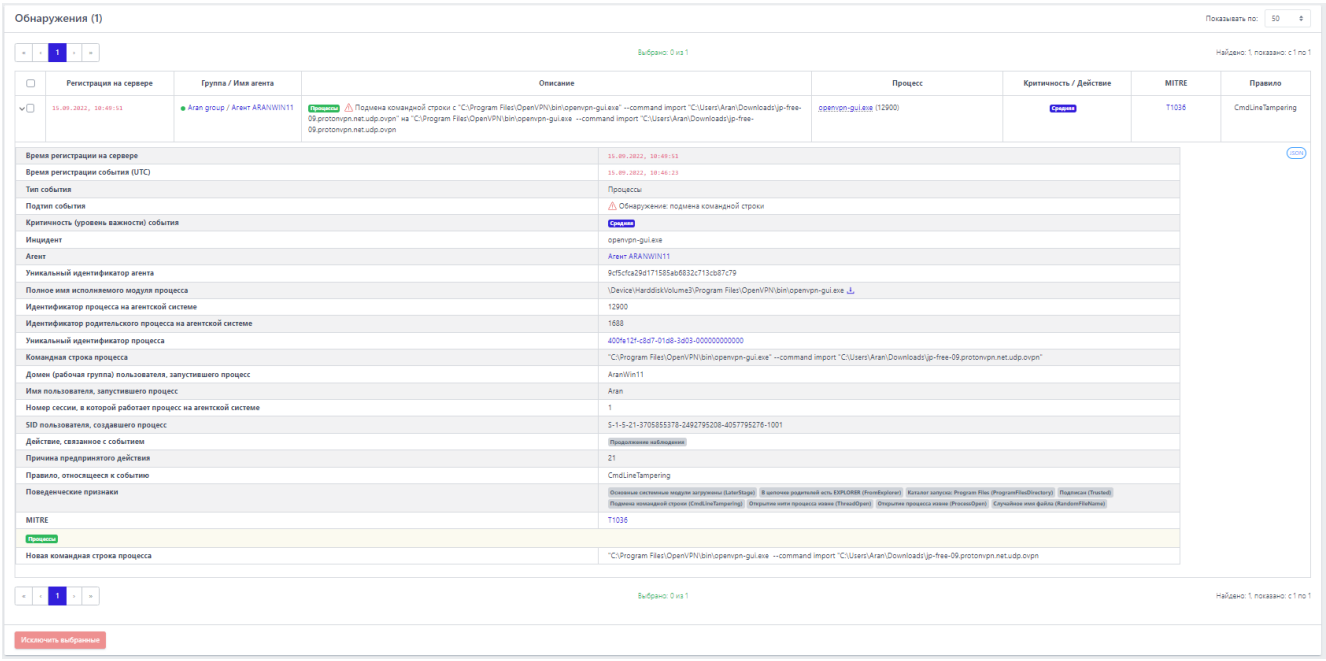


Рисунок 81 – Карточка событий на странице «Инцидент»

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»).

Страница раздела **Активность** при настройках по умолчанию представлена на рисунке 82.

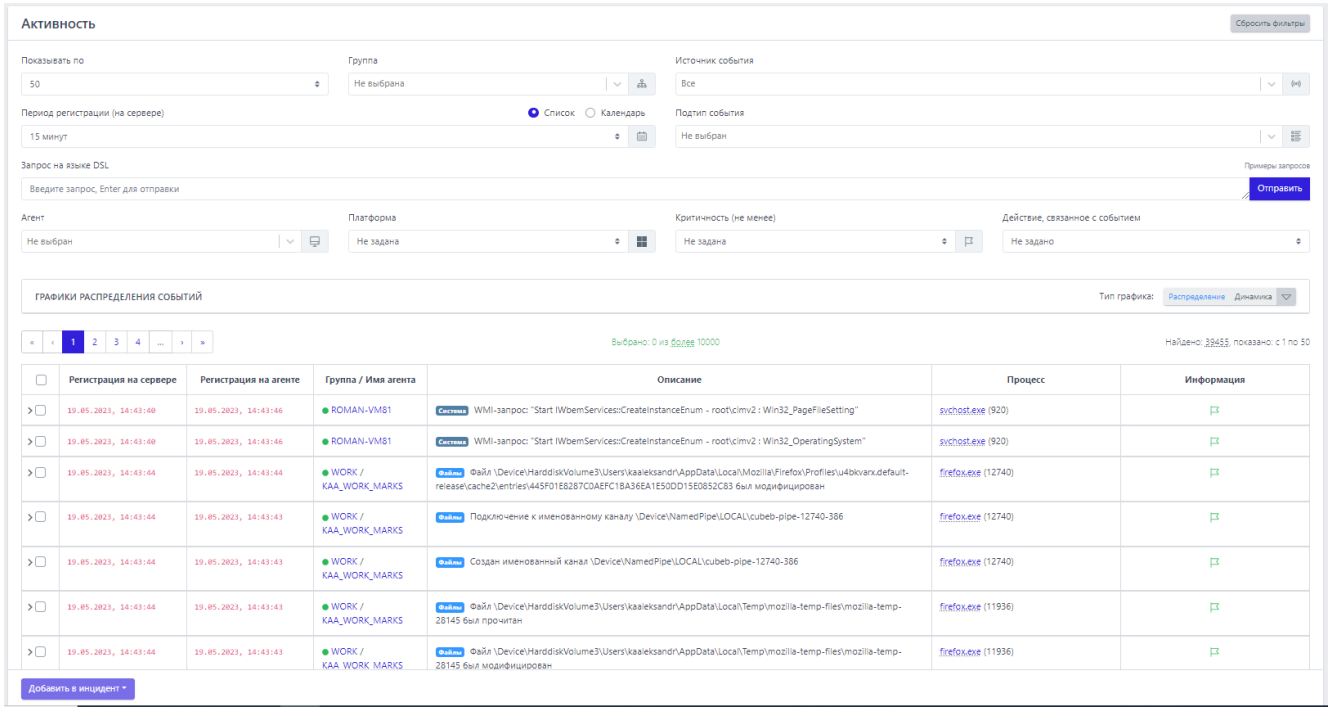


Рисунок 82 – Активность

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. 83).

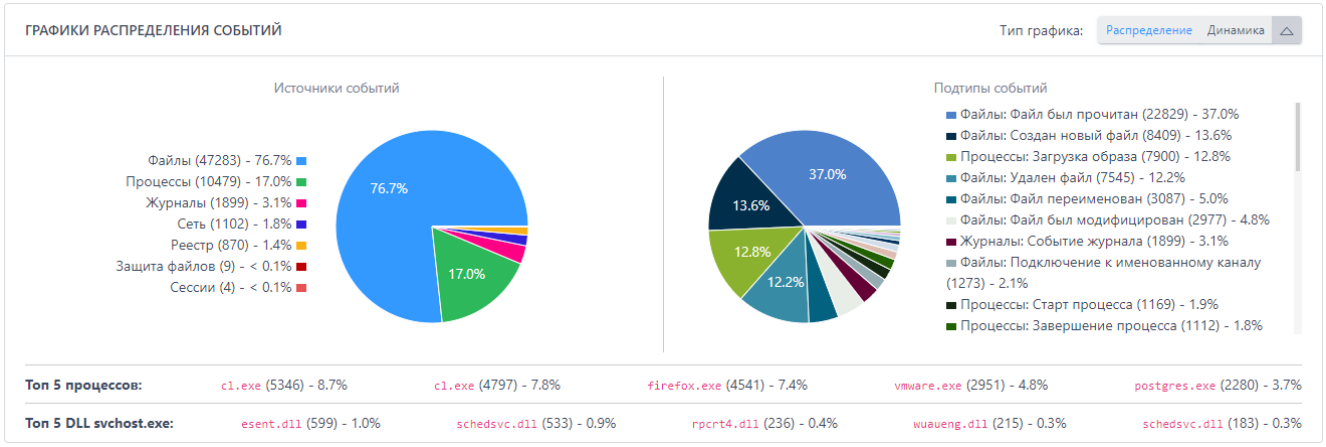


Рисунок 83 – Графики распределения событий

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 (рис. 84):

1) Кнопка выбора (☐);

2) **Регистрация на сервере;**

3) **Регистрация на агенте;**

4) **Группа/Имя агента;**

5) **Описание;**

6) **Процесс;**

7) **Информация.**

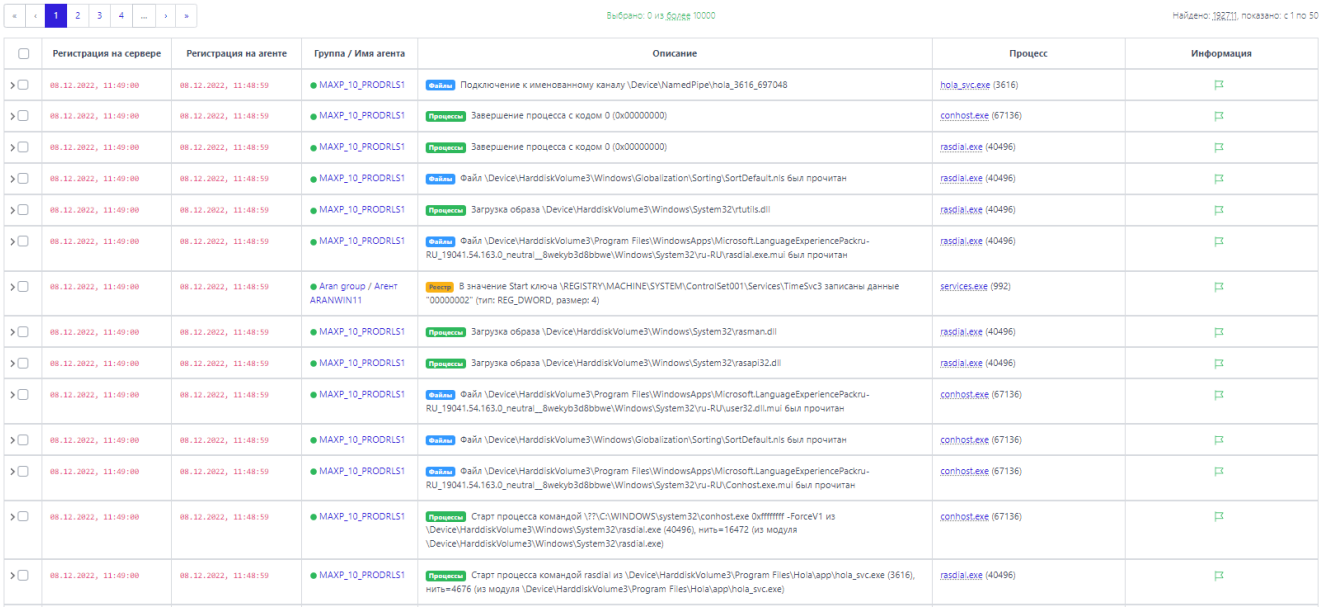


Рисунок 84 – Таблица отображения событий

Для просмотра страниц с событиями используется пагинатор в верхней и нижней части таблицы с левой стороны (см. рис. 19).

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. 85).

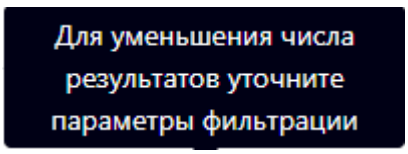


Рисунок 85 – Подсказка в таблице событий

Каждое событие содержит в себе сводную информацию, собранную в виде карточки события (рис. 86).

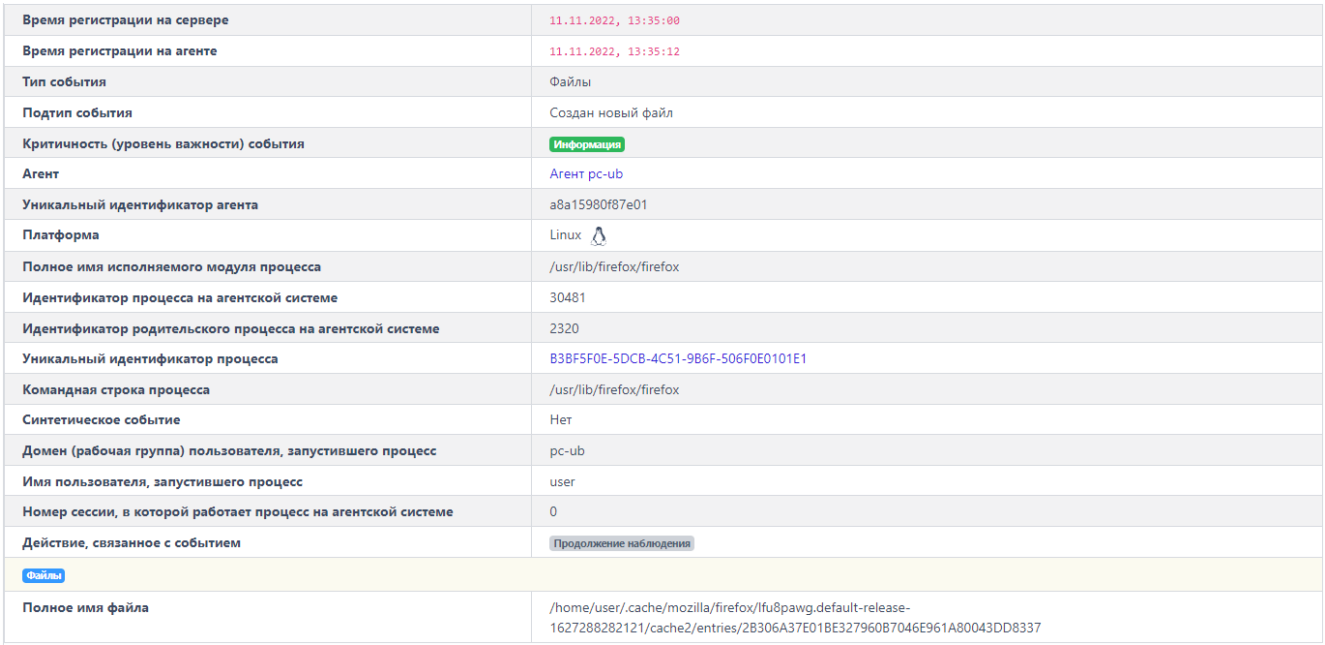


Рисунок 86 – Карточка событий

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. Общий список значений, отображаемых в JSON-формате, представлен в таблице 8.

Таблица 8 – Общий список полей событий

Назначение	Тип данных	JSON	Отображение/ фильтрация	Подсистема
Тип события	enum	**t**	По умолчанию	Общая
Время регистрации события	timestamp	**time**	По умолчанию	Общая
Действие, связанное с событием	enum	**act**	По умолчанию	Общая
Причина предпринятого действия	enum	**rsn**	По умолчанию	Общая
Правило, относящееся к событию	string	**rul**	По умолчанию	Общая

Назначение	Тип данных	JSON	Отображение/ фильтрация	Подсистема
Идентификатор техники/тактики MITRE	string	**mitre**	По умолчанию	Общая
Критичность (уровень важности) события	enum	**svrt** (по умолчанию: 0)	По умолчанию	Общая
Уникальный идентификатор процесса	int (индекс в массиве GUID'ов)	**uuid**	Опционально	Общая
Уникальный идентификатор группы процессов	int (индекс в массиве GUID'ов)	**huid**	Опционально	Общая
Идентификатор процесса на агентской системе	unsigned	**pid**	По умолчанию	Общая
Идентификатор родительского процесса на агентской системе	unsigned	**ppid**	По умолчанию	Общая
Полное имя исполняемого файла процесса	string MANGLED	**app**	По умолчанию	Общая
Номер сессии, в которой работает процесс на агентской системе	unsigned	**sess** (по умолчанию: 0)	По умолчанию	Общая
Имя пользователя, запустившего процесс	string	**usr**	По умолчанию	Общая
Домен (имя компьютера) пользователя, запустившего процесс	string	**dom**	По умолчанию	Общая
Подтип события	enum	**st**	По умолчанию	Общая
Поведенческие признаки процесса (первая группа)	uint64	**rfo**	Опционально	Общая
Поведенческие признаки процесса (вторая группа)	uint64	**rf1**	Опционально	Общая
Синтетическое событие	int (0/1)	**syn**	Опционально	Общая
Версия события	unsigned	**efmt**	Опционально	Общая
Протокол	enum	**proto**	По умолчанию	Сеть

Назначение	Тип данных	JSON	Отображение/ фильтрация	Подсистема
Признак работы по IPv6	int (0/1)	**ipv6**	Опционально	Сеть
Идентификатор сетевого потока	int64	**flow**	Опционально	Сеть
Отправка или прием	int (0/1)	**out**	Опционально	Сеть
Размер полезных данных (payload) сетевого пакета	int64	**size**	Опционально	Сеть
Имя хоста, соответствующее удаленному IP-адресу	string	**host**	По умолчанию	Сеть
Тип DNS-запроса	enum	**dnsq_t**	Опционально	Сеть
Статус DNS-запроса	unsigned	**dnsq_s**	Опционально	Сеть
Результат DNS-запроса	string	**dnsq_r**	Опционально	Сеть
Имя хоста из DNS-запроса	string	**dnsq_h**	Опционально	Сеть
Имя хоста (server_name) из сообщения SSL Client Hello	string	**ssl_h**	Опционально	Сеть
Удаленный IP-адрес	string	**r_ip**	По умолчанию	Сеть
Удаленный порт	unsigned	**r_p**	По умолчанию	Сеть
Локальный IP-адрес	string	**l_ip**	Опционально	Сеть
Локальный порт	unsigned	**l_p**	По умолчанию	Сеть
Имя хоста в индикаторе компрометации	string	**ioc_h**	Опционально	Сеть
Полное имя файла	string MANGLED	**name**	По умолчанию	Файлы
Время создания файла	timestamp	**crtime**	Опционально	Файлы, Процессы
Время последнего изменения файла	timestamp	**chtime**	Опционально	Файлы, Процессы
Размер файла	int64	**fsize**	Опционально	Файлы, Процессы
Тип файла	enum	**ftype**	Опционально	Файлы, Процессы
Атрибуты файла	unsigned	**attr**	Опционально	Файлы, Процессы
SHA-1 файла	string	**sha1**	Опционально	Файлы, Процессы

Назначение	Тип данных	JSON	Отображение/ фильтрация	Подсистема
MD5 файла	string	**md5**	Опционально	Файлы, Процессы
SHA-256 файла	string	**sha256**	Опционально	Файлы, Процессы
Электронная подпись файла	string	**sgnr**	Опционально	Файлы, Процессы
Статус электронной подписи файла	enum	**sgnr_s**	Опционально	Файлы, Процессы
Оригинальное имя файла	string	**ofn**	Опционально	Файлы, Процессы
Компания-издатель файла	string	**fcomp**	Опционально	Файлы, Процессы
Версия файла	string	**fver**	Опционально	Файлы, Процессы
Описание файла	string	**fdesc**	Опционально	Файлы, Процессы
Продукт, к которому относится файл	string	**fprod**	Опционально	Файлы, Процессы
Тип упаковщика файла	string	**pack**	Опционально	Файлы, Процессы
Файл расположен в директории автозапуска	int (0/1)	**arun**	Опционально	Файлы
Новое имя файла	string MANGLED	**fnew**	Опционально	Файлы
Файл был заменен	int (0/1)	**owrt**	Опционально	Файлы
Предыдущее время создания файла	timestamp	**old_t**	Опционально	Файлы
Новое время создания файла	timestamp	**new_t**	Опционально	Файлы
Файл содержит атрибут "скрытый"	int (0/1)	**hdn**	Опционально	Файлы
Файл содержит атрибут "системный"	int (0/1)	**sys**	Опционально	Файлы
Операция совершается над альтернативным потоком данных файла	int (-/1)	**ads**	Опционально	Файлы
Для файла была создана резервная копия	int (-/1)	**save**	Опционально	Файлы

Назначение	Тип данных	JSON	Отображение/ фильтрация	Подсистема
Доступ на удаление	int (-/1)	**delete**	Опционально	Файлы
Доступ на чтение	int (-/1)	**read**	Опционально	Файлы
Доступ на модификацию	int (-/1)	**modify**	Опционально	Файлы
Код оповещения	enum	**detect**	Опционально	Сеть, Файлы, Процессы, Реестр
Флаги исполняемого файла процесса	int64	**exclf**	Опционально	Сеть, Файлы, Процессы, Реестр
Полное имя исполняемого модуля–инициатора операции	string MANGLED	**who**	Опционально	Файлы, Процессы, Реестр
Идентификатор нити–инициатора операции	unsigned	**whotid**	Опционально	Файлы, Процессы, Реестр
Стартовый адрес нити–инициатора операции	uint64	**whoaddr**	Опционально	Файлы, Процессы, Реестр
Флаги исполняемого модуля-инициатора операции	uint64	**whof**	Опционально	Файлы, Процессы, Реестр
Командная строка процесса	string	**cmdl**	По умолчанию	Процессы
Командная строка родительского процесса	string	**cmdlp**	По умолчанию	Процессы
Командная строка прародителя (grand parent)	string	**cmdlg**	Опционально	Процессы
Рабочий каталог процесса	string MANGLED	**wdir**	Опционально	Процессы
Уровень защиты процесса	unsigned	**prot**	Опционально	Процессы
Уровень доверия (integrity level) процесса	unsigned	**integ**	Опционально	Процессы
Время создания процесса	timestamp	**when**	Опционально	Процессы

Назначение	Тип данных	JSON	Отображение/ фильтрация	Подсистема
Уникальный идентификатор родительского процесса	int (индекс в массиве GUID'ов)	**parent**	Опционально	Процессы
Уникальный идентификатор процесса-создателя	int (индекс в массиве GUID'ов)	**caller**	Опционально	Процессы
Идентификатор процесса-инициатора операции	unsigned	**cpid**	Опционально	Процессы
Полное имя процесса-инициатора операции	string MANGLED	**cpath**	Опционально	Процессы
SID пользователя, создавшего процесс	string	**sid**	По умолчанию	Процессы
Код завершения процесса	unsigned	**code**	Опционально	Процессы
Уникальный идентификатор целевого процесса	int (индекс в массиве GUID'ов)	**targ**	Опционально	Процессы
Полное имя целевого процесса	string MANGLED	**tpath**	По умолчанию	Процессы
Идентификатор целевого процесса	unsigned	**tpid**	По умолчанию	Процессы
Флаги образа целевого процесса	uint64	**targf**	Опционально	Процессы
Поведенческие признаки целевого процесса (первая группа)	uint64	**trfo**	Опционально	Процессы
Поведенческие признаки целевого процесса (вторая группа)	uint64	**trf1**	Опционально	Процессы
Стек вызовов операции	string	**trace**	Опционально	Процессы
Имя модуля целевой нити	string	**tmod**	Опционально	Процессы
Имя функции целевой нити	string	**tfunc**	Опционально	Процессы
Полное имя файла образа	string MANGLED	**path**	По умолчанию	Процессы
Флаги нити	unsigned	**tf**	Опционально	Процессы

Назначение	Тип данных	JSON	Отображение/ фильтрация	Подсистема
Флаги операции загрузки образа	unsigned	**ldf**	Опционально	Процессы
Флаги образа	int64	**imgf**	Опционально	Процессы
Базовый адрес образа	int64	**base**	Опционально	Процессы
Размер образа	unsigned	**isize**	Опционально	Процессы
Идентификатор целевой нити	unsigned	**tid**	Опционально	Процессы
Стартовый адрес целевой нити	int64	**taddr**	Опционально	Процессы
Имя открытого рабочего стола	string	**desk**	По умолчанию	Процессы
Запрашиваемые права	unsigned	**dsrd**	Опционально	Процессы
Предоставленные права	unsigned	**grnt**	Опционально	Процессы
Новый уровень защиты процесса	int	**prot1**	Опционально	Процессы
Новая командная строка	string	**cmdl1**	Опционально	Процессы
Локальная сессия	int (0/1)	**local**	Опционально	Сессии
Имя оконной станции	string	**win_stn**	Опционально	Сессии
Номер сессии	unsigned	**sess_id**	Опционально	Сессии
Тип дистанционного управления	unsigned (опционально)	**sess_opt**	Опционально	Сессии
Тип сессии	unsigned (опционально)	**sess_proto**	Опционально	Сессии
Имя клиента	string (опционально)	**sess_cl**	Опционально	Сессии
IP-адрес клиента	string (опционально)	**sess_claddr**	Опционально	Сессии
Имя пользователя	string (опционально)	**sess_usr**	Опционально	Сессии
Имя домена\компьютера	string (опционально)	**sess_dom**	Опционально	Сессии
Путь ключа	string	**key**	По умолчанию	Реестр
Имя значения	string	**val_n**	По умолчанию	Реестр
Тип данных значения	enum	**val_t**	Опционально	Реестр
Размер данных значения	unsigned	**val_s**	Опционально	Реестр
Данные значения	string	**val_d**	Опционально	Реестр
Новое имя ключа	string	**new**	Опционально	Реестр

Назначение	Тип данных	JSON	Отображение/ фильтрация	Подсистема
Имя файла-источника загружаемой в реестр информации	string MANGLED	**src**	Опционально	Реестр
Имя файла, в который записываются данные из реестра	string MANGLED	**dst**	Опционально	Реестр
Ключ/значение относится к категории автозапуска	int (0/1)	**asep**	Опционально	Реестр
WMI: Тип события	enum	**wmi**	По умолчанию	Система: WMI
WMI: Путь	string	**wmi_pth**	По умолчанию	Система: WMI
WMI: SID пользователя	string	**wmi_sid**	По умолчанию	Система: WMI
WMI: Пространство имен	string	**ns**	По умолчанию	Система: WMI
WMI: Путь до исполняемого файла	string MANGLED	**exe_path**	Опционально	Система: WMI
WMI: Имя файла	string MANGLED	**fname**	Опционально	Система: WMI
WMI: Имя фильтра событий	string	**wmi_nm**	Опционально	Система: WMI
WMI: Строка запроса	string	**qstr**	Опционально	Система: WMI
WMI: Имя файла скрипта	string MANGLED	**scrfname**	Опционально	Система: WMI
WMI: Текст скрипта	string	**scrtxt**	Опционально	Система: WMI
WMI: Имя источника	string MANGLED	**sname**	Опционально	Система: WMI
WMI: SMTP	string	**smtp**	Опционально	Система: WMI
WMI: Фильтр	string	**flt**	Опционально	Система: WMI
WMI: Потребитель	string	**cnsm**	Опционально	Система: WMI
WMI:Идентификатор процесса клиента	unsigned (по умолчанию 0)	**wmi_clpid**	Опционально	Система: WMI
WMI: Уникальный идентификатор процесса клиента	int (индекс в массиве GUID'ов)	**wmi_cluuid**	Опционально	Система: WMI

Назначение	Тип данных	JSON	Отображение/ фильтрация	Подсистема
WMI: Время создания процесса клиента	timestamp	**wmi_cltime**	Опционально	Система: WMI
WMI: Командная строка процесса клиента	string	**wmi_clcmdl**	Опционально	Система: WMI
WMI: Локальный запрос	int (0/1) (по умолчанию 1)	**wmi_local**	Опционально	Система: WMI
WMI: Идентификатор созданного процесса	unsigned	**wmi_crpid**	Опционально	Система: WMI
WMI: Уникальный идентификатор созданного процесса	int (индекс в массиве GUID'ов)	**wmi_cruuid**	Опционально	Система: WMI
WMI: Время создания созданного процесса	timestamp	**wmi_crtime**	Опционально	Система: WMI
WMI: Командная строка созданного процесса	string	**wmi_crcmdl**	Опционально	Система: WMI
WMI: Имя машины, выполнившей запрос	string	**wmi_cl**	Опционально	Система: WMI
WMI: FQDN машины, выполнившей запрос	string	**wmi_clfqdn**	Опционально	Система: WMI
WMI: Имя пользователя клиента, выполнившего запрос	string	**wmi_usr**	Опционально	Система: WMI
WMI: Имя домена клиента, выполнившего запрос	string	**wmi_dom**	Опционально	Система: WMI
WMI: Имя вызываемого метода	string	**wmi_mthd**	Опционально	Система: WMI
Атаки на Kerberos: Подтип атаки	enum	**atck**	По умолчанию	Система: Атаки на Kerberos
Golden ticket: Причина	enum	**goldent_r**	По умолчанию	Система: Атаки на Kerberos
Golden ticket: Имя пользователя	string	**goldent_u**	Опционально	Система: Атаки на Kerberos
Golden ticket: Имя домена	string	**goldent_d**	Опционально	Система: Атаки на Kerberos

Назначение	Тип данных	JSON	Отображение/ фильтрация	Подсистема
Golden ticket: IP-адрес	string	**goldent_ip**	Опционально	Система: Атаки на Kerberos
Silver ticket: Причина	enum	**silvert_r**	По умолчанию	Система: Атаки на Kerberos
Silver ticket: Имя пользователя	string	**silvert_u**	Опционально	Система: Атаки на Kerberos
Silver ticket: Имя домена	string	**silvert_d**	Опционально	Система: Атаки на Kerberos
Silver ticket: IP-адрес	string	**silvert_ip**	Опционально	Система: Атаки на Kerberos
Kerberoasting: Причина	enum	**kerberoasting_r**	По умолчанию	Система: Атаки на Kerberos
Kerberoasting: Имя пользователя	string	**kerberoasting_u**	Опционально	Система: Атаки на Kerberos
Kerberoasting: Имя домена	string	**kerberoasting_d**	Опционально	Система: Атаки на Kerberos
Kerberoasting: IP-адрес	string	**kerberoasting_ip**	Опционально	Система: Атаки на Kerberos
AS-REP roasting: Причина	enum	**asreproasting_r**	По умолчанию	Система: Атаки на Kerberos
AS-REP roasting: Имя пользователя	string	**asreproasting_u**	Опционально	Система: Атаки на Kerberos
AS-REP roasting: Имя домена	string	**asreproasting_d**	Опционально	Система: Атаки на Kerberos
AS-REP roasting: IP-адрес	string	**asreproasting_ip**	Опционально	Система: Атаки на Kerberos
Новое время	timestamp	**new_stime**	Опционально	Система: Изменение системного времени

Назначение	Тип данных	JSON	Отображение/ фильтрация	Подсистема
Предыдущее время	timestamp	**prev_stime**	Опционально	Система: Изменение системного времени
ID провайдера	int (индекс в массиве GUID'ов)	**e_prv_id**	По умолчанию	Журналы
Провайдер	string	**e_prv**	По умолчанию	Журналы
Флаги события	unsigned	**e_fl**	Опционально	Журналы
Источник анализа данных	unsigned	**e_prp**	Опционально	Журналы
TID нити	unsigned	**e_tid**	Опционально	Журналы
ID для создания отношений между событиями	int (индекс в массиве GUID'ов)	**e_act_id**	Опционально	Журналы
Источник события	enum	**e_ds**	Опционально	Журналы
Параметры события	JSON object	**e_p**	Опционально	Журналы
Дополнительные данные	JSON object	**e_ex**	Опционально	Журналы
ID события	unsigned	**e_id**	По умолчанию	Журналы
Имя события	string	**e_name**	Опционально	Журналы
Версия	unsigned	**e_ver**	Опционально	Журналы
Канал	unsigned	**e_ch**	Опционально	Журналы
Уровень	enum	**e_lvl**	По умолчанию	Журналы
ID типа задачи	unsigned	**e_op_id**	Опционально	Журналы
Тип задачи	string	**e_op**	Опционально	Журналы
ID задачи	unsigned	**e_tsk_id**	Опционально	Журналы
Задача	string	**e_tsk**	Опционально	Журналы
Ключевое слово	int64	**e_kw**	Опционально	Журналы
RPC: UUID интерфейса	int (индекс в массиве GUID'ов)	**rpc_id**	По умолчанию	Вызовы: RPC
RPC: Конечная точка	string	**endp**	По умолчанию	Вызовы: RPC
RPC: Сетевой адрес	string (опционально)	**n_addr**	Опционально	Вызовы: RPC
RPC: Уникальный идентификатор процесса клиента	int (индекс в массиве GUID'ов)	**c_uuid**	Опционально	Вызовы: RPC
RPC: PID процесса клиента	unsigned	**c_pid**	По умолчанию	Вызовы: RPC

Назначение	Тип данных	JSON	Отображение/ фильтрация	Подсистема
RPC: Исполняемый файл процесса клиента	string MANGLED	**c_path**	По умолчанию	Вызовы: RPC
RPC: Уникальный идентификатор процесса сервера	int (индекс в массиве GUID'ов)	**s_uuid**	Опционально	Вызовы: RPC
RPC: PID процесса сервера	unsigned	**s_pid**	По умолчанию	Вызовы: RPC
RPC: Исполняемый файл процесса сервера	string MANGLED	**s_path**	По умолчанию	Вызовы: RPC
Количество открытий/созданий файлов с последующими обращениями к ним	unsigned	**cf_ac**	Опционально	Защита файлов
Количество открытых файлов из защищаемых каталогов	unsigned	**cf_oc**	Опционально	Защита файлов
Количество созданных процессом файлов после активации мониторинга	unsigned	**cf_cc**	Опционально	Защита файлов
Количество удалённых файлов в защищаемых каталогах	unsigned	**si_dc**	Опционально	Защита файлов
Количество переименованных файлов в защищаемых каталогах	unsigned	**si_rc**	Опционально	Защита файлов
Количество перемещённых файлов в защищаемые каталоги	unsigned	**si_mi**	Опционально	Защита файлов
Количество перемещённых файлов из защищаемых каталогов	unsigned	**si_mo**	Опционально	Защита файлов

Назначение	Тип данных	JSON	Отображение/ фильтрация	Подсистема
Количество файлов из защищаемых каталогов, которые только читали	unsigned	**ro_fc**	Опционально	Защита файлов
Количество файлов из защищаемых каталогов, в которые только писали	unsigned	**wo_fc**	Опционально	Защита файлов
Количество файлов из защищаемых каталогов, которые читали и писали	unsigned	**rw_fc**	Опционально	Защита файлов
Среднее значений файловой энтропии по чтению	unsigned	**pr_re**	Опционально	Защита файлов
Среднее значений файловой энтропии по записи	unsigned	**pr_we**	Опционально	Защита файлов
Правило блокировки процесса	unsigned	**pr_lr**	Опционально	Защита файлов
Реакция модуля на идентификацию шифровальщика	unsigned	**pr_ra**	Опционально	Защита файлов
Количество файлов с нарушенной целостностью	unsigned	**a_fcc**	Опционально	Защита файлов
Количество файлов с превышенной энтропией	unsigned	**a_eoc**	Опционально	Защита файлов
Количество расширений файлов из которых читали	unsigned	**exrac_**	Опционально	Защита файлов
Количество расширений файлов в которые писали	unsigned	**exwac_**	Опционально	Защита файлов
Количество уникальных расширений файлов из которых только читали	unsigned	**exurac**	Опционально	Защита файлов

Назначение	Тип данных	JSON	Отображение/ фильтрация	Подсистема
Количество уникальных расширений файлов в которые только писали	unsigned	**exuwac**	Опционально	Защита файлов
Категории файлов, к которым осуществлялся доступ	unsigned	**gf_am**	Опционально	Защита файлов
Категории файлов, из которых производилось чтение	unsigned	**gf_rm**	Опционально	Защита файлов
Категории файлов, в которые производилось запись	unsigned	**gf_wm**	Опционально	Защита файлов
Категории файлов, которые удалялись	unsigned	**gf_dm**	Опционально	Защита файлов
Группа, к которой относится файл	unsigned	**gf_ai**	Опционально	Защита файлов

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

JSON-объект может использоваться аналитиком для анализа инцидентов или ретроспективного анализа событий и 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 {...} (рис. 87).

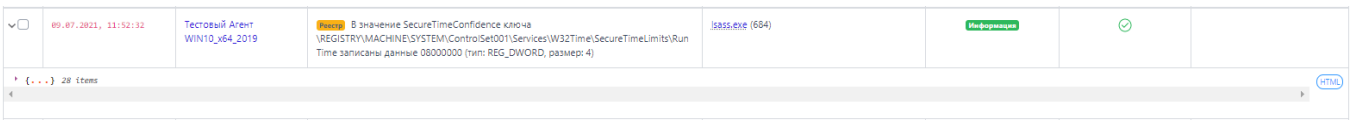


Рисунок 87 – Отображение JSON-объекта в свернутом виде

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. 88).

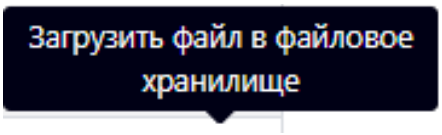


Рисунок 88 – Сообщение о загрузке файла в файловое хранилище

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. 89).

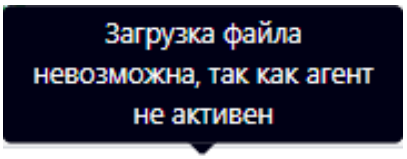


Рисунок 89 – Сообщение о том, что загрузка файла невозможна

Если агент, на котором произошло событие, активен и ссылка на скачивание файла доступна, то при нажатии кнопки отправляется запрос на загрузку файла и в нижней части страницы появляется сообщение **Отправлена команда на загрузку файла** (рис. 90).

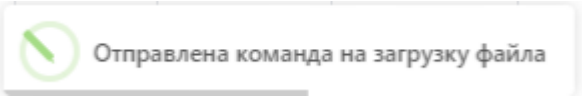


Рисунок 90 – Сообщение об отправке команды на загрузку файла

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 сервером аналитики объекта (рис. 91):

– ip-адрес;

– имя домена;

– хеш файла.

В верхней части карточки с кратким отчетом сервера аналитики содержится наименование или название проверяемого объекта и сообщение Данные сервера аналитики. 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 **Отчет сервера аналитики**, нажав на кнопку **Перейти к отчету**.

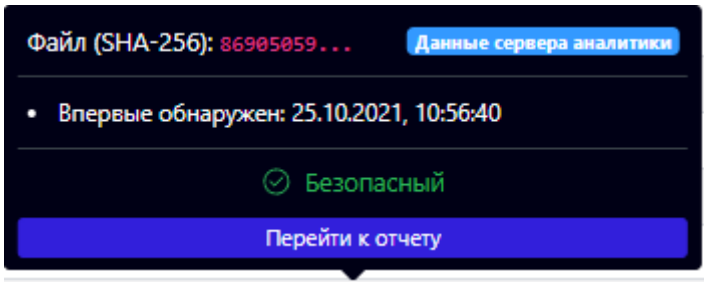


Рисунок 91 – Карточка информации о проверке объекта сервером аналитики

Проверяемые объекты в зависимости от содержания отчета отображаются на странице **Активность** в различной цветовой гамме. Объекты, которые сервер аналитики 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 сервере аналитики отсутствует или не проверялась, отмечаются серым цветом (74.125.131.94). Карточка для вредоносного объекта показана на рисунке 92.

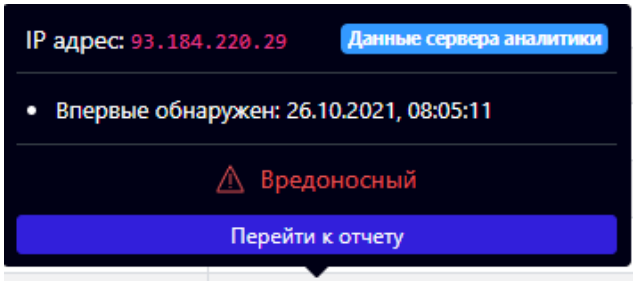


Рисунок 92 – Карточка сервера аналитики для вредоносного объекта

Карточка сервера аналитики для объекта, информация по которому обрабатывается в текущий момент, представлена на рисунке 93.

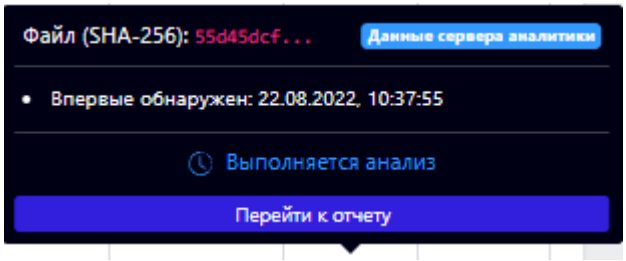


Рисунок 93 – Карточка сервера аналитики для объекта, анализируемого в настоящее время

Карточка сервера аналитики для объекта, информация по которому отсутствует, представлена на рисунке 94.

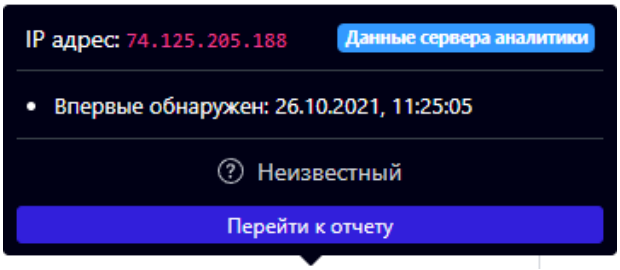


Рисунок 94 – Карточка сервера аналитики для отсутствующего в базе объекта

Для локальных ip-адресов и доменов проверка сервером аналитики не выполняется (рис. 95).

