# RT Protect TI

## Руководство администратора

Версия 1.0.20 от 17 октября 2024
Разработано компанией АО «РТ-Информационная безопасность»

RT Protect

# Оглавление

# 1. Общие положения

## 1.1 Идентификация документа

Данное руководство кратко можно идентифицировать согласно таблице 1.

**Таблица 1 – Идентификация документа**

| | |
|---|---|
| Название документа | «RT Protect TI»<br>Руководство Администратора |
| Версия документа | Версия 1.0.20<br>(актуальна для версии продукта<br>frontend 0.8.3/backend 2.9.4) |
| 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) 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 | Анализируемые TI-платформой объекты, которые потенциально могут являться вредоносными или содержать вредоносное содержимое. В данный момент поддерживаются следующие типы: 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-потоком или другими данными |
| WHOIS | Сетевой протокол прикладного уровня, базирующийся на протоколе TCP. Основное применение – получение регистрационных данных о владельцах доменных имён, IP-адресов и автономных систем |

| Термин | Описание |
|---|---|
| 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 |
|  | Информация, требующая внимания пользователя |
|  | 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, взаимодействующих с сервисом;

– администрирование организаций, взаимодействующих с сервисом;

– подключение различных источников данных с информацией о вредоносных или безопасных артефактах;

– формирование аналитики различных форматов для распространения клиентам TI-портала через API;

– получение вердикта по анализируемым артефактам;

– регистрация действий пользователей.

Программа функционирует под управлением ОС Linux Ubuntu 20.04.5 LTS.

Для распространения сервиса применяется две модели:

– on-premise (покупка дистрибутива и установка на мощностях клиента);

– on-cloud (установка и развертывание 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 осуществлять проверку поддерживаемых платформой артефактов, просматривать отчеты по артефактам, 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, регистрирует новые организации, подключенные к сервису, подключает новые источники данных, предоставляющие информацию, и осуществляет другие функции, описанные в данном руководстве;

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

# 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 |
|---|---|---|---|
| | Сервис по предоставлению аналитики<br>Модуль администрирования<br>«RT Protect TI» | 1 | |
| | Комплект документов согласно списку:<br>– «Руководство Администратора RT Protect TI»<br>– «Руководство Аналитика RT Protect TI»<br>– «Руководство Пользователя RT Protect TI» | 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.

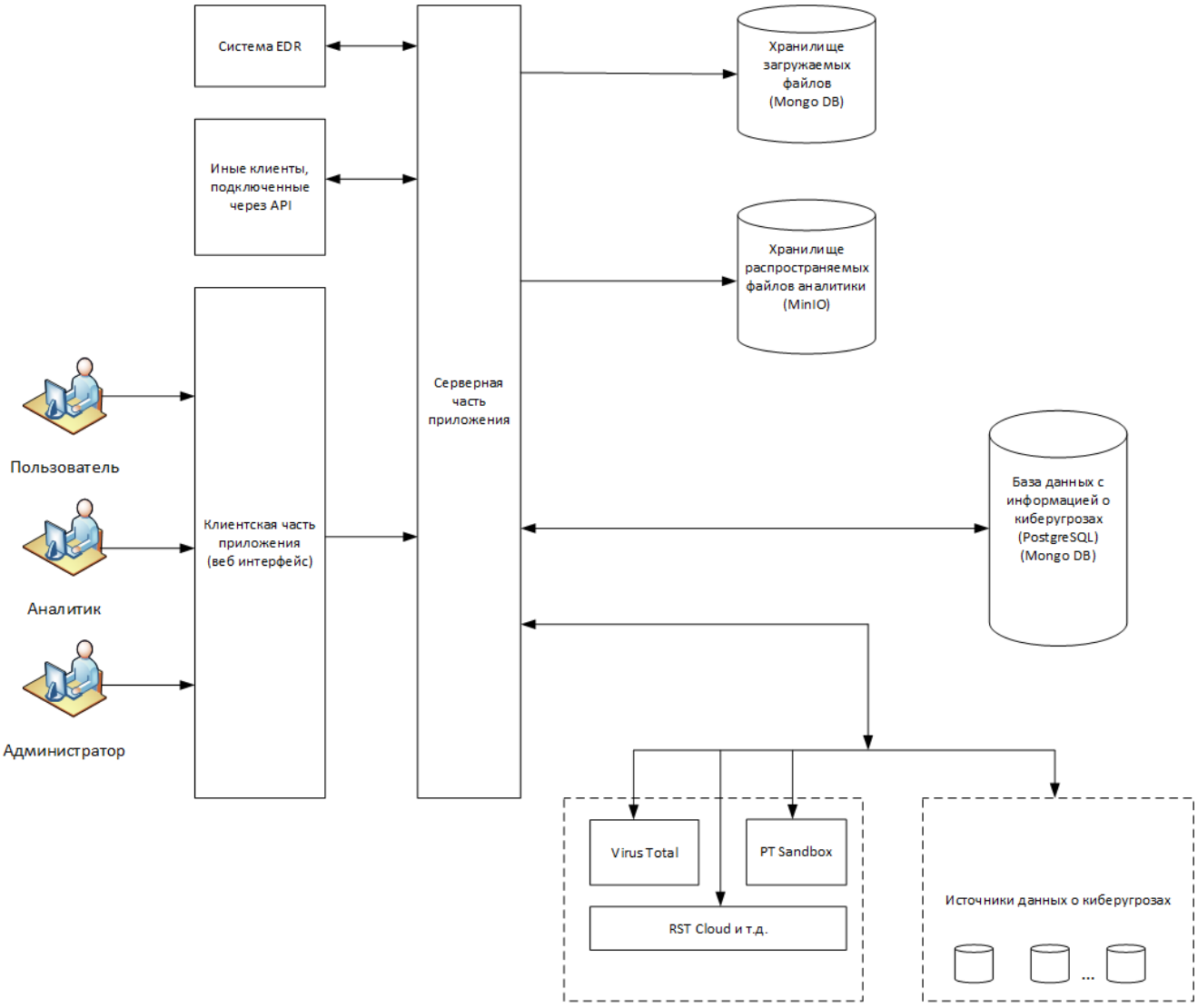



**Рисунок 1 – Схема архитектуры сервиса**

# 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 пригодна для функционирования на аппаратных платформах, указанных в таблице 5.

**Таблица 5 – Программно-аппаратное обеспечение**

| **Характеристики** | **Платформа** | |
|---|---|---|
| | Минимальные требования | Рекомендуемые требования |
| Процессор | Не менее 8 ядер частотой минимум 2,4 ГГц | Не менее 10 ядер частотой минимум 2,4 ГГц |
| Оперативная память | 16 ГБ | 32ГБ |
| Жесткий диск (свободное пространство) | 1 ТБ | 2 ТБ |

Программа поддерживает работу в браузерах, представленных в таблице 6.

**Таблица 6 – 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 Инструкция по развертыванию TI-платформы*

Шаг 1. Подготовка окружения

Для развертывания сервера понадобится ноутбук или любой другой компьютер, с установленным на нем программным обеспечением:

– Python (не ниже версии 3.10.0) [установка].

– Ansible (не ниже версии 5.7.1) [установка].

С компьютера должен быть доступ на сервер (Docker-хост) по SSH, а у удаленного пользователя права sudo (подойдет и root пользователь).

Для удобства использования Ansible добавьте свой открытый SSH-ключ на сервере, иначе вам может потребоваться установка дополнительной утилиты sshpass.

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

Шаг 2. Создание конфигурации сервера

Чтобы создать конфигурацию сервера, необходимо клонировать репозиторий на АРМ, на котором разворачивается сервер TI, перейдя по ссылке https://gitlab.rt-protect.ru/threat-intelligence/ti-deploy, либо осуществите запрос на получение данного репозитория к контактным лицам от поставщика.

Далее необходимо перейти в корень репозитория ti-deploy.

Структура каталогов будет представлена на рисунке 2.

```
. (ti-deploy)
│
├── README.md
├── compose-files
│   ├── docker-compose.yml
│   └── env.j2
├── config
│   └── default
│       ├── config.yml
│       ├── docker-compose.override.yml
│       ├── server.crt
│       └── server.key
├── ti-install.yml
└── ti-update.yml
```

**Рисунок 2 – Структура каталогов репозитория ti-deploy**

В каталоге config хранятся конфигурации серверов. Сюда нужно будет добавить свою новую конфигурацию. Следует обратить внимание, что каталог config не отслеживается гитом (записан в .gitignore) (кроме подкаталога default), поэтому можно добавлять свои собственные конфигурации в любом количестве и не бояться, что чувствительные данные из них попадут в общий репозиторий.

Правильным подходом будет держать все свои конфигурации в одном месте, в каталоге config в соответствующих подкаталогах. Можно одновременно управлять несколькими конфигурациями серверов. Именовать подкаталоги удобно, например, по IP-адресу сервера или домену. Тогда структура каталога config со временем примет вид, представленный на рисунке 3.

```
. (config)
│
├── 192.168.113.60           <- каталог не отслеживается гитом, хранится только на вашем компьютере
│   ├── config.yml
│   ├── docker-compose.override.yml
│   ├── server.crt
│   └── server.key
├── 192.168.113.7           <- каталог не отслеживается гитом, хранится только на вашем компьютере
│   ├── config.yml
│   ├── docker-compose.override.yml
│   ├── server.crt
│   └── server.key
└── default
    ├── config.yml
    ├── docker-compose.override.yml
    ├── server.crt
    └── server.key
```

**Рисунок 3 – Структура каталога config**

В данной структуре имеется две дополнительные конфигурации (помимо дефолтной): для сервера 192.168.113.60 и для сервера 192.168.113.7. Теперь следует создать свой подкаталог в каталоге config и скопировать в него содержимое каталога config/default:

– config.yml – настройки конфигурации;

– docker-compose.override.yml – compose-файл, дает возможность переопределить основной compose-файл на уровне отдельной конфигурации;

– server.crt – открытый сертификат сервера в формате PEM;

– server.key – закрытый ключ сертификата в формате PEM.

Далее следует настроить содержимое каждого файла так, как требуется. Это и будет ваша конфигурация. В файле config.yml содержатся все доступные настройки, включая версии компонентов системы.

Несмотря на то, что docker-compose.yml уже есть и настроен правильно (находится в каталоге compose-files), пользователь, устанавливающий систему, может внести свои коррективы. Это можно сделать на уровне вашей конфигурации, отредактировав файл docker-compose.override.yml. Такие изменения не затронут другие конфигурации, это хороший уровень изоляции.

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

Шаг 3. Запуск скрипта развертывания (Ansible Playbook)

Когда все файлы конфигурации будут настроены, следует перейти в корень репозитория (ti-deploy). Рядом должен находиться файл ti-install.yml. Для запуска скрипта развертывания следует выполнить в консоли команду:

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

Описание аргументов команды:

– @config/192.168.113.60/config.yml – это путь до файла config.yml вашей конфигурации. 192.168.113.60 – это каталог конфигурации. Следует обратить внимание на знак @ в начале пути;

– 192.168.113.60 - это адрес сервера для доступа по SSH (Docker-хост). Следует обратить внимание на знак , в конце.

– username - это имя удаленного пользователя.

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

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

Начнется процесс развертывания TI-сервера. В начале может потребоваться ввести пароль для доступа по SSH. Введите пароль и нажмите Enter.

Других вопросов не будет, так как все параметры уже известны демону Ansible – он возьмет их из файла config.yml. Так что следует просто дождаться окончания работы.

Когда Ansible закончит работу, следует перейти в окно веб-браузера, набрать адрес сервера, и проверить подключение, затем выполнить вход в систему с логином и паролем: admin@admin.ru/defaultadminpassword1234567, и поменять пароль по умолчанию. Сервер готов к эксплуатации.

Шаг 4 (опциональный). Обновление сервера

Если требуется обновить TI-сервер (например, вы изменили версию компонента в config.yml), то выполните команду выше, но замените ti-install.yml на ti-update.yml. Остальную часть команды менять не нужно.

Пример:

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

### *5.3 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**.

Сотруднику с ролью «Пользователь» доступны следующие действия:

1) добавление для проверки артефактов в поле для проверки и просмотр отчетов по артефактам следующих типов:

– IP-адрес;

– доменное имя;

– URL;

– контрольная сумма файла (хеш-сумма);

– Email.

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

3) просмотр графического представления по статистике выполненных проверок (отчеты Virus Total, отчеты Public TI, добавленные хеш суммы, добавленные IP-адреса, добавленные файлы, добавленные доменные имена).

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:

– создание и редактирование аналитических данных;

– добавление и редактирование источников данных;

– добавление и редактирование исключений для программ и файлов.

Для пользователя с ролью «Аналитик» не доступны для просмотра и редактирования следующие разделы:

– в области **Администрирование** (**Пользователи**);

– в области **Параметры** (**Журнал действий, Интеграции, Лицензия.**).

Для пользователя с ролью «Аналитик» раздел Организации в области **Администрирование** доступен только для просмотра.

Администратор – уполномоченный сотрудник организации заказчика или SOC-центра. Администратор устанавливает сервис, а также настраивает программу в соответствии с настоящим документом для его корректной и полнофункциональной работы.

В круг типовых задач администратора входит:

– действия, доступные пользователям с ролями «Аналитик» и «Пользователь»;

– редактирование и добавление подключенных к сервису организаций;

– редактирование и добавление пользователей, осуществляющих вход в модуль администрирования программы;

– просмотр действий пользователей, зарегистрированных в системе;

– поддержание администрируемой системы в рамках выбранной политики безопасности;

– обеспечение должного уровня конфиденциальности и целостности данных;

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

– создание и поддержание в актуальном состоянии пользовательских учётных записей;

– ответственность за информационную безопасность в компании;

– отслеживание информации об уязвимостях системы и своевременное принятие мер;

– периодическое практическое тестирование защищенности системы;

– документирование своей работы;

– устранение неполадок в системе.

# 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. 4).


**Рисунок 4 – Окно авторизации**

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 5

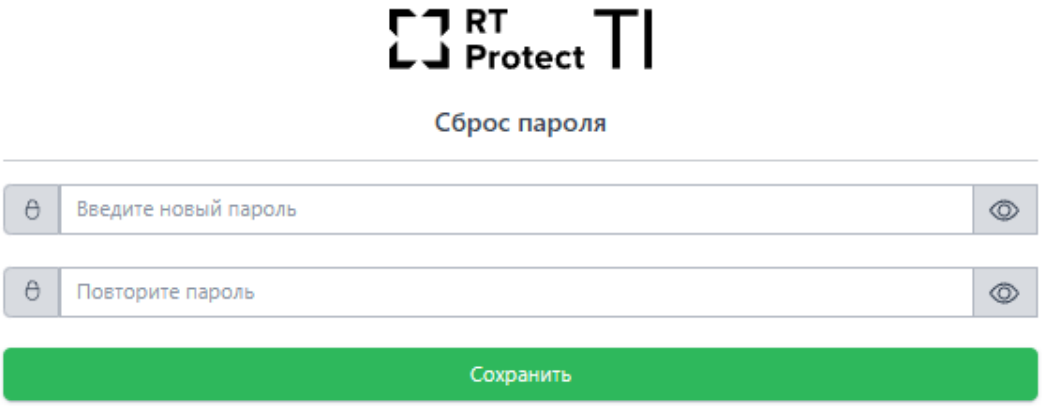



**Рисунок 5 – Окно ввода параметром для сброса пароля**

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. 6).

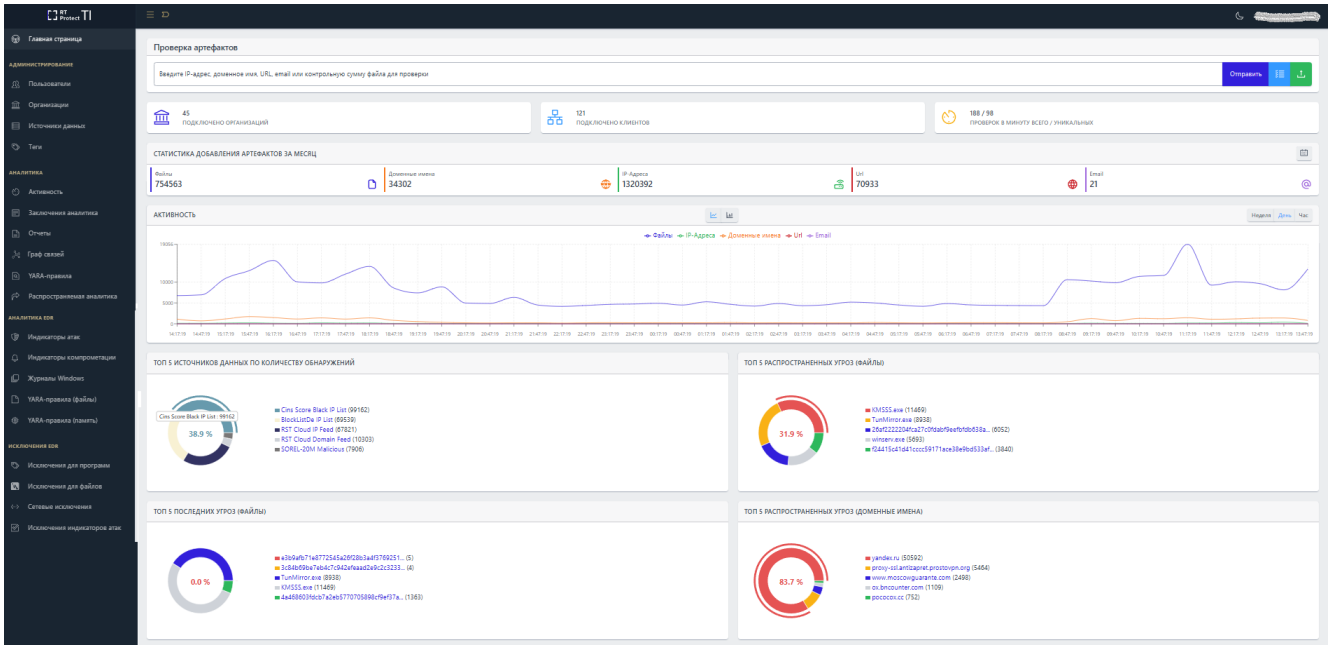



**Рисунок 6 – Основное окно программы**

Если в течение 5 минут пользователь выполнил 3 неудачных попытки входа, авторизация для него будет недоступна в течение 5 минут.

Функции, доступные в интерфейсе административного модуля управления:

– анализ передаваемых артефактов (IP-адресов, файлов, доменных имен, URL, Email) и просмотр отчетов по ним;

– администрирование пользователей и организаций, взаимодействующих с сервисом;

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

– работа с распространяемой аналитикой различных типов (индикаторы атак, индикаторы компрометации, yara-правила, журналы Windows, исключения для программ, исключения для файлов, сетевые исключения);

– просмотр действий пользователей, произведенных в модуле администрирования программы.

В левой части основного окна программы (см. рис. 6) 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 – RT Protect © 2024. Справа от текущей версии программы отображается надпись о том, где «RT Protect TI» разработана – Сделано в России.

### *6.2 Горизонтальная панель управления*

В верхней части окна находится горизонтальная панель управления (рис. 7).

**Рисунок 7 – Горизонтальная панель управления**

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

При нажатии кнопки **Скрыть/показать панель разделов** ( ) основное окно программы приобретает вид, как показано на рисунке 8. Для возврата первоначального вида необходимо повторно нажать на кнопку .

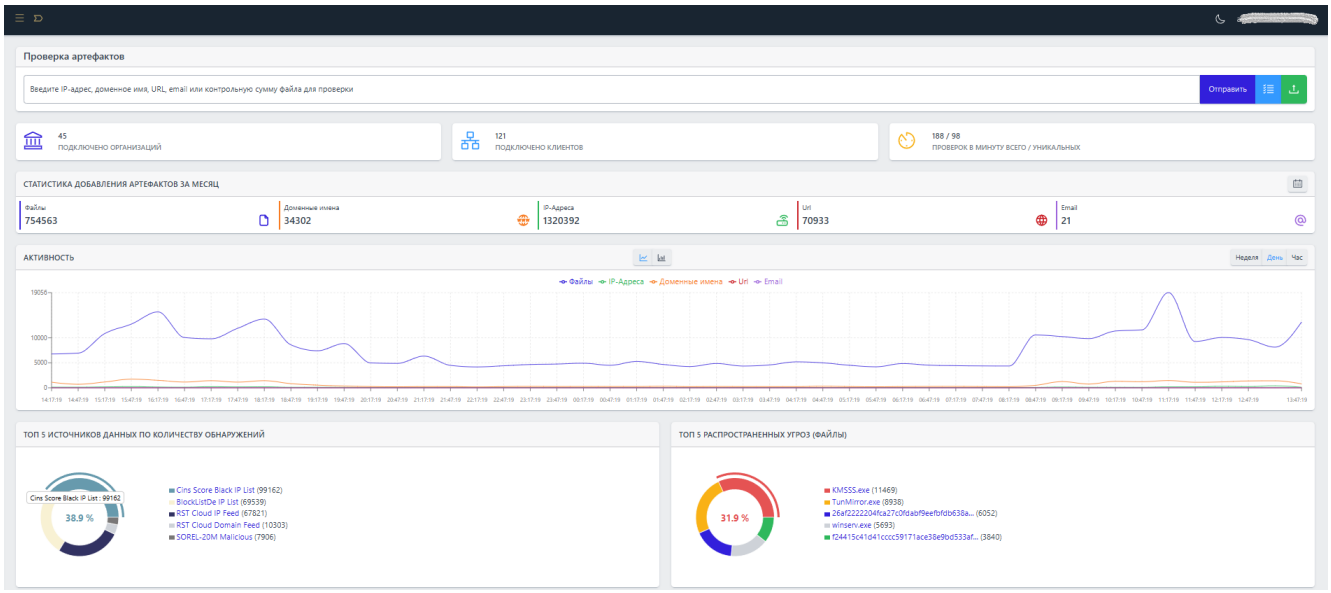



**Рисунок 8 – Основное окно программы при скрытой панели разделов**

При нажатии по иконке  в нижней части горизонтальной панели отображается, на какой странице с уровнем вложенности находится пользователь, например, Главная / Источники данных / Abuse MalwareBazaar.

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.

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** и кнопка **Выход** для выхода из программы с текущего устройства (рис. 9).

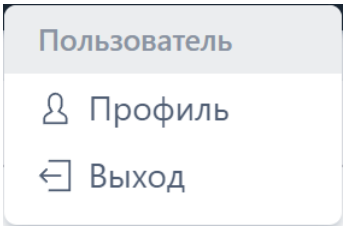



**Рисунок 9 – Меню «Пользователь»**

Подменю **Профиль** представлено на рисунке 10.

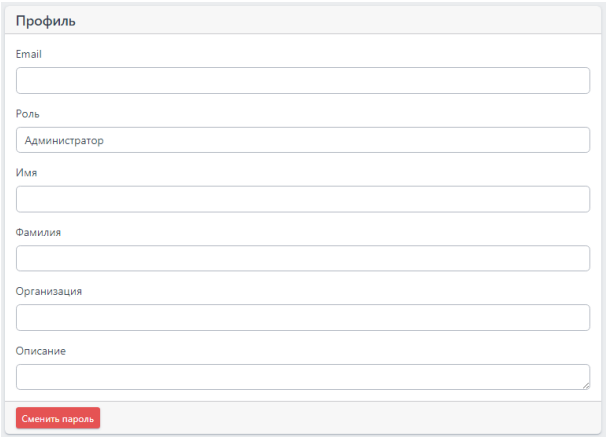



**Рисунок 10 – Подменю «Профиль»**

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).

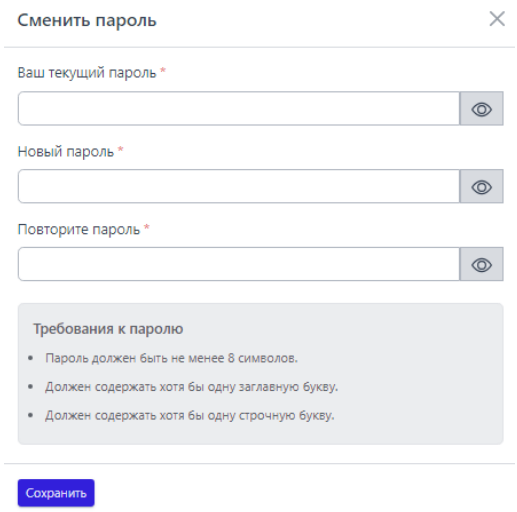



**Рисунок 11 – Окно смены пароля**

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.

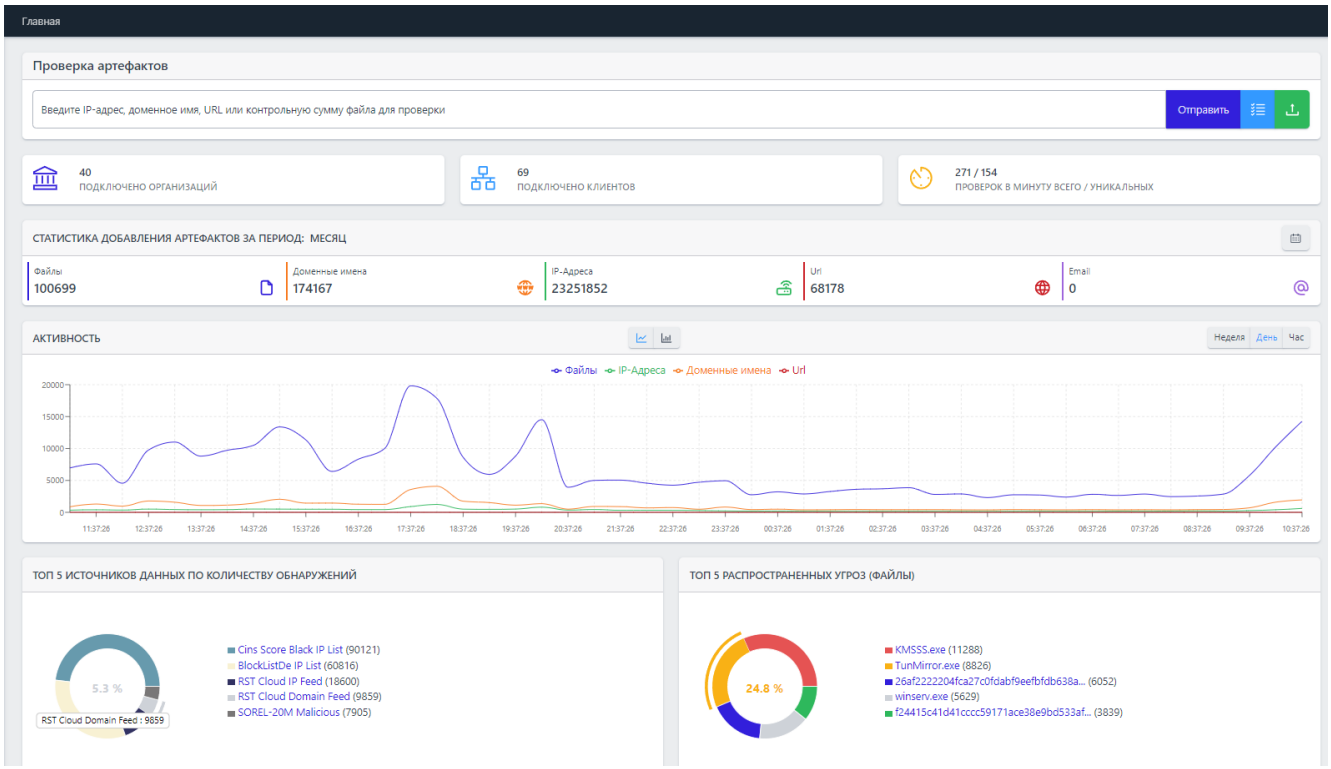



**Рисунок 12 – Главная страница**

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

– область проверки артефактов;

– информация о подключенных организациях и клиентах (сервиса);

– информация о количестве проверок в минуту (всего/уникальных);

– статистика добавления артефактов за период (по умолчанию – 1 месяц);

– графическое представление активности (отображение обнаружений);

– графические отображения Топ 5 источников данных по количеству обнаружений;

– графические отображения Топ 5 распространенных угроз по различным типам артефактов (файлы, доменные имена, IP-адреса, Email);

– графические отображения Топ 5 последних угроз по различным типам артефактов (файлы, доменные имена, IP-адреса, Email);

– графические отображения количества полученных отчетов от различных сторонних сервисов по анализу артефактов (Virus Total, Public TI);

– графические отображения количества добавленных для анализа различных артефактов по типам (IP-адреса, контрольные суммы, доменные имена, файлы).

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 кнопку **Отправить**.

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

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 13.

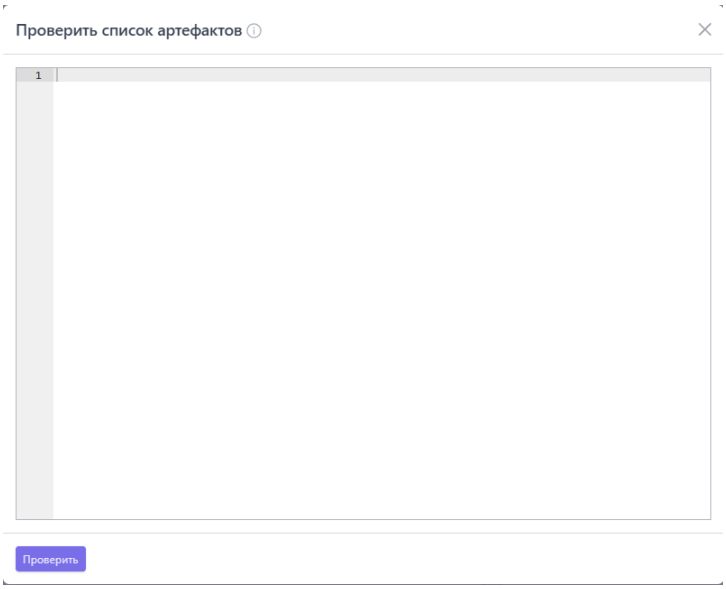



**Рисунок 13 – Окно для добавления списка артефактов для проверки**

В данном окне артефакт добавляется по одному в каждой строчке (строчки нумеруются). Проверка артефактов списком ограничена количеством в 100 строк. После написания артефактов, требуется нажать по иконке «Проверить».

В области **Статистика добавления артефактов** можно указать период, за который следует отображать информацию по статистике и нажать по иконке «Подтвердить».

### *6.4 Администрирование*

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

– **Пользователи;**

– **Организации;**

– **Источники данных;**

– **Тэги.**

Администратор может выполнять следующие действия:

– просматривать информацию о пользователях;

– создавать и удалять учетные записи пользователей;

– изменять параметры учетных записей пользователей;

– просматривать, создавать и удалять информацию об организациях, взаимодействующих с сервисом;

– просматривать, создавать и удалять клиентов, взаимодействующих с сервисом;

– просматривать, создавать, редактировать и удалять источники данных, из которых берется информация об артефактах;

– создавать и назначать теги для источников данных.

### 6.4.1. Пользователи

В разделе **Пользователи** в табличном виде показана информация обо всех зарегистрированных в программе пользователях (рисунок 14).

