

Веб-сервис RT Protect TI

Руководство администратора

Версия 1.0.35 от 19 июня 2026

Разработано компанией АО «РТ-Информационная безопасность»



1. Общие положения	5
1.1 Идентификация документа	5
1.2 Аннотация документа	5
1.3 Термины и определения	5
1.4 Условные обозначения	7
2. Общие сведения	8
2.1 Назначение и архитектура программы	8
3. Организационно-распорядительные меры	9
3.1 Общие сведения	9
3.2 Комплектность поставки	9
3.2.1. Процедуры и меры безопасности при распространении программы к месту назначения	9
4. Структура программы	10
5. Настройка программы	11
5.1 Требования к среде функционирования	11
5.2 Роли	11
6. Интерфейс программы	13
6.1 Окно авторизации и общие сведения	13
6.2 Горизонтальная панель управления	15
6.2.1. Меню «Пользователь»	17
6.3 Главная страница	20
6.4 Администрирование	21
6.4.1. Пользователи	21
6.4.2. Организация	28
6.4.3. Тэги	31
6.5 Аналитика	34
6.5.1. Активность	35

6.5.2. Заявки.....	41
6.5.3. Анализаторы	43
6.5.4. Граф связей	45
6.5.5. Распространяемая аналитика.....	46
6.5.6. Угрозы и злоумышленники	54
6.5.7. Вредоносное ПО	55
6.5.8. Инструменты	56
6.5.9. Матрица MITRE ATT&CK	57
6.5.10. Лента угроз.....	58
6.6 Аналитика EDR	59
6.6.1. Индикаторы атак	60
6.6.2. Индикаторы компрометации	67
6.6.3. Журналы.....	72
6.6.4. Yara-правила (файлы)	75
6.6.5. Yara-правила (память).....	79
6.7 Исключения EDR.....	82
6.7.1. Исключения для программ	82
6.7.2. Исключения для файлов.....	89
6.7.3. Сетевые исключения.....	95
6.7.4. Исключения индикаторов атак.....	99
6.8 Уязвимости	103
6.8.1. Общие сведения	103
6.8.2. Уязвимости	103
6.8.3. Программы	106
6.9 Параметры	111
6.9.1. Журнал действий	111
7. Сообщения администратору	114
7.1 Общие сведения	114

7.2 Сообщения об ошибках	114
7.2.1. Общие сообщения.....	114
7.2.2. Специфичные сообщения	116
8. Действия после сбоя и ошибки.....	119
8.1 Общие сведения	119
9. Перечень сокращений	120
10. Заключение	121

1. Общие положения

1.1 Идентификация документа

Данное руководство кратко можно идентифицировать согласно таблице 1.

Таблица 1 – Идентификация документа

Название документа	«Веб-сервис RT Protect TI» Руководство Администратора
Версия документа	Версия 1.0.35 (актуальна для версии продукта 3.4.0)
Идентификация программы	Сервис по предоставлению аналитики «RT Protect TI»
Идентификация разработчика	АО «РТ-Информационная безопасность»

1.2 Аннотация документа

Документ предназначен для ознакомления администраторам сервиса по предоставлению аналитики с технической информацией о программе «RT Protect TI» (далее по тексту программа).

Документ предназначен для пользователей сервиса в рамках организации, не являющейся владельцем TI-платформы, 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
Артефакты	Различные типы данных имеющие подозрительное содержимое и загружаемые на сервер для анализа (файлы, доменные имена, IP-адреса, URL)
Backend	Программно-аппаратная часть сервиса, отвечающая за функционирование его внутренней части
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
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
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
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-поток 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

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
 Примечание	Информация, требующая внимания пользователя
 Важно	Информация, связанная с важными конфигурационными настройками и особенностями работы RT Protect TI

2. Общие сведения

2.1 Назначение и архитектура программы

RT Protect TI – это программное решение, которое позволяет собирать, обрабатывать, накапливать и распространять данные о киберугрозах (Threat Intelligence), то есть выполняет функции TI-платформы. Решение предоставляет аналитикам информационной безопасности возможность работать с актуальными сведениями об угрозах для эффективных расследований инцидентов и упреждения вредоносной активности.

Модуль управления сервисом сбора TI-данных, находящийся на сервере, предназначен для следующих задач:

- администрирование пользователей организации, взаимодействующих с сервисом;
- выпуск токенов для клиентов;
- просмотр статистической информации по обнаружениям в графическом виде;
- получение вердикта по анализируемым артефактам;
- регистрация действий пользователей организации;
- просмотр информации о программах и уязвимостях, зарегистрированных для данных программ.

Программа функционирует под управлением ОС Linux Ubuntu 20.04.5 LTS.

Для распространения сервиса применяется модель on-cloud (установка и развертывание сервиса осуществляется на мощностях предприятия-разработчика сервиса уполномоченными сотрудниками, доступ к сервису как услуга).

Программа предназначена для обработки информации, не являющейся секретной.

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

Пользователь – может загружать для анализа на сервисе различные артефакты, просматривать отчеты по проверке артефактов, просматривать графики проверки артефактов с распределением по времени.

Администратор – выполняет установку и корректную настройку программы в соответствии с настоящим руководством, регистрирует новых пользователей, подключенных к сервису, и осуществляет другие функции, описанные в данном руководстве;

Аналитик – пользователь, ответственный за анализ поступающих от программы данных.

3. Организационно-распорядительные меры

3.1 Общие сведения

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

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

Программа поставляется заказчику согласно комплектности поставки.

3.2 Комплектность поставки

Комплектность поставки представлена в таблице 4.

Таблица 4 – Комплектность поставки

Обозначение	Наименование	Кол.	Примечание
	Предоставление доступа к Веб-сервису «RT Protect TI»	1	
	Комплект документов согласно списку: — «Веб-сервис RT Protect TI» Руководство Администратора; — «Веб-сервис RT Protect TI» «Руководство Аналитика; — «Веб-сервис RT Protect TI» «Руководство Пользователя .	1	

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

Архитектуру и взаимодействие компонентов сервиса можно представить согласно схеме, описанной на рисунке 1.

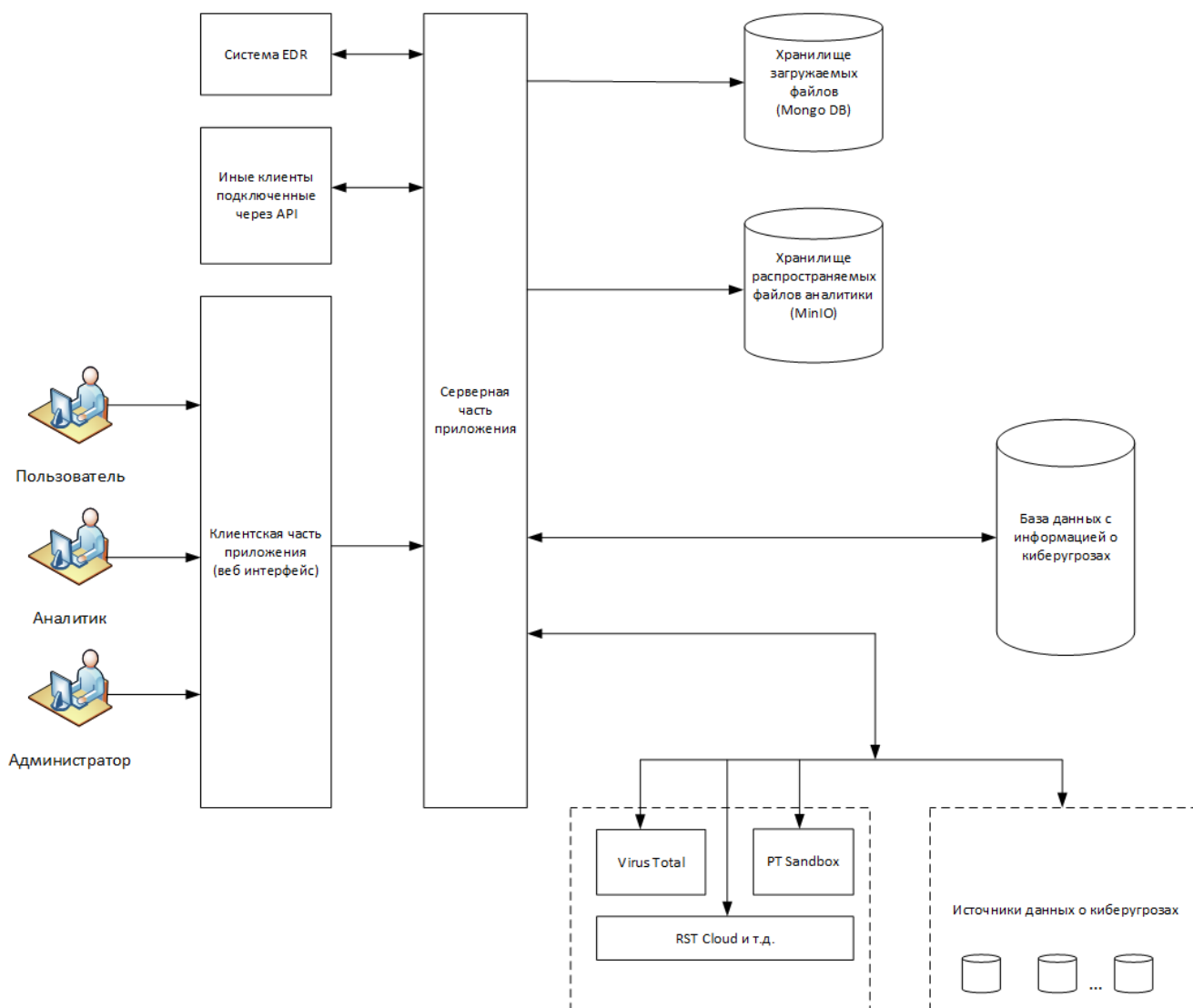


Рисунок 1 – Схема архитектуры сервиса

5. Настройка программы

5.1 Требования к среде функционирования

Программа 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 поддерживает работу в браузерах, представленных в таблице 5.

Таблица 5 – 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 Роли

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

- пользователь.
- аналитик;
- администратор.

Пользователь – сотрудник отдела ИБ или SOC-центра.

Сотруднику, осуществившему вход в модуль администрирования программы с ролью «Пользователь» доступны следующие страницы:

- Главная страница;
- Организация;
- Активность;
- Отчеты;
- Граф связей.

Сотруднику с ролью «Пользователь» доступны следующие действия:

1) добавление для проверки артефактов в поле для проверки данных согласно списку:

- IP-адрес;
- доменное имя;
- URL;
- контрольную сумму файла (хеш-суммы).

2) загрузка файла для проверки на сервисе с компьютера, с которого был произведен вход в модуль администрирования программы;

3) просмотр страницы отчета по проверенному артефакту.

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.

В круг типовых задач аналитика входят:

- проверка артефактов;
- анализ активности;
- просмотр отчетов об артефактах.

Администратор – уполномоченный сотрудник организации заказчика или SOC-центра. У администратора в наличии те же возможности, что и у аналитика, при добавлении возможностей управления пользователями и просмотра журналов действий пользователей.

6. Интерфейс программы

6.1 Окно авторизации и общие сведения

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. 2).

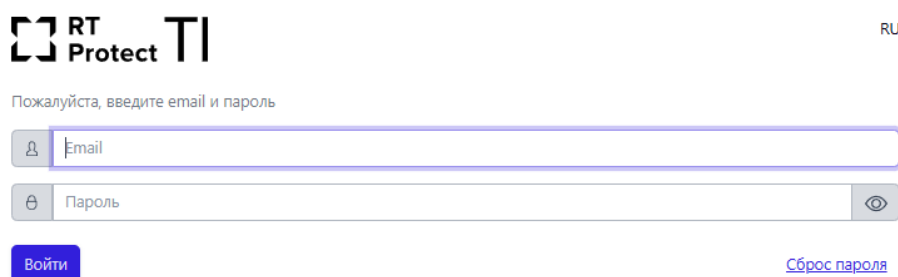


Рисунок 2 – Окно авторизации

В данном окне кроме данных по авторизации можно изменить язык локализации нажав по иконке **RU** (возможно выбрать Русский/Английский).

При нажатии по иконке Сброс пароля, откроется окно, в котором потребуется ввести действующую почту, на которую будет отправлена ссылка для сброса пароля. После перехода по данной ссылке открывается окно для сброса пароля представленное на рисунке 3.

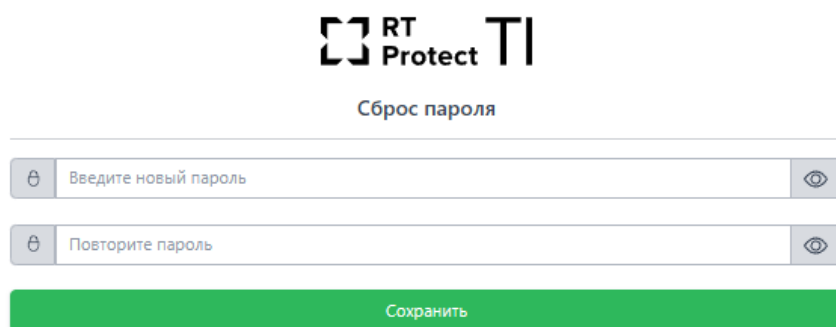


Рисунок 3 – Окно ввода параметром для сброса пароля

После ввода нового пароля потребуется вновь авторизоваться, введя в окне авторизации имеющийся логин (email) и новый пароль.

После ввода в окне авторизации пароля и логина администратора открывается основное окно программы (рис. 4).

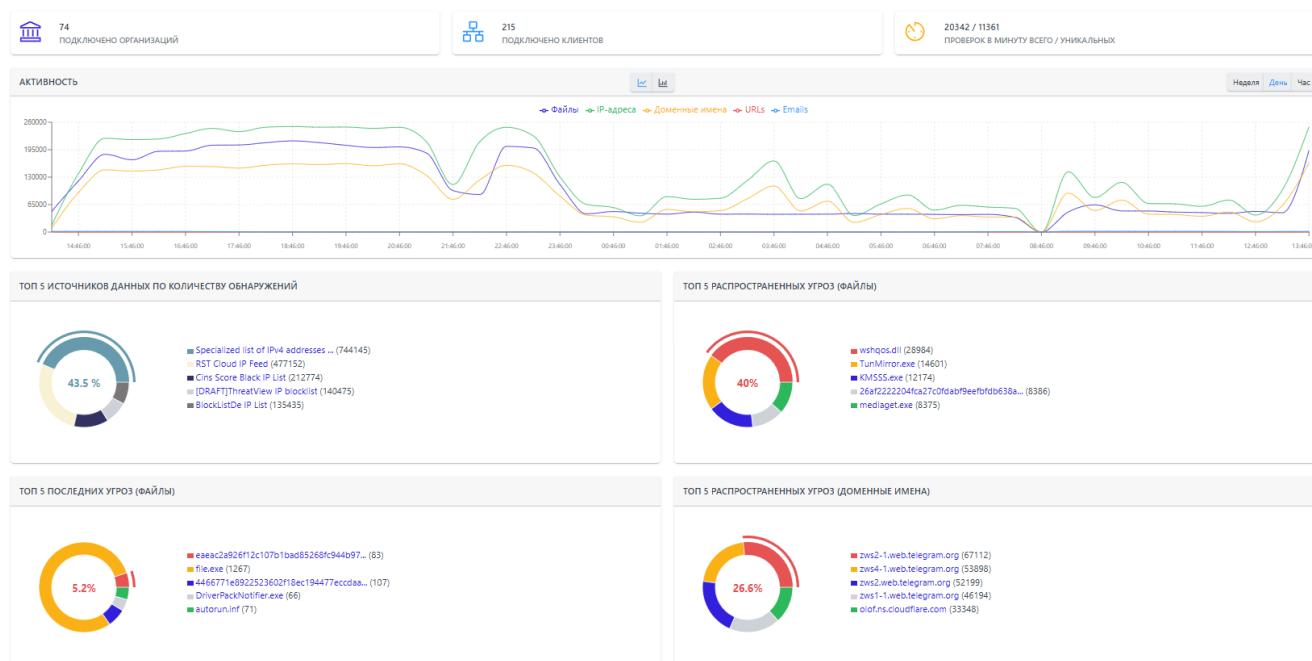


Рисунок 4 – Основное окно программы

Если в течение 5 минут пользователь выполнил 5 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:

- анализ загруженных артефактов (IP-адресов, файлов, доменных имен, URL);
- просмотр тегов;
- администрирование пользователей, взаимодействующих с сервисом;
- выпуск токенов для подключения программ (например, EDR);



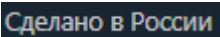
Важно

Клиенты с помощью токена получают доступ к API платформы TI.

- просмотр и анализ обнаружений на странице **Активность**;

- просмотр отчетов по анализу проверенных артефактов;
- просмотр действий пользователей, произведенных в модуле администрирования программы;
- просмотр уязвимостей и программ с найденными уязвимостями;
- просмотр журнала действий пользователей;

В левой части основного окна программы находится вертикальная панель управления, доступная администратору. С помощью панели управления пользователь может переходить по разделам программы для изменения настроек и просмотра информации по разделам. При выборе определенного раздела в правой части окна будет представлена информация выбранного раздела и основной инструментарий для работы пользователя программы.

В нижней части страницы находится информация о товарном знаке компании — . Справа от текущей версии программы отображается надпись о том, где «RT Protect TI» разработана — .

6.2 Горизонтальная панель управления

В верхней части окна находится горизонтальная панель управления (рис. 5).

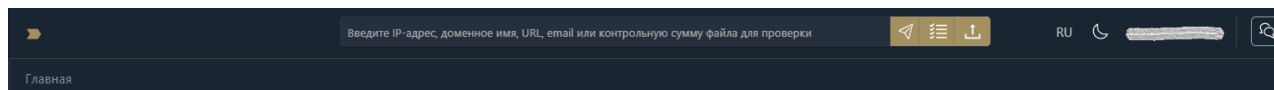
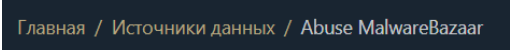


Рисунок 5 – Горизонтальная панель управления

При нажатии по иконке  в нижней части горизонтальной панели отображается, на какой странице с уровнем вложенности находится пользователь, например, .

При наведении указателя мыши на каждый уровень и нажатии по нему ЛКМ можно перейти на страницу с данным указателем.

При нажатии по иконке  все страницы будут представлены в темной теме. Для возврата светлой темы необходимо повторно нажать на иконку.

При нажатии ЛКМ по иконке  появляется область, представленная на рисунке 6.

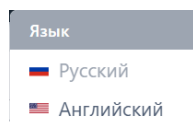


Рисунок 6 – Выбор языка

В данной области можно выбрать язык, на котором будет отображаться информация на всех страницах модуля администрирования.



При нажатии по иконке , открывается область чата, где пользователи могут оставлять сообщения и комментарии, отвечать на сообщения, оставленные другими пользователями, а также редактировать и удалять собственные комментарии.

В области представленной на рисунке 7 можно отправить артефакт, либо список артефактов на проверку.



Рисунок 7 – Область быстрой отправки артефактов на проверку

В области **Проверка артефактов** администратор может получить вердикт для IP-адреса, домена, EMAIL, URL-адреса или хеш-суммы. Для этого необходимо ввести данные соответствующего артефакта в строку и нажать по иконке **Отправить** ().

Откроется отчет TI-платформы (подробнее см. в пункте 6.5.1).

В области **Проверка артефактов** администратор также может проверить целый список артефактов, нажав по иконке , после чего откроется окно для загрузки списка артефактов, представленное на рисунке 8.

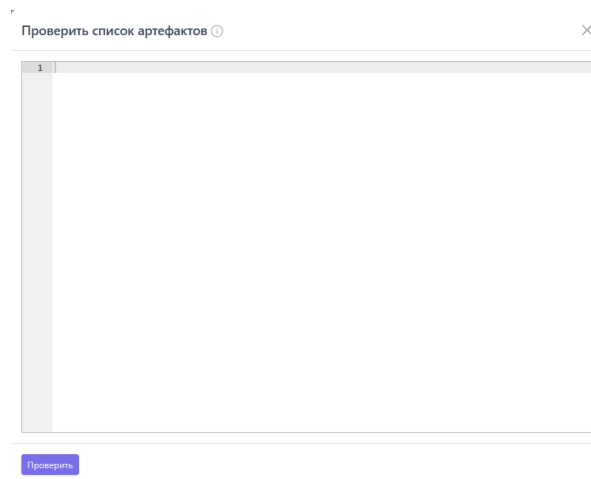


Рисунок 8 – Окно для добавления списка артефактов для проверки

В данном окне артефакт добавляется по одному в каждой строчке (строчки нумеруются). Проверка артефактов списком ограничена количеством в 1000 строк. После написания артефактов требуется нажать по иконке «Проверить».

Проверенный артефакт будет отображаться на странице **Активность** с вердиктом от TI-платформы (если артефакт уже присутствовал в базе). Можно создать заключение аналитика для одного или нескольких артефактов (создание заключения для группы артефактов).

Также в области проверки артефактов с помощью кнопки **Загрузить файл** () можно проверить файлы на компьютере, с которого осуществлен доступ к TI-серверу. После нажатия кнопки  откроется проводник, в котором можно выбрать файл, нуждающийся в проверке. Далее файл загружается на TI-платформу, а после завершения его загрузки выводится отчет с вердиктом.

6.2.1. 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 пользователя**, иконка для загрузки документации и кнопка **Выход** для выхода из программы с текущего устройства (рис. 9).

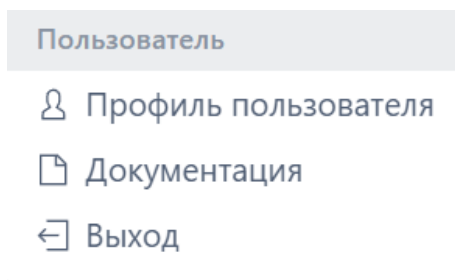


Рисунок 9 – Меню «Пользователь»

При нажатии по иконке **Документация** будет загружено руководство в формате pdf согласно роли, под которой был осуществлен вход, при этом руководства будут отличаться для ролей пользователей с выставленным признаком владельца и не владельца платформы.

Подменю **Профиль пользователя** представлено на рисунке 10.

Рисунок 10 – Подменю «Профиль пользователя»

В данном окне информация о профиле пользователя представлена в виде следующих полей:

- адрес электронной почты для своей учетной записи;
- роль, назначенная пользователю администратором (Администратор, Пользователь, Аналитик);
- имя и фамилия пользователя;
- организация (информация об организации, в которой работает пользователь);
- поле с описанием профиля пользователя.

Изменять пароль возможно с помощью кнопки **Сменить пароль**. При нажатии кнопки **Сменить пароль** открывается окно для смены пароля (рис. 11).

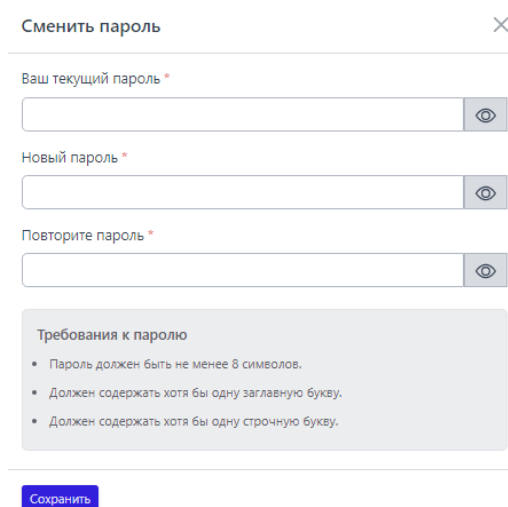


Рисунок 11 – Окно смены пароля

Введенный пароль должен соответствовать требованиям, указанным в нижней части окна. Для смены пароля необходимо ввести старый и новый пароль с подтверждением в соответствующие поля и нажать кнопку

Сохранить.

При нажатии по иконке  /  имеется возможность показать/скрыть пароль.

6.3 Главная страница

На рисунке 12 представлен раздел **Главная страница** модуля управления.

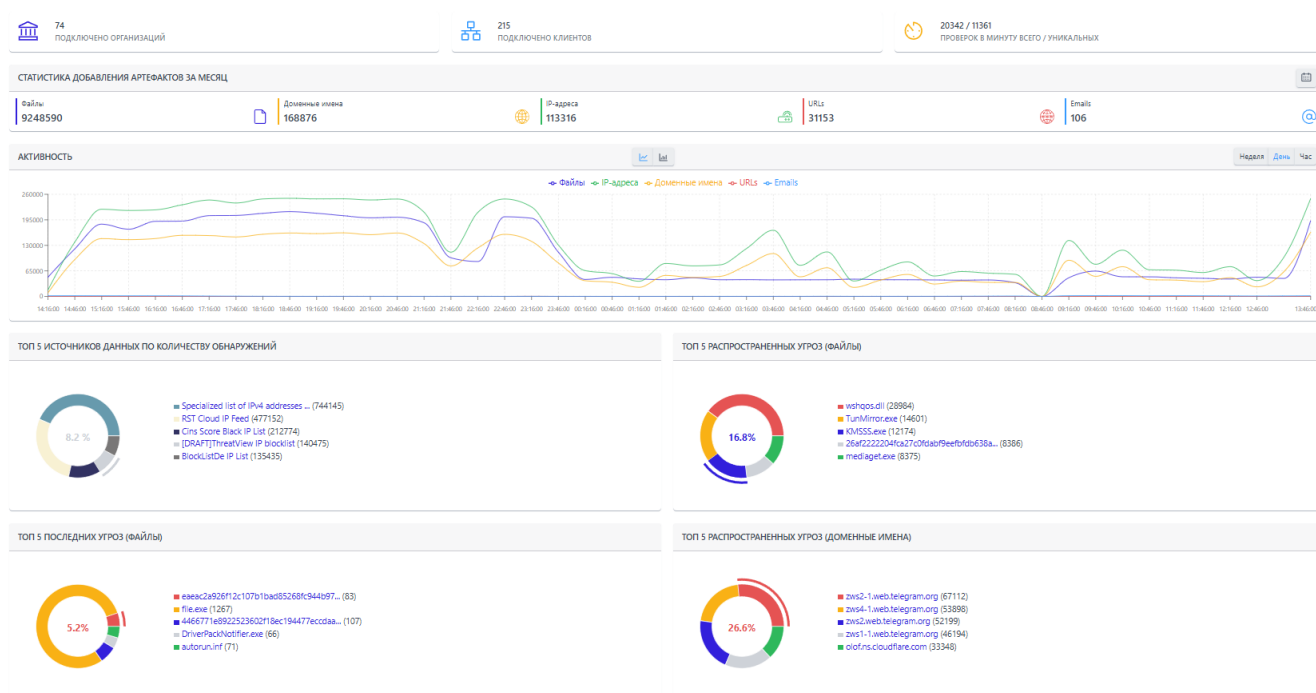


Рисунок 12 – Главная страница

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

- статистика добавления артефактов за месяц;
- графическое представление активности (отображение обнаружений);
- графические отображения Топ 5 распространенных угроз по различным типам артефактов (файлы, доменные имена, ip-адреса);
- графические отображения Топ 5 последних угроз по различным типам артефактов (файлы, доменные имена, ip-адреса);
- графические отображения количества добавленных для анализа различных артефактов по типам (IP-адреса, контрольные суммы, доменные имена, файлы).