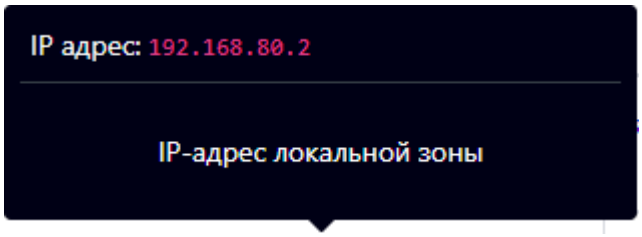


Рисунок 95 – Карточка сервера аналитики для локального ip-адреса

При отсутствии в базе сервера аналитики информации о выбранном артефакте или недоступности сервера аналитики пользователю выводится сообщение, представленное на рисунке 96.

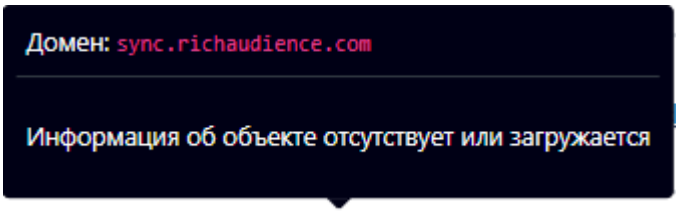


Рисунок 96 – Информация сервера аналитики недоступна

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).

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 или 100 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) 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 97. 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 97 – Выбор периода регистрации события из списка

Для задания параметра из календаря следует установить флаг **Календарь**, как показано на рисунке 98. 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. 99).

Рисунок 98 – Выбор периода регистрации события в календаре

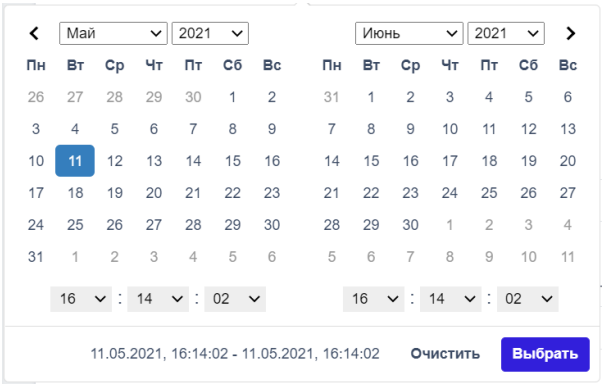


Рисунок 99 – Календарь для выбора периода регистрации событий

Значение выбранного временного интервала отобразится в поле **Период регистрации (на сервере)** (рис. 100).

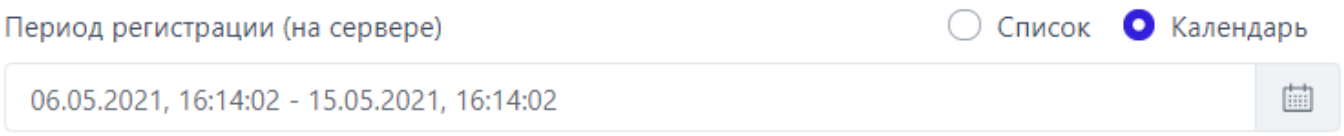


Рисунок 100 – Отображение периода регистрации

Для очистки установленного интервала необходимо нажать кнопку **Очистить** (см. рис. 99).

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) SSL HELLO;

7) Другие обнаружения;

8) Обнаружение: срабатывание индикатора компрометации;

9) Открытие локального порта на прием (LISTEN).

Рядом с обозначением подтипа содержится его цифровое значение **st**, которое можно использовать при составлении DSL-запросов.

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, например, в строке введен запрос ***chrome.exe***. В таком случае 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. 101).

```
app:*dns.exe  -  название процесса "dns.exe"
act:1  -  предпринятое действие "Разрешено"
act:0 AND svrt:4  -  предпринятое действие "Запрещено" и критичность "Критичная"
r_p:[80 TO 90] AND r_ip:217.65.12.8  -  удаленный порт с номером от 80 до 90 и удаленный IP-адрес 217.65.12.8
t:0 AND size:>=100  -  сетевые события, у которых размер сообщения больше 100 байт
NOT act:1  -  события, не имеющие статус "Разрешено"
```

Рисунок 101 – 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. 102), необходимо выбрать операцию **Новый.**

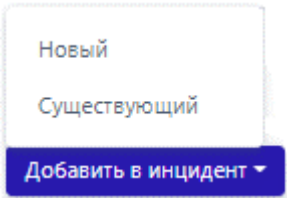


Рисунок 102 – Список операций с событиями на странице «Активность»

В результате выполнения операции откроется окно **Добавление событий в новый инцидент** (рис. 103), 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.

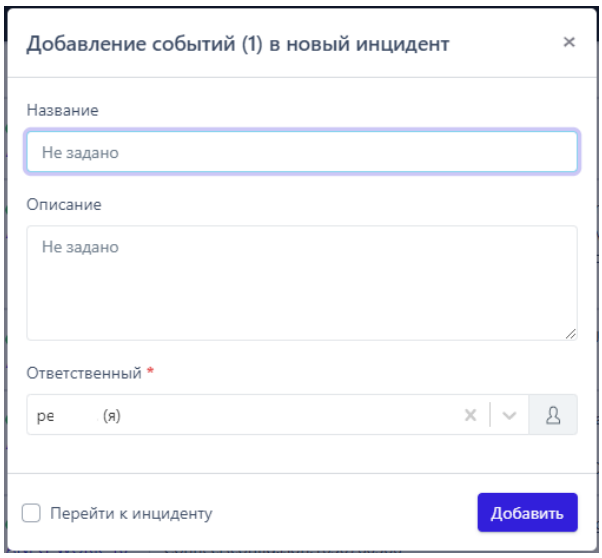


Рисунок 103 – Добавление событий в новый инцидент

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** (см. рис. 102), следует выбрать операцию **Существующий**. В результате выполнения операции откроется окно **Добавление событий в инцидент** (рис. 104), в котором в поле **Инцидент** необходимо выбрать существующий инцидент.

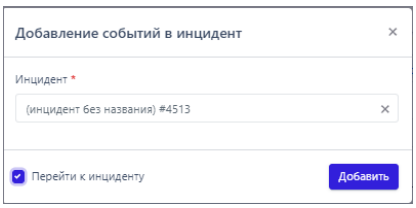
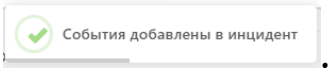


Рисунок 104 – Добавление события в существующий инцидент

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, после чего в нижней части экрана появится всплывающее сообщение вида 

. 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).

Общие сведения о событиях

Для каждого из событий, детектируемых программой, карточка события будет отличаться в зависимости от источника обнаруженной активности. Поля карточки добавляются и изменяются в зависимости от типа или подтипа события. Некоторые поля могут встречаться в разных карточках событий, вне зависимости от подтипа событий.

Каждому полю соответствует его обозначение в формате JSON, которое можно использовать для написания DSL-запросов на страницах **Активность** и **Список агентов**, а также индикаторов атак.

Описание подтипов (**st**) событий мониторинга сети представлено в таблице 9.

Таблица 9 – События мониторинга сети

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

Номер протокола **proto** может принимать следующие значения:

– 6 (TCP);

– 17 (UDP);

– 1 (ICMP);

– 58 (ICMPv6).

Тип DNS-запроса **dnsq_t** может принимать следующие значения:

– 1 (A);

– 5 (CNAME);

– 1C (AAAA);

– 0F (MX);

– 21 (SRV);

– 0C (PTR);

– 2 (остальные типы DNS-запросов).

Мониторинг файловых операций

Описание подтипов (**st**) событий мониторинга файловых операций представлено в таблице 10.

Таблица 10 – События мониторинга файловых операций

Код события	Имя события	Описание
0	Файлы: Создан новый файл	Создан новый файл **name**
1	Файлы: Файл переименован	Файл **name** переименован в **fnew**
2	Файлы: Удален файл	Удален файл **name**
3	Файлы: У файла изменен атрибут или время создания	У файла **name** [установлен/снят атрибут "системный" (если присутствует **sys, sys** = 0, то снят, **sys** = 1 - установлен)], [установлен атрибут "скрытый" (если присутствует **hdn**)], [изменено время создания с **old_t** на **new_t** (если присутствуют **old_t** и **new_t**)]
4	Файлы: Другие обнаружения	<Описание кода **detect**>
7	Файлы: Файл был модифицирован	Файл **name** был модифицирован
8	Файлы: Файл был прочитан	Файл **name** был прочитан
12	Файлы: прямой доступ к тому на чтение	Прямой доступ к диску (тому) **name** на чтение
13	Файлы: Прямой доступ к тому на запись	Прямой доступ к диску (тому) **name** на запись
14	Файлы: Создан именованный канал	Создан именованный канал **name**
15	Файлы: Подключение к именованному каналу	Подключение к именованному каналу **name**
16	Файлы: Обнаружение: доступ к файлу	Доступ к файлу **name**
17	Файлы: Обнаружение: срабатывание индикатора компрометации для файла	Срабатывание индикатора компрометации для файла **name**

Код события	Имя события	Описание
18	Файлы: Обнаружение: срабатывание исключения для файла	Срабатывание исключения для файла **name**
19	Файлы: Обнаружение: файл классифицирован как вредоносный (ML на агенте)	Файл **name** классифицирован как вредоносный (ML на агенте)
20	Файлы: Обнаружение: файл классифицирован как вредоносный (Yara-правила)	Файл **name** классифицирован как вредоносный (Yara-правила)
21	Файлы: Обнаружение: подмена образа процесса в памяти	Подмена образа процесса в памяти: HERPADERPING (имя образа: **name**)
22	Файлы: Создан альтернативный поток для файла	Создан альтернативный поток для файла **name**

Поле **ftype** (тип файла) событий мониторинга файлов и процессов может принимать следующие значения:

– 2 (исполняемый файл);

– 3 (файл с активным содержанием);

– 4 (скрипт Powershell).

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

– 0 (нет подписи);

– 1 (есть подпись);

– 2 (неизвестно).

Поле **attr** (атрибуты файла) событий мониторинга файлов и процессов может принимать значения, указанные в документации Microsoft.

Мониторинг реестра

Описание подтипов (**st**) событий мониторинга реестра представлено в таблице 11.

Таблица 11 – Подтипы событий мониторинга реестра

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

Мониторинг событий журналов Windows

Для событий, источником которых являются журналы ETW-подсистемы Windows, представлен только один подтип **Событие журнала** (**st:0**).

Поле **e_lvl** (уровень событий провайдера) подсистемы мониторинга журналов Windows может принимать следующие значения:

– 1 (критическая ошибка);

– 2 (ошибка);

– 3 (предупреждение);

– 4 (информация);

– 0 или 5 (подробно).

Мониторинг процессов

Описание подтипов (**st**) событий мониторинга процессов представлено в таблице 12.

Таблица 12 – Подтипы событий мониторинга процессов

Код события	Имя события	Описание
0	Процессы: Загрузка драйвера	Загрузка драйвера **path**
1	Процессы: Старт процесса	Старт процесса командой **cmdl** из **cpath** (**cpid**), нить = **whotid** (из модуля **who**)
2	Процессы: Завершение процесса	Завершение процесса с кодом **code**
3	Процессы: Загрузка образа	Загрузка образа **path**
6	Процессы: Доступ к процессу	Доступ к процессу **tpath** (**tpid**) с правами **dsrd**, {разрешено ИЛИ запрещено **dsrd-grnt**}, нить=**whotid** (из модуля **who**)
7	Процессы: Создание нити в стороннем процессе	Создание нити **tid** в процессе **tpath** (**tpid**), нить = **whotid** (из модуля **who**)
13	Процессы: Обнаружение: подмена командной строки	Подмена командной строки с **cmdl1** на **cmdl**
15	Процессы: Доступ к рабочему столу	Доступ к рабочему столу **desk** с правами **dsrd**, { разрешено ИЛИ запрещено **dsrd-grnt** }, нить = **whotid** (из модуля **who**)
16	Процессы: Обнаружение: изменение системной защиты процесса	Изменение системной защиты процесса с **prot** на **prot1**
18	Процессы: Доступ к нити процесса	Доступ к нити **tid** процесса **tpath** (**tpid**) с правами **dsrd**, {разрешено ИЛИ запрещено **dsrd-grnt**}, нить = **whotid** (из модуля **who**)
20	Процессы: Загрузка образа в сторонний процесс	Загрузка образа **path** в процесс **tpath** (**tpid**), нить = **whotid** (из модуля **who**)
23	Процессы: Другие обнаружения	Описание кода **detect**

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

– 0 (низкий);

– 1 (средний);

– 2 (высокий).

Мониторинг сессий

Описание подтипов (**st**) событий мониторинга сессий представлено в таблице 13.

Таблица 13 – Подтипы событий пользовательских сессий

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

Примечание

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

Параметр **sess_opt** (тип дистанционного управления) может принимать одно из значений, указанных в таблице 14.

Таблица 14 – Типы дистанционного управления

Значение	Описание
0	Дистанционное управление отключено

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

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

– 0 (консольная сессия);

– 2 (RDP-сессия).

Мониторинг событий защиты файлов от шифровальщиков

Описание подтипов (**st**) событий мониторинга защиты файлов от шифровальщиков представлено в таблице 15.

Таблица 15 – Подтипы событий anti-ransomware-модуля

Код события	Имя события	Описание	Расшифровка
0	ARW_EVENT_RANSOMWARE_PROCESS	Заблокирован вредоносный процесс	Заблокирован вредоносный процесс
1	ARW_EVENT_FILE_RESERVED	Создана резервная копия файла	Создана резервная копия файла **name**

Описание подтипов событий мониторинга системы представлено в таблице 16.

Таблица 16 – Подтипы событий мониторинга системы

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

Поле **wmi** (тип события WMI) мониторинга системы может принимать значения, представленные в таблице 17.

Таблица 17 – Подтипы wmi

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

Поле **atck** (атаки на Kerberos: подтип атаки) мониторинга системы может принимать значения, представленные в таблице 18.

Таблица 18 – Подтипы атак

Код события	Имя события	Описание
0	STEAL_OR_FORGE_KERBEROS_TICKETS_TYPE_GOLDEN_TICKET	Атака Golden ticket

1	STEAL_OR_FORGE_KERBEROS_TICKETS_TYPE_SILVER_TICKET	Атака Silver ticket
2	STEAL_OR_FORGE_KERBEROS_TICKETS_TYPE_KERBEROASTING	Атака Kerberoasting
3	STEAL_OR_FORGE_KERBEROS_TICKETS_TYPE_AS_REP_ROASTING	Атака AS-REP roasting

Поля **goldent_r**, **silvert_r**, **kerberoasting_r** и **asreproasting_r** в карточках мониторинга системы содержат значения для подтипов атак на Kerberos, расшифровываемые в таблице 19. Эта информация вместе с другими параметрами отображается на странице **Активность** в поле **Описание**. Примеры отображения подтипов атак на Kerberos приведены в таблице 20.

Таблица 19 – Подтипы атак на Kerberos

Код события	Имя события	Описание
0	KERBEROS_ATTACK_REASON_NO_TGT	Отсутствует запрос TGT
1	KERBEROS_ATTACK_REASON_LIFETIME_TICKET	Превышено время жизни билета, установленное групповой политикой
2	KERBEROS_ATTACK_REASON_WEAK_ENCRYPTION	Возможна атака, т.к. используется слабый алгоритм шифрования
3	KERBEROS_ATTACK_REASON_INTEGRITY_FAILED	Билет зашифрован с помощью не сессионного ключа
4	KERBEROS_ATTACK_REASON_DOMAINNAME_IS_EMPTY	Имя домена не задано
5	KERBEROS_ATTACK_REASON_DOMAINNAME_IS_INVALID	Неправильное имя домена
6	KERBEROS_ATTACK_REASON_LARGE_COUNT_REQUEST_TGS	Большое количество запросов билетов TGS со слабым шифрованием

Таблица 20 – Примеры описания атак на странице «Активность»

Причина	Описание
0	[Система] Атака Golden ticket. Отсутствует запрос TGT. Пользователь: **goldent_u@goldent_d**, ip-адрес: **goldent_ip**
1	[Система] Атака Silver ticket. Имя домена не задано. Пользователь: **silvert_u@silvert_d**, ip-адрес: **silvert_ip**

2	[Система] Атака Kerberoasting. Возможна атака, т.к. используется слабый алгоритм шифрования. Пользователь: **kerberoasting_u@kerberoasting_d**, ip-адрес: **kerberoasting_ip**
3	[Система] Атака AS-REP roasting. Используется слабый алгоритм шифрования. Пользователь: **asreproasting_u@asreproasting_d**, ip-адрес: **asreproasting_ip**

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

– 1 (штатное завершение работы компьютера);

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

– 3 (штатная остановка агента).

Мониторинг RPC-вызовов

Описание подтипов (**st**) событий RPC-вызовов представлено в таблице 21.

Таблица 21 – Подтипы событий монитора вызовов

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

6.5.3. Проверка сервером аналитики

Общая информация

Сервер аналитики сопоставляет и анализирует данные компьютерных угроз из нескольких источников в режиме реального времени для поддержки защитных действий программы «RT Protect EDR». 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) NSRL;

2) Kaspersky TI;

3) Sophos;

4) Внешние источники;

5) VirusTotal;

6) Заключение аналитика;

7) YARA;

8) IOC;

9) Whois.

Вердикты сервера аналитики равнозначны с аналитикой сервера EDR. Например, если вердикт сервера аналитики 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 сервер аналитики как безопасный. Если правила сервера аналитики и правила сервера EDR будут дублировать друг друга, то в случае обнаружения вредоносной активности создадутся два независимых инцидента. Страницы отчета сервера аналитики открываются на вкладке **Общая информация**, которая содержит сводные данные из всех доступных для выбранного артефакта источников (рис. 105).

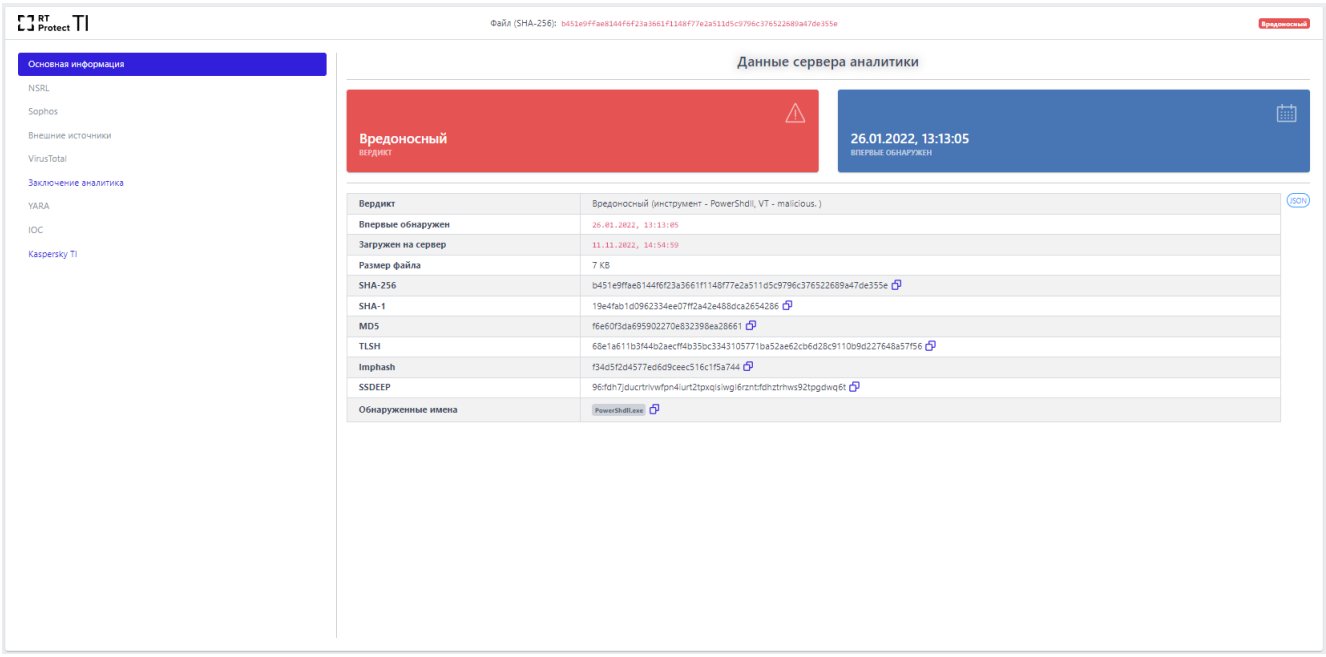


Рисунок 105 – Отчет сервера аналитики

В верхней части страницы отчета отображается наименование и значение артефакта и вердикт сервера аналитики. На левой панели отчета отображаются вкладки с наименованиями источников данных, от которых были получены сведения для вынесенного сервером аналитики 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 JSON . При нажатии кнопки формат отчета меняется на JSON-формат (рис. 106).

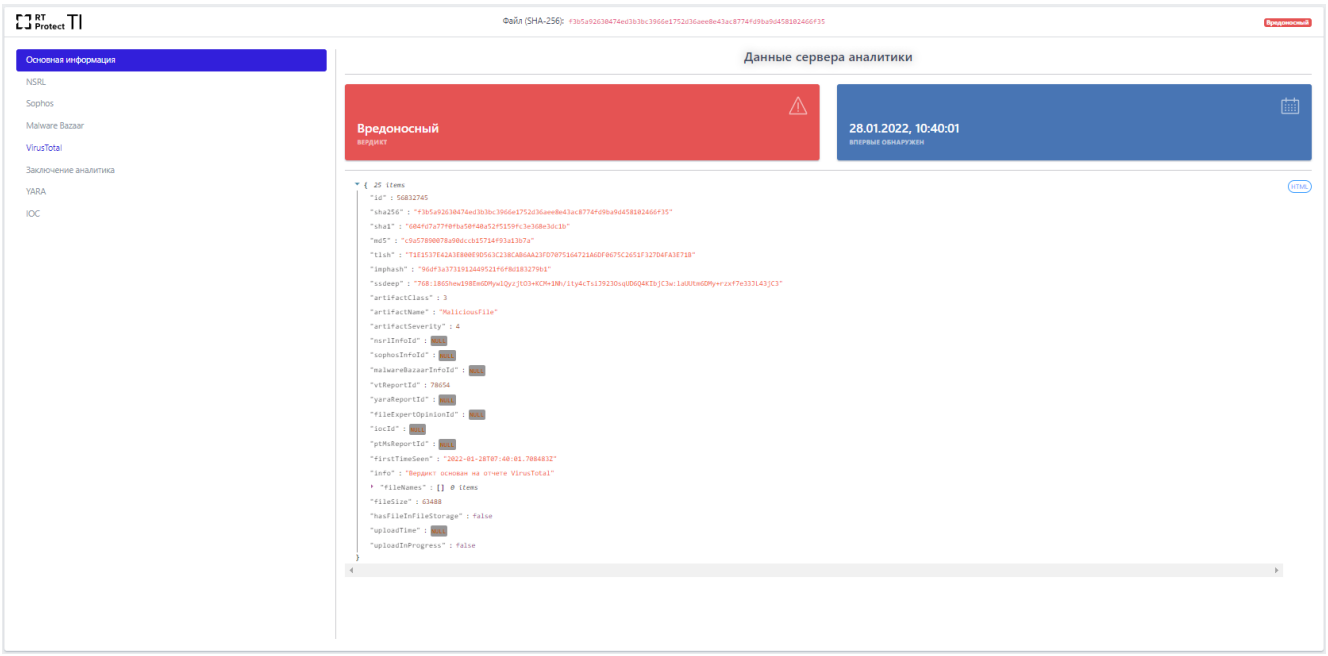


Рисунок 106 – Отчёт в JSON

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 «RT Protect EDR» 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. 107).

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**.

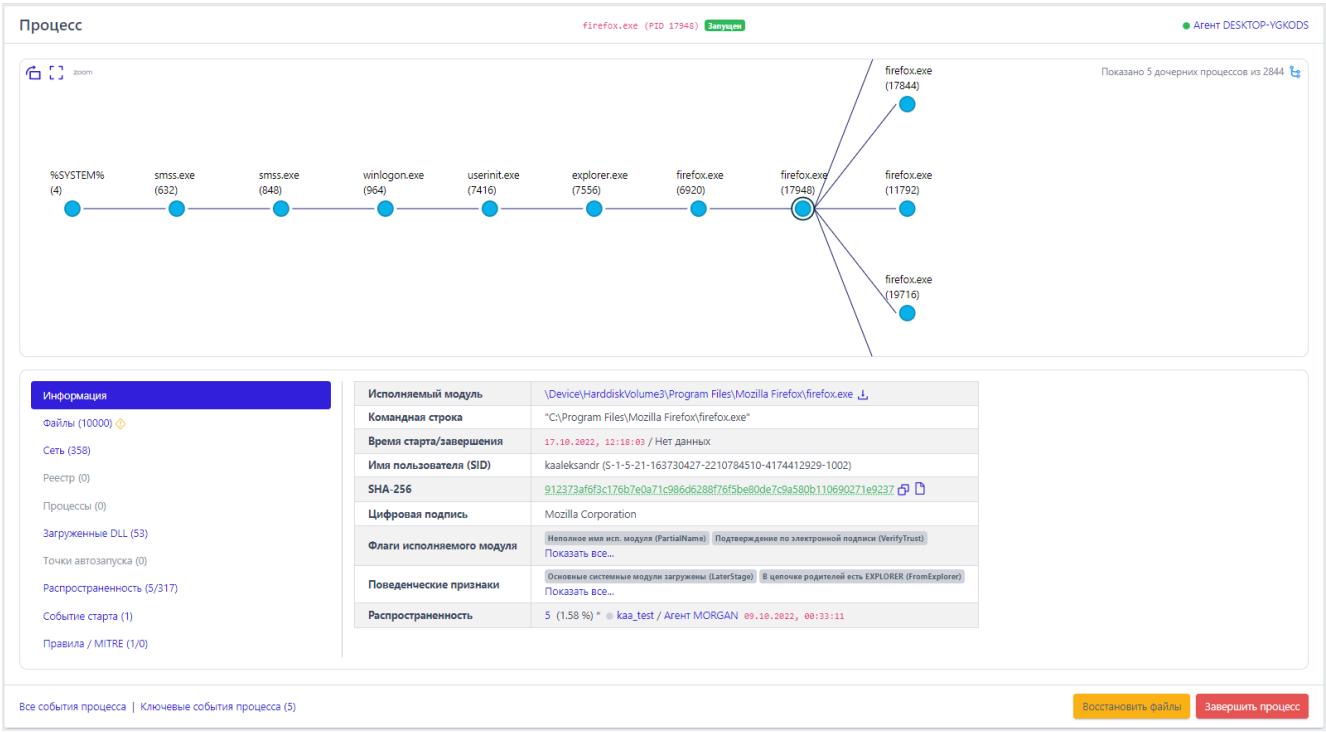


Рисунок 107 – Информация о процессе

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 (рис. 108).

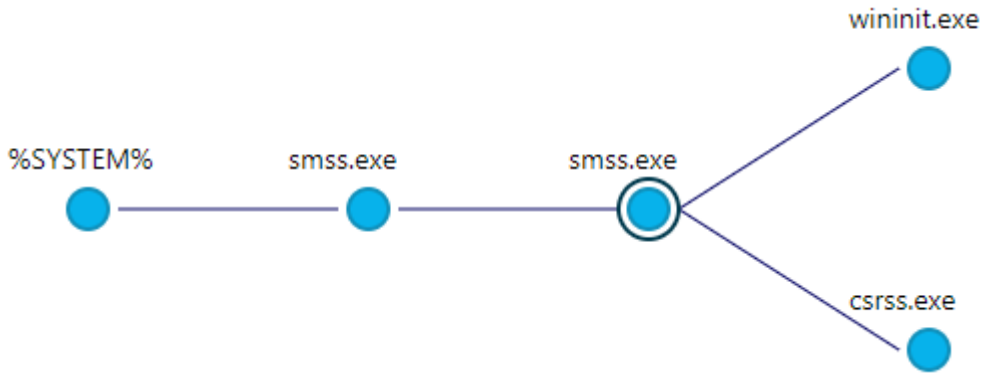


Рисунок 108 – Дерево процесса

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 (рис. 109).

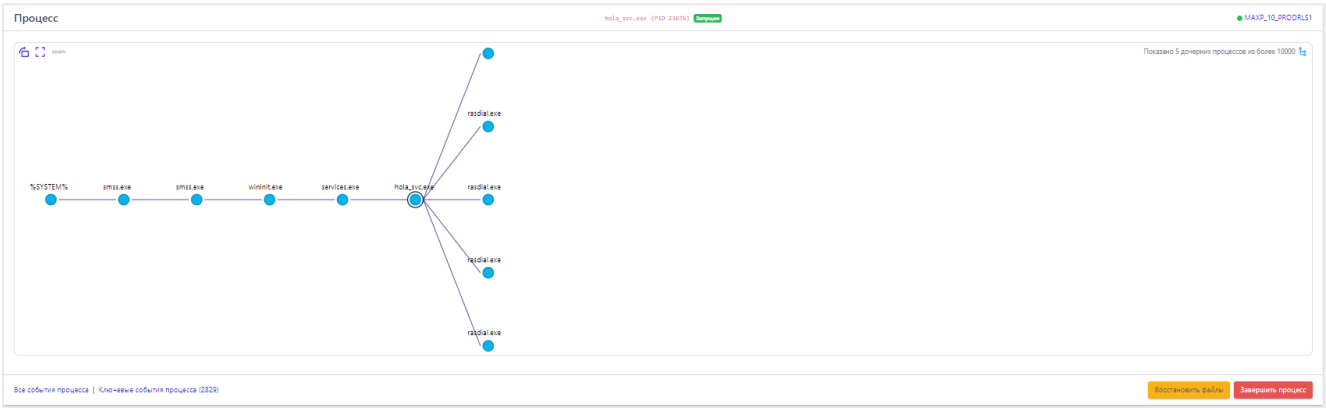


Рисунок 109 – Изменение размера области дерева

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 (рис. 110).

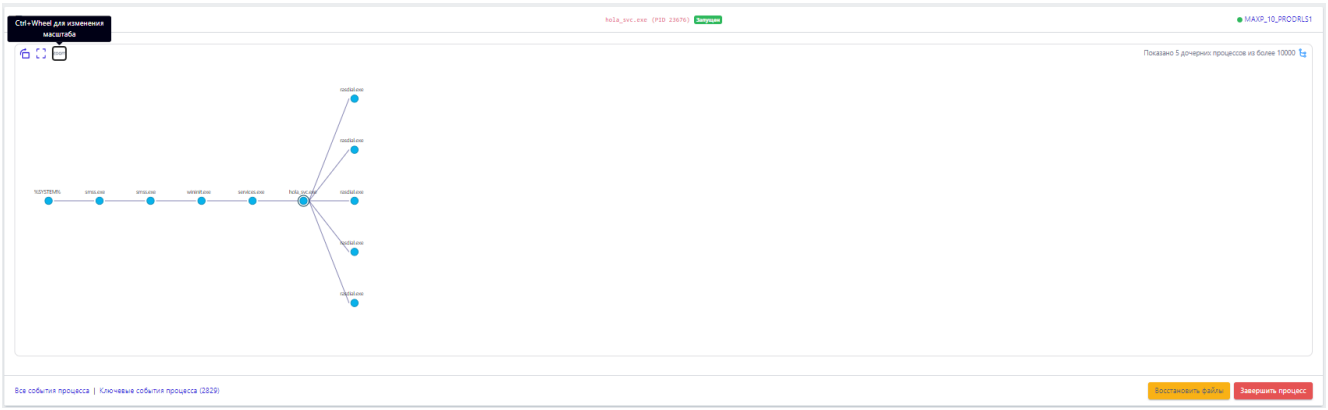


Рисунок 110 – Изменение масштаба дерева процессов

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 (см. рис. 110). Чтобы возвратить дерево в исходное состояние, то есть убрать дочерние процессы выбранного процесса, необходимо нажать ЛКМ на значок еще раз.

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

В таблице отображаются следующие вкладки:

1) Информация;

2) Файлы;

3) Сеть;

4) Реестр;

5) 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) Все события процесса ;

2) Ключевые события процесса (1) ;

3) Восстановить файлы ;

4) Завершить процесс .

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. 111).

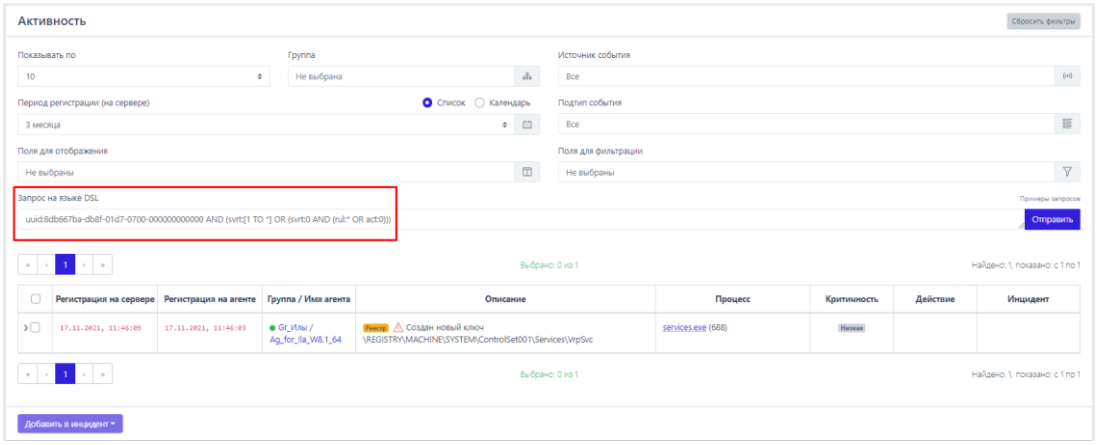


Рисунок 111 – Ключевые события процесса

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 (рис. 112):

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.

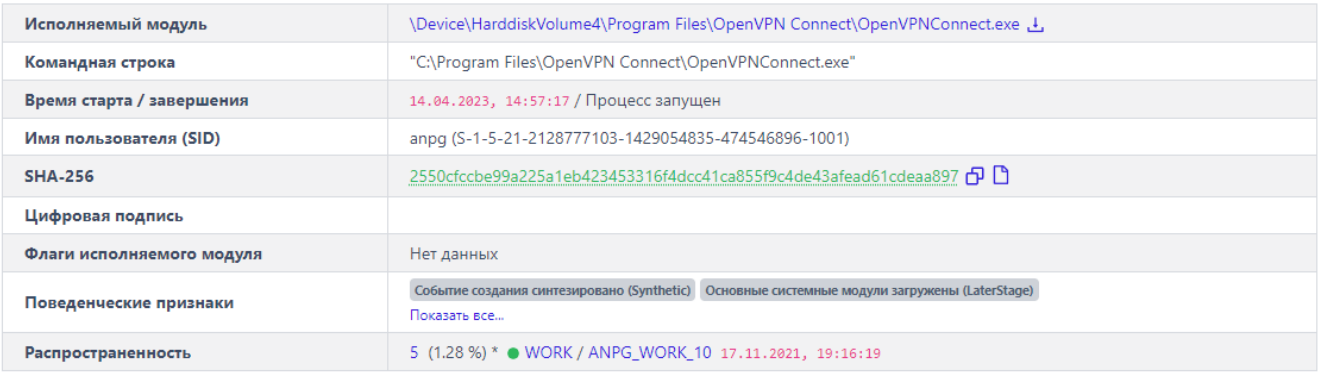


Рисунок 112 – Общая информация о процессе

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 6.6.7).

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 сервера аналитики 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. 113).

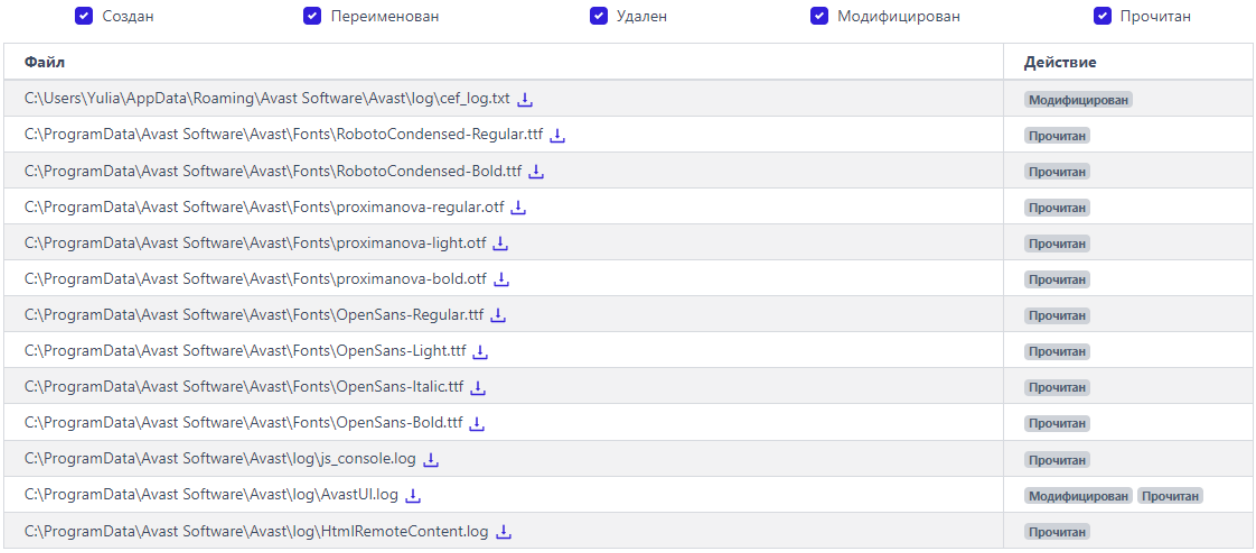


Рисунок 113 – Информация о файлах процесса

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 сервера аналитики или Hex-редактора.

Если среди действий с файлом, присутствующим в списке, было удаление, то он помечается значком . При наведении курсора мыши на значок пользователю выводится предупреждающее сообщение (рис. 114).

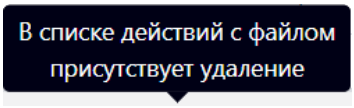


Рисунок 114 – Сообщение о присутствии в списке удаления файла

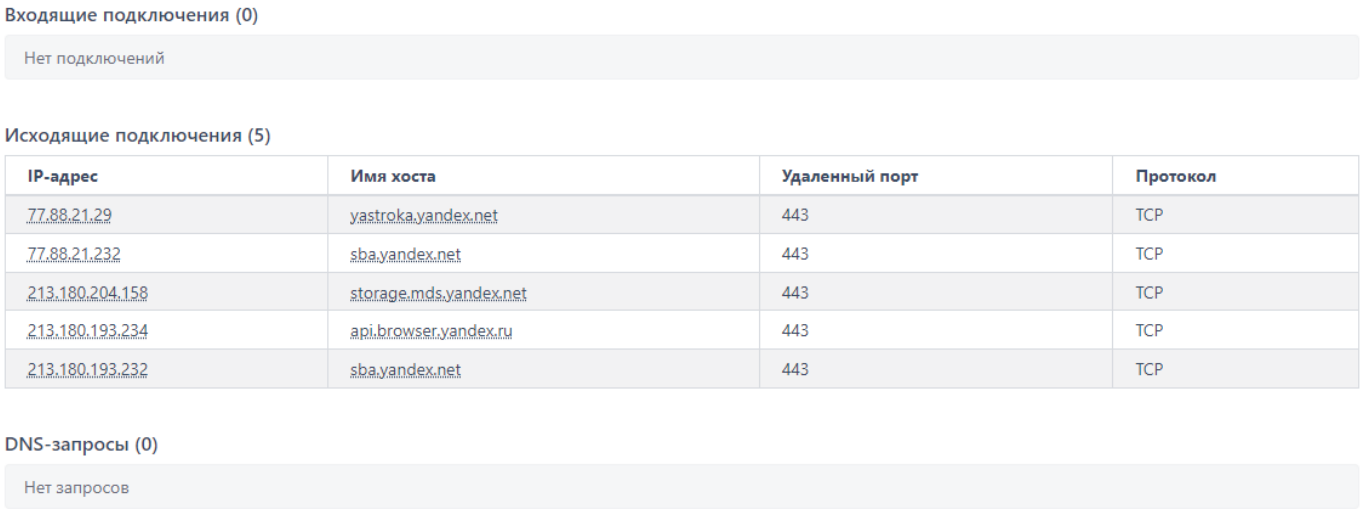
Вкладка «Сеть»

Во вкладке **Сеть** отображается информация о сетевых подключениях процесса (рис. 115):

1) Входящие подключения;

2) Исходящие подключения;

3) DNS-запросы.