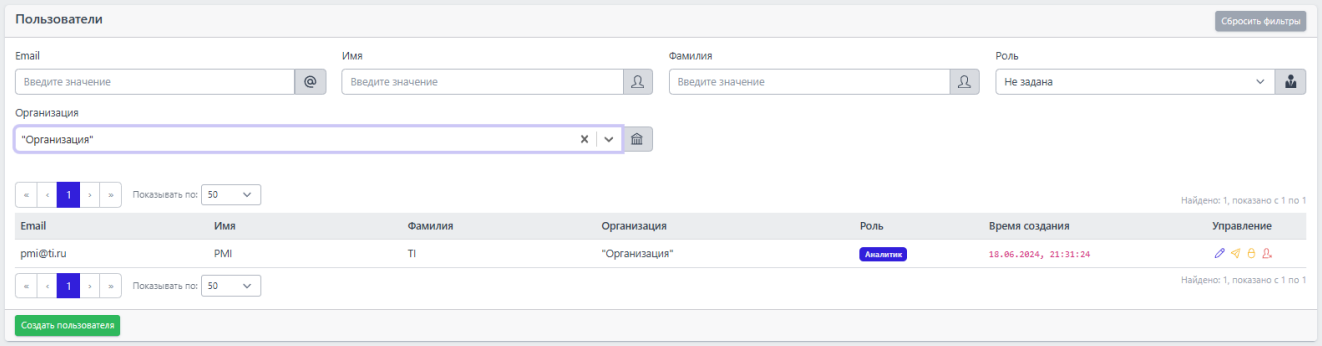



**Рисунок 14 – Раздел «Пользователи»**

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:

– **Показывать по**;

– **Имя**;

– **Фамилия**;

– **Email**;

– **Роль пользователя**;

– **Организация**.

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

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


**Рисунок 15 – 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 Сбросить фильтры.

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, организацию, которой принадлежит пользователь, а также изменить описание учетной записи (рис. 16).

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.

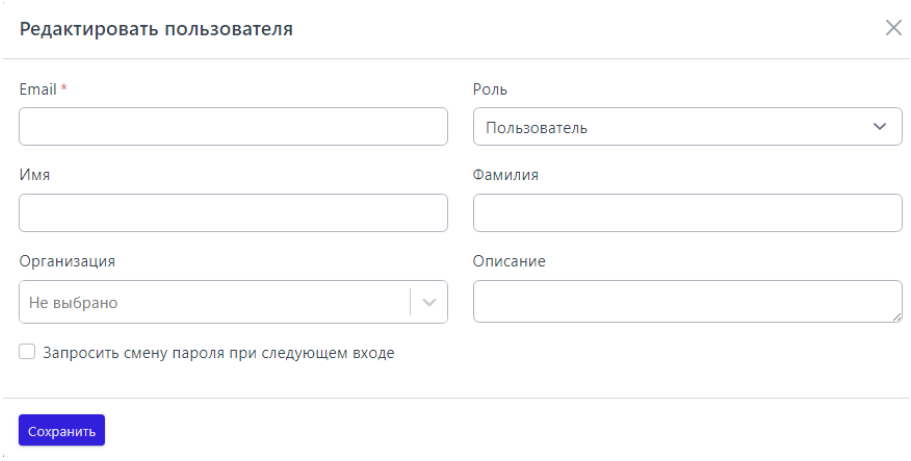



**Рисунок 16 – Окно редактирования пользователя**

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. 17).


**Рисунок 17 – Сообщение о сохранении данных пользователя**

При нажатии кнопки **Сменить пароль** открывается окно, представленное на рисунке 18. 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.

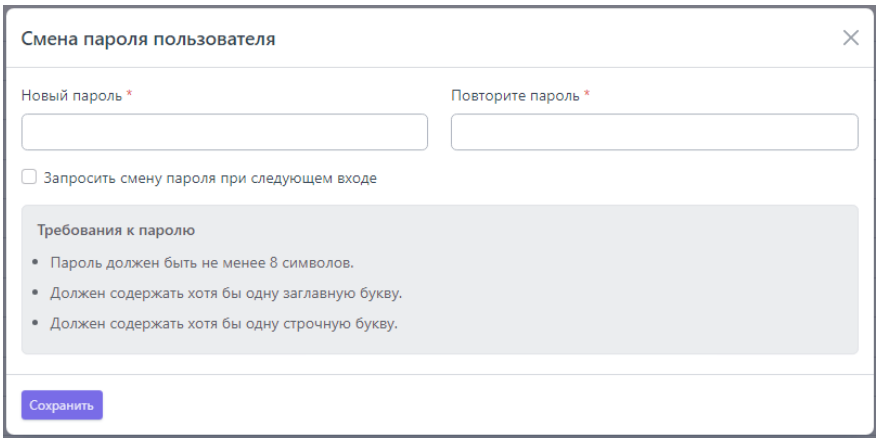
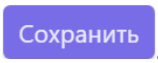



**Рисунок 18 – Окно «Смена пароля пользователя»**

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. 19). Для отмены удаления учетной записи необходимо нажать кнопку **Отмена** или закрыть окно.

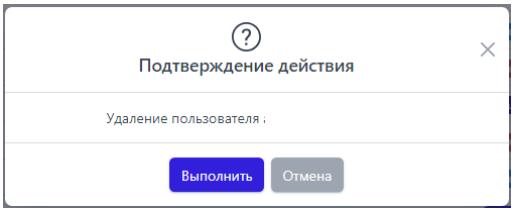



**Рисунок 19 – Окно подтверждения удаления пользователя**

После удаления учетной записи пользователя в нижней части основного окна программы появляется сообщение (рис. 20).

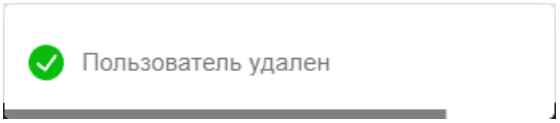



**Рисунок 20 – Сообщение об удалении пользователя**

В нижней части панели администрирования находится кнопка **Создать пользователя.** При нажатии кнопки открывается окно **Создать пользователя** (рис. 21).

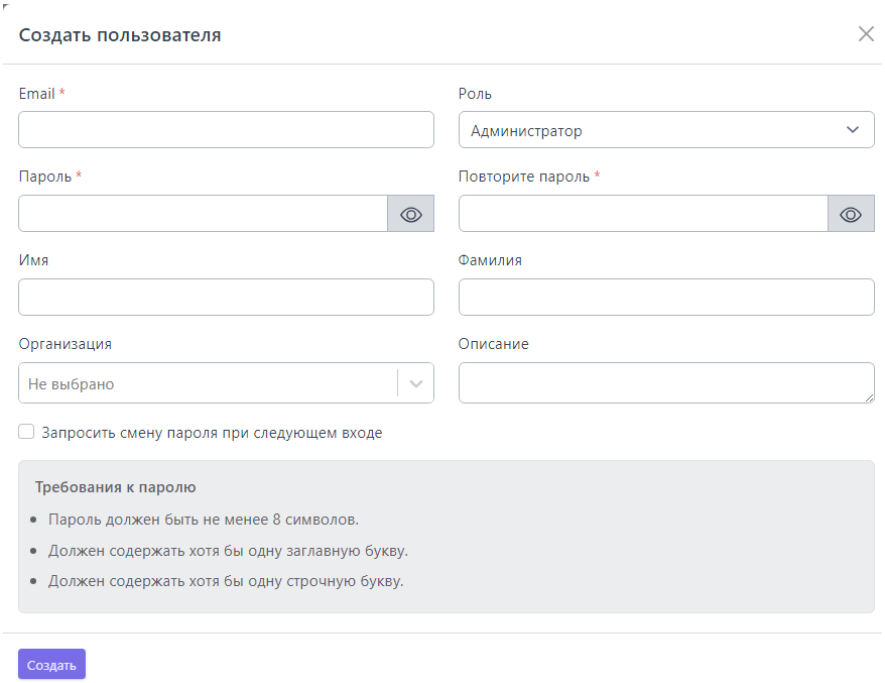



**Рисунок 21 – Окно создания нового пользователя**

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

– **Email;**

– **Роль;**

– **Пароль;**

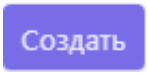
– **Повторить пароль;**

– **Имя;**

– **Фамилия;**

– **Организация;**

– **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. 22). Такое же сообщение выводится во всех полях, требующих ввода информации.

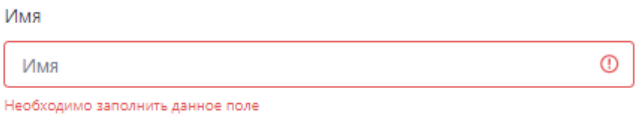



**Рисунок 22 – Сообщение о пустом поле ввода**

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. 23).

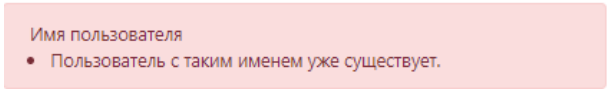



**Рисунок 23 – Сообщение о совпадении имени пользователя**

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. 24).

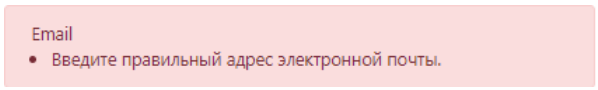



**Рисунок 24 – Сообщение о неправильном адресе электронной почты**

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. 25).

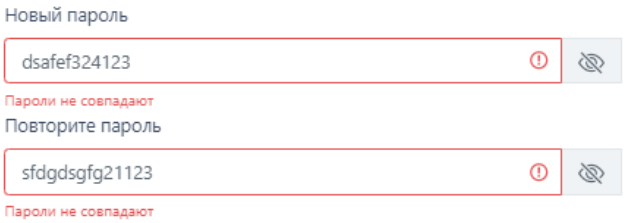



**Рисунок 25 – Сообщение о несовпадении паролей**

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. Организации

В разделе **Организации** в табличном виде показана информация обо всех организациях, подключенных к программе (рис. 26).

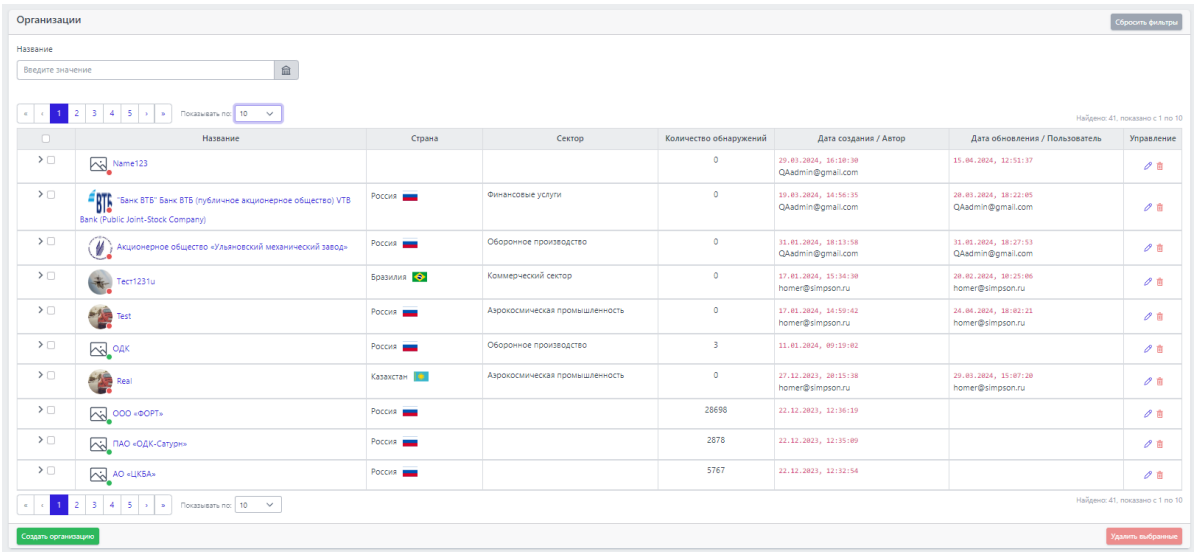



**Рисунок 26 – Окно раздела «Организации»**

Таблица имеет следующие поля:

– кнопка выбора элемента ( ☐ );

– **Название** (содержит название организации);

– **Страна;**

– **Сектор** (информация о подразделении в организации, подключенной к сервису);

– **Количество обнаружений;**

– **Дата создания/Автор;**

– **Дата обновления/ Пользователь;**

– **Управление.**

Для фильтрации информации в таблице предусмотрен фильтр по названию организации.

Элементы управления информацией в таблице аналогичны тем, что описаны в разделе **Пользователи.**

Название организации, например, «РТ-Информационная безопасность» является активной ссылкой, при нажатии по которой ЛКМ происходит переход на страницу редактирования информации об организации, представленную на рисунке 27.

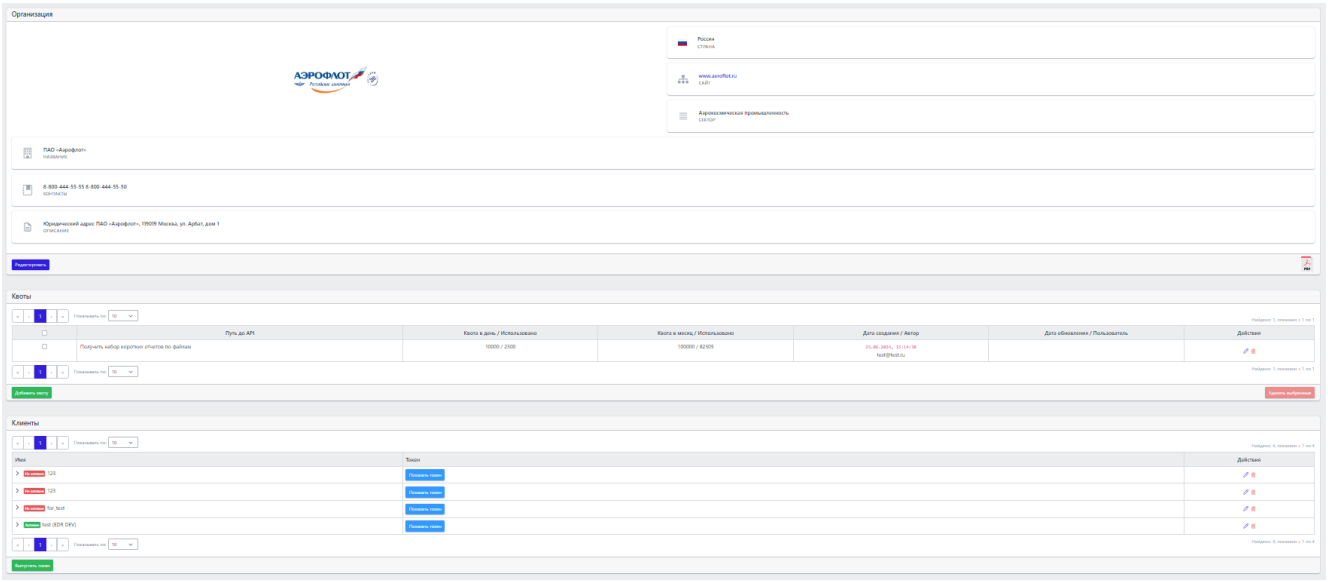



**Рисунок 27 – Окно редактирования информации по выбранной организации**

В окне редактирования имеются следующие области:

– **Организация**;

– **Квоты**;

– **Клиенты**.

В области **Организация** редактируется общая информация по организации.

В области **Организация** имеется иконка , показывающая, что данная организация является владельцем платформы (при наведении на данную иконку указателя мыши выводится соответствующее сообщение).

Также в данной области имеется иконка , позволяющая просмотреть/скачать отчет по организации в формате PDF за выбранный период.

В области **Квоты** имеется возможность добавить квоты (ограничения) по использованию API-вызовов для получения отчетов по проверке файлов, проверке доменов и другой информации. Область с указанием созданных квот представлена в табличном виде (см. рисунок 28).

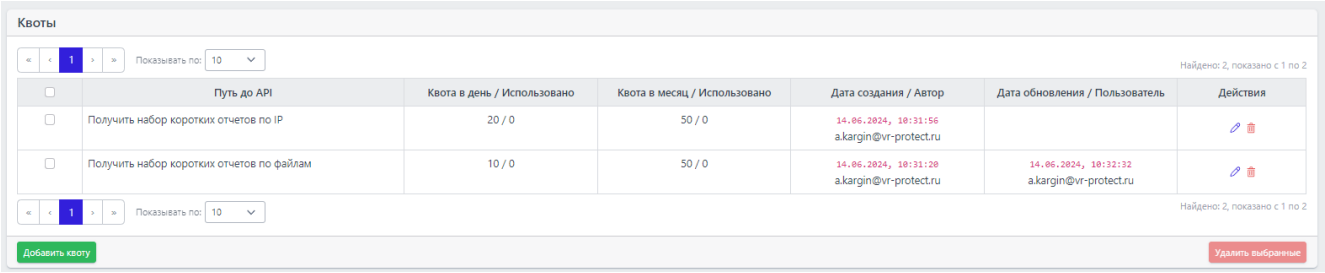



**Рисунок 28 – Таблица созданных квот**

В таблице имеются следующие поля:

– Путь до API;

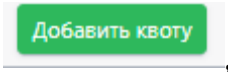
– Квота в день/Использовано;

– Квота в месяц/Использовано;

– Дата создания/Автор;

– Дата обновления/Пользователь;

– Действия ( - редактировать квоту, - удалить квоту).

Для добавления новой квоты требуется нажать по иконке 

, после чего откроется окно добавления информации для создания новой квоты (рисунок 29).

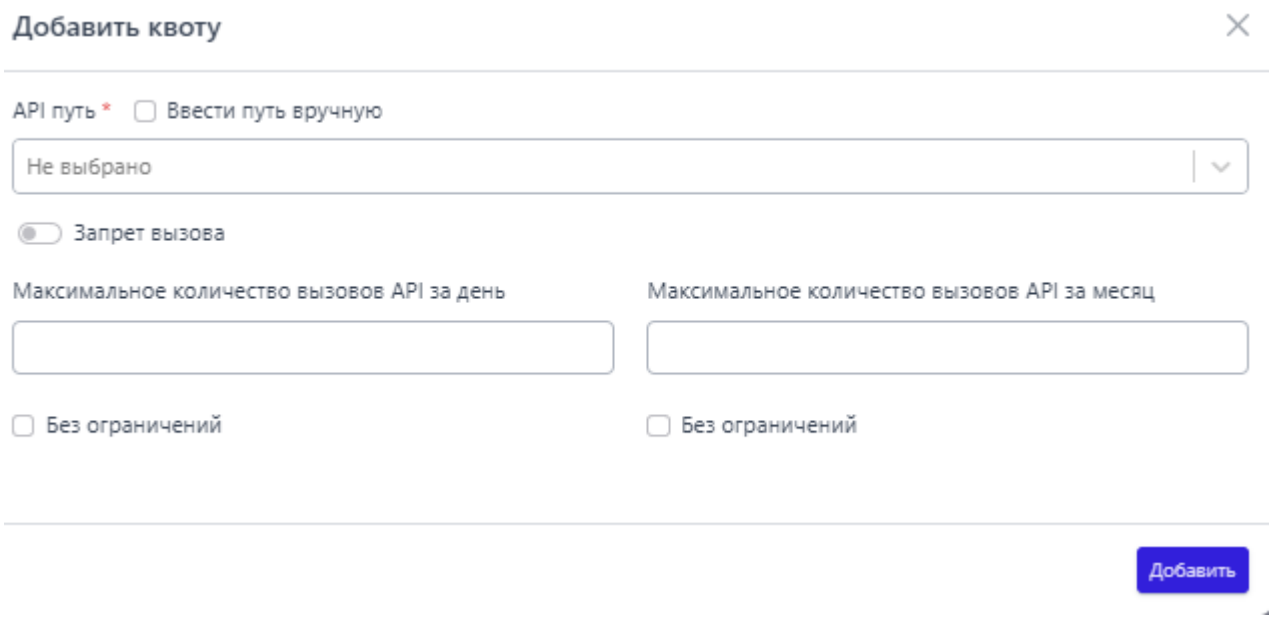



**Рисунок 29 – Окно добавления информации для создания квоты**

В данном окне требуется указать либо вручную, либо выбрать из выпадающего списка путь до API-вызова, для которого требуется создать квоту (т.е. фактически ограничить количество запросов) для организации.

Можно ограничить настройками максимальное количество вызовов за день и за месяц. Также можно запретить вызовы API либо поставить галочку «Без ограничений».

После добавления квоты, информация о ней будет добавлена в таблицу квот.

При создании нескольких квот для одного API в рамках одной организации данное действие не выполняется и всплывает на короткое время предупреждение об ошибке, представленное на рисунке 30.

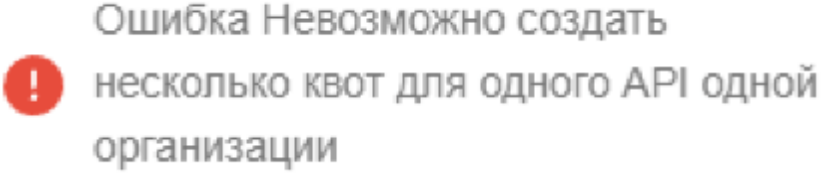



**Рисунок 30 – Сообщение об ошибке при создании одинаковых квот**

Для удаления выбранных кнопкой выбора квот требуется нажать по иконке Удалить выбранные либо в поле «Действия» напротив выбранной квоты нажать по иконке .

**Важно**

Действия по удалению, редактированию и добавлению квот открыты только при авторизации пользователя с ролью «Администратор безопасности», принадлежащего организации, имеющей признак «Владелец платформы». Квоты можно создавать как для других организаций, подключенных к сервису, так и для собственной организации (имеющей признак владельца платформы).

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

Рядом с именем токена находится иконка , при нажатии по которой открывается графическая область, показывающая активность запросов по данному клиенту (см. рисунок 31).


**Рисунок 31 – Активность запросов по выбранному клиенту**

Добавление токенов необходимо для последующего подключения к TI-платформе различных клиентов через API.

Данный токен будет служить для сервера идентификатором того или иного клиента.

Идентификацией того что клиент активен, является иконка показывающая активность 

. Для неактивных клиентов иконка имеет вид 

.

При проверке артефактов клиентом каждый артефакт будет фиксироваться в разделе «Активность» в качестве обнаружения на конкретном клиенте.

---

**Примечание**

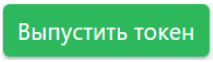
Токен представляет собой зашифрованную последовательность символов, передаваемую клиентом серверу при запросе, которая позволяет серверу однозначно идентифицировать инициатора запроса.

---

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

– удаление токена (иконка  );

– редактирование имени токена (иконка  );

– выпуск нового токена (иконка 

).

При нажатии по иконке редактирования имени токена появляется окно редактирования, представленное на рисунке 32.

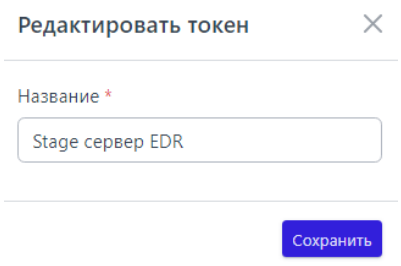



**Рисунок 32 – Окно редактирования названия токена**

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

При нажатии по иконке Выпустить токен появляется окно, представленное на рисунке 33.

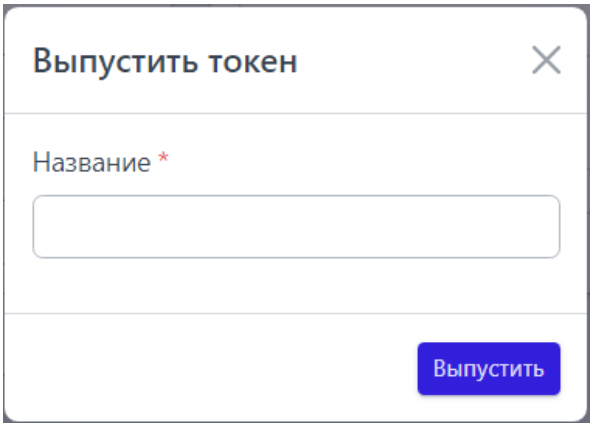



**Рисунок 33 – Окно «Выпустить токен»**

После ввода названия в данном окне для завершения действия требуется нажать по иконке **Выпустить**, после чего новый токен будет отображаться в списке токенов.

Для удаления токена требуется нажать по иконке , после чего появится окно подтверждения удаления, представленное на рисунке 34.

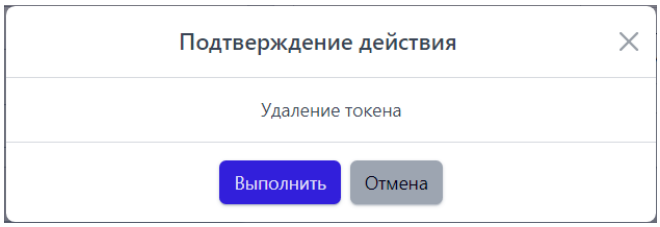



**Рисунок 34 – Окно подтверждения удаления токена**

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

Для отображения информации о новой организации, подключенной к сервису, требуется нажать по иконке Создать организацию, после чего будет отображаться окно внесения информации (рис. 35).

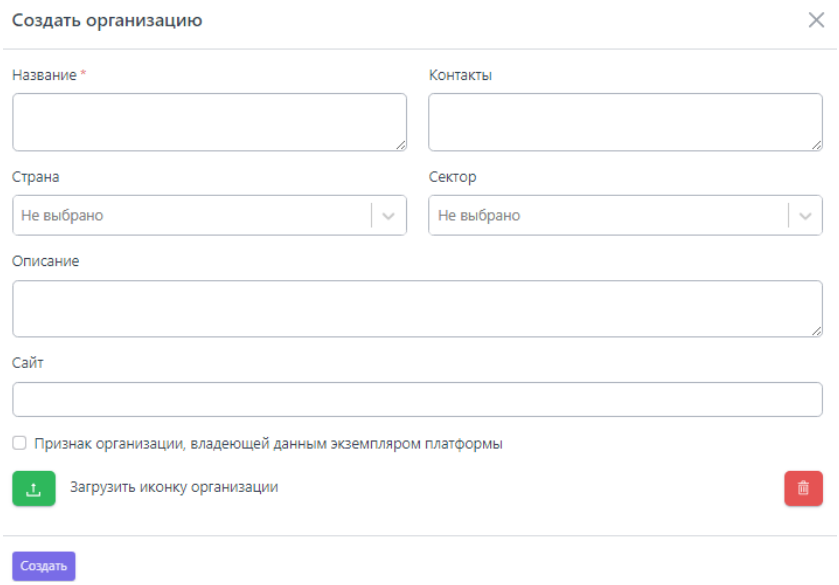



**Рисунок 35 – Окно внесения информации при создании организации**

В данном окне необходимо заполнить информацию, которая позволит идентифицировать организацию, имеющую доступ к TI-серверу.

При выставлении галочки напротив поля «Признак организации, владеющей экземпляром данной платформы» пользователям, входящим в данную организацию, доступна вся информация по отчетам и активности в других организациях (у которых данный признак не выставлен).

После заполнения всех полей требуется нажать по иконке **Создать**, после чего будет выведено короткое сообщение (рис. 36), и информация о новой организации будет отображаться в таблице.

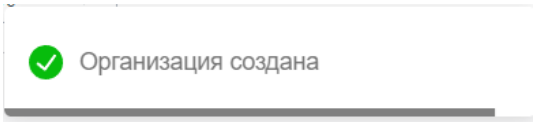



**Рисунок 36 – Сообщение о создании организации**

Для удаления организации из списка требуется отметить кнопкой выбора строчку с организацией в таблице и нажать по иконке 

.

Также для удаления организации можно воспользоваться иконкой  , которая находится в столбце **Управление** в строчке напротив выбранной организации.

Для подтверждения действия по удалению организации требуется во всплывающем окне (рис. 37) нажать по иконке **Выполнить.**

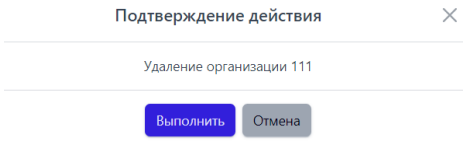



**Рисунок 37 – Подтверждение удаления организации**

Для редактирования информации по организации в столбце **Управление** требуется нажать по иконке  , после чего появится окно редактирования информации, представленное на рисунке 38.

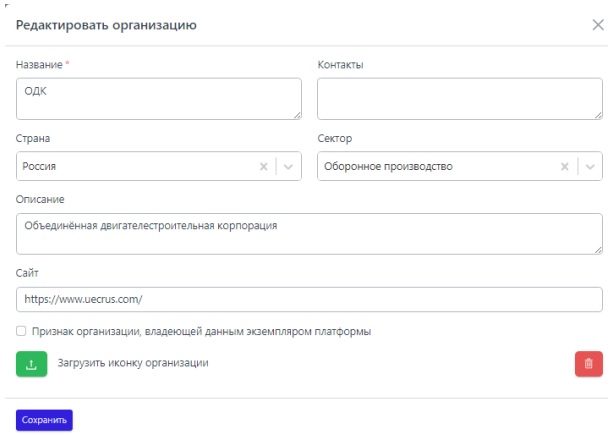



**Рисунок 38 – Окно редактирования информации организации**

После редактирования информации для подтверждения действия требуется нажать по иконке **Сохранить.**

6.4.3. Источники данных

Раздел **Источники данных** предназначен для конфигурирования получения информации из файлов с данными об артефактах, распространяемых различными вендорами на платной и безвозмездной основе.

Источник данных может содержать как данные о киберугрозах (индикаторы компрометации), которые в зависимости от настройки TI-платформа будет классифицировать как вредоносные (либо подозрительные), так и белые списки артефактов, которые TI-платформа будет классифицировать как безопасные.

Общий вид окна раздела **Источники данных** представлен на рисунке 39.

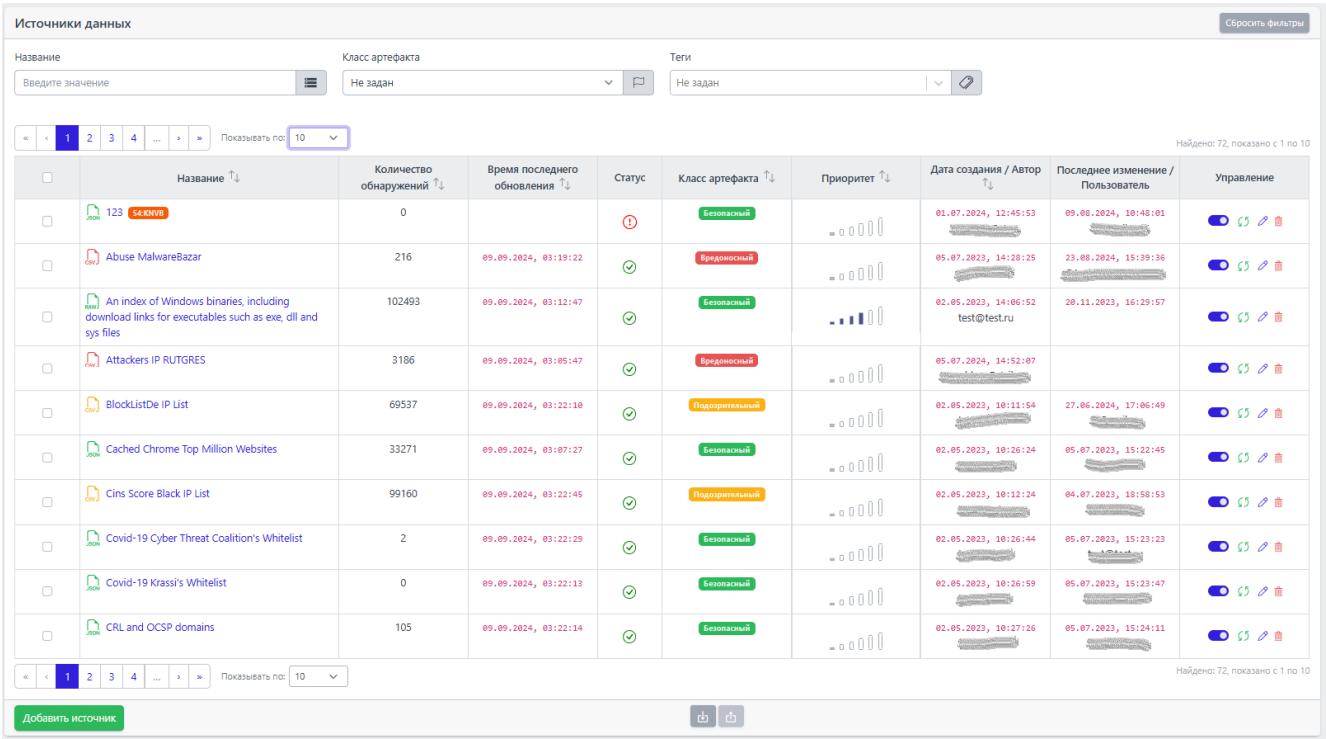



**Рисунок 39 – Окно раздела «Источники данных»**

Таблица имеет следующие поля:

– Кнопка выбора;

– **Название** (отображается название базы данных);

– **Количество обнаружений;**

– **Время последнего обновления;**

– **Статус** (отображается информация о статусе обновления базы);

– **Класс артефакта** (отображается вердикт для артефакта, если артефакт будет найден в текущем источнике данных);

– **Приоритет** (минимальный /средний);

– **Дата создания/автор;**

– **Последнее изменение/пользователь;**

– **Управление** (в данной области имеются иконки управления источником данных: активация/деактивация источника  , синхронизация источника данных, подключенного к сервису с базой источника извне  , редактирование информации об источнике  , удаление источника  .