6.4 Администрирование

В области **Администрирование** основной панели программы находятся следующие разделы:

- Пользователи;
- Организация;
- Теги.

Администратор может выполнять следующие действия:

- просматривать информацию о пользователях;
- создавать и удалять учетные записи пользователей;
- изменять параметры учетных записей пользователей;
- просматривать теги и псевдонимы для ранжирования элементов активности.

6.4.1. Пользователи

В разделе **Пользователи** в табличном виде показана информация о зарегистрированных в программе пользователях принадлежащих данной организации (рисунок 13).

Email	Имя	Фамилия	Роль	Время создания	Управление
test@t.com			Администратор	02.12.2024, 15:53:24	✎ 🔍 🗑️ 👤
			Пользователь	21.05.2024, 11:28:21	✎ 🔍 🗑️ 👤
			Ассистент	04.04.2024, 11:46:10	✎ 🔍 🗑️ 👤
			Администратор	26.01.2024, 16:44:57	✎ 🔍

Рисунок 13 – Раздел «Пользователи»

Таблица содержит следующие поля:

- 1) Email;
- 2) Имя;
- 3) Фамилия;

4) Роль;

5) Время создания;

6) Управление.

Email – электронный почтовый адрес, указанный пользователем при регистрации.

Имя – содержит имя, которое пользователь указал при регистрации.

Фамилия – содержит фамилию, которую пользователь указал при регистрации.

Роль – функциональная роль пользователя (предусмотрены 3 роли: «Администратор», «Аналитик», «Пользователь»).

Время создания – время создания пользователя.

Управление – в указанном поле содержатся кнопки **Редактировать** () , **Отправить пользователю ссылку для сброса пароля** () , **Сменить пароль** () , **Удалить пользователя** () для изменения параметров учетных записей пользователей и удаления учетных записей.

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

— Имя;

— Фамилия;

— Email;

— Роль.

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

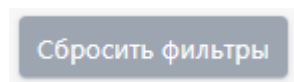


Рисунок 14 – Пагинатор

Ниже строки с фильтрами находится строка с элементами навигации в таблицах. В этой же строке находится элемент отображения количества найденных и показанных результатов *Найдено: 18, показано: с 1 по 10*. Все элементы строки дублируются в нижней части окна программы, снизу от таблицы, для удобства просмотра и навигации.

Описанные выше элементы навигации по информации на страницах являются универсальными и применяются на всех страницах. В некоторых таблицах может добавляться поле с кнопкой выбора элемента таблицы (содержит чекбокс ☐).

Для отмены фильтрации информации на странице в правом верхнем углу предусмотрена иконка



Изменение параметров учетных записей пользователей

В поле Управление находятся кнопки Редактировать пользователя , Отправить пользователю ссылку для сброса пароля (), Сменить пароль  и Удалить пользователя .

При нажатии кнопки **Редактировать пользователя** открывается окно, в котором можно изменить имя и фамилию пользователя, адрес электронной почты, роль выбранного пользователя, а также изменить описание учетной записи (рис. 15). Опция удаления пользователя не применяется по отношению к собственной учетной записи.

При редактировании пользователя можно установить параметр, при котором во время следующего входа пользователя в программу будет осуществлен запрос на смену пароля. Эта возможность применяется и для своей учетной записи.

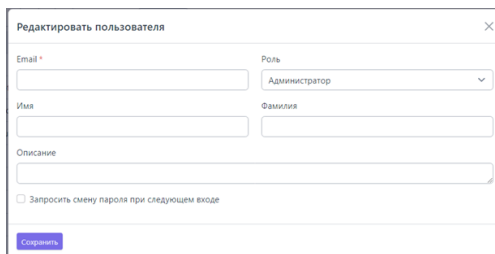


Рисунок 15 – Окно редактирования пользователя

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. 16).

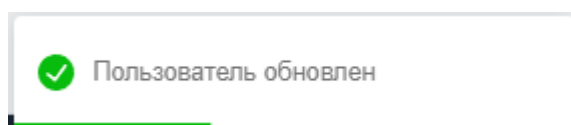


Рисунок 16 – Сообщение о сохранении данных пользователя

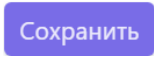
При нажатии по иконке  на действующую почту будет отправлена ссылка, при переходе по которой будет осуществляться изменение пароля.

При нажатии кнопки **Сменить пароль** открывается окно, представленное на рисунке 17.

Пароль должен соответствовать параметрам, указанным в нижней части окна:

- 1) Должен быть длиннее 8 символов;
- 2) Должен содержать хотя бы одну заглавную букву;
- 3) Должен содержать хотя бы одну строчную букву.

Рисунок 17 – Окно «Смена пароля пользователя»

После указания нового пароля требуется нажать по иконке . Кнопка смены пароля недоступна для своей учетной записи.

При нажатии кнопки **Удалить пользователя** открывается окно, в котором для удаления учетной записи выбранного пользователя следует нажать кнопку **Выполнить** (рис. 18). Для отмены удаления учетной записи необходимо нажать кнопку **Отмена** или закрыть окно.

Рисунок 18 – Окно подтверждения удаления пользователя

После удаления учетной записи пользователя в нижней части основного окна программы появляется сообщение (рис. 19).

Рисунок 19 – Сообщение об удалении пользователя

Создание учетной записи пользователя

В нижней части панели администрирования находится кнопка **Создать пользователя**. При нажатии кнопки открывается окно **Создать пользователя** (рис. 20).

The screenshot shows a modal window titled "Создать пользователя" (Create user) with a close button (X) in the top right corner. The form contains the following fields and controls:

- Email ***: A text input field.
- Роль**: A dropdown menu with "Администратор" (Administrator) selected.
- Пароль ***: A password input field with a toggle icon (eye) to show/hide the password.
- Повторите пароль ***: A second password input field with a toggle icon.
- Имя**: A text input field for the user's first name.
- Фамилия**: A text input field for the user's last name.
- Описание**: A text area for additional user information.
- ☐ **Запросить смену пароля при следующем входе**: A checkbox to request a password change on the next login.
- Требования к паролю** (Password requirements): A section with three bullet points:
 - Пароль должен быть не менее 8 символов.
 - Должен содержать хотя бы одну заглавную букву.
 - Должен содержать хотя бы одну строчную букву.
- Создать**: A blue button at the bottom left of the form.

Рисунок 20 – Окно создания нового пользователя

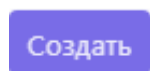
Для добавления пользователя необходимо заполнить в окне **Создать пользователя** следующие поля:

- Email;
- Роль;
- Пароль;
- Повторить пароль;
- Имя;
- Фамилия;
- Описание.

При установке галочки в строке **Запросить смену пароля при следующем входе** пользователь устанавливает функцию смены пароля при следующем входе пользователя с данным именем. Для завершения регистрации нового пользователя следует заполнить все поля ввода. В поле ввода **Адрес электронной почты** необходимо ввести адрес электронной почты вида login@domain. 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. Для подтверждения значений, установленных для новой учетной записи пользователя, необходимо нажать кнопку



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



Рисунок 21 – 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. 22).

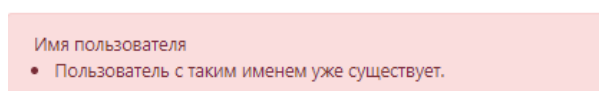


Рисунок 22 – Сообщение о совпадении имени пользователя

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. 23).

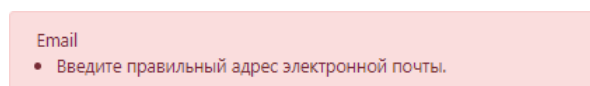
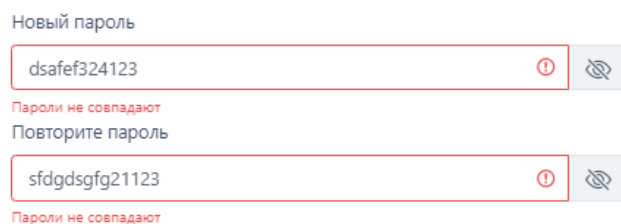


Рисунок 23 – Сообщение о неправильном адресе электронной почты

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. 24).



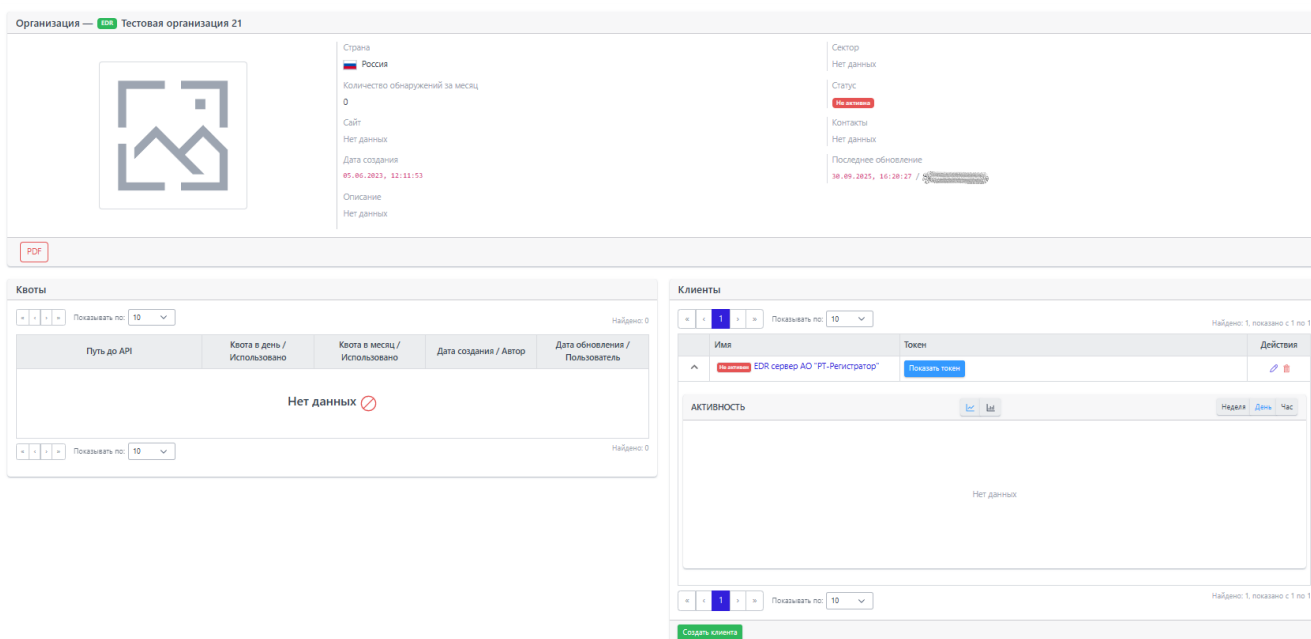
The image shows two password input fields. The first field is labeled 'Новый пароль' (New password) and contains the text 'dsafef324123'. The second field is labeled 'Повторите пароль' (Repeat password) and contains the text 'sfdgdsfg21123'. Below each field, a red error message 'Пароли не совпадают' (Passwords do not match) is displayed. Both fields have a red border and a red icon in the bottom right corner.

Рисунок 24 – Сообщение о несовпадении паролей

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**.

6.4.2. Организация

В разделе **Организация** представлена информация об организации, в которой работают пользователи программы (рис. 25). Здесь содержатся данные о стране происхождения, сайте организации, секторе экономики. Также представлена информация по названию, контактам и описанию организации.



The image shows the 'Организация' (Organization) section of the RT Protect TI interface. The top part displays the organization's name 'Тестовая организация 21' and a logo. Below this, there are several fields for organization details: 'Страна' (Country) set to 'Россия', 'Сектор' (Sector) set to 'Нет данных', 'Статус' (Status) set to 'Активен', 'Контакты' (Contacts) set to 'Нет данных', 'Дата создания' (Creation date) set to '01.06.2023, 12:11:53', and 'Последнее обновление' (Last update) set to '30.09.2023, 16:30:27'. Below these fields, there are two tabs: 'Квоты' (Quotas) and 'Клиенты' (Clients). The 'Квоты' tab is currently selected and shows a table with columns: 'Путь до API', 'Квота в день / Использовано', 'Квота в месяц / Использовано', 'Дата создания / Автор', and 'Дата обновления / Пользователь'. The table is empty and shows 'Нет данных' (No data). The 'Клиенты' tab is also visible and shows a table with columns: 'Имя', 'Токен', and 'Действия'. The table is empty and shows 'Нет данных' (No data).

Рисунок 25 – Окно раздела «Организация»

В области **Организация** имеется иконка , при нажатии по которой можно скачать отчет за определенный период об обнаруженных в организации угрозах в формате pdf.

В области **Квоты** администратор может просматривать квоты на использование вызовов API для пользователей в рамках своей организации.

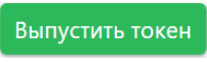
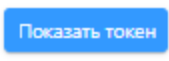
В области **Клиенты** указывается имя токена и его значение (для его отображения необходимо нажать кнопку **Показать токен**).



Примечание

Токен представляет собой зашифрованную последовательность символов, передаваемую клиентом серверу при запросе, которая позволяет серверу однозначно идентифицировать инициатора запроса.

В области **Клиенты** предусмотрены следующие действия с токенами:

- удаление токена (иконка );
- редактирование имени токена (иконка );
- выпуск нового токена (иконка );
- просмотр токена (иконка );
- копирование токена в буфер обмена (иконка ).

При нажатии по иконке редактирования имени клиента появляется окно редактирования, представленное на рисунке 26.

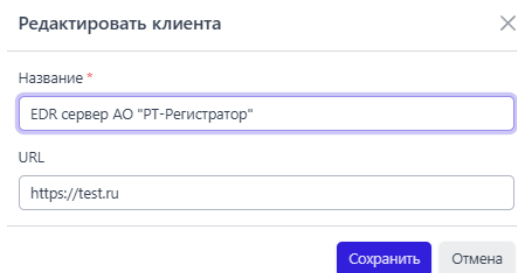
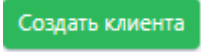
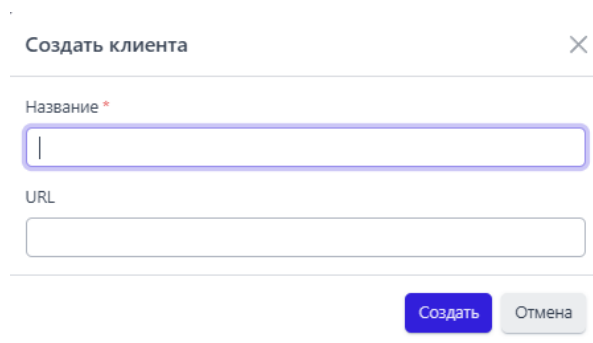


Рисунок 26 – Окно редактирования клиента

После редактирования названия клиента требуется нажать по иконке **Сохранить**.

При нажатии по иконке  появляется окно, представленное на рисунке 27.

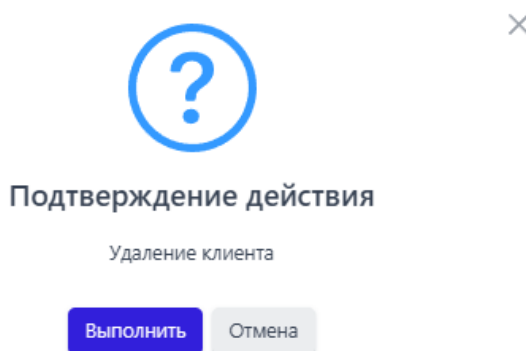


Скриншот диалогового окна «Создать клиента». В окне заголовок «Создать клиента» и кнопка закрытия. Ниже два текстовых поля: «Название *» (с курсором) и «URL». В нижнем правом углу кнопки «Создать» (синяя) и «Отмена» (серая).

Рисунок 27 – Окно «Создать клиента»

После ввода названия в данном окне для завершения действия требуется нажать по иконке **Создать**, после чего новый клиент будет отображаться в списке клиентов.

Для удаления клиента требуется нажать по иконке , после чего появится окно подтверждения удаления, представленное на рисунке 28.



Скриншот диалогового окна подтверждения действия. В центре — большая синяя иконка вопроса. Надпись «Подтверждение действия» и «Удаление клиента». Внизу кнопки «Выполнить» (синяя) и «Отмена» (серая).

Рисунок 28 – Окно подтверждения удаления клиента

В данном окне для подтверждения удаления клиента требуется нажать по иконке **Выполнить**. Для отмены удаления требуется нажать по иконке **Отмена**.

6.4.3. Тэги

Тэги в разделе **Администрирование** предназначены для удобства маркировки и ранжирования источников данных. Создание Тегов и Псевдонимов для пользователей не владельцев не доступно. Доступен только просмотр.

Общий вид страницы **Тэги** представлен на рисунке 29.

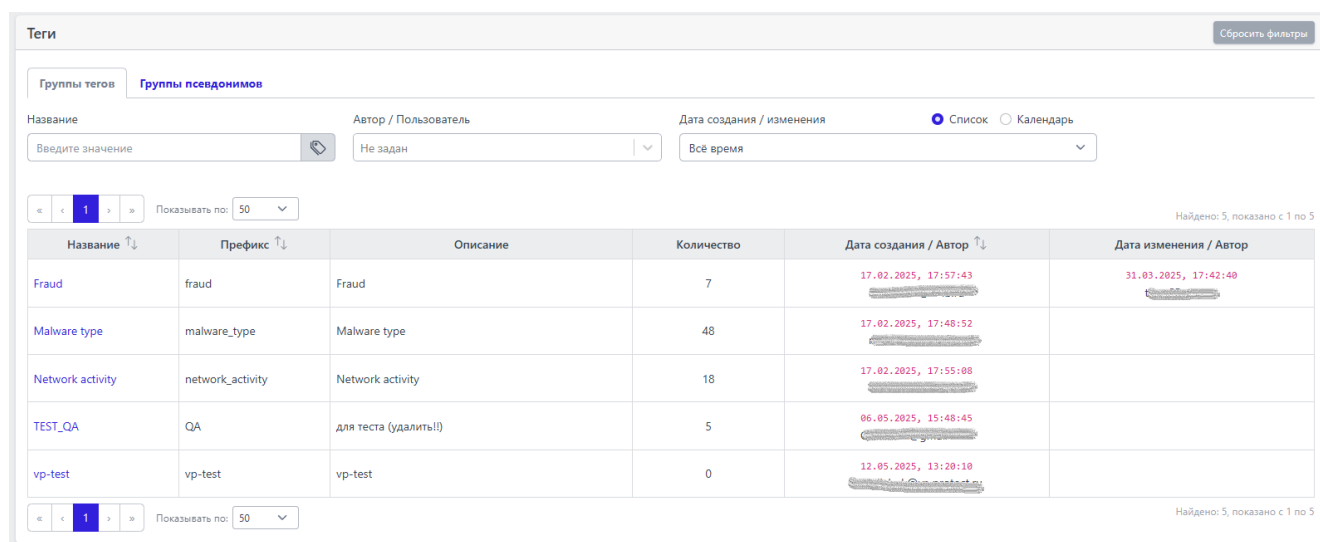


Рисунок 29 – Общий вид страницы Наборы Тегов

Общий вид страницы имеет вид таблицы с полями, зависящими от вкладки, выбранной в верхней части страницы (**Группы тегов/Группы псевдонимов**).

Фильтрация на страницах **Группы тегов/Группы псевдонимов** осуществляется с помощью фильтров, представленных в следующем списке:

- Название;
- Автор/Пользователь;
- Дата создания/изменения.

Таблица с полями для выбранной вкладки (вкладка помечена серым цветом), например, **Группы тегов** представлена полями согласно следующему списку:

- **Название** (название группы тегов);
- Префикс;
- Описание;

- **Количество** (количество элементов в группе);
- Дата создания/Автор;
- Дата изменения /Автор.

Название группы тегов на странице **Теги** вкладки **Группы тегов** является активной ссылкой, при нажатии по которой открывается окно с тегами данной группы (рисунок 30).

Группа тегов - Network activity Сбросить фильтры

Название Дата создания / изменения ☒ Список ☐ Календарь Автор / Пользователь

Введите значение Все время

Показывать по: 10

Найдено: 18, показано с 1 по 10

Название	Описание	Дата создания / Автор	Дата изменения / Автор
network_activity:webattack	webattack	17.02.2025, 17:57:31	
network_activity:vpn	vpn	17.02.2025, 17:57:25	
network_activity:torrent	torrent	17.02.2025, 17:57:18	
network_activity:tor	tor	17.02.2025, 17:57:12	
network_activity:spyware	spyware	17.02.2025, 17:56:55	
network_activity:shopping	shopping	17.02.2025, 17:56:50	
network_activity:shellprobe	shellprobe	17.02.2025, 17:56:41	
network_activity:self-signed	self-signed	17.02.2025, 17:56:34	
network_activity:scan	scan	17.02.2025, 17:56:25	
network_activity:public_share	public_share	17.02.2025, 17:56:19	

Показывать по: 10

Найдено: 18, показано с 1 по 10

Рисунок 30 – Окно Теги в группе тегов

Для фильтрации информации на странице **Теги** определенной группы используется система фильтров, представленная в следующем списке:

- Название;
- Дата создания/изменения.

В данном окне информация о тегах, входящих в группу, представлена в виде таблицы со следующими полями:

- Кнопка выбора ☐;
- Название;
- Описание;
- Дата создания/Автор;
- Дата изменения/Автор.

Общий вид страницы **Теги** вкладки **Группы псевдонимов** представлен на рисунке 31.

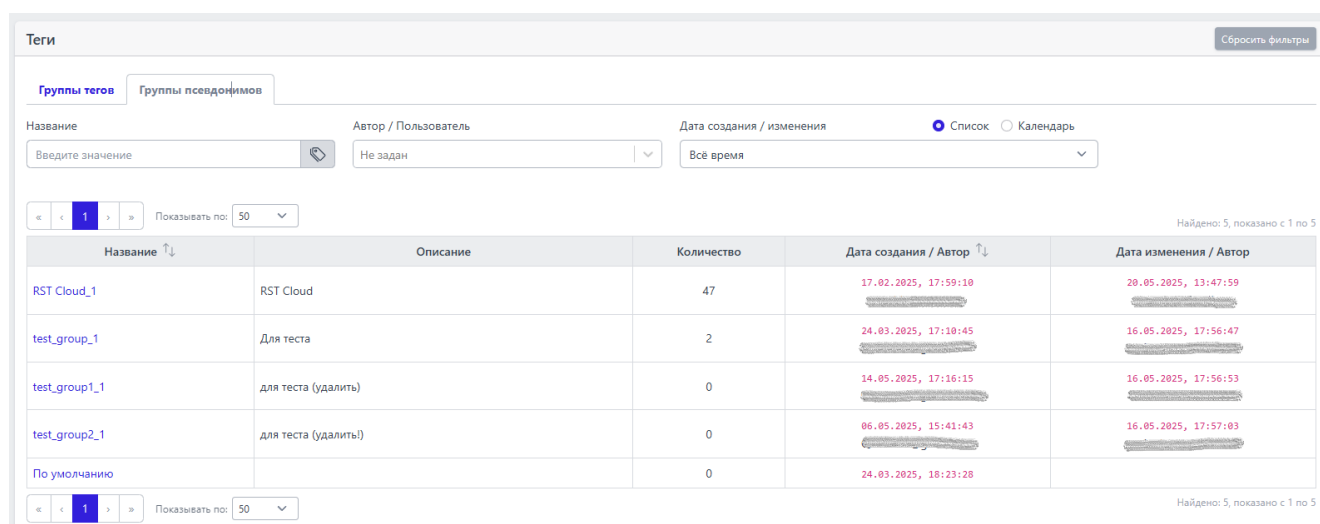


Рисунок 31 – Общий вид страницы Наборы псевдонимов

Псевдонимы служат для привязки тегов из различных внешних систем тегирования к внутренним тегам TI-платформы. Группы псевдонимов нужны для удобства управления псевдонимами, позволяют сгруппировать их по вендору, внешней системе тегов и т.д.

Таблица с полями для выбранной вкладки **Группы псевдонимов** представлена полями согласно следующему списку:

- Название (название группы псевдонимов);
- Описание;
- Количество (количество элементов в группе);
- Дата создания/Автор;
- Дата изменения /Автор.

Название группы псевдонимов на странице **Теги** вкладки **Группы псевдонимов** является активной ссылкой, при нажатии по которой открывается окно с псевдонимами данной группы (рисунок 32).

Группа псевдонимов - По умолчанию Сбросить фильтры

Название: Дата создания / изменения: Всё время Список ☒ Календарь ☐ Автор / Пользователь: Не задан

Показывать по: 50 Найдено: 3, показано с 1 по 3

Название ↑↓	Тег	Дата создания / Автор ↑↓	Дата изменения / Автор
phishing	fraud:phishing ☐	07.10.2025, 17:48:05	
scam	fraud:scam	07.10.2025, 17:47:37	
dga	network_activity:dga	07.10.2025, 17:44:33	

Показывать по: 50 Найдено: 3, показано с 1 по 3

Рисунок 32 – Окно Псевдонимы в выбранной группе

В данном окне информация о псевдонимах, входящих в группу, представлена в виде таблицы со следующими полями:

- Название;
- Тег;
- Дата создания/Автор;
- Дата изменения/Автор.

Для фильтрации информации на странице **Псевдонимы** определенной группы используется система фильтров, представленная в следующем списке:

- Псевдоним;
- Автор/Пользователь;
- Дата создания/изменения.

6.5 Аналитика

Область **Аналитика** содержит информацию об активности, происходящей в организации: обнаружения вредоносных артефактов и отчетах по исследуемым ТИ-платформой артефактам.

Эта информация представлена в следующих разделах:

- 1) Активность;
- 2) Заключение аналитика;
- 3) Анализаторы;
- 4) Граф связей;
- 5) Yara-правила;

- 6) Распространяемая аналитика;
- 7) Угрозы и злоумышленники;
- 8) Вредоносное ПО;
- 9) Инструменты;
- 10) Матрица MitreATT&CK;
- 11) Лента угроз;
- 12) Уязвимости.

Общий вердикт по артефакту от TI платформы высчитывается по алгоритму, в котором присутствуют значения вердикта от анализаторов, заключения аналитики и вердикта от внутренних правил.

6.5.1. Активность

В разделе **Активность** в табличной форме представлена информация о последних угрозах, которые обнаружены в инфраструктуре, подключенной к сервису аналитики (рисунок 33).