Входящие подключения (0)

Нет подключений

Исходящие подключения (5)

IP-адрес	Имя хоста	Удаленный порт	Протокол
77.88.21.29	yastroka.yandex.net	443	TCP
77.88.21.232	sba.yandex.net	443	TCP
213.180.204.158	storage.mds.yandex.net	443	TCP
213.180.193.234	api.browser.yandex.ru	443	TCP
213.180.193.232	sba.yandex.net	443	TCP

DNS-запросы (0)

Нет запросов

Рисунок 115 – Информация о сетевых подключениях процесса

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.

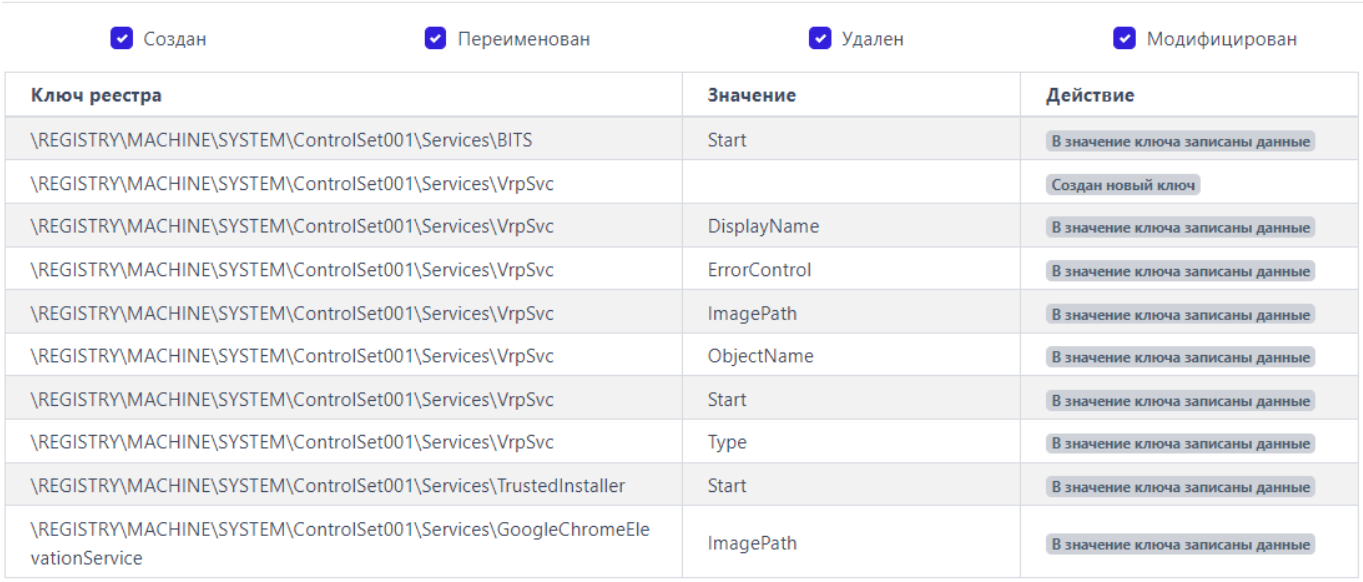


Рисунок 116 – Ключи реестра, на которые действовал процесс

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.

Информация разбита на две информационные области **Доступ к процессу** и **Доступ к нити процесса** (рис. 117).

Доступ к процессу (6)

Имя исполняемого образа	Запрошенные права	Предоставленные права	Кол-во событий
C:\Windows\System32\smss.exe	0x001FFFFF (PROCESS_ALL_ACCESS)	0x001FFFFF (PROCESS_ALL_ACCESS)	4
C:\Windows\System32\autochk.exe	0x001FFFFF (PROCESS_ALL_ACCESS)	0x001FFFFF (PROCESS_ALL_ACCESS)	1
C:\Windows\System32\csrss.exe	0x00101441 (SYNCHRONIZE, PROCESS_DUP_HANDLE, PROCESS_QUERY_INFORMATION, PROCESS_QUERY_LIMITED_INFORMATION, PROCESS_TERMINATE)	0x00101441 (SYNCHRONIZE, PROCESS_DUP_HANDLE, PROCESS_QUERY_INFORMATION, PROCESS_QUERY_LIMITED_INFORMATION, PROCESS_TERMINATE)	2
C:\Windows\System32\wininit.exe	0x001FFFFF (PROCESS_ALL_ACCESS)	0x001FFFFF (PROCESS_ALL_ACCESS)	1
C:\Windows\System32\winlogon.exe	0x001FFFFF (PROCESS_ALL_ACCESS)	0x001FFFFF (PROCESS_ALL_ACCESS)	1
C:\Windows\System32\svchost.exe	0x00101441 (SYNCHRONIZE, PROCESS_DUP_HANDLE, PROCESS_QUERY_INFORMATION, PROCESS_QUERY_LIMITED_INFORMATION, PROCESS_TERMINATE)	0x00101441 (SYNCHRONIZE, PROCESS_DUP_HANDLE, PROCESS_QUERY_INFORMATION, PROCESS_QUERY_LIMITED_INFORMATION, PROCESS_TERMINATE)	1

Доступ к нити процесса (4)

Имя исполняемого образа	Запрошенные права	Предоставленные права	Кол-во событий
C:\Windows\System32\smss.exe	0x001FFFFF (THREAD_ALL_ACCESS)	0x001FFFFF (THREAD_ALL_ACCESS)	2
C:\Windows\System32\autochk.exe	0x001FFFFF (THREAD_ALL_ACCESS)	0x001FFFFF (THREAD_ALL_ACCESS)	1
C:\Windows\System32\wininit.exe	0x001FFFFF (THREAD_ALL_ACCESS)	0x001FFFFF (THREAD_ALL_ACCESS)	1
C:\Windows\System32\winlogon.exe	0x001FFFFF (THREAD_ALL_ACCESS)	0x001FFFFF (THREAD_ALL_ACCESS)	1

Рисунок 117 – Информация на вкладке «Процессы»

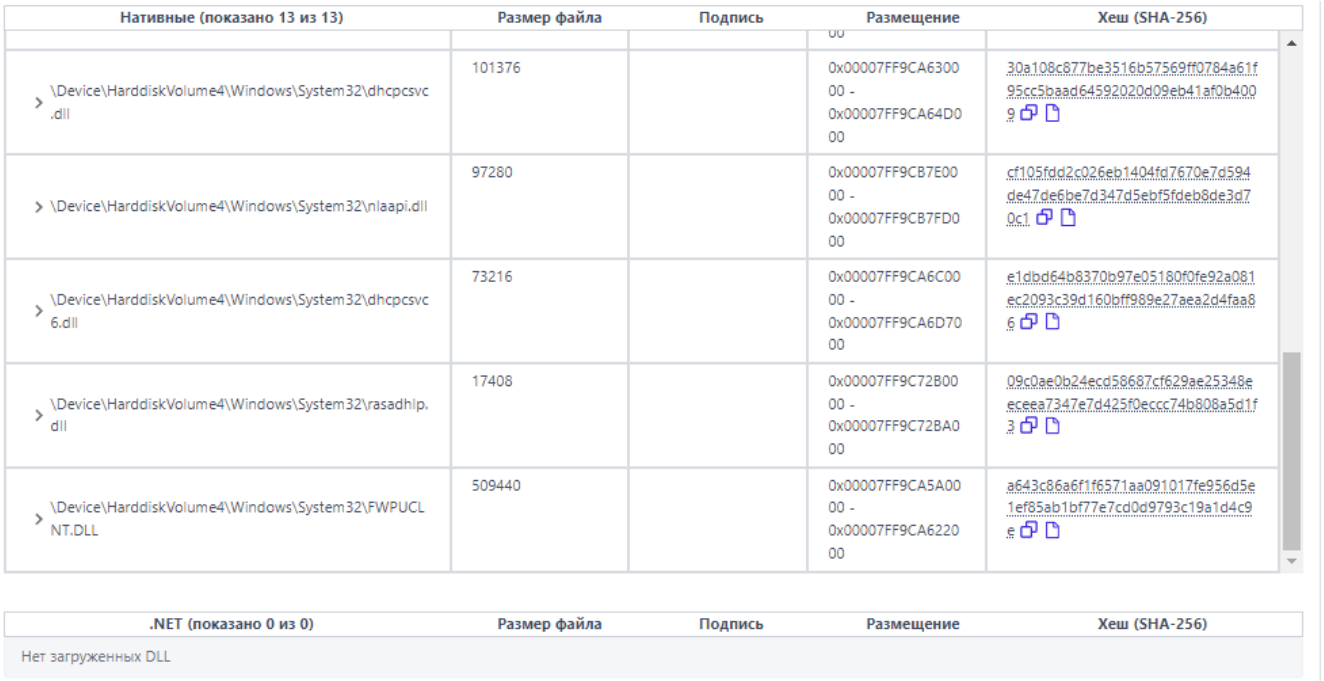
Информация представлена в таблице, которая содержит следующие поля: **Имя исполняемого образа, Запрошенные права, Предоставленные права, Кол-во событий.**

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. 118).



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 118 – Список загруженных библиотек DLL

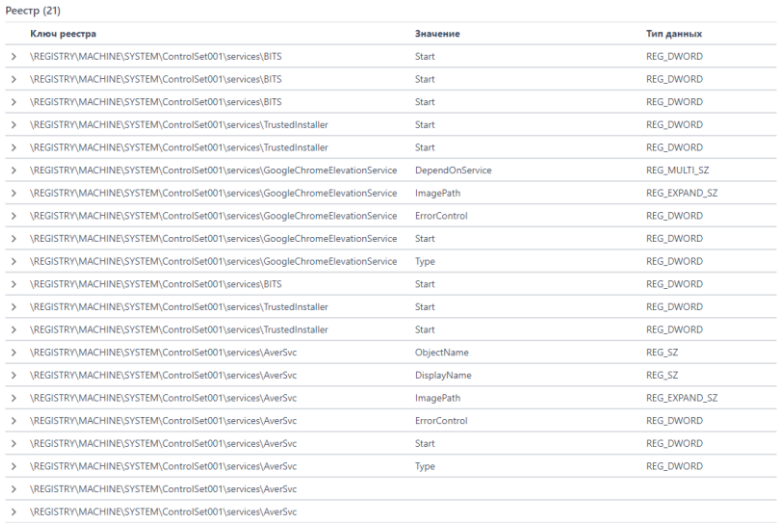
Важно

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 (рис. 119).



Реестр (21)

	Ключ реестра	Значение	Тип данных
>	\REGISTRY\MACHINE\SYSTEM\ControlSet001\services\BITS	Start	REG_DWORD
>	\REGISTRY\MACHINE\SYSTEM\ControlSet001\services\BITS	Start	REG_DWORD
>	\REGISTRY\MACHINE\SYSTEM\ControlSet001\services\BITS	Start	REG_DWORD
>	\REGISTRY\MACHINE\SYSTEM\ControlSet001\services\TrustedInstaller	Start	REG_DWORD
>	\REGISTRY\MACHINE\SYSTEM\ControlSet001\services\TrustedInstaller	Start	REG_DWORD
>	\REGISTRY\MACHINE\SYSTEM\ControlSet001\services\GoogleChromeElevationService	DependOnService	REG_MULTI_SZ
>	\REGISTRY\MACHINE\SYSTEM\ControlSet001\services\GoogleChromeElevationService	ImagePath	REG_EXPAND_SZ
>	\REGISTRY\MACHINE\SYSTEM\ControlSet001\services\GoogleChromeElevationService	ErrorControl	REG_DWORD
>	\REGISTRY\MACHINE\SYSTEM\ControlSet001\services\GoogleChromeElevationService	Start	REG_DWORD
>	\REGISTRY\MACHINE\SYSTEM\ControlSet001\services\GoogleChromeElevationService	Type	REG_DWORD
>	\REGISTRY\MACHINE\SYSTEM\ControlSet001\services\BITS	Start	REG_DWORD
>	\REGISTRY\MACHINE\SYSTEM\ControlSet001\services\TrustedInstaller	Start	REG_DWORD
>	\REGISTRY\MACHINE\SYSTEM\ControlSet001\services\TrustedInstaller	Start	REG_DWORD
>	\REGISTRY\MACHINE\SYSTEM\ControlSet001\services\AverSvc	ObjectName	REG_SZ
>	\REGISTRY\MACHINE\SYSTEM\ControlSet001\services\AverSvc	DisplayName	REG_SZ
>	\REGISTRY\MACHINE\SYSTEM\ControlSet001\services\AverSvc	ImagePath	REG_EXPAND_SZ
>	\REGISTRY\MACHINE\SYSTEM\ControlSet001\services\AverSvc	ErrorControl	REG_DWORD
>	\REGISTRY\MACHINE\SYSTEM\ControlSet001\services\AverSvc	Start	REG_DWORD
>	\REGISTRY\MACHINE\SYSTEM\ControlSet001\services\AverSvc	Type	REG_DWORD
>	\REGISTRY\MACHINE\SYSTEM\ControlSet001\services\AverSvc		
>	\REGISTRY\MACHINE\SYSTEM\ControlSet001\services\AverSvc		

Рисунок 119 – Точки автозапуска

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. 120)

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 120 – Вкладка «Распространенность»

Вкладка «Событие старта»

Во вкладке **Событие старта** показана карточка события для старта процесса (рис. 121).

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 121 – 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. 122).

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 122 – 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 сервера аналитики по этой программе (рис. 123). Распространённость программы показывает, на каких агентах появлялся файл с определенной хеш-суммой.

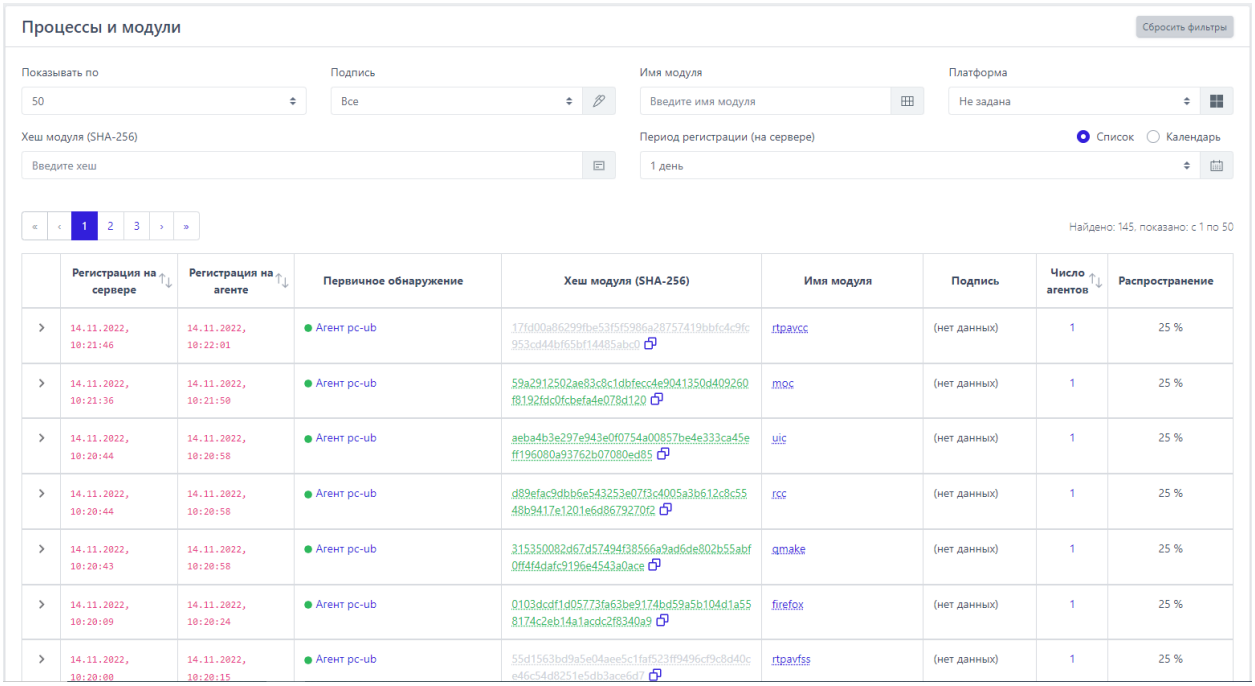


Рисунок 123 – Процессы и модули

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 сервера аналитики 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.

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 внести изменения в конфигурацию отдельно взятой группы агентов: добавить агента, исключить его из группы, создать новую группу и т.д.

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 сервера аналитики, удалять загруженные файлы или просматривать их в Hex-редакторе 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 124.

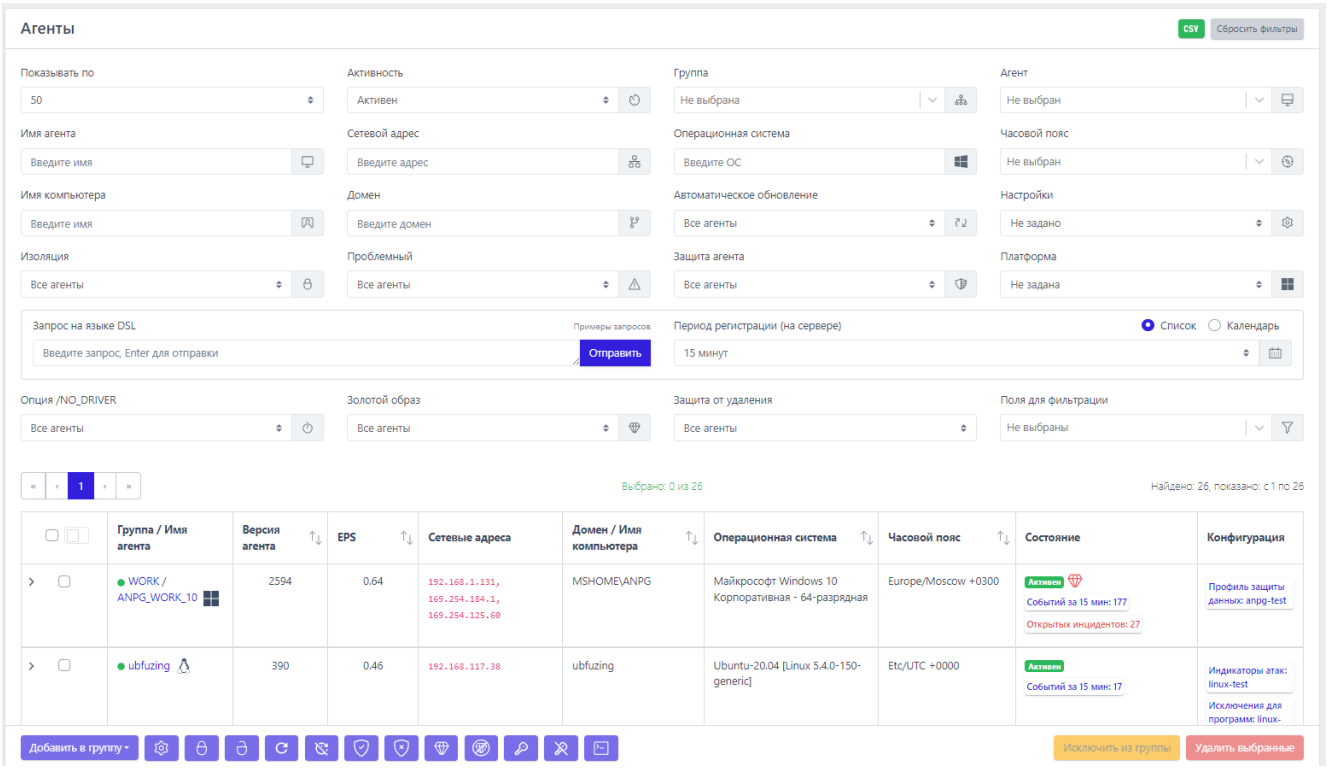


Рисунок 124 – Страница «Агенты»

`Поля фильтрации на странице «Агенты»`

На странице **Агенты** предусмотрены следующие поля фильтрации (рис. 125):

1) **Показывать по;**

2) **Активность;**

3) **Группа;**

4) **Агент;**

5) **Имя агента;**

6) **Сетевой адрес;**

7) **Операционная система;**

8) **Часовой пояс;**

9) **Имя компьютера;**

10) **Домен;**

11) **Автоматическое обновление;**

12) **Настройки;**

13) **Изоляция;**

14) **Проблемный;**

15) **Защита агента;**

16) **Платформа;**

17) **Запрос на языке DSL;**

18) **Период регистрации на сервере;**

19) **Опция /NO_DRIVER;**

20) **Золотой образ;**

21) **Защита от удаления.**

22) **Поля для фильтрации;**

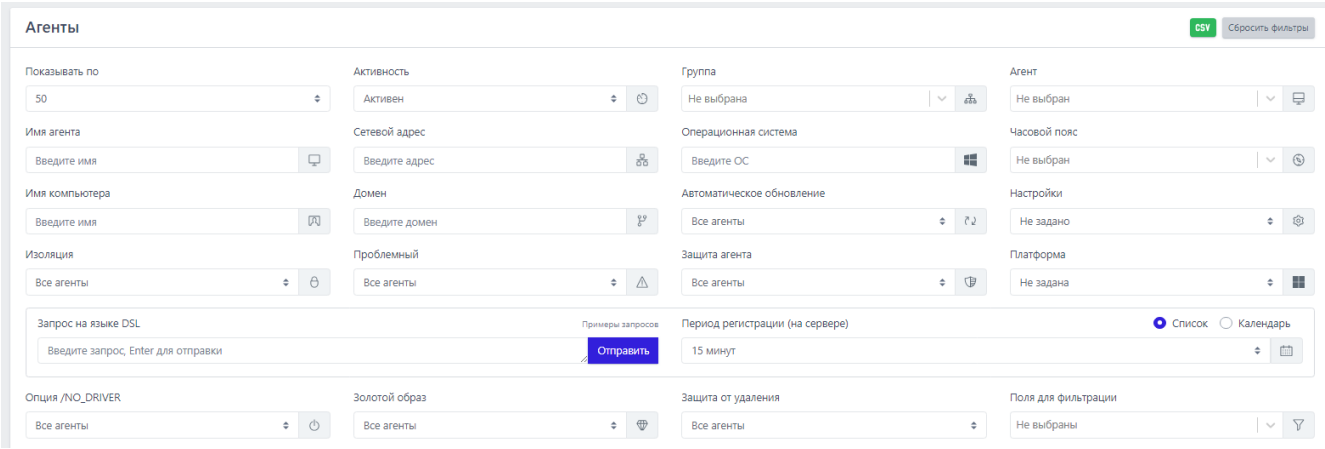


Рисунок 125 – Поля фильтрации в области «Агенты»

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 хэшем 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** (рис. 126).

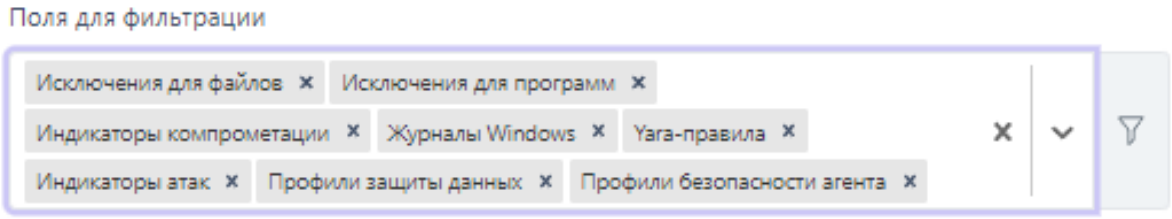


Рисунок 126 – Дополнительные поля фильтрации в области «Агенты»

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 – 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) Сетевые адреса;

4) Домен/Имя компьютера;

5) Операционная система;

6) Часовой пояс;

7) Состояние;

8) Конфигурация.

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.

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).

Конфигурация – в поле отображается информация о наборах, прикрепленных к агенту.

Каждая строка таблицы агентов содержит дополнительную информацию (рис. 127). Для просмотра этой информации необходимо нажать кнопку раскрытия › в поле с кнопкой выбора элемента таблицы **Агенты.**

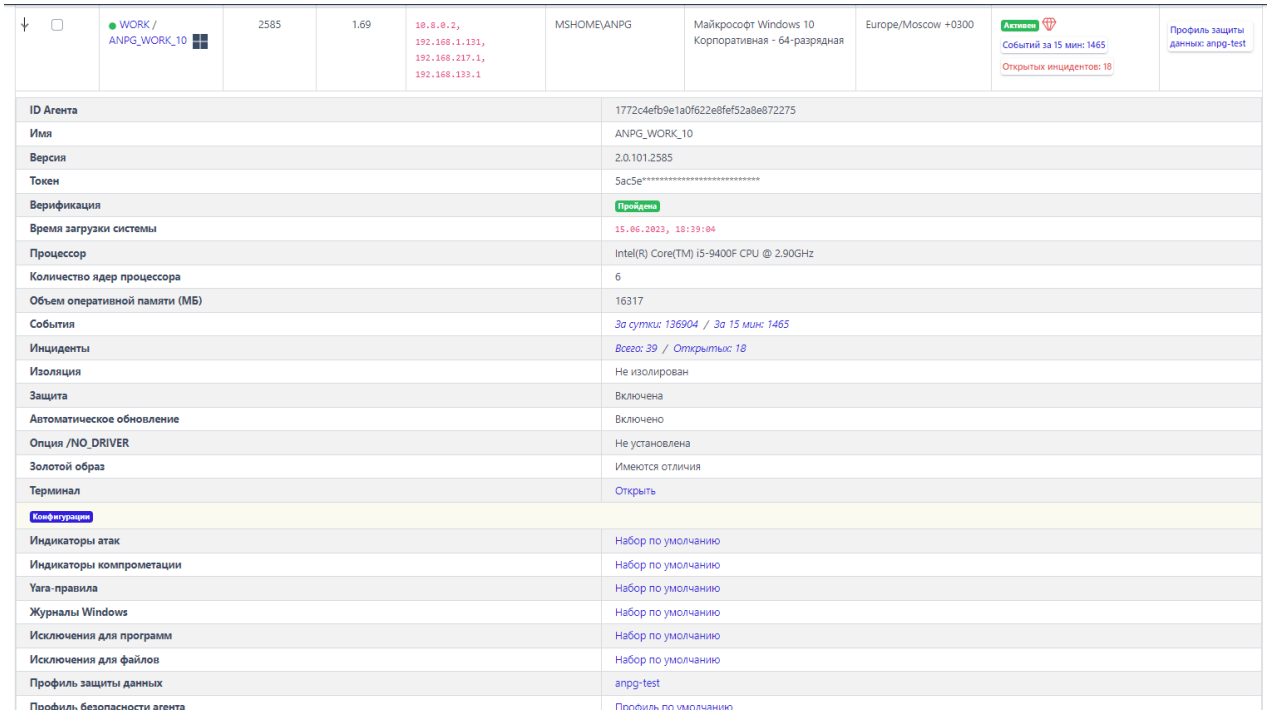


Рисунок 127 – Дополнительная информация об агенте

Дополнительная информация об агенте представлена в табличном виде и содержит поля:

1) ID Агента;

2) Имя;

3) Версия;

4) Токен;

5) Верификация;

6) Время загрузки системы;

7) Процессор;

8) Количество ядер процессора;

9) Объем оперативной памяти (МБ);

10) События;

11) Инциденты;

12) Изоляция;

13) Защита;

14) Автоматическое обновление;

15) Опция /NO_Driver;

16) Золотой образ;

17) Консоль управления.

Часть полей вынесено в отдельную область **Конфигурации**, в которой показаны привязанные к агенту конфигурационные наборы:

1) Индикаторы атак.

2) Индикаторы компрометации;

3) Yara-правила;

4) Журналы Windows;

5) Исключения для программ;

6) Исключения для файлов;

7) Профиль защиты данных;

8) Профиль безопасности агента.

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 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).

Консоль управления – 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**.

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.

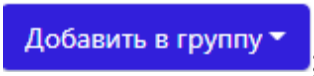
Операции с агентами

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 из группы;

15) Удалить выбранные.

Добавить в группу – функция позволяет добавлять агентов в выбранную группу. Для добавления необходимо отметить флажком одного или нескольких агентов, далее нажать кнопку Добавить в группу, после чего выбрать операцию из списка (рис. 128).

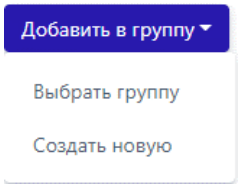


Рисунок 128 – Выбор операции с агентом

Если следует добавить выбранного/выбранных агента/агентов в уже созданную группу, то следует кликнуть по кнопке **Выбрать группу**, после чего в открывшемся окне (рис. 129) выбрать необходимую группу (рис. 130) и нажать кнопку Добавить.

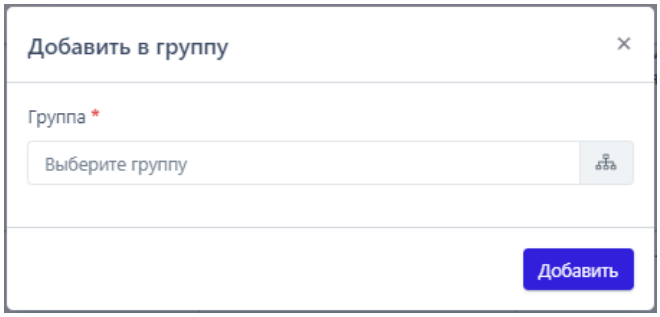


Рисунок 129 – Добавление агента в ранее созданную группу

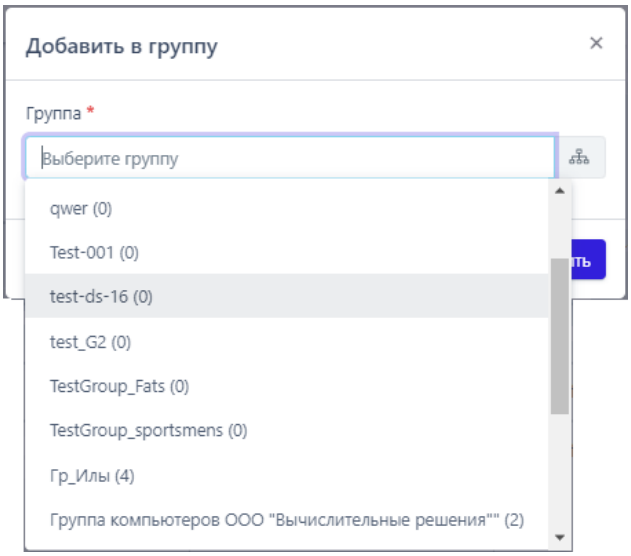


Рисунок 130 – Выбор группы из списка

Далее в открывшемся окне **Подтверждение действия** (рис. 131) нажать кнопку Выполнить. Для отмены добавления выбранных агентов в группу необходимо нажать кнопку Отмена или кнопку закрытия окна ×.

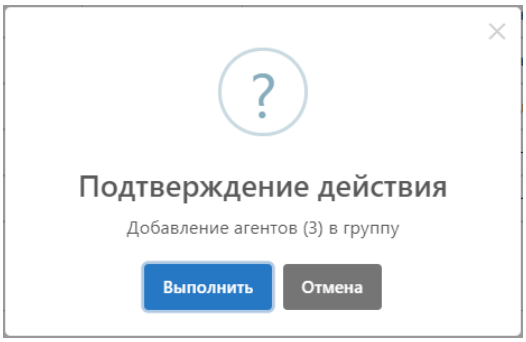


Рисунок 131 – Подтверждение действия добавления агентов в группу

После выполнения операции добавления выбранных агентов в нижней части страницы появится всплывающее окно с сообщением **Агенты добавлены в группу** (рис. 132).

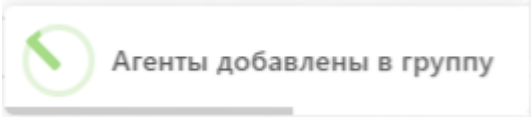


Рисунок 132 – Сообщение о добавлении агентов в группу

Если необходимо добавить выбранных агентов во вновь создаваемую группу, то следует кликнуть по кнопке **Создать новую** (см. рис. 128), после чего в открывшемся окне (рис. 133) ввести название в строке **Название группы** и нажать кнопку Создать.

Рисунок 133 – Добавление агента во вновь создаваемую группу

После выполнения операции добавления выбранных агентов в нижней части страницы появится всплывающее окно с сообщением **Агенты добавлены в группу** (см. рис. 132). Для отмены операции следует нажать кнопку ✕ в окне **Создать группу**.

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 (рис. 134).

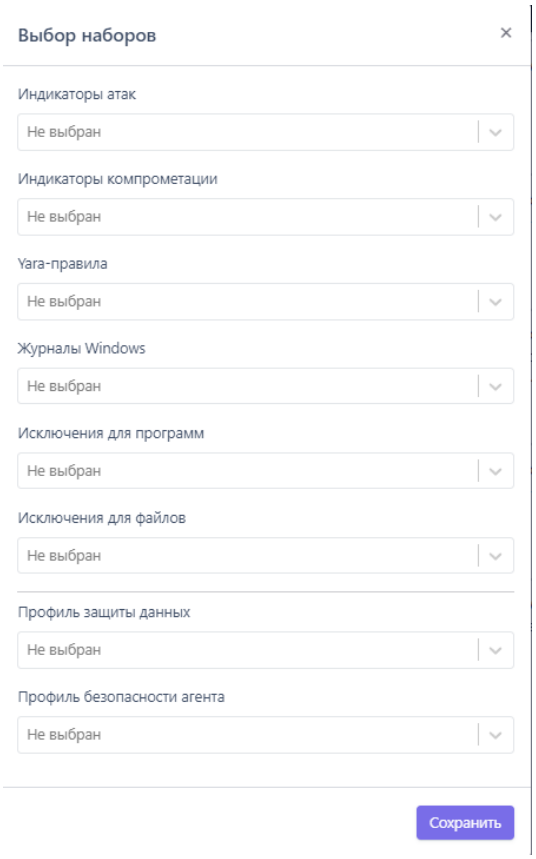


Рисунок 134 – Окно выбора наборов

После завершения выбора необходимо нажать кнопку **Сохранить**, после чего в нижней части страницы появится окно с сообщением **Конфигурация применена** (рис. 135).

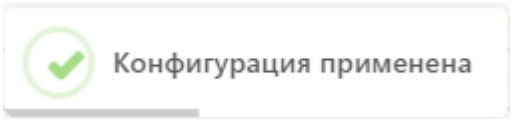


Рисунок 135 – Сообщение о применении конфигурации

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 (см. рисунок 136). 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  .

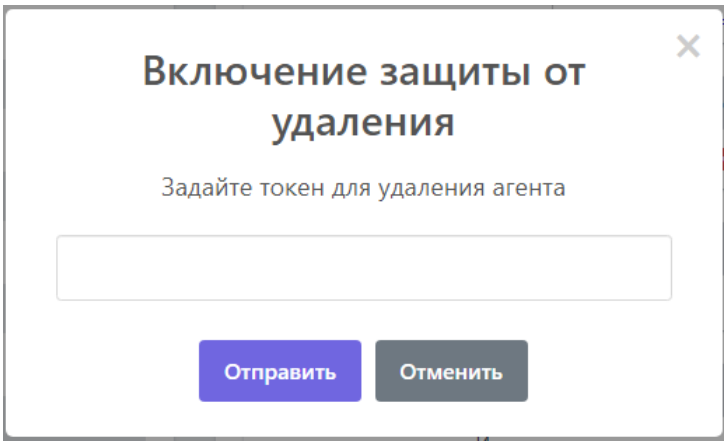


Рисунок 136 – Ввод пароля при включении функции «Защита от удаления»

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 137.

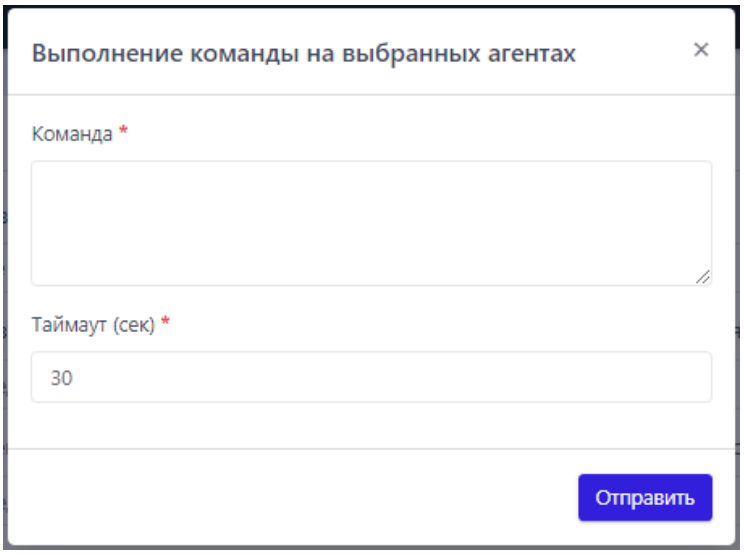


Рисунок 137 – Окно ввода команд

После ввода команды необходимо нажать кнопку **Отправить**. Список команд аналогичен командам, описанным в разделе 6.6.5.

Исключить из группы – функция позволяет исключать выбранных агентов из группы. Для выполнения операции следует выбрать агентов, принадлежащих какой-либо группе, отметив их флажком в столбце выбора, после чего нажать кнопку Исключить из группы. В открывшемся окне **Подтверждение действия** (рис. 138) необходимо нажать кнопку Выполнить. Для отмены операции следует нажать кнопку Отмена или кнопку закрытия окна ×.

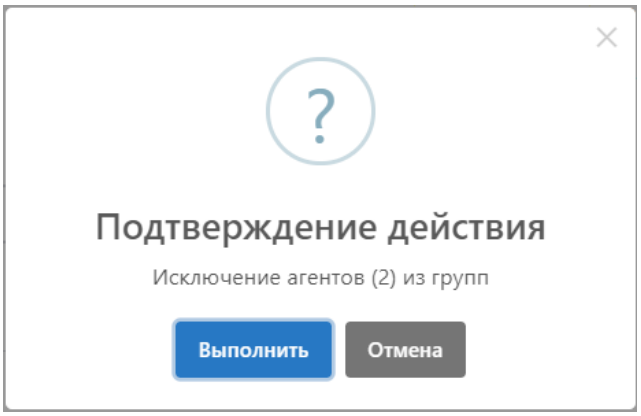


Рисунок 138 – Исключение агента из группы

После подтверждения операции в нижней части страницы появится сообщение **Агенты исключены из группы** (рис. 139).

Рисунок 139 – Сообщение об исключении агентов из группы

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, после чего нажать кнопку Удалить выбранные. В открывшемся окне **Подтверждение действия** (рис. 140) необходимо нажать кнопку Выполнить. После завершения операции агенты будут удалены.

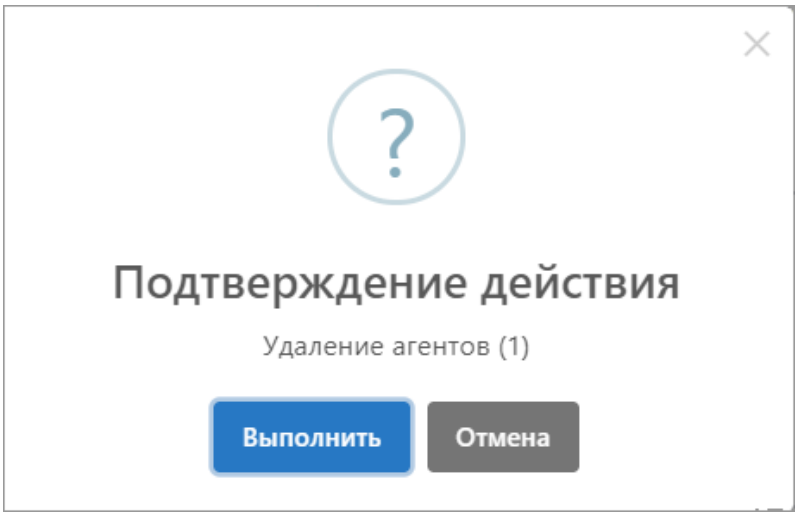


Рисунок 140 – Подтверждение удаления агента

Для отмены операции следует нажать кнопку Отмена или кнопку закрытия окна ×.

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;

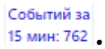
5) Версия дистрибутива агента;

6) Сетевые адреса.

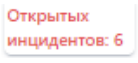
В файле будет присутствовать информация о тех агентах, которые отсортированы на странице **Агенты** в зависимости от выставленных фильтров, либо будет информация обо всех агентах, если фильтры отсутствуют.

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 в списке агентов кликнуть по имени агента, после чего появится окно, представленное на рисунке 141.