При деактивации источника данных сервер прекращает выполнять периодическое обновление информации из этого источника.

Полученная ранее информация продолжит отображаться в отчетах по артефактам, но эта информация будет помечена как неактуальная. Вердикт на основе этой информации выноситься не будет.

Добавить файл из внешнего источника можно нажав по иконке  .

Для возможности добавления файла внешнего источника на TI-платформу файл должен соответствовать следующим условиям:

– загрузка файла должна осуществляться по фиксированной ссылке;

– файл должен загружаться по ссылке непосредственно либо должен загружаться архив поддерживаемого формата, в котором находится единственный файл;

– файл должен быть одного из поддерживаемых форматов (CSV, JSON либо текстовые файлы произвольного формата).

Для экспорта информации об источнике в файл требуется нажать по иконке  .

Для фильтрации информации в таблице имеется система фильтров, которая представлена следующими фильтрами:

– **Название** (название базы данных);

– **Класс артефакта** (неизвестный, безопасный, вредоносный, в процессе анализа, подозрительный);

– **Тэги** (ключевые слова, которые задаются при редактировании/добавлении источника и нужны для дополнительного удобства категорирования и классификации источников).

Для сортировки данных в столбцах таблицы используются иконки , , , .

В столбце **Статус** в строчке напротив источника, который обновляется с ошибкой, имеется иконка с предупреждением .

При наведении на данную иконку указателя мыши появляется всплывающее окно, представленное на рисунке 40.

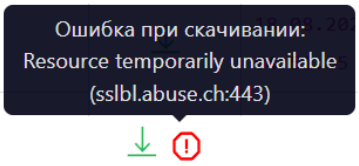



**Рисунок 40 – Сообщение об ошибке при скачивании обновления источника**

При нажатии по названию источника, например, Abuse MalwareBazaar откроется окно с информацией по источнику, представленное на рисунке 41.

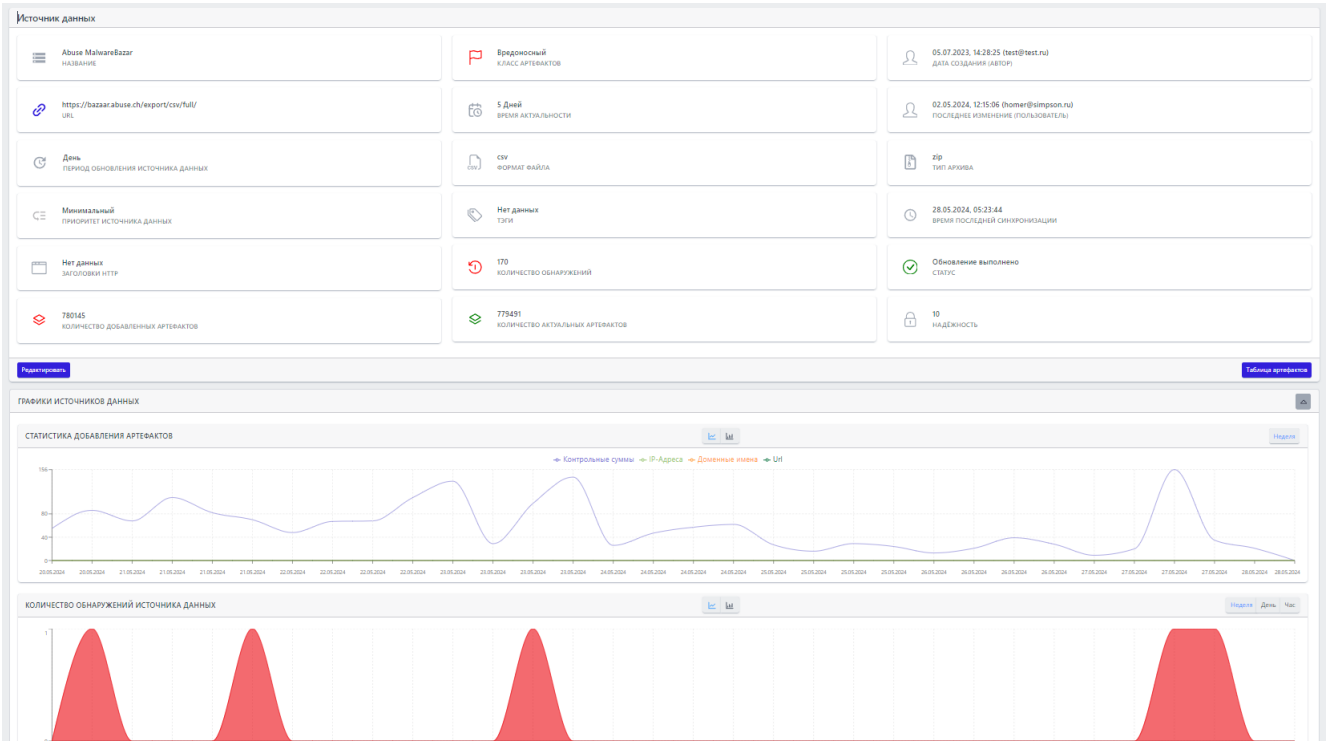



**Рисунок 41 – Окно информации по источнику данных**

В данном окне представлены следующие области:

– **Источник данных** (выводится информация о подключенном источнике);

– **Статистика добавления артефактов** (выводится в графическом виде статистика по добавленным артефактам, относящимся к данному источнику);

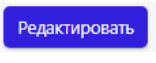
– **Количество обнаружений источника данных** (выводится в графическом виде количество обнаружений, относящихся к данному источнику).

График статистики может быть представлен в линейном или столбчатом виде.

Для изменения вида графика имеются следующие иконки:

–  – линейное представление графика статистики;

–  – столбчатое представление графика статистики.

При нажатии по иконке 

откроется окно, где можно редактировать информацию, относящуюся к настройке источника данных.

При нажатии по иконке Таблица артефактов, откроется страница, где в табличной форме отображается список артефактов, представленных в выбранном источнике данных (рисунок 42).

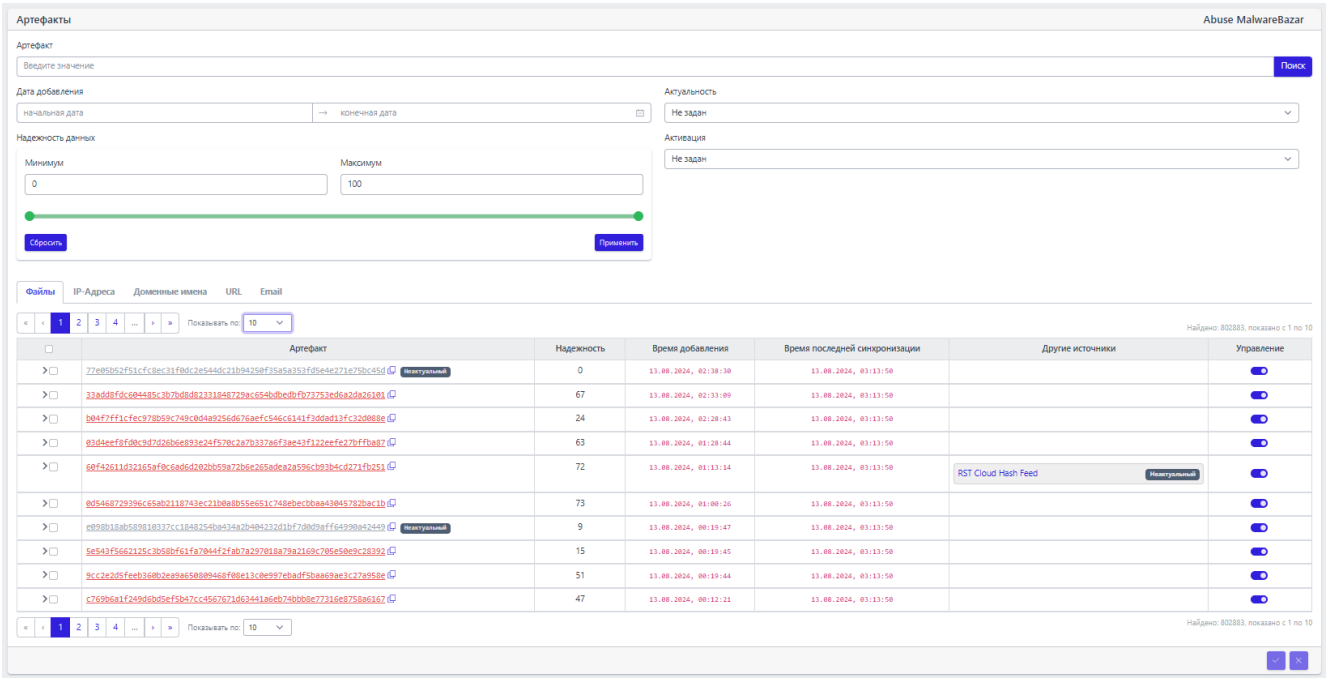



**Рисунок 42 – Артефакты по выбранному источнику данных**

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

– Столбец с иконкой раскрытия информации по артефакту ›;

– Артефакт;

– Надежность данных (указывается в процентах надежность каждого артефакта);

– Время добавления артефакта;

– Время последней синхронизации;

– Другие источники;

– Управление (активация/деактивация артефакта).

Над таблицей имеется система фильтров и область указания надежности данных для всего источника.

Система фильтров представлена следующими фильтрами:

– Артефакт;

– Дата добавления артефакта (начальная и конечная);

– Признак актуальности (не задан, актуальный, не актуальный);

– Активация (незадан, активирован, не активирован).

В области указания надежности артефактов по источнику данных можно изменить параметр надежности, заданный в источнике данных в процентном соотношении. При этом, если надежность данных артефакта в источнике будет меньше надежности данных, заданных при общей настройке надежности данных для источника, то такой артефакт будет обозначен, как неактуальный и не будет использоваться при вынесении вердикта.

Также можно выставить признак неактуальности артефакта в столбце **Управление**, деактивировав артефакт.

Для добавления нового источника данных требуется нажать ЛКМ по иконке Добавить источник, после чего будет открыто окно добавления источника, представленное на рисунке 43.

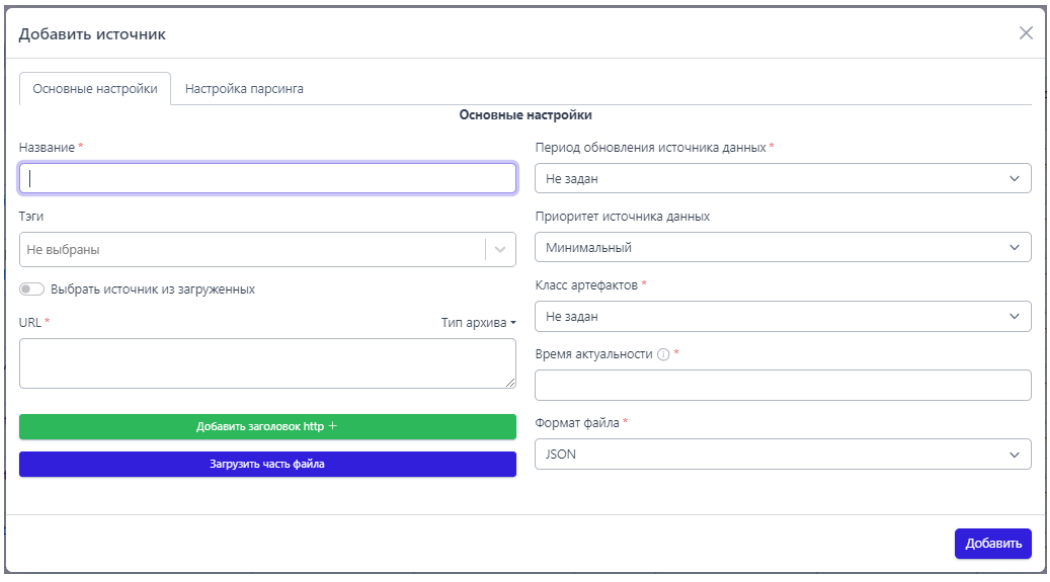



**Рисунок 43 – Окно добавления источника данных**

Параметры, требуемые для настройки источников данных, в данном окне разделены на 2 группы:

1) **Основные настройки;**

2) **Настройки парсинга.**

Основные настройки

Название источника.

Тэги (ключевые слова для удобства категорирования и классификации).

Переключатель «Выбрать источник из загруженных» позволяет загрузить файл с источником данных вручную, без использования внешних URL. При таком режиме работы поля для выбора URL и HTTP-заголовков становятся недоступны. Также теряет актуальность поле «Период обновления источников данных». В данном режиме работы синхронизация источника данных произойдет единожды при его сохранении. При успешной синхронизации загруженный файл будет удален из хранилища сервера. В дальнейшем для указанного источника данных можно загрузить новый файл через модальное окно редактирования.

Для выбора источника данных из имеющихся загруженных источников следует сделать активной кнопку выбора ***Выбрать источник из загруженных***, переведя ползунок кнопкой мыши вправо (рисунок 44), при этом становятся активны иконки  - **Загрузить файл,**  - **Перейти к хранилищу**.

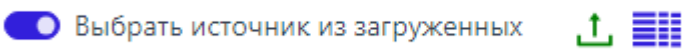



**Рисунок 44 – Выбор источника из загруженных**

При нажатии по иконке **Загрузить файл** происходит переход на страницу **Загрузки** на компьютере, с которого был осуществлен вход в модуль администрирования TI, для выбора уже имеющегося ранее загруженного файла с источником данных.

При нажатии по иконке **Перейти к хранилищу** происходит переход на страницу внутреннего хранилища файлов с источниками (рисунок 45).

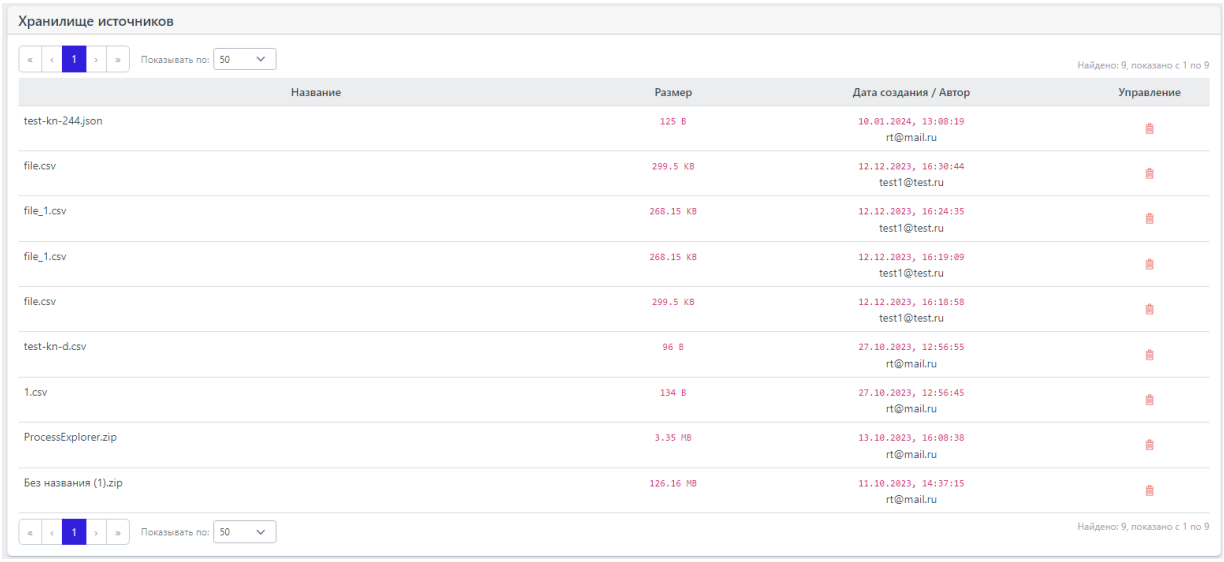



**Рисунок 45 – Страница «Хранилище источников»**

URL – фиксированная ссылка, по которой сервер может загрузить файл с данными.

Тип архива (формат архива, загружаемого по ссылке, в котором содержится целевой файл с данными), тип архива не указывается, если файл скачивается не в архиве.

Заголовки http – набор заголовков, которые будут передаваться серверу в запросе на скачивание целевого файла, могут содержать токены доступа и прочую информацию, которая требуется целевому серверу для возврата файла.

Период обновления источника данных – задает периодичность загрузки и синхронизации данных из источника с имеющимися на сервере данными,

имеется возможность выбора следующих периодов обновления (никогда, день, 3 дня, неделя, месяц).

Класс артефактов – задает вердикт, который будет выноситься артефактам, обнаруженным в данном источнике данных, для источника белого списка класс артефактов должен быть безопасный, для источника данных об угрозах класс артефактов должен быть вредоносный либо подозрительный.

Приоритет источника данных – задает степень доверия к источнику данных по сравнению с другими источниками. Если артефакт находится одновременно в двух источниках данных, по которым настроен различный класс артефактов, вердикт по артефакту будет выдаваться на основании источника с самым высоким приоритетом. Если артефакт находится одновременно в двух источниках данных, по которым настроен различный класс артефактов, при этом приоритет обоих источников одинаков, приоритетным будет выбираться источник белого списка (класс артефактов безопасный). При настройке данного параметра имеется возможность задания следующих приоритетов (**Минимальный**, **Низкий**, **Ниже среднего**, **Средний**, **Выше среднего**, **Высокий**).

Время актуальности – период после последней синхронизации, в который полученные об артефакте из файла данные будут считаться актуальными и влиять на вердикт по артефакту.

Время актуальности не должно быть меньше периода обновления источника данных, иначе по истечению периода актуальности все данные источника будут считаться устаревшими до следующей синхронизации. Если при последующей синхронизации артефакт пропадает из получаемых данных, данные по нему будут считаться актуальными в указанный период.

Формат файла – указывает формат целевого файла (JSON, CSV, любой формат). На основании выбранного формата отображаются дополнительные настройки парсинга.

JSON:

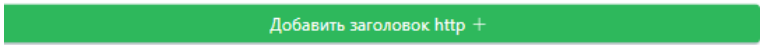
Путь до списка объектов с артефактами, путь до артефактов в рамках элемента списка.

CSV:

Порядковый номер колонки, в которой содержится артефакт – формат CSV подразумевает наличие на каждой строке записи с несколькими колонками. Требуется указать номер колонки (начиная с 0), в котором содержится целевой артефакт.

Любой формат:

Регулярное выражение для разбора каждого элемента – при парсинге произвольного формата требуется указать регулярное выражение для поиска требуемых данных на каждой строке целевого файла. Выражение должно содержать как минимум одну группу, заключенную в круглые скобки, в которой будет содержаться артефакт.

При нажатии по иконке 

появляются поля, где можно заполнить соответственно ключ и значение заголовка. Эти заголовки могут требоваться вендорам, предоставляющим файл с данными (например, на платной основе). При указании галочки скрыть заголовок  значение заголовка не будет доступно для дальнейшего просмотра и редактирования.

Корректную настройку данных параметров можно проверить, нажав кнопку **Загрузить часть файла**. Если все настроено верно, на форме редактирования должны корректно отобразиться первые несколько строк целевого файла с данными.

Настройки получения данных из файла (парсинга)

Под парсингом понимается разбор файла источника данных для получения артефактов, обрабатываемых TI-платформой.

Поле настройки получения данных из файла (парсинга) в зависимости от выставленного ранее типа формата файла имеет разные настройки и представлено на рисунках 46 - 48.

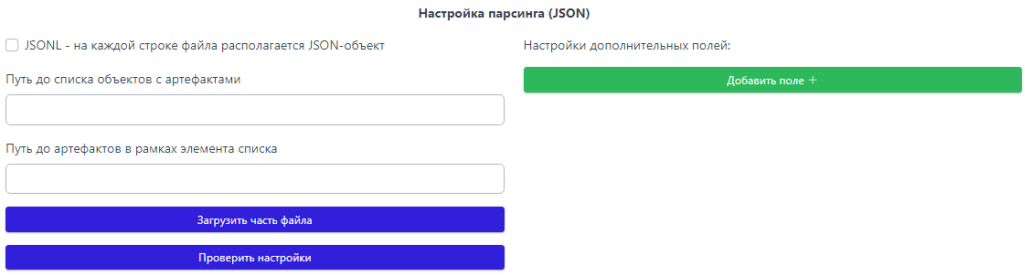



**Рисунок 46 – Настройка парсинга файлов в формате JSON**

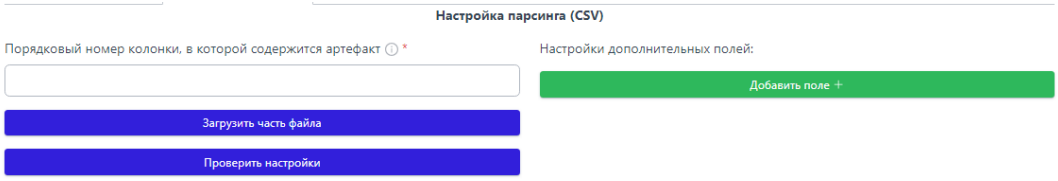



**Рисунок 47 – Настройка парсинга файлов в формате CSV**

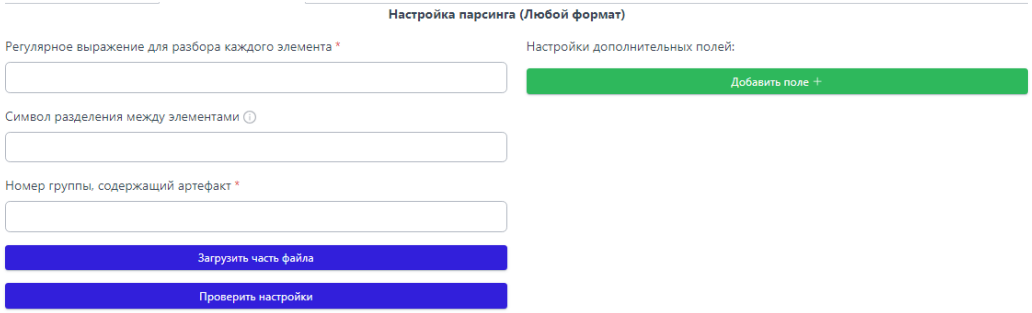



**Рисунок 48 – Настройка парсинга файлов любого формата**

Настройка парсинга файлов в формате JSON

**Путь до списка объектов с артефактами** – если не установлен флаг JSONL, требуется указать путь до JSON-списка, содержащего объекты с артефактами в формате "property.property". Если JSON-список является корневым объектом, поле нужно оставить пустым.

**Путь до артефактов в рамках элемента списка** – требуется указать путь до элемента в формате "property.property", в котором содержится строка с

целевым артефактом в рамках одного элемента списка. Если это корневой элемент, поле можно оставить пустым.

Для настройки дополнительных полей следует нажать кнопку «Добавить поле». При ее нажатии будут добавлены для поля ввода, для наименования поля и в зависимости от типа файла колонка, группа или JSON-свойство для получения значения поля в рамках одного артефакта. В строке «Наименование поля» можно указать как произвольные значения, так и выбрать значения из предложенных сервером: **Надежность данных** и **Дата обнаружения**.

При выборе параметра настройки **Надежность данных** в общей области настройки данных парсинга появляется дополнительное окно, с помощью которого можно мышью изменять параметр надежности данных (указывается в процентах). ( рис 49).

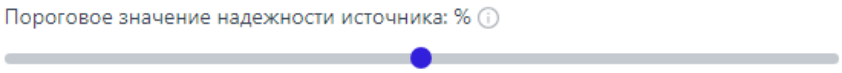



**Рисунок 49 – Инструмент по управлению настройки параметра значения надежности источника**

### Примечание

Поле надежность данных (Confidence) означает надежность, уверенность в данных, доступных об индикаторе компрометации. Можно указать пороговое значение данного поля, ниже которого вердикт из источника данных не будет учитываться. Например, в файле источника данных имеется запись об артефакте, в которой есть поле confidence со значением 40, и получение данной записи в поле «Надежность данных» настроена корректно. В этом случае, если для источника данных установлено пороговое значение 50, то запись в этом источнике данных об артефакте будет считаться неактуальной и

не будет влиять на вердикт. При этом наличие сведений об артефакте в источнике данных и дополнительные поля будут отображаться и обновляться.

Настройка парсинга файлов в формате CSV

При настройке парсинга файлов в формате CSV в основном поле следует указать **Порядковый номер колонки, в которой содержится артефакт** (номера колонок начинаются с 0). Настройка дополнительных полей аналогична настройке, описанной выше.

Настройка парсинга файлов любого формата

В поле **Регулярное выражение для разбора каждого элемента** можно написать выражение, по которому будет произведен разбор элемента.

**Символ разделения между элементами** – должен указываться, если вместо разбора файла построчно требуется разделить его содержимое по другому разделителю. По умолчанию для разделения между элементами используется новая строка.

**Номер группы, содержащий артефакт** – содержит номер группы в регулярном выражении, содержащий артефакт.

После добавления информации об источнике данных можно проверить правильность заполнения полей, нажав по иконке **Проверить настройки**.

Если параметры указаны некорректно, либо имеются незаполненные поля, выводятся соответствующие сообщения, например, как на рисунке 50.

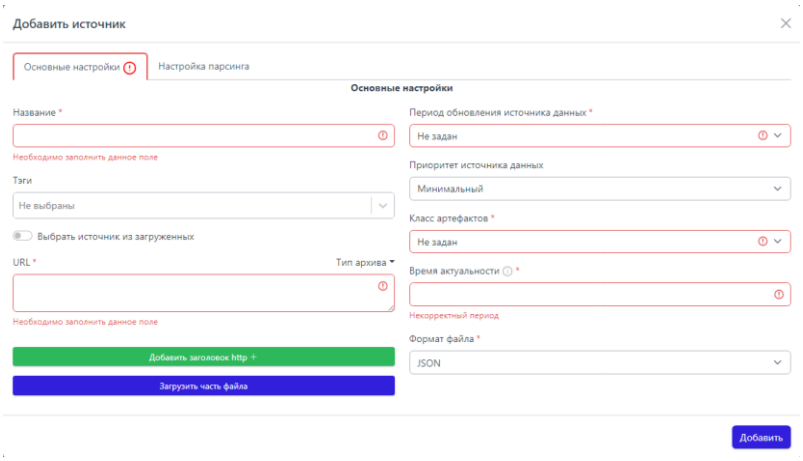



**Рисунок 50 – Сообщение об ошибках при добавлении/редактировании информации о источнике**

При нажатии по иконке **Загрузить часть файла** в отдельном окне ниже данной иконки будет показана часть файла, предоставленного источником данных (рисунок 51).

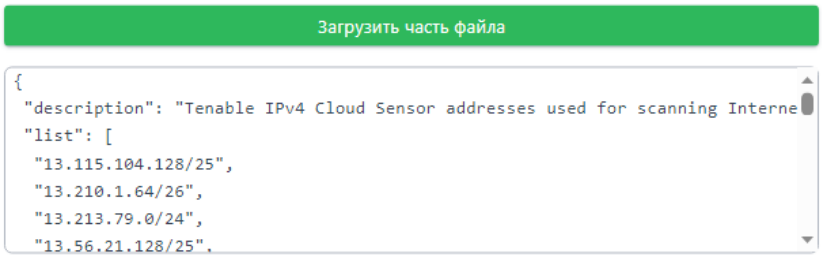



**Рисунок 51 – Часть файла, предоставленного источником данных**

Пример настройки источника данных на основе источника Malware Bazaar

Рассмотрим процедуру конфигурации источника данных на примере ресурса Malwarebazaar. На ресурсе в разделе export (https://bazaar.abuse.ch/export/) находится прямая ссылка на zip-файл со всеми данными - https://bazaar.abuse.ch/export/csv/full/ (см. рисунок 52).

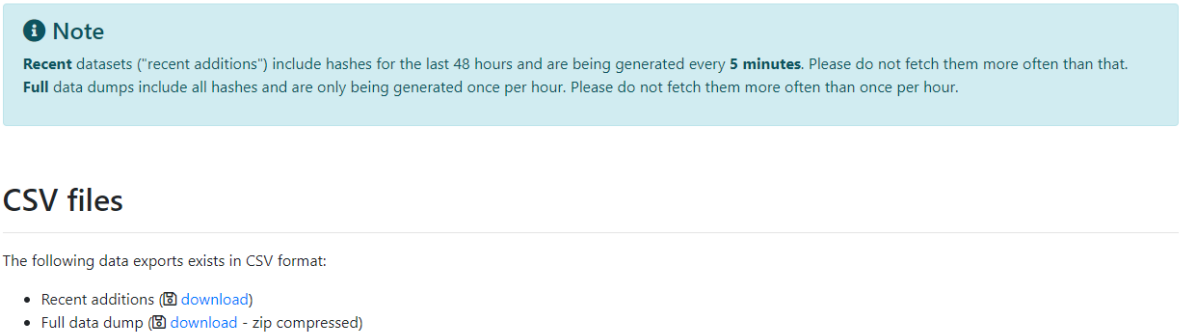



**Рисунок 52 – Информация со страницы ссылки на источник**

В описании содержится информация, что данный файл обновляется каждый час. В этом случае оптимальным периодом обновления файла в TI будет 1 день. Имея прямую ссылку, мы можем приступить к настройке источника данных.

Заполняем поле **Название**, в поле **URL** указываем ссылку на файл, в выпадающем списке **Тип архива** выбираем значение **ZIP-архив**. После заполнения этих полей мы можем нажать на кнопку **Загрузить часть файла** и проверить правильность введенных полей.

Если поля заполнены правильно, через некоторое время на форме отобразится окно, содержащее несколько строчек настраиваемого файла. Это свидетельствует о том, что сервер смог загрузить файл по переданному URL и смог распаковать содержимое файла из архива согласно переданному типу архива (рисунок 53).