Активизация

Артефакты

Кампании

Тип артефакта

Вид артефакта

Период регистрации (на сервере)

Не задан

Видео

Политический

1 неделя

Дополнительные фильтры

Тег

Не задан

Правила обнаружения

1

2

3

Поискать по 10

Название артефакта

Принадлежит ресурс / Временная

Количество обнаружений

Время последнего обнаружения

17.222.68.223

Неизвестный

118

07.05.2025, 12:00:12

8276f3e6859479308605922466063292c7040801c4e773002c44c31a85066

Неизвестный

13

07.05.2025, 10:49:18

73308111630873381310d010ba759045c90a13c7f50a0c173a013c90a0c0b

Видео

50

26.05.2025, 15:43:22

8a568f72248f36808e0830aac9c2095c7630836478665c478ac8e2473686

Политический

45

06.05.2025, 12:12:05

0c8012067cf2302040656453e73078706308013030513c09005e10003a8

Неизвестный

30

05.05.2025, 10:14:11

0c3e44431e703445917307074080f3a8c4080770608050e1c0607502976

Политический

53

05.05.2025, 07:45:10

03a080e23508c54920a0e0705050808031c7e1210c508c20a05020a0e0

Неизвестный

854

29.05.2024, 00:17:08

080536f32a648c9e0336e270a060300336800b76c3080e08003e3c70c70609

Политический

1694

26.05.2024, 12:19:52

0c74952140b03107c560906070c70d0800a077202c240c0200670c050310

Безопасный

11773

24.05.2025, 07:23:24

0a3000051220771323043750705080e770a00810e0a0c3145130e1000

Неизвестный

8

05.05.2025, 00:58:08

Рисунок 33 – Общий вид страницы Активность вкладки Артефакты

В верхней части страницы **Активность** имеются следующие активные вкладки: **Артефакты**, **Клиенты**. При переходе по каждой вкладке на странице **Активность** отображается информация, соответствующая данной вкладке, при этом вкладка, на которую был произведен переход, отмечается серым цветом.



Важно

На странице **Активность** вкладки **Артефакты** показывается информация по обнаруженным артефактам во всей инфраструктуре, подключенной к сервису.

На странице **Активность** вкладки **Клиенты** показывается информация по обнаруженным артефактам в инфраструктуре организации, подключенной к сервису и не являющейся владельцем платформы.

Таблица на вкладке **Артефакты** имеет следующие поля:

- **Название артефакта** (в данном столбце в зависимости от типа артефакта отображается различная информация: контрольная сумма файла-угрозы в формате SHA-256, ip-адреса, доменные имена, URL);
- **Предыдущий вердикт/Время** (отображается вердикт и время вынесения вердикта);
- **Количество обнаружений** (отображается общее количество обнаружений по данному артефакту);
- **Время последнего обнаружения** (отображается время последнего обнаружения файла с угрозой).

Для удобства и наглядного отображения вердикта по артефакту в столбце «Название артефакта» информация отображается разным цветом шрифта:

- 630ae106a99ae7da5d8dd33e7704b27701f65 – вредоносный файл (шрифт красного цвета);
- 02f0c498bb4e5f62722ab5e8a63f5b3779db88ef – безопасный файл (шрифт зеленого цвета);
- B73753C4C69A03F9A3E09F121B6599D7781A48E0247F9B71B56572555E1FE12B – неизвестный файл (шрифт серого цвета);
- 61F897ED69646E0509F6802F82D7C5E88C3E3893C4CA86942E24D203AA878863 – подозрительный файл (шрифт оранжевого цвета).

86.25



В столбце **Название артефакта** слева от артефакта имеется иконка , показывающая в процентах общий вердикт для данного артефакта. В примере, приведенном выше, иконка показывает, что артефакт является вредоносным на 86.25 процента.

В столбце **Название артефакта** справа от информации, характеризующей артефакт (контрольной суммы файла, IP-адреса, или доменного имени), имеется иконка , нажав ЛКМ по которой, можно скачать данную информацию в буфер обмена, а также иконка тега для артефакта.

Контрольная сумма файла угрозы, а также информация по другим типам артефактов является активной ссылкой, при нажатии по которой ЛКМ открывается окно отчета TI-платформы, представленное на рисунке 34.

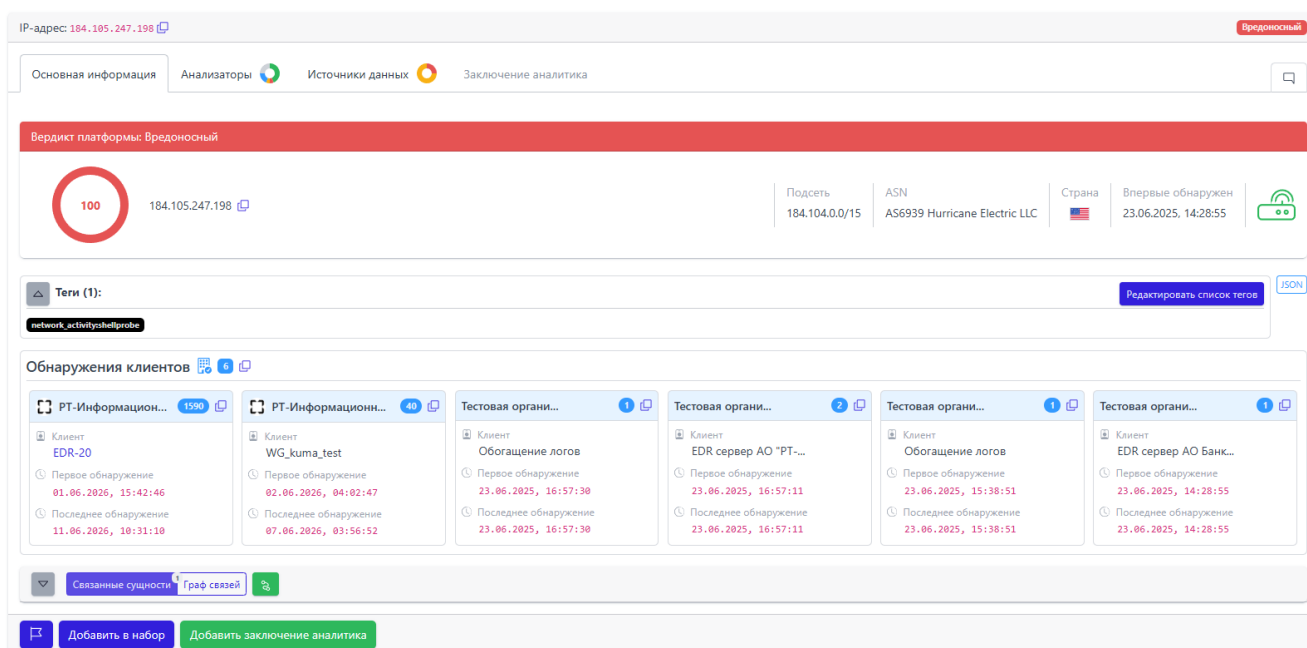


Рисунок 34 – Страница отчета сервиса по обнаруженной угрозе

Страница отчета программы об угрозе разделена на следующие области:

- 1) Область краткой информации об угрозе;
- 2) Область вкладок (Основная информация, Анализаторы, Источники данных, Заключение аналитика);
- 3) Область основной информации отчета об угрозе;
- 4) Область расширенной аналитики (Теги, Обнаружения клиентов, Связанные сущности);

В области краткой информации отображена информация об анализируемой угрозе в зависимости от типа артефакта (контрольная сумма проанализированного файла в формате SHA-256, IP-адрес, доменное имя, URL и вердикт TI-портала по данной угрозе).

В области **Анализаторы** показан список анализаторов.

При наведении указателя мыши на иконку  , рядом с названием вкладки, открывается окно показывающее статусы отчетов полученных для данного артефакта (рисунок 35).

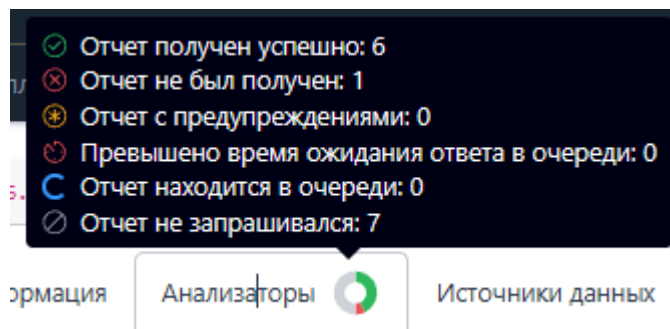


Рисунок 35 – Статусы отчетов по артефакту

При наведении указателя мыши на Название анализатора и нажатия ЛКМ, открывается отчет от анализатора по артефакту.

В области **Источники данных** отображаются отчеты от источников данных по артефакту.

В области названия вкладки **Источники данных** имеется иконка  , при наведении на которую указателя мыши открывается окно с указанием вердиктов по артефакту полученных от источников данных (рисунок 36).

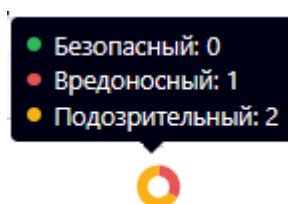


Рисунок 36 – Вердикты по артефакту

Окно основной информации по результатам анализа артефакта в формате JSON представлено на рисунке 37.

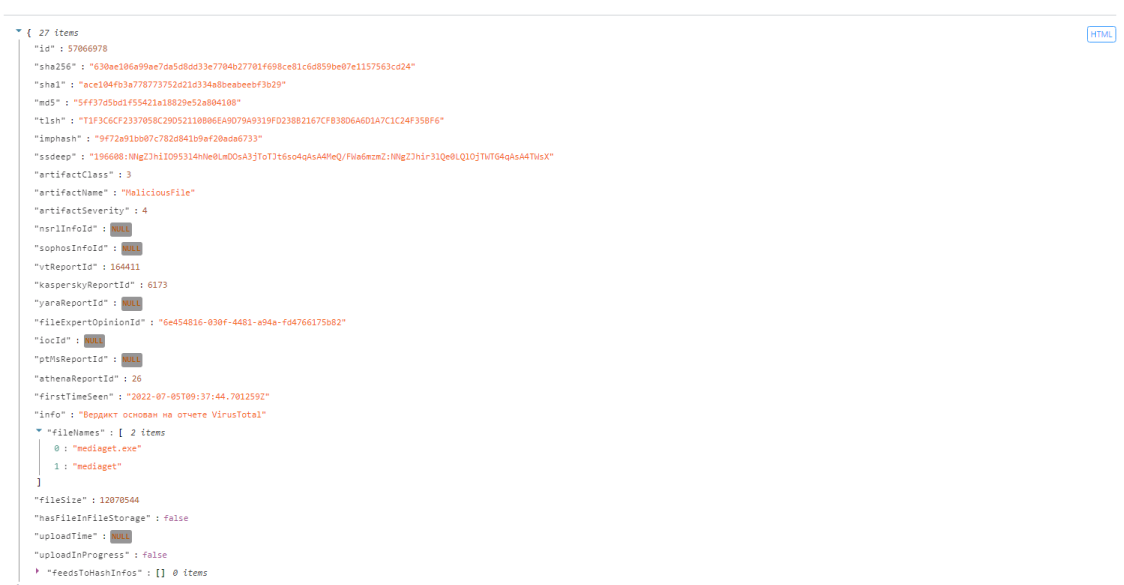


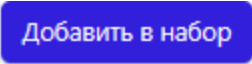
Рисунок 37 – Информация отчета об артефакте в формате JSON

При нажатии по иконке  в поле **Обнаружения клиентов**, показывается таблица в которой отображается список клиентов организации и количество обнаружений артефакта за месяц.

При нажатии по иконке  в поле **Связанные сущности** открывается таблица в которой показаны сущности связанные с рассматриваемым артефактом.

В области связанные сущности имеется иконка  нажав по которой ЛКМ можно привязать к артефакту различные сущности (другие артефакты, уязвимости, организации, отчеты и другое).

При нажатии по иконке  **Граф связей**, открывается область отображающая граф связей для данного артефакта.

На странице отчета по артефакту имеется иконка для создания заявки на корректировку вердикта по артефакту  и иконка для добавления артефакта в набор  **Добавить в набор**.

Для того чтобы добавить артефакт в набор, нужно указать тип набора и название набора.

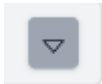
Для фильтрации информации на странице **Активность** вкладка **Артефакты** предусмотрена система основных фильтров, представленная в следующем списке:

- **Тип артефакта** (файл, IP-адрес, доменное имя, URL);
- **Вердикт** (неизвестный, безопасный, вредоносный, подозрительный);

— **Период регистрации (на сервере)** может задаваться в виде списка (15 минут, 1 час, 8 часов, 1 день, 1 неделя, 1 месяц, 3 месяца) либо в виде календаря (начальная и конечная даты);

— Теги.

Также имеется система дополнительных фильтров, которая по умолчанию скрыта. Для открытия поля

с дополнительными фильтрами требуется нажать по иконке  в области **Дополнительные фильтры**.

Имеются следующие дополнительные фильтры:

- Артефакт;
- Количество обнаружений не менее;
- Количество обнаружений не более;
- Предыдущий вердикт;
- Время последнего изменения вердикта;
- Вердикт.

На странице **Активность** вкладки **Клиенты** имеется область с графическим отображением информации по обнаруженным угрозам (рисунок 38).

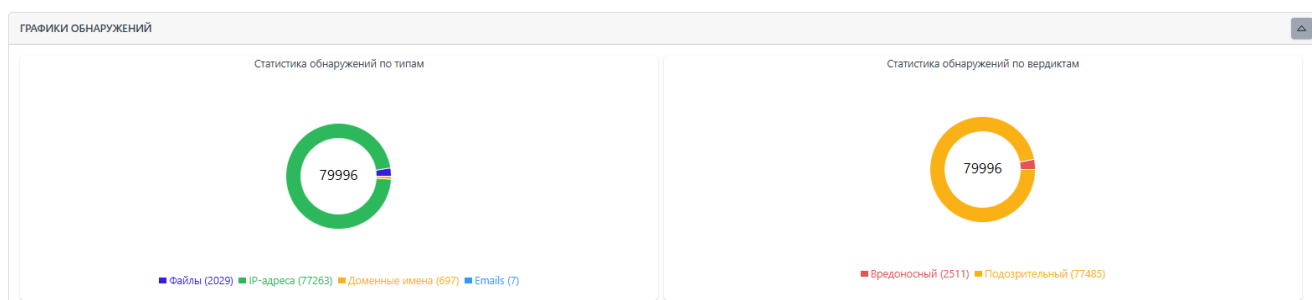


Рисунок 38 – Область графического отображения информации по обнаруженным угрозам вкладки «Артефакты»

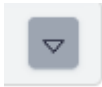
В данной области для наглядности представления информации имеются графики, отображающие следующие статистические данные:

- статистика обнаружений по типам;
- Статистика обнаружений по вердиктам.

Для фильтрации информации на странице **Активность** вкладка **Клиенты** предусмотрена система фильтров, представленная в следующем списке:

- **Тип артефакта** (файл, IP-адрес, доменное имя, URL);
- **Вердикт** (неизвестный, безопасный, вредоносный, подозрительный);
- **Период регистрации (на сервере)** может задаваться в виде списка (15 минут, 1 час, 8 часов, 1 день, 1 неделя, 1 месяц, 3 месяца), либо в виде календаря (начальная и конечная даты);
- Клиенты.

Также имеется система дополнительных фильтров, которая по умолчанию скрыта. Для открытия поля

с дополнительными фильтрами требуется нажать по иконке  в области **Дополнительные фильтры**.

Имеются следующие дополнительные фильтры:

- Артефакт;
- Количество обнаружений не менее;
- Количество обнаружений не более;
- Предыдущий вердикт;
- Время последнего изменения вердикта;
- Вердикт.

6.5.2. Заявки

На странице Заявки представлены заявки на корректировку вердикта по артефакту созданные в рамках организации не владельца платформы.

Страница Заявки представлена на рисунке 39.

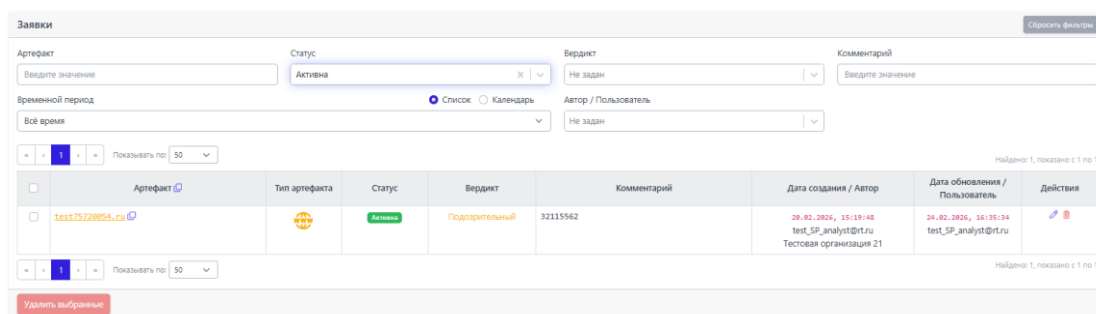


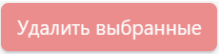
Рисунок 39 – Страница Заявки

В таблице имеются следующие поля:

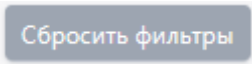
- Кнопка выбора;
- Артефакт;
- Тип артефакта;
- Статус;
- Вердикт;
- Комментарий;
- Дата создания/Автор;
- Дата обновления/Пользователь;
- Действия.

Для фильтрации информации на странице имеется система фильтров, представленная в следующем списке;

- Артефакт;
- Статус;
- Вердикт;
- Комментарий;
- Временной период;
- Автор/Пользователь.

Заявку можно удалить с помощью иконки  в столбце действия, либо отметив кнопкой выбора и нажав по иконке .

Для корректировке заявки, требуется нажать по иконке  в строчке напротив.

На странице имеется иконка  для сброса выставленных фильтров.

6.5.3. Анализаторы

Анализаторы представляют собой функционал для расширения возможностей анализа артефактов с помощью программы RT Protect TI.

Создание и редактирование анализаторов для пользователей не владельцев платформы недоступно.

Процедура создания анализаторов описывается в отдельном документе.

В общем случае можно сказать, что сущность анализаторов это сложно структурированный созданный инструмент по анализу артефактов, на основе заданных при написании анализатора правил.

Общий вид страницы **Анализаторы** представлен на рисунке 40.

Анализаторы				
Сбросить фильтры				
Активные интеграции				
Название		Типы артефактов	Признак активации	
Введите значение		Не заданы	Не задан	
Показывать по 10		Найдено: 19, показано с 1 по 10		
	Название	Приоритет	Описание	Типы артефактов
▼	MetaDefender	» 0 0 0 0	Получает отчеты MetaDefender по артефактам	📄 🌐 📧 📁
▼	MetaDefender	» 0 0 0 0	Metadefender TI request agent	📄 🌐 📧 📁
▼	IPData	» 0 0 0 0	IPData threat intelligence enrichment agent	📄 🌐
▼	PulseConnect	» 0 0 0 0	Получает отчеты PulseConnect по артефактам	📄 🌐 📧 📁
▼	IPQuery	» 0 0 0 0	Получает отчеты Ipquery по IP-адресам	📄 🌐
▼	Google Safe Browsing	» 0 0 0 0	Анализатор Google Safe Browsing	📄 🌐 📧 📁
▼	GreyNoise	» 0 0 0 0	Получает отчеты GreyNoise по IP-адресам	📄 🌐
▼	ABUSE IP	» 0 0 0 0	Получает отчеты Malware Bazaar по артефактам	📄
▼	AlienVault	» 0 0 0 0	Получает отчеты AlienVault OTX по артефактам	📄 🌐 📧 📁
▼	Malshare	» 0 0 0 0	Получает отчеты Malshare TI по артефактам	📄
Показывать по 10		Найдено: 19, показано с 1 по 10		

Рисунок 40 – Общий вид страницы Анализаторы

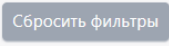
Информация на странице **Анализаторы** представлена в виде таблицы со следующими полями:

- Иконка для раскрытия информации по анализатору (▼);
- Название анализатора;
- Приоритет;
- Описание;
- Типы артефактов.

Для фильтрации информации на странице имеются следующие фильтры:

- Название;
- Признак активации (не задано, активировано, не активировано);
- Типы артефактов (Файл, IP-Адрес, доменное имя, URL, Email).

На странице **Анализаторы** имеются следующие иконки:

-  (при нажатии, сбрасываются выставленные фильтры на странице).

При нажатии по иконке, раскрывающей информацию по анализатору, открывается окно, представленное на рисунке 41.

^		netlas.3r		Получает отчеты Netlas по артефактам		
Максимальное время анализа артефакта (в минутах)				0		
Для работы анализатора требуется загруженный файл				Нет		
Время актуальности получаемых отчетов (в днях)				0		
Автоматически запрашивать отчет по артефакту при открытии				Да		
Название группы псевдонимов				По умолчанию		
Дата создания				25.03.2025, 11:55:44		
Последнее изменение / Пользователь				21.05.2025, 14:20:04 / test@test.ru		

Рисунок 41 – Информация по анализатору

6.5.4. Граф связей

Страница **Граф связей** с незаполненным полем артефакта представлена на рисунке 42.

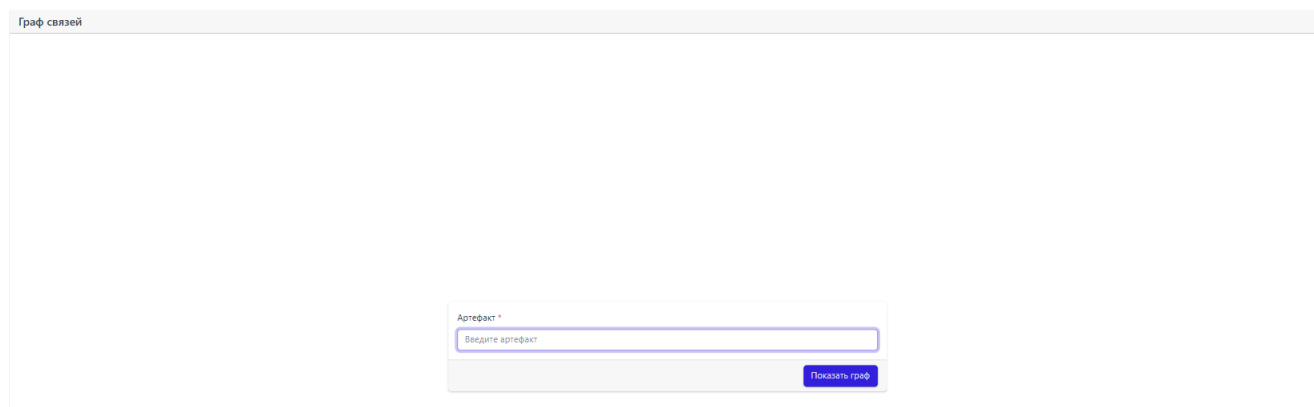


Рисунок 42 – Общий вид пустой страницы «Граф связей»

В поле артефакт следует указать артефакт, для которого необходимо построить граф.

Пример отображения графа после заполнения поля артефакта в виде IP-адреса представлен на рисунке 43.



Рисунок 43 – Отображение графа связей для артефакта типа ip-адрес

При наведении указателя мыши на элемент графа и нажатии ЛКМ открывается окно, представленное на рисунке 44.

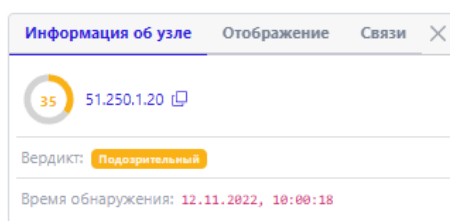


Рисунок 44 – Информация о элементе графа

В окне имеется информация об элементе графа.

При переходе во вкладку Отображение открывается информация о сущностях, связанных с данным элементом графа.

При нажатии по иконке  можно открыть на графе связи сущности с другим элементом графа.

При переходе во вкладку Связи открывается область где показаны связи с другими элементами графа.

На странице графа связей имеются следующие иконки:

— Изменение размера отображения графа (увеличение/уменьшение)   ;

— Поиск  ;

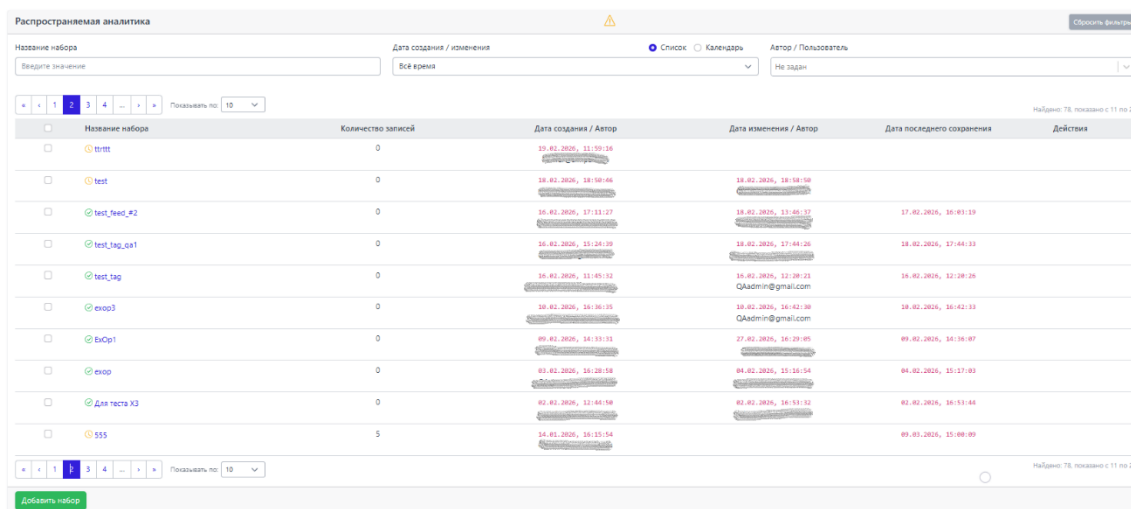
—  (изменение глубины графа и отображения артефактов и типов связей).

При выборе значения глубины графа отличного от 1, связи выбранной ноды будут обновлены при клике на нее.

6.5.5. Распространяемая аналитика

На данной странице Администратор организации видит наборы распространяемой аналитики, созданные в рамках своей организации, наборы созданные в организации владельце и указанные для данной организации как доступные для просмотра, или доступные всем организациям.

Страница раздела «Распространяемая аналитика» представлена на рисунке 45.