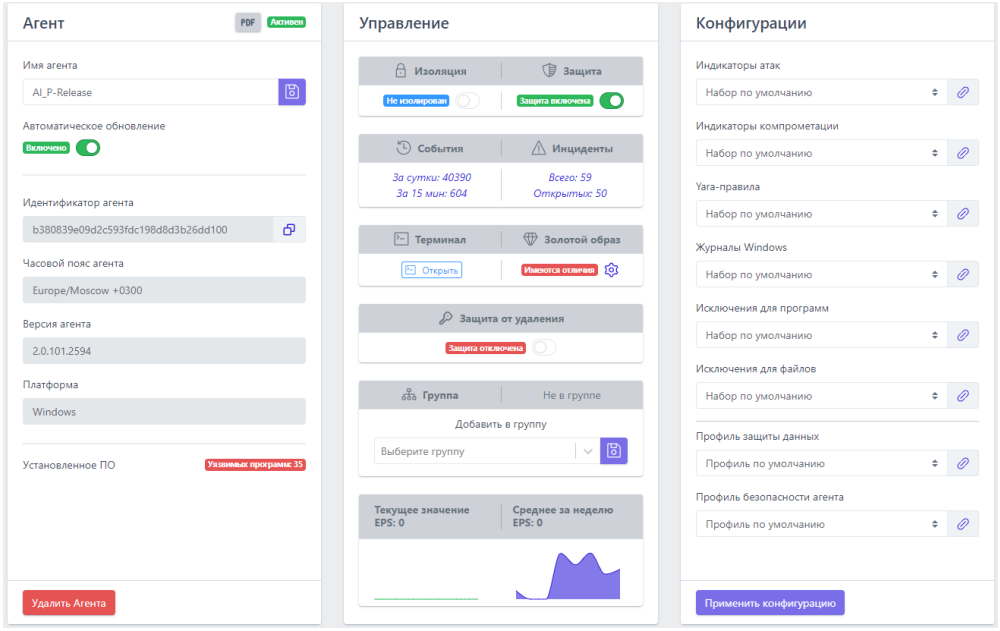


Рисунок 141 – Страница «Агент»

Общая информация

Страница разделена на пять областей:

1) Агент;

2) Управление;

3) Конфигурации;

4) Информация о системе;

5) Графики.

Агент – в области отображается информация об основных параметрах агента, некоторые из них администратор может изменять и сохранять сделанные изменения (рис. 142).

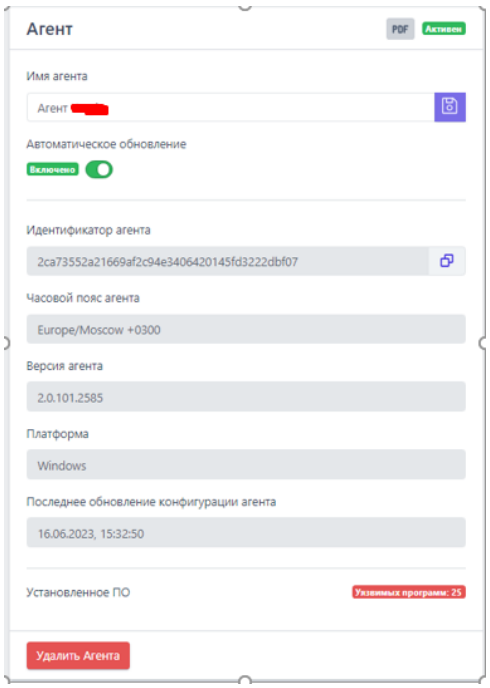


Рисунок 142 – Область «Агент»

Управление – в области администратор может управлять различными состояниями агента, а также открыть терминал для управления агентом (рис. 143). Агент управляется через консоль с помощью функционала командной строки или оболочки PowerShell.

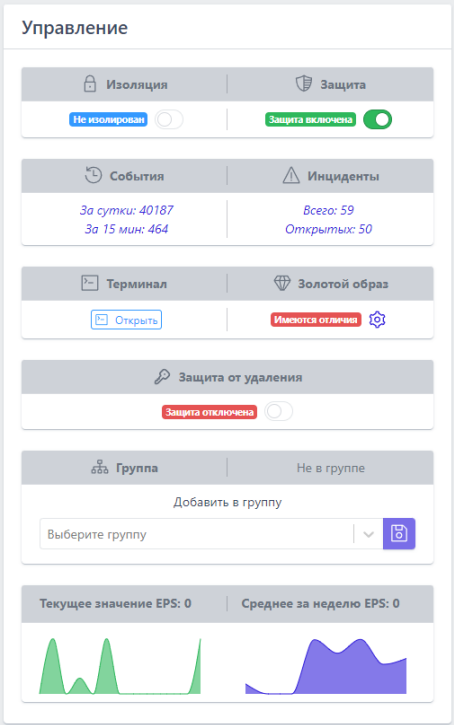


Рисунок 143 – Область «Управление»

Важно

Для агентов, у которых установлена опция с выключением драйвера, будет отсутствовать возможность переводить агента в изоляцию и включать защиту.

Конфигурации – в области отображаются все наборы конфигураций, которые прикреплены к агенту. Каждый набор можно изменить, после чего применить измененную конфигурацию (рис. 144). Прикрепленный к агенту несохраненный набор отмечается значком справа от названия набора, сохраненный набор отмечается значком .

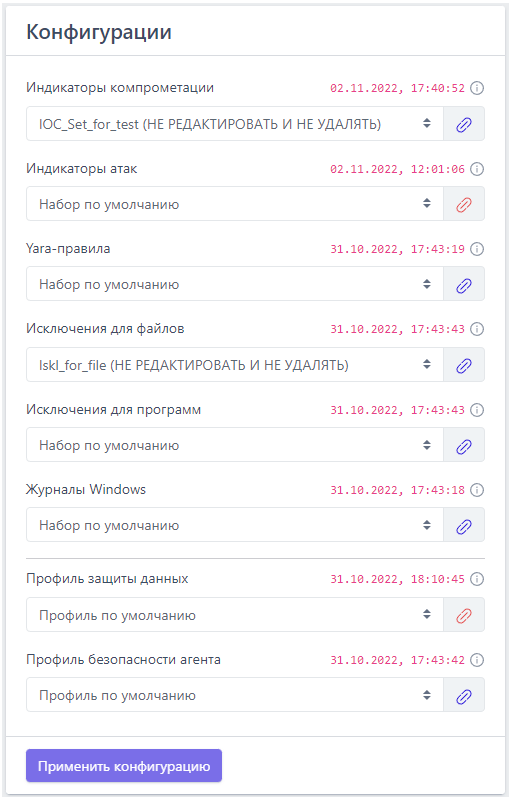


Рисунок 144 – Область «Конфигурации»

Информация о системе – в области отображается информация об операционной системе и основных характеристиках компьютера, на котором установлен выбранный агент (рис. 145).

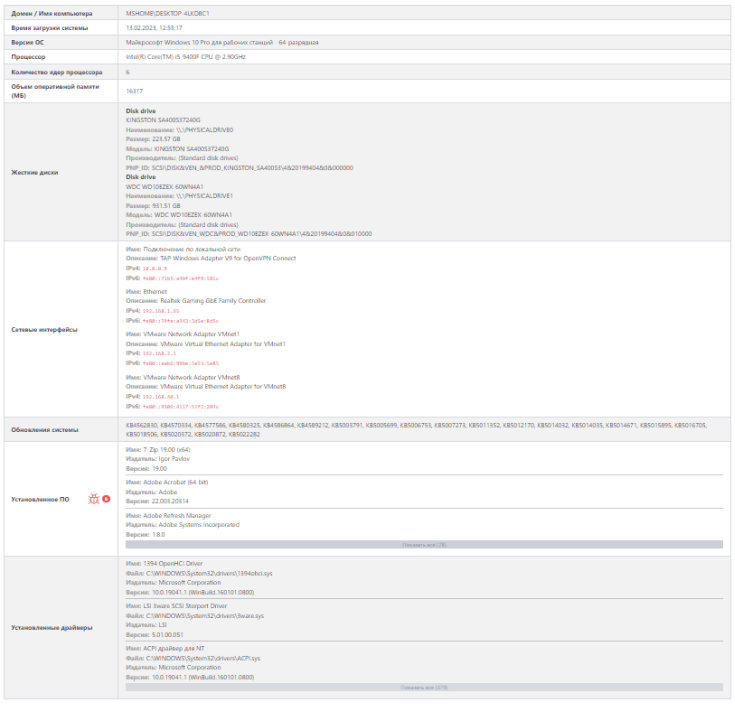


Рисунок 145 – Область «Информация о системе»

Графики – в области отображается информация о работе компьютера, на котором установлен агент, в графическом виде (рис. 146).

Рисунок 146 – Область «Графики»

Область «Агент»

В области **Агент** (см. рис. 142) 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) Сохранить изменения имени агента;

9) Просмотреть количество программ с уязвимостями;

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

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. 147).

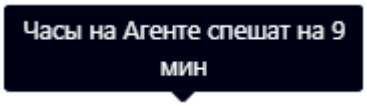


Рисунок 147 – Предупреждение о несоответствии настройкам часового пояса

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, представленное на рисунке 148.

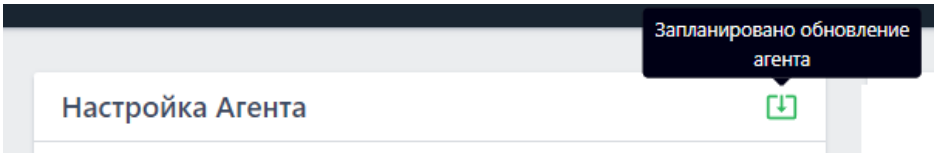


Рисунок 148 – Запланировано обновление агента

Данное сообщение 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** ( ). Название агента будет изменено, а в нижней части страницы появится сообщение (рис. 149).

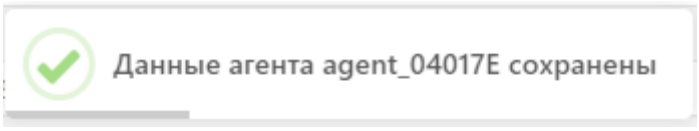


Рисунок 149 – Сообщение об изменении данных агента

Для всех агентов, верифицируемых в программе, кнопка **Автоматическое обновление** ( ) включена по умолчанию. Чтобы снять автоматическое обновление необходимо перевести кнопку в состояние **Отключено**.

Для удаления агента необходимо нажать кнопку Удалить Агента. Далее в открывшемся окне **Подтверждение действия** (рис. 150) следует нажать кнопку Выполнить, после чего в нижней части страницы появится сообщение об удалении агента. Для отмены операции следует нажать кнопку Отмена или кнопку закрытия окна .

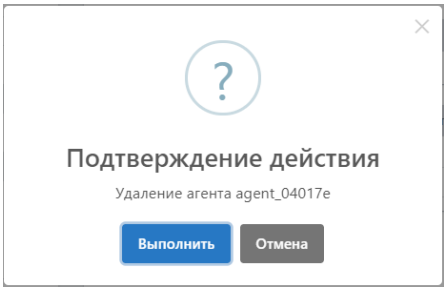


Рисунок 150 – Подтверждение удаления агента

Область «Управление»

В области **Управление** (см. рис. 143) 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 (см. рис. 151).

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».

Для отмены изоляции следует нажать кнопку Отмена или кнопку закрытия окна ×.

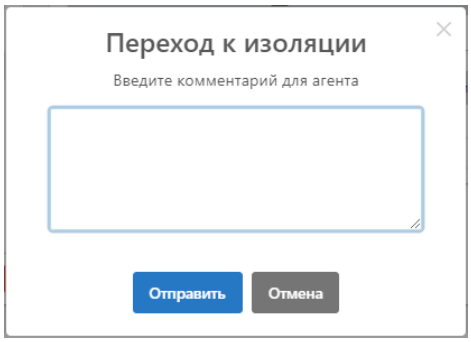


Рисунок 151 – Ввод комментария перед изоляцией агента

После ввода комментария в окне и нажатия кнопки Отправить режим Не изолирован будет изменен на режим Переход к изоляции. Изоляция агента происходит в течение 10 секунд, после чего статус агента в области **Управление** поменяется на Изолирован. 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** (рис. 152) следует нажать кнопку Выполнить, после чего в нижней части страницы появится сообщение об отправке команды на отмену изоляции (рис. 153). Для отмены операции необходимо нажать кнопку Отмена или кнопку закрытия окна ×.

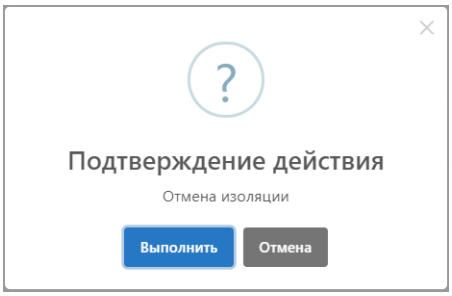


Рисунок 152 – Подтверждение отмены изоляции агента

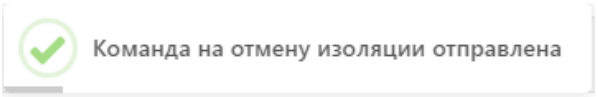


Рисунок 153 – Сообщение об отмене изоляции

Отмена изоляции агента происходит в течение 10 секунд. За это время статус агента в области **Управление** поменяется на Отмена изоляции , 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. 154).

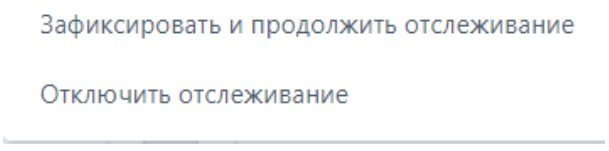


Рисунок 154 – Действия с золотым образом

В поле **Информация о системе** в списке **Установленное ПО** программы из списка золотого образа, удаленные на агенте, будут помечены красным цветом и зачеркиванием, а программы, вновь установленные но не зафиксированные агентом в золотом образе будут помечены зеленым цветом (рис. 155).

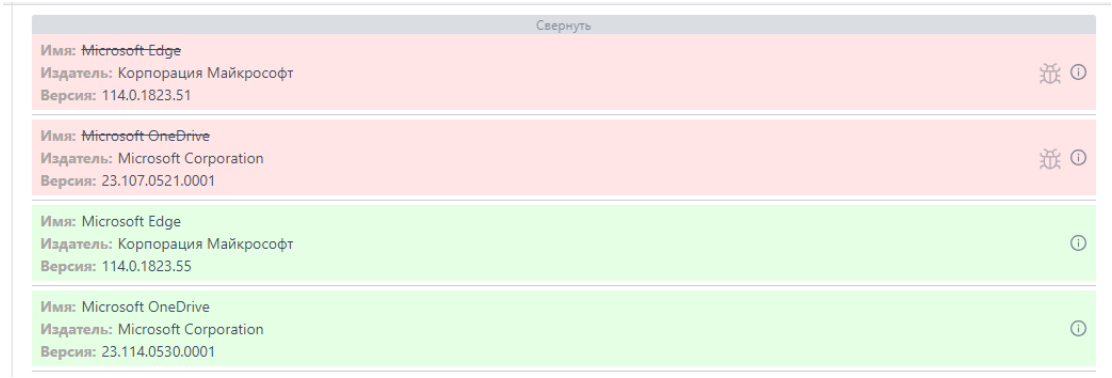


Рисунок 155 – Отображение программ в списке установленного ПО, не соответствующих зафиксированному состоянию (Золотому образу)

Для фиксации списка установленных программ требуется выбрать в действие **Зафиксировать и включить отслеживание**, после чего появится окно подтверждения действия фиксации золотого образа (рис. 156).

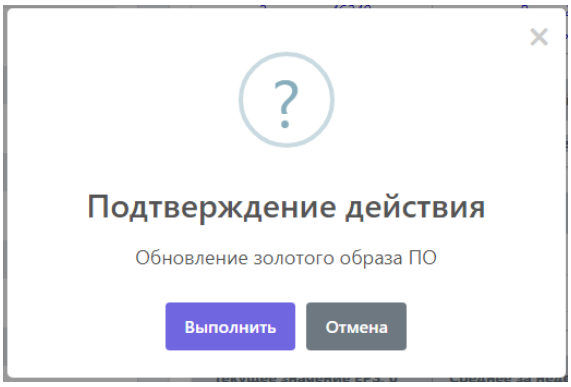


Рисунок 156 – Подтверждения фиксации золотого образа

Для фиксации требуется в окне, представленном выше, 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 6.6.5.

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 157.

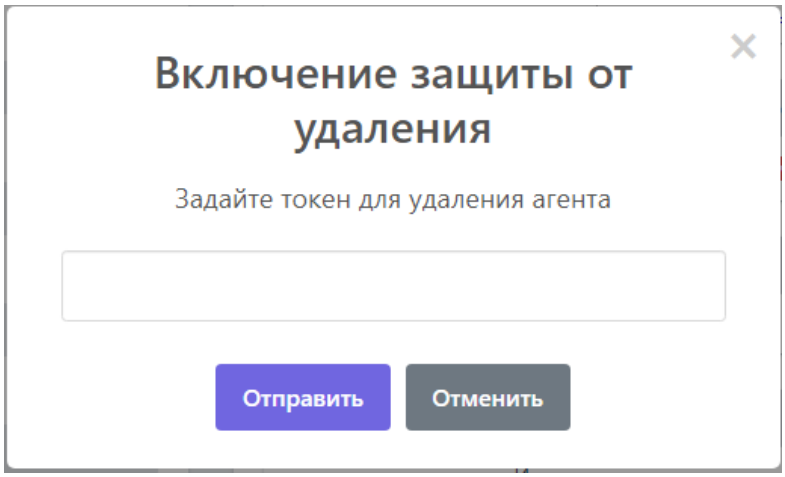


Рисунок 157 – Окно ввода пароля при включении функции защиты агента от удаления

После введения 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 (рис. 158).

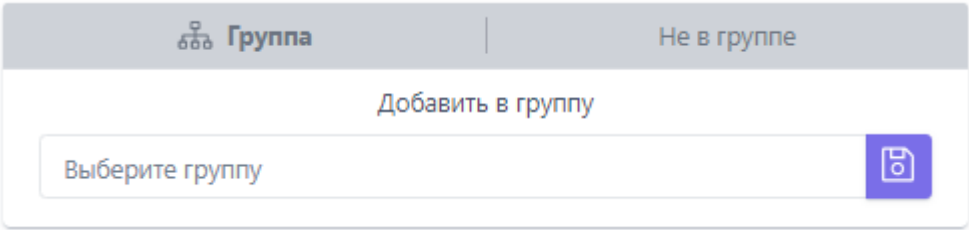


Рисунок 158 – Агент не в группе

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** (рис. 159) следует нажать кнопку 

, после чего в нижней части страницы появится сообщение о добавлении агента в группу (рис. 160). Для отмены операции необходимо нажать кнопку 

или кнопку закрытия окна .

Рисунок 159 – Подтверждение добавления агента в группу

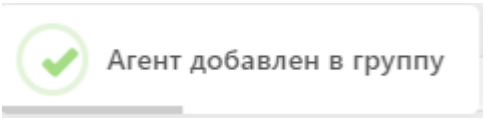


Рисунок 160 – Сообщение о добавлении агента в группу

После добавления агента в группу в поле **Группа** будет указано название группы, в которую теперь входит агент (рис. 161).

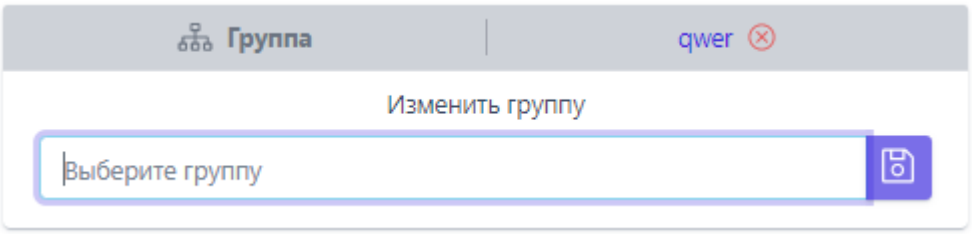


Рисунок 161 – Агент в группе

Для удаления агента из группы следует нажать кнопку **Исключить из группы** . Далее в открывшемся окне **Подтверждение действия** (рис. 162) следует нажать кнопку Выполнить, после чего в нижней части страницы появится сообщение об исключении агента из группы (рис. 163). Для отмены операции необходимо нажать кнопку Отмена или кнопку закрытия окна .

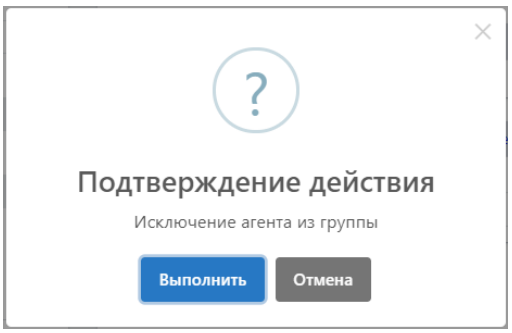


Рисунок 162 – Исключение агента из группы

Рисунок 163 – Сообщение об исключении агента из группы

Область «Конфигурации»

В области **Конфигурации** (см. рис. 144) пользователь 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 определенный набор индикаторов компрометации;

– применять к выбранному агенту определенный набор журналов Windows;

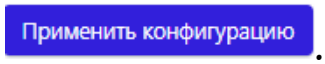
– применять к выбранному агенту определенный набор файловых сигнатур;

– применять к выбранному агенту определенный набор индикаторов атак;

– применять к выбранному агенту определенный профиль защиты данных;

– применять к выбранному агенту определенный профиль безопасности.

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, соответствующем выбранному набору, нажать ЛКМ на строке с названием текущего набора и из выпадающего списка выбрать новый набор, после чего нажать кнопку 

. После применения конфигурации в нижней части страницы появится сообщение о сохранении конфигурации агента (рис. 164).

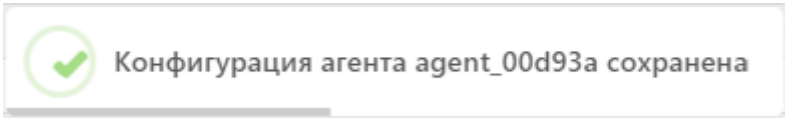


Рисунок 164 – Сообщение о сохранении измененной конфигурации агента

Для изменения конфигурационных наборов, прикрепленных к агенту, необходимо нажать кнопку **Перейти к набору** справа от названия соответствующего набора.

Область «Информация о системе»

В области **Информация о системе** отображается следующая информация (см. рис. 145):

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;

9) Установленное ПО;

10) Установленные драйверы.

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.

Установленное ПО – в поле отображается информация о программах, установленных на машине с агентом. Поле содержит значок для запуска сканера уязвимостей ( ) и информацию о найденных уязвимостях.

Установленные драйверы – в поле отображается информация об установленных на машине с агентом драйверах.

Область «Графики»

В графическом виде показана информация о работе компьютера, на котором установлен агент (см. рис. 146). 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 (рис. 165).

Рисунок 165 – График загрузки центрального процессора

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 (рис. 166).

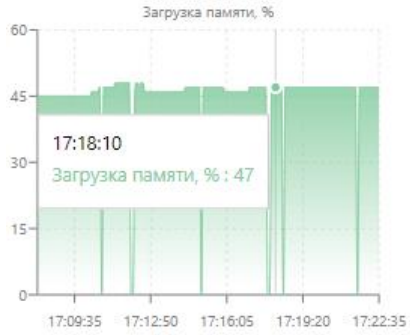


Рисунок 166 – График загрузки оперативной памяти

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 в всплывающем окне будет показано точное количество процессов в конкретный момент времени (см. рис. 167).

Рисунок 167 – График количества активных процессов

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 (рис. 168).

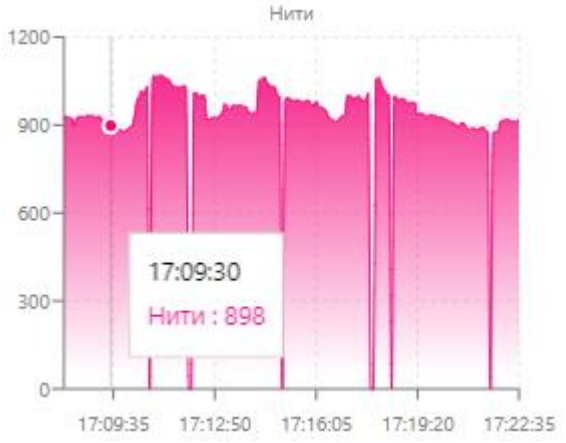


Рисунок 168 – График количества активных нитей

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 (рис. 169).

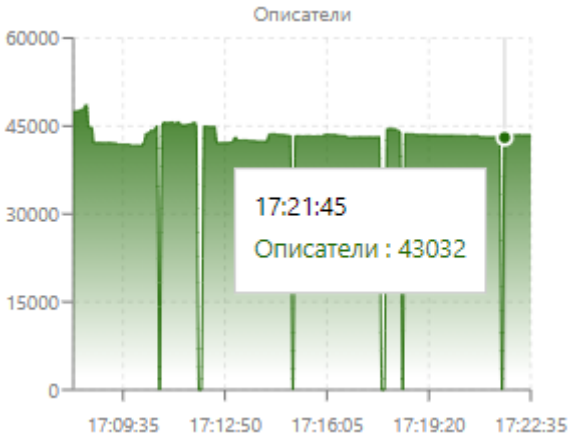


Рисунок 169 – График количества активных описателей

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 в всплывающем окне будет показана точная скорость загрузки диска на чтение в конкретный момент времени (рис. 170).

Рисунок 170 – График загрузки диска во время чтения с диска

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 (рис. 171).

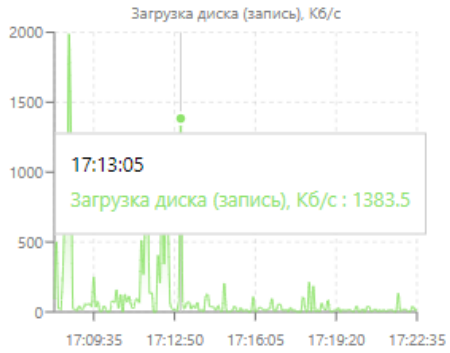


Рисунок 171 – График загрузки диска во время записи на диск

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 в всплывающем окне будет показана точная скорость сетевой передачи файлов в конкретный момент времени (рис. 172).

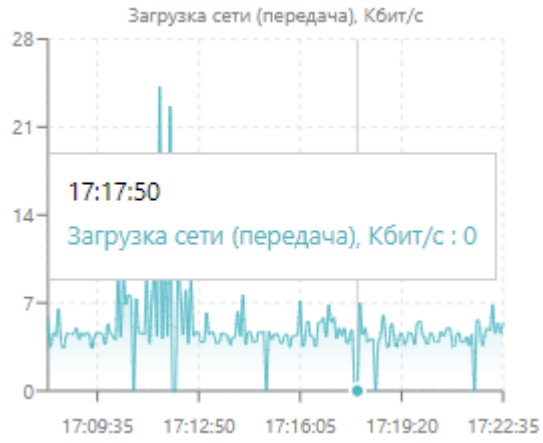


Рисунок 172 – График загрузки сети во время передачи с машины агента

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 в всплывающем

окне будет показана точная скорость сетевой передачи файлов в конкретный момент времени (рис. 173).

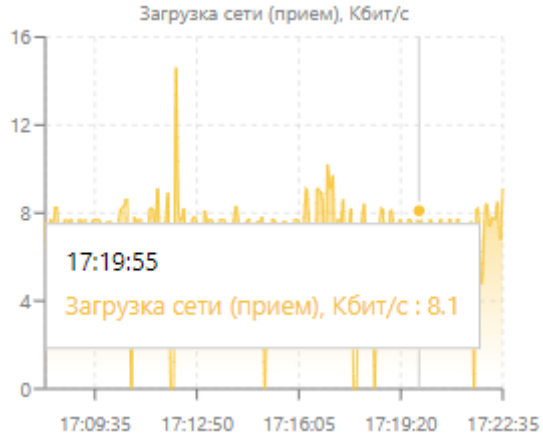


Рисунок 173 – График загрузки сети во время приёма передачи на машину агента

Сканер уязвимостей на странице «Агент»

Для запуска сканера уязвимостей необходимо кликнуть значок в поле **Установленное ПО** на странице **Агент**. Открывается окно **Данные сканера уязвимостей** с кнопкой **Запустить сканирование**, ее нажатие запускает сканирование системы с установленным агентом на наличие уязвимых программ. После завершения сканирования значок поменяет цвет на красный (если уязвимости будут найдены) или зеленый (если сканер не обнаружит уязвимости). При наличии уязвимостей в списке установленного ПО будут показаны программы с выявленными уязвимостями. Такие программы обозначаются значком и содержат число, обозначающее количество найденных в программе уязвимостей. Кликнув на значок, можно открыть окно, содержащее полный список найденных уязвимостей и просмотреть их (рис. 174).

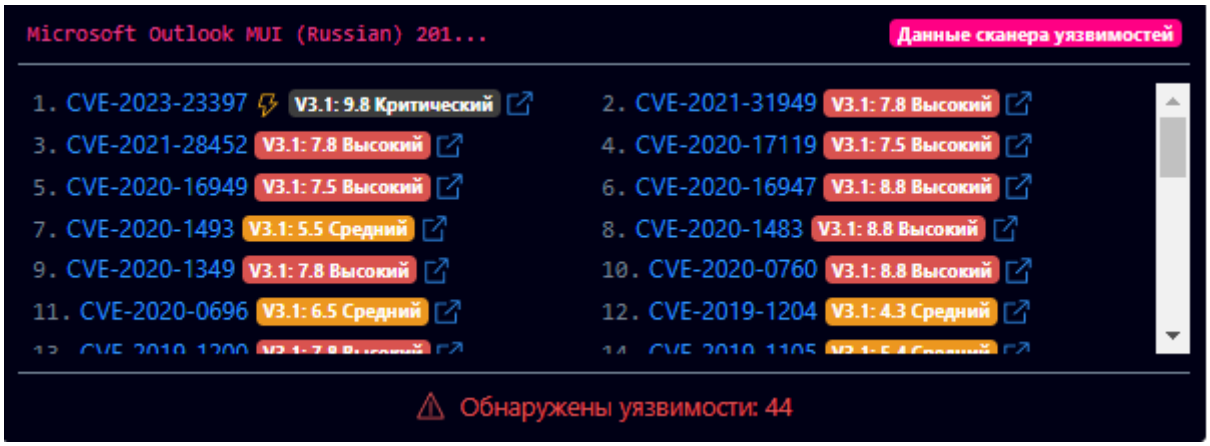


Рисунок 174 – Уязвимости ПО

Чтобы просмотреть полную информацию об уязвимости, необходимо нажать на её кодовое обозначение, после чего откроется страница NVD (National Vulnerability Database) Национального института стандартов и технологий США (NIST). Кроме CVE-представления (Common Vulnerability and Exposures) уязвимости для некоторых из уязвимостей в строке отображается CWE-представление (Common Weakness Enumeration), на которое также можно перейти, нажав ссылку с CWE-номером.

Чтобы просмотреть информацию об уязвимости на сайте Банка данных угроз безопасности ФСТЭК, необходимо нажать кнопку .

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 команды:

– Remove-ItemProperty HKLM:\SYSTEM\CurrentControlSet\services\VrpSvc -Name no_driver;

– Restart-Service vrpsvc;

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

Страница «Группы агентов»

Общий вид страницы **Группы агентов** представлен на рисунке 175.

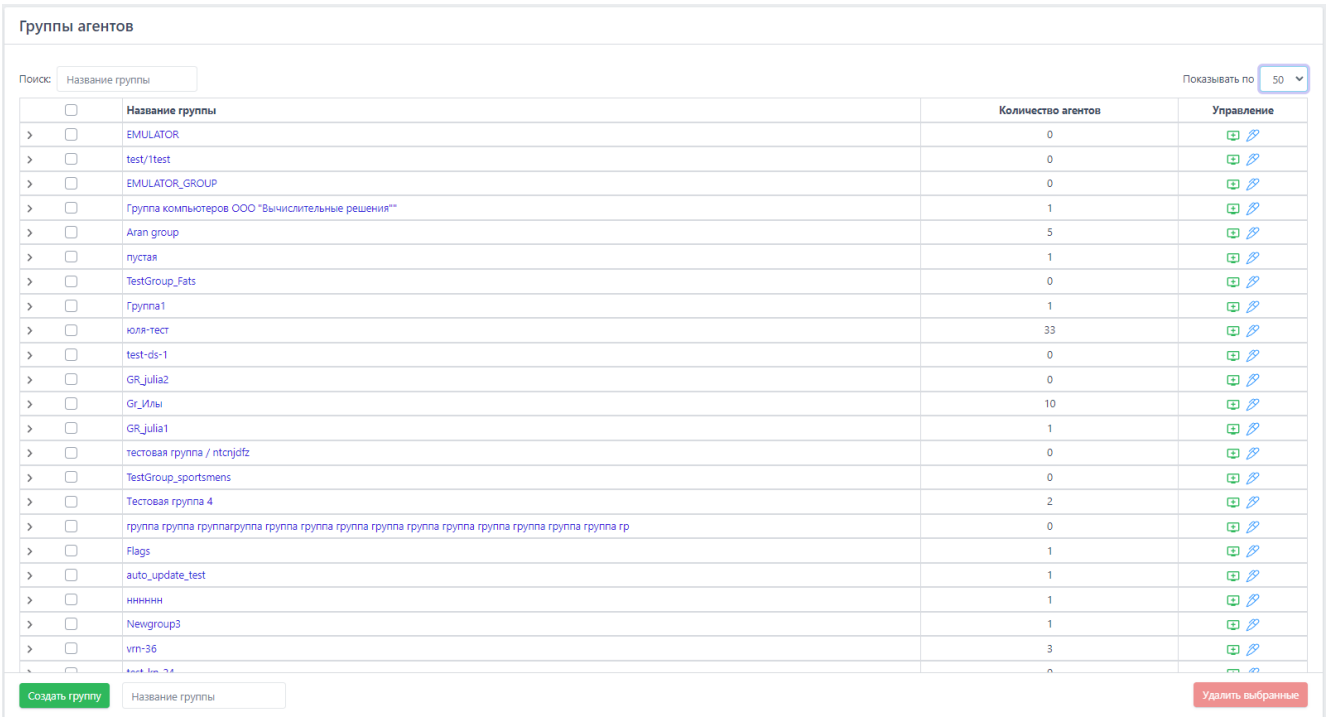


Рисунок 175 – Страница «Группы агентов»

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 для добавления агентов в выбранную группу ( ) и кнопка изменения названия 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.

Для удаления агента из группы в раскрытой строке необходимо нажать на кнопку **Исключить из группы** . В открывшемся окне **Подтверждение действия** следует нажать кнопку Выполнить, после чего в нижней части страницы появится всплывающее сообщение (рис. 176).

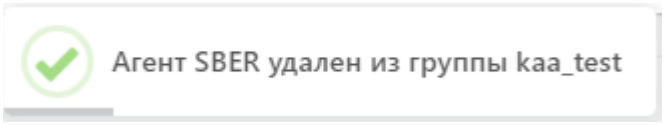


Рисунок 176 – Сообщение об удалении агента из группы

После завершения операции выбранный агент будет удален из группы. Для отмены операции необходимо нажать кнопку Отмена или кнопку закрытия окна .

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** (рис. 177).

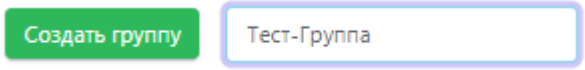


Рисунок 177 – Создание группы агентов (ввод названия)

После этого в нижней части страницы появится сообщение о добавлении новой группы (рис. 178), а в таблице со списком групп появится строка с информацией о новой группе.

Рисунок 178 – Сообщение о добавлении группы агентов

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** (рис. 180) следует нажать кнопку Выполнить, после чего в нижней части страницы появится сообщение об удалении группы или групп агентов (рис. 179). Для отмены операции необходимо нажать кнопку Отмена или кнопку закрытия окна ×.

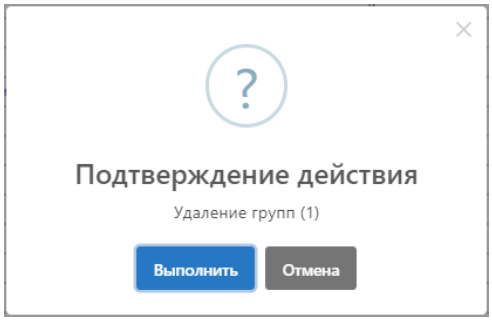


Рисунок 179 – Подтверждение удаления группы агентов

Рисунок 180 – Сообщение об удалении группы агентов

После удаления выбранные группы агентов не будут отображаться в списке таблицы.

Для добавления агента в группу необходимо нажать на кнопку в строке с названием группы, после чего выбрать агента в открывшемся окне и нажать кнопку **Добавить**.

Имя группы является активной ссылкой, при нажатии по которой осуществляется переход на страницу **Группа**.

Страница «Группа»

На странице **Группа** пользователь может изменить название группы, сохранив изменения с помощью кнопки . После сохранения изменений в нижней части страницы появится сообщение об изменении данных группы. В области **Группа** возможно удалить выбранную группу агентов с помощью кнопки . Операция удаления требует подтверждения действия.

Для добавления агентов в группу в области **Состав Группы** нужно нажать ЛКМ на строку **Выберите Агента**, после чего выбрать необходимого агента из выпадающего списка и нажать кнопку Добавить агента. Далее в открывшемся окне **Подтверждение действия** следует нажать кнопку Выполнить, после чего в нижней части страницы появится сообщение о добавлении выбранного агента в группу. Для отмены операции необходимо нажать кнопку Отмена или кнопку закрытия окна . После добавления агента или агентов в группу они отобразятся в области **Состав Группы** (рис. 181).

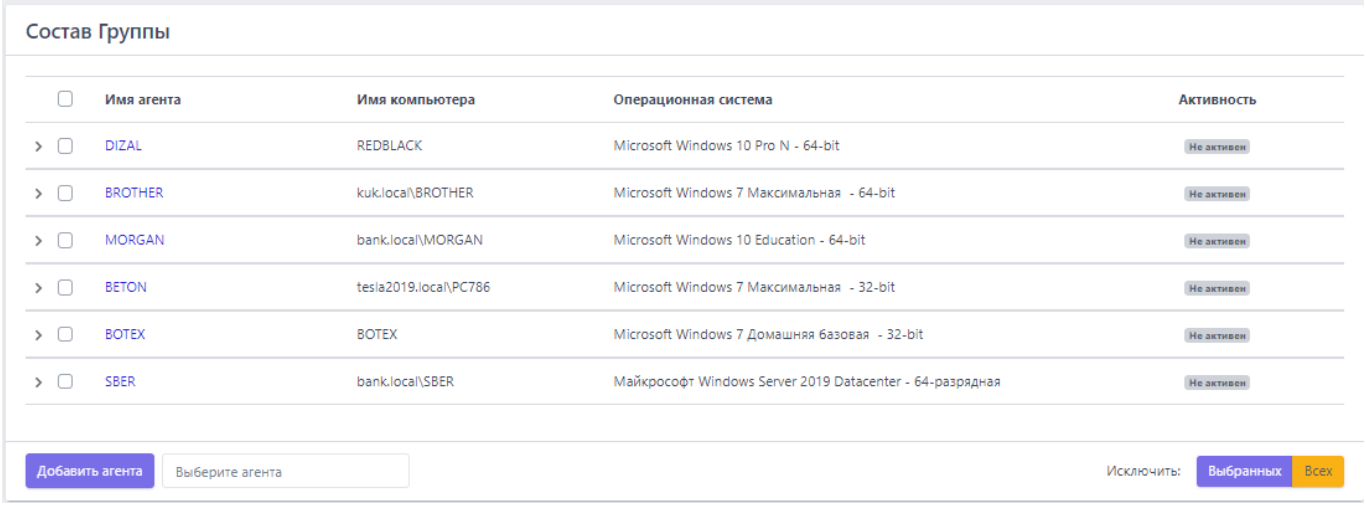


Рисунок 181 – Область «Состав Группы»

Информация об агентах в области **Состав Группы** представлена в табличном виде. Таблица содержит следующие поля:

1) Поле выбора (отмечено кнопкой ☐);

2) **Имя агента;**

3) **Имя компьютера;**

4) **Операционная система;**

5) **Активность.**

Для выбора в таблице одного или нескольких агентов необходимо отметить флажком кнопки выбора для соответствующих агентов (рис. 182). Для отмены выбора следует повторно нажать на кнопку ☑.