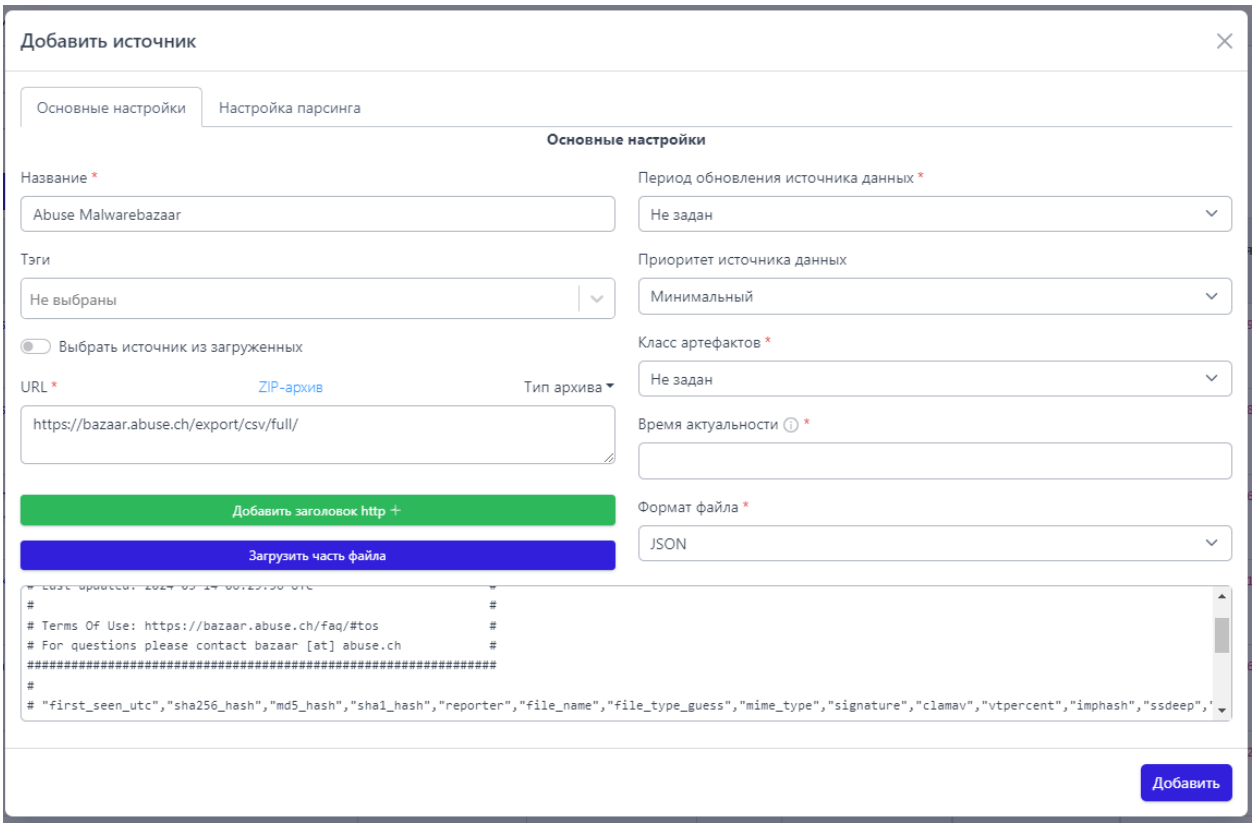



**Рисунок 53 – Настройка при добавлении источника**

Далее заполняем остальные поля на вкладке **Основные настройки**:

– Период обновления источника данных устанавливаем «День»;

– Приоритет источника данных выбираем согласно уровню доверия относительно других источников данных (можно оставить «Минимальный»);

– Класс артефактов выбираем «Вредоносный» либо «Подозрительный» в зависимости от уровня доверия к содержимому файла;

– Время актуальности устанавливаем больше, чем заданный период обновления (1 день), чтобы элементы сохраняли признак актуальности в случае, когда очередная синхронизация не была завершена успешно. Вводим в поле 5 дней.

– Формат файла выбираем CSV, исходя из содержимого файла.

Заполнение полей при настройке источника данных согласно выше приведенному описанию представлено на рисунке 54.

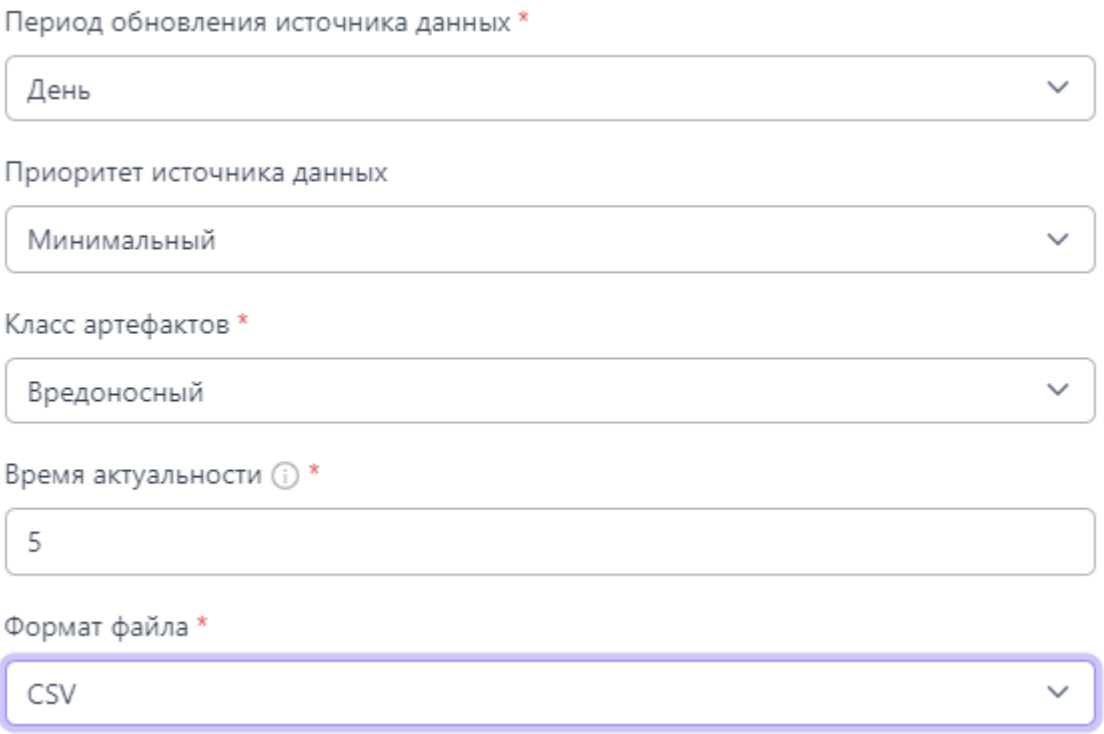



**Рисунок 54 – Пример заполнения полей при настройке источника**

Переходим на вкладку **Настройка парсинга**. Из загруженной части файла мы видим заголовки всех csv-колонок, доступных в файле.

"first_seen_utc","sha256_hash","md5_hash","sha1_hash","reporter","file_name","file_type_guess","mime_type","signature","clamav","vtpercent","imphash","ssdeep","tlsh"

Артефактом в данном случае для нас будет являться SHA-256 от файла, которая находится в колонке sha256_hash. Данная колонка находится под порядковым номером один, если вести отсчет от нуля. Вводим «1» в поле **Порядковый номер колонки, в которой содержится артефакт**.

Мы можем добавить информацию из всех остальных колонок csv-файла при помощи раздела **Настройки дополнительных полей** в правой части формы. Например, добавим время обнаружения артефакта. Для этого нажимаем на кнопку **Добавить поле**. На форме отображается два поля для ввода имени поля и номера колонки.

При нажатии на поле ввода **Наименование поля** отобразится выпадающий список, отображающий предустановленные на TI-платформе дополнительные поля. Выбираем из списка **Дата обнаружения**, т.к. это поле соответствует по смыслу тому полю, которое мы хотим добавить. В строку **Номер колонки** вводим порядковый номер колонки, если считать от нуля – 0.

Добавим также дополнительное поле из колонки file_name. Нажимаем на кнопку **Добавить поле**, чтобы на форме отобразились поля для ввода настроек для еще одной колонки. В поле **Наименование поля** не выбираем значение из выпадающего списка, а вводим своё. Записываем в строку ввода **Имя файла**. В поле **Номер колонки** вводим порядковый номер целевой колонки – 5.

Настройка дополнительных полей при настройке парсинга источника данных представлена на рисунке 55.

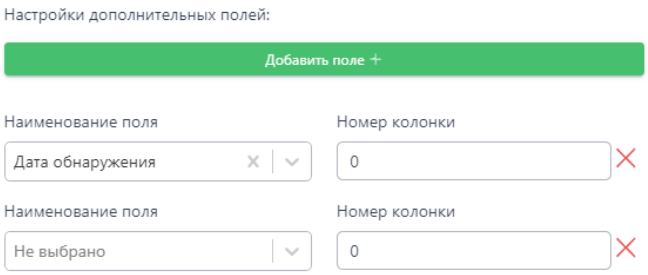



**Рисунок 55 – Пример заполнения дополнительных полей при настройке парсинга**

После завершения настройки основного поля, содержащего артефакт, и всех желаемых дополнительных полей мы можем проверить корректность введенных нами настроек парсинга, нажав кнопку **Проверить настройки**. Через некоторое время на форме отобразится окно, содержащее несколько полученных из файла записей об артефактах.

Нам требуется проверить корректность отображения следующих элементов:

– Поле **Артефакт** у элементов заполнено хешами SHA-256 файлов и отображается красным или желтым цветом (в зависимости от установленного в источнике данных класса артефактов).

– Поле **Дата обнаружения** заполнено значением, полученным из файла (время должно отличаться у каждого элемента).

– Поле **Имя файла** содержит имя каждого файла, а не иные данные.

Чтобы убедиться в корректности настроек, достаточно проверить 1-2 элемента (см. рисунок 56).

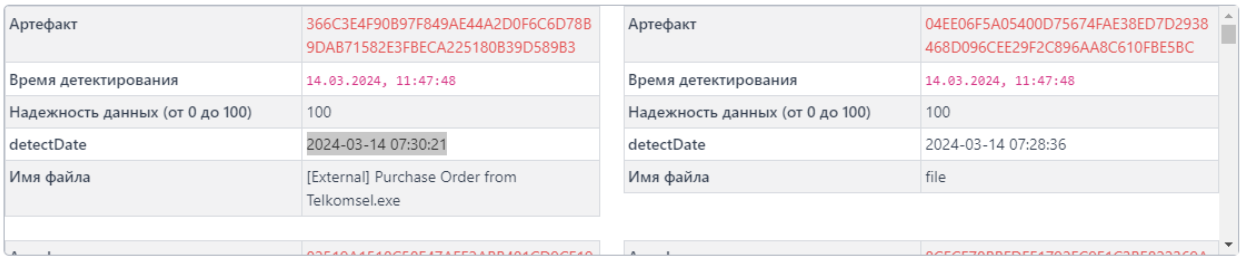



**Рисунок 56 – Проверка корректности настроек**

Если настройка всех полей произведена корректно, нажимаем на кнопку **Добавить**. Источник данных будет сохранен и доступен для просмотра и редактирования в табличной форме. Синхронизация данных из источника будет произведена в 03:00 по времени сервера.

6.4.4. Теги

Теги в разделе **Администрирование** предназначены для удобства маркировки и ранжирования источников данных, а также для назначения своих тегов (псевдонимов) источникам данных, которые уже маркированы собственными тегами.

Общий вид страницы **Теги** представлен на рисунке 57.

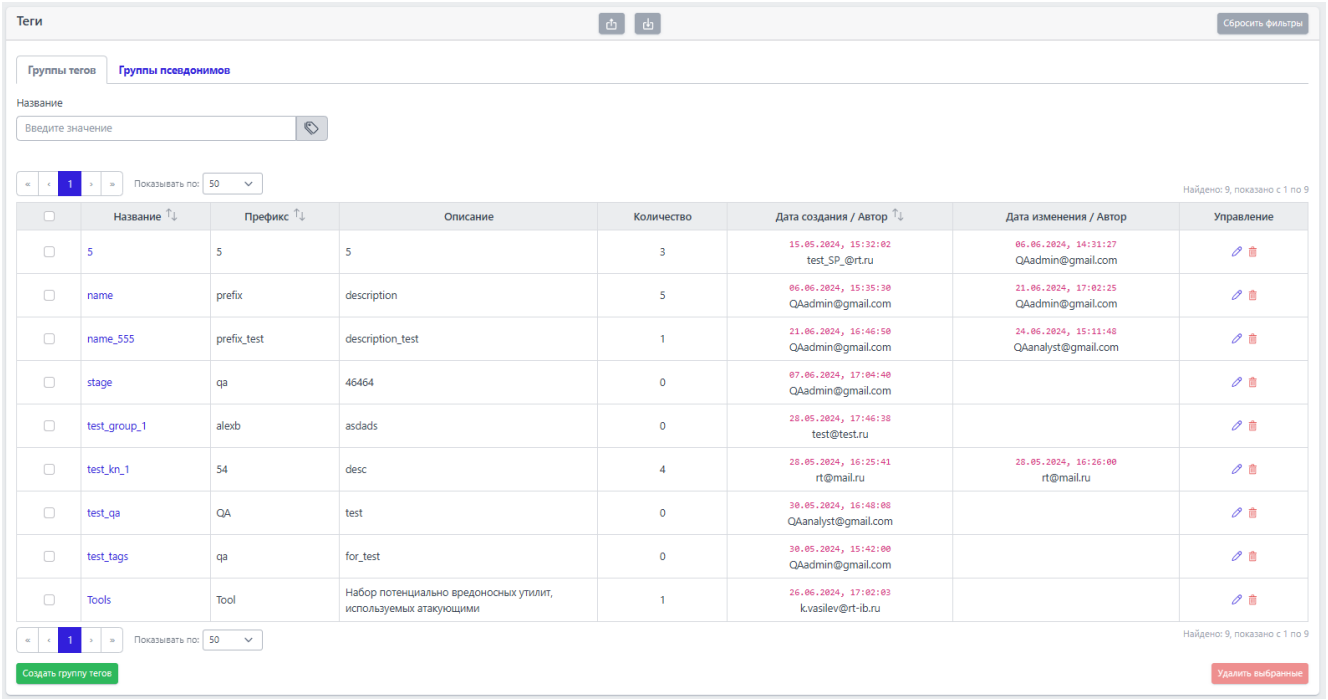



**Рисунок 57 – Страница Теги**

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 фильтра **Название**.

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

– Кнопка выбора ☐ / ☑;

– Название (название группы тегов);

– Префикс;

– Описание;

– Количество (количество элементов в группе);

– Дата создания/Автор;

– Дата изменения /Автор;

– Управление (редактирование группы , удаление группы ).

Для удаления группы тегов необходимо в поле **Управление** нажать по иконке удаления группы.

Для удаления нескольких групп тегов следует пометить необходимые группы кнопкой выбора и нажать по иконке Удалить выбранные.

Для создания новой группы тегов требуется нажать по иконке Создать группу тегов, после чего откроется окно создания группы тегов, представленное на рисунке 58.

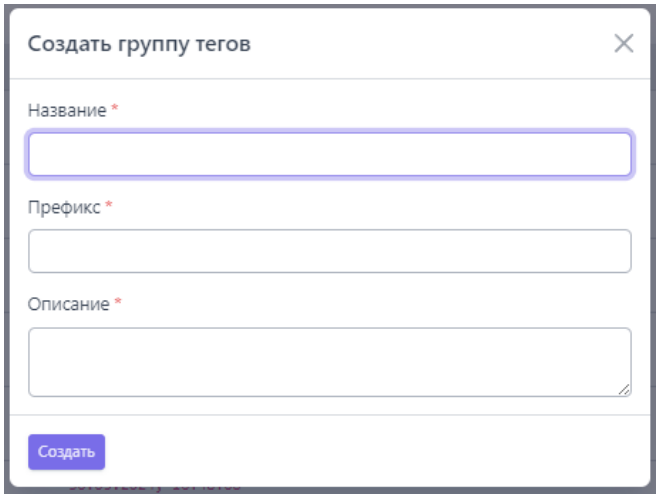



**Рисунок 58 – Окно создания группы тегов**

Для создания группы тегов в данном окне требуется заполнить поля **Название**, **Префикс**, **Описание** и нажать по иконке **Создать**, после чего новая группа тегов появится в списке групп.

Для редактирования группы тегов следует в области **Управление** нажать по иконке , после чего появится окно редактирования группы, представленное на рисунке 59.

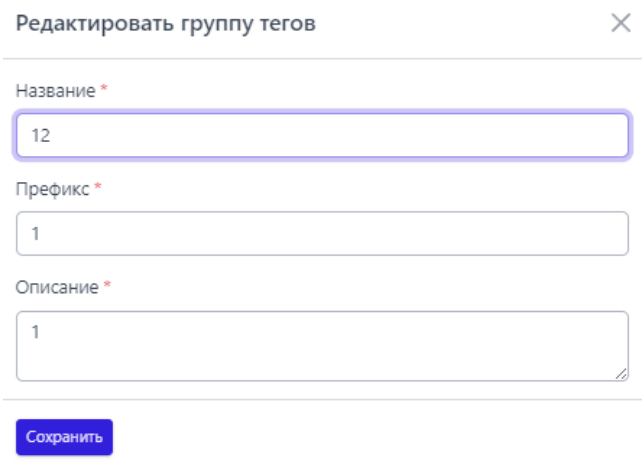



**Рисунок 59 – Окно редактирования группы тегов**

Название группы тегов на странице **Теги** вкладки **Группы тегов** является активной ссылкой, при нажатии по которой открывается окно с тегами данной группы (рисунок 60).

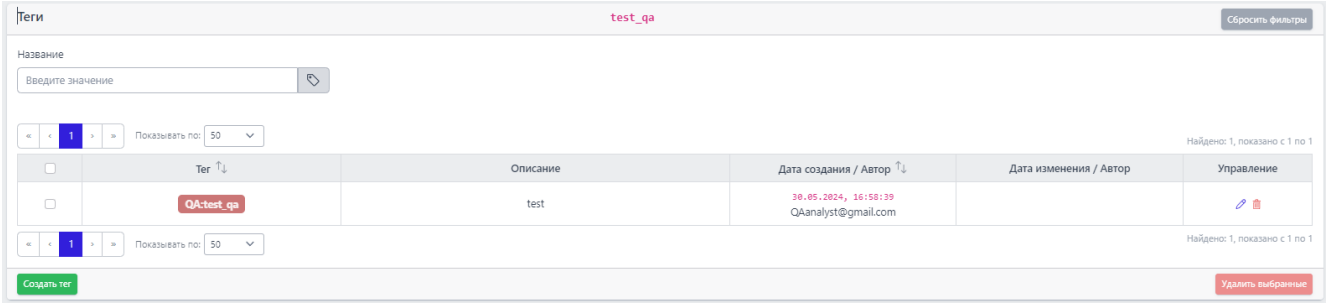



**Рисунок 60 – Окно Теги в группе тегов**

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

– Кнопка выбора ;

– Тег;

– Описание;

– Дата создания/Автор;

– Дата изменения/Автор;

– Управление (редактировать тег , удалить тег ).

Для редактирования тега следует в области **Управление** нажать по иконке , после чего появится окно редактирования тега, представленное на рисунке 61.

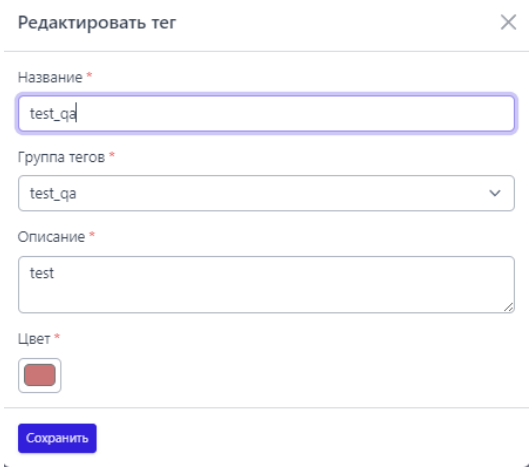



**Рисунок 61 – Окно редактирования информации о теге**

Для создания нового тега в данной группе следует нажать по иконке Создать тег, после чего откроется окно создания тега, представленное на рисунке 62.

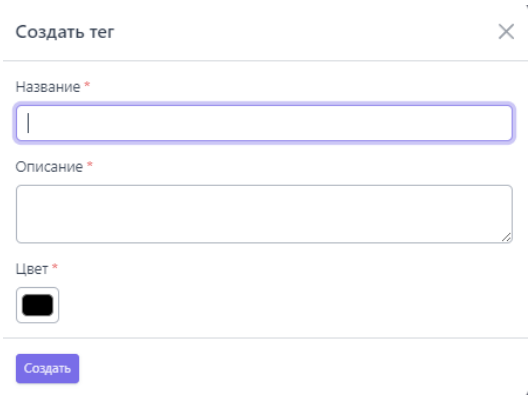



**Рисунок 62 – Окно создания тега**

В данном окне для создания тега следует заполнить все поля и нажать по иконке **Создать**.

Общий вид страницы **Теги** вкладки **Группы псевдонимов** представлен на рисунке 63.

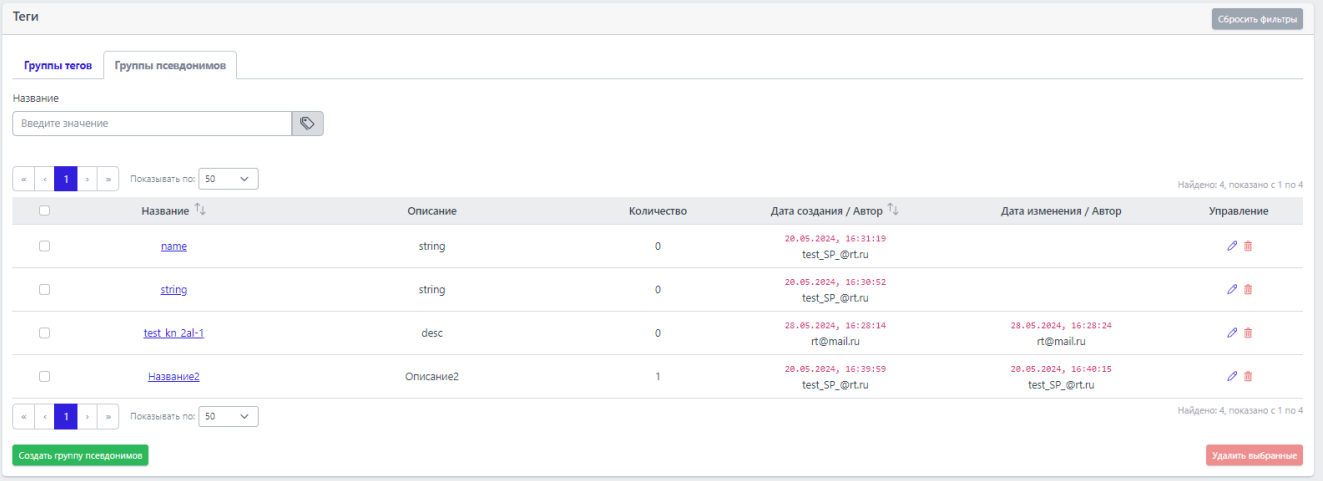



**Рисунок 63 – Окно вкладки Группы псевдонимов**

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

– Кнопка выбора / ;

– Название (название группы псевдонимов);

– Описание;

– Количество (количество элементов в группе);

– Дата создания/Автор;

– Дата изменения /Автор;

– Управление (редактирование группы , удаление группы ).

Для удаления группы псевдонимов необходимо в поле **Управление** нажать по иконке удаления группы.

Для удаления нескольких групп псевдонимов следует пометить необходимые группы кнопкой выбора и нажать по иконке Удалить выбранные.

Для создания новой группы псевдонимов требуется нажать по иконке Создать группу псевдонимов, после чего откроется окно создания группы, представленное на рисунке 64.

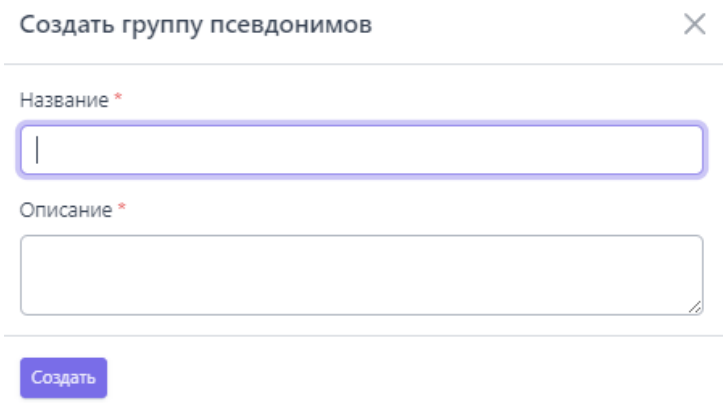



**Рисунок 64 – Окно создания группы псевдонимов**

Для создания группы псевдонимов в данном окне требуется заполнить поля **Название**, **Описание** и нажать по иконке **Создать**, после чего новая группа псевдонимов появится в списке групп.

Для редактирования группы псевдонимов следует в области **Управление** нажать по иконке , после чего появится окно редактирования группы, представленное на рисунке 65.

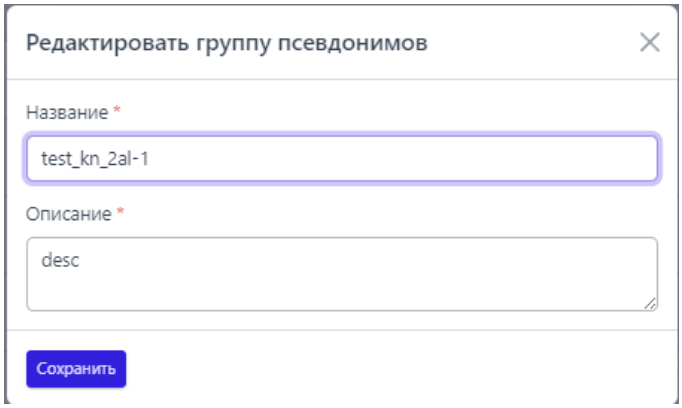



**Рисунок 65 – Окно редактирования группы псевдонимов**

Название группы псевдонимов на странице **Теги** вкладки **Группы псевдонимов** является активной ссылкой, при нажатии по которой открывается окно с псевдонимами данной группы (рисунок 66).

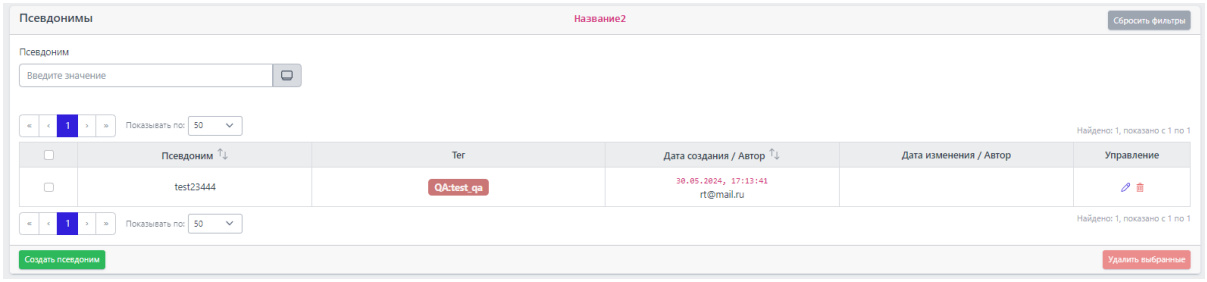



**Рисунок 66 – Окно Псевдонимы в группе псевдонимов**

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

– Кнопка выбора ;

– Псевдоним;

– Тег;

– Дата создания/Автор;

– Дата изменения/Автор;

– Управление (редактировать псевдоним , удалить псевдоним ).

Для редактирования псевдонима следует в области **Управление** нажать по иконке , после чего появится окно редактирования псевдонима, представленное на рисунке 67.

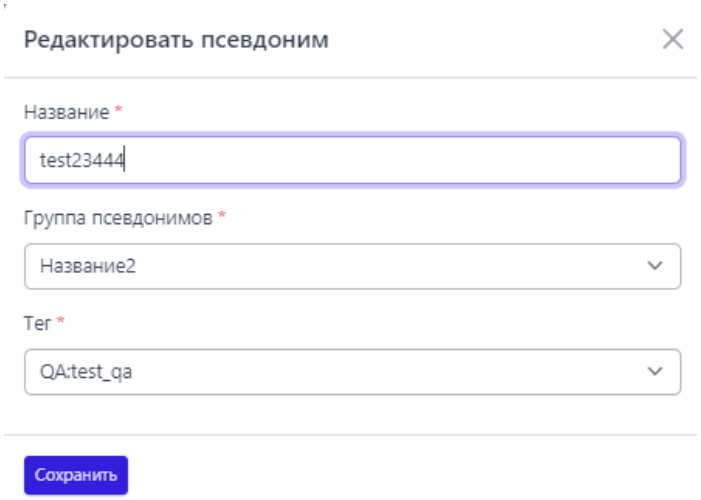



**Рисунок 67 – Окно редактирования информации о псевдониме**

Для создания нового тега в данной группе следует нажать по иконке Создать тег, после чего откроется окно создания псевдонима, представленное на рисунке 68.

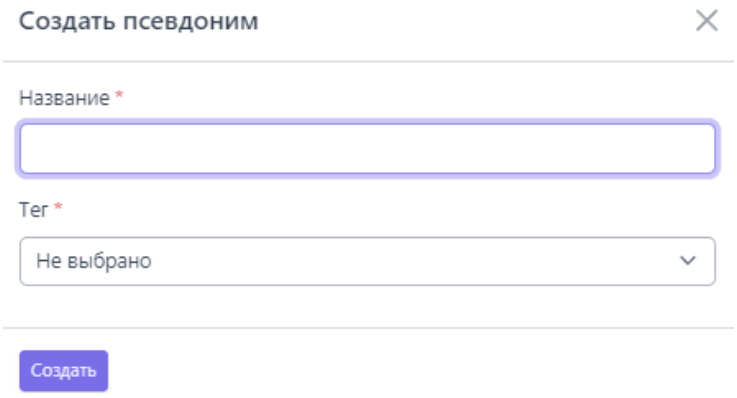



**Рисунок 68 – Окно создания псевдонима**

В данном окне для создания тега следует заполнить все поля и нажать по иконке **Создать.**

У пользователя имеется возможность экспортировать в файл наборы с группами тегов, нажав по иконке . Для импорта файла в набор тегов используется иконка .

**Важно**

Теги, созданные на странице данного раздела можно назначить для источника данных либо для отдельного артефакта, с помощью инструментов на различных страницах.

Для назначения Тега источнику данных, требуется перейти на страницу «Источники данных», нажать по имени источника, и далее редактировать. Добавить тег для источника данных в поле «Теги».

Для назначения тега артефакту, требуется на странице активность, либо на странице в таблице артефактов перейти к информации о артефакте и в поле теги нажать по иконке  .

### *6.5 Аналитика*

Основное назначение инструментов, представленных в области **Аналитика** – это создание условий для предотвращения простых и сложных угроз, в том числе, известных и неизвестных APT-атак. Для этого в TI-сервере предусмотрены возможности создания, хранения и просмотра различных данных киберразведки. Большая часть этих данных представлена в области **Аналитика**.

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

1) **Активность;**
2) **Заключение аналитика;**
3) **Отчеты;**
4) **Граф связей;**
5) **Yara-правила;**
6) **Распространяемая аналитика;**
7) **Угрозы и злоумышленники.**

6.5.1. Активность

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

В верхней части страницы **Активность** имеются следующие активные вкладки Артефакты , Источники данных, Организации и 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.