Название набора	Количество записей	Дата создания / Автор	Дата изменения / Автор	Дата последнего сохранения	Действия
test	0	10.02.2020, 11:59:38			
test	0	10.02.2020, 10:50:06	10.02.2020, 10:50:06		
test_feed_#2	0	10.02.2020, 17:13:27	10.02.2020, 17:05:17	17.02.2020, 16:01:19	
test_tag_0x1	0	10.02.2020, 11:04:28	10.02.2020, 17:04:28	10.02.2020, 17:04:33	
test_tag	0	10.02.2020, 11:05:32	10.02.2020, 12:28:23	10.02.2020, 12:28:26	
exor3	0	10.02.2020, 10:56:35	10.02.2020, 10:02:30	10.02.2020, 10:02:33	
ExOr1	0	09.02.2020, 14:55:31	27.02.2020, 16:29:05	09.02.2020, 16:16:07	
exor	0	03.02.2020, 10:28:58	04.02.2020, 15:28:54	04.02.2020, 15:27:03	
Для теста X3	0	02.02.2020, 12:04:58	02.02.2020, 16:53:52	02.02.2020, 16:53:44	
555	5	14.03.2020, 10:15:54		09.03.2020, 15:00:09	

Рисунок 45 – Страница раздела «Распространяемая аналитика»

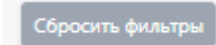
Страница представлена в виде таблицы с наборами аналитических данных.

В таблице имеются следующие поля:

- Название набора;
- Количество записей;
- Дата создания/автор;
- Дата изменения/автор;
- Дата последнего сохранения;
- Действия.

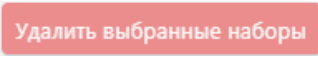
Для фильтрации информации в таблице имеются следующие фильтры:

- Название набора;
- Автор/Пользователь;
- Дата создания/Изменения.

В верхней части страницы имеется иконка  для отмены примененных для фильтрации настроек.

Для навигации на странице имеется стандартный элемент пагинатор.

Действия, возможные над наборами (только для наборов, созданных в рамках своей организации):

-  (редактирование набора);
-  (принудительная синхронизация);
-  (скачивание набора или получение ссылки на скачивание набора);
-  (удаление набора);
-  (добавление нового набора);
-  (удалить выбранные наборы).

При нажатии по иконке  появится окно, представленное на рисунке 46.

Рисунок 46 – Окно создания набора

В данном окне для создания набора требуется ввести в соответствующих полях следующие параметры:

- Название набора;
- Доступен организациям (в данном поле требуется указать организацию, для которой будет доступен данный набор с распространяемой аналитикой);
- Не доступен организациям (в данном поле требуется указать организацию, для которой будет недоступен данный набор с распространяемой аналитикой);
- Почтовый адрес для получения обновленных данных набора аналитики;
- Период обновления набора;
- Тип создаваемого архива;
- Формат создаваемого файла;
- Признак автоматического сохранения после синхронизации;
- Настройки экспорта (порядок вывода экспортируемых полей);
- Название набора и период обновления источника данных.

Далее следует произвести настройку данных в наборе. Для настройки данных имеются области, которые будут различаться в зависимости от выбранной вкладки, на которой представлены настройки.

Выбранная вкладка подсвечивается синим цветом. Поля с настройками по выбранной вкладке **Источники данных** представлены на рисунке 47.

Создать набор

Общие настройки | **Источник данных** | Активность | Заключение аналитика | Фильтры

Источник данных:

Тип артефакта:

Количество:

Актуальность:

Надежность (Минимум):

Сортировка:

Направление сортировки:

Дата добавления: ☒ Список ☐ Календарь

Дата добавления:

Дата синхронизации: →

Активация:

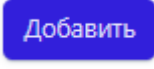
Добавить

Создать

Рисунок 47 – Настройка полей выбранной вкладки «Источники данных»

В данной вкладке можно настроить следующие параметры:

- Источник данных (добавляется источник данных, для которого происходит настройка данных в наборе);
- Тип артефакта (указывается один или несколько типов артефактов согласно выпадающему списку);
- Актуальность (указывается, какие артефакты будут использоваться (актуальные, не актуальные));
- Сортировка (дата обнаружения, по убыванию/по возрастанию);
- Дата добавления (указывается начальная и конечная даты, когда был добавлен артефакт);
- Количество;
- Активация.

После выставления настроек требуется нажать по иконке , после чего появится поле с зафиксированными настройками конфигурации источника данных (рисунок 48).

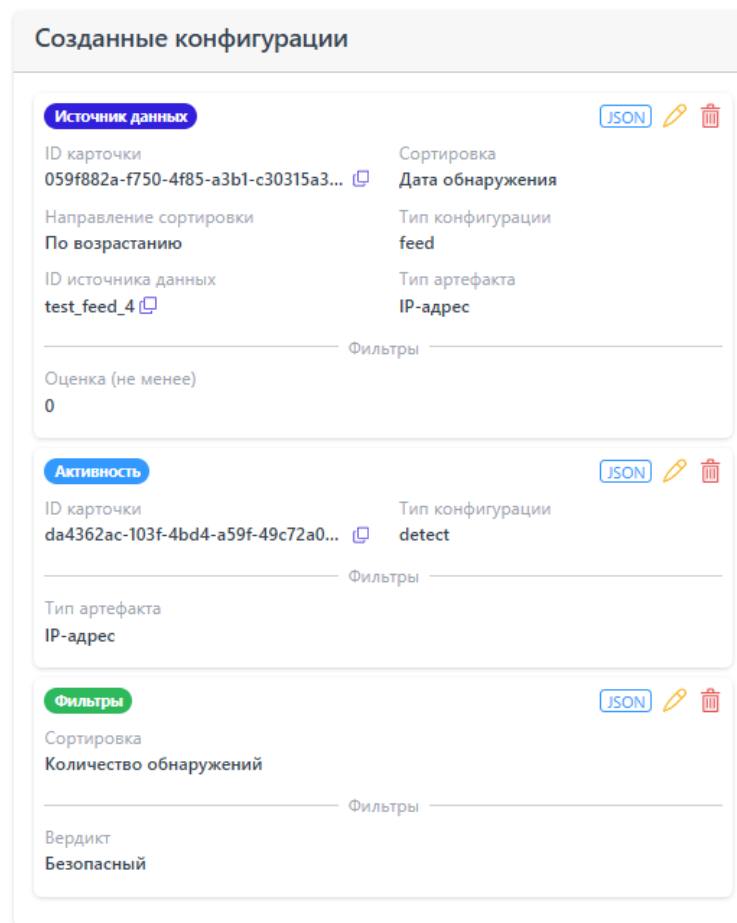


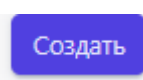
Рисунок 48 – Создание конфигурации набора распространяемой аналитики

В области настроенной конфигурации имеются кнопки, не зависящие от конфигурации и являющиеся общими для всех трех вкладок.

При нажатии по иконке  имеется возможность редактирования настроенной конфигурации.

При нажатии по иконке , имеется возможность просмотра настроенной конфигурации в соответствующем формате.

При нажатии по иконке  происходит удаление настроек параметров в конфигурации.

После редактирования настроек конфигурации для сохранения измененных настроек требуется нажать по иконке .

Поля настройки по выбранной вкладке **Активность** представлены на рисунке 49.

Создать набор

Общие настройки | Источник данных | **Активность** | Заключение аналитика | Фильтры

Тип артефакта: Не задан (выпадающий список) | Количество: 0 (текстовое поле)

Вердикт: Не задан (выпадающий список)

Сортировка: Не задан (выпадающий список) | Направление сортировки: Не задан (выпадающий список)

Оценка (не менее): Введите значение (текстовое поле с иконкой) | Оценка (не более): Введите значение (текстовое поле с иконкой)

Количество обнаружений не менее: Введите значение (текстовое поле с иконкой) | Количество обнаружений не более: Введите значение (текстовое поле с иконкой)

Период регистрации (на сервере): Все время (выпадающий список) | ☒ Список ☐ Календарь

Добавить **Создать**

Рисунок 49 – Настройка полей выбранной вкладки «Активность»

В области настроек параметров по данной вкладке имеется возможность настроить следующие параметры:

- Количество (количество получаемых элементов для каждого выбранного типа артефакта);
- Тип артефакта (Файл, IP-адрес; доменное имя; URL, EMAIL);
- Вердикт (Неизвестный, безопасный, вредоносный, подозрительный);
- Сортировка (по количеству обнаружений, по времени последнего обнаружения, по возрастанию/убыванию);
- количество обнаружений не менее;
- количество обнаружений не более;
- Период регистрации (на сервере) (начальная и конечная даты);
- Оценка (от -100 до 100).

Поля настройки по выбранной вкладке **Заключения аналитика** представлены на рисунке 50.

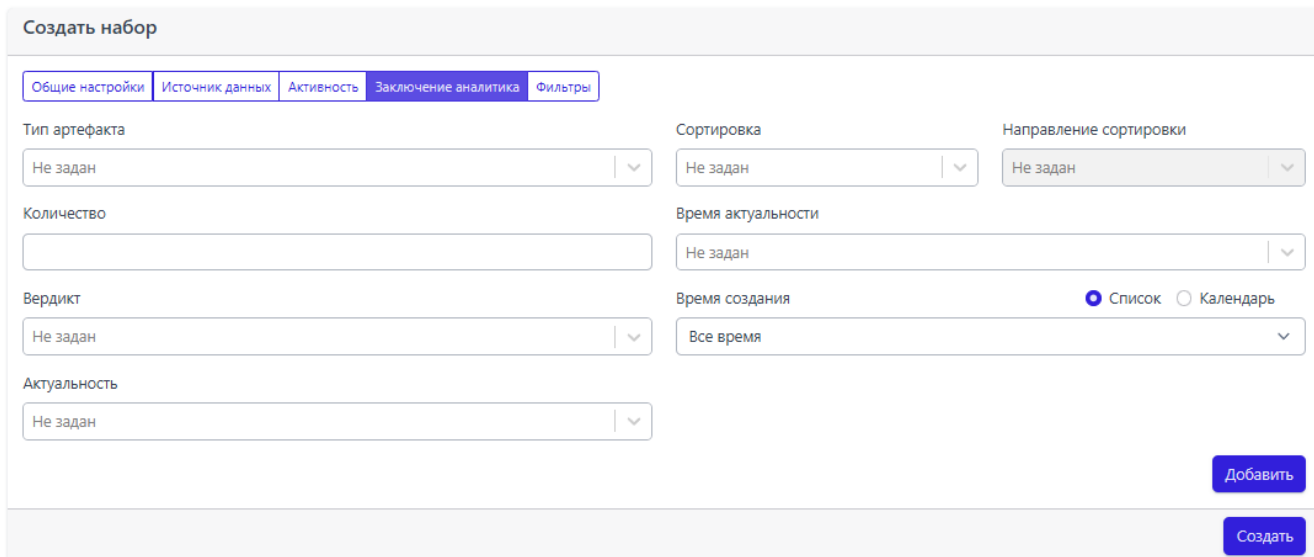


Рисунок 50 – Настройка полей выбранной вкладки «Заклучение аналитика»

В области настроек параметров по данной вкладке имеется возможность настроить следующие параметры:

- Количество (количество записей артефактов по выбранному набору, отображающихся на странице

Заклучение аналитика);

- Тип артефакта (Файл, IP-адрес; доменное имя; URL, EMAIL);
- Вердикт (Неизвестный, безопасный, вредоносный, подозрительный);
- Сортировка (по количеству обнаружений, по времени последнего обнаружения, по

возрастанию/убыванию);

- Время актуальности (день, неделя, месяц, 3 месяца, бесконечно);
- Время создания (начальная и конечная дата),
- Актуальность.

Поля настройки по выбранной вкладке **Фильтры** представлены на рисунке 51.

Создать набор

Общие настройки | Источник данных | Активность | Заключение аналитика | **Фильтры**

Вердикт

Безопасный x v

Дата изменения вердикта:

Все время | v

Сортировка

Количество обнаруже... x v

Направление сортировки

Не задан | v

Оценка (не менее):

Не задана ↗

Оценка (не более):

Не задана ↘

Первое обнаружение

☒ Список ☐ Календарь

Все время | v

Последнее обнаружение

☒ Список ☐ Календарь

Все время | v

Количество обнаружений не менее:

Не задано ↗

Количество обнаружений не более:

Не задано ↘

Количество

Не задано

Теги

Не задан | v

Отмена

Сохранить

Создать

Рисунок 51 – Настройка полей выбранной вкладки «Фильтры»

В области настроек параметров по данной вкладке имеется возможность настроить следующие параметры:

- Вердикт;
- Дата изменения вердикта;
- Сортировка;
- Направление сортировки;
- Оценка (не менее);
- Оценка (не более);
- Первое обнаружение;
- Последнее обнаружение;
- Количество обнаружений не менее;
- Количество обнаружений не более;
- Количество;
- Теги.

6.5.6. Угрозы и злоумышленники

На данной странице пользователь может ознакомиться со списком организаций, совершающих вредоносные действия и характерными угрозами.

Данные получены из источников, подключенных к RT Protect TI.

Примером одного из источников может быть Threat actors MISP.

Общий вид страницы угрозы и злоумышленники представлен на рисунке 52.

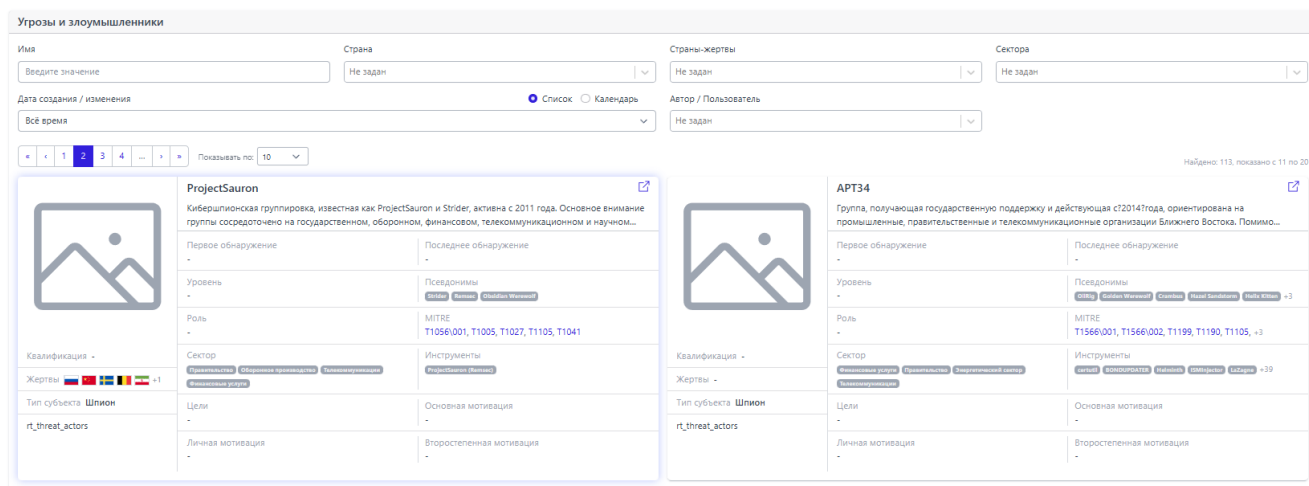


Рисунок 52 – Общий вид страницы Угрозы и злоумышленники

Для фильтрации информации на странице имеется следующая система фильтров:

- Имя;
- Страна;
- Страны жертвы;
- Сектора;
- Дата создания/Изменения;
- Автор/Пользователь.

На странице также можно просмотреть граф связей для артефактов упоминающихся на странице.

6.5.7. Вредоносное ПО

На странице Вредоносное ПО в виде таблицы представлен перечень вредоносного ПО (рисунок 53).

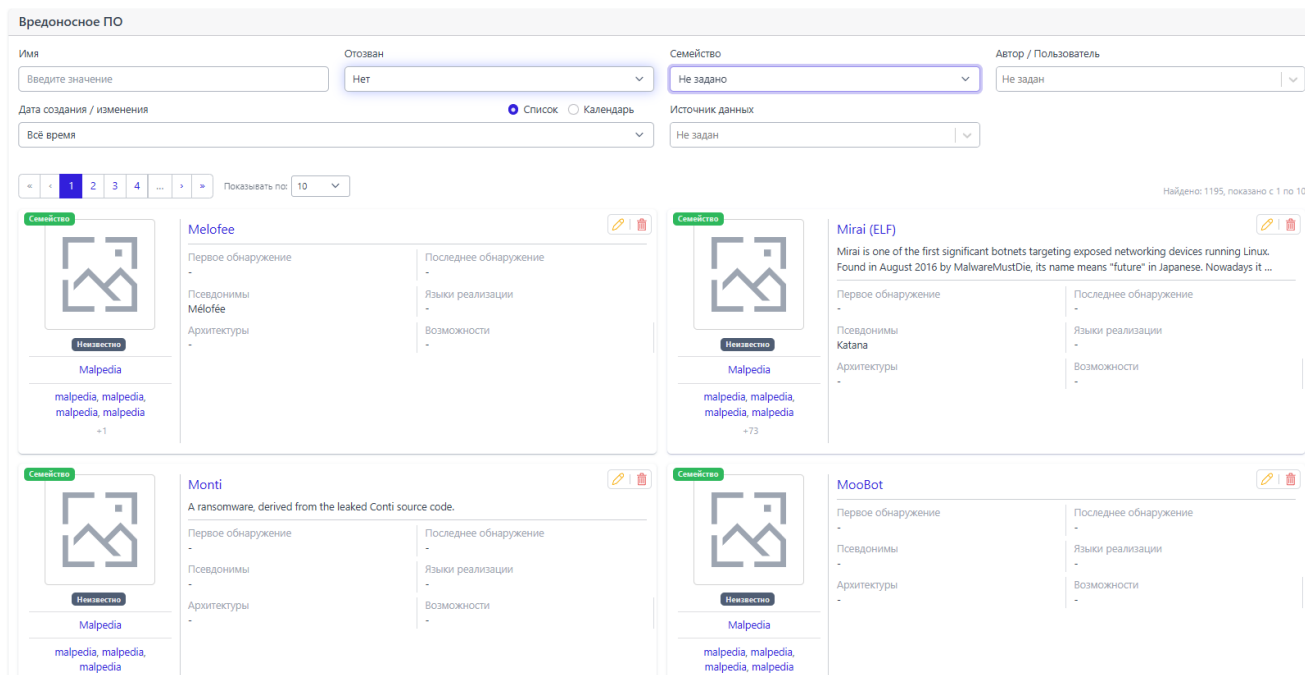


Рисунок 53 – Страница Вредоносное ПО

Информация о вредоносном ПО пополняется из источников данных типа STIX, а также, может быть добавлена вручную.

Для фильтрации информации на странице предусмотрена система фильтров, представленная в следующем списке:

- Имя;
- Отозван;
- Семейство (Не задано, Семейство, Экземпляр);
- Автор/Пользователь;
- Дата создания/Изменения (Все время, 15 минут, 1 час, 8 часов, 1 день, 1 неделя, 1 месяц, 3 месяца);
- Источник данных.

При нажатии по иконке имени вредоносного ПО (выделено синим шрифтом), открывается информация о вредоносном ПО, а также связанные сущности и граф связей.

6.5.8. Инструменты

На странице **Инструменты** показана информация по вредоносным инструментам, используемым злоумышленниками при проведении вредоносных действий.

Общий вид страницы представлен на рисунке 54.

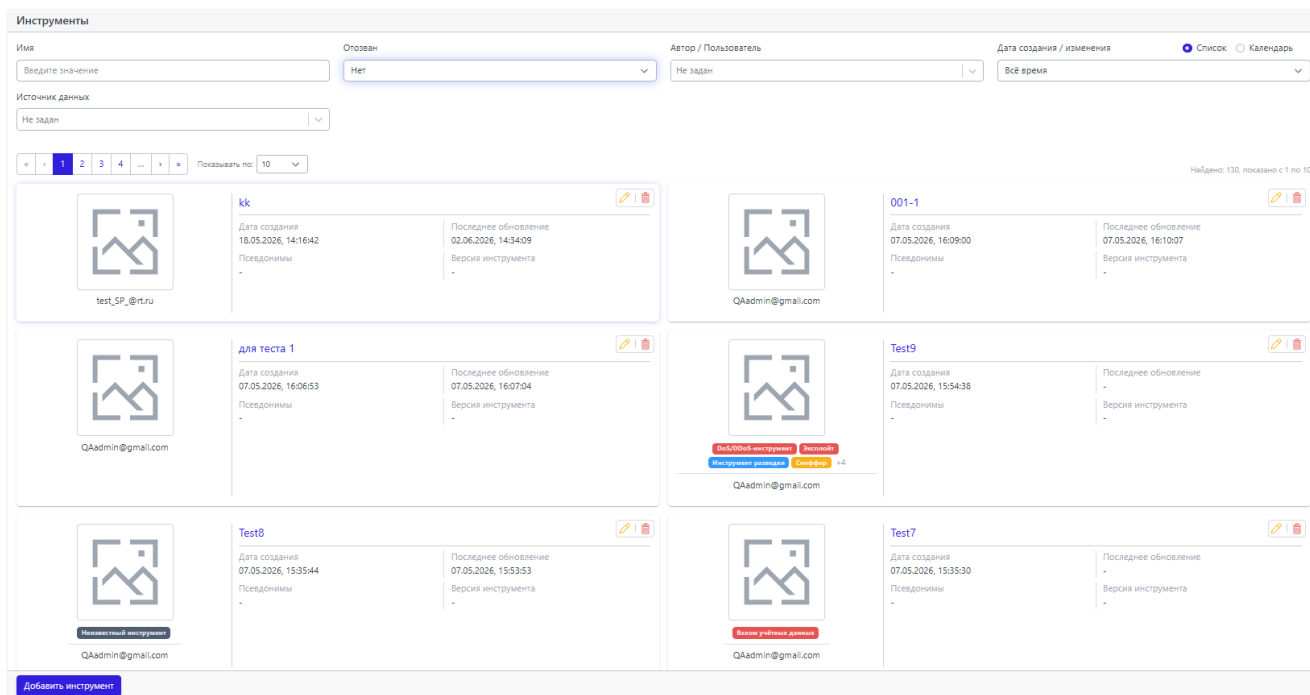


Рисунок 54 – Общий вид страницы «Инструменты»

Информация о вредоносных инструментах пополняется из источников данных типа STIX, а также, может быть добавлена вручную.

Для фильтрации информации имеется система фильтров, представленная в следующем списке:

- Имя;
- Отозван;
- Автор/Пользователь;
- Дата создания/изменения;
- Источник данных.

6.5.9. Матрица MITRE ATT&CK

На рисунке 55 представлен общий вид страницы Матрица MITRE ATT&CK. На данной странице приведено описание техник Mitre описывающих различные вредоносные действия. Аналитик и администратор для удобства описания и понимания вредоносных техник упоминающихся в отчетах может обратиться к странице.

Поиск

Поиск по названию или ID техники...

Reconnaissance	12	Resource Development	9	Initial Access	11	Execution	24	Persistence	25	Privilege Escalation	14	Stealth	33
T1589 Gather Victim Identity I...	1	T1583 Acquire Infrastructure	1	T1078 Valid Accounts	1	T1047 Windows Management Inst...		T1034 Path Interception		T1034 Path Interception		T1006 Direct Volume Access	
T1590 Gather Victim Network ...	1	T1584 Compromise Infrastruct...	1	T1091 Replication Through Remov...		T1053 Scheduled Task/Job	1	T1037 Boot or Logon Initializat...	1	T1037 Boot or Logon Initializat...	1	T1014 Rootkit	
T1591 Gather Victim Org Infor...	1	T1585 Establish Accounts	1	T1133 External Remote Services		T1059 Command and Scriptin...	11	T1053 Scheduled Task/Job	1	T1053 Scheduled Task/Job	1	T1027 Obfuscated Files or Inf...	11
T1592 Gather Victim Host Info...	1	T1586 Compromise Accounts	1	T1189 Drive-by Compromise		T1061 Graphical User Interface		T1062 Hypervisor		T1055 Process Injection	11	T1036 Masquerading	11
T1593 Search Open Websites/...	1	T1587 Develop Capabilities	1	T1190 Exploit Public-Facing Applic...		T1064 Scripting		T1078 Valid Accounts	1	T1068 Exploitation for Privilege Es...		T1055 Process Injection	11
T1594 Search Victim-Owned Webs...		T1588 Obtain Capabilities	1	T1195 Supply Chain Comprom...	1	T1072 Software Deployment Tools		T1098 Account Manipulation	1	T1078 Valid Accounts	1	T1064 Scripting	
T1595 Active Scanning	1	T1608 Stage Capabilities	1	T1199 Trusted Relationship		T1106 Native API		T1108 Redundant Access		T1098 Account Manipulation	1	T1070 Indicator Removal	1
T1596 Search Open Technical ...	1	T1650 Acquire Access		T1200 Hardware Additions		T1127 Trusted Developer Utilit...	1	T1112 Modify Registry		T1134 Access Token Manipulat...	1	T1078 Valid Accounts	1
T1597 Search Closed Sources	1	T1683 Generate Content	1	T1566 Phishing	1	T1129 Shared Modules		T1133 External Remote Services		T1484 Domain or Tenant Polic...	1	T1108 Redundant Access	
T1598 Phishing for Information	1			T1659 Content Injection		T1153 Source		T1136 Create Account	1	T1543 Create or Modify Syste...	1	T1127 Trusted Developer Utilit...	1
T1681 Search Threat Vendor Data				T1669 Wi-Fi Networks		T1175 Component Object Model a...		T1137 Office Application Start...	1	T1546 Event Triggered Execut...	11	T1134 Access Token Manipulat...	1
T1682 Query Public AI Services						T1197 BITS Jobs		T1176 Software Extensions	1	T1547 Boot or Logon Autosta...	11	T1140 Deobfuscate/Decode Files ...	
						T1203 Exploitation for Client Execu...		T1197 BITS Jobs		T1548 Abuse Elevation Control...	1	T1149 LC_MAIN Hijacking	
						T1204 User Execution	1	T1205 Traffic Signaling	1	T1611 Escape to Host		T1197 BITS Jobs	
						T1559 Inter-Process Communi...	1	T1505 Server Software Compo...	1			T1202 Indirect Command Execution	
						T1569 System Services	1	T1525 Implant Internal Image				T1205 Traffic Signaling	1
						T1574 Hijack Execution Flow	11	T1542 Pre-OS Boot	1			T1211 Exploitation for Stealth	
						T1609 Container Administration C...		T1543 Create or Modify Syste...	1			T1216 System Script Proxy Exe...	1
						T1610 Deploy Container		T1546 Event Triggered Execut...	11			T1218 System Binary Proxy Ex...	11
						T1648 Serverless Execution		T1547 Boot or Logon Autosta...	11			T1220 XSL Script Processing	
						T1651 Cloud Administration Com...		T1554 Compromise Host Software...				T1221 Template Injection	
						T1674 Input Injection		T1556 Modify Authentication ...	1			T1480 Execution Guardrails	

Рисунок 55 – Общий вид страницы Матрица MITRE ATT&CK

6.5.10. Лента угроз

В данном разделе представлена информация о статьях касающихся информационной безопасности, полученных из различных источников.