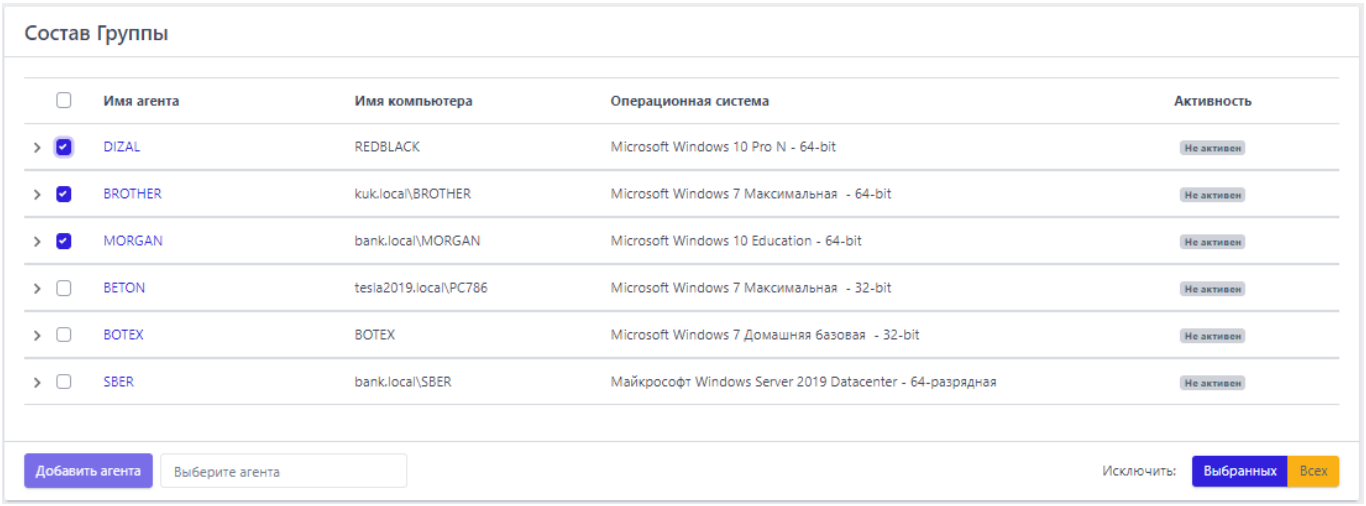


Рисунок 182 – Выбор агента в таблице «Состав Группы»

Для выбора в таблице всех агентов, показанных на одной странице, необходимо отметить флажком верхнюю кнопку выбора (рис. 183).

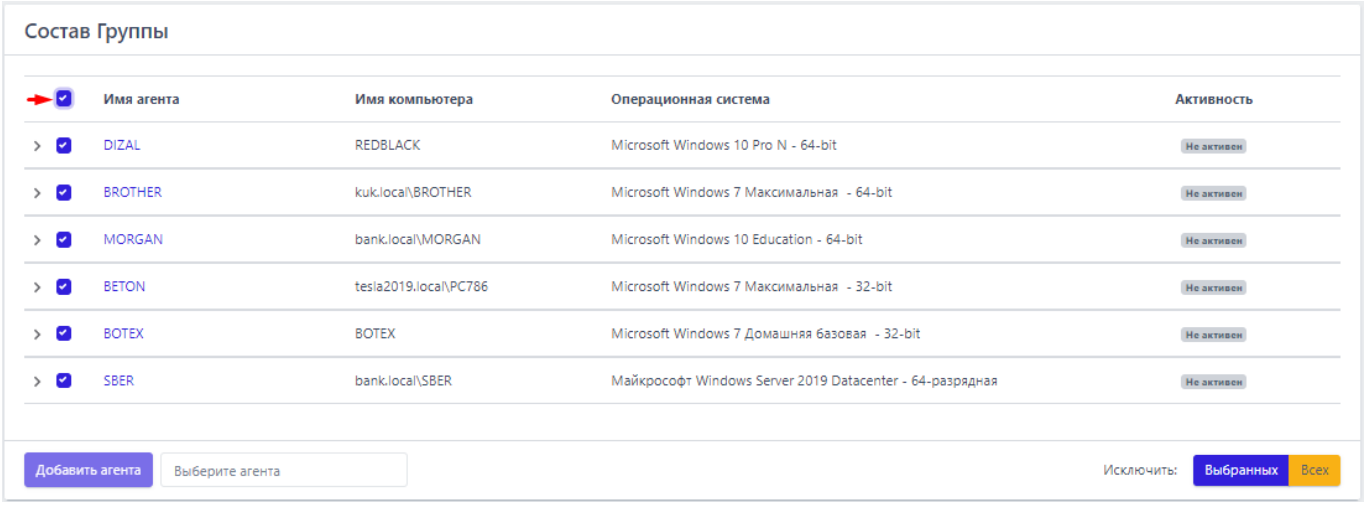


Рисунок 183 – Выбор всех агентов в таблице «Состав Группы»

Имя агента – в поле отображается имя агента, присвоенное ему администратором во время регистрации в программе.

Имя компьютера – в поле отображается имя компьютера, на котором установлен агент.

Операционная система – в поле отображается название ОС, установленной на компьютере, на котором работает агент.

Активность – в поле показывается состояние активности агента (активен/не активен).

При нажатии ЛКМ на значок › рядом с кнопкой выбора в таблице с агентами снизу строки открывается таблица с дополнительной информацией по агенту (см. рис. 127).

В нижней части области **Состав Группы** находятся кнопки операций с агентами, входящими в группу:

1) Добавить агента;

2) Исключить: Выбранных;

3) Исключить: Всех.

Для добавления агента в группу необходимо выбрать его из выпадающего списка в строке **Выберите агента,** после чего нажать кнопку **Добавить агента.** В открывшемся окне **Подтверждение действия** следует нажать кнопку Выполнить, после чего в нижней части страницы появится сообщение о добавлении выбранного агента. Для отмены операции следует нажать кнопку Отмена или кнопку закрытия окна ×.

Для исключения выбранного агента или нескольких агентов из группы необходимо отметить флажками соответствующие этим агентам кнопки выбора, после чего нажать кнопку **Исключить:** Выбранных. В открывшемся окне **Подтверждение действия** следует нажать кнопку Выполнить, после чего в нижней части страницы появится сообщение об исключении агента/агентов из группы. Для отмены операции следует нажать кнопку Отмена или кнопку закрытия окна ×

.

Для исключения всех агентов из группы следует нажать кнопку **Исключить:** Всех. В открывшемся окне **Подтверждение действия** необходимо нажать кнопку Выполнить, после чего в нижней части страницы появится сообщение

об исключении агента/агентов из группы. Для отмены операции следует нажать кнопку 

или кнопку закрытия окна  .

6.6.4. 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. 184).

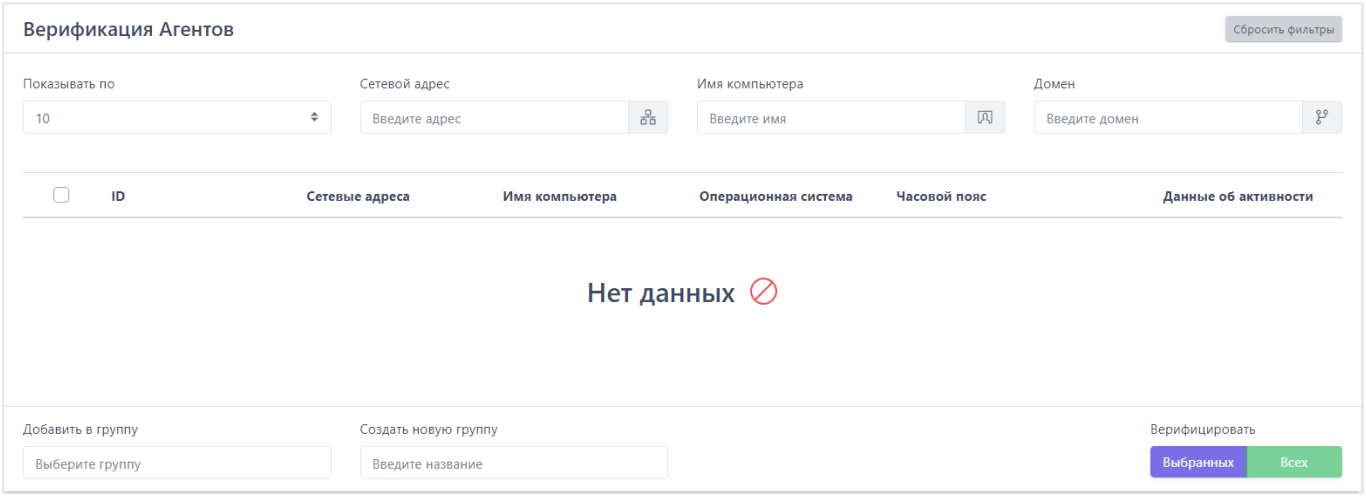


Рисунок 184 – Страница «Верификация» (нет верифицируемых агентов)

На рисунке 184 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. 185).

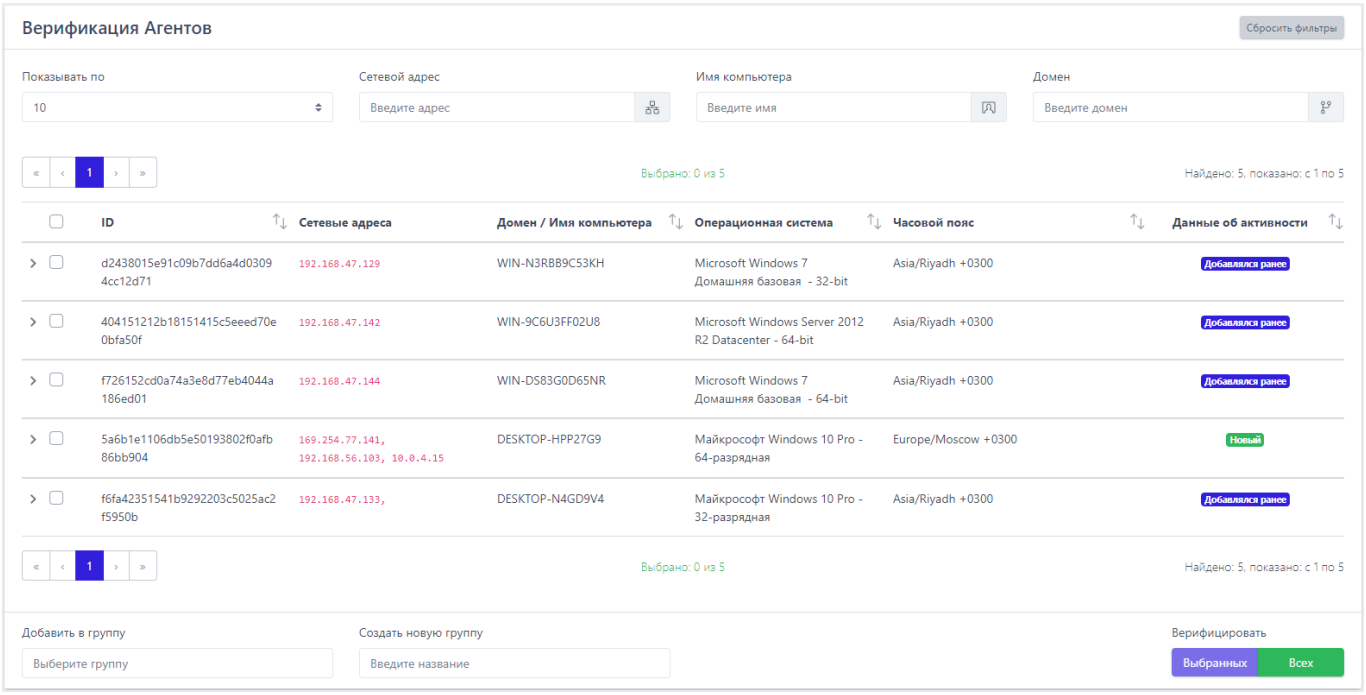


Рисунок 185 – Страница «Верификация» (есть верифицируемые агенты)

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 Сбросить фильтры. При активации кнопки все настройки фильтрации сбрасываются на значения, заданные по умолчанию.

В шапке таблицы представлены следующие поля:

1) Кнопка выбора (отмечена элементом ▢);

2) ID;

3) Сетевые адреса;

4) Домен/Имя компьютера;

5) Операционная система;

6) Часовой пояс;

7) Данные об активности (Новый/Добавлялся ранее).

Рядом с кнопкой выбора агента находится элемент ›, который позволяет открывать дополнительную информацию об агенте, требующем верификацию (рис. 186):

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;

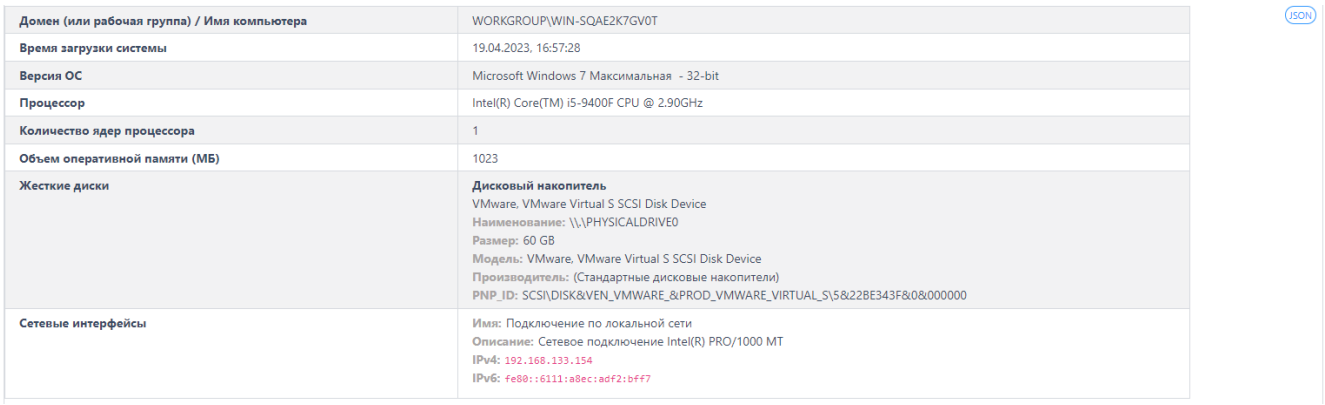


Рисунок 186 – Дополнительная информация о верифицируемом агенте

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** (рис. 187).

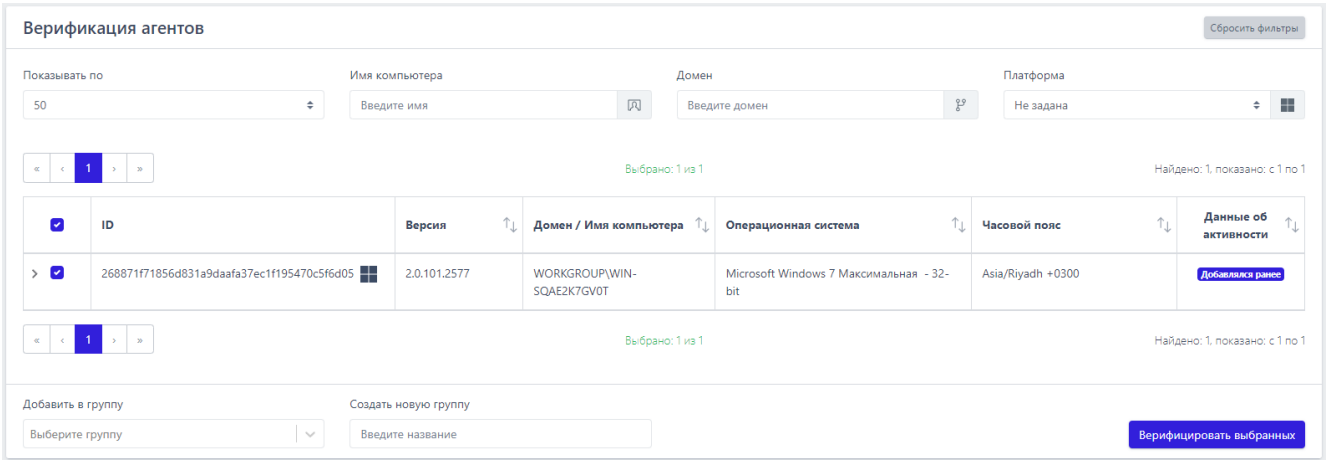


Рисунок 187 – Агент, требующий верификации

Элементы навигации в таблице с агентами, требующими верификации, идентичны описанным в пункте 6.2.1 (см. рис. 19).

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.

6.6.5. Терминал

Общая информация

Терминал является консолью управления, предназначенной для задания команд определенному агенту. Формат команд аналогичен формату команд интерпретатора Windows, а также средства автоматизации PowerShell. При переходе на страницу **Терминал** появится окно, представленное на рисунке 188.

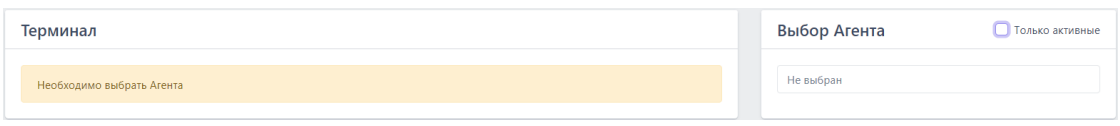


Рисунок 188 – Страница «Терминал»

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 (рис. 189):

1) Область просмотра истории работы с терминалом;

2) Область ввода команд.

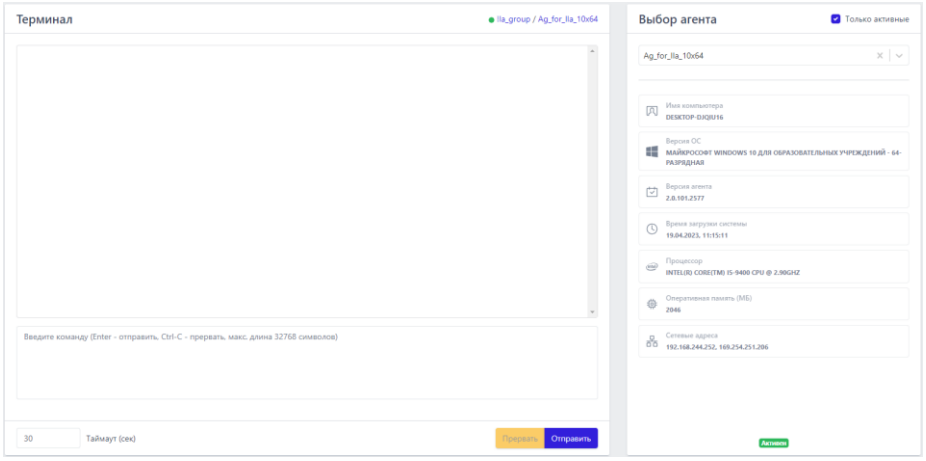


Рисунок 189 – Страница «Терминал» активного агента

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)** (рис. 190).

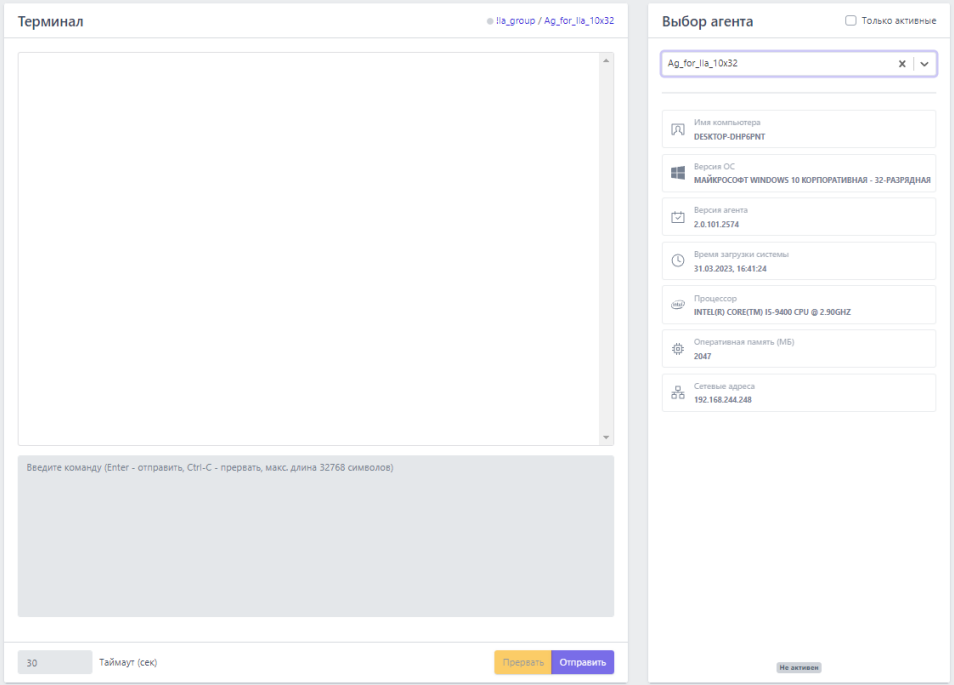


Рисунок 190 – Страница «Терминал» неактивного агента

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. 191).

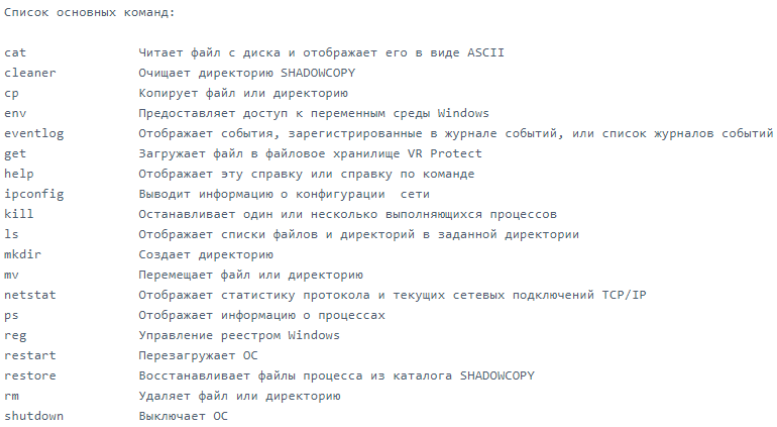


Рисунок 191 – Список основных команд терминала

Если требуется справка о команде из представленного списка, необходимо ввести команду, написание которой удовлетворяет синтаксису:

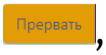
1) **get-helphelp {<имя_командлета> | <название_раздела>};**

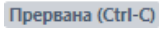
2) **help {<имя_командлета> | <название_раздела>};**

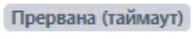
3) **<имя_командлета> -?.**

Снизу от области просмотра истории терминала находится кнопка перехода к результату последнего ввода команды 

.

В нижней части области **Терминал** содержится кнопка 

, ее действие дублируется с помощью нажатия сочетания клавиш Ctrl+C во время выполнения команды в терминале. С помощью кнопки или сочетания клавиш можно прервать выполнение команды. Статус команды поменяется на 

, а через единицу времени, указанную в поле **Таймаут (сек)** статус поменяется на 

.

Для установки времени ожидания ответа от агента при отправке команд в поле **Таймаут (сек)** необходимо указать нужный интервал времени в секундах. По умолчанию время ожидания составляет 30 секунд.

Для изменения агента в области **Выбор Агента** нужно нажать кнопку  в строке с названием текущего агента, после чего из выпадающего списка выбрать нового агента.

Перечень команд, реализованных в службе агента:

– clean;

– get;

– put;

– inventory;

– restore;

– startas;

– stop;

– tray;

– off;

– enable;

– Перезапуск службы агента.

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 **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 – сервер аналитики, 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 сервер аналитики).

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\ИБ Реформ\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\ИБ Реформ\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 – сервер аналитики (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 сервера аналитики: 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

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 – 

.

6.6.6. 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 (рис. 192).

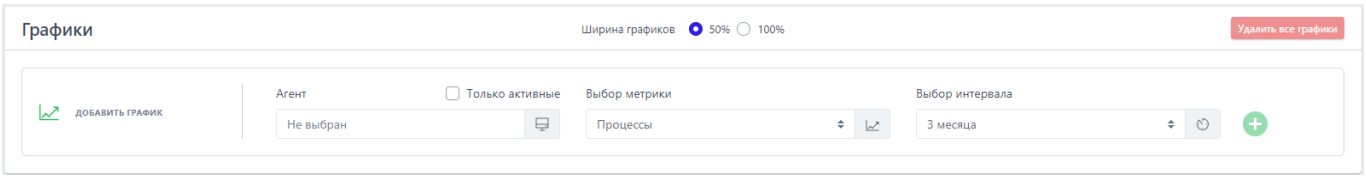


Рисунок 192 – Страница «Графики»

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:

1) График с выбранной шириной 50% (рис. 193);

2) График с выбранной шириной 100% (рис. 194).

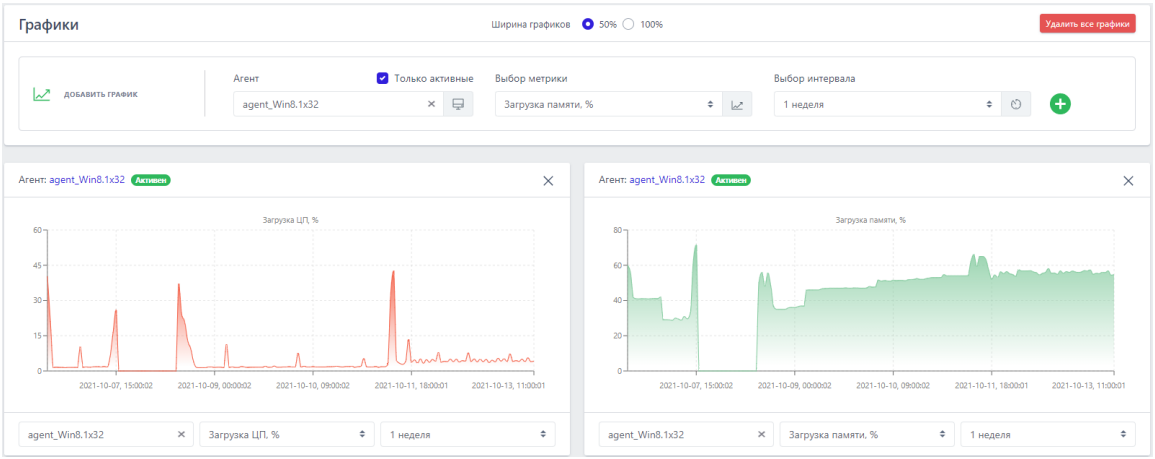


Рисунок 193 – Ширина графиков 50%

Рисунок 194 – Ширина графиков 100%

Область отображения графика включает в себя:

1) 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.

6.6.7. Хранилище

Общая информация

На странице **Хранилище** отображаются все файлы, загруженные в файловое хранилище программы (рис. 195). 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 **сервера аналитики** 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**.

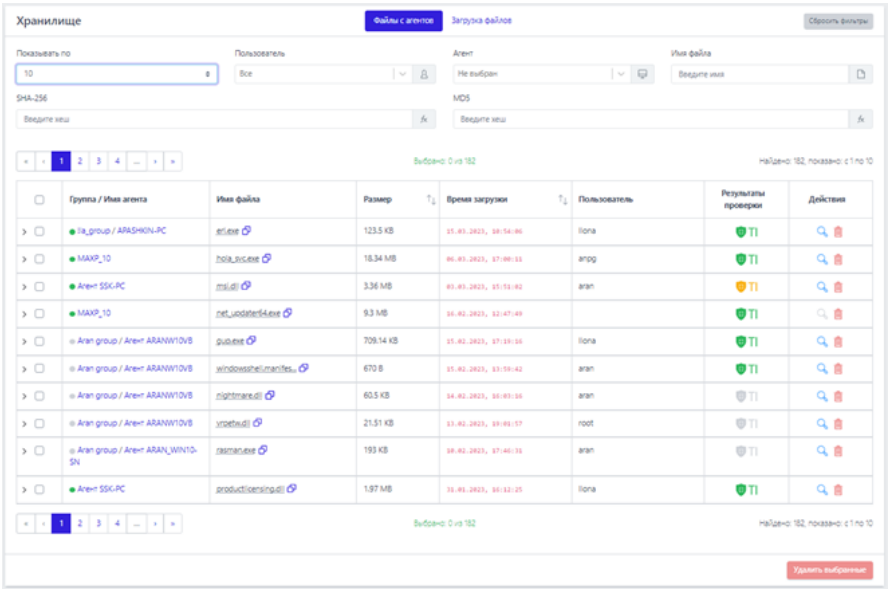


Рисунок 195 – Страница «Хранилище»

Информация о файлах, полученных от агента, представлена в табличном виде. Навигация (см. рисунок 19) 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 Файл загружается... .

Для перехода к странице **Агент** необходимо нажать ЛКМ на названии агента в столбце **Группа/Имя агента**.

Для перехода к странице **Группа** следует нажать ЛКМ на названии группы агентов в столбце **Группа/Имя агента**.

Имя файла – поле содержит относительное имя файла, загруженного с агента. Для отображения полного имени файла необходимо навести курсор на значение относительного имени.

Размер – поле содержит размер файла, загруженного с агента. Размер указывается в единицах кратных байту (байтах, килобайтах и т.д.).

Время загрузки – в поле отображается время в формате UTC, в которое файл был загружен с агента на сервер.

Пользователь – в поле отображается имя пользователя, загрузившего файл.

Результаты проверки – в поле отображается кнопка отчета сервера аналитики по загруженному файлу (подробная информация об отчётах сервера аналитики содержится в пункте 6.5.3). Кнопка со значком TI обозначает безопасный файл (рис. 196).

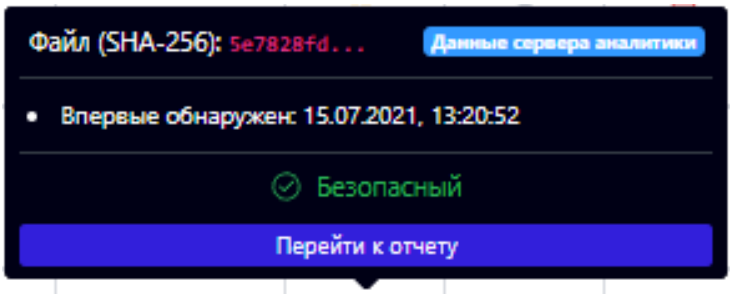


Рисунок 196 – Угроз нет (отчёт сервера аналитики)

Кнопка со значком TI обозначает вредоносный файл (рис. 197).

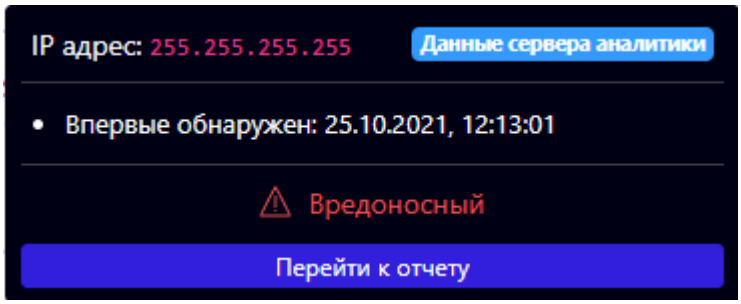


Рисунок 197 – Вредоносный файл (отчёт сервера аналитики)

Кнопка со значком TI обозначает проверку файла сервером аналитики в текущий момент времени (рис. 198). Для получения данных необходимо нажать кнопку **Перейти к отчету**.

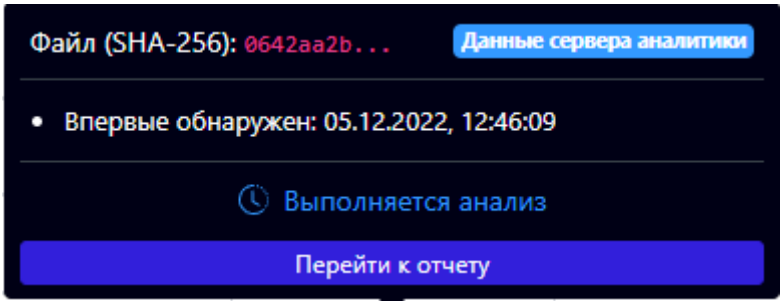


Рисунок 198 – Выполняется проверка сервером аналитики

В случае загрузки файла, информация по которому отсутствует в сервере аналитики, кнопка отчета файла отображается со значком TI, и окно с отчетом приобретает вид, как указано на рисунке 199.

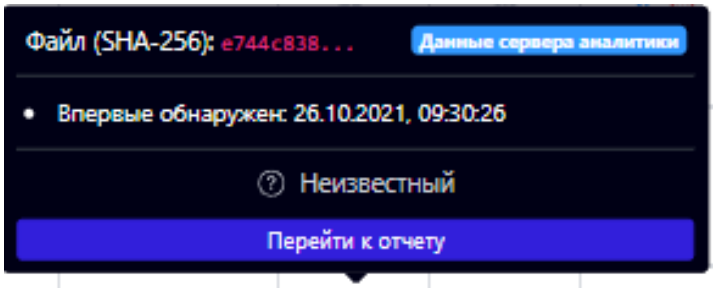


Рисунок 199 – Файл неизвестен

При нажатии ЛКМ на кнопки в столбце результаты проверки пользователь сможет увидеть краткий отчет о состоянии загруженного в **Хранилище** файла (см. рис. 196 – 198).

Действие – в поле отображаются кнопки операций, выполняемых с загруженным файлом. Пользователю доступны операции **Просмотреть файл** и **Удалить файл** . Во вкладке **Загрузка файлов** в этом поле также будет отображаться значок **Получить ссылку на скачивание** ( ). Скопировав его в строку браузера, администратор может загрузить файл с вкладки **Загрузка файлов**.

Кнопка **Просмотреть файл** открывает окно **Просмотр файла**. Кнопка **Удалить файл** удаляет загруженный файл с сервера. После нажатия кнопки открывается окно **Подтверждение действия** (рис. 200), в котором необходимо нажать кнопку Выполнить. В нижней части страницы появится сообщение об удалении выбранного файла (рис. 201). Для отмены операции следует нажать кнопку Отмена или кнопку закрытия окна .

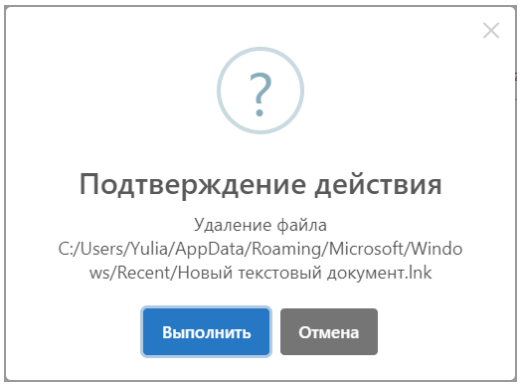


Рисунок 200 – Удаление загруженного файла

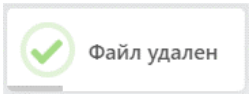


Рисунок 201 – Сообщение об удалении загруженного файла

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** (рис. 202).

Имя	C:\Program Files (x86)\Microsoft Visual Studio\2019\Community\Common7\IDE\PrivateAssemblies\Microsoft.VisualStudio.Telemetry.dll
Время загрузки	20.05.2021, 12:07:15
Размер	858.37 KB
Пользователь	admin-Dmitry-S
MD5	25464f31f0f26cdcea07b1e98bd7381e
SHA-256	d6bb742e660586f277ef86d15e64c96aa9eeeb9904bc4d8c3a162d2abf6e90a0

Рисунок 202 – Дополнительная информация о загруженном файле

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

открывшемся окне **Подтверждение действия** (рис. 203) следует нажать кнопку Выполнить. В нижней части страницы появится сообщение об удалении выбранных файлов (рис. 204). Для отмены операции необходимо нажать кнопку Отмена или кнопку закрытия окна ×.

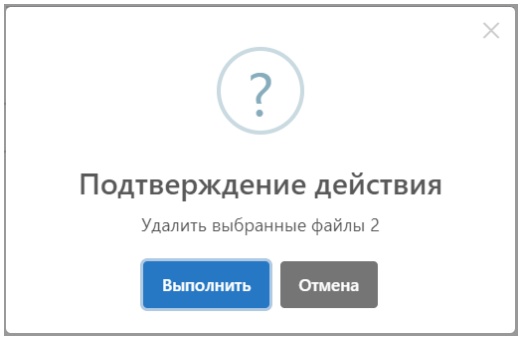


Рисунок 203 – Подтверждение удаления загруженных файлов

Рисунок 204 – Сообщение об удалении загруженных файлов

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. 205), необходимо нажать кнопку 🔍 на странице **Файлы Агента** в разделе **Хранилище**.

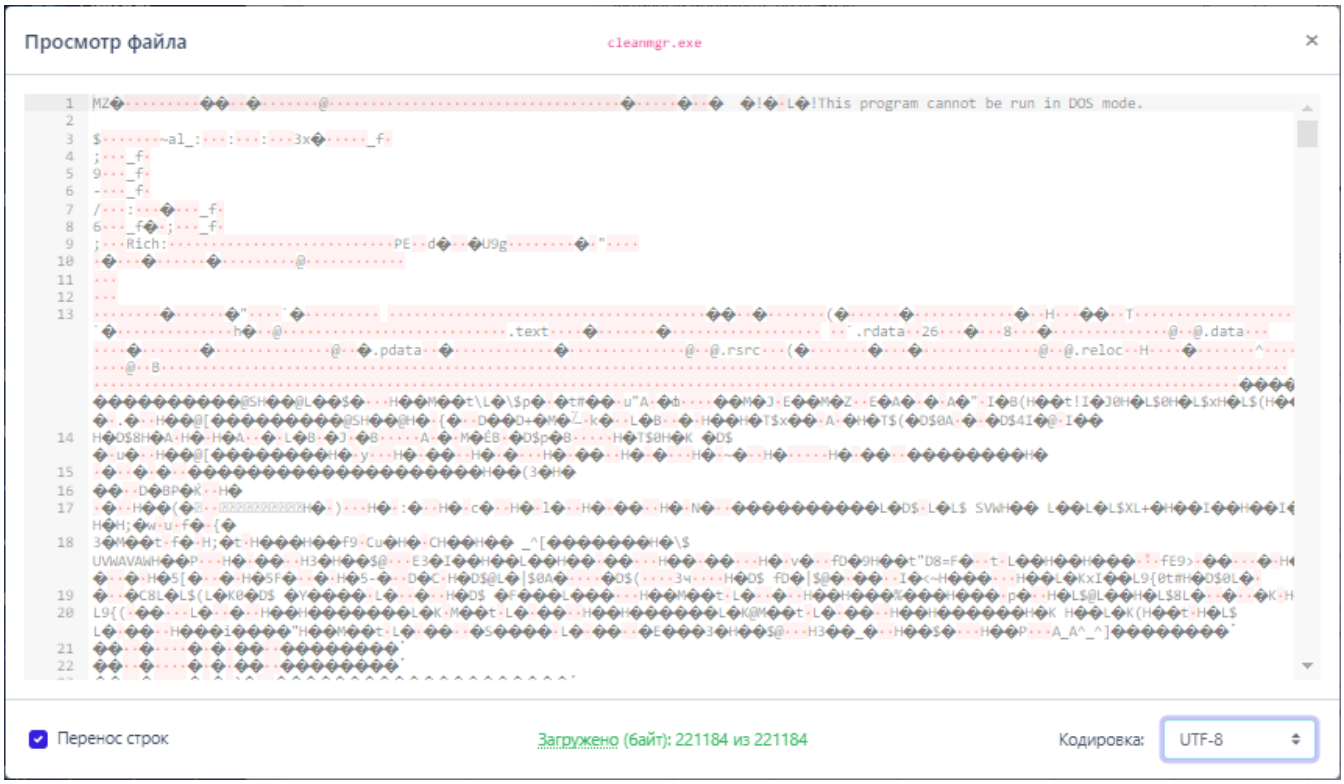


Рисунок 205 – Просмотр файла

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. 206) .

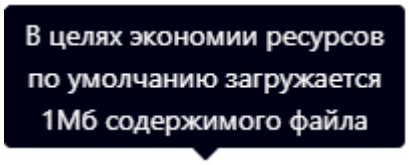


Рисунок 206 – Сообщение в окне «Просмотр файлов»

Для просмотра информации в бинарном формате следует изменить формат отображения в строке **Кодировка** с **UTF-8** на **Нет (Binary)** (рис. 207).

Рисунок 207 – Просмотр файла (бинарный)

6.6.8. Управление уязвимостями

Управление уязвимостями осуществляется в разделе **Уязвимости.** Страница **Управление уязвимостями** содержит список сканирований агентов за последние 3 месяца, список ПО, просканированного программой, а также список уязвимостей, найденных на агентах. Для изучения статистики по сканируемой инфраструктуре в верхней части страницы находятся диаграммы с информацией по общему количеству выполненных сканирований, количеству уникальных и уязвимых программ, обнаруженных на просканированных агентах, количеству обнаруженных уязвимостей, разделенных по степени критичности, и количеству проверенных и непроверенных агентов в общей защищаемой инфраструктуре. При нажатии строк с количественными значениями на диаграммах **Сканирование** и **Уязвимости** происходит переход на соответствующие вкладки.

Подробную информацию о сканировании агента можно просмотреть, нажав номер ID сканирования. Страница **Сканирование** содержит следующие вкладки:

1) ПО с уязвимостями (информация содержит название программы, издателя, версию и количество найденных уязвимостей);

2) Критические уязвимости (информация содержит номер CVE и CWE, уровень критичности и ссылку на расчеты калькулятора БДУ на сайте ФСТЭК).

3) Рекомендации по устранению (содержит общедоступные известные способы устранить уязвимости).

На странице **Сканирование** также отображается общая информация о сканировании и уязвимостях: название агента, идентификатор и статус сканирования, дата начала и завершения операции, диаграмма с числом и уровнем критичности уязвимостей, которые были найдены для выбранного сканирования.

В разделе **Список программ** аналитик может просмотреть список всех программ, установленных в защищаемой инфраструктуре, которые были просканированы на наличие уязвимостей. Можно сортировать программы на те, у которых уязвимости были найдены, и программы без найденных уязвимостей. Информация о программах представлена в таблице, которая содержит следующие поля:

1) Название;

2) Издатель;

3) Версия;

4) Число агентов с установленным ПО;

5) Количество уязвимостей.