Вид страницы **Активность** в зависимости от того, по какой вкладке был произведен вход, показан на рисунках 69 - 71.

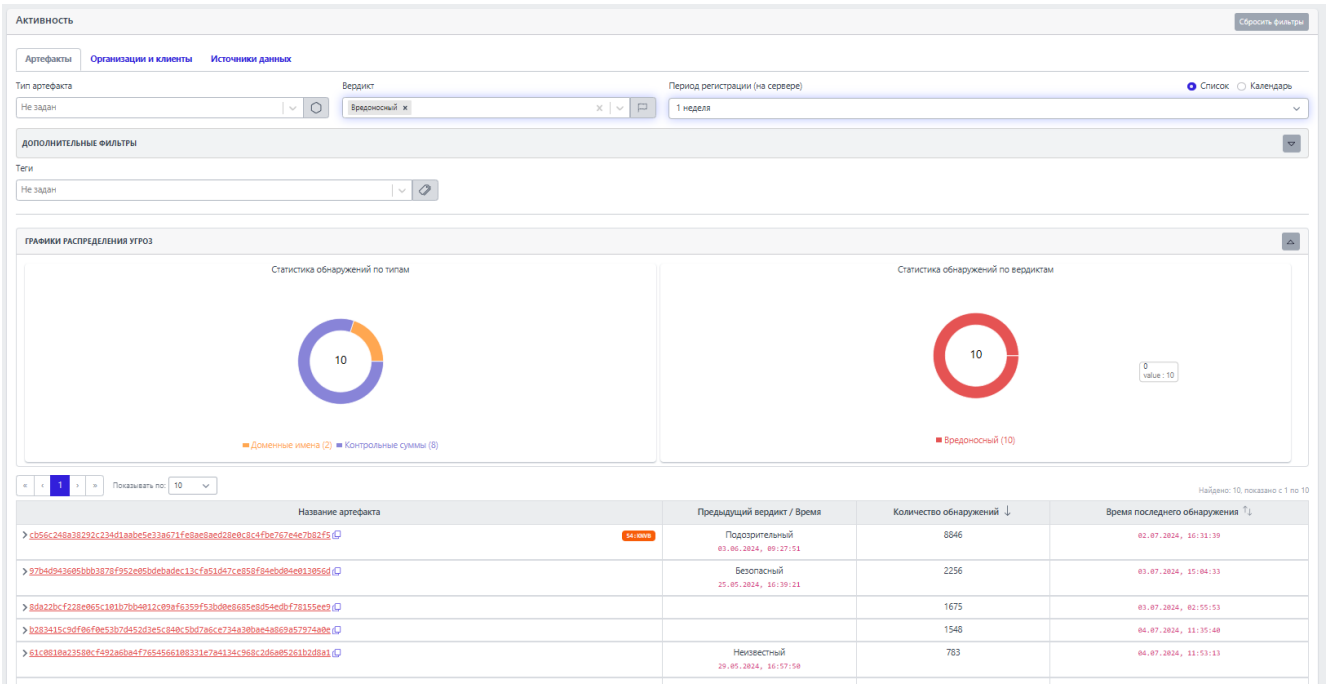



**Рисунок 69 – Страница Активность вкладка Артефакты**

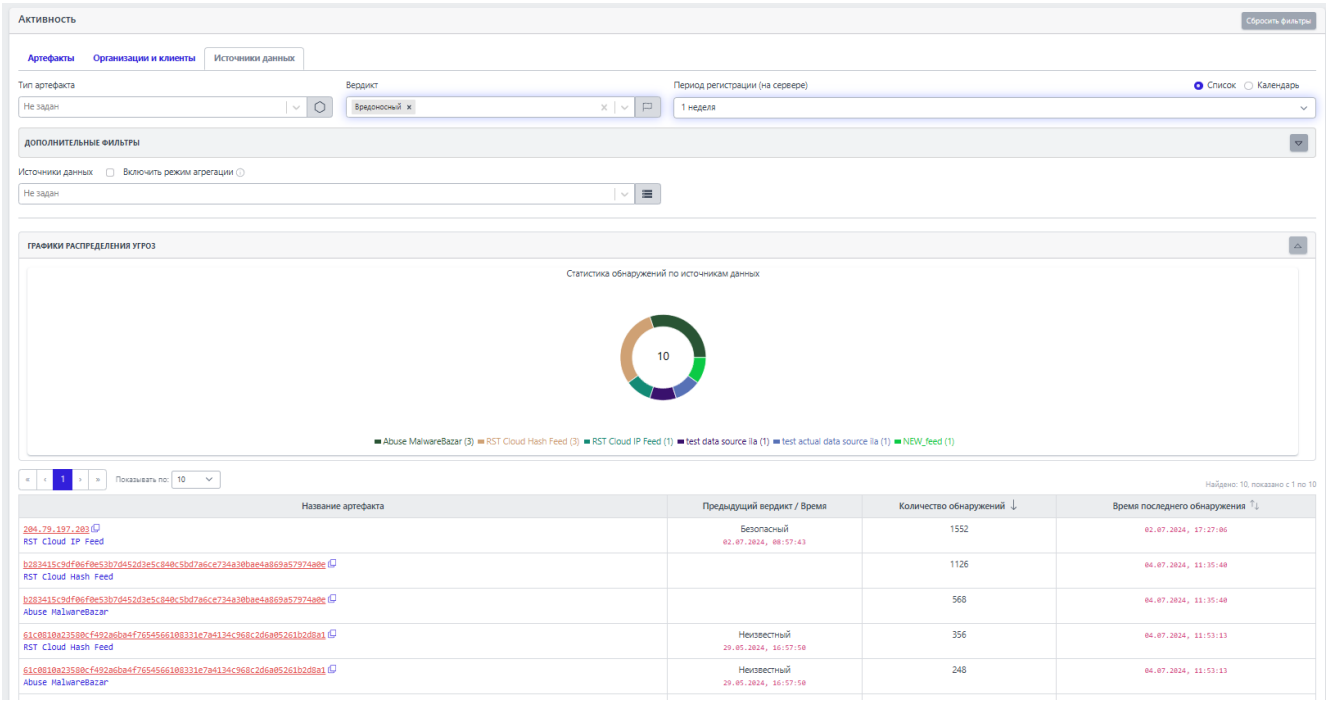



**Рисунок 70 – Страница Активность вкладка Источники данных**

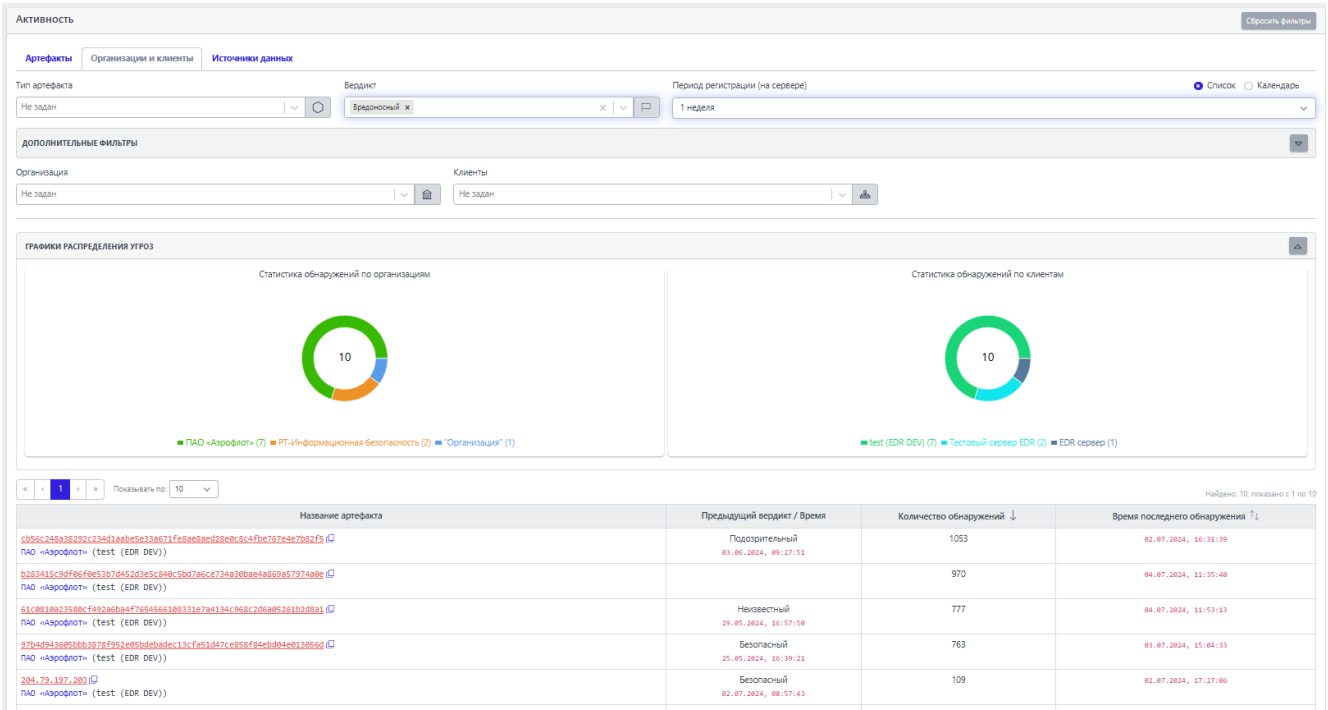



**Рисунок 71 – Страница Активность вкладка Организации и клиенты**

Таблица 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** (предыдущий вердикт по артефакту, а также дата и время внесения 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:

– 630ae106a99ae7da5d8dd33e7704b27701f69 – вредоносный артефакт (шрифт красного цвета);

– 02f0c498bb4e5f62722ab5e8a63f5b3779db88ef – безопасный артефакт (шрифт зеленого цвета);

– B73753C4C69A03F9A3E09F121B6599D77B1A4BE0247F9B71B56572555E1FE12B – неизвестный артефакт (шрифт серого цвета);

– 61F897ED69646E0509F6802FB2D7C5E88C3E3B93C4CA86942E24D203AA878863 – подозрительный артефакт (шрифт оранжевого цвета).

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.

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 72.

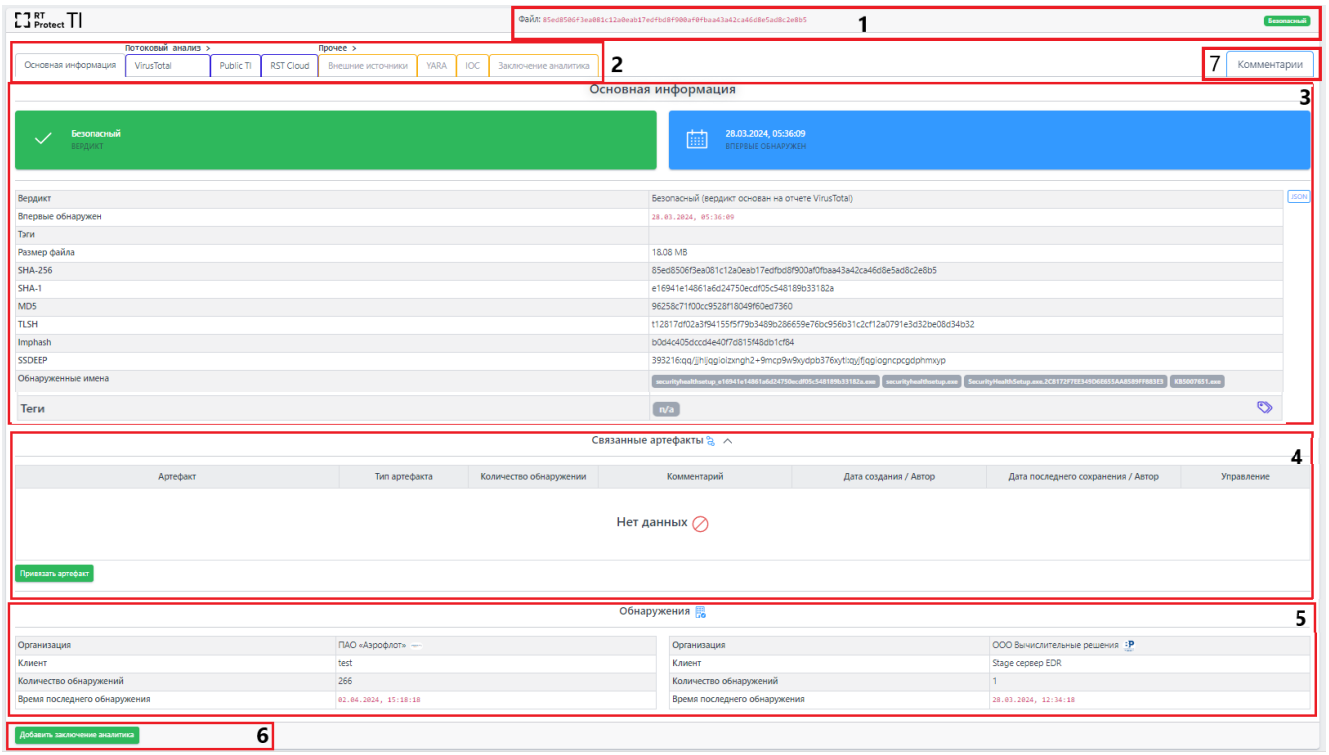



**Рисунок 72 – Страница отчета сервиса по обнаруженной угрозе**

Страница отчета программы об угрозе разделена на следующие области:

1) область краткой информации об угрозе;

2) область вкладок;

3) область основной информации;

4) область связанных с артефактом других артефактов;

5) область обнаружения (оказывает другие организации на которых были обнаружения по данному артефакту);

6) область добавления заключения аналитика;

7) область для добавления комментария.

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 вкладок отображается вкладка основной информации отчета TI-платформы, вкладки отчетов по угрозе от сторонних подключенных сервисов, разделенных по группам:

1) потоковый анализ (Virus Total, Public TI, RST Cloud и т.д.);

2) остальные (Внешние источники, YARA, IOC, Заключение аналитика).

Состав этих вкладок может меняться в зависимости от интегрированных модулей и интеграций.

Если в области вкладок запись отображается серым цветом, запрос информации по данному артефакту в том или ином сервисе недоступен. При нажатии ЛКМ по одной из вкладок появляется окно результатов по анализу артефакта (рис. 73).

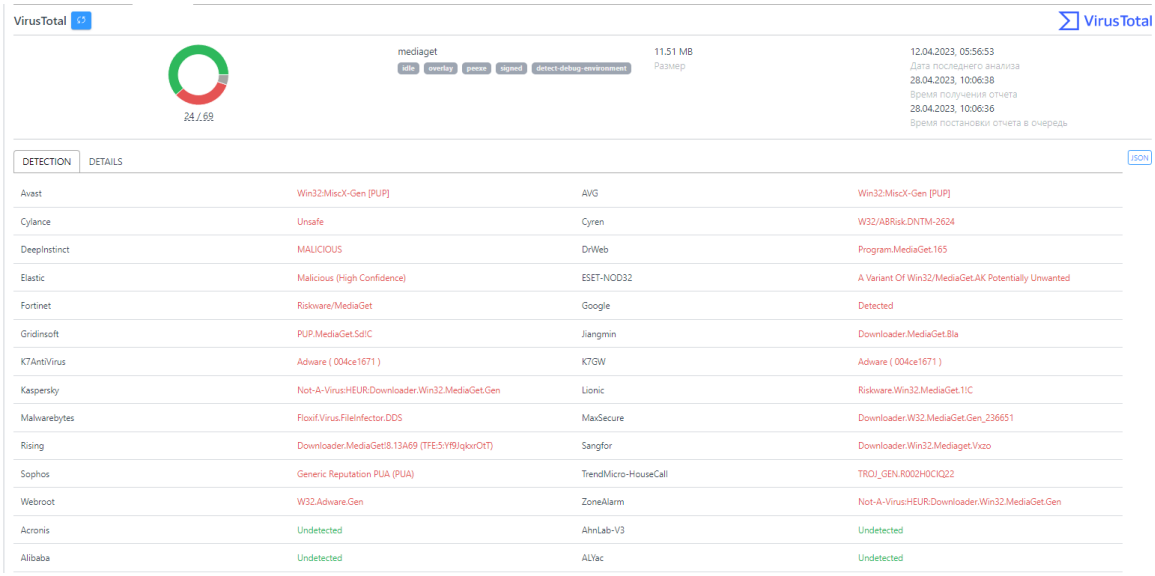



**Рисунок 73 – Результаты анализа артефакта на странице Virus Total**

Окно основной информации по результатам анализа артефакта в формате HTML представлено на рисунке 74.

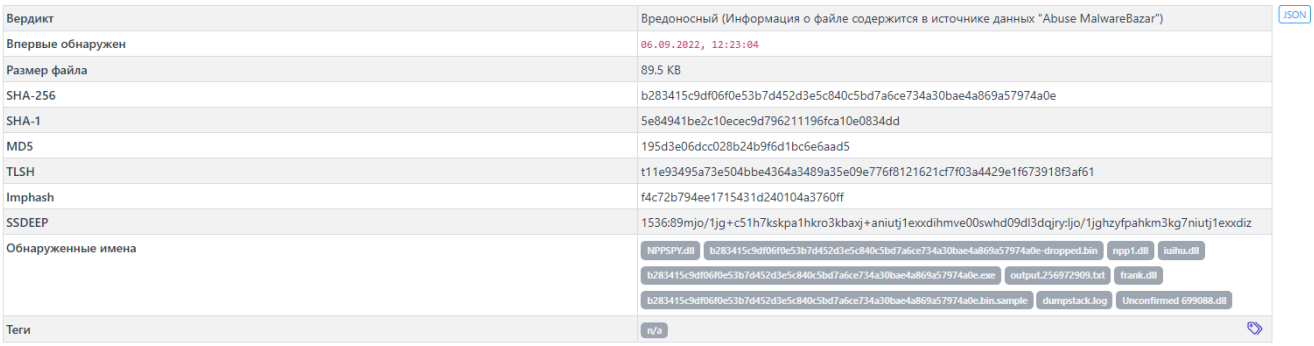



**Рисунок 74 – Информация  отчета об артефакте в формате HTML**

Окно основной информации по результатам анализа артефакта в формате JSON представлено на рисунке 75.

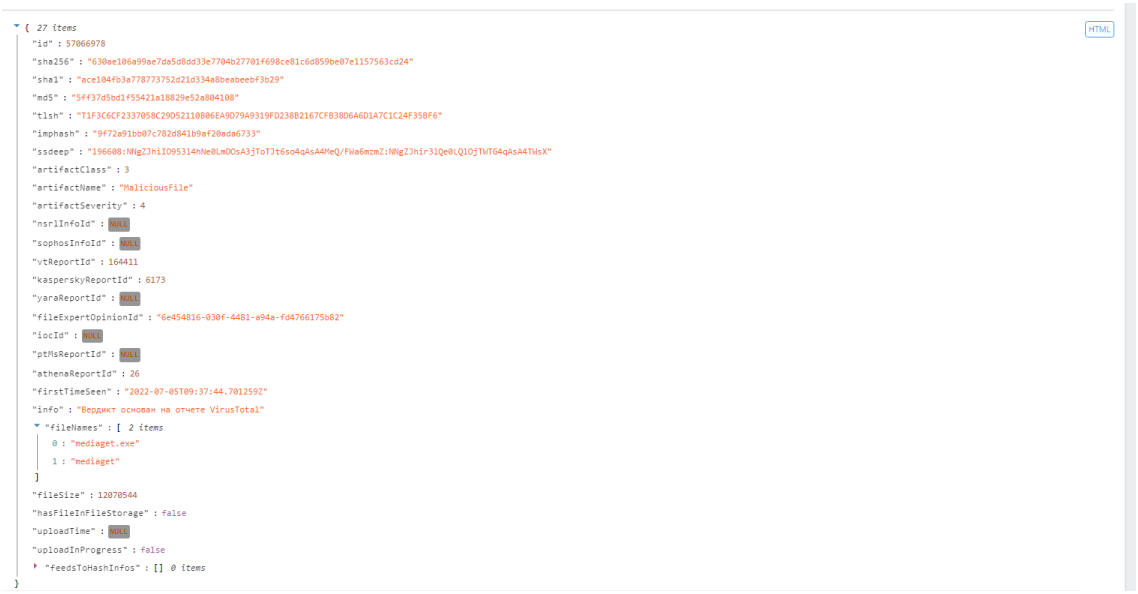
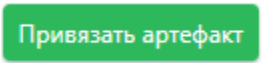



**Рисунок 75 – Информация отчета об артефакте в формате JSON**

В области **Связанные артефакты** показывается таблица с описанием артефакта, связанного с тем артефактом, отчет по которому просматривается на данный момент. При нажатии по иконке 

открывается окно для привязки артефактов друг к другу (см. рисунок 76).

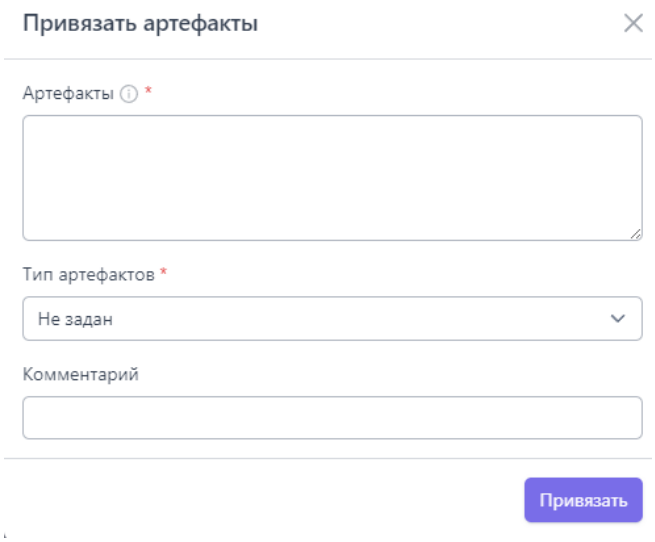



**Рисунок 76 – Окно для привязки артефакта**

В данном окне добавляется один или несколько артефактов, тип артефакта и комментарий.

После добавления информации следует нажать по иконке **Привязать**. После привязки артефакт появится в списке связанных артефактов.

---

**Примечание**

Привязка разных типов артефактов допускается. Т.е. ip-адрес и хеш-сумма могут быть привязаны друг к другу.

---

Для любого артефакта, хранящегося на сервере аналитики, администратор или аналитик может создать заключение, которое будет показывать, как артефакт определяется в программе. То есть заключение аналитика является приоритетным по отношению к любым внешним источникам данных.

При нажатии по иконке Добавить заключение аналитика появляется окно, в котором администратор/аналитик выносят вердикт по результатам анализа артефакта (рис. 77).

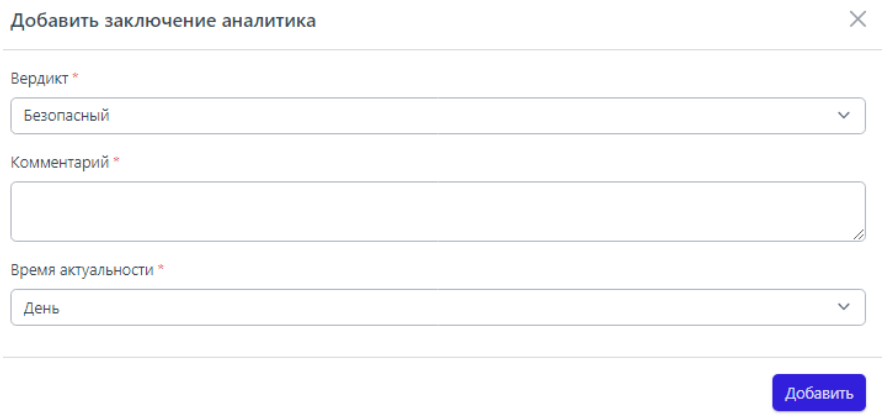



**Рисунок 77 – Окно добавления заключения аналитика**

После заполнения информации в данном окне требуется сохранить результат, нажав по иконке **Добавить.**

После добавления заключения аналитика информацию можно просмотреть, перейдя на вкладку **Заключение аналитика** на странице с отчетом (рисунок 78).

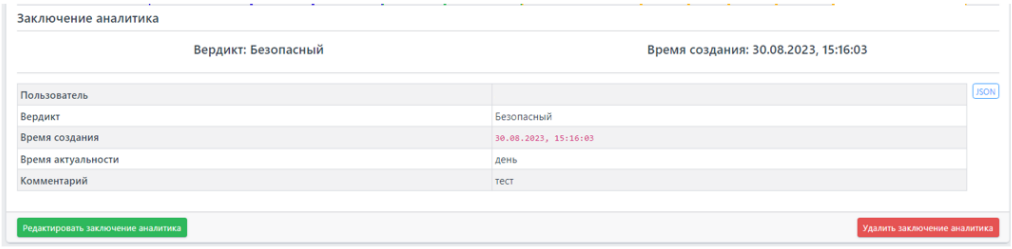



**Рисунок 78 – Информация в поле «Заключение аналитика»**

Заключение аналитика можно редактировать или удалить, нажав по соответствующим иконкам.

Заключение аналитика является приоритетным для любого артефакта в программе, поэтому пользователь программы может обозначать артефакты, которые внешними источниками отмечены безопасными, как вредоносные и наоборот. Пользователь может в любой момент отредактировать вердикт по артефакту по своему усмотрению, добавив или отредактировав заключение аналитика.

Для добавления комментария на странице отчет TI-платформы по обнаруженной угрозе требуется нажать по иконке 

, после чего откроется поле добавления комментария, представленное на рисунке 79.


**Рисунок 79 – Окно введения комментария**

После ввода текста комментария требуется нажать по иконке  , после чего появится короткое всплывающее сообщение о добавлении комментария, и он будет добавлен в поле **Комментарии** с указанием, какой пользователь и когда добавил комментарий. После добавления комментария имеется возможность его редактировать или удалить.

В области **Основная информация** в нижней строке имеется иконка  , с помощью которой можно добавить тег для артефакта. При нажатии по данной иконке во всплывающем окне (см. рисунок 80) можно выбрать тег из списка тегов, созданных с помощью раздела **Теги**.

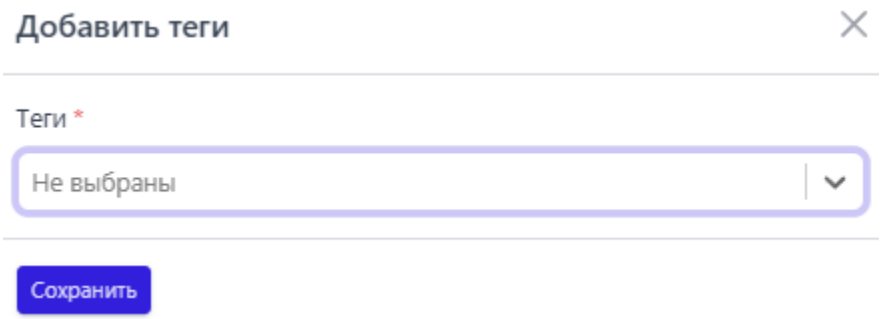



**Рисунок 80 – Добавление Тега**

Для фильтрации информации на странице **Активность** вкладки **Артефакты** 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, все время), либо в виде календаря (начальная и конечная даты);

– **Теги.**

Также имеется система дополнительных фильтров, которые по умолчанию скрыты, но при нажатии по кнопке  появляются следующие фильтры, которые представлены на рисунке 81.

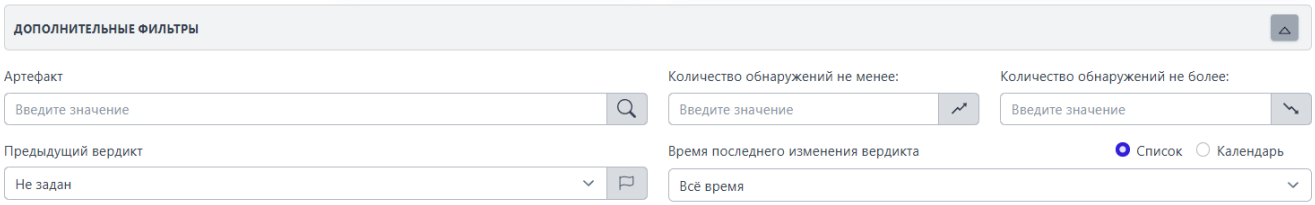



**Рисунок 81 – Дополнительные фильтры на странице Активность/Артефакты**

Дополнительные фильтры представлены согласно следующему списку:

– **Артефакт** (в данном фильтре можно указать любой артефакт: IP-адрес, доменное имя и т.д.);

– **Количество обнаружений не менее** (фильтрация по количеству обнаружений, не менее указанного в фильтре);

– **Количество обнаружений не более** (фильтрация по количеству обнаружений, не более указанного в фильтре);

– **Предыдущий вердикт;**

– **Время последнего изменения вердикта.**

На странице **Активность** вкладки **Артефакты** имеется область с графическим отображением информации по обнаруженным угрозам (рисунок 82).

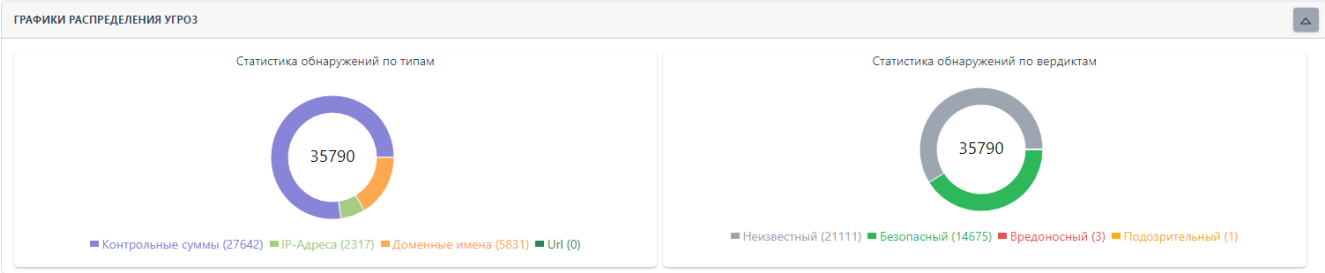



**Рисунок 82 – Область графического отображения информации по обнаруженным угрозам вкладка «Артефакты»**

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 **Источники данных** 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).

Также имеется система дополнительных фильтров, которые по умолчанию скрыты, но при нажатии по кнопке  появляются следующие фильтры, которые представлены на рисунке 83.

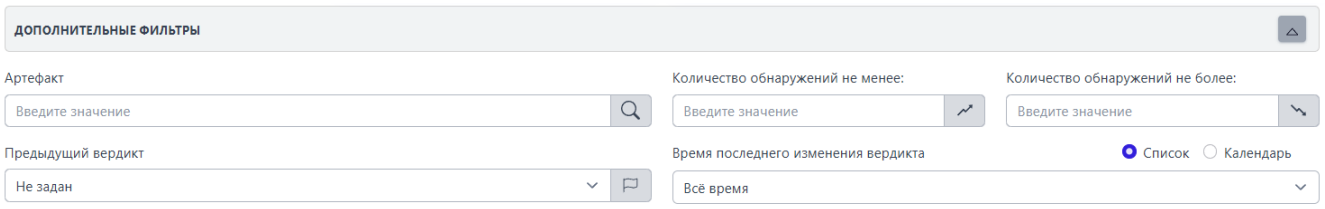



**Рисунок 83 – Дополнительные фильтры на странице Активность/ вкладки Источники данных**

Дополнительные фильтры представлены согласно следующему списку:

– **Артефакт** (в данном фильтре можно указать любой артефакт: IP-адрес, доменное имя и т.д.);

– **Количество обнаружений не менее** (фильтрация по количеству обнаружений, не менее указанного в фильтре);

– **Количество обнаружений не более** (фильтрация по количеству обнаружений, не более указанного в фильтре);

– **Предыдущий вердикт;**

– **Время последнего изменения вердикта;**

В фильтре источника данных можно осуществить выборку по критериям согласно следующему списку:

– по одному источнику данных;

– по нескольким источникам данных;

– по всем источникам данных согласно одной категории.