Общий вид страницы представлен на рисунке 56.

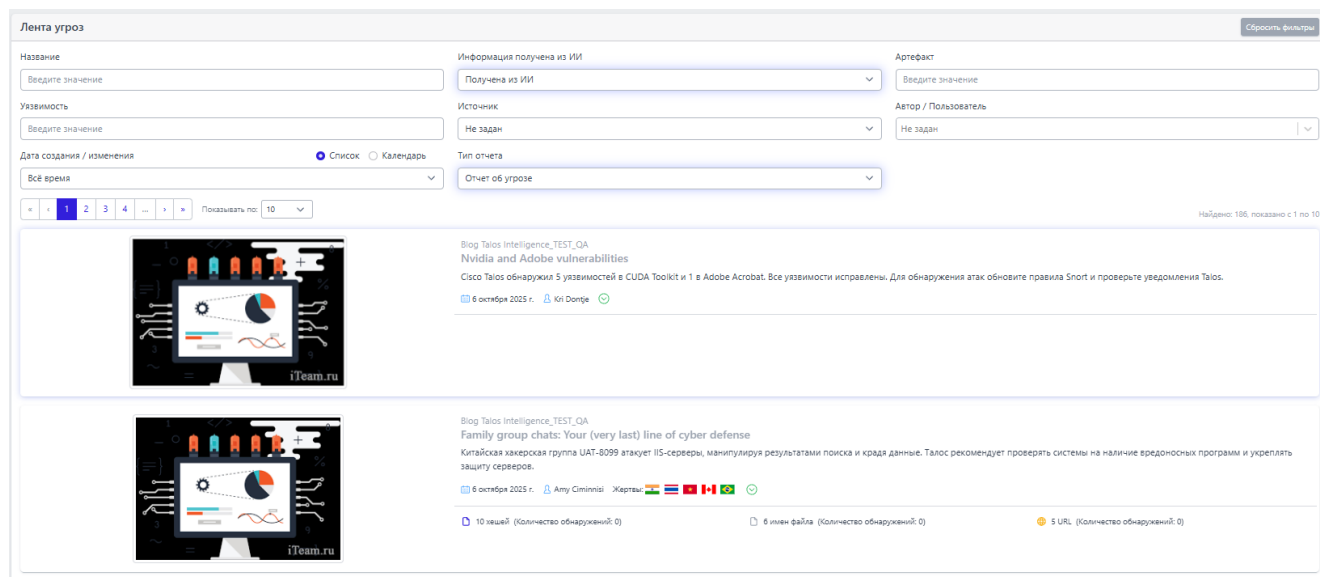


Рисунок 56 – Общий вид страницы Лента угроз

Для фильтрации информации на странице используются следующие фильтры:

- Название;
- Информация получена из ИИ;
- Артефакт;
- Уязвимость;
- Источник;
- Автор/пользователь;
- Дата создания/Изменения;
- Тип отчета.

При нажатии по имени статьи, происходит переход на страницу с информацией по угрозам описанной в статье.

Для информативности, на странице отображается граф связей артефактов, отображенных в отчете.

6.6 Аналитика EDR

Для пользователей программы предусмотрена возможность создавать и редактировать собственные наборы индикаторов атак, индикаторов компрометации, YARA-правил и журналов Windows.

Это позволяет централизованно управлять наборами, которые будут предоставлены потребителям сервиса, а также увеличивает эффективность процесса обнаружения вредоносных атак и объектов, благодаря возможности оперативно внести данные о новых угрозах на сервер аналитики.

Разделы аналитика EDR и исключения EDR для пользователей организаций не владельцев будут видны в модуле администрирования только в том случае, если выставлен признак EDR для организации. Данный признак устанавливается администратором владельцем платформы.



Важно

Редактирование наборов и элементов наборов в разделах **Аналитика EDR** и **Исключения EDR** недоступны для пользователей с ролью **Администратор** и **Аналитик** не владельцев платформы. Доступно редактирование и создание только наборов, созданных в рамках собственной организации не владельца.

Также для пользователей с ролью **Администратор** и **Аналитик** не владельцев платформы недоступно создание теневого набора.

Возможно редактирование и изменение наборов и их элементов, созданных только в рамках данной организации не владельца.



Важно

Следует обратить внимание, что после создания правил аналитики в наборах для последующего распространения и применения данных правил, их необходимо сохранить, нажав по иконке .

6.6.1. Индикаторы атак

Общая информация

Инструменты аналитики, описанные в разделах **Индикаторы атак**, **Индикаторы компрометации**, **Журналы**, а также все инструменты по созданию исключений служат только для хранения данных, распространяемых в дальнейшем клиентам TI-платформы и непосредственно не связаны с логикой работы TI-платформы.

Индикаторы атак в общем смысле – это правила, позволяющие идентифицировать характерные потенциально опасные с точки зрения ИБ поведенческие паттерны программ, работающих на компьютерах защищаемого контура. В отличие от индикаторов компрометации, которые являются артефактами уже свершившейся кибератаки на ИС, индикаторы атак характеризуют определенную стадию прогрессирующей в данный конкретный момент кибератаки.

Это принципиальное отличие позволяет детектировать и реагировать на кибератаку (в том числе автоматически) непосредственно в момент ее развития, в том числе на самом раннем этапе.

Для иллюстрации возможно провести аналогию с банком и грабителем. Индикаторы компрометации в таком случае – это улики, оставленные грабителем после совершения им преступления.

А индикаторы атак – это характерные признаки грабителя, которые охрана банка распознает через систему видеонаблюдения, когда грабитель только приближается к банку или входит в него.

Процесс поиска в потоке событий определенной последовательности событий, удовлетворяющих некоторому условию, называется корреляцией событий или матчингом над потоком событий.

Этот процесс может происходить в режиме реального времени (на стороне агента EDR, в рамках его потока событий) или в оффлайн-режиме на стороне сервера EDR.

Первый вариант позволяет выполнить противодействие (если требуется) в режиме реального времени, не давая атаке шанса развиться, однако ограничен рамками событий только одного агента. Второй вариант не позволяет выполнить противодействие в режиме реального времени, т.к. требуется какое-то время, чтобы события, возникающие на агенте, были доставлены до сервера и обработаны им, перед тем как сервер сможет выполнить корреляцию.

При этом возможно произвести корреляцию среди нескольких агентов и источников событий (как, например, в SIEM-системах).

Автоматизированное реагирование в таком случае заключается в отправке команды по нейтрализации атаки от сервера к агенту. Весь процесс при этом, как правило, стремится выполняться за некоторое нормативное (но не гарантированное) сравнительно короткое время, чтобы прогресс атаки с момента ее обнаружения был минимальным.

Подробная информация о создании индикаторов атак содержится в документе «Руководство Аналитика RT Protect TI».

Наборы индикаторов атак

Страница с наборами индикаторов атак (рис. 57) включает в себя следующие структурные элементы:

- Фильтры;
- таблица с наборами индикаторов атак;
- кнопка Добавить набор;
- кнопка Удалить выбранные наборы;
- кнопка Сбросить фильтры.

Название набора	Количество записей	Дата создания / Автор	Дата изменения / Автор	Дата последнего сохранения	Действия
def	0	14.05.2025, 11:59:51		14.05.2025, 11:59:51	
[LFI] Базовый (v4)	208	11.05.2025, 18:20:48		11.05.2025, 18:20:48	
[LFI] OTСОВит (v4)	21	11.05.2025, 18:20:47		11.05.2025, 18:20:47	
[WNI] Базовый (v7)	515	11.05.2025, 18:14:51		11.05.2025, 18:15:39	
[WNI] Threat Hunting ICA	11	11.05.2025, 18:14:27		11.05.2025, 18:14:42	
[WNI] Расширенный (v7)	96	11.05.2025, 18:13:51		11.05.2025, 18:14:12	
test	1	14.05.2025, 17:08:04		17.05.2025, 14:50:58	
vp-test-loc-1	55	11.05.2025, 10:12:42		11.05.2025, 18:12:42	
hina_Test	33	06.01.2025, 17:41:58		06.01.2025, 17:41:58	
test_errors	3	06.01.2025, 15:40:27		06.01.2025, 15:40:27	

Рисунок 57 – Наборы индикаторов атак

В таблице с наборами индикаторов содержатся следующие поля:

- Название набора;
- **Количество записей** (показывает, сколько индикаторов атак содержится в наборе);
- **Дата создания/Автор** (отображается дата создания набора и автор, создавший набор);

- **Дата изменения/автор** (отображается дата изменения и автор изменивший набор);
- **Дата последнего сохранения** (отображается дата последнего сохранения набора);
- Действия (содержит кнопки Редактировать, Удалить).

В поле **Действия** функционал по удалению и редактированию наборов, доступен только для наборов, созданных пользователем не владельцем платформы (при этом в поле **Название набора**, такой набор помечается иконкой ).

Редактирование наборов, созданных пользователями других организаций, невозможно.

Для фильтрации информации используются следующие фильтры:

- Название набора;
- Автор/Пользователь;
- Дата создания/изменения;
- Поиск по полям набора

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.

Рядом с именем набора имеется иконка , которая показывает, что набор не был сохранен в файл, который экспортируется другим потребителям, подключенным к серверу аналитики.

Кнопка  позволяет сохранить и обновить файл, который используется всеми серверами EDR как база с индикаторами атак. Точно такой же файл экспорта есть у всех разделов аналитики и исключений.

Для перехода к странице **Индикаторы атак** необходимо нажать ЛКМ на имени набора в поле **Название набора**.

Для добавления нового набора с индикаторами атак требуется нажать по иконке  **Добавить набор**, после чего появиться окно представленное на рисунке 58.

Название набора *

Создать

Рисунок 58 – Окно создания набора

В данном окне требуется ввести название набора с индикаторами атак.

Страница «Индикаторы атак»

На странице **Индикаторы атак** содержится информация о правилах. Правила позволяют проводить динамический анализ событий, поступающих с агента в системах типа EDR. 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. 59).

Индикаторы атак vp-test-10a-1

Поиск по полям набора (🔍)

Введите значение:

Имя:

Условие:

Тип:

Критичность (не менее):

MITRE:

Действие:

Комментарий:

Описание:

Признак активации:

Автор / Пользователь:

Дата создания / изменения:

Всё время

Показывать по: 10

Имя	Тип	Критичность / Действия	MITRE	Дата создания / Автор	Последнее изменение / Пользователь	Управление
10a_2	Входящее подключение	Ссылка 🔍		14.03.2025, 13:46:52	18.03.2025, 17:15:11 homer@simpson.ru	🔍 🗑️
10a_3	SSL HELLO	Выполнить 🔍		14.03.2025, 13:46:52		🔍 🗑️
10a_2	Входящее подключение	Ссылка 🔍		14.03.2025, 13:44:52		🔍 🗑️
10a_3	SSL HELLO	Выполнить 🔍		14.03.2025, 13:44:52		🔍 🗑️
10a_4x	DNS-ответ	Критическое 🔍		12.03.2025, 11:33:33 test_SP_@rt.ru	14.03.2025, 11:19:23 homer@simpson.ru	🔍 🗑️
10a_3	SSL HELLO	Выполнить 🔍		12.03.2025, 11:33:33 test_SP_@rt.ru		🔍 🗑️
10a_2	Входящее подключение	Ссылка 🔍		12.03.2025, 11:33:33 test_SP_@rt.ru		🔍 🗑️
10a_test1	Входящее подключение	Выполнить 🔍		12.03.2025, 11:33:33 test_SP_@rt.ru		🔍 🗑️
10a_test1	Входящее подключение	Критическое 🔍		12.03.2025, 11:33:33 test_SP_@rt.ru		🔍 🗑️
10a_4	DNS-ответ	Критическое 🔍		12.03.2025, 18:17:41		🔍 🗑️

Найдено: 55, показано с 1 по 10

Добавить индикатор

Удалить выбранный

Рисунок 59 – 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.

Для фильтрации информации с индикаторами атак на странице набора с индикаторами предусмотрена система фильтров, представленная в следующем списке:

- **Поиск по полям набора** (Поиск осуществляется по подстроке без учета регистра в полях: Значение, Издатель ЭП, Правила, Комментарий);

- Имя;
- Условие;
- Тип;
- **Критичность** (не менее) (не задана, Низкая, Средняя, Высокая, Критичная);
- Mitre;
- **Действие** (Не задано, Блокировать, Детектировать);
- Комментарий;
- Описание;
- **Признак активации** (Не задано, активировано, не активировано);
- Автор/Пользователь;
- Дата создания/изменения.

Для добавления нового индикатора атаки необходимо нажать кнопку **Добавить индикатор** в нижней части страницы. В открывшемся окне **Добавить индикатор** (рис. 60) следует прописать условия, на основании которых будет срабатывать правило.

Рисунок 60 – Добавление индикатора

После написания условия необходимо нажать кнопку **Добавить**. В нижней части страницы появится сообщение о добавлении нового правила (рис. 61).

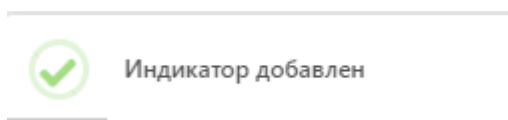


Рисунок 61 – Сообщение о добавлении индикатора атаки

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.62).

Если во время редактирования перейти на вкладку **Конструктор**, то условие необходимо переписывать полностью, редактировать часть условия индикатора атаки возможно только в ручном режиме.

Рисунок 62 – Редактирование индикатора атаки

Для сохранения внесенных изменений необходимо нажать кнопку **Сохранить**, после чего в нижней части страницы появится сообщение об изменении правила (рис. 63).

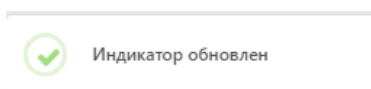


Рисунок 63 – Сообщение об обновлении индикатора атаки

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);
- 3) Однократная генерация обнаружения (будет создан только один инцидент, даже если событие, которое сгенерировало инцидент, произойдет неоднократно).

Чтобы экспортировать индикаторы атак в файл, необходимо нажать кнопку . Экспорт производится в файл формата CSV и 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  в поле **Управление**. Деактивация или активация правила тоже считается изменением в наборе, поэтому информация о пользователе, выполнившем это действие, будет отображаться в поле **Последнее изменение/Пользователь**.

Для удаления индикатора атаки необходимо выбрать его с помощью кнопки выбора, установив флажок, после чего нажать кнопку **Удалить выбранные**. Также можно нажать кнопку  в строке с индикатором.

Для завершения операции ее необходимо подтвердить в открывшемся окне **Подтверждение действия**.

6.6.2. Индикаторы компрометации

Индикаторы компрометации, обрабатываемые программой, подразделяются на сетевые и файловые. Особенностью работы с файловыми индикаторами является то, что все файлы, находящиеся на конечных точках с установленным на них агентом, проверяются только по имени файла и по хешам.

Файловые индикаторы компрометации работают только для исполняемых файлов и файлов с активным содержимым.

Исполняемые файлы анализируются по содержимому (файлы типа EXE, DLL, SYS, COM, OCX, SCR, CPL), а файлы с активным содержимым анализируются по расширению.

При обращении к файлу, хеш-сумма которого совпадает с хеш-суммой, указанной в индикаторе компрометации, обращение блокируется, а в модуле администрирования формируется (или дополняется) инцидент, объединяющий в себе все события, соответствующие индикатору.

Эти события могут иметь разный тип в зависимости от выполняемой операции: открытие файла, чтение, удаление, а также могут относиться к разным процессам в системе. Таким образом блокируются все операции с файлом, изолируя его «по месту», без перемещения в карантин. Запуск исполняемого файла, хеш которого присутствует в перечне индикаторов компрометации, будет блокироваться монитором файловой системы агента RT Protect EDR на самом раннем этапе запуска, когда системный объект **процесс** для него еще не сформирован.

Общая информация

При открытии раздела **Индикаторы компрометации** администратор видит информацию о наборах с индикаторами компрометации. Обнаружение событий, связанных с описанными в наборах компрометации артефактами, вызывает определенное действие, зафиксированное в наборе.

Таким действием может быть блокирование или детектирование вызываемого процесса, связанного с артефактом (например, блокируется открытие сайта, связанного с блокируемым доменом).

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 **Индикаторы компрометации** представлена на рисунке 64. На странице отображаются наборы с индикаторами компрометации, сохраненные на сервере аналитики.

☐	Название набора	Количество записей	Дата создания / Автор	Дата изменения / Автор	Дата последнего сохранения	Действия
☐	1111	1	20.05.2025, 18:22:52		20.05.2025, 18:30:54	
☐	teteetet	2	15.04.2025, 16:18:30		15.04.2025, 16:18:30	
☐	qfwefqwe	9	17.03.2025, 14:54:12		17.03.2025, 14:54:12	
☐	dsfbsdfb	0	17.03.2025, 14:54:09		17.03.2025, 14:54:09	
☐	ewvqewv	0	17.03.2025, 14:54:07		17.03.2025, 14:54:07	
☐	erhwreh	0	17.03.2025, 14:54:03		17.03.2025, 14:54:03	
☐	vqwevqewv	0	17.03.2025, 14:54:01		17.03.2025, 14:54:01	
☐	asdfsdf	0	17.03.2025, 14:53:58		17.03.2025, 14:53:58	
☐	Test_Irina	7	10.03.2025, 16:48:23		10.03.2025, 16:48:23	

Рисунок 64 – Наборы индикаторов компрометации

Информация на странице представлена в табличном виде.

В шапке таблицы представлены следующие поля:

- 1) Кнопка выбора (отмечена элементом ☐);
- 2) Название набора;
- 3) Количество записей;
- 4) Дата создания/Автор (показывает, когда и кто создал набор);
- 5) Дата изменения/Автор (показывает, когда и кто производил последние изменения с набором);

6) **Дата последнего сохранения;**

7) **Действие** (содержит кнопки **Редактировать** (позволяет редактировать название набора) и **Удалить**).

В нижней части страницы **Индикаторы компрометации** находятся кнопки **Добавить набор**, и

Удалить выбранные наборы.

Для фильтрации информации на странице предусмотрена следующая система фильтров:

— Название набора;

— **Поиск по полям набора** (Поиск осуществляется по подстроке без учета регистра в полях: Значение, Издатель ЭП, Правила, Комментарий);

— Автор/Пользователь;

— Дата создания/изменения.

Для добавления нового набора индикаторов компрометации необходимо нажать кнопку **Добавить набор**, после чего в открывшемся окне **Создать набор** (рис. 65) в строке **Название** ввести название нового набора.

Рисунок 65 – Окно «Создать набор»

Для завершения операции добавления необходимо нажать кнопку **Создать**, после чего в нижней части страницы появится сообщение о добавлении набора (рис. 66), а строка с новым набором появится в таблице.



Рисунок 66 – 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**.

Переход на страницу с таблицей **Индикаторы компрометации** происходит при нажатии ЛКМ на названии набора в таблице с наборами индикаторов компрометации.

На странице **Индикаторы компрометации** пользователь может выполнить следующие операции:

- просматривать информацию об индикаторах, входящих в выбранный набор;
- создавать новые индикаторы компрометации;
- изменять индикаторы компрометации, входящие в выбранный набор;
- экспортировать индикаторы в файлы формата CSV;
- импортировать данные из файла в набор индикаторов;
- активировать/деактивировать выбранные индикаторы компрометации.
- удалять из набора выбранные индикаторы компрометации.

Для фильтрации информации на странице с выбранным набором индикаторов компрометации предусмотрена следующая система фильтров:

- **Поиск по полям набора** (Поиск осуществляется по подстроке без учета регистра в полях: Значение, Издатель ЭП, Правила, Комментарий);
- Имя индикатора;
- Артефакт;
- **Тип индикатора** (Не задан, Файл, SHA-256, IP адрес, Доменное имя, Сетевая сигнатура, SHA-256, MD 5, URL);
- Комментарий;
- **Признак активации** (на задано, Активировано, не активировано);
- Автор/Пользователь;
- Дата создания/Изменения.

Шапка таблицы с индикаторами содержит следующие поля:

- 1) Кнопка выбора (отмечена элементом 
- 2) **Имя** (отображается название индикатора);
- 3) **Тип артефакта** (имя файла, SHA-256, IP-адрес, доменное имя, сетевая сигнатура, TLSH, подпись, SHA-1, MD5, URL);

- 4) Артефакт;
- 5) Комментарий;
- 6) Дата создания/Автор;
- 7) Последнее изменение/Пользователь;
- 8) Действия (в поле содержатся кнопки активации/деактивации индикатора, кнопки **Редактировать** и **Удалить**).

В нижней части таблицы индикаторов находятся кнопки операций с индикаторами:

- 1) **Добавить индикатор** ;
- 2) Импортировать CSV-файл –  ;
- 3) Экспортировать набор в файл формата CSV;
- 4) 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. 67) следует заполнить поля, обязательными для заполнения из которых являются поля **Имя индикатора**, **Тип артефакта** и **Артефакт**, после чего нажать кнопку **Добавить** .

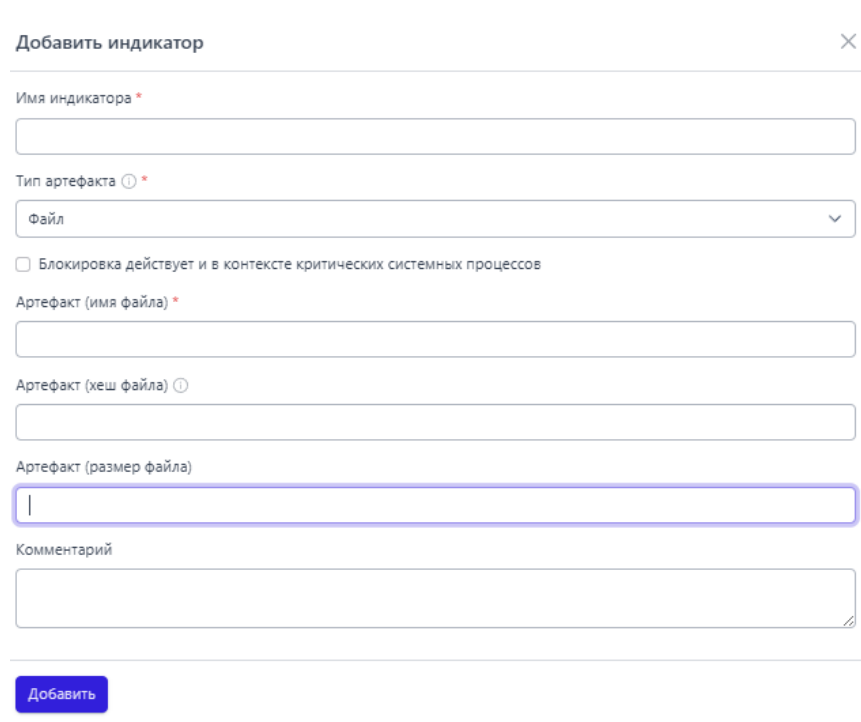


Рисунок 67 – Окно «Добавить индикатор»

В нижней части страницы появится сообщение о добавлении индикатора компрометации (рис. 68).

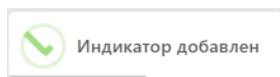


Рисунок 68 – Сообщение о добавлении индикатора

Для экспорта набора в файл следует нажать кнопку **Экспортировать набор в файл формата CSV или json** . Созданный файл будет сохранен в папку, в которую настроена загрузка файлов в операционной системе.

Для импорта данных из файла с индикаторами следует нажать кнопку  **Импортировать CSV или json-файл**. 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.

6.6.3. Журналы

Общая информация

Правила, создаваемые в разделе **Журналы**, позволяют отслеживать события ETW-системы для Windows. Для этого пользователь, используя инструментарий сервера аналитики, может подписаться на события определенного провайдера.

Наборы с журналами

Страница с наборами журналов (рис. 69) открывается при выборе на панели слева раздела **Журналы** и включает в себя следующие структурные элементы:

- кнопка Сбросить фильтры;
- фильтры;
- таблица с наборами журналов Windows;
- кнопка Добавить набор;
- кнопка Обновить файл экспорта;
- кнопка Удалить выбранные наборы.

Журналы

Название набора: Поиск по полям набора: Автор / Пользователь:

Дата создания / изменения: ☒ Список ☐ Календарь

Всё время

Показывать по: 10

Название набора	Количество записей	Дата создания / Автор	Дата изменения / Автор	Дата последнего сохранения	Действия
1111	2	17.03.2025, 15:40:00		17.03.2025, 15:40:00	
21312	1	17.03.2025, 15:37:43		17.03.2025, 15:37:43	
Irina_Test	1	18.03.2025, 16:49:19		18.03.2025, 16:49:19	
123	5	17.02.2025, 17:47:20		03.03.2025, 10:19:43	
test-qa	4	18.01.2025, 11:58:42		03.03.2025, 10:20:15	
test_api	3	19.11.2024, 17:33:19		19.11.2024, 17:33:19	
PMI_Test_1.1	2	11.11.2024, 19:24:32		19.11.2024, 17:13:58	
WinEv-Test	0	03.09.2024, 17:58:33		03.09.2024, 17:58:33	
test_QA1	3	09.08.2024, 17:27:05	29.01.2025, 17:33:38	18.01.2025, 10:54:42	
fghfg	0	17.07.2024, 14:06:56		17.07.2024, 14:06:56	

Добавить набор

Удалить выбранные

Рисунок 69 – Наборы с журналами

Для фильтрации информации на странице с наборами журналов, используется следующая система фильтров:

- Название набора;
- Поиск по полям набора;
- Автор/Пользователь;
- Дата создания/изменения.

Для добавления нового набора необходимо нажать кнопку **Добавить набор**, после чего в окне **Создать набор** ввести название нового набора журналов и указать будет ли доступен набор всем организациям, или только организациям указанным при создании набора. Для завершения операции необходимо нажать кнопку **Создать**. Для удаления набора необходимо нажать кнопку **Удалить** (🗑️) или **Удалить выбранные наборы**.

При нажатии ЛКМ на имени набора открывается страница **Журналы** для выбранного набора (рис. 70).