Нажав ЛКМ на название программы в списке, аналитик может перейти на страницу **Сведения о программе**, на которой представлена информация о

найденных в программе уязвимостях, их критичности, количестве, количестве агентов с этой уязвимостью, поименный список этих агентов и т. д.

В разделе **Список уязвимостей** аналитик может изучить найденные на всех просканированных агентах уязвимости. Информация о них представлена в таблице, которая содержит следующие поля:

1) CVE (содержит CVE-идентификатор);

2) Опубликована (содержит дату публикации уязвимости, то есть время первичного обнаружения на агенте);

3) Изменена (содержит последнюю дату изменения информации об уязвимости);

4) Статус;

5) Балл по CVSS 2.0 (количественная оценка уязвимости безопасности по указанному стандарту);

6) Балл по CVSS 3.0;

7) Критичность;

8) Количество уязвимых программ.

Уязвимости можно сортировать с помощью следующих фильтров:

1) Количество уязвимостей на странице;

2) Критичность;

3) Статус;

4) Наличие уязвимых программ;

5) CVE;

6) Период публикации;

7) Период изменения.

Идентификатор уязвимости в таблице служит гиперссылкой для перехода на страницу, содержащую сводные сведения о найденной уязвимости. На этой странице будет содержаться источник, на основе которого предоставлены сведения об уязвимости, ее описание и критичность, список агентов, на которых

уязвимость была найдена, рекомендации по устранению и другие сведения, относящиеся к найденной уязвимости. Кнопка  в верхней части страницы **Сведения об уязвимости** позволяет перейти к источнику сведений. Сводная информация по уязвимости может быть показана по двум различным стандартам 2.0 и 3.0.

Формирование отчетности на странице с уязвимостями

Администратор может сформировать отчет о найденных на агентах уязвимостях и сохранить этот отчет на компьютер, с которого осуществляется доступ к модулю администрирования программы. Отчет формируется на странице **Управление уязвимостями** в разделе **Сканирования**. Чтобы сохранить отчет в формате csv, необходимо нажать кнопку  , после чего отчет будет доступен в папке **Загрузки**. Для формирования отчета необходимо использовать кнопку  . В отчете отображается полный список ПО на просканированных агентах, в котором присутствуют программы с найденными уязвимостями.

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;

4) Журналы Windows.

Разделы содержат наборы определенных активностей или объектов, а также наборы правил индикации и наборы с исключениями.

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. 208) включает в себя следующие структурные элементы:

– таблица с наборами индикаторов атак;

– кнопка **Добавить набор**;

– кнопка **Применить набор**;

– кнопка **Удалить выбранные наборы**.

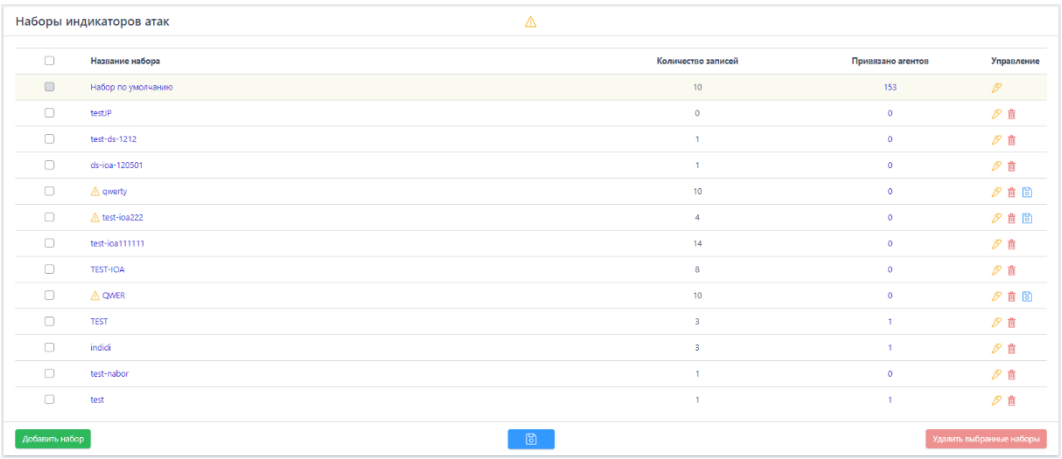


Рисунок 208 – Наборы индикаторов атак, есть не сохраненные наборы

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**.

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 (рис. 209).

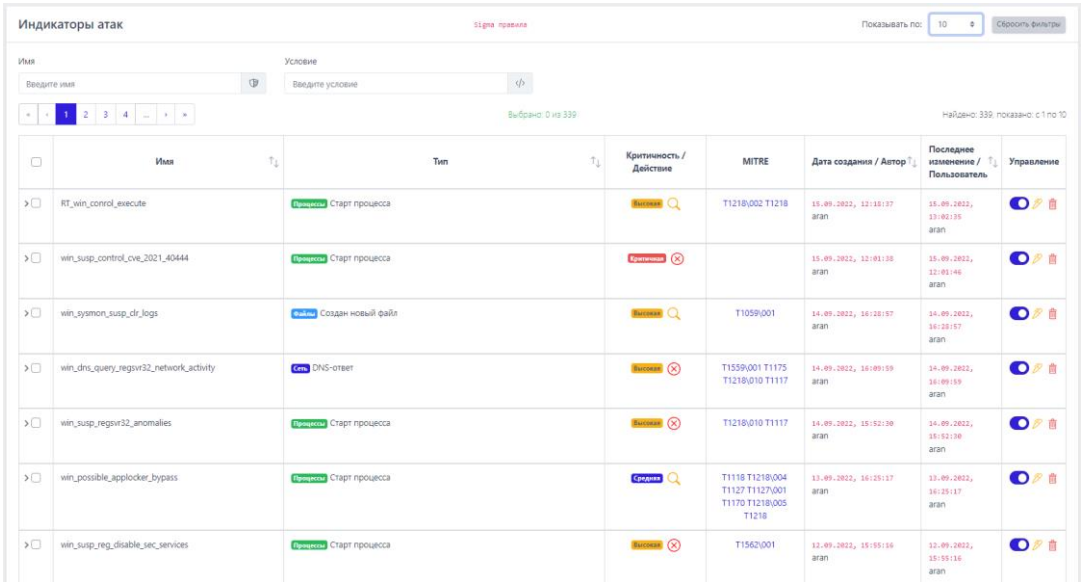


Рисунок 209 – Индикаторы атак

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. В открывшемся окне **Добавить индикатор** (рис. 210) следует прописать условия, на основании которых будет срабатывать правило. Особенности написания индикаторов атак, их синтаксис подробно описывается в документе «Руководство аналитика RT Protect EDR».

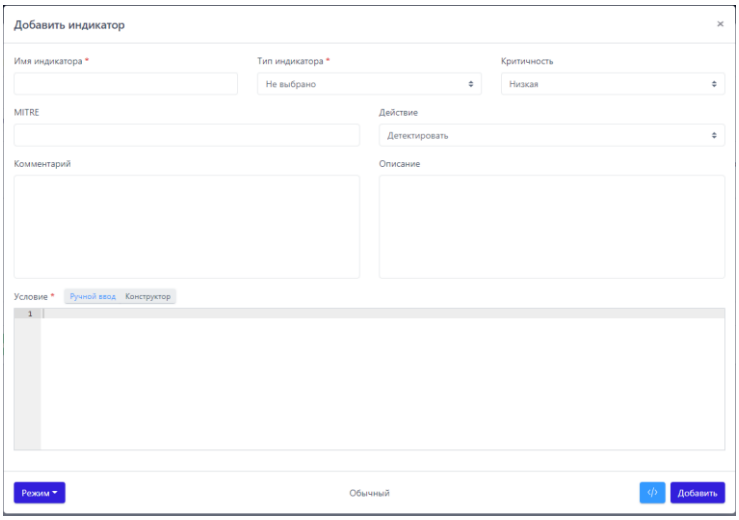


Рисунок 210 – Добавление индикатора

После написания условия необходимо нажать кнопку Добавить. В нижней части страницы появится сообщение о добавлении нового правила (рис. 211).

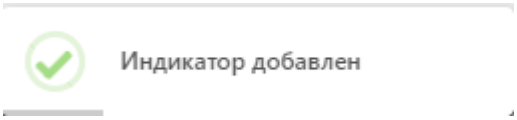


Рисунок 211 – Сообщение о добавлении индикатора атаки

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 (рис. 212).

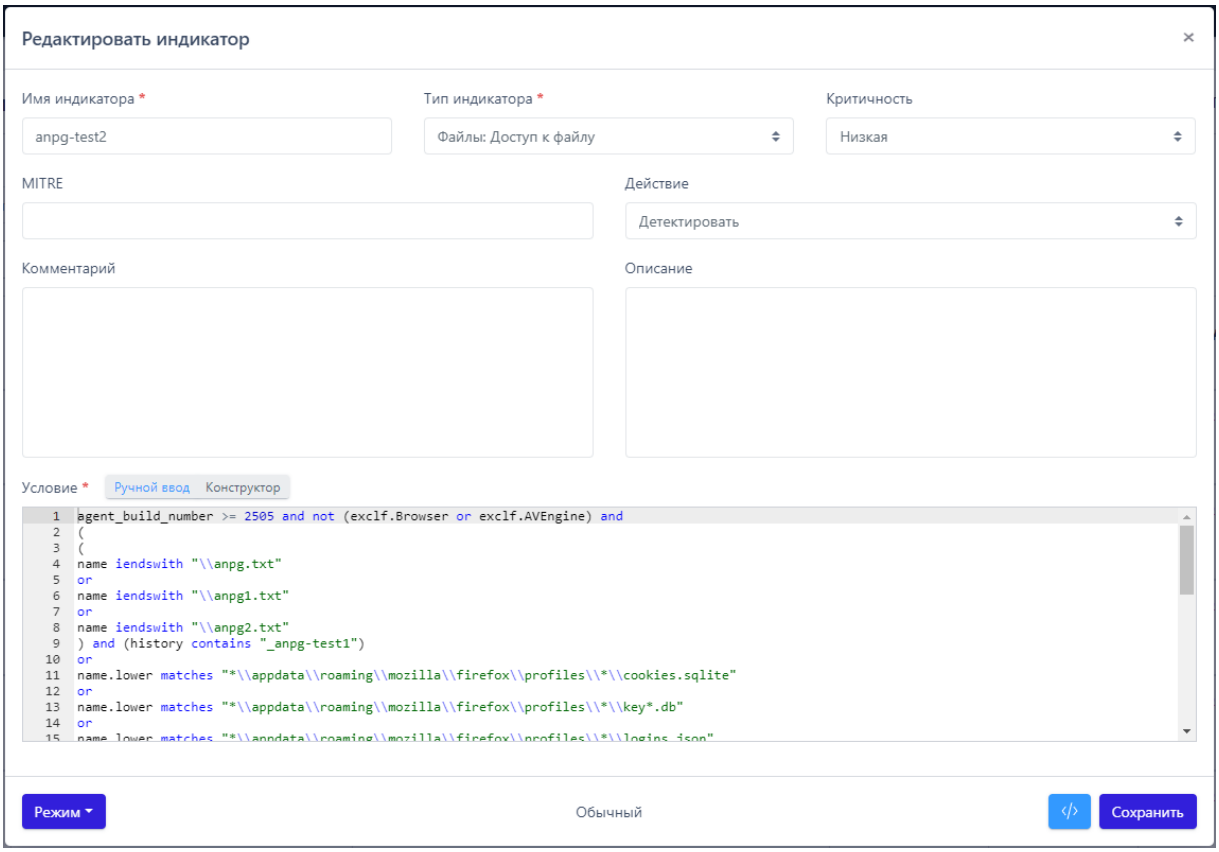


Рисунок 212 – Редактирование индикатора атаки

Для сохранения внесенных изменений необходимо нажать кнопку **Сохранить**, после чего в нижней части страницы появится сообщение об изменении правила (рис. 213).

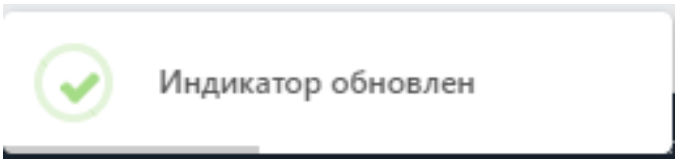


Рисунок 213 – Сообщение об обновлении индикатора атаки

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**.

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.

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.

Важно

Индикаторы по хэш-сумме файла работают только для файлов с активным содержимым. К файлам с активным содержимым в текущей реализации относятся исполняемые файлы (определяются по формату или расширению EXE, DLL, SYS, COM, OCX, SCR, CPL), а также файлы с расширениями PDF, PS1, PSM1, PSD1.

Запуск исполняемого файла, хэш 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 214.

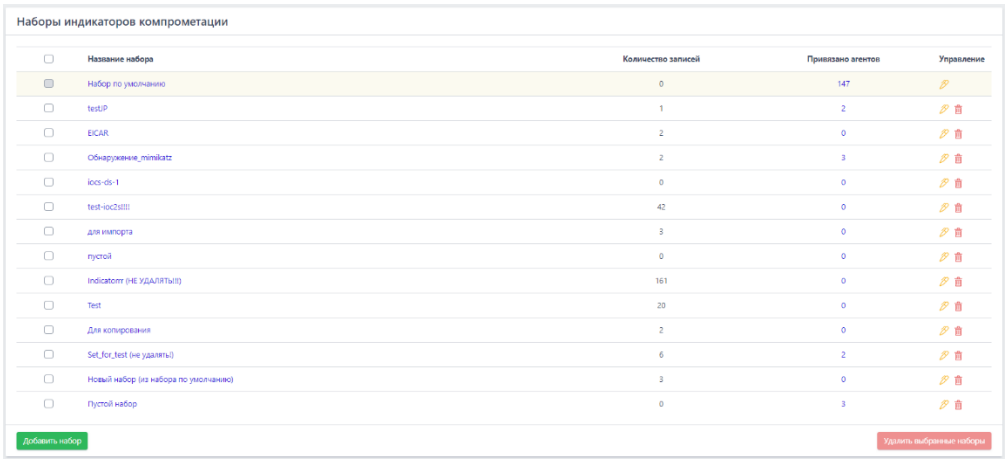


Рисунок 214 – Наборы индикаторов компрометации

Информация на странице представлена в табличном виде. Если на странице присутствует хотя бы один неприменный 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** (рис. 215).

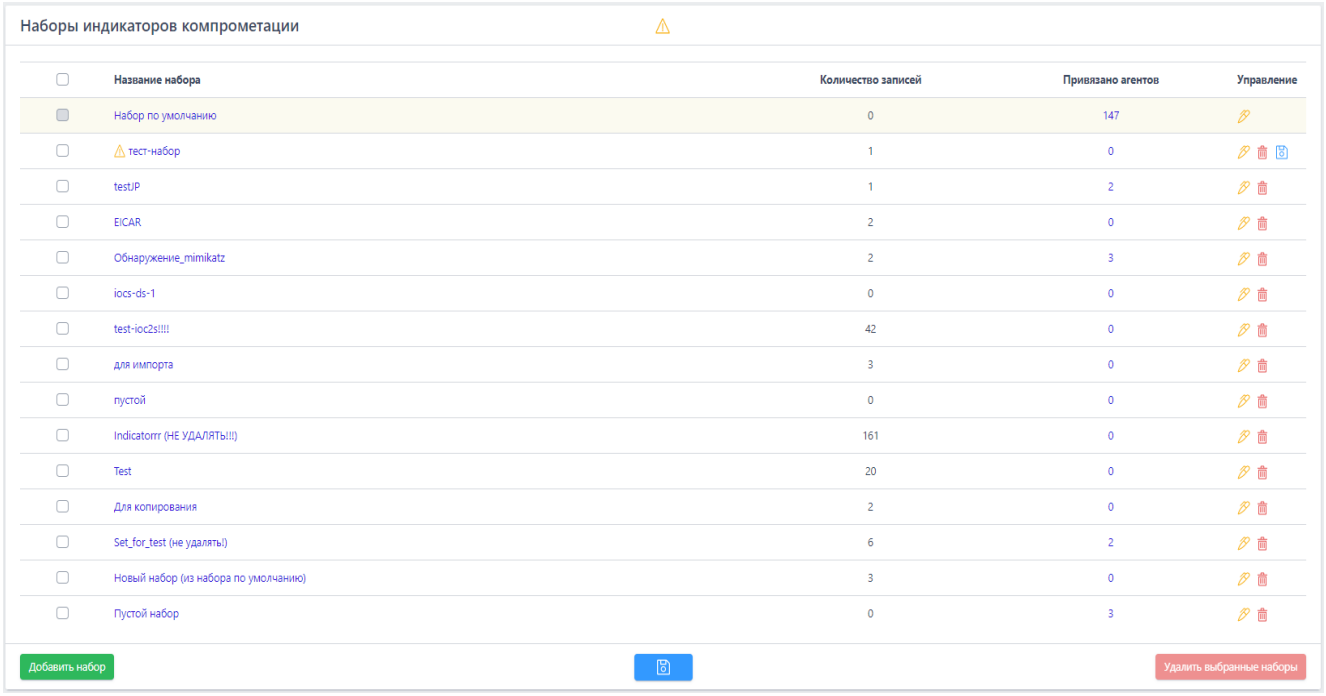


Рисунок 215 – Наборы индикаторов компрометации, есть непримененные наборы

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 (рис. 216).

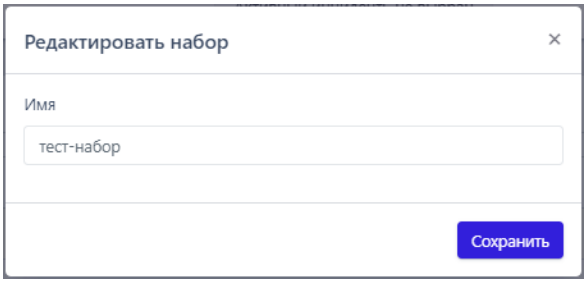


Рисунок 216 – Редактирование имени набора индикаторов компрометации

После сохранения изменений в наборе в нижней части страницы появится сообщение об обновлении набора (рис. 217).

Рисунок 217 – Сообщение об изменении набора индикаторов компрометации

Удалить – при нажатии кнопки открывается окно **Подтверждение действия** (рис. 218).

Далее для удаления набора необходимо нажать кнопку Выполнить, после чего в нижней части страницы появится сообщение об удалении набора

индикаторов компрометации (рис. 219). Для отмены операции следует нажать кнопку Отмена или кнопку закрытия окна .

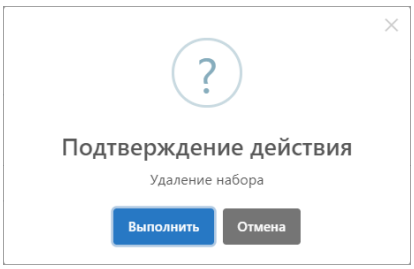


Рисунок 218 – Подтверждение удаления набора индикаторов компрометации

Рисунок 219 – Сообщение об удалении набора индикаторов компрометации

Применить – кнопка отображается в поле **Управление** при условии, что набор индикаторов компрометации не применен. При нажатии кнопки **Применить** открывается окно **Подтверждение действия** (рис. 220). Далее для применения набора необходимо нажать кнопку Выполнить, после чего в нижней части страницы появится сообщение о применении набора индикаторов компрометации (рис. 221). Для отмены операции следует нажать кнопку Отмена или кнопку закрытия окна .

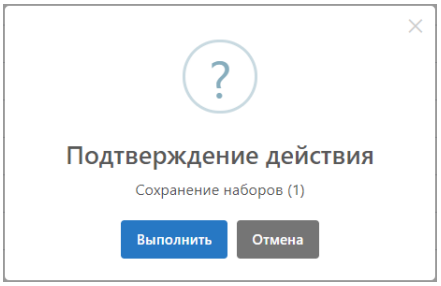


Рисунок 220 – Подтверждение сохранения набора индикаторов компрометации

Рисунок 221 – Сообщение о применении набора индикаторов компрометации

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** (рис. 222) 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.

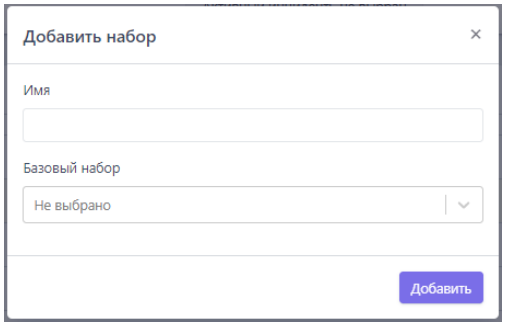


Рисунок 222 – Окно «Добавить набор»

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**, после чего в нижней части страницы появится сообщение о добавлении набора (рис. 223), а строка с новым набором появится в таблице.

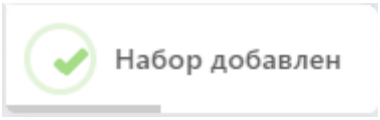


Рисунок 223 – Сообщение о добавлении набора

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** (рис. 224) необходимо нажать кнопку Выполнить, после чего в нижней части страницы появится сообщение об удалении наборов индикаторов компрометации (рис. 225). Для отмены операции следует нажать кнопку Отмена или кнопку закрытия окна .

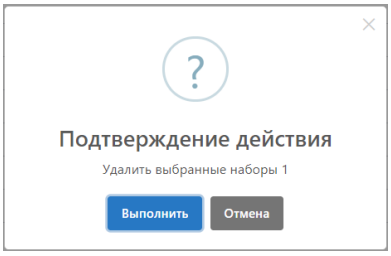


Рисунок 224 – Подтверждение удаления наборов индикаторов компрометации

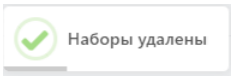


Рисунок 225 – Сообщение об удалении наборов индикаторов компрометации

Страница «Индикаторы компрометации»

Переход на страницу с таблицей **Индикаторы компрометации** (рис. 226) происходит при нажатии ЛКМ на названии набора в таблице **Наборы индикаторов компрометации.**

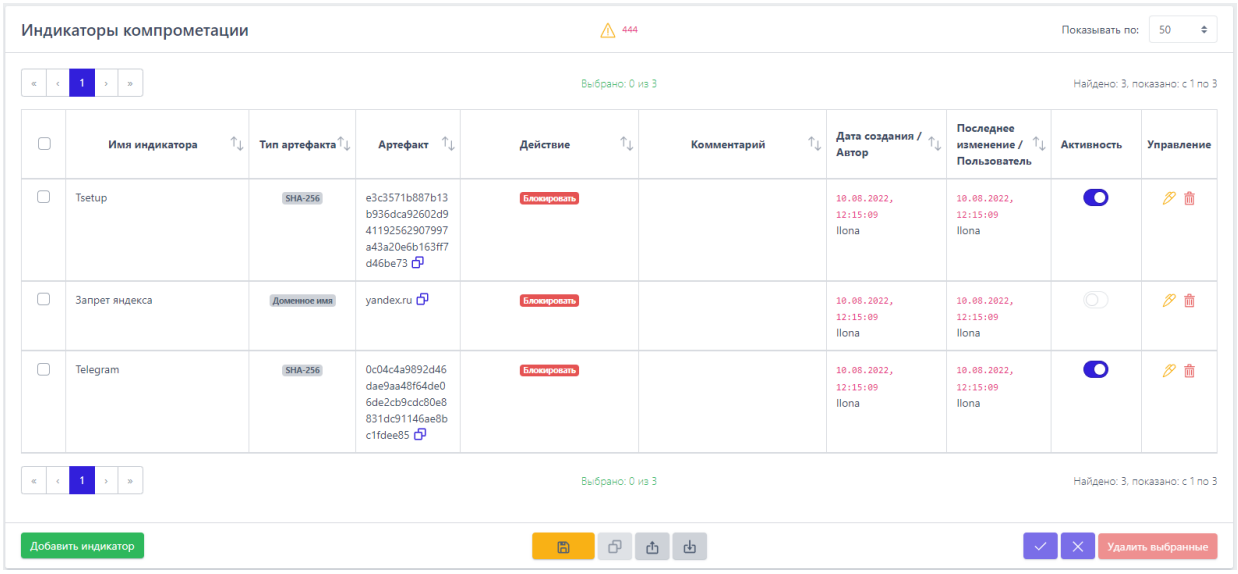


Рисунок 226 – Индикаторы компрометации, несохраненный набор

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** и **100**).

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) **Не выбрано** (тип, устанавливаемый по умолчанию, для добавления индикатора необходимо менять на любой другой тип);

2) **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)**;

3) **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;

4) **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;

5) **MD5** – в качестве индикатора компрометации в поле **Артефакт** будет выбрано значение хеша, рассчитанного по алгоритму MD5, для объекта, при обнаружении которого программа создаст инцидент;

6) **IP-адрес** – в качестве индикатора компрометации в поле **Артефакт** будет выбран IP-адрес сетевого соединения, при взаимодействии с которым программа создаст инцидент;

7) **Доменное имя** – в качестве индикатора компрометации в поле **Артефакт** будет выбрано имя домена, например, mail.ru, 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** (рис. 227). Поля формы **Редактировать индикатор** идентичны полям таблицы индикаторов, описанным выше.

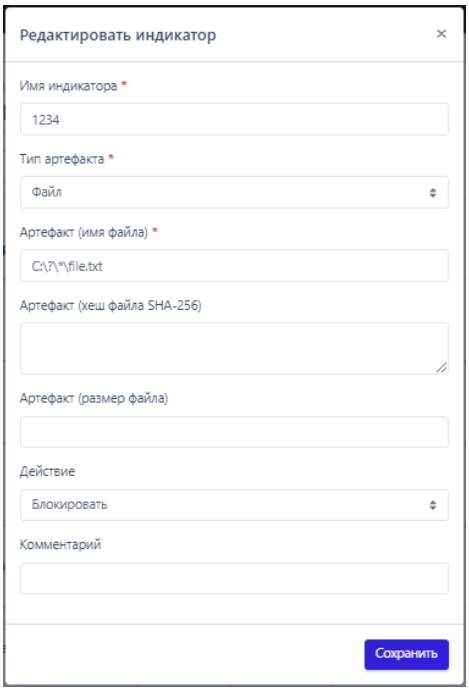


Рисунок 227 – Окно «Редактировать индикатор» тип артефакта «Файл»

После сохранения изменений в нижней части страницы появится сообщение об изменении индикатора (рис. 228).

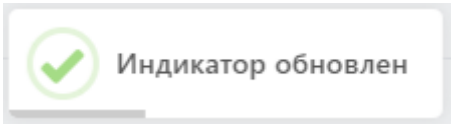


Рисунок 228 – Сообщение об изменении индикатора компрометации

Для удаления индикатора компрометации необходимо нажать кнопку **Удалить** . В открывшемся окне **Подтверждение действия** (рис. 229) следует нажать кнопку Выполнить, после чего в нижней части страницы появится сообщение об удалении индикаторов компрометации (рис. 230). Для отмены операции необходимо нажать кнопку Отмена или кнопку закрытия окна .

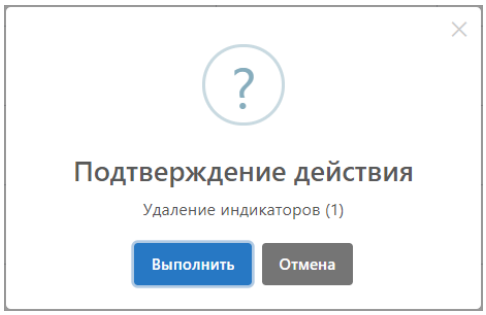


Рисунок 229 – Подтверждение удаления индикаторов компрометации

Рисунок 230 – Сообщение об удалении индикатора компрометации

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

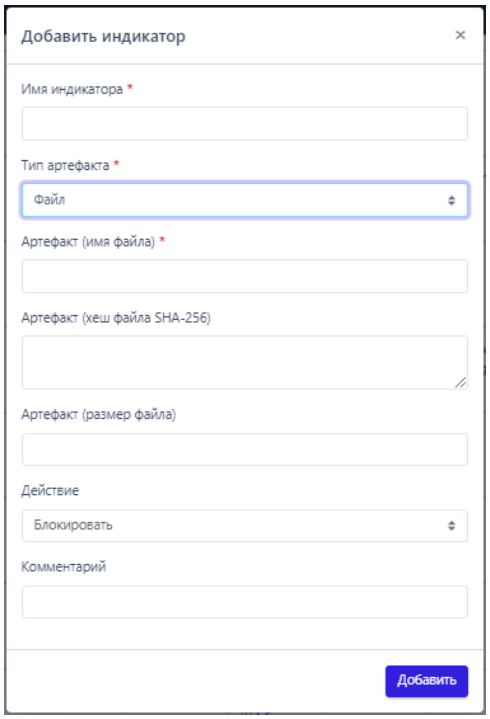


Рисунок 231 – Окно «Добавить индикатор» с типом артефакта «Файл»

В нижней части страницы появится сообщение о добавлении индикатора компрометации (рис. 232).

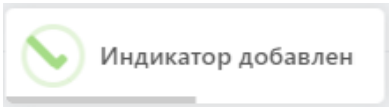


Рисунок 232 – Сообщение о добавлении индикатора

Для применения любого изменения в индикаторах набора необходимо нажать кнопку **Применить набор**. После сохранения изменений в нижней части страницы появится всплывающее сообщение о применении набора (рис. 233). Кнопка  не будет отображаться на странице до внесения следующих изменений в набор.

Рисунок 233 – Сообщение о применении набора индикаторов

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** (рис. 234) 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 .

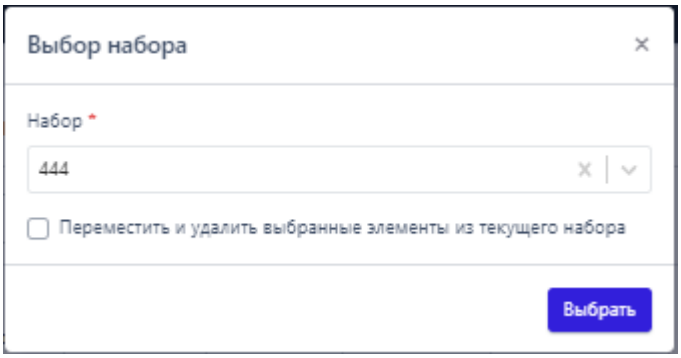


Рисунок 234 – Выбор набора (копирование/перемещение индикаторов в набор)

После завершения копирования/перемещения в нижней части страницы появится сообщение о том, что данные скопированы или перемещены в выбранный набор (рис. 235).

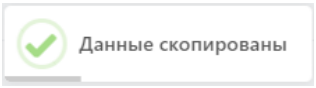


Рисунок 235 – Сообщение о копировании индикаторов компрометации

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

Общая информация

Правила, указанные в разделе **Yara-правила**, 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

Страница с наборами Yara-правил (рис. 236) включает в себя следующие структурные элементы:

– таблица с наборами Yara-правил;

– кнопка **Добавить набор**;

– кнопка **Применить набор**;

– кнопка **Удалить выбранные наборы**.

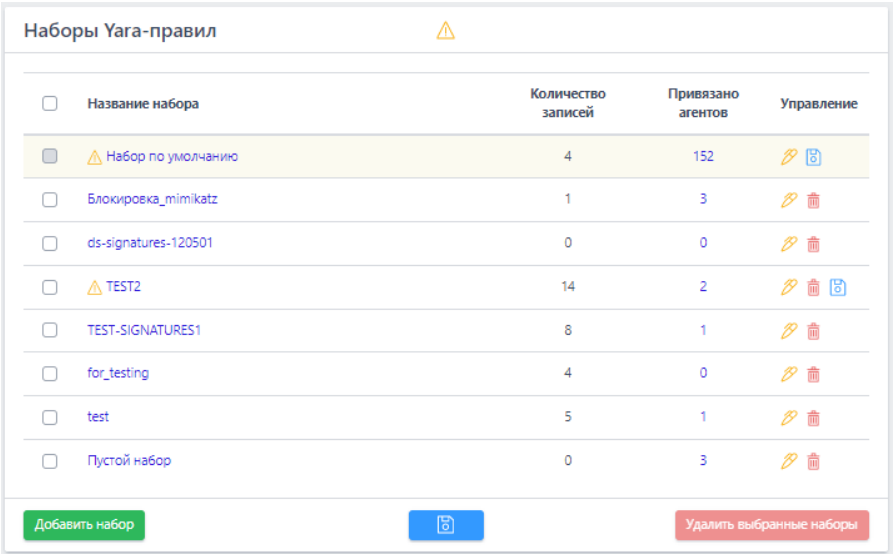


Рисунок 236 – Наборы Yara-правил

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.**

При нажатии ЛКМ на имени набора открывается страница **Yara-правила** для выбранного набора (рис. 237).

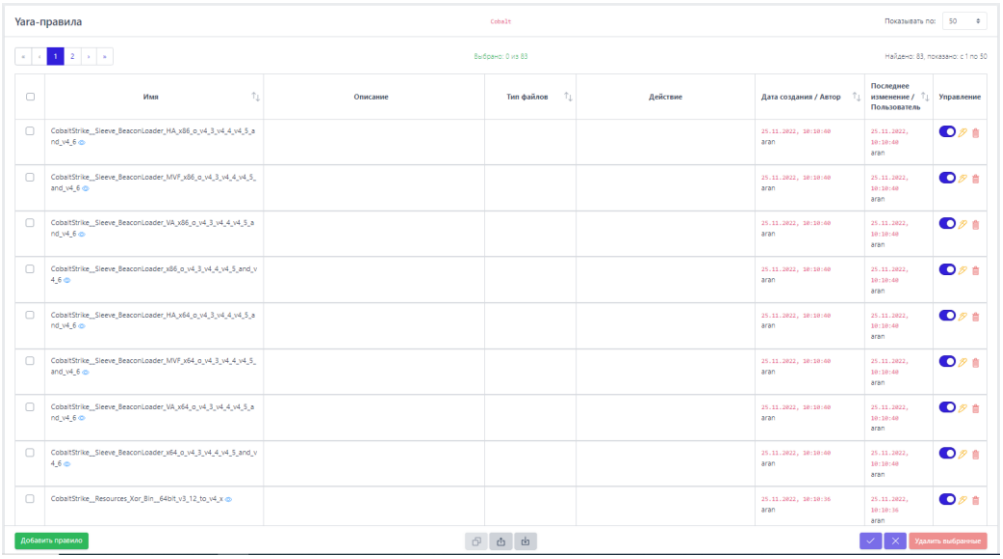


Рисунок 237 – Yara-правила

Страница «Yara-правила»

На странице **Yara-правила** 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 правило**, после чего откроется окно **Добавление YARA-правила**, в котором необходимо прописать условие в соответствии с синтаксисом Yara (рис. 238).

Рисунок 238 – Добавление YARA-правила

Подробная информация о синтаксисе Yara содержится в документе «Руководство аналитика» и официальной документации Yara. Пример правила Yara приведен на рисунке 239.

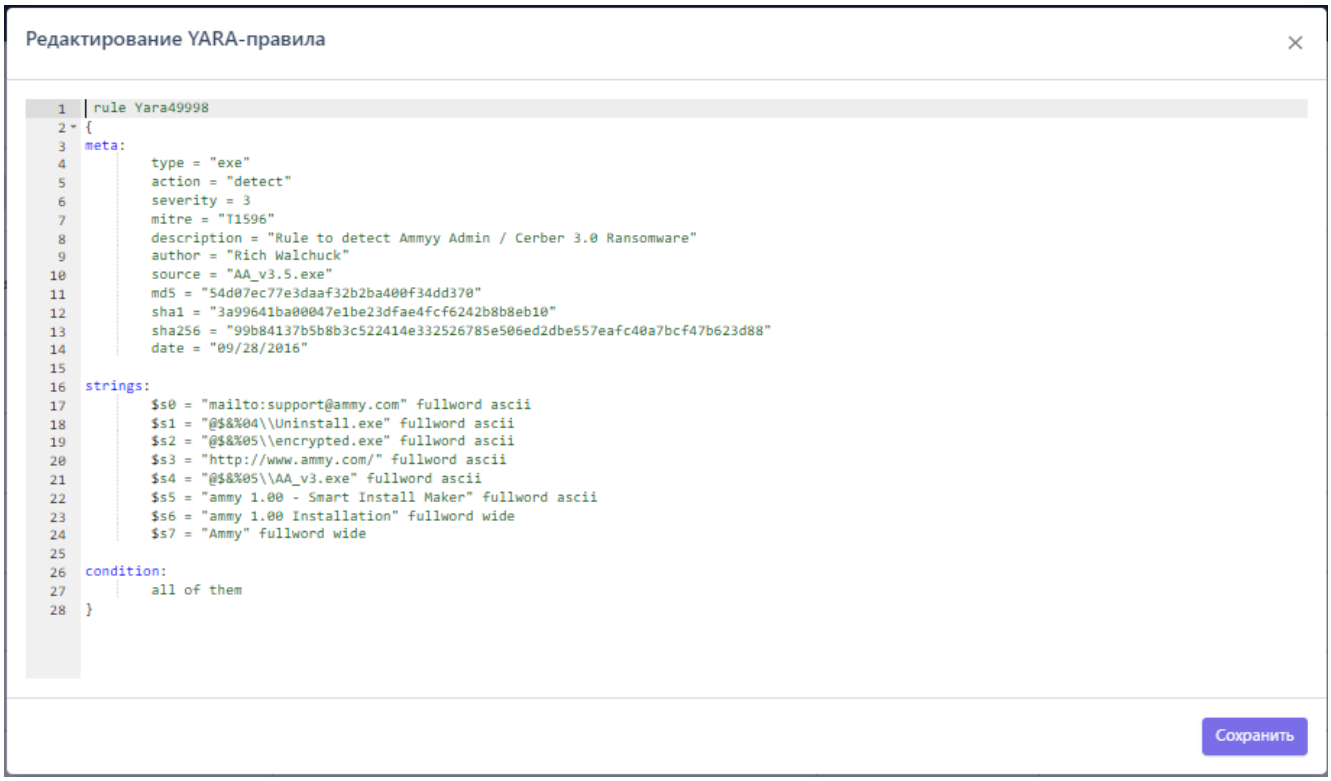


Рисунок 239 – Пример правила Yara

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

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 формата Yara** ( ). Набор будет сохранен в папке **Загрузки** в формате *.yara. Для импорта правил из файла требуется нажать кнопку **Импортировать данные из файла в набор, поддерживаемые форматы: Yara** (

). 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**.

6.7.4. 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 подсистемы **Журналы Windows** программы RT Protect EDR. Информация о собранных ETW-событиях может быть использована при написании индикаторов атак.

Важно

Индикаторы атак, основанные на журналах Windows, могут работать только на детектирование, так как обрабатывают события постфактум, то есть после того, как они произошли на агенте и были зафиксированы подсистемой ETW.

Наборы журналов Windows

Страница **Наборы журналов Windows** содержит следующие структурные элементы (рис. 240):

– таблица с наборами журналов Windows;

– кнопка **Добавить набор**;

– кнопка **Применить все наборы**;

– кнопка **Удалить выбранные наборы**.

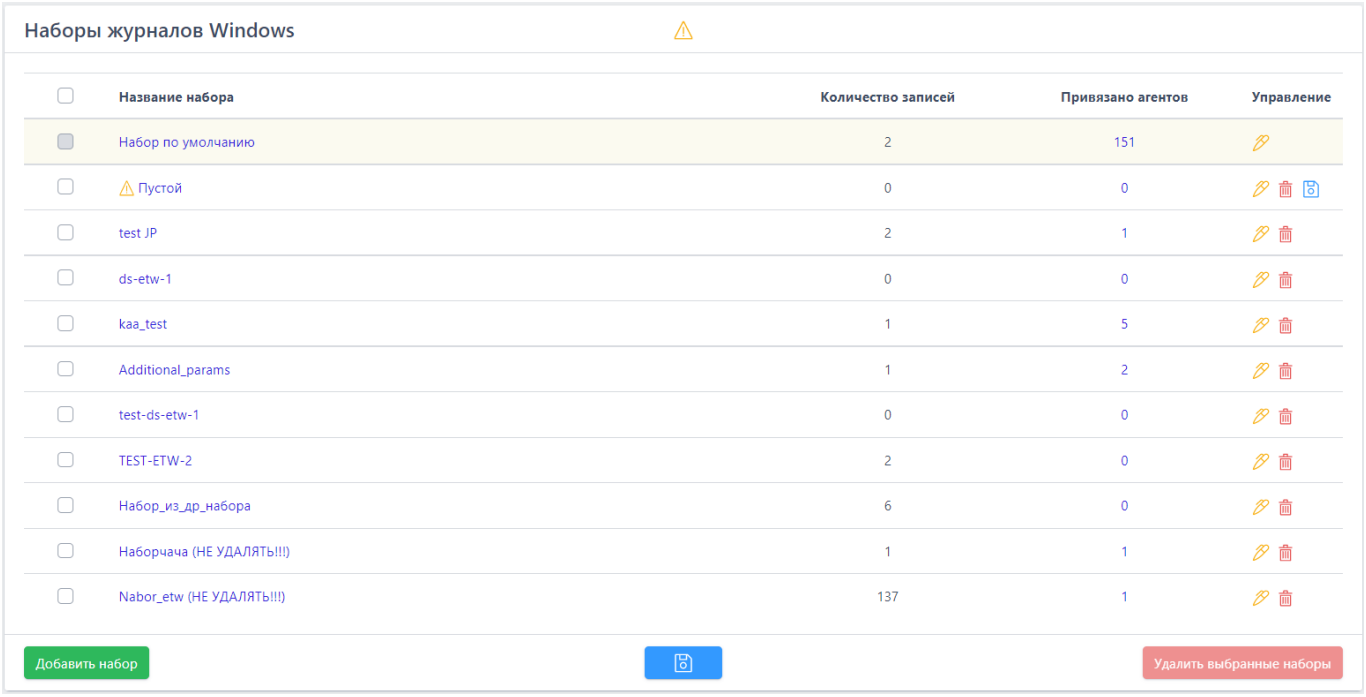


Рисунок 240 – Наборы журналов Windows

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. (рис. 241).