---

**Важно**

Следует отметить, что после выставления в фильтре источников данных параметров для фильтрации, в таблице активности будут отображаться артефакты согласно выставленным источникам данных, но основополагающим вердиктом будет вердикт, установленный аналитиком.

---

При установке галочки напротив надписи «Включить режим агрегации» в фильтре **Источники данных** появятся два поля, с помощью которых можно производить фильтрацию в таблице активности (см. рисунок 84).

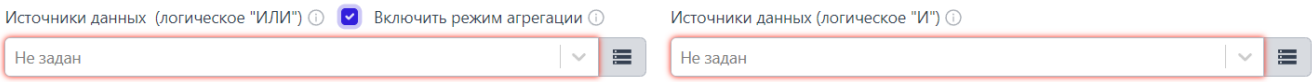



**Рисунок 84 – Фильтр по источнику данных на странице Активность**

На странице **Активность** вкладки **Источники данных** имеется область с графическим отображением информации по обнаруженным угрозам (рисунок 85).

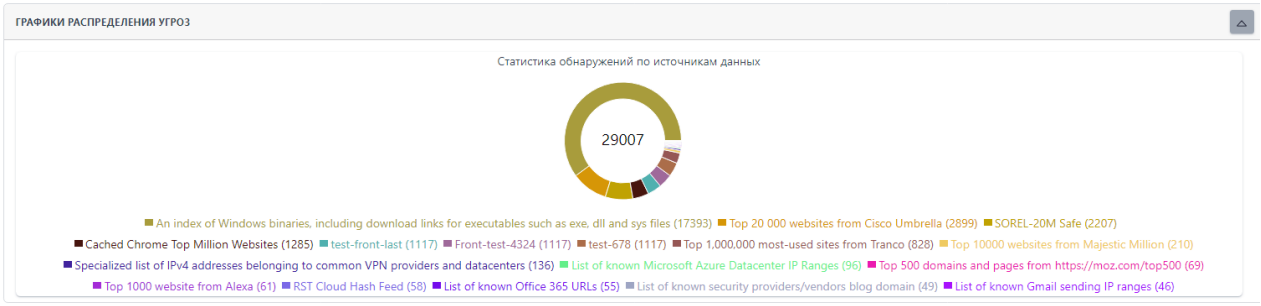



**Рисунок 85 – Область графического отображения информации по обнаруженным угрозам вкладка Источники данных**

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

– статистика обнаружений по источникам данных.

Для фильтрации информации на странице **Активность** вкладка **Организации и 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);

Также имеется система дополнительных фильтров, которые по умолчанию скрыты, но при нажатии по кнопке появляются следующие фильтры, которые представлены на рисунке 86.

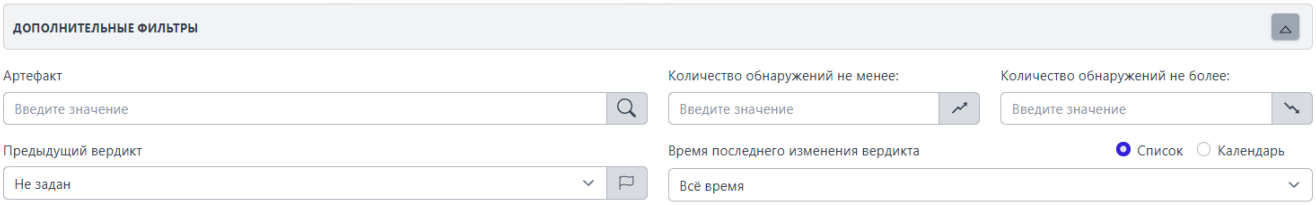



**Рисунок 86 – Дополнительные фильтры на странице Активность/Организации и клиенты**

Дополнительные фильтры представлены согласно следующему списку:

– **Артефакт** (в данном фильтре можно указать любой артефакт: IP-адрес, доменное имя и т.д.);

– **Количество обнаружений не менее** (фильтрация по количеству обнаружений, не менее указанного в фильтре);

– **Количество обнаружений не более** (фильтрация по количеству обнаружений, не более указанного в фильтре);

– **Предыдущий вердикт;**

– **Время последнего изменения вердикта;**

– **Организация;**

– **Клиенты.**

На странице **Активность** вкладки **Организации и клиенты** имеется область с графическим отображением информации по обнаруженным угрозам (рисунок 87).

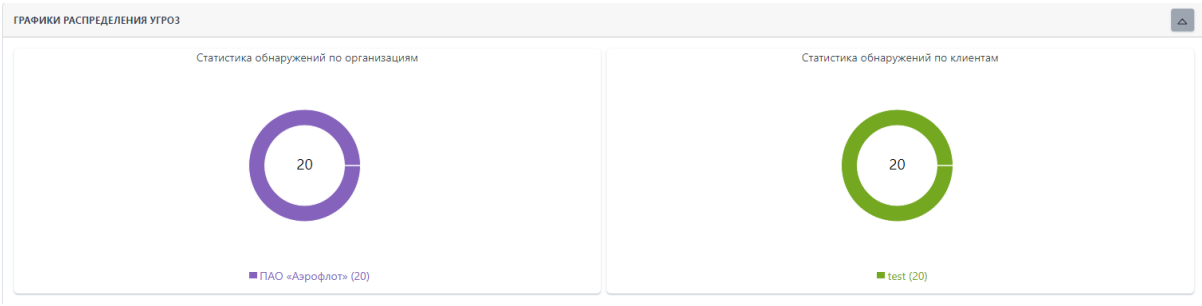



**Рисунок 87 – Область графического отображения информации по обнаруженным угрозам вкладка Организации и клиенты**

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

– статистика обнаружений по организациям;

– статистика обнаружений по клиентам.

### 6.5.2. Заключения аналитика

В разделе **Заключение аналитика** в табличной форме представлена информация о зарегистрированных на портале заключениях аналитика. Общий вид страницы представлен на рисунке 88.

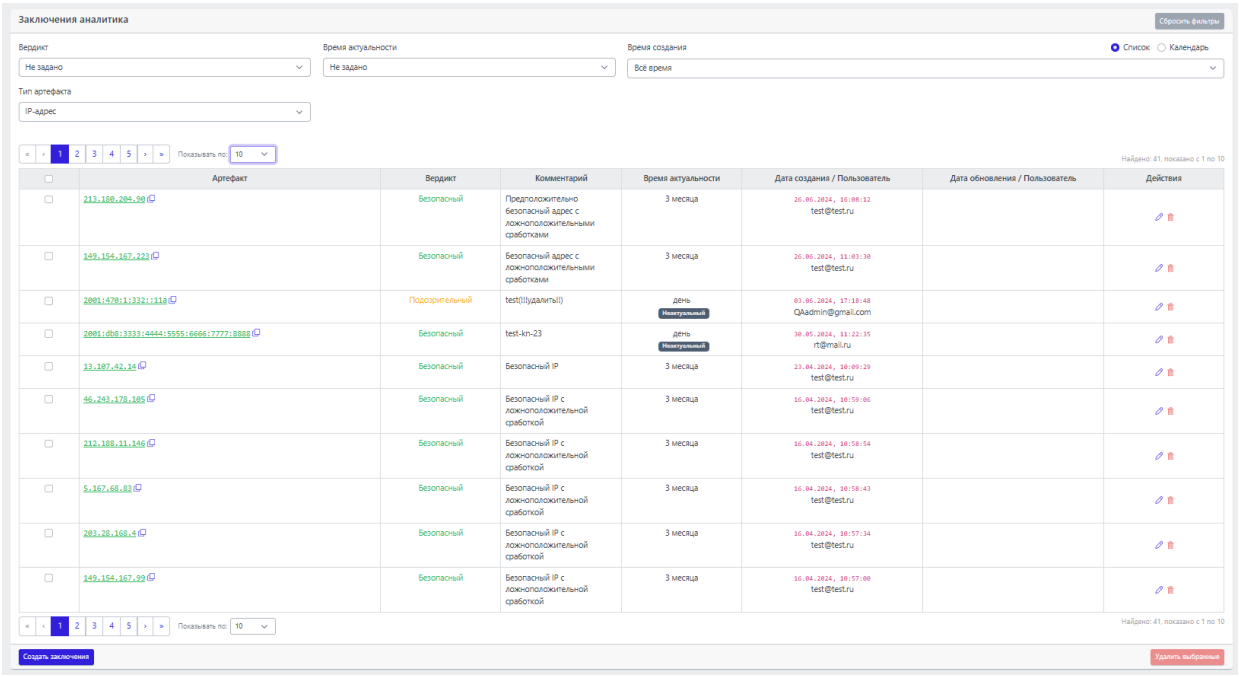



**Рисунок 88 – Страница Заключения аналитика**

В таблице имеются следующие поля:

– Артефакт (в столбце отображается артефакт, для которого имеется заключение аналитика);

– Вердикт (в столбце отображается вердикт для артефакта);

– Комментарий;

– Время актуальности (отображается время, показывающее, сколько будет актуален вердикт (заключение аналитика) по данному артефакту;

– Дата создания/Пользователь;

– Дата обновления/Пользователь;

– Действия (редактирование, удаление заключения аналитика).

Для фильтрации информации на странице имеется система фильтров, представленная согласно следующему списку:

– Вердикт (не задано, безопасный, вредоносный, подозрительный);

– Время актуальности (не задано, день, неделя, месяц, три месяца, бесконечно);

– Время создания (возможно задать начальную и конечную дату, а также время создания заключения);

– Тип артефакта (файл, ip-адрес, доменное имя, URL, Email).

В столбцах **Артефакт** и **Вердикт** для наглядности представления записи выделены различными цветами согласно следующему списку:

– 630ae106a99ae7da5d8dd33e7704b27701f69 – вредоносный артефакт (шрифт красного цвета);

– 02f0c498bb4e5f62722ab5e8a63f5b3779db88ef – безопасный артефакт (шрифт зеленого цвета);

– 61F897ED69646E0509F6802FB2D7C5E88C3E3B93C4CA86942E24D203AA878863 – подозрительный артефакт (шрифт оранжевого цвета).

В столбце **Артефакт** 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.

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

Для редактирования заключения аналитика необходимо в столбце **Действия** нажать по иконке , при этом открывается окно, представленное на рисунке 89.

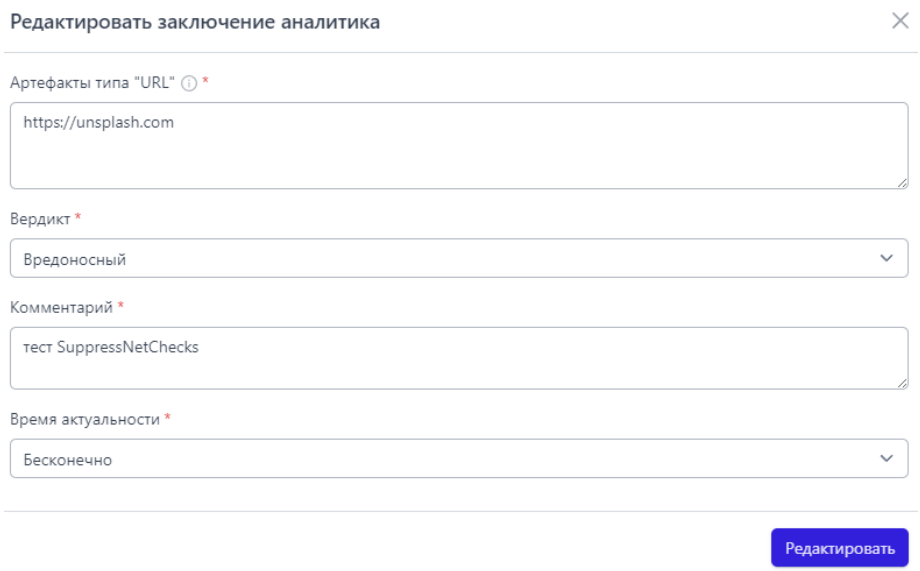



**Рисунок 89 – Окно редактирования заключения аналитика**

В данном окне после редактирования информации по заключению требуется нажать по иконке **Редактировать**, после чего окно редактирования исчезнет, и появится короткое всплывающее сообщение с надписью **Заключение обновлено**.

Для удаления заключения аналитика в столбце **Действия** требуется нажать по иконке , после чего появится окно, в котором следует подтвердить (либо отменить) действие удаления (рисунок 90).

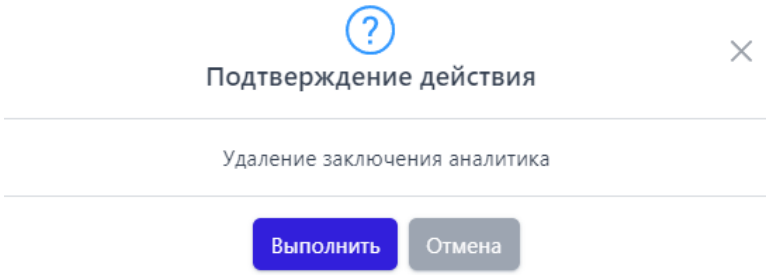
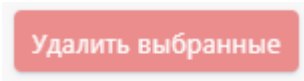
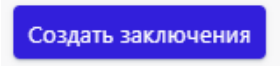



**Рисунок 90 – Окно подтверждения действия удаления заключения аналитика**

Для удаления нескольких записей на странице необходимо отметить кнопкой выбора запись (либо несколько записей), которые необходимо удалить, после чего нажать по иконке 

. Для завершения операции следует в окне подтверждения подтвердить, либо отменить запись.

Для создания нового заключения аналитика требуется нажать по иконке 

, после чего откроется окно создания заключения, представленное на рисунке 91.

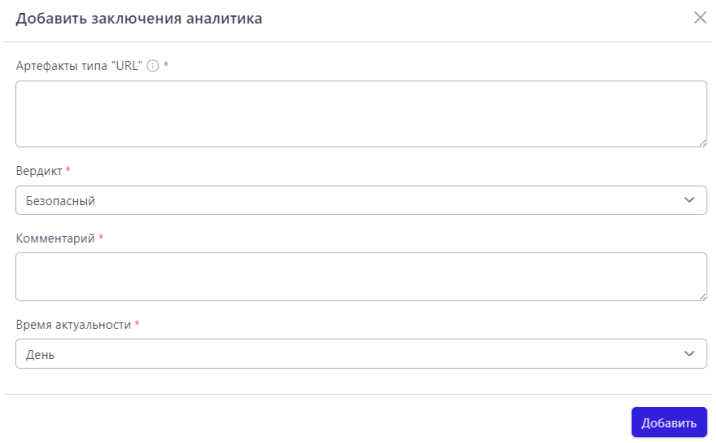



**Рисунок 91 – Окно добавления заключения аналитика**

В списке артефактов для которых добавляется заключение аналитика можно указать разные типы артефактов и после добавления заключения аналитика, заключение будет добавлено для каждого типа артефакта.

После заполнения полей следует нажать по иконке **Добавить**. После подтверждения действия по добавлению новое заключение аналитика будет отображаться в списке на странице **Заключения аналитика.**

### 6.5.3. Отчеты

В разделе **Отчеты** в табличной форме представлена информация о проверенных внешними анализаторами артефактах, для которых настроена интеграция. Общий вид страницы представлен на рисунке 92.

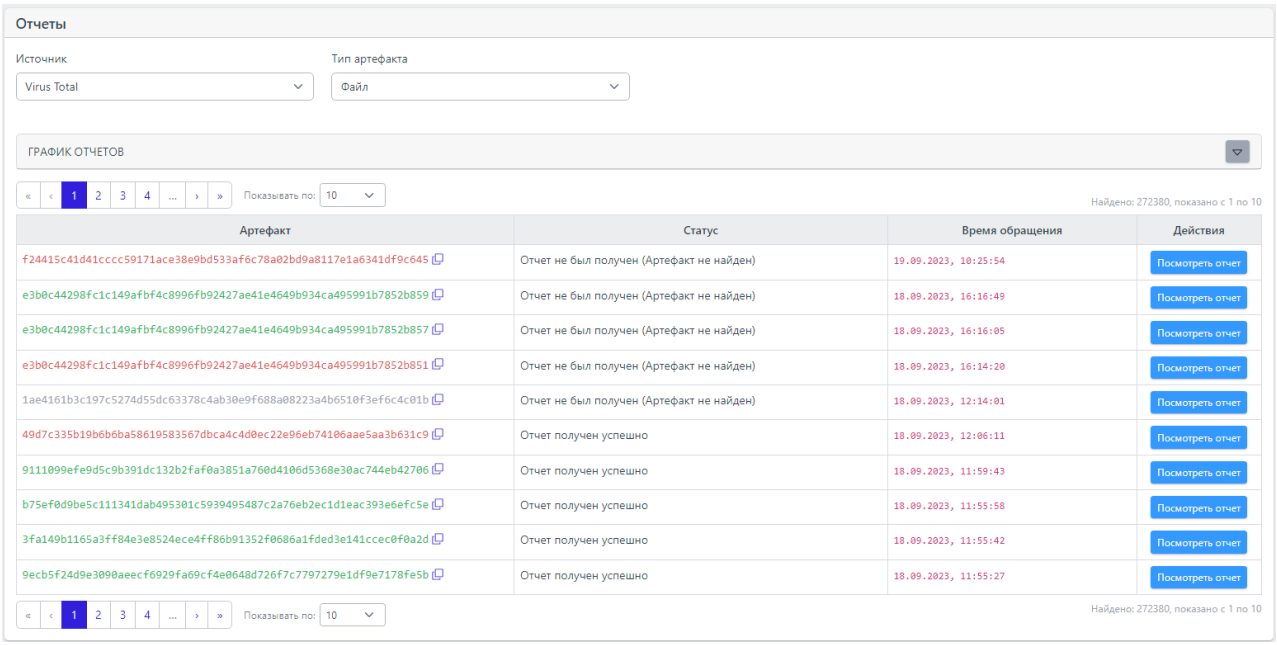



**Рисунок 92 – Окно раздела «Отчеты»**

В таблице имеются следующие поля:

– **Артефакт** (в столбце отображается информация о проверенном артефакте в зависимости от типа артефакта (хеш сумма, IP-адрес, доменное имя, URL);

– **Статус** (в столбце отображается информация о получении отчета (отчет получен успешно, отчет не был получен));

– **Время обращения** (время, в которое был запрошен отчет);

– **Действия** (получить отчет).

Информация об артефакте отображается разными цветами:

– шрифт красного цвета (артефакт является вредоносным);

– шрифт зеленого цвета (артефакт является безопасным);

– шрифт серого цвета (неизвестный артефакт);

– шрифт оранжевого цвета (артефакт является подозрительным).

Над таблицей для фильтрации информации имеются следующие фильтры:

– **Источник** (Virus Total, Public TI, Athena, RST Cloud);

– **Тип артефакта** (файл, IP-адрес, доменное имя, URL).

Над таблицей для отображения визуальной информации имеется область с графиком полученного числа отчетов за определенный период в зависимости от установленного в фильтре источника данных (рисунок 93).

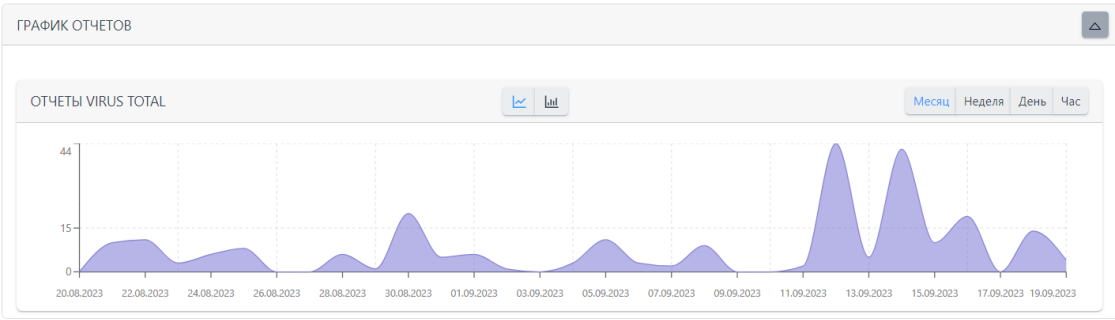



**Рисунок 93 – Отчеты Virus Total**

Для сворачивания области **График отчетов** требуется нажать по иконке .

Для просмотра отчета по артефакту нужно нажать по иконке Посмотреть отчет.

Страница отчета по артефакту представлена на рисунке 94.

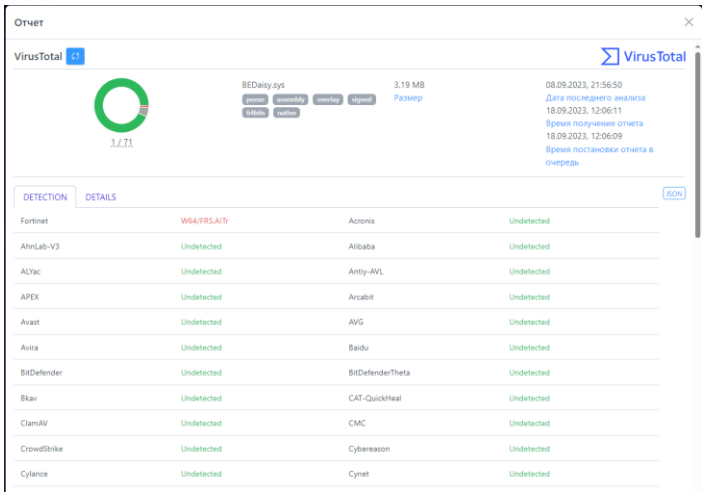



**Рисунок 94 – Страница отчета по артефакту от источника Virus Total**

6.5.4. Граф связей

Страница **Граф связей** с незаполненным полем артефакта представлена на рисунке 95.

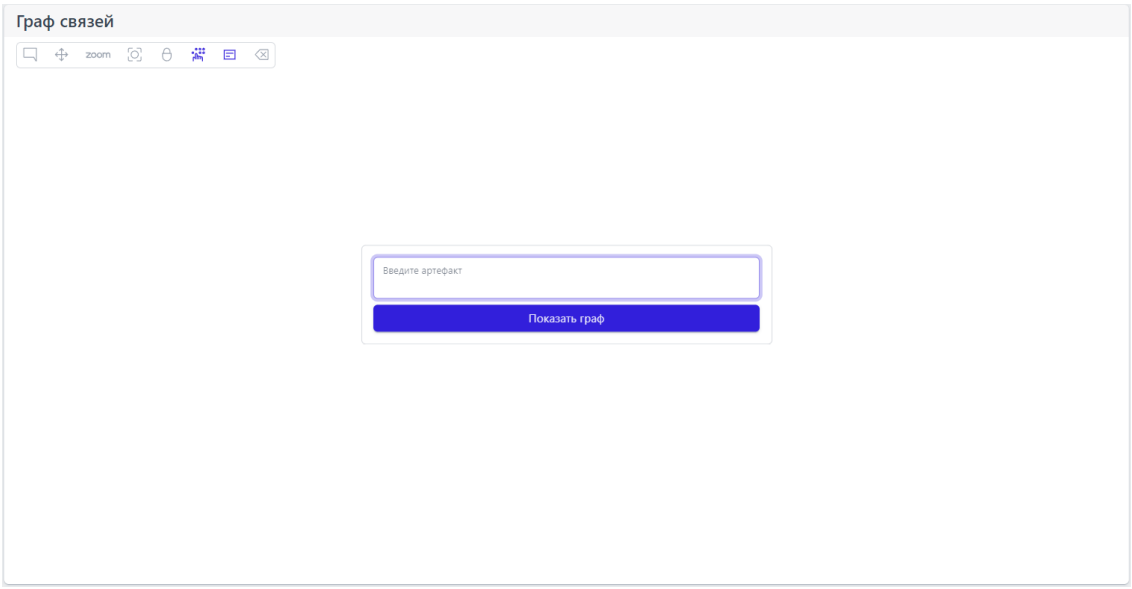



**Рисунок 95 – Общий вид пустой страницы «Граф связей»**

На странице имеется две области:

– область с иконками-подсказками для управления визуальной частью графа;

– область для введения информации по артефакту, для которого требуется построить граф.

В области управления визуальной частью графа находятся иконки, при наведении на которые указателя мыши появляются всплывающие сообщения (подсказки) для управления графом.

Пример отображения графа после заполнения поля артефакта в виде ip-адреса представлен на рисунке 96.

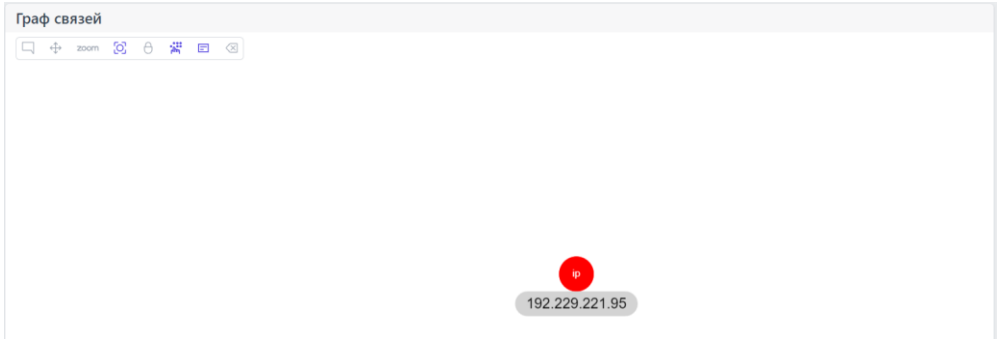



**Рисунок 96 – Отображение графа связей для артефакта типа ip-адрес**

Пример отображения графа связей для артефакта типа домен с привязанными артефактами представлен на рисунке 97.

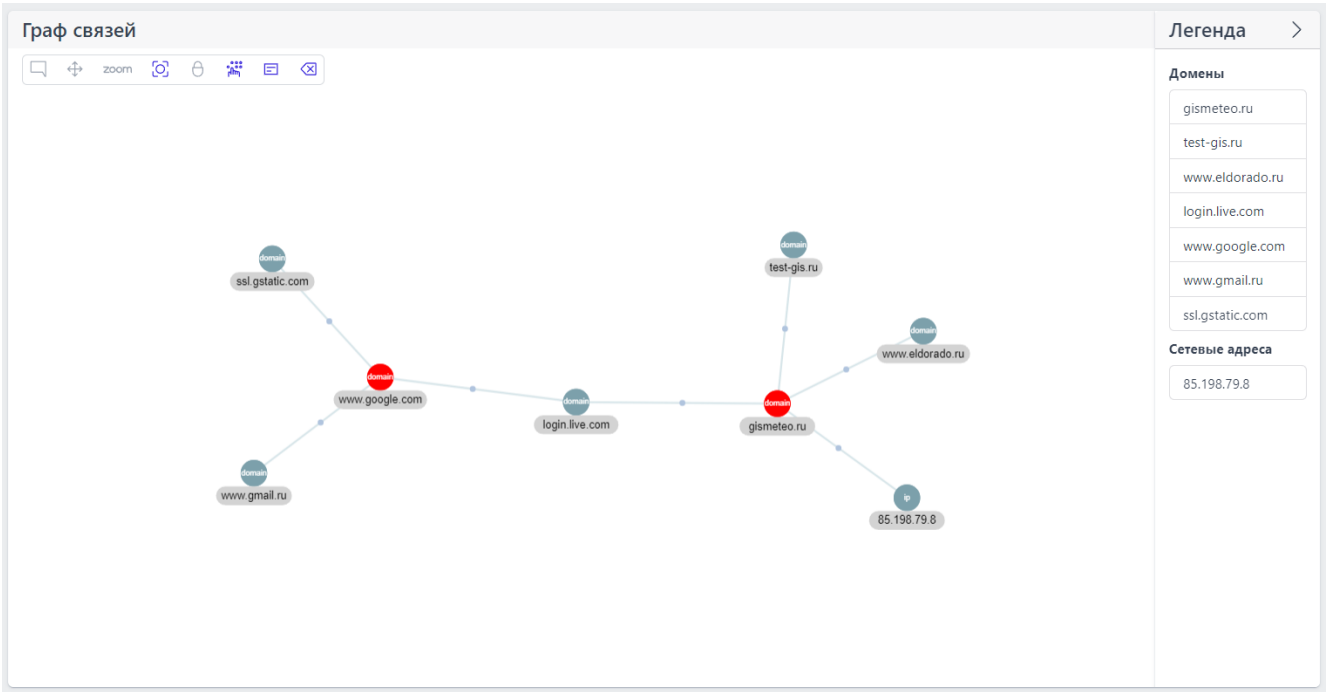



**Рисунок 97 – Отображения графа связей для артефакта типа домен с привязанными артефактами**

На данной странице графа в правой части имеется столбец **Легенда**, отображающий связанные с артефактом другие артефакты.

Для того, чтобы скрыть столбец с информацией по привязанным артефактам, следует нажать ЛКМ по иконке  .

При нажатии ЛКМ по круглой области отрисовки графа отображается информация об артефакте (смотри рисунок 98).

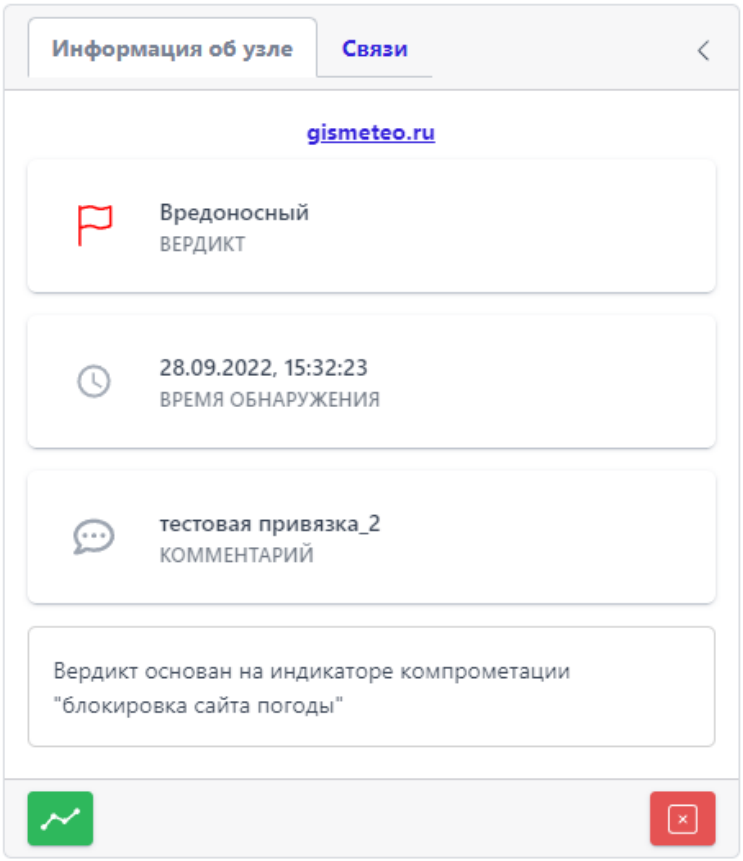



**Рисунок 98 – Информация по артефакту**

При нажатии по активной области **Связи** появится окно, показывающее список связей данного артефакта (рисунок 99).