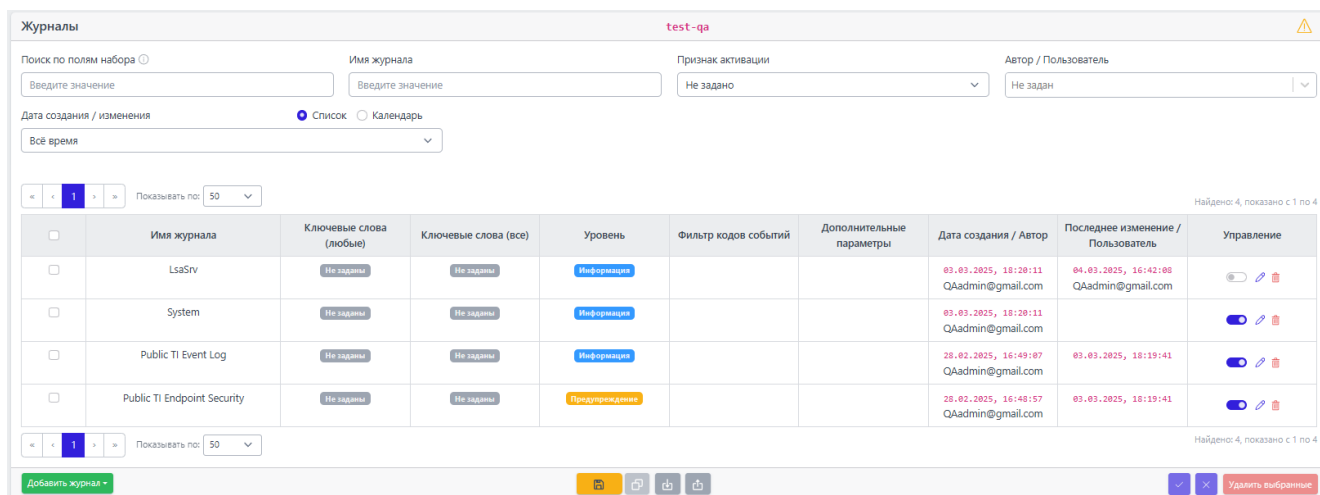


Рисунок 70 – Страница «Журналы» выбранного набора

Страница «Журналы»

На странице **Журналы** можно выполнять следующие операции:

- просматривать ETW-журналы из выбранного набора;
- добавлять новые журналы в выбранный набор;
- экспортировать выбранный набор в файл;
- импортировать данные из файла в выбранный набор правил;
- активировать или деактивировать журнал;
- редактировать настройки логирования выбранного журнала;
- удалить выбранный журнал из набора.

Для фильтрации информации на странице используется следующая система фильтров:

- **Поиск по полям набора** (Поиск осуществляется по подстроке без учета регистра в полях: Значение,

Издатель ЭП, Правила, Комментарий);

- Имя журнала;
- Признак активации;
- Автор/Пользователь;
- Дата создания/изменения.

Для добавления нового журнала необходимо нажать кнопку **Добавить журнал**, после чего выбрать, добавлять журнал по GUID или по именованному каналу.

В зависимости от выбора откроется окно **Добавить журнал по GUID** или **Добавить журнал по именованному каналу**. В этих окнах необходимо указать требуемые для выбранного провайдера параметры логирования.

Для экспорта набора в файл следует нажать кнопку **Экспортировать набор в файл формата CSV или json** ()

Набор будет сохранен в папке **Загрузки** в указанном формате. Для импорта журналов из файла требуется нажать кнопку **Импортировать CSV-файл или json** () . Далее выбрать на компьютере файл, содержащий нужные журналы, и нажать кнопку **Открыть**.

Чтобы активировать или деактивировать журнал из выбранного набора, необходимо нажать кнопку  или  . Действия требуют подтверждения в отдельном окне.

Для удаления журнала(ов) из набора необходимо отметить флажками журнал(ы), который(е) требуется удалить и нажать кнопку **Удалить выбранные** или удалить журналы по отдельности с помощью кнопки **Удалить** ()

Для редактирования условий логирования выбранного провайдера следует нажать кнопку **Редактировать** () , после чего внести изменения в открывшемся окне с журналом. После внесения изменений в журнал необходимо нажать кнопку **Сохранить**.

6.6.4. Yara-правила (файлы)

Общая информация

Правила, указанные в разделе **YARA-правила (файлы)**, используются в качестве инструмента анализа угроз для защищаемой инфраструктуры в части анализа вредоносных файловых сигнатур.

Подробное описание структуры правил, особенностей их написания и работы с YARA-правилами содержится в документе «Руководство аналитика RT Protect TI».

Наборы YARA-правил (файлы)

Страница с наборами YARA-правил для файлов (рис. 71) включает в себя следующие структурные элементы:

— таблица с наборами YARA-правил;

- кнопка **Добавить набор**;
- кнопка **Удалить выбранные наборы**;
- Таблицу со списком экспортируемых наборов из основного раздела (раздел Yara-правила).

YARA-правила (файлы) Сбросить фильтры

Название набора: Поиск по полям набора: Автор / Пользователь:

Дата создания / изменения: ☒ Список ☐ Календарь

Всё время

Показывать по: 10

☐	Название набора	Количество записей	Дата создания / Автор	Дата изменения / Автор	Дата последнего сохранения	Действия
☐	set_sk	9	22.04.2025, 17:01:03		22.04.2025, 17:02:26	
☐	Irina_Test	0	10.03.2025, 16:53:43		10.03.2025, 16:53:43	
☐	проверка_2	1	24.01.2025, 12:06:04		24.01.2025, 12:11:48	
☐	Проверка	28	24.01.2025, 11:59:39		28.02.2025, 16:55:55	
☐	ABC	1	20.11.2024, 14:21:26		14.04.2025, 16:59:00	
☐	abcd	0	12.11.2024, 17:25:54	10.11.2024, 14:15:44	09.03.2025, 10:21:14	
☐	test	1	12.11.2024, 17:24:11		12.11.2024, 17:24:12	
☐	PMI_Test_1.1	1	11.11.2024, 19:30:40		11.11.2024, 19:32:52	
☐	111	0	06.11.2024, 14:37:03		06.11.2024, 14:37:16	
☐	new_name	0	06.11.2024, 12:35:22	06.11.2024, 12:59:19	06.11.2024, 12:35:22	

Найдено: 19, показано с 1 по 10

Добавить набор Удалить выбранные

Рисунок 71 – Наборы YARA-правил (файлы)

Для фильтрации информации на странице имеется система фильтров, представленная в следующем списке:

- Название набора;
- **Поиск по полям набора** (Поиск осуществляется по подстроке без учета регистра в полях: Значение, Издатель ЭП, Правила, Комментарий);
- Автор/Пользователь;
- Дата создания/Изменения.

Для добавления нового набора необходимо нажать кнопку **Добавить набор**, после чего в окне **Добавить набор** ввести название нового набора YARA-правил, а так же указать будет ли доступен набор всем организациям, или только организациям указанным при создании набора.

Для завершения операции необходимо нажать кнопку **Добавить**.

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

Страница «YARA-правила (файлы)»

При нажатии ЛКМ по имени набора открывается страница **YARA-правила (файлы)** для выбранного набора (рис. 72).

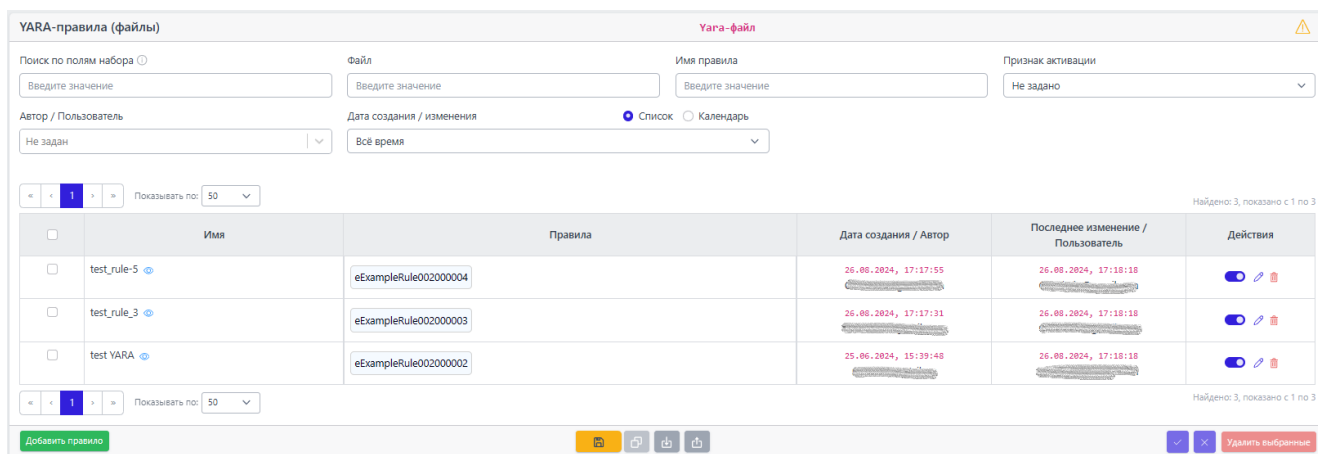


Рисунок 72 – YARA-правила (файлы)

На странице **YARA-правила (файлы)** можно выполнять следующие операции:

- просматривать правила из выбранного набора;
- добавлять новые правила в выбранный набор;
- применять наборы после изменения правил;
- копировать/перемещать выбранные правила в другой набор;
- экспортировать выбранный набор в файл;
- импортировать данные из файла в выбранный набор правил;
- активировать или деактивировать правило;
- редактировать выбранное правило;
- удалить выбранное правило из набора.

Для фильтрации информации на странице имеется система фильтров, представленная в следующем списке:

— Поиск по полям набора (Поиск осуществляется по подстроке без учета регистра в полях: Значение, Издатель ЭП, Правила, Комментарий);

- Файл;
- Имя правила;
- Признак активации;
- Автор/Пользователь;
- Дата создания/изменения.

Для добавления нового правила необходимо нажать кнопку **Добавить правило**.

Подробная информация о синтаксисе YARA содержится в документе «Руководство аналитика RT Protect EDR» и [официальной документации YARA](#). Пример правила YARA приведен на рисунке 73.

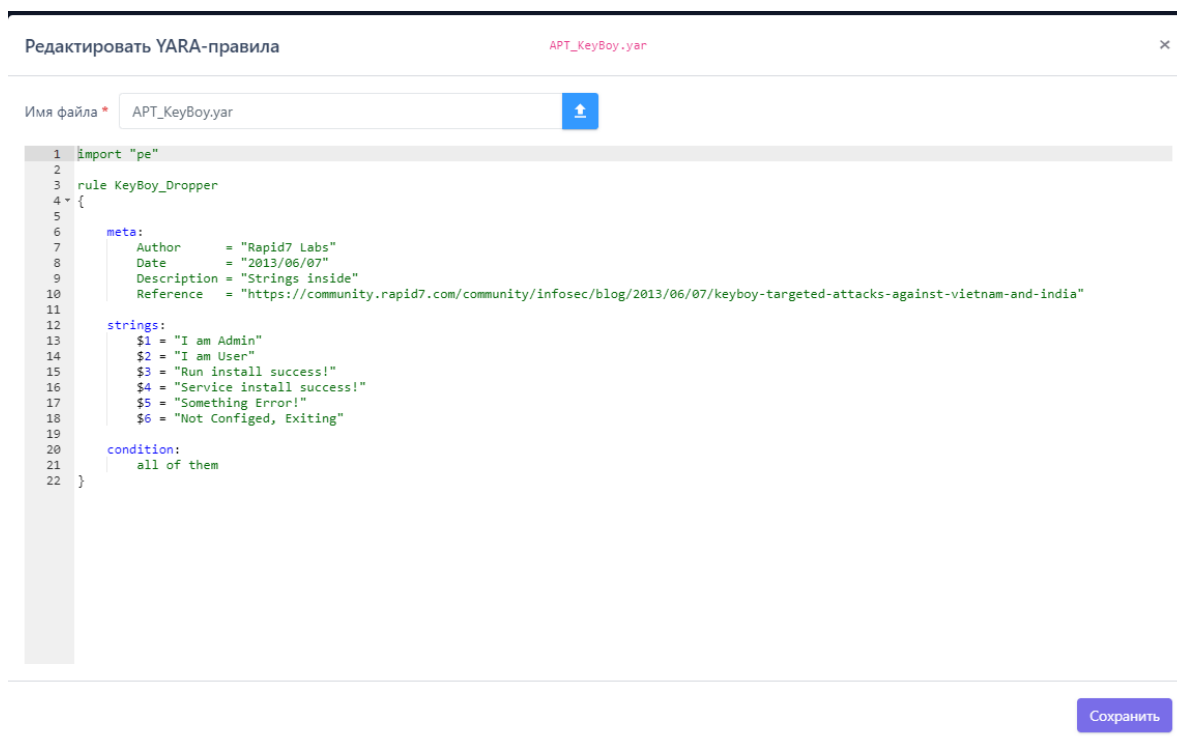


Рисунок 73 – Пример правила YARA

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

Для экспорта набора в файл следует нажать кнопку **Экспортировать набор в файл формата YARA** (📄) (формат YARA/JSON). Набор будет сохранен в папке **Загрузки** в соответствующем формате.

Для импорта правил из файла требуется нажать кнопку **Импортировать YARA файл** () (формат YARA/JSON).

Далее выбрать на компьютере файл соответствующего формата, содержащий нужные правила, и нажать кнопку **Открыть**.

Чтобы активировать или деактивировать правило из выбранного набора, необходимо нажать кнопку .

Для удаления правил из набора необходимо 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 **Редактировать**.

Для фильтрации информации в таблице набора с Yara-правилами, предусмотрены следующие фильтры:

- Имя файла;
- Имя правила.

6.6.5. Yara-правила (память)

Правила, указанные в разделе **YARA-правила (память)**, используются в качестве инструмента анализа угроз для защищаемой инфраструктуры в части анализа памяти процесса на наличие вредоносных сигнатур. В Программе предусмотрены YARA-правила в наборе по умолчанию, а также инструментарий для создания новых правил.

Наборы YARA-правил (память)

Страница с наборами YARA-правил для памяти включает в себя те же структурные элементы, что и страница **Наборы YARA-правил (файлы)**:

- таблица с наборами YARA-правил;
- кнопка **Добавить набор**;
- кнопка **Применить набор**;

- кнопка **Удалить** выбранные наборы;
- таблица с экспортируемыми наборами правил из основного раздела.

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 (память)** для выбранного набора.

Страница «YARA-правила (память)»

На странице **YARA-правила (память)** можно выполнять следующие операции:

- просматривать правила из выбранного набора;
- добавлять новые правила в выбранный набор;
- применять наборы после изменения правил;
- копировать/перемещать выбранные правила в другой набор;
- экспортировать выбранный набор в файл;
- импортировать данные из файла в выбранный набор правил;
- активировать или деактивировать правило;
- редактировать выбранное правило;
- удалить выбранное правило из набора.

Для добавления нового правила необходимо нажать кнопку **Добавить правила**, после чего необходимо выбрать операцию **Новый файл** (для добавления одного файла в режиме набора текста или загрузки с хоста администратора) или **Загрузить файлы** (для добавления одного или нескольких файлов путём загрузки с хоста администратора).

После выбора операции **Новый файл** откроется окно **Добавить YARA-правила**, в котором необходимо добавить имя YARA-файла и написать правило или несколько правил в соответствии с синтаксисом YARA.

Администратор может добавить файл в формате .yag с помощью кнопки **Импортировать yaga-файл** ().

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

При выборе операции **Импортировать yaga-файл** откроется окно, в котором необходимо нажать кнопку **Выбрать файлы**, после чего в открывшемся окне выбрать один или несколько файлов с расширением .yag. Для завершения операции необходимо нажать кнопку **Загрузить файлы на сервер**.

Для копирования или перемещения правила из одного набора в другой необходимо выбрать нужные элементы и нажать кнопку **Копировать/Переместить выбранные элементы в другой набор** (). Далее выбрать набор, в который будет копироваться выбранный элемент. Если необходимо переместить элемент, то следует в окне **Выбор набора** установить флажок **Переместить и удалить выбранные элементы из текущего набора**. Для завершения операции необходимо нажать кнопку **Выбрать**.

Для экспорта набора в файл следует нажать кнопку **Экспортировать набор в файл формата YARA** (). Набор будет сохранен в папке **Загрузки** в соответствующем формате.

Для импорта правил из файла требуется нажать кнопку **Импортировать YARA файл** (.

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 .

Для удаления правил из набора необходимо 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 **Редактировать**.

Для фильтрации информации в таблице набора с Yaga-правилами (память), предусмотрены следующие фильтры:

— **Поиск по полям набора** (Поиск осуществляется по подстроке без учета регистра в полях: Значение, Издатель ЭП, Правила, Комментарий);

- Файл;
- Имя правила;
- Признак активации;
- Автор/Пользователь;
- Дата создания/Изменения.

6.7 Исключения EDR

В области **Исключения EDR** содержатся разделы:

- Исключения для программ;
- Исключения для файлов;
- Сетевые исключения;
- Исключения индикаторов атак.

С помощью этих разделов выполняется настройка исключений для исполняемых файлов, которые позволяют разрешить работу программ или запретить операции с ними без создания инцидентов.

Кроме наборов, создаваемых вручную, в представленных выше разделах могут содержаться автоматически создаваемые наборы.

В эти наборы попадают артефакты согласно алгоритмам сервера, например, в исключения для файлов попадают наиболее часто встречающиеся безопасные хеши.

6.7.1. Исключения для программ

Общая информация

На странице с наборами исключений для программ (рис. 74) содержится список программ, исполнение которых должно соответствовать определенным 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 уменьшить количество ложных срабатываний, а также настроить особенности исполнения программ в защищаемой инфраструктуре.

Название набора	Количество записей	Дата создания / Автор	Дата изменения / Автор	Дата последнего сохранения	Действия
test	5	14.01.2017, 14:10:10		14.01.2017, 14:10:10	
test1	22	14.01.2017, 13:12:44		14.01.2017, 13:12:44	
test2	6	14.01.2017, 10:02:10		14.01.2017, 10:02:10	
test3	4	14.01.2017, 10:12:51		14.01.2017, 10:12:51	
test4	151	19.01.2017, 10:10:51	19.01.2017, 10:10:51	19.01.2017, 10:10:51	
test5	20	19.01.2017, 17:11:45		19.01.2017, 17:11:45	
test6	7	19.01.2017, 13:17:50		19.01.2017, 13:17:50	
test7	11	12.01.2017, 15:01:27		12.01.2017, 15:01:27	
test8	27	19.01.2017, 13:11:49		19.01.2017, 13:11:49	
test9	13	19.01.2017, 10:11:55		19.01.2017, 10:11:55	

Рисунок 74 – Наборы исключений для программ

Наборы исключений для программ

Страница с наборами исключений для программ включает в себя следующие структурные элементы:

- кнопка Сбросить фильтры;
- фильтры;
- таблица с наборами исключений для программ;
- кнопка Добавить набор;
- кнопка Удалить выбранные наборы.

Для фильтрации информации на странице с наборами исключений для программ, предусмотрена система фильтров, представленная в следующем списке:

- Название набора;
- Поиск по полям набора (Поиск осуществляется по подстроке без учета регистра в полях: Значение, Издатель ЭП, Правила, Комментарий);
- Автор/Пользователь;
- Дата создания/Изменения.

Чтобы добавить новый набор с исключениями для программ, необходимо нажать кнопку **Добавить набор**, после чего ввести название нового набора, а так же указать будет ли доступен набор всем организациям, или только организациям указанным при создании набора. 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. 75) 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;
- экспортировать набор с исключениями в файл;
- импортировать исключения из файла в набор;
- активировать/деактивировать исключения в наборе;
- редактировать исключение;
- удалять выбранные исключения.

Исключения для программ									
Поиск по полям набора		Признак активации		Автор / Пользователь					
Введите значение		Не задано		Не задан					
Дата создания / изменения		Список		Календарь					
Всё время									
Показывать по 50				Найдено: 27, показано с 1 по 27					
	Тип	Значение	Флаги	Издатель ЭП	Правила	Комментарий	Дата создания / Автор	Последнее изменение / Пользователь	Управление
☐	Командная строка	schtasks.exe /Create /tn "\Microsoft\Office\Office ClickToRun Service Monitor" /XML "%Program Files\Common Files\Microsoft Shared\ClickToRun\Service Watcher\Schedule.xml" /schtasks.exe /Create /tn "\Microsoft\Office\Office ClickToRun Servi ***	Исключение из телеметрии файловых событий				27.02.2025, 18:23:21 QAdmin@gmail.com		☐
☐	Командная строка	***	Исключение из телеметрии файловых событий				27.02.2025, 17:55:17 QAdmin@gmail.com		☐
☐	Командная строка	***	Исключение из телеметрии файловых событий	Microsoft Windows Hardware Compatibility Publisher_Microsoft Windows Hardware Compatibility Publisher_Microsoft Windows Hardware Compatibility Publisher_Microsoft Windows Hardware Compatibility Publisher_Microsoft Windows Hardware Compatibility Publisher1			27.02.2025, 17:41:31 QAdmin@gmail.com		☐

Рисунок 75 – Исключения для программ определенного набора

Для фильтрации информации на странице исключений для программ, предусмотрена система фильтров, представленная в следующем списке:

- Поиск по полям набора (Поиск осуществляется по подстроке без учета регистра в полях: Значение, Издатель ЭП, Правила, Комментарий);
- Признак активации;
- Автор/Пользователь;
- Дата создания/Изменения.

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. 76).

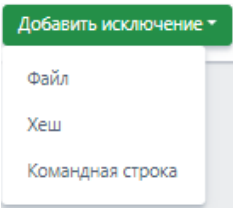
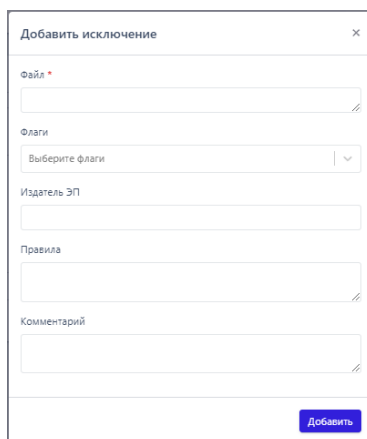


Рисунок 76 – Добавить исключение для программ (выбор типа)

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.

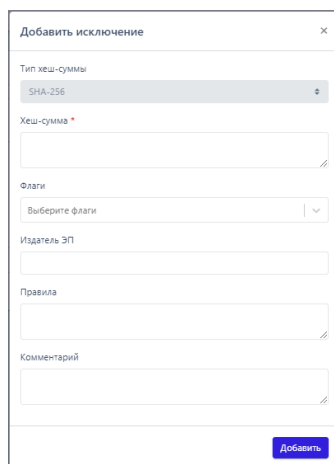
Для типа исключений **Файл** необходимо определить следующие параметры: **Файлы**, **Флаги**, **Издатель ЭП**, **Правила**, **Комментарий** (рис. 77).



The screenshot shows a dialog box titled "Добавить исключение" (Add Exception) with a close button (X) in the top right corner. The dialog contains several input fields: "Файл *" (File) with a text input and a file selection icon; "Флаги" (Flags) with a dropdown menu showing "Выберите флаги" (Select flags); "Издатель ЭП" (Code Signing Publisher) with a text input; "Правила" (Rules) with a text input; and "Комментарий" (Comment) with a text input. A blue "Добавить" (Add) button is located at the bottom right.

Рисунок 77 – 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. 78).



The screenshot shows a dialog box titled "Добавить исключение" (Add Exception) with a close button (X) in the top right corner. The dialog contains several input fields: "Тип хеш-суммы" (Hash type) with a dropdown menu showing "SHA-256"; "Хеш-сумма *" (Hash sum) with a text input; "Флаги" (Flags) with a dropdown menu showing "Выберите флаги" (Select flags); "Издатель ЭП" (Code Signing Publisher) with a text input; "Правила" (Rules) with a text input; and "Комментарий" (Comment) with a text input. A blue "Добавить" (Add) button is located at the bottom right.

Рисунок 78 – 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. 79).

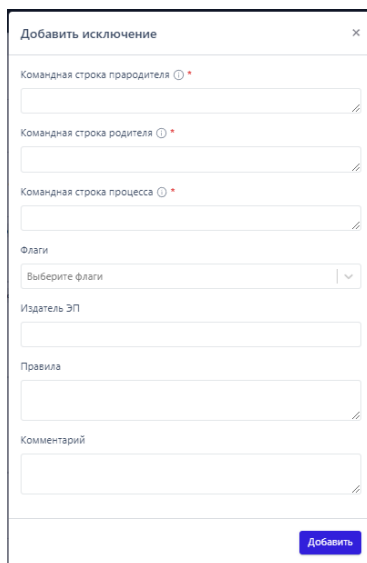


Рисунок 79 – Добавление исключения для программы (тип «Командная строка»)

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 RT Protect TI предусмотрены следующие флаги:

- 1) Разрешить внедрение кода в сторонние программы;
- 2) Разрешить запись памяти сторонних программ;
- 3) Разрешить чтение памяти сторонних программ и управления ими;
- 4) Компонент имеет 32-х битную и 64-х битную версию (NOTE: (syswow 64/system 32));
- 5) Хост-процесс;
- 6) Подтверждение по электронной подписи;
- 7) Разрешение прямого доступа к диску для записи;
- 8) Разрешение прямого доступа к диску для чтения;
- 9) Право взаимодействия с критическими системными программами;
- 10) Антивирусный компонент;
- 11) Исключение из телеметрии сетевых событий;
- 12) Исключение из телеметрии файловых событий;
- 13) Исключение из телеметрии событий реестра Windows;
- 14) Исключение из телеметрии событий поведения;
- 15) Исключение всей телеметрии.

Все установленные для добавляемого исключения флаги будут отображаться в таблице **Исключения для программ** в поле **Флаги**.

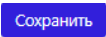
Издатель ЭП – в поле прописывается имя издателя электронной подписи для исполняемого файла. После добавления исключения имя издателя отобразится в таблице **Исключения для программ** в поле **Издатель ЭП**.

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**.

Чтобы удалить исключение для программы, необходимо отметить одно или несколько исключений, установив флажок в кнопке выбора, и нажать кнопку **Удалить выбранные**. Также можно удалить исключение из набора с помощью кнопки **Удалить** (). 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. Для завершения редактирования необходимо нажать кнопку  после внесения изменений в редактируемый элемент.

Для экспорта набора с исключениями в файл следует нажать кнопку **Экспортировать набор в файл** ().

Набор будет сохранен в папке **Загрузки**. Для импорта исключений из файла требуется нажать кнопку **Импортировать-файл** (). Далее выбрать на компьютере файл, содержащий нужные исключения, и нажать кнопку **Открыть**.

Чтобы активировать или деактивировать исключение из выбранного набора, необходимо нажать кнопку .

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** (.

6.7.2. Исключения для файлов

Общая информация

На странице **Наборы исключений для файлов** (рис. 80) содержится список файлов, исполнение которых должно быть разрешено или заблокировано (без создания инцидента, как в случае с индикатором

компрометации). В отличие от исключений для программ, где можно задавать различные параметры с помощью флагов, тем самым влияя на динамику исполнения программы, исключения для файлов работают в статике, то есть разрешение или запрет на запуск файла происходит в момент обращения к этому файлу. Наличие этой возможности позволяет администратору уменьшить количество ложных срабатываний, а в случае необходимости, заблокировать ту или иную программу в целях обеспечения безопасности.