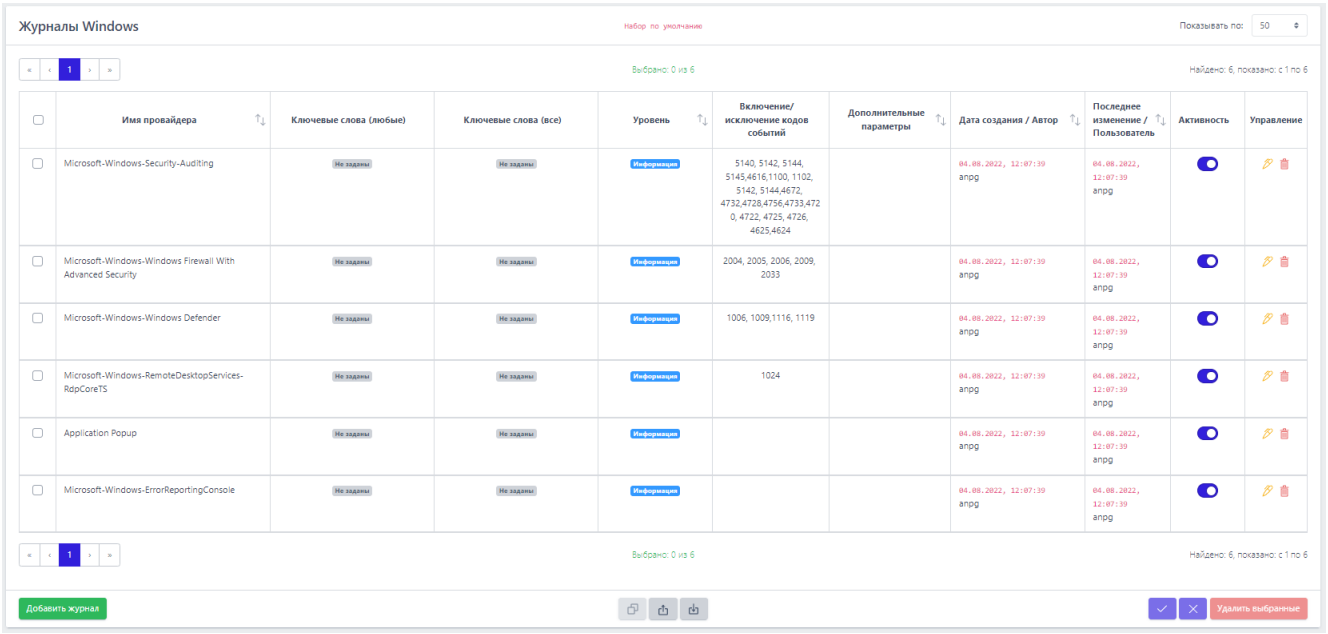


Рисунок 241 – Журналы Windows

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. 242).

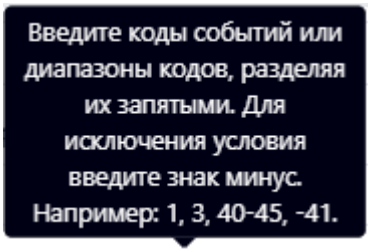


Рисунок 242 – Правила записи кодов событий

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.

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.

6.8.1. Исключения для программ

Общая информация

На странице **Наборы исключений для программ** (рис. 243) 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.

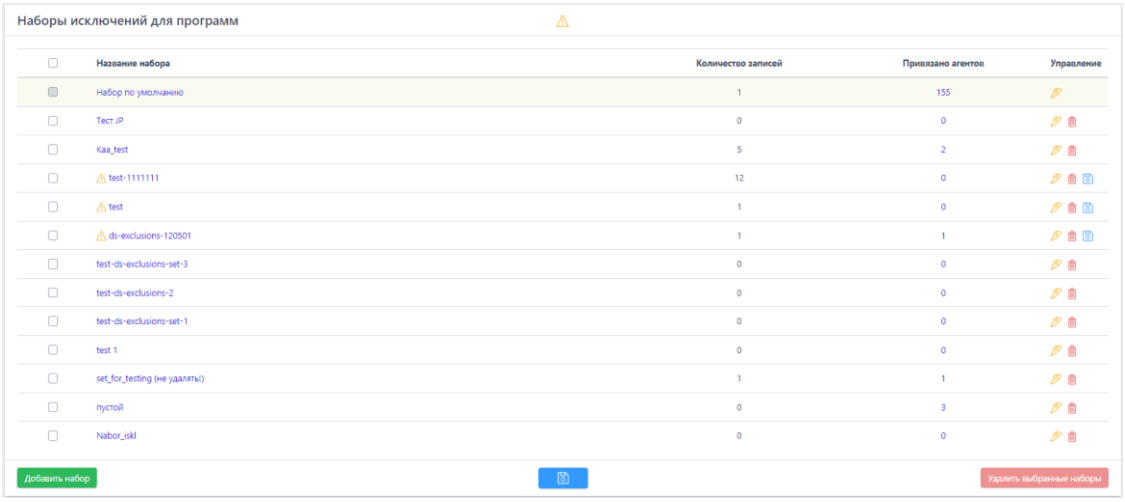


Рисунок 243 – Наборы исключений для программ

`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** (рис. 244) 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.

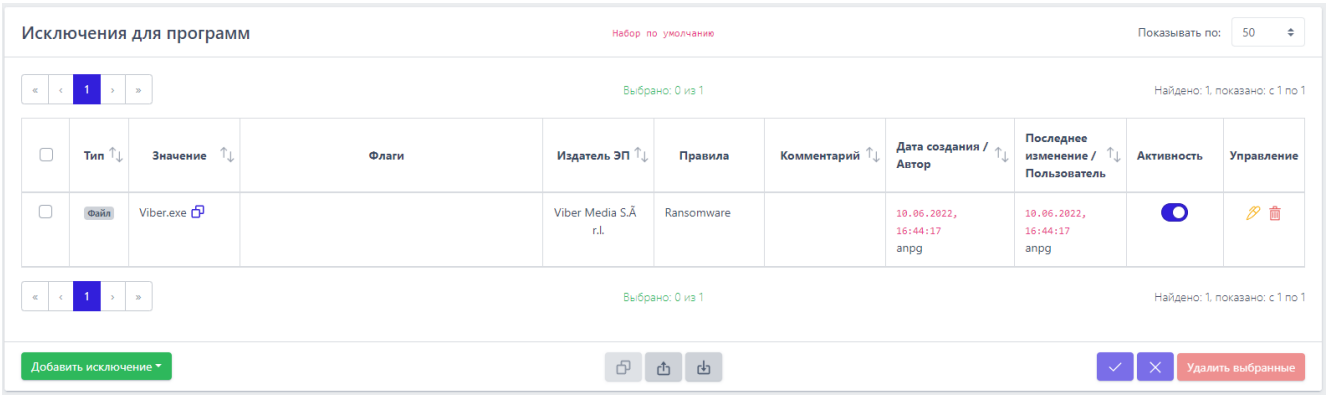


Рисунок 244 – Исключения для программ

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** (рис. 245).

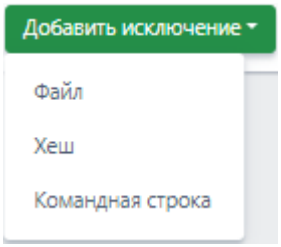


Рисунок 245 – Добавить исключение для программ (выбор типа)

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** (рис. 246).

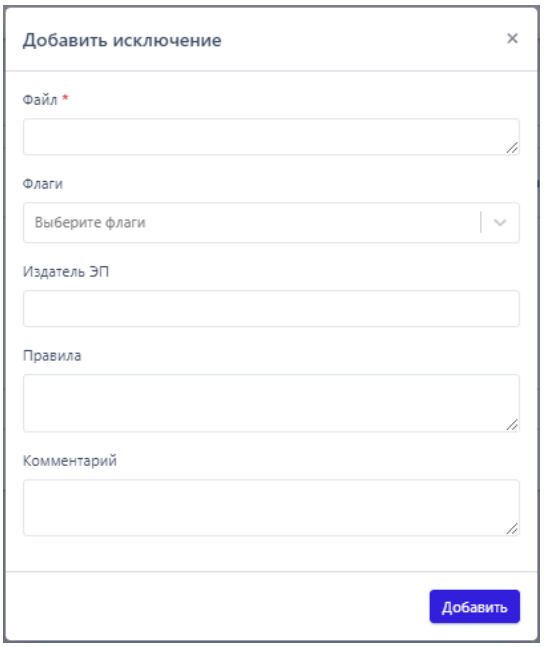


Рисунок 246 – Добавление исключения для программы (тип «Файл»)

Для типа исключений **Хеш** следует определить следующие параметры: **Тип хеш-суммы, Хеш-сумма, Флаги, Издатель ЭП, Правила, Комментарий** (рис. 247).

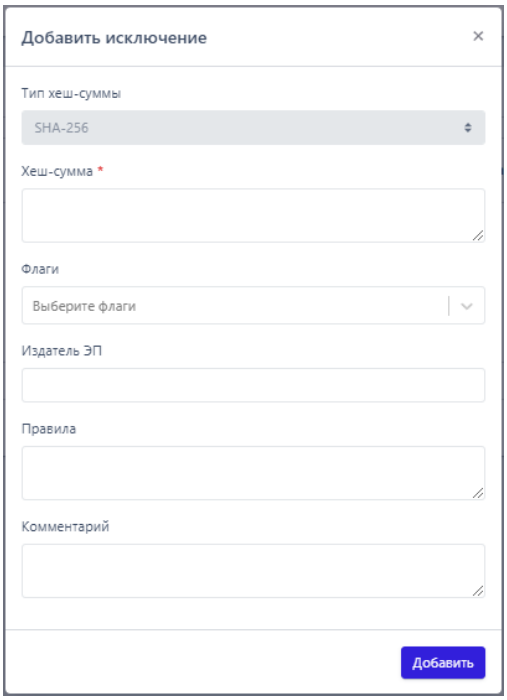


Рисунок 247 – Добавление исключения для программы (тип «Хеш»)

Для типа исключений **Командная строка** необходимо определить следующие параметры: **Командная строка прародителя, Командная строка родителя, Командная строка процесса, Флаги, Издатель ЭП, Правила, Комментарий** (рис. 248).

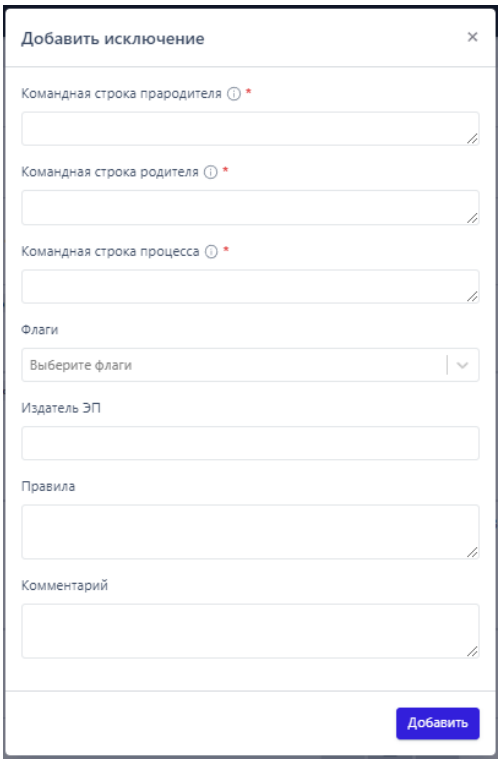


Рисунок 248 – Добавление исключения для программы (тип «Командная строка»)

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) Разрешить внедрение кода в сторонние программы;

2) Разрешить запись памяти сторонних программ;

3) Разрешить доступ к сторонним программам для чтения памяти и управления;

4) Право взаимодействия с критическими системными программами;

5) Разрешить и игнорировать прямой доступ к диску для чтения;

6) Разрешить и игнорировать прямой доступ к диску для записи;

7) Компонент имеет 32-х битную и 64-х битную версию;

8) Хост-процесс;

9) Подтверждение по электронной подписи;

10) Исключить из телеметрии сетевые события;

11) Исключить из телеметрии файловые события;

12) Исключить из телеметрии события реестра Windows;

13) Исключить из телеметрии события поведения.

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.

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** (рис. 249, 250, 251) будет содержать разный набор полей, соответствующий набору полей окна **Добавить исключение** (см. рис. 246 и рис. 247).

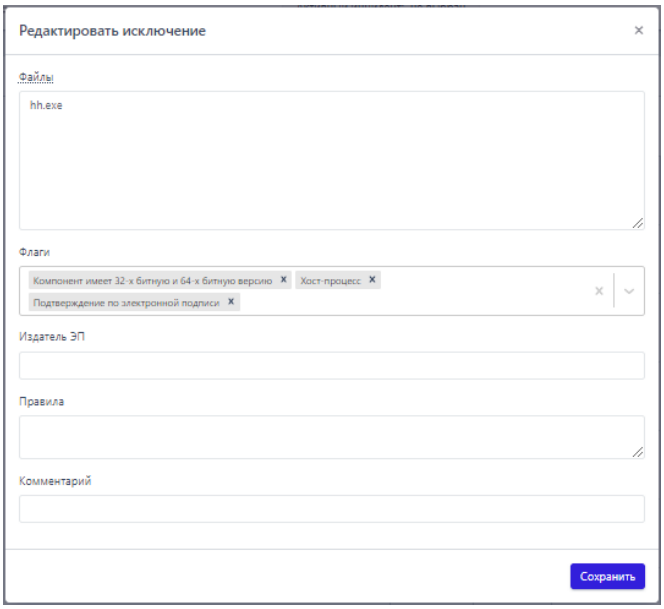


Рисунок 249 – Редактировать исключение для программы (тип «Файл»)

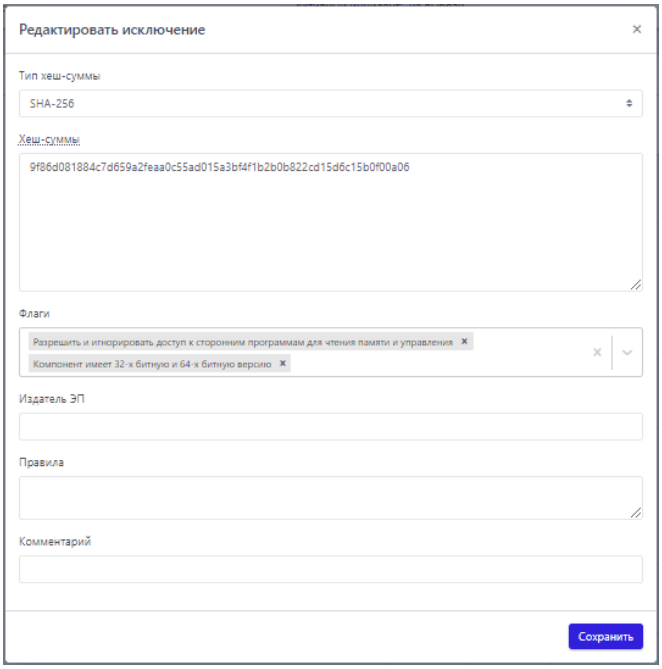


Рисунок 250 – Редактировать исключение для программы (тип «Хеш»)

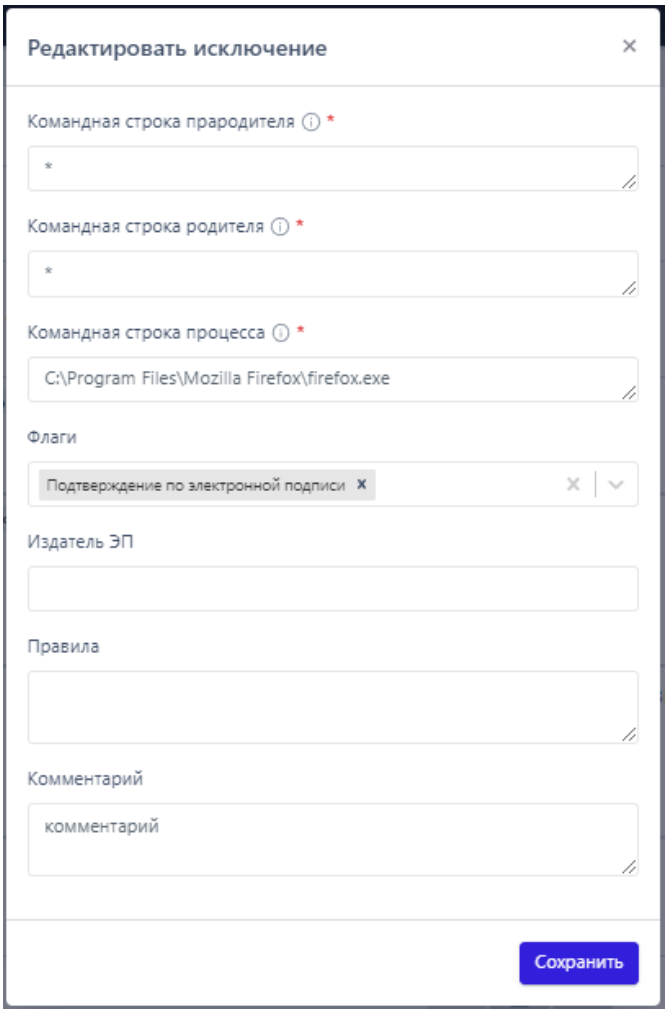


Рисунок 251 – Редактировать исключение для программы (тип «Командная строка»)

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. 252):

– таблица с наборами исключений для файлов;

– кнопка **Добавить набор**;

– кнопка **Применить набор**;

– кнопка **Удалить выбранные наборы**.

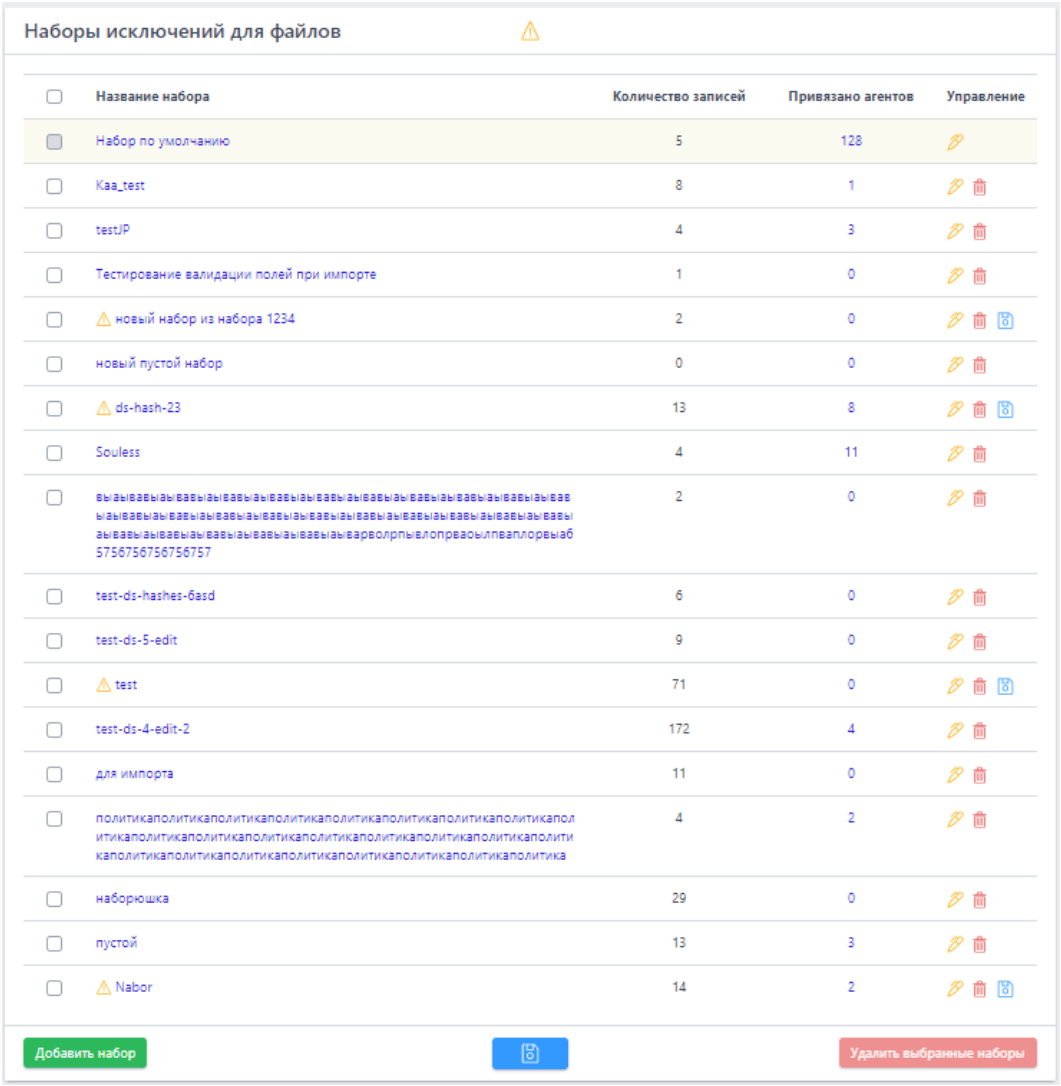


Рисунок 252 – Наборы исключений для файлов

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** (рис. 253) 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.

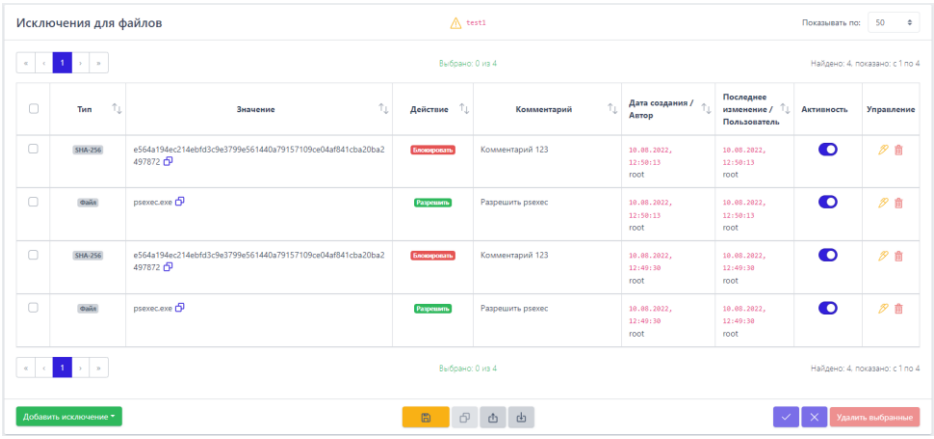


Рисунок 253 – Исключения для файлов

Для добавления исключения в выбранный набор необходимо нажать кнопку **Добавить исключение** и выбрать тип добавляемого исключения: **Файл** или **Хеш** (рис. 254).

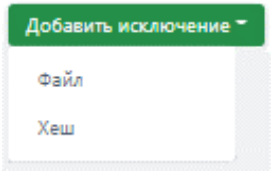


Рисунок 254 – Добавить исключение для файла (выбор типа)

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** (см. рис. 255).

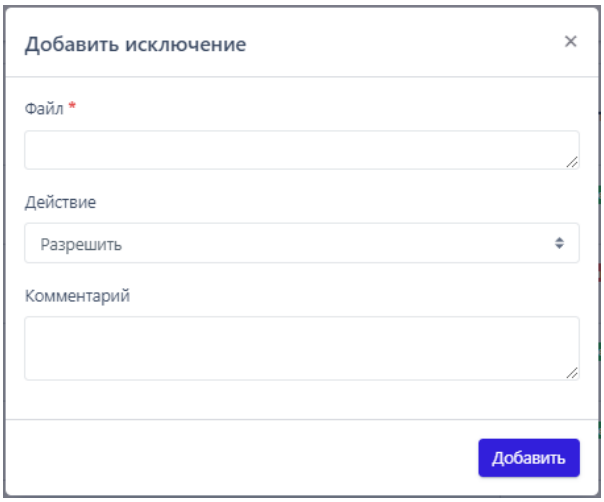


Рисунок 255 – Добавление исключения (тип «Файл»)

Для типа **Хеш** следует определить следующие параметры: **Тип хеш-суммы, Хеш-сумма, Действие** и **Комментарий** (рис. 256)

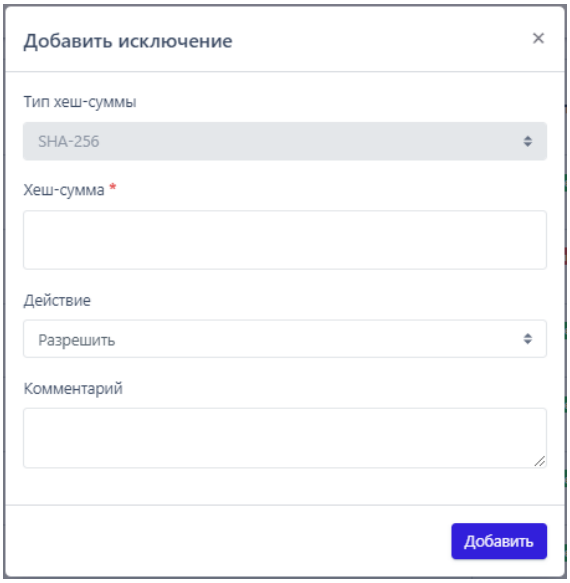


Рисунок 256 – Добавление исключения (тип «Хеш»)

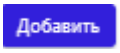
Файл – в поле прописывается имя файла, которого необходимо добавить в исключения. Имена файлов после добавления исключения будут отображаться в таблице **Исключения для файлов** в поле **Значение**, а в поле **Тип** прописывается тип исключения. Поле является обязательным для заполнения, на что указывает 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 

.

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 (рис. 257 и рис. 258) будет содержать разный набор полей, соответствующий окну **Добавить исключение** (см. рис. 255 и рис. 256).

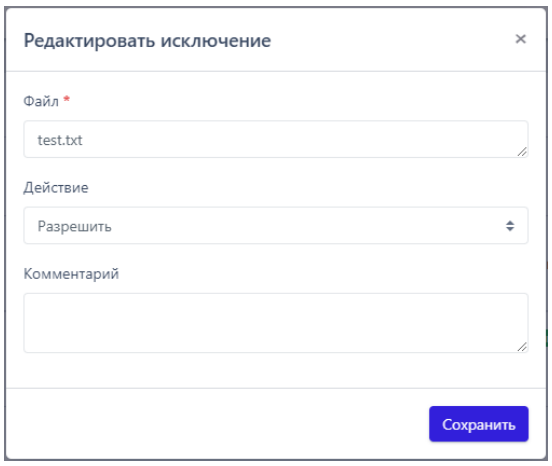


Рисунок 257 – Редактировать исключение (тип «Файл»)

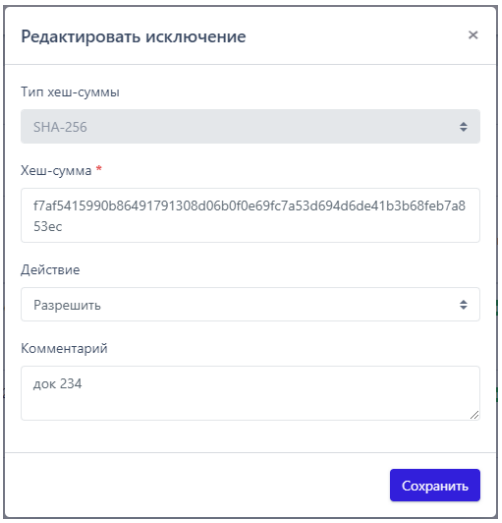


Рисунок 258 – Редактировать исключение (тип «Хеш-сумма»)

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 безопасности

В области **Профили безопасности** администратор программы может настраивать работу модуля защиты от программ-шифровальщиков и профиль безопасности 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 Anti-ransomware-модуля;

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).

Anti-ransomware-модуль включен на всех агентах по умолчанию, для этого каждому новому верифицированному агенту назначается набор настроек **Профиль по умолчанию** (рис. 259).

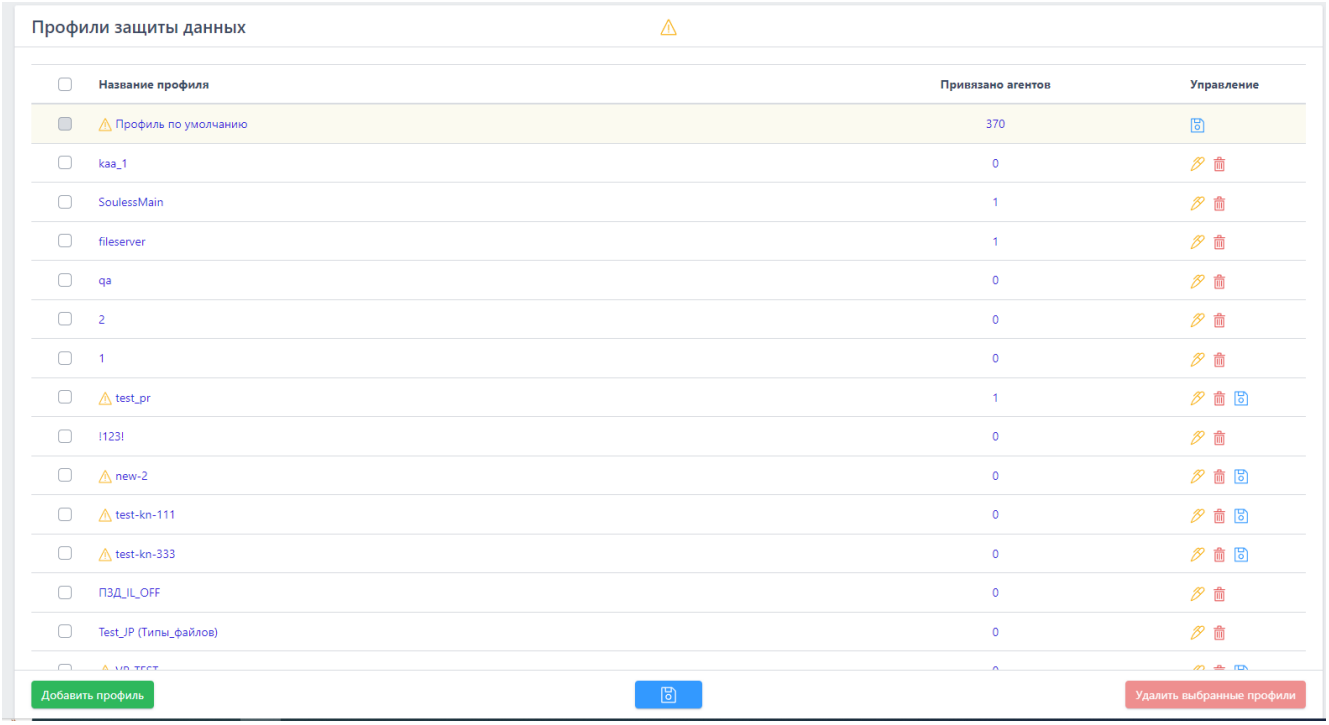


Рисунок 259 – Страница «Профили защиты данных»

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. 260).

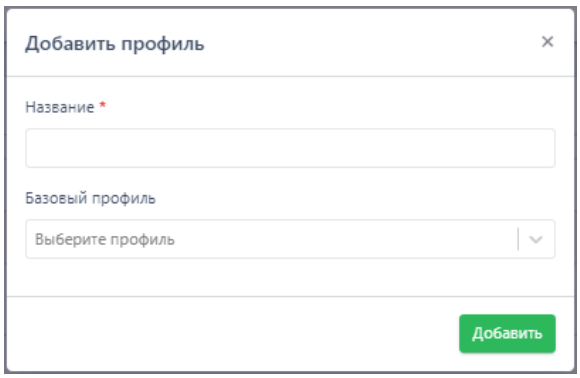


Рисунок 260 – Добавление профиля защиты

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. После завершения операции в нижней части страницы появится сообщение о добавлении нового профиля защиты данных (рис. 261).

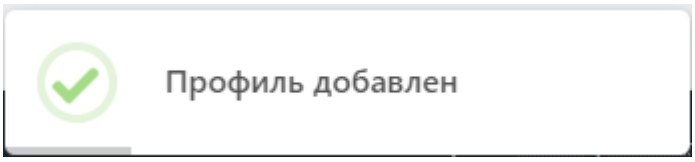


Рисунок 261 – Сообщение о добавлении профиля защиты данных

С помощью кнопки **Редактировать** ( ) можно изменить название профиля (рис. 262).

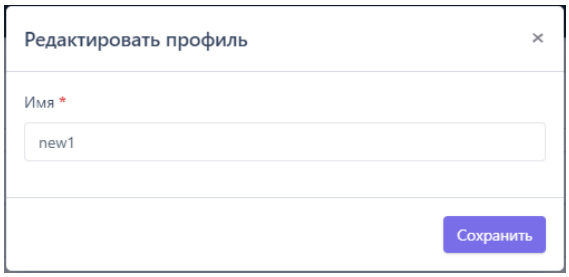


Рисунок 262 – Редактирование названия профиля защиты данных

После изменения профиля и сохранения настроек в нижней части страницы появится сообщение (рис. 263).

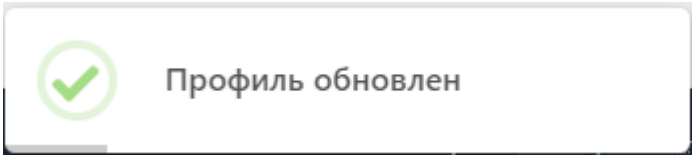


Рисунок 263 – Сообщение об успешном обновлении профиля защиты

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 (рис. 264).

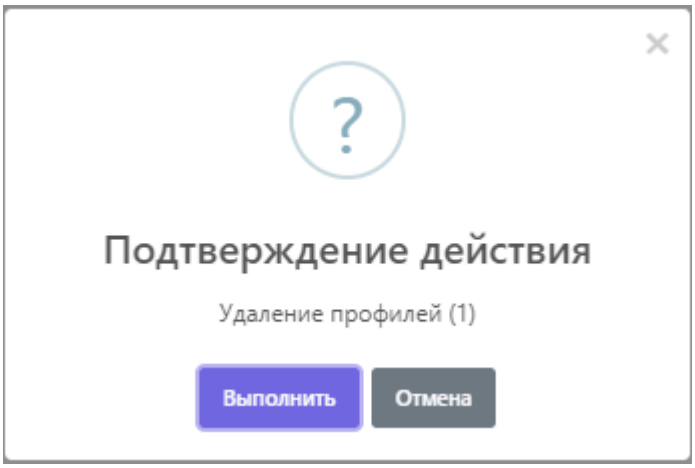


Рисунок 264 – Окно подтверждения удаления профилей защиты

После подтверждения операции в нижней части страницы появится сообщение об удалении профиля (рис. 265).

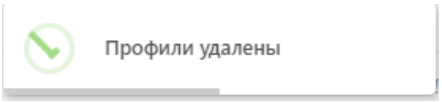


Рисунок 265 – Сообщение об удалении профиля защиты данных

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. 266):

1) Базовые настройки;

2) Настройки резервирования;

3) Список защищаемых каталогов.

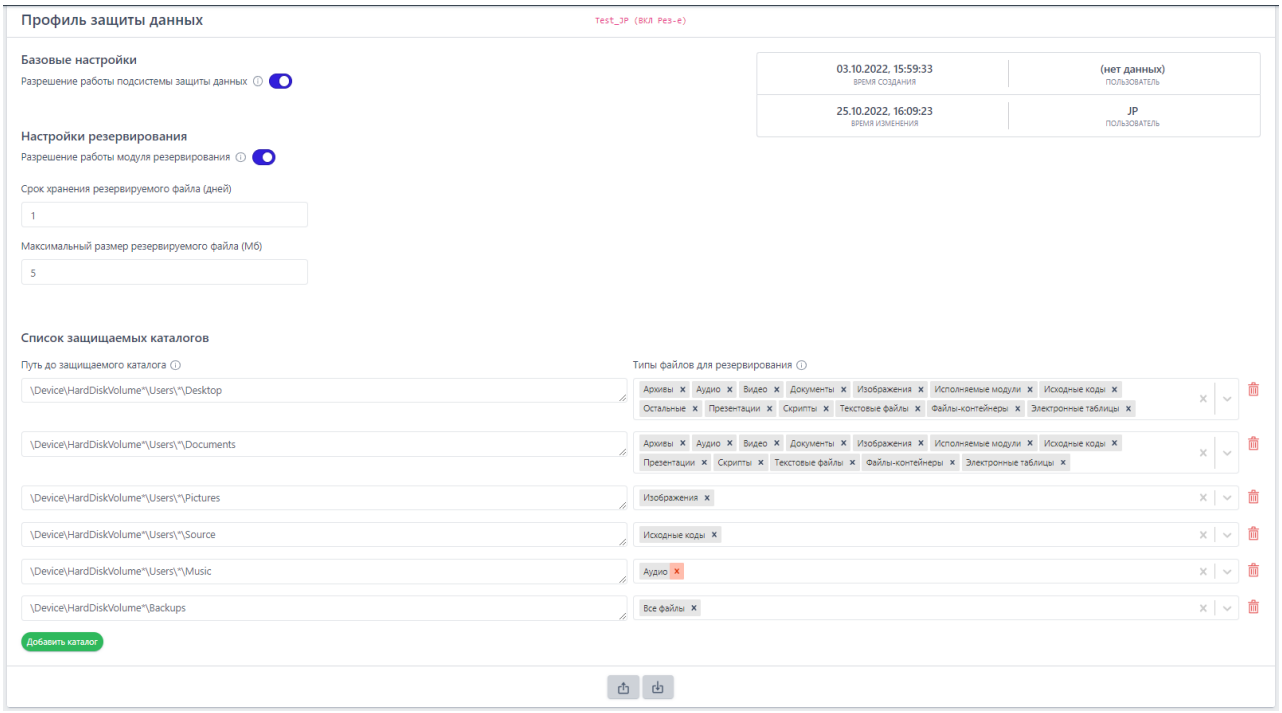


Рисунок 266 – Страница «Профиль защиты данных»

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 ⓘ.