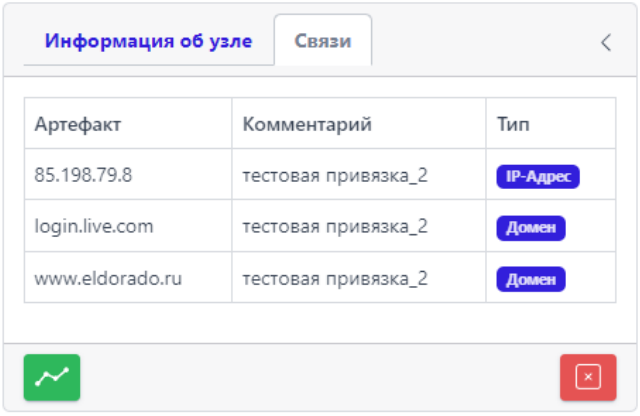



**Рисунок 99 – Связи по данному артефакту**

При нажатии по иконке, идентифицирующей артефакт, происходит переход на страницу отчета по данному артефакту.

Для привязки нового артефакта к выбранному артефакту следует нажать по иконке  , после чего появляется окно для внесения информации по привязанному артефакту, представленное на рисунке 100.

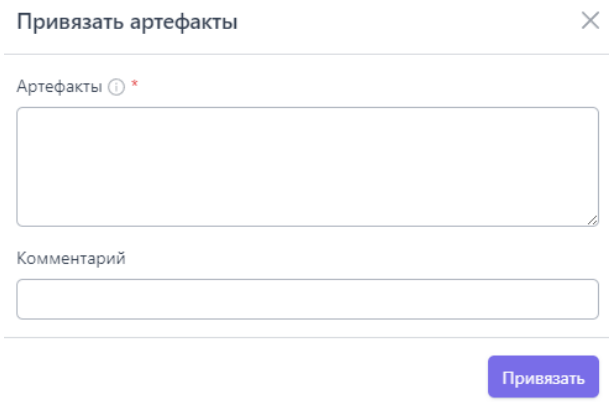



**Рисунок 100 – Окно добавления информации для привязывания артефакта**

После добавления информации в данном окне следует нажать по иконке **Привязать.** Привязанный артефакт будет отображаться на странице граф связей.

Для удаления связи между двумя артефактами из привязанных артефактов следует нажать по иконке  , после чего появится окно указания того, какую связь и для какого узла требуется удалить (рисунок 101).


**Рисунок 101 – Удаление связей между артефактами**

Для подтверждения удаления связи требуется нажать по иконке **Удалить**.

### 6.5.5. Yara-правила

#### Общая информация

Правила, указанные в разделе **Yara-правила** используются в качестве инструмента анализа угроз для защищаемой инфраструктуры в части анализа вредоносных файловых сигнатур. Пользователи сервера аналитики могут создавать наборы с правилами, импортировать их из CSV-файлов, а также экспортировать в CSV-файл. Добавляемые YARA-файлы используются движком YARA внутри TI-платформы для проверки загружаемых через главную страницу или API файлов.

#### Наборы Yara-правил

Страница с наборами YARA-правил (рис. 102) открывается при выборе на панели слева раздела **YARA-правила** и включает в себя следующие структурные элементы:

– кнопка **Сбросить фильтры**;

– фильтры **Название набора** и **Показывать по**;

– таблица с наборами YARA-правил;

– кнопка **Добавить набор;**

– кнопка **Удалить выбранные наборы.**

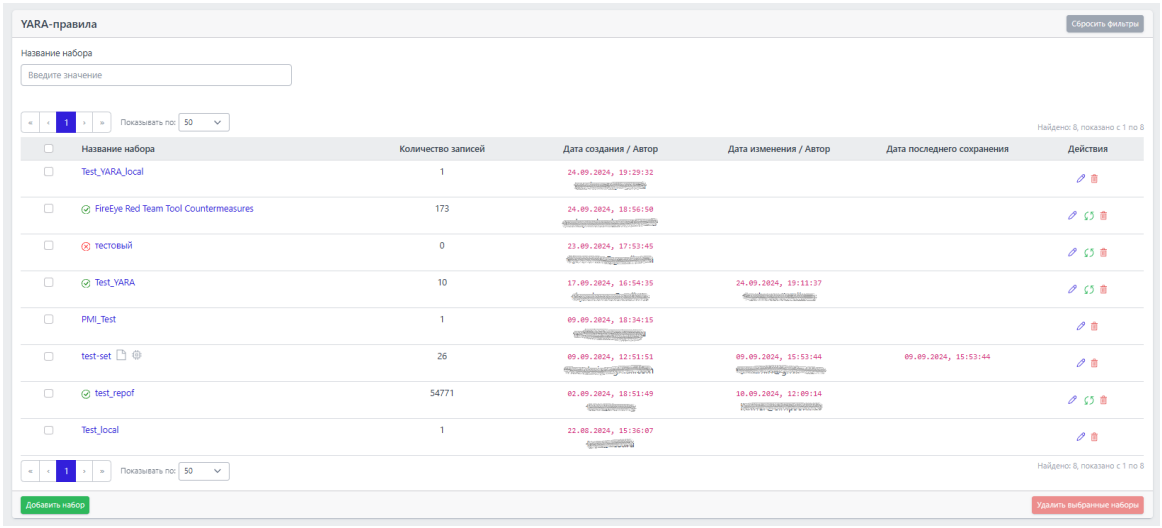



**Рисунок 102 – Наборы YARA-правил**

Наборы можно искать по названию с помощью фильтра **Название набора**.

В столбце **Действия** можно выполнить следующие действия:

– редактировать название набора (иконка );

– синхронизация правил в наборе с источником указанным при создании набора (иконка);

– удаление набора правил (иконка ).

Для добавления нового набора необходимо нажать кнопку **Добавить набор**, после чего в окне **Создать набор** (см. рисунок 103) ввести название нового набора YARA-правил. Если требуется, чтобы набор экспортировался в YARA-правила системы RT Protect EDR, необходимо поставить галочку в соответствующей строчке ниже строки названия набора.

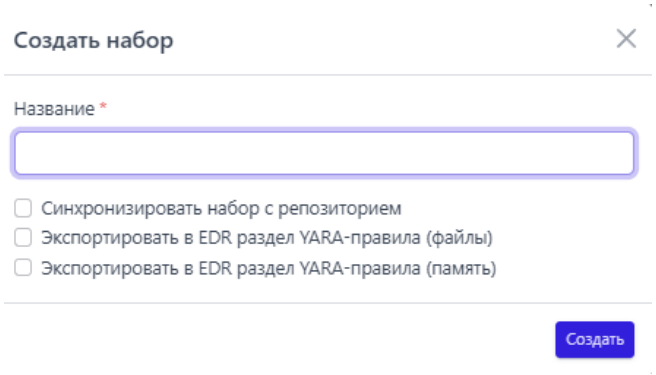



**Рисунок 103 – Создать набор YARA-правил**

При создании набора после указания что набор нужно синхронизировать с репозиторием, окно создания набора изменится и будет иметь вид представленный на рисунке

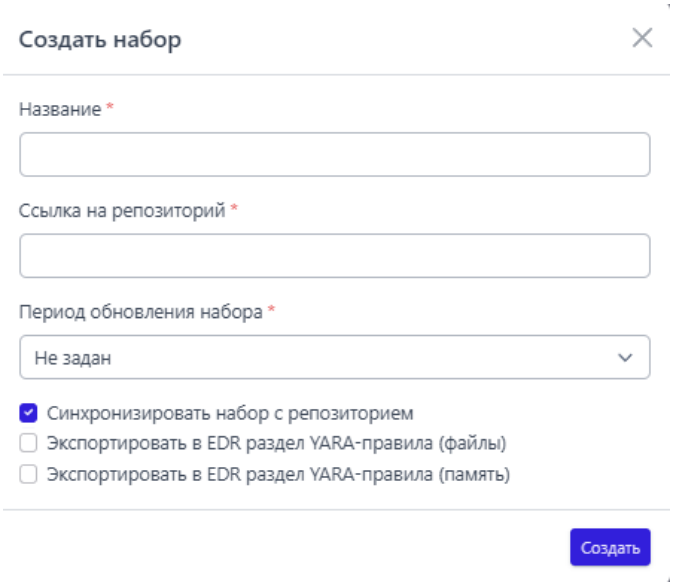



**Рисунок 104 – Создание набора синхронизированного с репозиторием**

При создании набора, требуется указать в поле **Сссылка на репозиторий** адрес репозитория, и указать период обновления набора.

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

В списке наборов на странице YARA-правила набор, который будет экспортироваться в EDR, будет помечен иконками YARA-правил для файлов и YARA-правил для памяти .

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

При нажатии ЛКМ на имени набора открывается страница **YARA-правила** для выбранного набора (рис. 105).

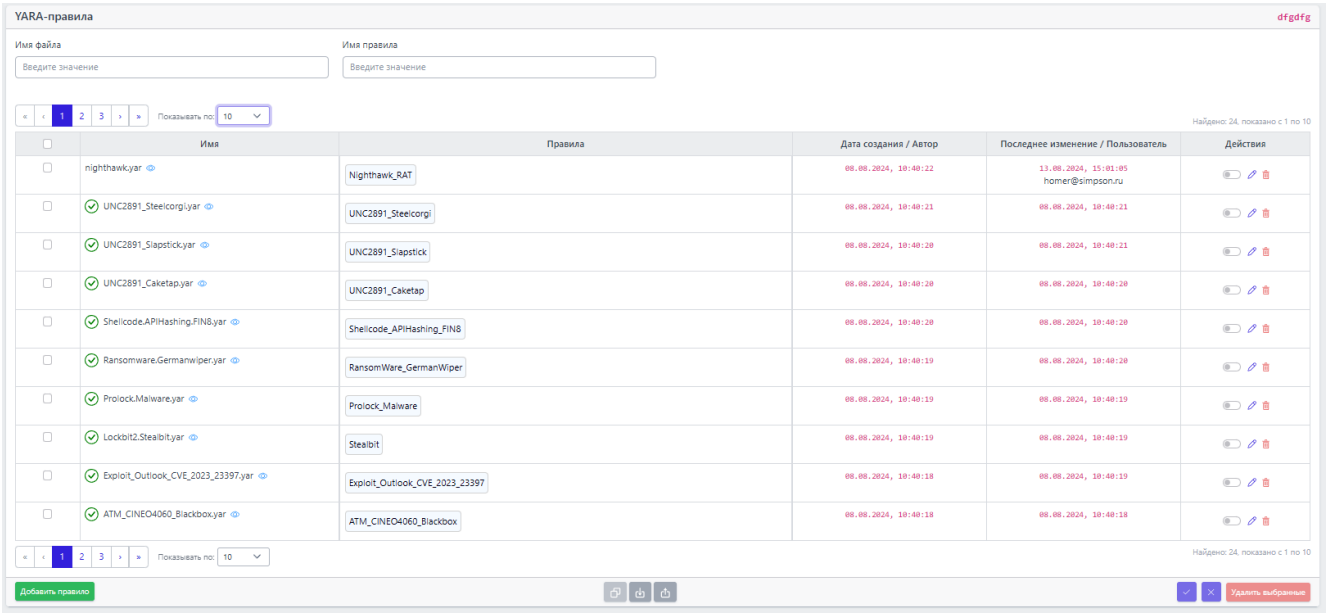



**Рисунок 105 – YARA-правила**

Страница «Yara-правила»

На странице **YARA-правила** можно выполнять следующие операции:

– просматривать правила из выбранного набора;

– добавлять новые правила в выбранный 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;

– синхронизация с GitHub.

На странице с правилами фильтрация осуществляется с помощью следующих фильтров:

– имя файла;

– имя правила.

Для добавления нового правила необходимо нажать кнопку **Добавить правило**, после чего откроется окно **Добавить правило** (рисунок 106) , в котором необходимо прописать имя правила и условие в соответствии с синтаксисом YARA, либо добавить правило из внешнего источника, предварительно выбрав источник. Подробная информация о синтаксисе YARA содержится в официальной документации YARA. Пример правила YARA приведен на рисунке 107.

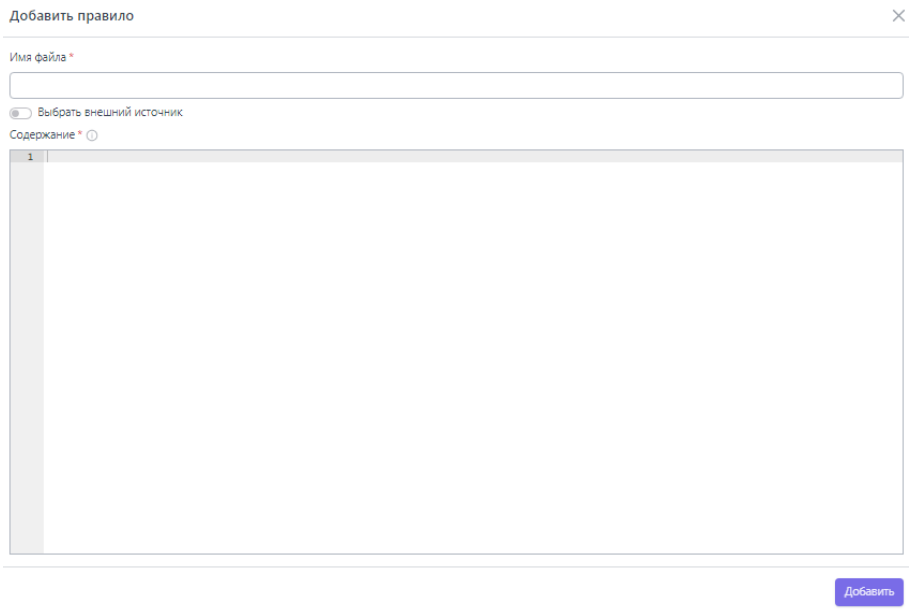



**Рисунок 106 – Окно добавления правила**


**Рисунок 107 – Пример правила YARA**

В окне добавления правила возможно добавить несколько правил, при этом каждое правило будет записано с новой строки.

Для добавления правила из внешнего источника требуется передвинуть ползунок  в положение  , при этом откроется новое окно добавления правила, представленное на рисунке 108.

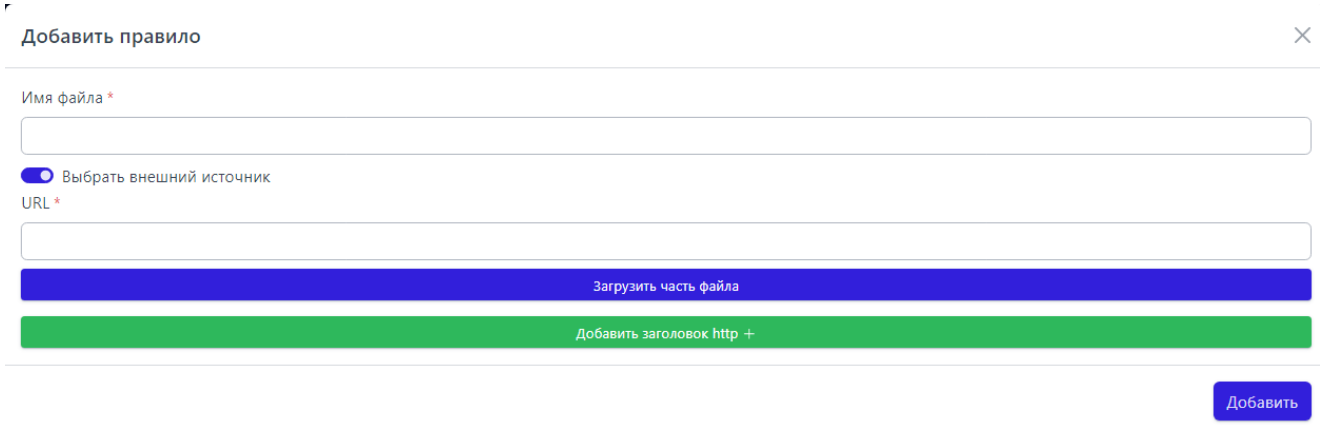



**Рисунок 108 – Окно добавления правила из внешнего источника**

Поля, помеченные символом * , являются обязательными для заполнения.

Для корректного добавления правила в данном окне требуется указать URL внешнего источника.

В списке с YARA-правилами в наборе имеется иконка , показывающая, что данное правило синхронизировано с источником.

При нажатии по иконке имеется возможность просмотреть правило.

Для экспорта набора в файл следует нажать кнопку **Экспортировать набор в файл формата YARA** (). Набор будет сохранен в папке **Загрузки** в указанном формате. Для импорта правил из файла требуется нажать кнопку **Импортировать YARA-файл** (). Далее выбрать на компьютере файл, содержащий нужные правила, и нажать кнопку **Открыть**.

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

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

Для редактирования правила следует нажать кнопку **Редактировать** ( ), после чего внести изменения в открывшемся окне с правилом. После внесения изменений в правило необходимо нажать кнопку **Сохранить**.

### 6.5.6. Распространяемая аналитика

Общие сведения

Распространяемая аналитика позволяет определить артефакты, в автоматическом режиме распространяемые на всех клиентов, взаимодействующих с TI, если они поддерживают соответствующий формат данных. Аналитика основана на концепции «теневых наборов». Подробнее о «теневых наборах» смотри в пункте 6.5.8.

На странице раздела Распространяемая аналитика пользователь сервиса RT Protect TI, имеющий права Администратора/Аналитика, создает аналитические наборы, которые могут быть предоставлены пользователю, подключенному к платформе, при составлении договора на обслуживание и переданы ссылкой вместе с токеном, сгенерированным для нового клиента.

Наборы распространяемой аналитики

Страница раздела «Распространяемая аналитика» представлена на рисунке 109.

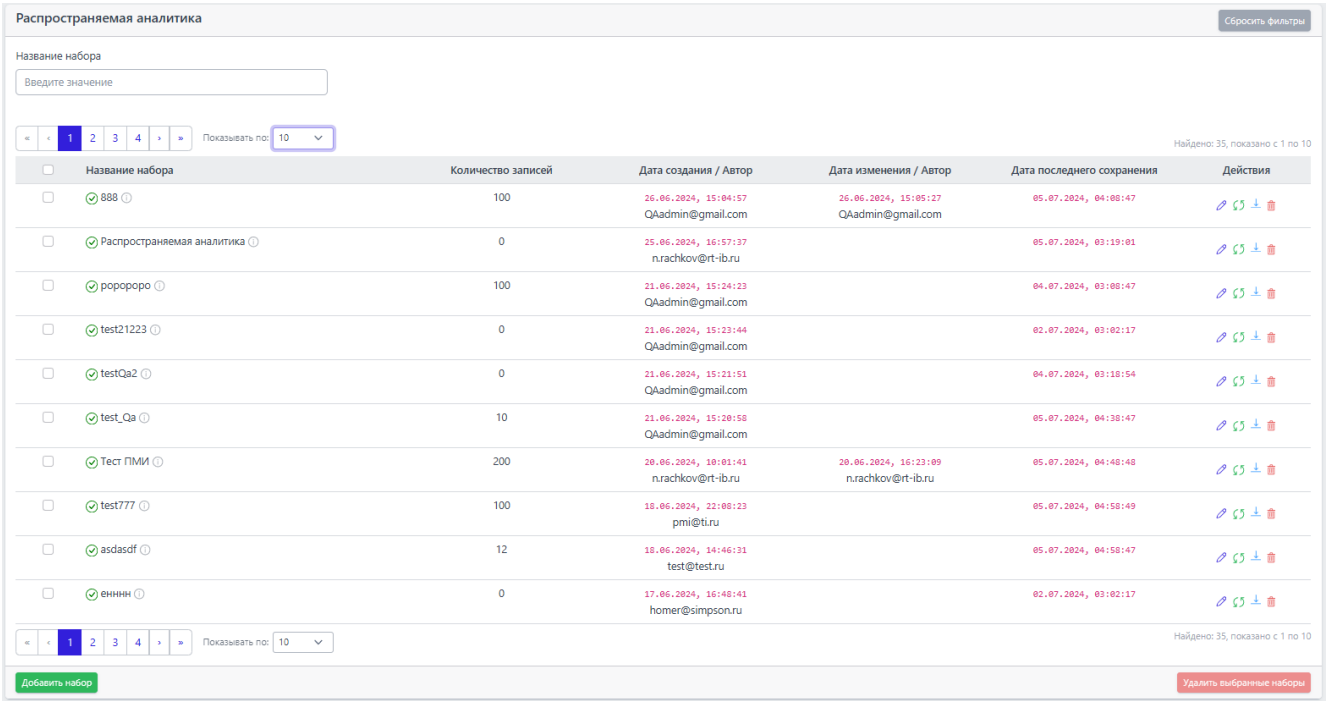



**Рисунок 109 – Страница раздела «Распространяемая аналитика»**

Страница представлена в виде таблицы с наборами аналитических данных.

В таблице имеются следующие поля:

– название набора;

– количество записей;

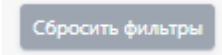
– дата создания/автор;

– дата последнего изменения/автор;

– дата последнего сохранения;

– действия.

Для фильтрации информации в таблице имеется фильтр **Название набора**.

В верхней часть страницы имеется иконка 

, для отмены примененных для фильтрации настроек.

Для навигации на странице имеется стандартный элемент пагинатор.

Действия возможные над наборами:

–  (редактирование набора);

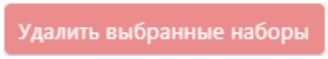
–  (принудительная синхронизация);

–  (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 **Ошибка! Источник ссылки не найден.**.

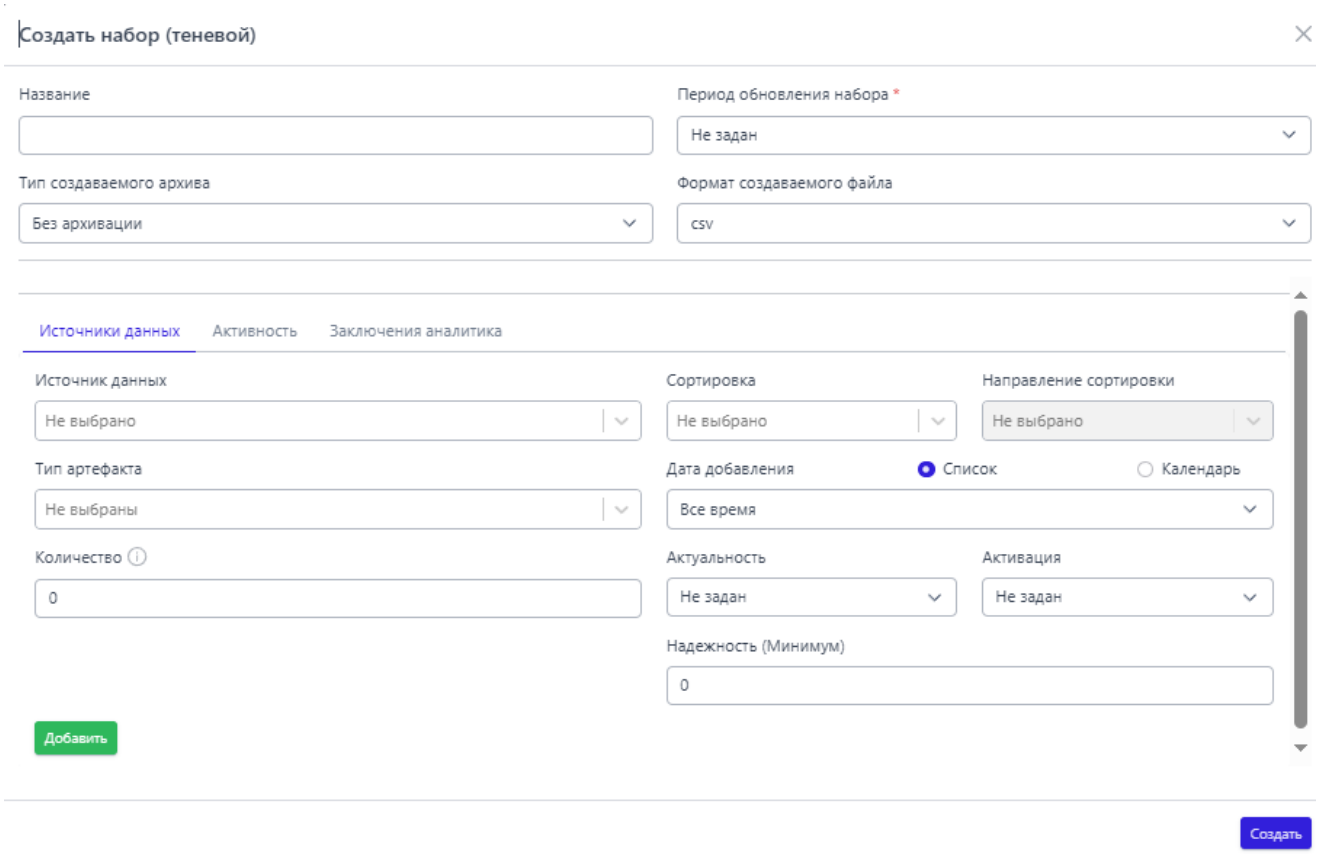



**Рисунок 110 – Окно создания набора**

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

– Название набора;

– Период обновления набора;

– Тип создаваемого архива;

– Формат создаваемого файла.

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 111.

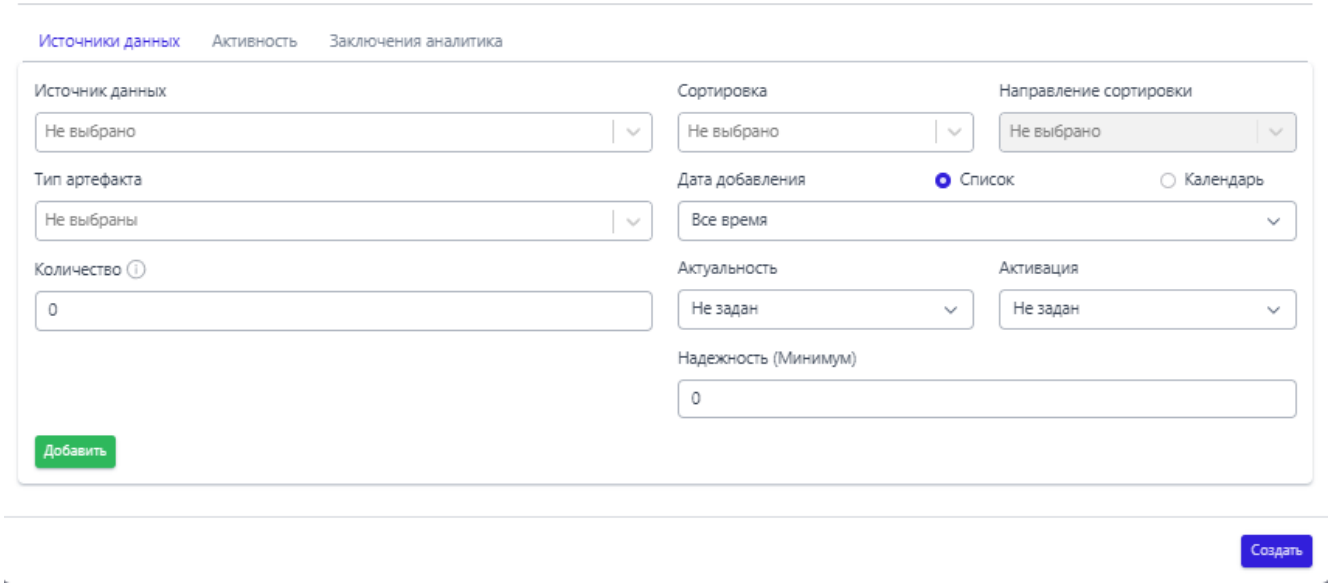



**Рисунок 111 – Настройка полей выбранной вкладки «Источники данных»**

По данной вкладке можно настроить следующие параметры:

– Количество (количество получаемых элементов для каждого выбранного типа артефакта);

– 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);

– Надежность (задается минимальное значение надежности для артефактов по источнику).

После выставления настроек требуется нажать по иконке Добавить, после чего появится поле с зафиксированными настройками конфигурации источника данных ( рисунок 112 ).

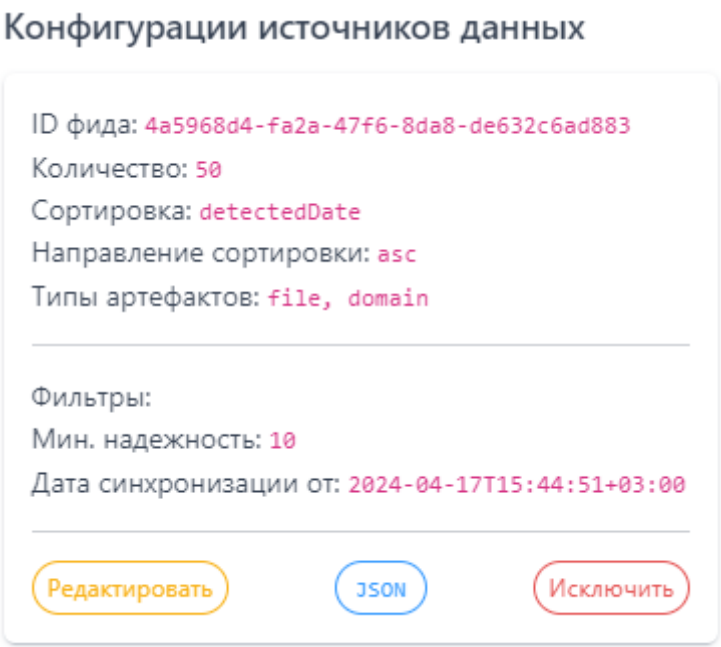



**Рисунок 112 – Настройки конфигурации источника данных**

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

При нажатии по иконке Редактировать имеется возможность редактирования настроенной конфигурации.

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

При нажатии по иконке Исключить происходит удаление настроек параметров в конфигурации.

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

Поля настройки по выбранной вкладке **Активность** представлены на рисунке 113.

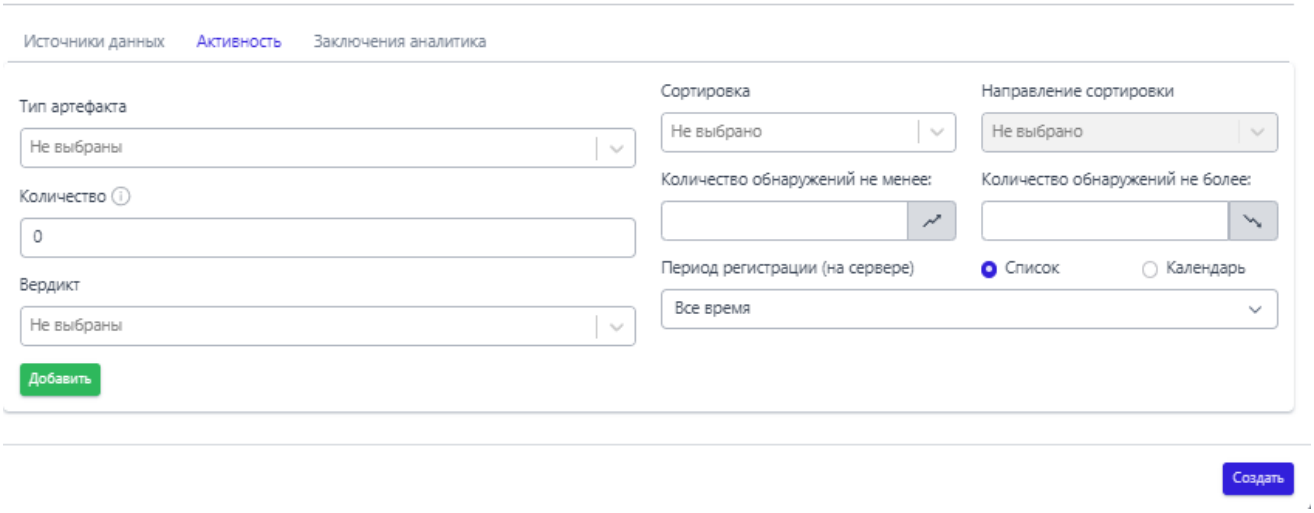



**Рисунок 113 – Настройка полей выбранной вкладки «Активность»**

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 менее;

– Период регистрации (на сервере) (начальная и конечная даты).