Название набора	Количество записей	Дата создания / Автор	Дата изменения / Автор	Дата последнего сохранения	Действия
irina	1	04.04.2025, 12:00:13		04.04.2025, 12:00:13	
для импорта	6	06.03.2025, 17:30:14		06.03.2025, 17:30:14	
test_0011	7	19.02.2025, 16:14:22	19.02.2025, 16:38:53	06.03.2025, 17:27:36	
test_jp+_1	8	13.02.2025, 16:38:20		13.02.2025, 16:38:20	
test_jp	10922	13.02.2025, 16:16:25		03.03.2025, 18:25:46	
test_jp	18	15.01.2025, 18:33:37		04.03.2025, 18:53:01	
test	6	13.01.2025, 17:51:11		13.01.2025, 17:51:11	
test#503	0	05.03.2025, 15:22:22		23.05.2025, 11:06:07	
TestFileExcl_123	10	03.03.2025, 17:40:06	29.04.2025, 17:13:03	23.05.2025, 11:09:29	
set(shadow)	100	20.12.2024, 16:22:08		21.05.2025, 04:07:29	

Рисунок 80 – Наборы исключений для файлов

Наборы исключений для файлов

Страница с наборами исключений для файлов включает в себя следующие структурные элементы:

- кнопка Сбросить фильтры;
- Показывать по;
- таблица с наборами исключений для файлов;
- кнопка Добавить набор;
- кнопка Удалить выбранные наборы.

Чтобы добавить новый набор с исключениями для файлов, необходимо нажать кнопку **Добавить набор**, после чего ввести название нового набора, указать признак будет ли набор теневым, а также

определить, будет ли доступен набор всем организациям или только организациям, указанным при создании набора.

Для фильтрации информации на странице исключений для файлов предусмотрена система фильтров, представленная в следующем списке:

- Название набора;
- **Поиск по полям набора** (поиск осуществляется по подстроке без учета регистра в полях: **Значение, Издатель ЭП, Правила, Комментарий**);
- Автор/Пользователь;
- Дата создания/Изменения.

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. 81) можно выполнять следующие операции:

- просматривать исключения для файлов в выбранном наборе;
- добавлять новое исключение по имени файла;
- добавлять новое исключение по хешу;
- экспортировать набор с исключениями в файл;
- импортировать исключения из файла в набор;
- активировать/деактивировать исключения в наборе;
- редактировать исключение;
- удалять выбранные исключения.

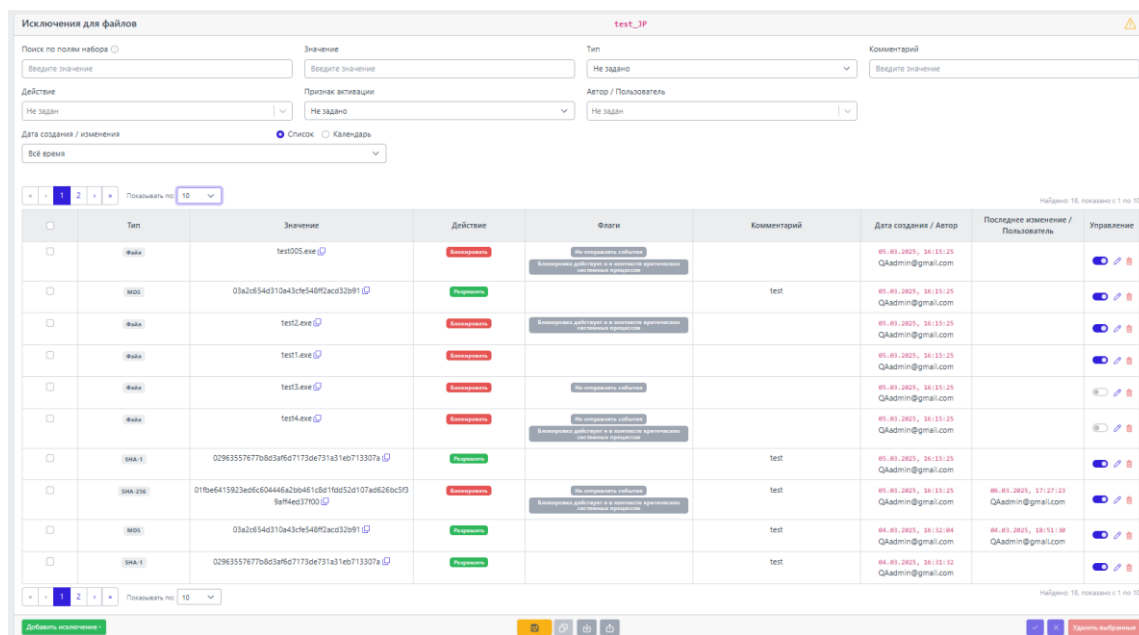


Рисунок 81 – Исключения для файлов

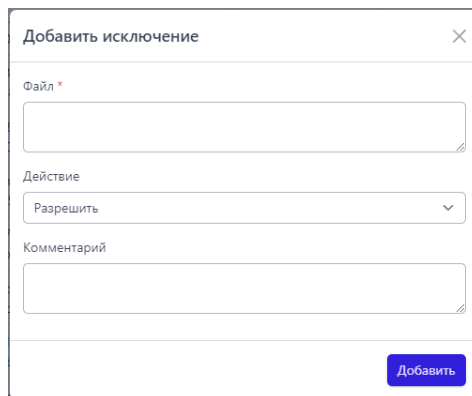
Для фильтрации информации в таблице набора с исключениями для файлов, предусмотрены следующие фильтры:

- Поиск по полям набора (Поиск осуществляется по подстроке без учета регистра в полях: Значение, Издатель ЭП, Правила, Комментарий);
- Значение;
- Тип;
- Комментарий;
- Действие;
- Признак активации;
- Автор/Пользователь;
- Дата создания/Изменения.

Для добавления в набор нового исключения для файлов необходимо нажать кнопку **Добавить исключение** и в открывшемся списке выбрать тип добавляемого исключения: **Файл** или **Хеш**.

Далее в открывшемся окне **Добавить исключение** следует выбрать параметры исключения. В зависимости от выбора типа исключения (**Файл** или **Хеш**) окно **Добавить исключение** будет содержать поля с различными параметрами.

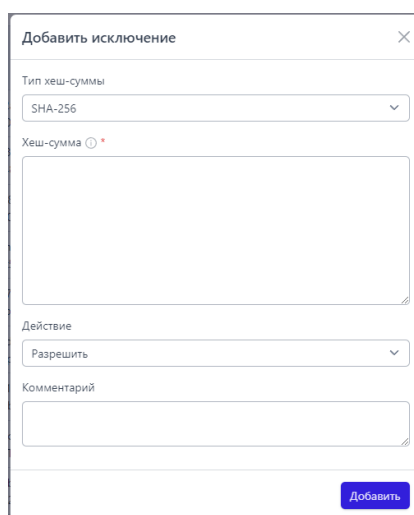
Для типа исключений **Файл** необходимо определить следующие параметры: **Файл** (прописывается имя файла, добавляемого в исключения), **Действие** (блокировать или разрешить), **Комментарий** (рис. 82).



The screenshot shows a dialog box titled "Добавить исключение" (Add exclusion) with a close button (X) in the top right corner. Inside the dialog, there are three main sections: "Файл" (File) with a text input field and a red asterisk indicating it is required; "Действие" (Action) with a dropdown menu currently set to "Разрешить" (Allow); and "Комментарий" (Comment) with a text input field. At the bottom right of the dialog is a blue button labeled "Добавить" (Add).

Рисунок 82 – Добавление исключения для файла (тип «Файл»)

Для типа исключений **Хеш** следует определить следующие параметры: **Тип хеш-суммы**, **Хеш-сумма** (можно добавлять несколько хеш-сумм построчно), **Действие** (разрешить или блокировать), **Комментарий** (рис. 83).



The screenshot shows a dialog box titled "Добавить исключение" (Add exclusion) with a close button (X) in the top right corner. Inside the dialog, there are four main sections: "Тип хеш-суммы" (Hash type) with a dropdown menu set to "SHA-256"; "Хеш-сумма" (Hash sum) with a text input field, a red asterisk, and a circular icon with a plus sign; "Действие" (Action) with a dropdown menu set to "Разрешить" (Allow); and "Комментарий" (Comment) with a text input field. At the bottom right of the dialog is a blue button labeled "Добавить" (Add).

Рисунок 83 – Добавление исключения для файла (тип «Хеш»)

Файл – в поле прописываются имена исполняемых файлов, которые необходимо добавить в исключения.

Имена файлов после добавления исключения будут отображаться в таблице **Исключения для файлов** 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**.

Хеш-сумма – в поле прописываются значения хеш-сумм для исполняемых файлов, которые необходимо добавить в исключения.

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**.

Чтобы удалить исключение для файла, необходимо отметить одно или несколько исключений, установив флажок в кнопке выбора, и нажать кнопку **Удалить выбранные**. Также можно удалить исключение из набора с помощью кнопки **Удалить** (). 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. Для завершения редактирования необходимо нажать кнопку **Сохранить** () после внесения изменений в редактируемый элемент.

Для экспорта набора с исключениями в файл следует нажать кнопку **Экспортировать набор в файл формата CSV** ().

Набор будет сохранен в папке **Загрузки**. Для импорта исключений из файла требуется нажать кнопку **Импортировать CSV-файл** (). Далее выбрать на компьютере файл, содержащий нужные исключения, и нажать кнопку **Открыть**.

Чтобы активировать или деактивировать исключение из выбранного набора, необходимо нажать кнопку .

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** ().

6.7.3. Сетевые исключения

Общая информация

На странице **Сетевые исключения** представлены имена наборов исключений, в которых указываются IP-адреса и доменные имена в качестве идентификаторов при создании исключений. Предусмотрены следующие действия при создании сетевых исключений для взаимодействия с IP-адресами и доменными именами: **Разрешить (всегда)**, **Блокировать**, **Разрешить (кроме изоляции)**.

При создании сетевого исключения, действия, которые следует прописать в соответствующем поле, имеют следующий смысл:

— **Разрешить (всегда)** (означает, что взаимодействие машины, на которой установлен агент, с указанным в исключении IP-адресом или доменным именем разрешается, при этом функциональность сохраняется даже тогда, когда агент изолирован);

— **Блокировать** (означает, что взаимодействие машины, на которой установлен агент, с указанным в исключении IP-адресом или доменным именем блокируется, при этом (в отличие от действия **Блокировать** в индикаторах), не создается событий с критичностью **Средняя** или выше, которые необходимы для создания инцидента, создается событие с критичностью **Низкая**;

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

Использование сетевых исключений позволяет подавлять сетевые срабатывания на конечных точках и снижать количество анализируемой системой информации, так как при сетевом взаимодействии с элементами “белого” списка агент EDR, с которым выполняет взаимодействие TI-платформа, не анализирует данные потока (не производит матчинг сетевых сигнатур).

Наборы сетевых исключений

Страница **Сетевые исключения** содержит наборы с сетевыми исключениями и включает в себя следующие структурные элементы (рис. 84):

- таблица с наборами сетевых исключений;
- кнопка **Добавить набор**;
- кнопка **Удалить выбранные наборы**.

Рисунок 84 – Страница наборов сетевых исключений

Для фильтрации информации на странице **Сетевые исключения**, предусмотрена система фильтров, представленная в следующем списке:

- **Название набора**;
- **Поиск по полям набора** (Поиск осуществляется по подстроке без учета регистра в полях: Значение, Издатель ЭП, Правила, Комментарий);
- **Автор/Пользователь**;
- **Дата создания/Изменения**.

Чтобы добавить новый набор с сетевыми исключениями, необходимо нажать кнопку **Добавить набор**, после чего ввести название нового набора.

Для редактирования названий наборов применяется кнопка **Редактировать** (✎).

Чтобы удалить набор/наборы, требуется отметить нужные наборы флажками и нажать кнопку **Удалить** выбранные наборы или удалить их по отдельности с помощью кнопки **Удалить** (🗑).

Для перехода к странице **Сетевые исключения** необходимо нажать ЛКМ на имени набора в поле **Название набора**.

Страница «Сетевые исключения»

На странице **Сетевые исключения** (рис. 85) можно выполнять следующие операции:

- просматривать сетевые исключения в выбранном наборе;
- добавлять новое исключение по IP-адресу;
- добавлять новое исключение по доменному имени;
- сохранять набор в файл экспорта;
- экспортировать набор с исключениями в файл;
- импортировать исключения из файла в набор;
- активировать/деактивировать исключения в наборе;
- редактировать исключение;
- удалять выбранные исключения.

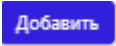
Рисунок 85 – Страница «Сетевые исключения»

Для фильтрации информации в таблице набора с сетевыми исключениями предусмотрены следующие фильтры:

— Поиск по полям набора (поиск осуществляется по подстроке без учета регистра в полях: **Значение**, **Издатель ЭП**, **Правила**, **Комментарий**);

- Значение;
- Тип;
- Комментарий;
- Действие;
- Признак активации;
- Автор/Пользователь;
- Дата создания/Изменения.

Для добавления исключения в выбранный набор необходимо нажать кнопку **Добавить исключение**, после чего откроется одноименное окно. Далее в открывшемся окне **Добавить исключение** следует заполнить поля с параметрами исключения. Поле, отмеченное значком звездочки (*), является обязательным для заполнения.

Чтобы завершить операцию, после ввода параметров в окне **Добавить исключение** следует нажать кнопку . В одном исключении можно написать несколько доменов или IP-адресов, каждое новое значение следует писать в новую строку.

В поле **Значение** таблицы с сетевыми исключениями отображается элемент , который позволяет скопировать IP-адрес или доменное имя в буфер обмена.

Для внесения изменений в исключение необходимо нажать кнопку **Редактировать**  в соответствующей строке таблицы **Сетевых исключений** и в открывшемся окне **Редактировать исключение** изменить необходимую информацию. Для сохранения внесенных изменений необходимо нажать кнопку . Для отмены изменений следует нажать кнопку **Заккрыть окно** – .

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 файл** (). 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 **Деактивировать сетевое исключение/Активировать сетевое исключение** .

Для удаления исключений из набора необходимо отметить флажками исключения, которые требуется удалить, и нажать кнопку **Удалить выбранные** или удалить исключения по отдельности с помощью кнопки **Удалить** ().

При добавлении/редактировании исключения, если в обязательном для заполнения поле было введено не валидное значение, появляется надпись о некорректно введенном значении (IP-адреса или доменного имени) и исключение не будет создано.

6.7.4. Исключения индикаторов атак

Общая информация

Исключения индикаторов атак – это программные элементы, позволяющие переопределить логику индикаторов атак, то есть исключить блокирующее или детектирующее действие при совпадении с условием исключения.

Исключение работает по имени и типу индикатора, к условию которого добавляется условие исключения, поэтому важно указывать правильные имя и тип индикатора атак.

При срабатывании исключения на странице **Активность** будет показано событие со статусом **Разрешено** и причиной **Исключение для индикаторов атак**.

Наборы исключений индикаторов атак

Страница **Наборы исключений индикаторов атак** включает в себя следующие структурные элементы (рис. 86):

- таблица с наборами исключений для индикаторов атак;
- кнопка **Добавить набор**;
- кнопка **Применить набор**;
- кнопка **Удалить выбранные наборы**.

Исключения индикаторов атак

Название набора: Поиск по полям набора: Автор / Пользователь:

Дата создания / изменения: ☒ Список ☐ Календарь

Всё время

Показывать по: 10

Название набора	Доступен организациям	Количество записей	Дата создания / Автор	Дата изменения / Автор	Дата последнего сохранения	Действия
☐ lma_test	Доступен всем	0	18.09.2025, 15:54:35	18.09.2025, 15:54:35	18.09.2025, 15:54:35	
☐ 555	Доступен всем	3	05.09.2025, 16:53:32	24.09.2025, 12:41:05	24.09.2025, 12:41:06	
☐ 333	Доступен всем	1	05.09.2025, 16:52:39	24.09.2025, 12:41:07	24.09.2025, 12:41:07	
☐ 1115	Доступен всем	1	05.09.2025, 16:27:50	24.09.2025, 12:41:06	24.09.2025, 12:41:06	
☐ test_julia	Доступен всем	6	05.09.2025, 12:57:11	24.09.2025, 12:41:04	24.09.2025, 12:41:04	
☐ testimport	Доступен всем	5	04.09.2025, 12:23:44	04.09.2025, 12:23:44	04.09.2025, 12:23:44	
☐ julia	Доступен всем	6	03.09.2025, 18:47:11	03.09.2025, 18:39:43	03.09.2025, 18:39:43	
☐ test1	Доступен всем	7	03.09.2025, 11:39:15	03.09.2025, 18:39:51	03.09.2025, 18:39:51	
☐ PMI_Test_1.1	Доступен всем	3	11.11.2024, 20:05:34	19.11.2024, 18:00:10	19.11.2024, 18:00:10	
☐ Test_10a1	Доступен всем	32	27.09.2024, 12:52:55	03.02.2025, 17:19:12	03.02.2025, 11:30:02	

Показывать по: 10

Добавить набор

Удалить выбранные

Рисунок 86 – Страница «Наборы исключений индикаторов атак»

Для фильтрации информации на странице **Исключения индикаторов атак** предусмотрена система фильтров, представленная в следующем списке:

- Название набора;
- Поиск по полям набора (поиск осуществляется по подстроке без учета регистра в полях: **Значение**, **Издатель ЭП**, **Правила**, **Комментарий**);
- Автор/Пользователь;
- Дата создания/Изменения.

Чтобы добавить новый набор с сетевыми исключениями, необходимо нажать кнопку **Добавить набор**, после чего ввести имя набора, а также указать, будет ли доступен набор всем организациям или только организациям, указанным при создании набора. Для завершения операции необходимо нажать кнопку **Создать**.

Для редактирования названий наборов применяется кнопка **Редактировать** ().

Чтобы удалить набор/наборы, требуется отметить нужные наборы флажками и нажать кнопку **Удалить выбранные наборы** или удалить их по отдельности с помощью кнопки **Удалить** ().

Для перехода к странице **Исключения индикаторов атак** необходимо нажать ЛКМ на имени набора в поле **Название набора**.

На странице **Исключения индикаторов атак** можно выполнять следующие операции:

- просматривать исключения в выбранном наборе;
- добавлять новое исключение индикатора атак;
- применять изменения в наборе исключений;
- копировать/перемещать выбранные исключения из одного набора в другой;
- экспортировать набор с исключениями в файл;
- импортировать исключения из файла в набор;
- активировать/деактивировать исключения в наборе;
- редактировать исключение;
- удалять выбранные исключения.

Общий вид страницы с исключениями для выбранного набора представлен на рисунке 87.

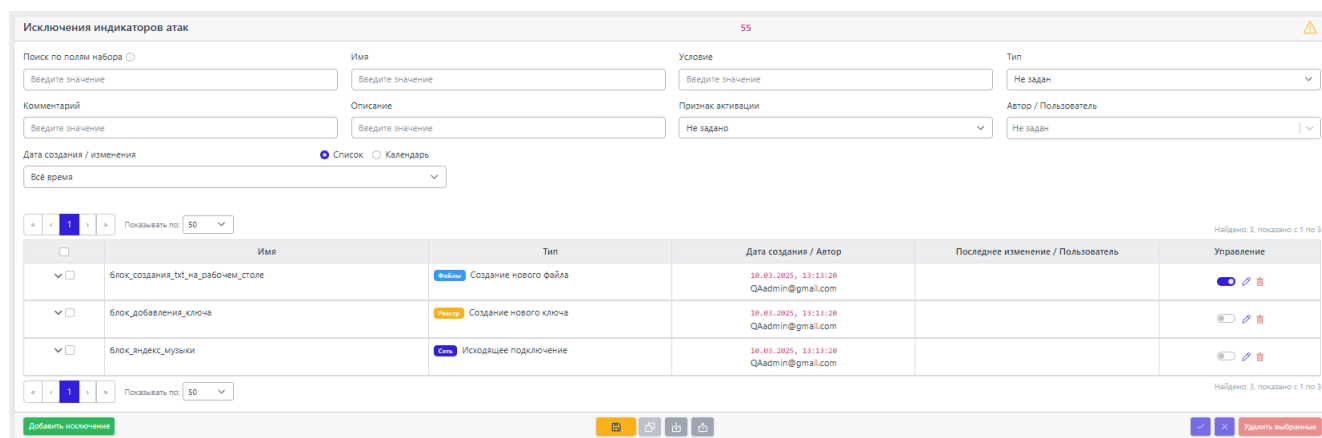


Рисунок 87 – Страница исключений индикаторов атак для выбранного набора

Для фильтрации информации в таблице набора с Исключениями для индикаторов атак предусмотрены следующие фильтры:

- **Поиск по полям набора** (поиск осуществляется по подстроке без учета регистра в полях: **Значение**, **Издатель ЭП**, **Правила**, **Комментарий**);
- **Имя**
- **Условие**;
- **Тип**;

- Комментарий;
- Описание;
- Признак активации;
- Автор/Пользователь;
- Дата создания/Изменения.

Для добавления исключения в выбранный набор необходимо нажать кнопку **Добавить исключение**, после чего откроется одноименное окно. Далее в открывшемся окне **Добавить исключение** следует заполнить поля с параметрами исключения. Поле, отмеченное значком звездочки (*), является обязательным для заполнения.



Важно

Имя исключения должно соответствовать имени исключаемого индикатора.

Добавить условие исключения индикатора атак можно как вручную, так и с помощью конструктора. Также, как и для индикаторов атак, в исключениях для них доступна функция проверки синтаксиса.

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

Для внесения изменений в исключение необходимо нажать кнопку **Редактировать**  в соответствующей строке таблицы **Исключений индикаторов атак** и в открывшемся окне **Редактировать исключение** изменить необходимую информацию.

Для сохранения внесенных изменений необходимо нажать кнопку **Сохранить**. Для отмены изменений следует нажать кнопку **Закрыть окно** – .

Для копирования или перемещения исключения из одного набора в другой необходимо выбрать нужные элементы и нажать кнопку **Копировать/Переместить выбранные элементы в другой набор** . Далее выбрать набор, в который будет копироваться выбранный элемент.

Если необходимо переместить элемент, то следует в окне **Выбор набора** установить флажок **Переместить и удалить выбранные элементы из текущего набора**. Для завершения операции необходимо нажать кнопку **Выбрать**.

Для экспорта набора с исключениями в файл следует нажать кнопку **Экспортировать набор в файл** (). Далее выбрать формат, в котором будет экспортироваться набор (csv или json). Набор будет сохранен в папке **Загрузки** в выбранном формате.

Для импорта исключений из файла требуется нажать кнопку **Импортировать данные из файла в набор**, поддерживаемые форматы: **CSV, JSON** (). Далее выбрать на компьютере файл соответствующего формата, содержащий нужные правила, и нажать кнопку **Открыть**.

Чтобы активировать или деактивировать исключение из выбранного набора, необходимо нажать кнопку  или выполнить активацию/деактивацию с помощью кнопок **Активировать выбранные элементы/Деактивировать выбранные элементы** ( )

Для удаления исключений из набора необходимо отметить флажками исключения, которые требуется удалить, и нажать кнопку **Удалить выбранные** или удалить исключения по отдельности с помощью кнопки **Удалить** ().

6.8 Уязвимости

6.8.1. Общие сведения

В данном разделе представлена информация по обнаруженным с помощью платформы RT Protect TI уязвимостям.

Отдельно представлены таблица с уязвимостями и таблица с программами, в которых обнаружены уязвимости.

Уязвимости идентифицированы в общепринятом формате CVE. Приведено описание уязвимости по БДУ ФСТЭК и базе данных от Национального института стандартов и технологий (NIST).

Типы уязвимостей представлены по CWE (Common Weakness Enumeration). Также имеются рекомендации по предотвращению и устранению уязвимостей и информация по описанию уязвимостей.

Оценка серьезности уязвимости представлена по классификации CVSS (Common Vulnerability Scoring System).

6.8.2. Уязвимости

Общий вид страницы «Уязвимости» представлен на рисунке 88.

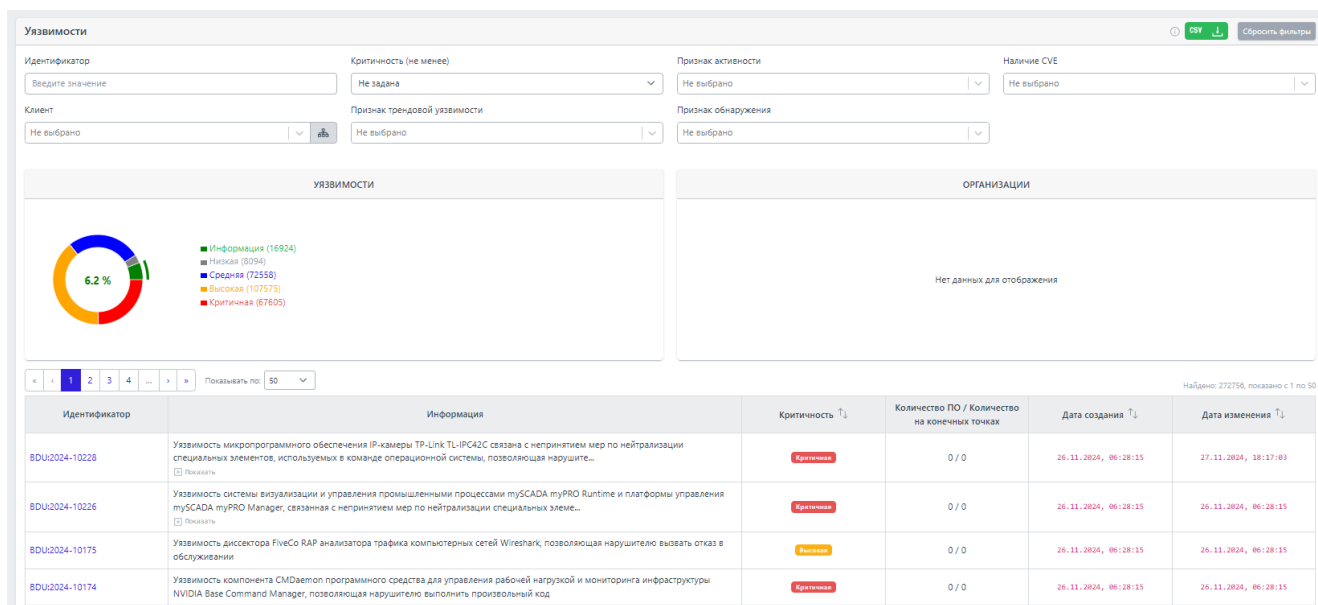


Рисунок 88 – Страница Уязвимости

На данной странице в виде таблицы представлена информация по найденным уязвимостям.