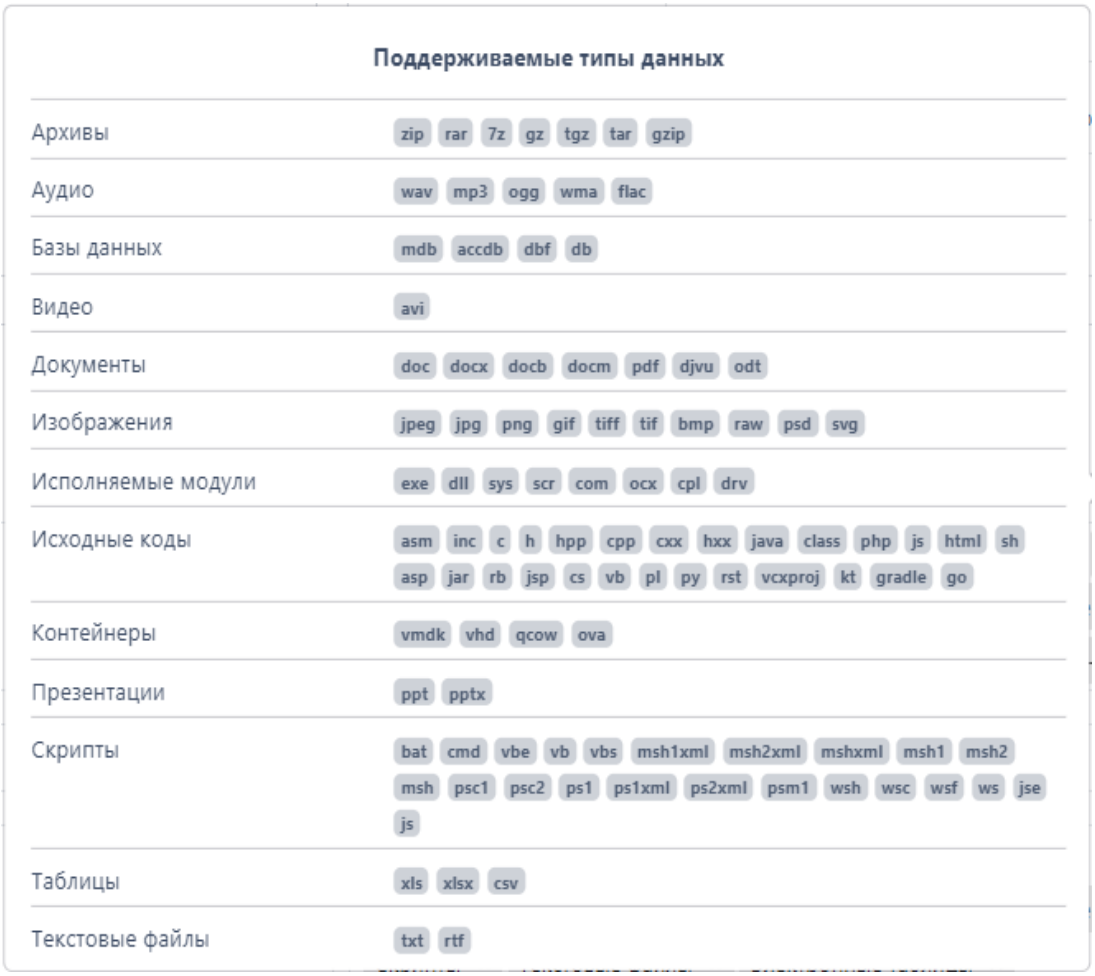


Рисунок 267 – Поддерживаемые типы данных

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 Добавить каталог, далее выбрать типы файлов, которые необходимо резервировать для указанного каталога и применить его ( ).

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.

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 (рис. 268).

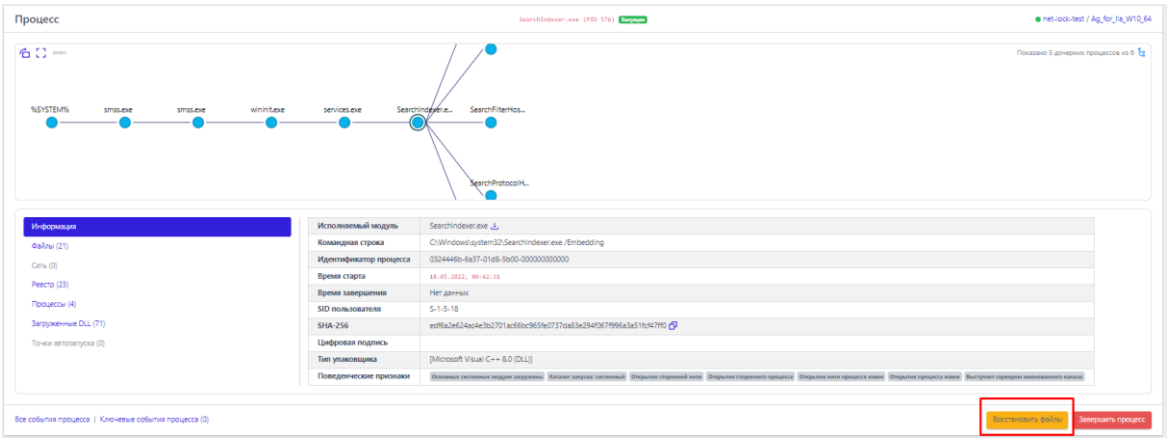


Рисунок 268 – Операция восстановления файлов на странице «Процесс»

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.

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. 269).

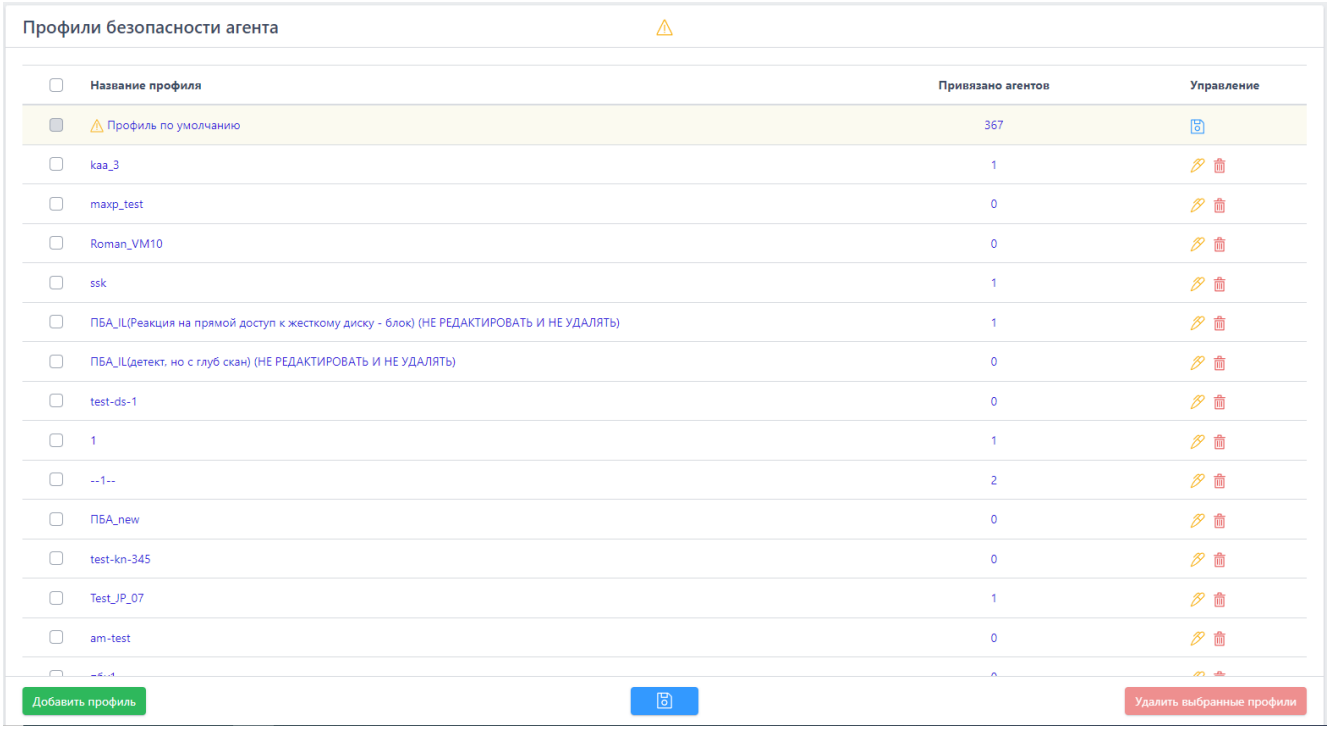


Рисунок 269 – Профили безопасности агента

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 (рис. 270). Такая предварительная настройка позволит управлять нагрузкой на систему.

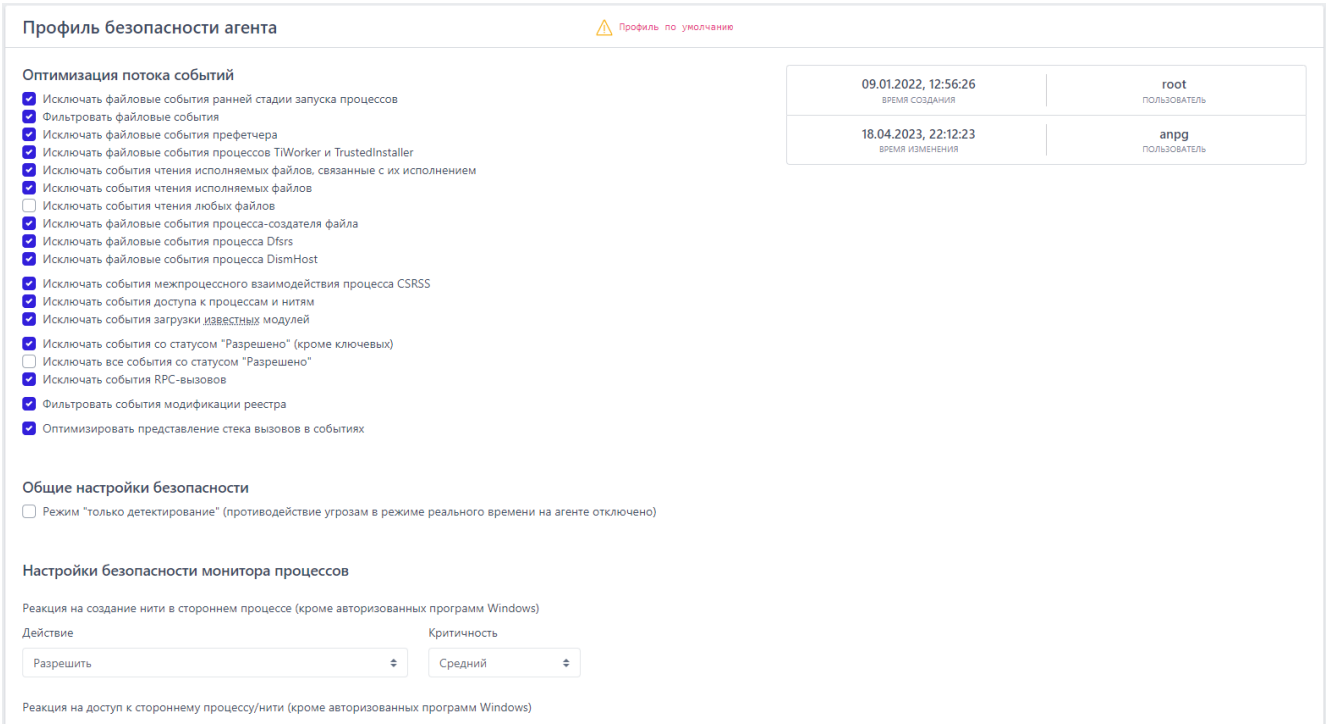


Рисунок 270 – Профиль безопасности агента

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 файловые события процессов TiWorker и TrustedInstaller;

5) Исключать события чтения исполняемых файлов, связанные с их исполнением;

6) Исключать события чтения исполняемых файлов;

7) Исключать события чтения любых файлов;

8) Исключать файловые события процесса-создателя файла;

9) Исключать файловые события процесса Dfsrs;

10) Исключать файловые события процесса Dismhost;

11) Исключать события межпроцессного взаимодействия процесса CSRSS;

12) Исключать события доступа к процессам и нитям;

13) Исключать события загрузки известных модулей (под известными модулями подразумеваются следующие динамически загружаемые библиотеки):

– ntdll.dll;
– kernel32dll;
– kernelbase.dll;
– sechost.dll;
– advapi32.dll;
– combase.dll;
– msvcrt.dll;
– gdi32.dll;
– user32.dll;
– ole32.dll;
– comdlg32.dll;
– comctl32.dll;
– shell32.dll;
– shlwapi.dll;
– oleaut32.dll;
– version.dll;
– imm32.dll;
– rpcrt4.dll;
– winmm.dll;
– ws2_32.dll;
– setupapi.dll;
– dwmapi.dll;
– winspool.drv;
– msctf.dll;
– uxtheme.dll;

– userenv.dll;

– msimg32.dll;

– usp10.dll;

– lpk.dll;

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

15) Исключать все события со статусом «Разрешено»;

16) Исключать события RPC-вызовов;

17) Фильтровать события модификации реестра;

18) Оптимизировать представление стека вызовов в событиях.

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.

В профиле безопасности агента 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.

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. Аналитик может выбрать для профиля безопасности одну из следующих реакций на события прямого доступа к жесткому диску:

– Блокировать;

– Блокировать запись;

– Блокировать запись только для неподписанных программ;

– Разрешить.

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 указанных выше настроек в программе предусмотрены настройки безопасности сетевого монитора и монитора реестра. Настройки безопасности сетевого монитора включаются и отключаются флагом **Оптимизировать поток сетевых событий,** а настройки монитора реестра флагом **Оптимизировать поток событий реестра.**

Важно

Оптимизация потока событий означает, что при появлении обнаружений, информация о них будет регистрироваться в программе только один раз за сессию.

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

Как правильно использовать профиль безопасности при развертывании агентов в защищаемой инфраструктуре?

Первоначально при установке агентов в защищаемой инфраструктуре необходимо использовать профиль безопасности агента **Профиль по умолчанию**. Особенность настройки этого профиля заключается в том, что в нем установлен режим «только детектирование». Работа с этим режимом позволяет наблюдать за происходящими в инфраструктуре событиями без блокирования работающих в системе процессов. На первоначальном этапе развертывания необходимо убедиться, что работа агентов не порождает значительного количества ложноположительных срабатываний и в целом инфраструктура работает без сбоев. В случае выявления ложноположительных срабатываний необходимо добавлять события в список исключений.

После этого первоначального этапа можно постепенно подключать агенты к работе в режиме противодействия угрозам в реальном времени, отключив режим «только детектирование». То есть необходимо использовать принципы так называемого канареечного развертывания, когда часть инфраструктуры некоторое время работает в режиме «только детектирование», а часть переходит в «боевой режим» с обнаружением и противодействием угрозам.

После включения режима противодействия угрозам в реальном времени можно также постепенно, используя стратегию канареечного развертывания, менять настройки безопасности монитора процессов и настройки безопасности файлового монитора в сторону усиления защитных функций EDR.

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. 271).

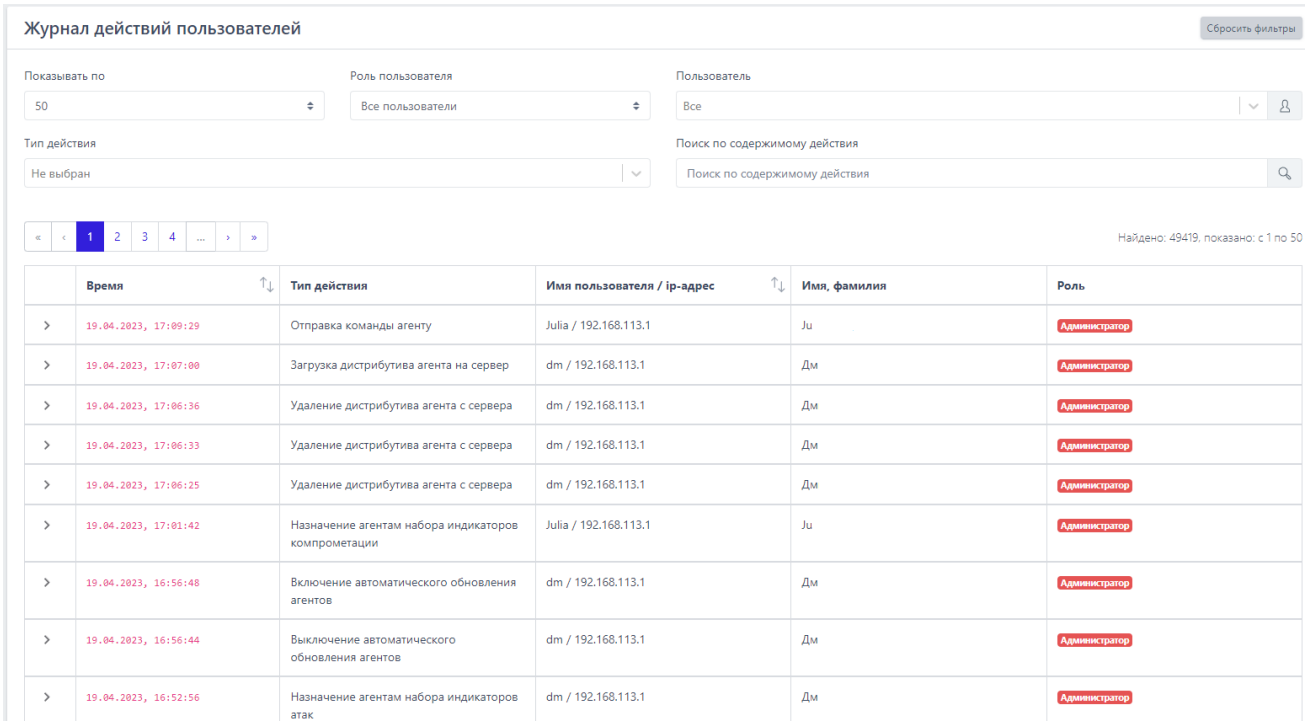


Рисунок 271 – Журнал действий

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;

20) Назначение агентам набора индикаторов атак;

21) Назначение агентам профиля защиты данных;

22) 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. 272):

1) Имя пользователя (логин);

2) Email;

3) Имя и фамилия, указанные при регистрации;

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

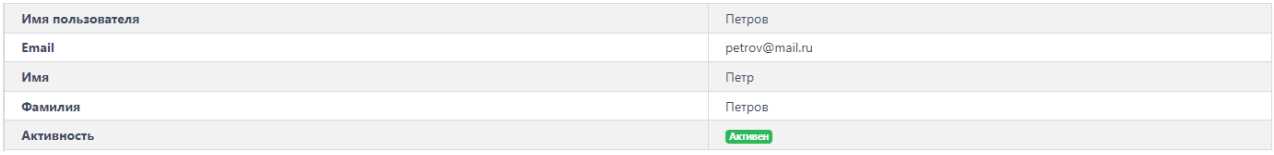


Рисунок 272 – Информация о пользователе, с которым совершались действия

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. 273).

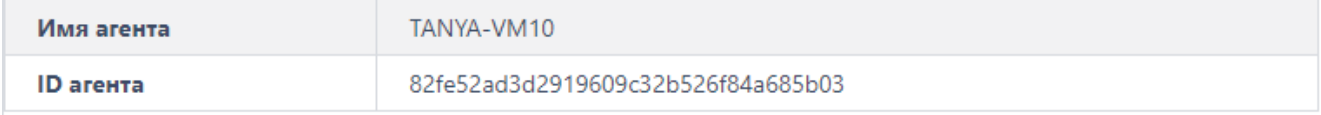


Рисунок 273 – Отмена верификации агента

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. 274).

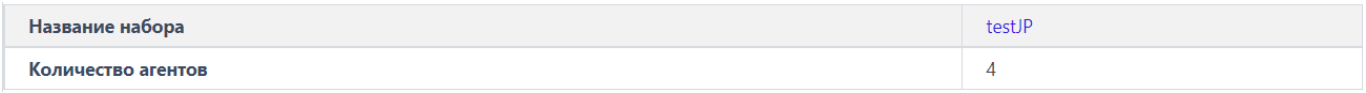
Имя агента	ID агента	Группа
agent_Win_7x64	f726152cd0a74a3e8d77eb4044a186ed01	юля-тест

Рисунок 274 – 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. 275).



Название набора	testJP
Количество агентов	4

Рисунок 275 – 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. 276).

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

Рисунок 276 – 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. 277).

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

Рисунок 277 – 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. 278).

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

Рисунок 278 – 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. 279). Для перехода к странице **Инцидент** следует кликнуть по имени инцидента, указанному в таблице.

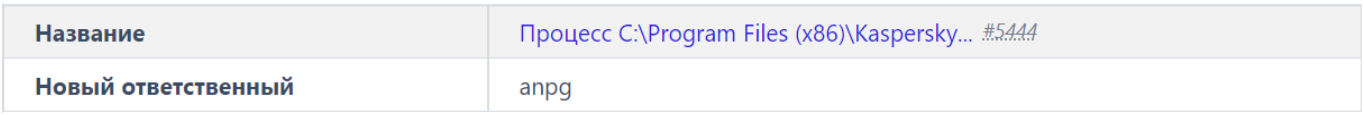


Рисунок 279 – Информация о новом ответственном за инцидент

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. 280). Для перехода к странице **Инцидент** необходимо кликнуть по имени инцидента, указанному в таблице.

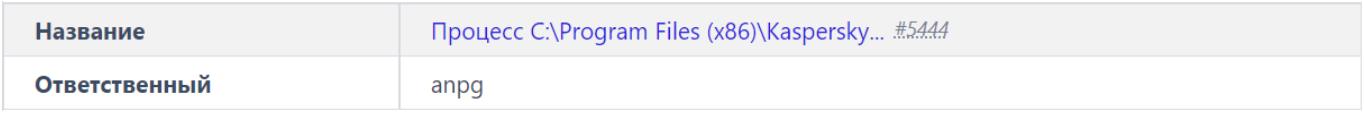


Рисунок 280 – Информация об ответственном за инцидент

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. 281):

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 загрузки и удаления дистрибутива /).

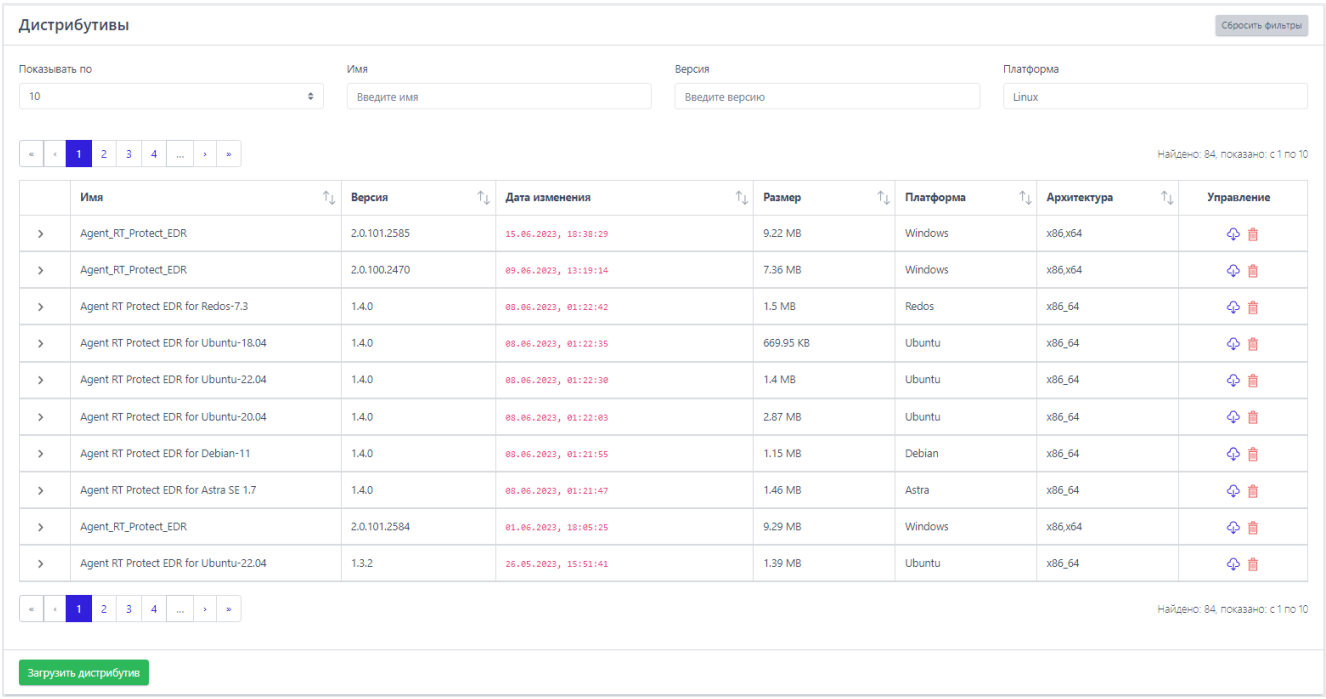


Рисунок 281 – Дистрибутивы

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).

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: Linux, Windows, Mac OS, Ubuntu).

При нажатии кнопки 

, 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. 282).

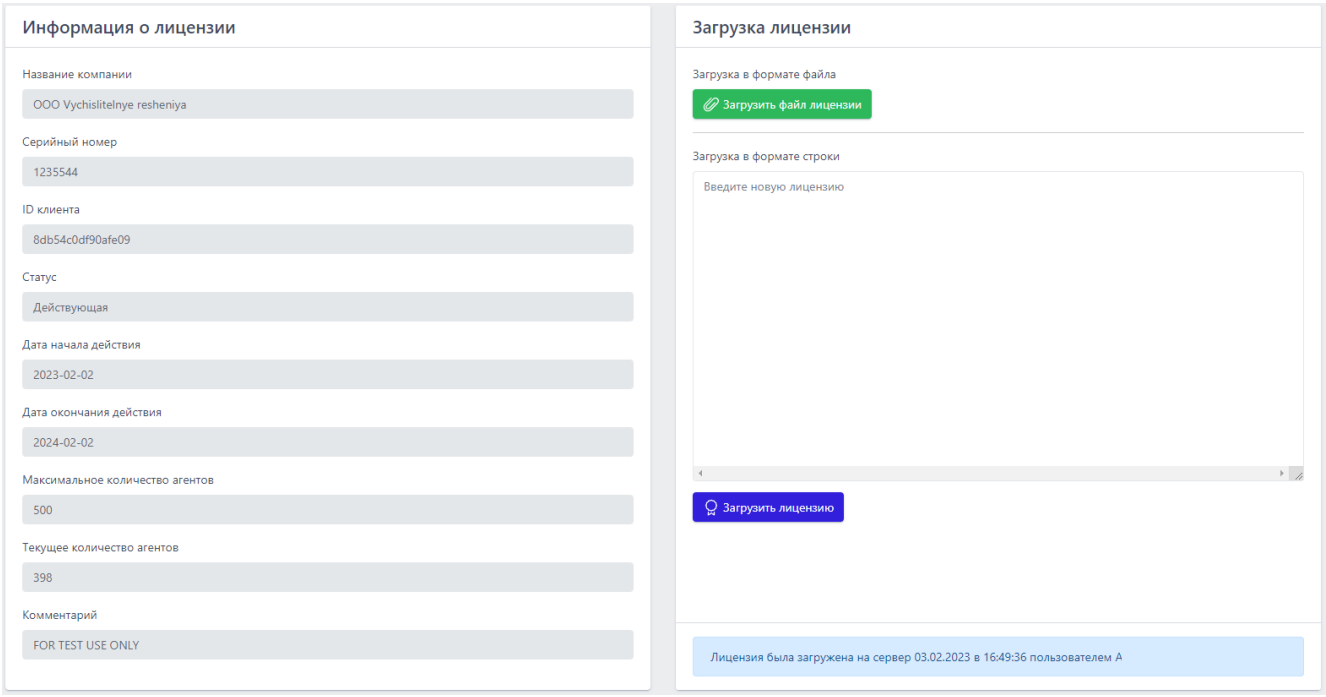


Рисунок 282 – Раздел «Лицензия»

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) Произвольный комментарий.

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. 283).

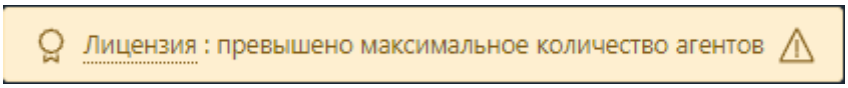
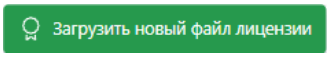
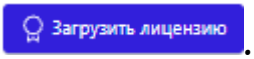


Рисунок 283 – Сообщение о превышении числа агентов

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.

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 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.

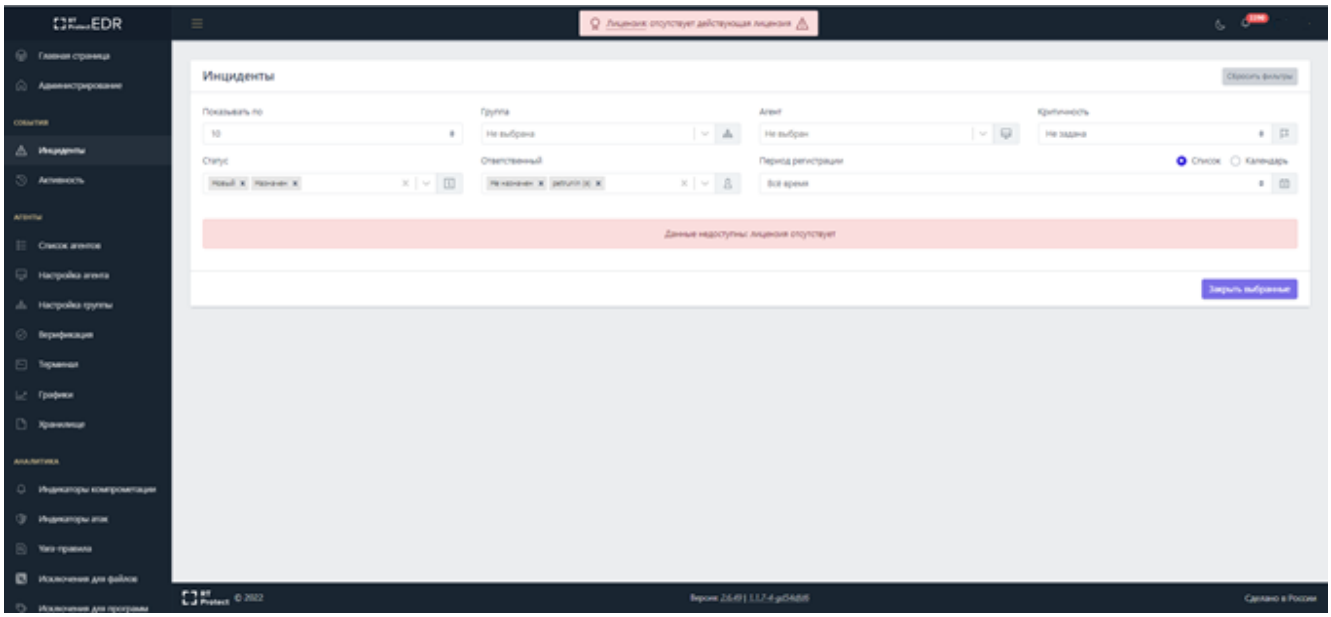


Рисунок 284 – Отсутствие действующей лицензии

Для корректной работы необходимо загрузить файл лицензии на сервер.

Действия при окончании лицензии на сервере

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 агент и с агента;

5) Отключается возможность добавлять пользователей и менять их имена.

7. Проверка программы

7.1 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**.

7.2 Контроль целостности исполняемых файлов и файлов конфигурации

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

8. Сообщения администратору

8.1 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.

8.2 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.

8.2.1. 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 285.

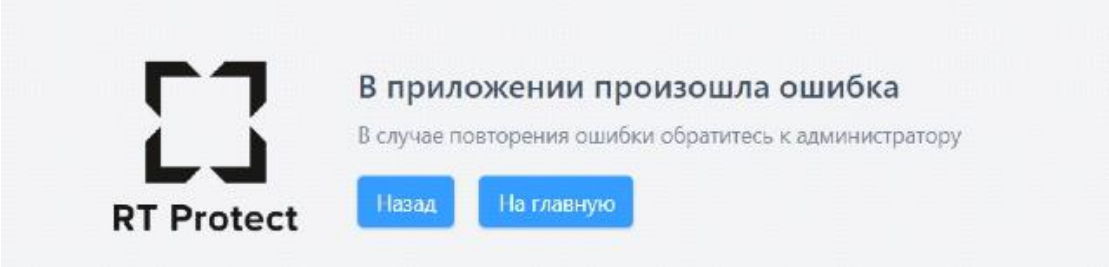


Рисунок 285 – Сообщение об ошибке типа «Экран ошибки»

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 286.

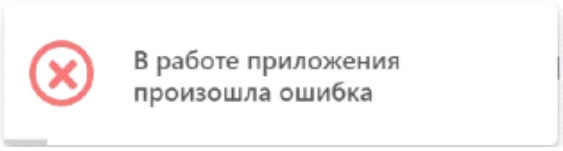


Рисунок 286 – Всплывающее сообщение об ошибке

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.

8.2.2. Специфичные сообщения

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

1) Ошибка при удалении пользователя (выводимое сообщение «Ошибка при удалении пользователя» представлено на рисунке 287).

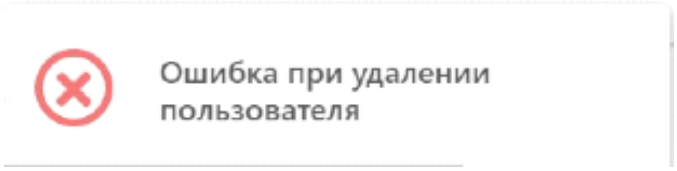


Рисунок 287 – Ошибка при удалении пользователя

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 288).

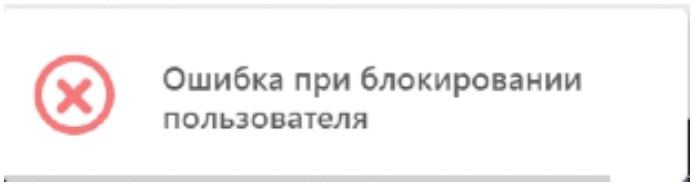


Рисунок 288 – Ошибка при блокировании пользователя

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 289).

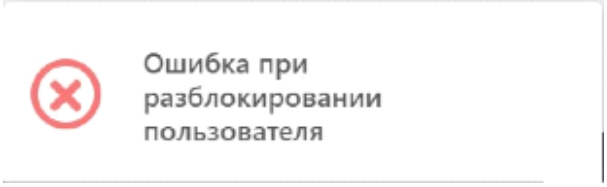


Рисунок 289 – Ошибка при разблокировании пользователя

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 290).

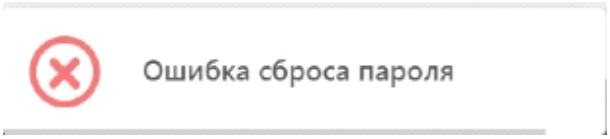


Рисунок 290 – Ошибка сброса пароля

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 291.

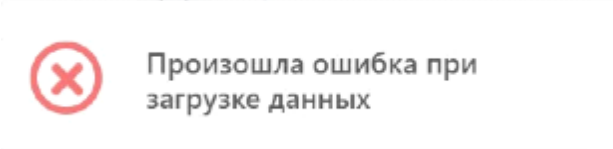


Рисунок 291 – Ошибка при загрузке данных

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 292.

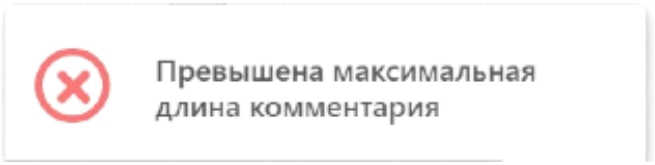


Рисунок 292 – Превышена максимальная длина комментария

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 293.

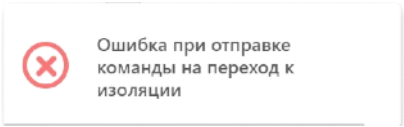


Рисунок 293 – Ошибка при отправке команды на переход к изоляции

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 294.

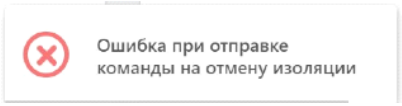


Рисунок 294 – Ошибка при отправке команды на отмену изоляции

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 295.

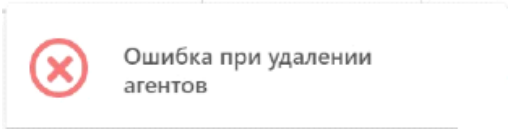


Рисунок 295 – Ошибка при удалении агентов

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 296.

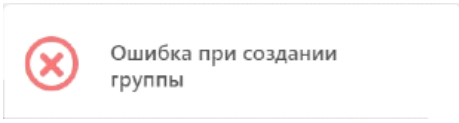


Рисунок 296 – Ошибка при создании группы

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 297.

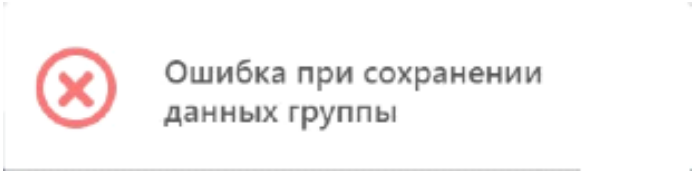


Рисунок 297 – Ошибка при сохранении данных группы

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 298.

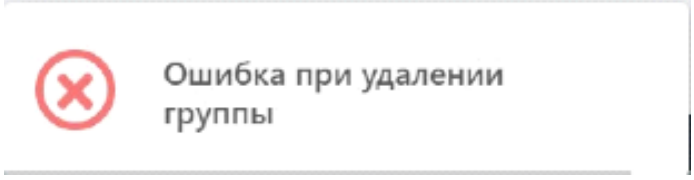


Рисунок 298 – Ошибка при удалении группы

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 299.

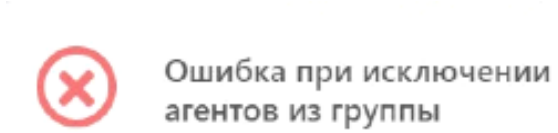


Рисунок 299 – Ошибка при исключении агентов из группы

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 300.

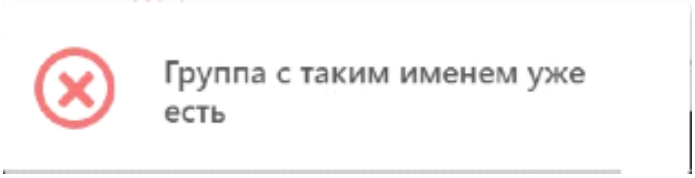


Рисунок 300 – Группа с таким именем уже есть

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 301.

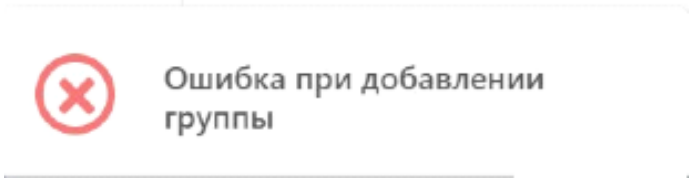


Рисунок 301 – Ошибка при добавлении группы

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 302.

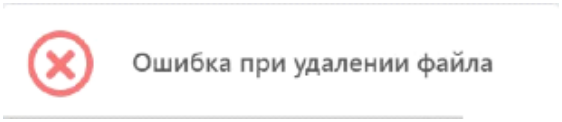


Рисунок 302 – Ошибка при удалении файла

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 303.

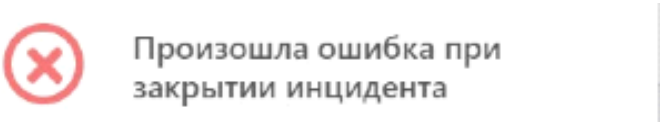


Рисунок 303 – Ошибка при закрытии инцидента

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 304.

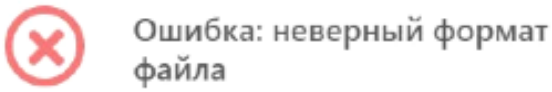


Рисунок 304 – Не верный формат файла

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 305.

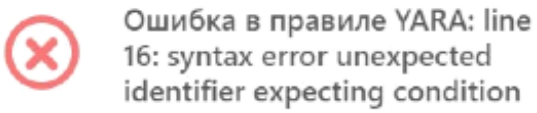


Рисунок 305 – Ошибка в правиле Yara

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 306.

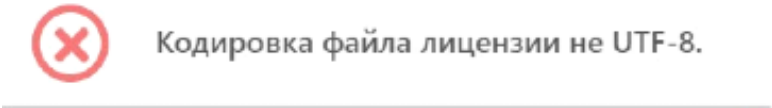


Рисунок 306 – Кодировка файла лицензии

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 307.

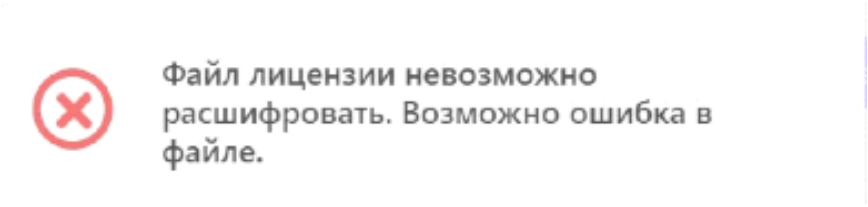


Рисунок 307 – Ошибка в файле лицензии

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 308.

Рисунок 308 – 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 309.

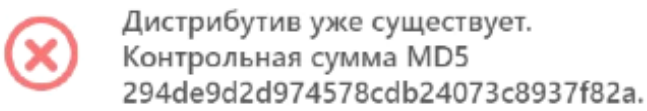


Рисунок 309 – Дистрибутив уже существует

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. 310).

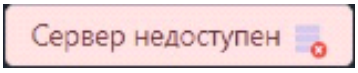


Рисунок 310 – Ошибка соединения с сервером

9. Действия после сбоя и ошибки

9.1 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 его из ранее сделанной резервной копии, либо восстановить программу с установочного носителя согласно рекомендациям настоящего руководства.

9.2 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».

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 22.

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 22 – 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**.

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.

10.5 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.

10.6 Контроль установки обновления

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

11. Перечень сокращений

Основные сокращения, указанные в документе, представлены в таблице 23.

Таблица 23 – 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
ФБО	Функции безопасности объекта оценки
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)
CSRSS	Client/Server Runtime Subsystem (подсистема клиент/сервер времени выполнения)
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)