Таблица имеет следующие поля:

- Идентификатор (идентификация уязвимости по CVE);
- Информация (описание уязвимости);
- Критичность уязвимости;
- Количество ПО/Количество на конечных точках (в таблице отображается количество программ, в которых найдена данная уязвимость и количество конечных точек, на которых зарегистрировано ПО с данной уязвимостью);
- Дата создания;
- Дата изменения;

Для фильтрации информации в таблице имеются следующие фильтры:

- Идентификатор (в фильтре указывается идентификатор уязвимости в формате CVE);
- Критичность (не менее) (низкая, средняя, высокая, критичная);
- Признак активности (активирована, деактивирована);
- Наличие CVE (имеется, отсутствует);
- Признак трендовой уязвимости (обычная уязвимость, трендовая уязвимость).

В столбце **Идентификатор** трендовая уязвимость отмечена иконкой . Признаком того, что уязвимость является трендовой, можно выставить при редактировании уязвимости. Признаком выставляется аналитиком/администратором на основании анализа информации об уязвимости.

При нажатии в столбце **Идентификатор** по CVE-идентификатору уязвимости открывается информация об уязвимости, представленная на рисунке 89.

Сведения об уязвимости

CVE-2007-0865

БДУ ФСТЭК

NIST

Критичность

Критичная

Дата публикации

13.02.2008, 02:00:00

Дата изменения

06.09.2024, 10:54:28

Список CWE

CWE-44

Критерии соответствия уязвимости

Критерий соответствия: cpe2.3:microsoft/windows_2000*sp4*****

Критерий соответствия: cpe2.3:microsoft/windows_2003_server*1*****

Критерий соответствия: cpe2.3:microsoft/windows_2003_server*2*****

Критерий соответствия: cpe2.3:microsoft/windows_vista*****

Критерий соответствия: cpe2.3:microsoft/windows_xp*sp2*****

Критерий соответствия: cpe2.3:microsoft/office**mac**os*****

Критерий соответствия: cpe2.3:microsoft/visual_basic*6.0*sp6*****

Описание уязвимости по NIST

EN

Heap-based buffer overflow in Object Linking and Embedding (OLE) Automation in Microsoft Windows 2000 SP4, XP SP2, Server 2003 SP1 and SP2, Vista, Office 2004 for Mac, and Visual Basic 6.0 SP6 allows remote attackers to execute arbitrary code via a crafted script request.

Краткое содержание

Сводная информация и базовые метрики

CVSS Version 3.x

CVSS Version 2.0

Источник	nvd@nist.gov
Тип	Перестроенный
Версия CVSS	2.0
Оценка	10
Показатель эксплуатационной способности	10
Показатель воздействия	10
Вектор атаки	AV:N/AC:L/AU:N/C:C/SC:N/EC:N
Тип вектора	Сетевой (N)
Сложность доступа	Низкая (L)
Аутентификация	Не требуется (N)
Влияние на конфиденциальность	Полное (C)
Влияние на целостность	Полное (C)
Влияние на доступность	Полное (C)

Дополнительная информация

URL	Источник	Теги
http://marc.info/?l=bugtraq&m=120561015026386&m=2	cve@mitre.org	
http://secunia.com/advisories/28902	cve@mitre.org	

Рисунок 89 – Информация по уязвимости

На данной странице информация по уязвимости представлена в двух вкладках БДУ ФСТЭК и NIST. Также по уязвимости можно просмотреть информацию по описанию CWE, перейдя по активной ссылке, подсвеченной синим цветом (**Список CWE: CWE-259**).

Данная ссылка находится в поле рядом с полем, где указывается дата публикации и изменения информации по уязвимости.

При нажатии по иконке  пользователь загружает на компьютер, с которого осуществлен вход в модуль администрирования RT Protect TI информацию о всех найденных уязвимостях в организации в Excel-формате.

6.8.3. Программы

Общий вид страницы **Программы** сервиса RT Protect TI возможно просмотреть в двух вариантах отображения.

Для переключения режима отображения используется иконка «Выбрать режим агрегации»  / .

В первом варианте название программы и их модификации отображаются по группам в формате CPE (см. рис 90).

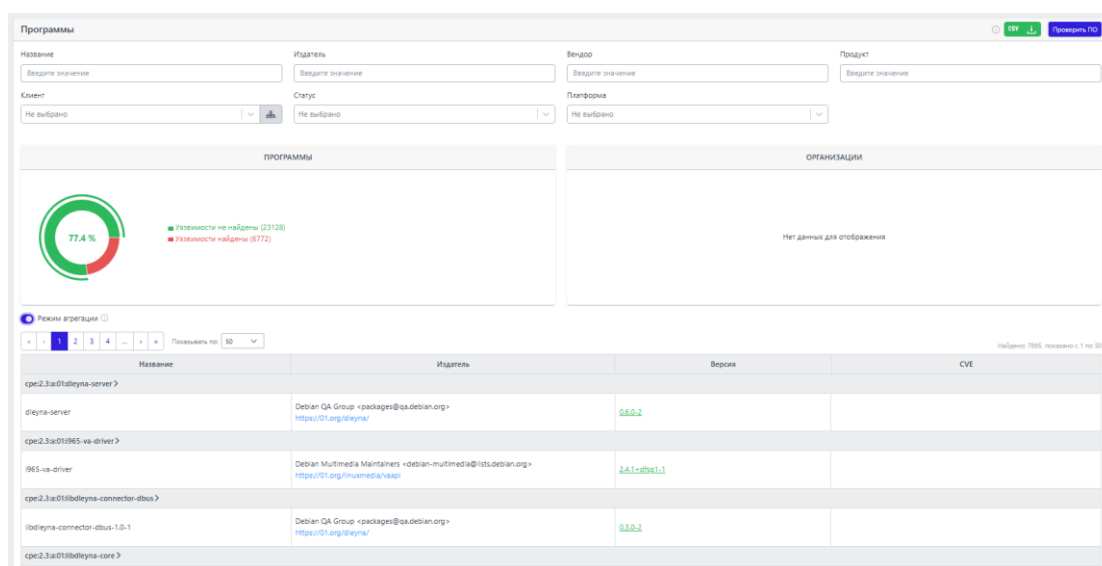


Рисунок 90 – Отображение страницы Программы
(название программы в формате CPE)

На странице имеются следующие области:

- Область с указанием параметров фильтрации;
- Область с графическим отображением для программ (уязвимости найдены/уязвимости не найдены);
- Область с графическим отображением организаций, в установленных программах которых найдены уязвимости;
- Таблица с информацией о программах, которые проанализированы на предмет уязвимостей.

На странице «Программы» в табличной форме представлена информация о программах, которые проанализированы на предмет уязвимостей.

Таблица имеет следующие поля:

- Название (указывается идентификация программы в формате CPE)
- Издатель;
- Версия (версия ПО);
- CVE (описание уязвимостей, найденных для программы в формате CVE с указанием критичности).

CPE (описание программ по стандарту для машиночитаемого именования и идентификации всех видов программного обеспечения (софта) и устройств).

В таблице **Программы**, если программа имеет несколько версий, в столбце CVE отображаются все уязвимости в формате CVE, найденные для программы (рисунок 91).

libpoppler-glib8 	Debian freedesktop.org maintainers <pkg-freedesktop-maintainers@lists.aliases.debian.org> https://poppler.freedesktop.org/	22.02.0-2ubuntu0.5  22.12.0-2+b1  22.02.0-2 	CVE-2021-30860  CVE-2022-38171  CVE-2022-38784  CVE-2024-6239 
--	--	---	---

Рисунок 91 – Пример отображения таблицы с уязвимостями для версий программы

Рядом с версией программы имеется иконка , при нажатии по которой можно просмотреть уязвимости для конкретной версии программы.

Во втором режиме отображения таблицы с проанализированными программами название программы отображается в обычном виде (рисунок 92).

Программы

Название

Введите значение

Издатель

Введите значение

Версия

Введите значение

Продукт

Введите значение

Организация

Не выбрано

Ключ

Не выбрано

Статус

Не выбрано

Платформа

Не выбрано

ПРОГРАММЫ

81.6 %

Уязвимости не найдены (22623)

Уязвимости найдены (5118)

Организация

41.8 %

Интерфакс (3674)

ТМД «Аэрофлот» (5118)

Режим агрегации

Показать по: 50

Название	Издатель	Версия	CPE	Распространенность на конечных точках	Время сканирования	CVE
Yandex	Yandex	24.10.4.756	cpe:2.3:ayenderxindex_bookreader:24.10.4.756:****	1	27.11.2024, 10:18:33	
Yandex	Yandex	24.10.3.825	cpe:2.3:ayenderxindex_bookreader:24.10.3.825:****	4	27.11.2024, 10:18:33	
Mozilla Firefox 124.0	Mozilla https://www.mozilla.org	132.0.2	cpe:2.3:mozilla:firefox:132.0.2:****:x64	4	26.11.2024, 00:18:37	CVE-2022-45868 11 CVE-2022-42126 11 CVE-2022-34889 11 CVE-2022-13887 11
Mozilla Firefox 124.0	Mozilla https://www.mozilla.org	133.0	cpe:2.3:mozilla:firefox:133.0:****:x64	1	26.11.2024, 00:18:37	CVE-2022-45868 11 CVE-2022-42126 11 CVE-2022-34889 11 CVE-2022-13887 11

Рисунок 92 – Отображение страницы программы (название программы в обычном формате)

В таблице для удобного представления и быстрого анализа названия программ выделены различными цветами:

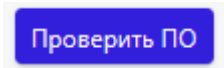
- Программы, в которых имеются уязвимости (шрифт красного цвета, например, [Microsoft Edge](#));
- Программы, в которых отсутствуют уязвимости (шрифт зеленого цвета, например, [Windows SDK](#)).

Таблица имеет следующие поля:

- Название;
- Издатель;
- Версия;
- CPE (описание программ по стандарту для машиночитаемого именования и идентификации всех видов программного обеспечения (софта) и устройств);
- Распространенность на конечных точках;
- Время сканирования;
- CVE (описание уязвимостей, найденных для программы в формате CVE с указанием критичности).

Для фильтрации информации на странице **Программы** для обоих вариантов отображения используются следующие фильтры:

- Название (в области фильтра задается имя программы);
- Издатель;
- Продукт;
- Вендор;
- Организация;
- Клиент;
- Статус (не задан, уязвимости не найдены, уязвимости найдены, в процессе анализа, ошибка при формировании CPE, ошибка при сканировании);
- Платформа (Linux/Windows).

В правом верхнем углу страницы **Программы** имеется иконка  , при нажатии по которой открывается окно для задания параметров для проверки новой программы, отсутствующей в списке (рисунок 93).

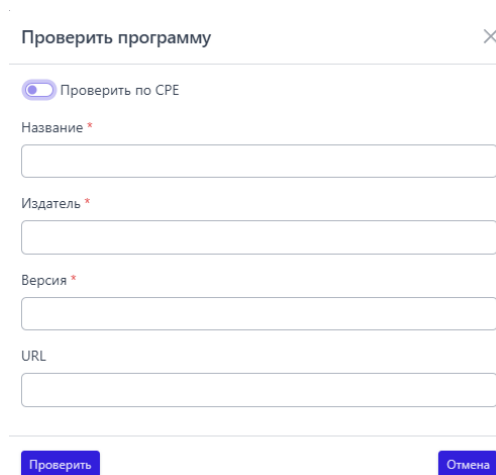


Рисунок 93 – Окно задания параметров проверяемой программы

В данном окне требуется задать параметры проверяемой программы и нажать по иконке **Проверить**.

Окно задания параметров для проверки программы при нажатии по иконке



имеет вид, представленный на рисунке 94.

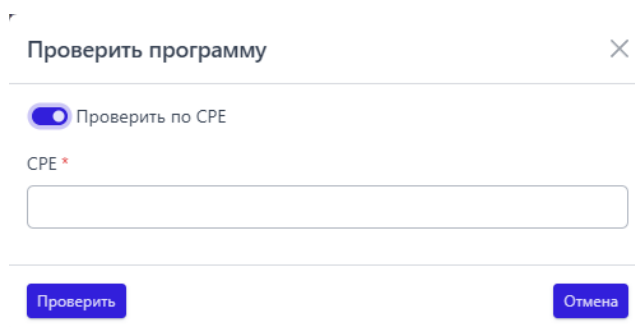


Рисунок 94 – Проверка программы, заданной в формате CPE

В данном окне после указания программы в формате CPE требуется нажать по иконке **Проверить**.

При нажатии по иконке с названием программы на странице **Программы**, происходит переход на страницу сведений о программе, представленную на рисунке 95.

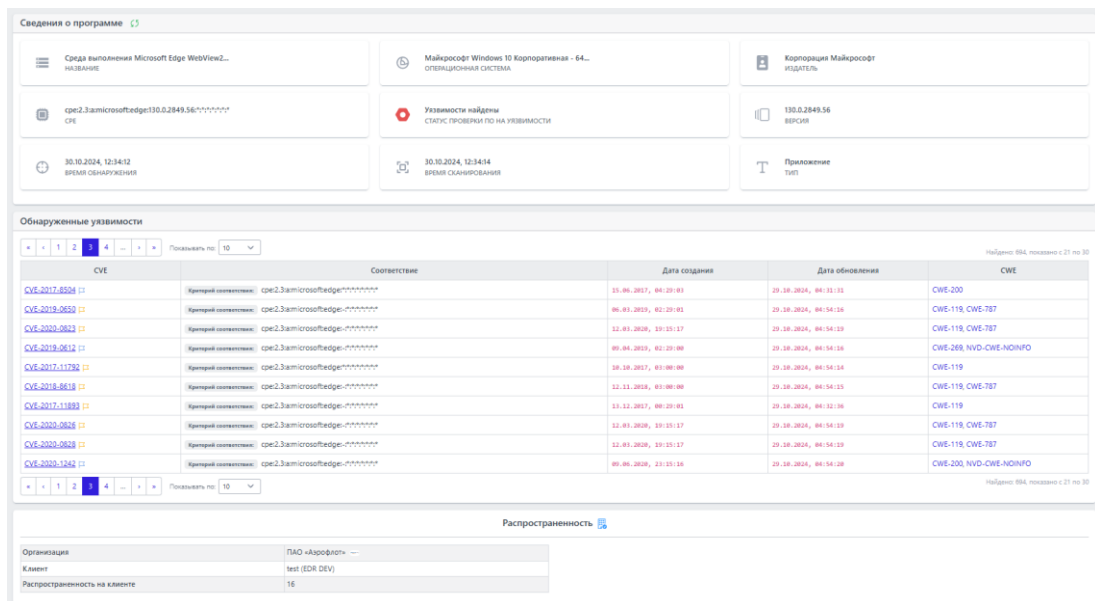


Рисунок 95 – Сведения о программе

На данной странице сведения о программе представлены в следующих областях:

- Общие сведения о программе;
- Таблица с обнаруженными уязвимостями;
- Распространенность (показывается распространенность программы с уязвимостями у различных клиентов).

Идентификатор уязвимости в CVE-формате является активной ссылкой, при нажатии по которой открывается страница с описанием уязвимости, представленная на рисунке 96.

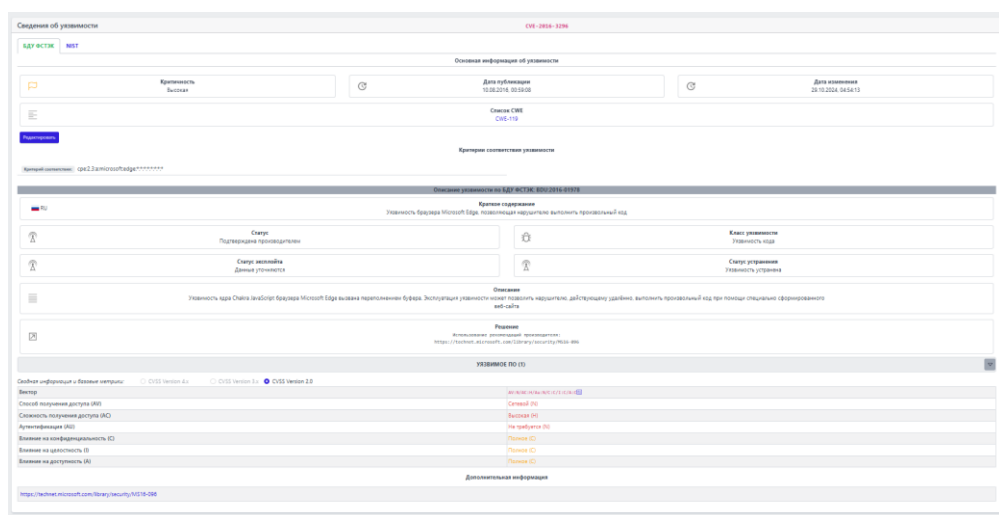


Рисунок 96 – Сведения об уязвимости

На данной странице сведения об уязвимости представлены от различных источников: БДУ ФСТЭК и NIST. Для отображения информации по уязвимости от источников требуется нажать по иконке  .

На странице информации об уязвимости при нажатии по иконке  происходит переход на страницу с описанием уязвимости в CWE-формате.

6.9 Параметры

6.9.1. Журнал действий

На странице **Журнал действий пользователей** в табличном виде представлена информация о действиях пользователей (в рамках организации, указанной в разделе **Организации**) (рис. 97).

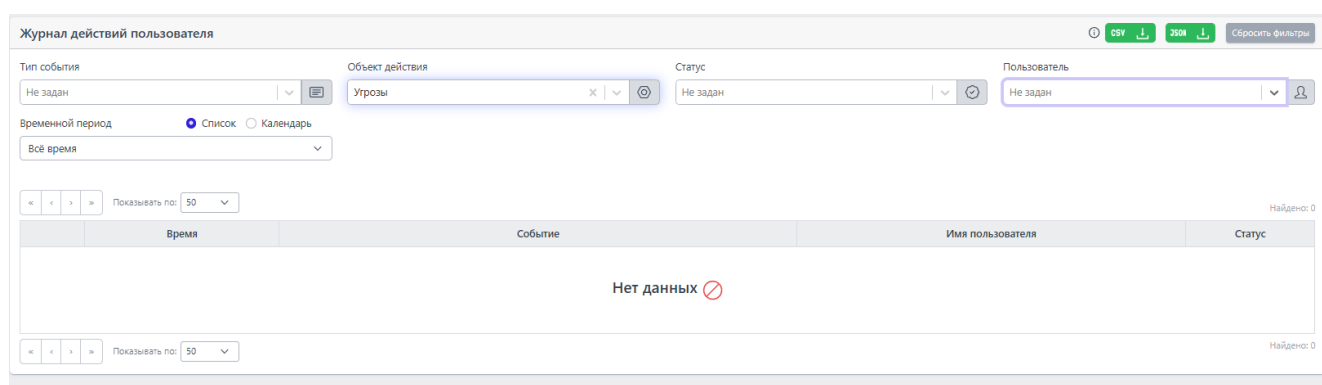


Рисунок 97 – Журнал действий пользователя

Таблица представлена следующими полями:

- иконка  (при нажатии отображается информация о событии);
- **Время** (отображается время регистрации события);
- **Событие** (отображаются события в формате «Объект действия: Тип события», например, «Индикатор атаки: Создание записи»);
- **Имя пользователя** (отображается имя пользователя, который произвел определенное действие);
- **Статус** (отображается статус действия или события).

Над таблицей с целью удобства и фильтрации информации, отображающейся в таблице, имеется система фильтров, представленная следующими фильтрами:

- 1) Тип события:

- Создание записи;
- Модификация записи;
- Удаление записи;
- Вход в систему;
- Выход из системы.

2) Объект действия:

- Источник;
- Пользователь;
- Токен;
- Угрозы.

3) Временной период (начало);

4) Временной период (окончание);

5) Статус (успешно/неудачно).

Фильтрацию информации в таблице можно производить как по одному из фильтров, так и по комбинации фильтров.

При нажатии ЛКМ по иконке  открывается более подробное описание события. Информация о событии может отображаться в двух форматах (HTML/JSON). Для переключения формата отображения используется иконка .

На рисунке 98 отображается информация о событии в формате HTML.

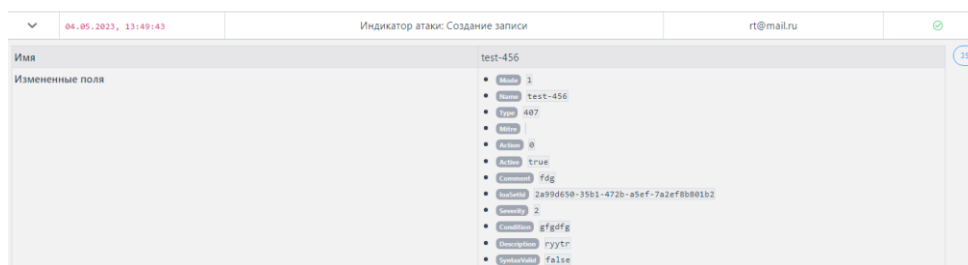


Рисунок 98 – Отображение информации о событии в формате HTML

На рисунке 99 отображается информация в формате JSON.

7. Сообщения администратору

7.1 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.

7.2 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.

7.2.1. Общие сообщения

Общие сообщения – универсальные сообщения, которые выводятся в тех ситуациях, когда ошибка была обработана особым 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 100.

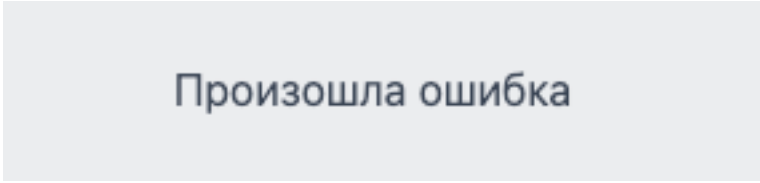


Рисунок 100 – Сообщение об ошибке типа «Экран ошибки»

Такие сообщения выводятся в том случае, если ошибка возникла внутри приложения, в логике работы одного из его компонентов.

При этом обработка ошибок в приложении строится таким образом, чтобы по возможности локализовать те компоненты, в которых возникают ошибки, и остальные части приложения работали нормально.

Например, ошибка может возникнуть в одном из компонентов футера. В этом случае на футере будет выведен текст «Произошла ошибка». При этом остальная часть страницы будет выглядеть как обычно и сохранит работоспособность, если это возможно.

Возможна ситуация, при которой ошибка возникла в корневом компоненте приложения. В этом случае текст «Произошла ошибка» будет отображаться по центру экрана.

Возможные причины: ошибки в логике работы приложения внутреннего характера.

Действия по устранению: обновить страницу, сообщить администратору.

Сообщение об ошибке типа «Экран ошибки» также может иметь вид, представленный на рисунке 101.

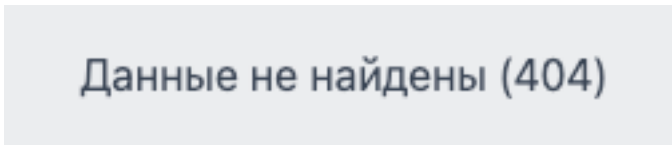


Рисунок 101 – Сообщение об ошибке

Данное сообщение отображается по центру экрана и выводится в том случае, если приложение не может осуществить роутинг и открыть нужный экран (в адресной строке введен неизвестный путь).

Возможные причины: несоответствие версии приложения, ввод некорректного пути в адресной строке вручную, ошибки роутинга в приложении.

Действия по устранению: перейти на главную страницу, сообщить администратору.

Пример сообщения типа «Всплывающее сообщение об ошибке» показан на рисунке 102.

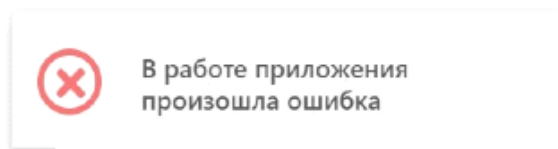


Рисунок 102 – Всплывающее сообщение об ошибке

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.

7.2.2. Специфичные сообщения

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

Страница «Пользователи»

1) Ошибка при удалении пользователя (выводимое сообщение «Ошибка при удалении пользователя» представлено на рисунке 103).

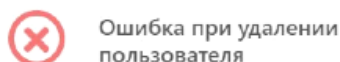


Рисунок 103 – Ошибка при удалении пользователя

Возможная причина: некорректный ответ сервера.

Возможные действия по устранению: убедиться в наличии связи с сервером, перезагрузить страницу, повторить действие.

2) Ошибка сброса пароля (выводимое сообщение «Ошибка сброса пароля» представлено на рисунке 104).



Рисунок 104 – Ошибка сброса пароля

Возможная причина: некорректный ответ сервера.

Возможные действия по устранению: убедиться в наличии связи с сервером, перезагрузить страницу, повторить действие.

Страницы раздела «Аналитика».

1) Ошибка: неверный формат файла.

Выводимое сообщение представлено на рисунке 105.

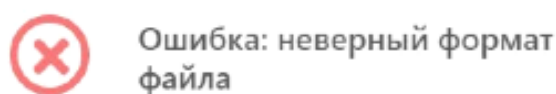


Рисунок 105 – Неверный формат файла

Возможная причина: неверный формат импортируемого файла, некорректный ответ сервера.

Возможные действия по устранению: убедиться, что файл имеет корректный формат, убедиться в наличии связи с сервером, перезагрузить страницу, повторить действие.

Экран авторизации

1) Сообщение об ошибке при вводе неправильных учетных данных представлено на рисунке 106.



Рисунок 106 – Сообщение об ошибке при вводе неправильных учетных данных

Возможные причины: вводятся неправильные учетные данные, пользователь был удален.

Действия по устранению: сообщить администратору, убедиться, что пользователь не был удален из системы.

2) Уведомление о том, что пользовательская сессия была завершена (принудительный выход) представлено на рисунке 107.

Сессия была завершена. Требуется повторная авторизация

Рисунок 107 – Уведомление о завершении сессии пользователя

Данная ситуация не является ошибкой.

Возможные причины: пользователь не был активен в течение определенного времени, истекло время жизни сессии (оно составляет несколько дней).

Действия по устранению: осуществить повторный вход в систему.

8. Действия после сбоя и ошибки

8.1 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 серверной части.

Для устранения ошибки требуется обратиться к поставщику программы.

9. Перечень сокращений

Основные сокращения, указанные в документе, представлены в таблице 6.

Таблица 6 – Перечень сокращений

ИС	Информационная система
ИТ	Информационная технология
ЛКМ	Левая кнопка мыши
ПКМ	Правая кнопка мыши
ПО	Программное обеспечение
ФСТЭК	Федеральная служба по техническому и экспортному контролю
ЦП	Центральный процессор
APT	Advanced Persistent Threat (постоянная серьезная угроза)
ID	Identifier (идентификатор)
IT	Information Technology (информационные технологии)
NSRL	National Software Reference Library (Национальная справочная библиотека программного обеспечения)
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)
URL	Uniform Resource Locator

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