Поля настройки по выбранной вкладке **Заключения аналитика** представлены на рисунке 114.

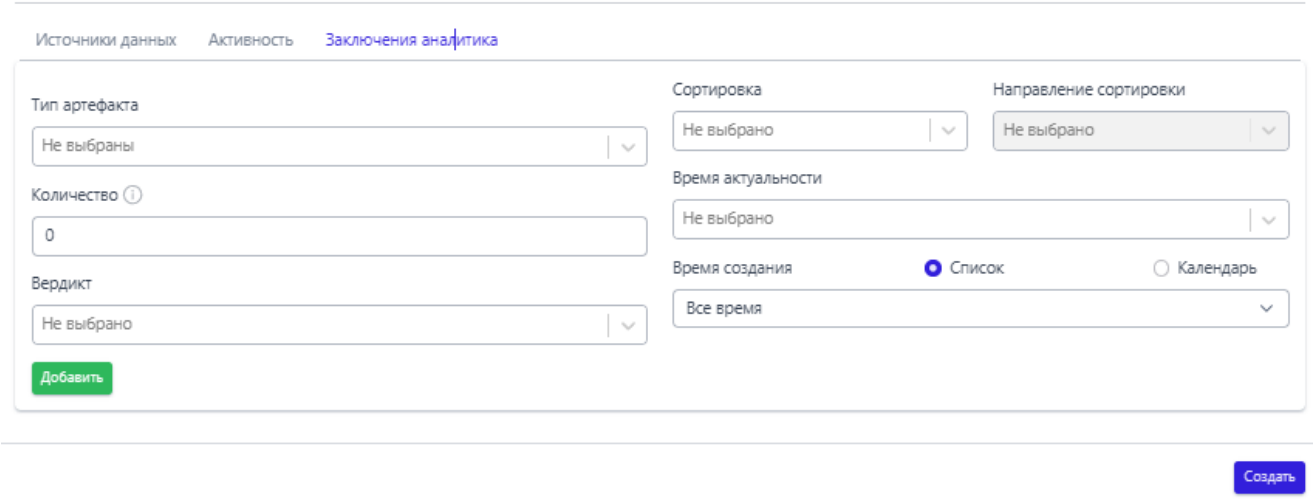



**Рисунок 114 – Настройка полей выбранной вкладки «Заключение аналитика»**

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

– Количество (количество записей артефактов по выбранному набору, отображающихся на странице Заключение эксперта);

– 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).

### 6.5.7. Алгоритм вынесения вердикта в TI

При вынесении вердикта TI действует пошагово. Если на текущем шаге имеется информация для вынесения вердикта, то вердикт выносится и следующие шаги не выполняются.

Алгоритм для типа артефакта - Файлы

1) Проверяется наличие заключения аналитика. Если оно имеется и актуально, то вердикт выносится по вердикту заключения.

2) Проверяется наличие индикатора компрометации. Если он есть, и у него установлен признак активности в true, то выносится вердикт «Вредоносный».

3) Проверяется наличие артефакта в источниках данных. Анализируются только актуальные записи (в которых время жизни артефакта больше, чем время с последней синхронизации). Из всех источников выбирается источник с самым большим приоритетом. Если таких источников несколько, приоритет отдается безопасному источнику. Выносится тот вердикт, который указан в настройках выбранного источника данных.

4) Проверяется наличие для файла отчета по собственному YARA-движку. Если в отчете имеется хотя бы одно сработавшее правило, то выносится вердикт «Вредоносный».

5) Проверяется наличие у файла отчетов в очереди по следующим анализаторам: Virus Total, PT Sandbox, Kaspersky TI. Если хотя бы один из отчетов находится в очереди, то выносится вердикт «В процессе анализа».

6) Проверяется наличие для файла отчета PT Sandbox (PT Multiscanner). Вердикт выносится на основании поля verdict отчета.

7) Проверяется наличие для файла отчета Virus Total. Вердикт выносится на основании вердиктов доверенных вендоров в отчете Virus Total. Если хотя бы

два доверенных вендора признали артефакт вредоносным, то выносится вердикт «Вредоносный», иначе вердикт «Безопасный».

Список доверенных вендоров («TrustedFileVendors»):

– CrowdStrike;

– FireEye;

– McAfee;

– TrendMicro;

– Kaspersky;

– Microsoft;

– Sophos;

– Symantec;

– BitDefender;

– Malwarebytes;

– SentinelOne;

– Paloalto.

8) Проверяется наличие для файла отчета Kaspersky TI. Вердикт выносится на основании поля zone отчета.

9) Если ни на одном предыдущем шаге не удалось вынести вердикт, то вердикт определяется как «Неизвестный».

Нужно отметить, что на текущий момент на вердикт не влияют отчеты остальных анализаторов: Athena, RST Cloud.

Алгоритм для типа артефакта - IP-адреса

1) Проверяется наличие заключения аналитика. Если оно имеется и актуально, то вердикт выносится по вердикту заключения.

2) Проверяется, что IP находится в приватном диапазоне. Если это так, то выносится вердикт «Безопасный».

3) Проверяется наличие индикатора компрометации. Если он есть и у него установлен признак активности в true, то выносится вердикт «Вредоносный».

4) Проверяется наличие артефакта в источниках данных. Подробнее см пункт 3 в разделе «Файлы».

5) Проверяется наличие у файла отчетов в очереди по следующим анализаторам: Virus Total, Kaspersky TI. Если хотя бы один из отчетов находится в очереди, то выносится вердикт «В процессе анализа».

6) Проверяется наличие для файла отчета Virus Total. Если хотя бы два любых вендора признали артефакт вредоносным, то выносится вердикт «Вредоносный», иначе вердикт определяется как «Безопасный».

7) Проверяется наличие для файла отчета Kaspersky TI. Вердикт выносится на основании поля zone отчета.

8) Если ни на одном предыдущем шаге не удалось определить вердикт, то выносится вердикт «Неизвестный».

Алгоритм для типа артефакта - Доменные имена

1) Проверяется наличие заключения аналитика. Если оно имеется и актуально, то вердикт выносится по вердикту заключения.

2) Проверяется наличие индикатора компрометации. Если он есть и у него установлен признак активности в true, то выносится вердикт «Вредоносный».

3) Проверяется наличие артефакта в источниках данных. Подробнее см. пункт 3 в разделе «Файлы».

4) Проверяется наличие у файла отчетов в очереди по следующим анализаторам: Virus Total, Kaspersky TI. Если хотя бы один из отчетов находится в очереди, то выносится вердикт «В процессе анализа».

5) Проверяется наличие для файла отчета Virus Total. Если хотя бы два любых вендора признали артефакт вредоносным, то выносится вердикт «Вредоносный», иначе вердикт определяется как «Безопасный».

6) Проверяется наличие для файла отчета Kaspersky TI. Вердикт выносится на основании поля zone отчета.

7) Если ни на одном предыдущем шаге не удалось определить вердикт, то выносится вердикт «Неизвестный».

Алгоритм для типа артефакта - URL

1) Проверяется наличие заключения аналитика. Если оно имеется и актуально, то вердикт выносится по вердикту заключения.

2) Проверяется наличие индикатора компрометации. Если он есть и у него установлен признак активности в true, то выносится вердикт «Вредоносный».

3) Проверяется наличие артефакта в источниках данных. Подробнее см пункт 3 в разделе «Файлы».

4) Проверяется наличие у файла отчетов в очереди по следующим анализаторам: Virus Total, Kaspersky TI. Если хотя бы один из отчетов находится в очереди, то выносится вердикт «В процессе анализа».

5) Проверяется наличие для файла отчета Virus Total. Если хотя бы два любых вендора признали артефакт вредоносным, то выносится вердикт «Вредоносный», иначе присваивается вердикт «Безопасный».

6) Проверяется наличие для файла отчета Kaspersky TI. Вердикт выносится на основании поля zone отчета.

7) Если ни на одном предыдущем шаге не удалось вынести вердикт, то присваивается вердикт «Неизвестный».

### 6.5.8. Теневые наборы

В разделах **Распространяемая аналитика**, **Индикаторы компрометации**, **Исключения для файлов** и **Сетевые исключения** присутствуют наборы с артефактами, которые обозначаются как «теневые». Теневые наборы являются основой распространяемой TI-аналитики, но для работы с EDR выделены

отдельные теневые наборы, формат данных которых совпадает с форматом данных EDR.

Теневые наборы – это наборы артефактов, автоматически переопределяемые на основе указанных аналитиком или администратором параметров. Эти параметры задаются администратором или аналитиком при формировании теневого набора.

Теневые наборы формируются на основе трех конфигураций с параметрами:

1) Источники данных (конфигурация набора на основе одного или несколько источников из таблицы артефактов **Источники данных** со своими определенными настройками, в соответствии с которыми артефакты будут отбираться в набор);

2) Активность (конфигурация набора на основе артефактов таблицы **Активность** со своими определенными настройками, в соответствии с которыми артефакты будут отбираться в набор);

3) Заключение аналитика (конфигурация набора на основе артефактов таблицы **Заключение аналитика** со своими определенными настройками, в соответствии с которыми артефакты будут отбираться в набор).

В результате конфигурирования появляется набор, который позволяет в автоматическом режиме отслеживать изменения в таблицах артефактов в соответствии с выбранными параметрами и применять эти изменения для аналитики, распространяемой на EDR, или общей распространяемой аналитики для любых клиентов TI-платформы.

В качестве примера можно рассмотреть такой «теневой набор» (см. рисунок 115).

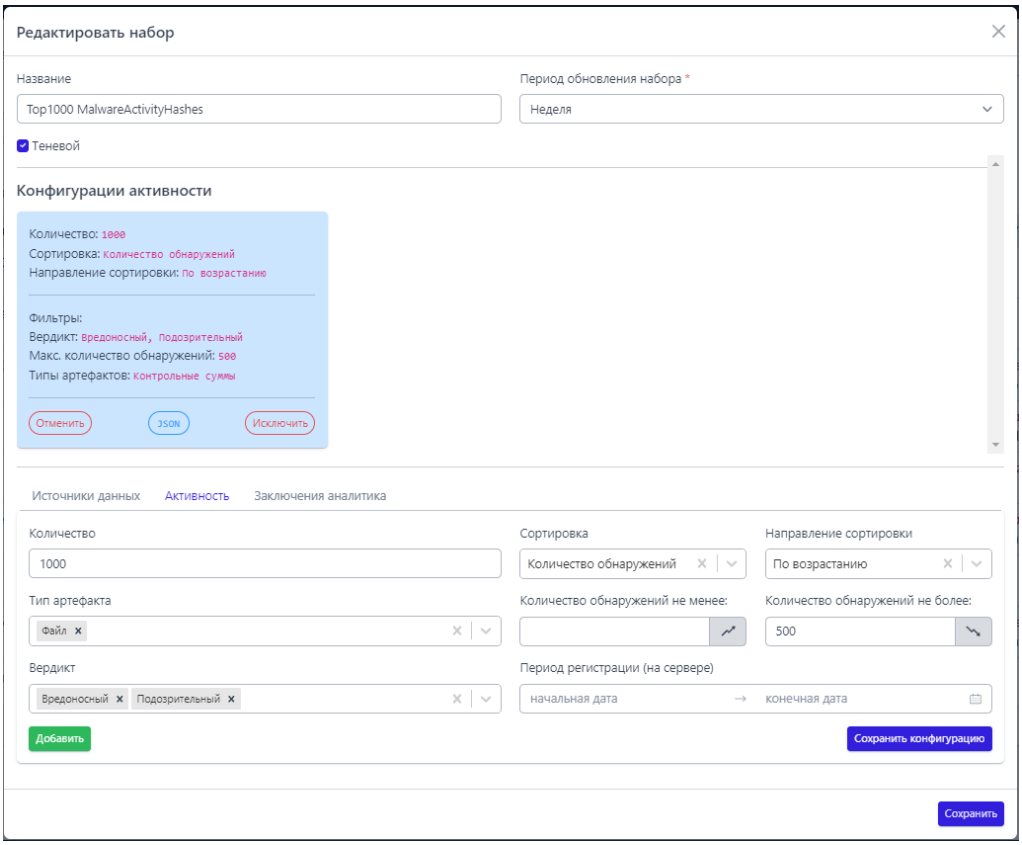



**Рисунок 115 – Пример теневого набора**

Здесь можно увидеть, что в качестве вредоносных и подозрительных артефактов типа «Файл» в набор будут попадать 1000 файловых артефактов таблицы «Активность», встречавшиеся менее 500 раз за последнюю неделю в этой таблице. Файлы будут сортироваться по количеству обнаружений от малого числа к большему.

При обнаружении артефакта из списка такого теневого набора на клиенте (EDR, SIEM и т.д.) будет предпринято запрограммированное на клиенте же действие, соответствующее вердикту.

В теневых наборах можно смешивать конфигурации в любых сочетаниях. Подробнее о конфигурациях и параметрах настройки см. пункт 6.5.6.

### *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.

---

**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 Windows**, 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 выполниться 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. 116) включает в себя следующие структурные элементы:

– Фильтры **Название набора** и **Показывать по**;

– таблица с наборами индикаторов атак;

– кнопка **Добавить набор**;

– кнопка **Удалить выбранные наборы**;

– кнопка **Сбросить фильтры.**

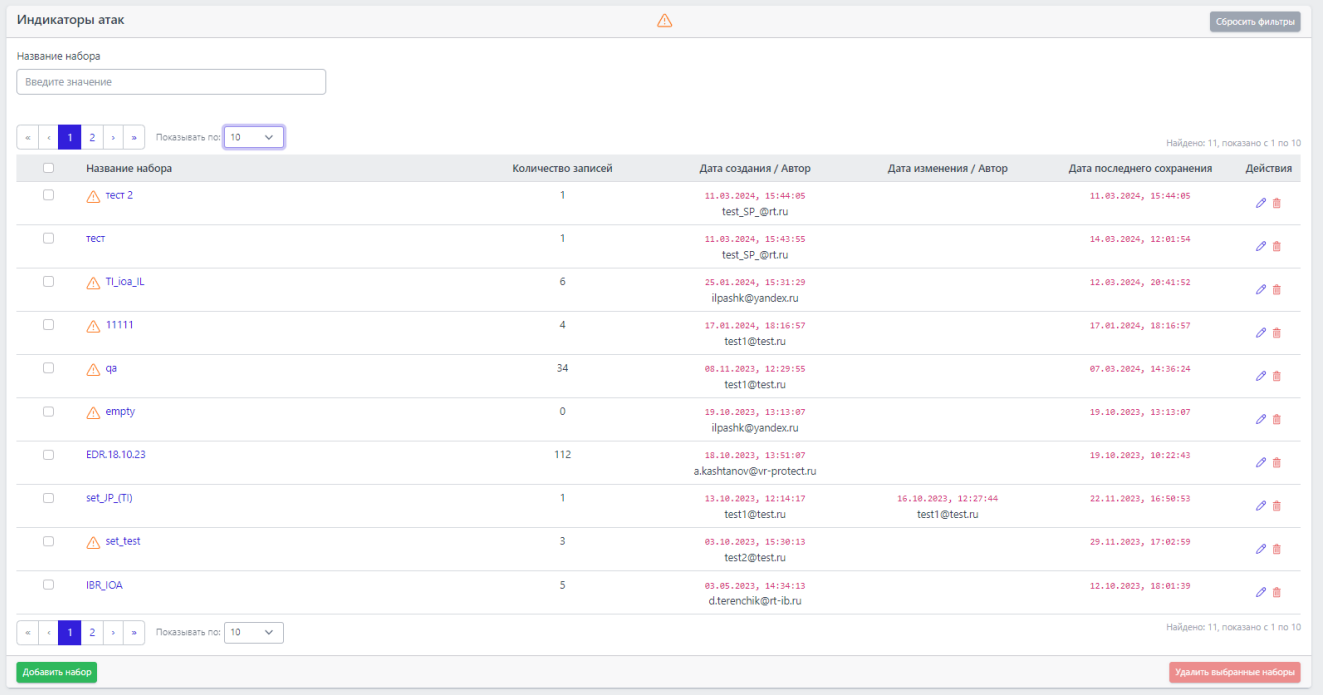



**Рисунок 116 – Наборы индикаторов атак**

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**).

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**.

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. 117).

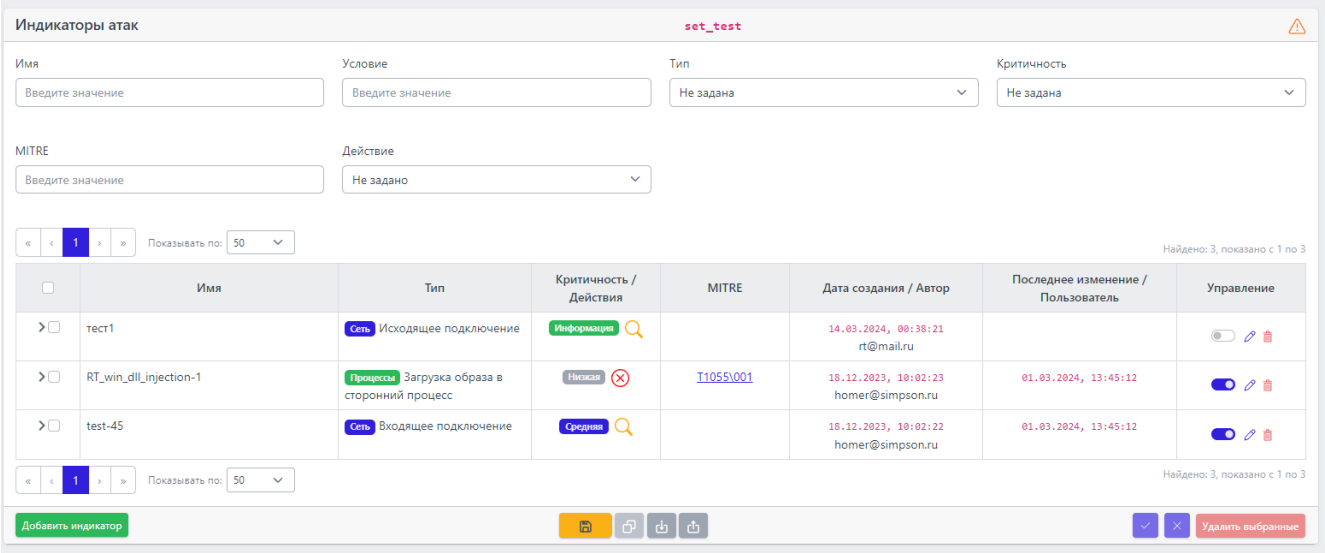



**Рисунок 117 – Индикаторы атак**

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 добавления нового индикатора атаки необходимо нажать кнопку **Добавить индикатор** в нижней части страницы. В открывшемся окне **Добавить индикатор** (рис. 118) следует прописать условия, на основании которых будет срабатывать правило.

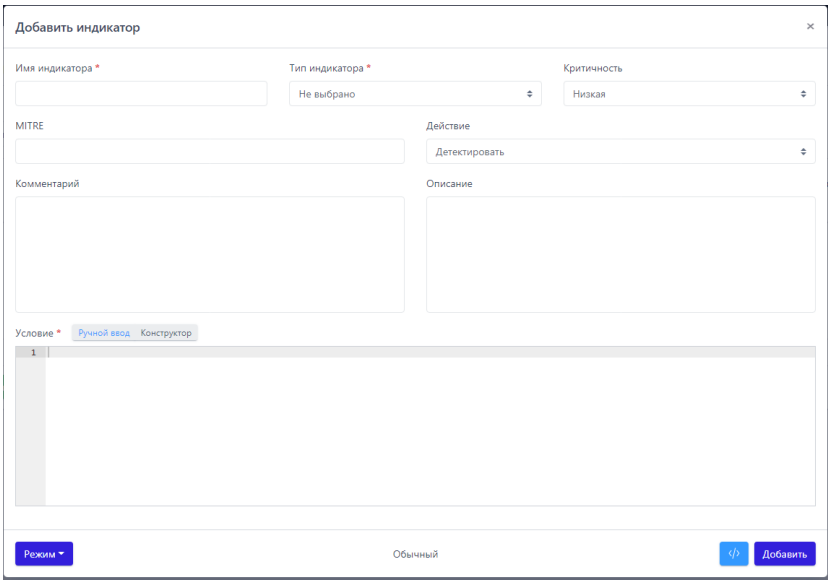



**Рисунок 118 – Добавление индикатора**

После написания условия необходимо нажать кнопку Добавить. В нижней части страницы появится сообщение о добавлении нового правила (рис. 119).

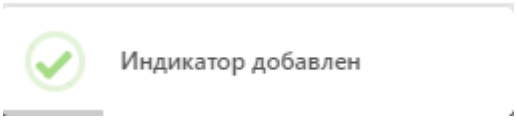



**Рисунок 119 – Сообщение о добавлении индикатора атаки**

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.120).

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

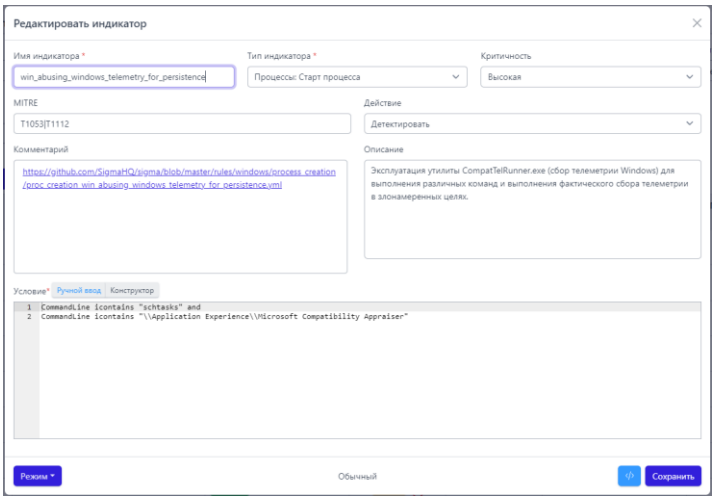



**Рисунок 120 – Редактирование индикатора атаки**

Для сохранения внесенных изменений необходимо нажать кнопку **Сохранить**, после чего в нижней части страницы появится сообщение об изменении правила (рис. 121).


**Рисунок 121 – 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.

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

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».

Страница **Индикаторы компрометации** представлена на рисунке 122. На странице отображаются наборы с индикаторами компрометации, сохраненные на сервере аналитики.

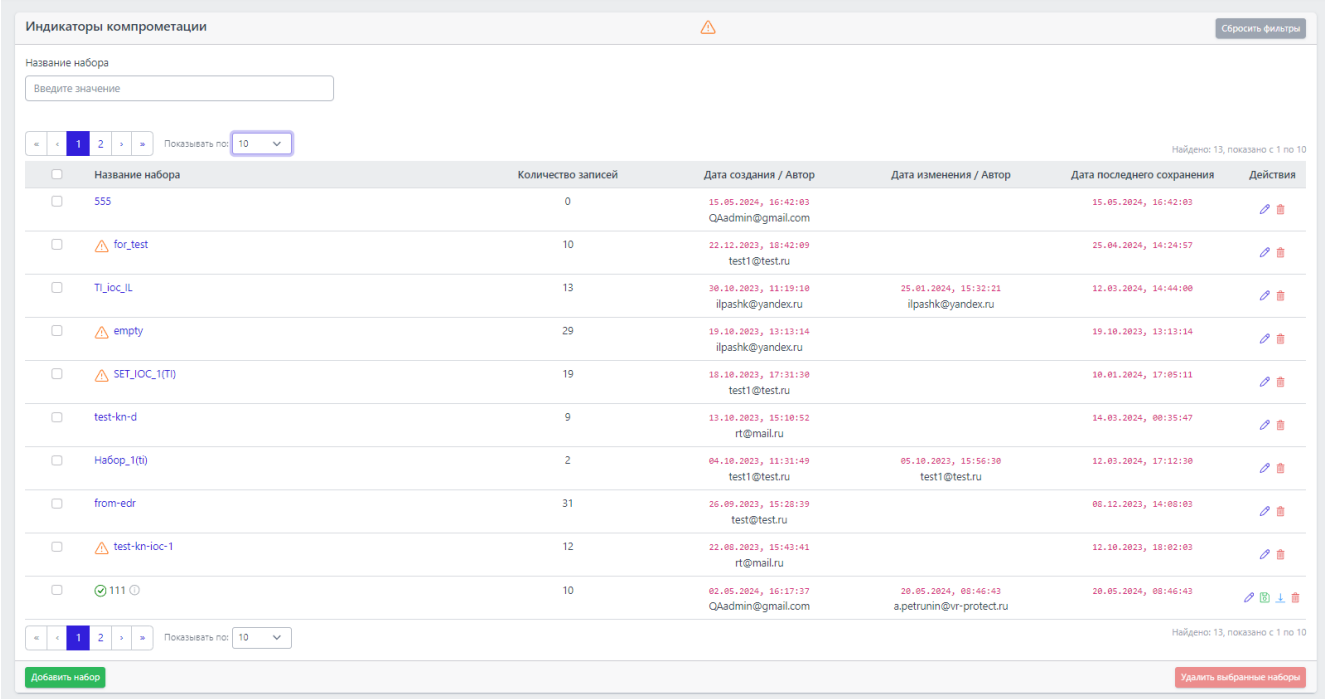



**Рисунок 122 – Наборы индикаторов компрометации**

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.

В таблице с наборами индикаторов компрометации кроме обычных наборов можно создать «теневой набор», указав при создании набора параметр **теневой**. Общая информация о теневых наборах рассмотрена в разделе 6.5.8. Описание настроек при создании теневого набора подробно рассмотрено в разделе 6.5.6.

Имя теневого набора индикаторов компрометации в таблице наборов отмечено другим цветом шрифта, а также имеется признак синхронизации с источником данных. Вид записи теневого набора представлен на рисунке 123.

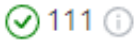



**Рисунок 123 – Пример набора индикаторов компрометации в виде теневого набора**

Для добавления нового набора индикаторов компрометации необходимо нажать кнопку **Добавить набор**, после чего в открывшемся окне **Создать набор** (рис. 124) в строке **Название** ввести название нового набора и выбрать если необходимо параметр будет ли набор являться теневым.


**Рисунок 124 – Окно «Создать набор»**

Для завершения операции добавления необходимо нажать кнопку **Создать,** после чего в нижней части страницы появится сообщение о добавлении набора (рис. 125), а строка с новым набором появится в таблице.


**Рисунок 125 – 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**.

Страница «Индикаторы компрометации»

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.

В верхней части области **Индикаторы компрометации** отображается имя набора и фильтр **Показывать по** (возможно задавать значения **10**, **20**, **50** и **100**), **Имя индикатора**, **Артефакт** (фильтрует по значению артефакта), **Тип** (фильтрует по типу артефакта).

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. 126) следует заполнить поля, обязательными для заполнения из которых являются поля **Имя индикатора**, **Тип индикатора** и **Артефакт**, после чего нажать кнопку Добавить.

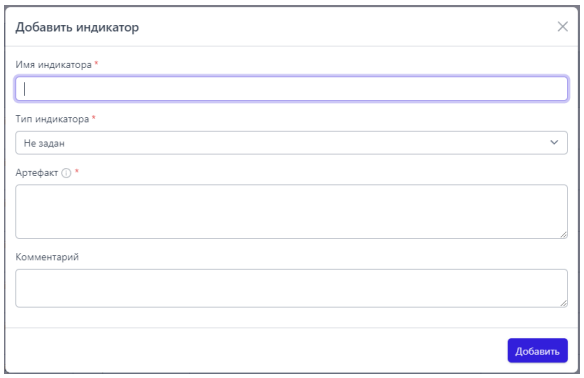



**Рисунок 126 – Окно «Добавить индикатор»**

В нижней части страницы появится сообщение о добавлении индикатора компрометации (рис. 127).

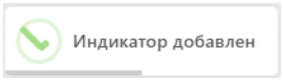



**Рисунок 127 – Сообщение о добавлении индикатора**

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 Windows

#### Общая информация

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

#### Наборы с журналами Windows

Страница с наборами журналов (рис. 128) открывается при выборе на панели слева раздела **Журналы Windows** и включает в себя следующие структурные элементы:

– кнопка **Сбросить фильтры;**

– фильтры **Название набора** и **Показывать по;**

– таблица с наборами журналов Windows;

– кнопка **Добавить набор;**

– кнопка **Обновить файл экспорта;**

– кнопка **Удалить выбранные наборы.**

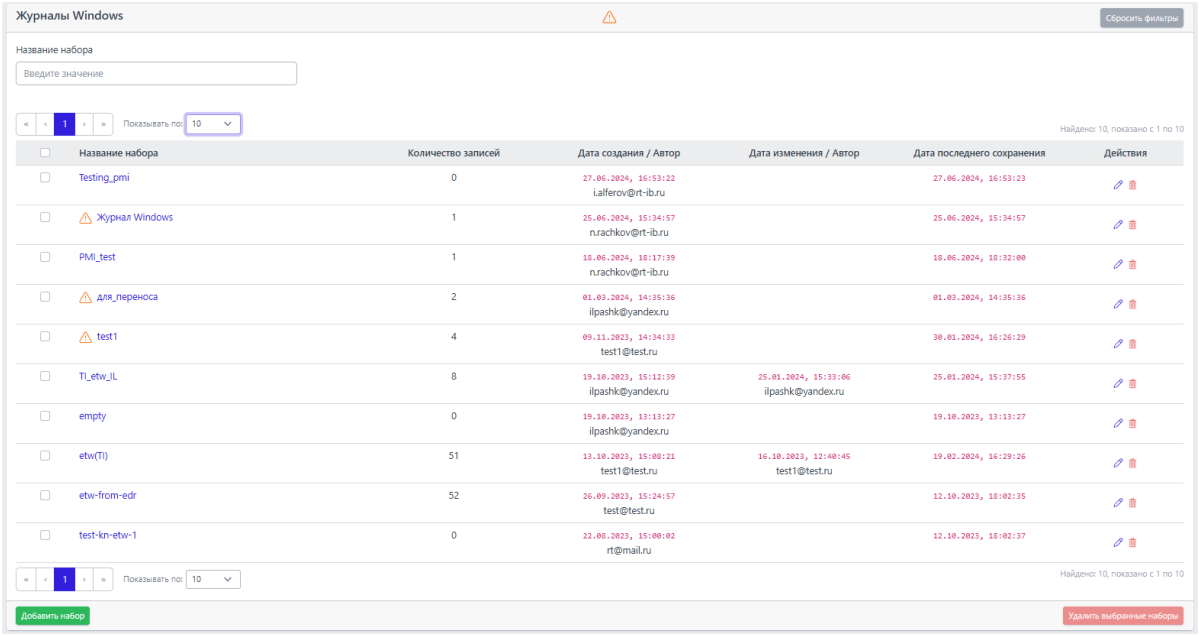



**Рисунок 128 – Наборы с журналами Windows**

Наборы можно искать по названию с помощью фильтра **Название набора**.

Для добавления нового набора необходимо нажать кнопку **Добавить набор**, после чего в окне **Создать набор** ввести название нового набора журналов. 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 Windows** для выбранного набора (рис. 129).

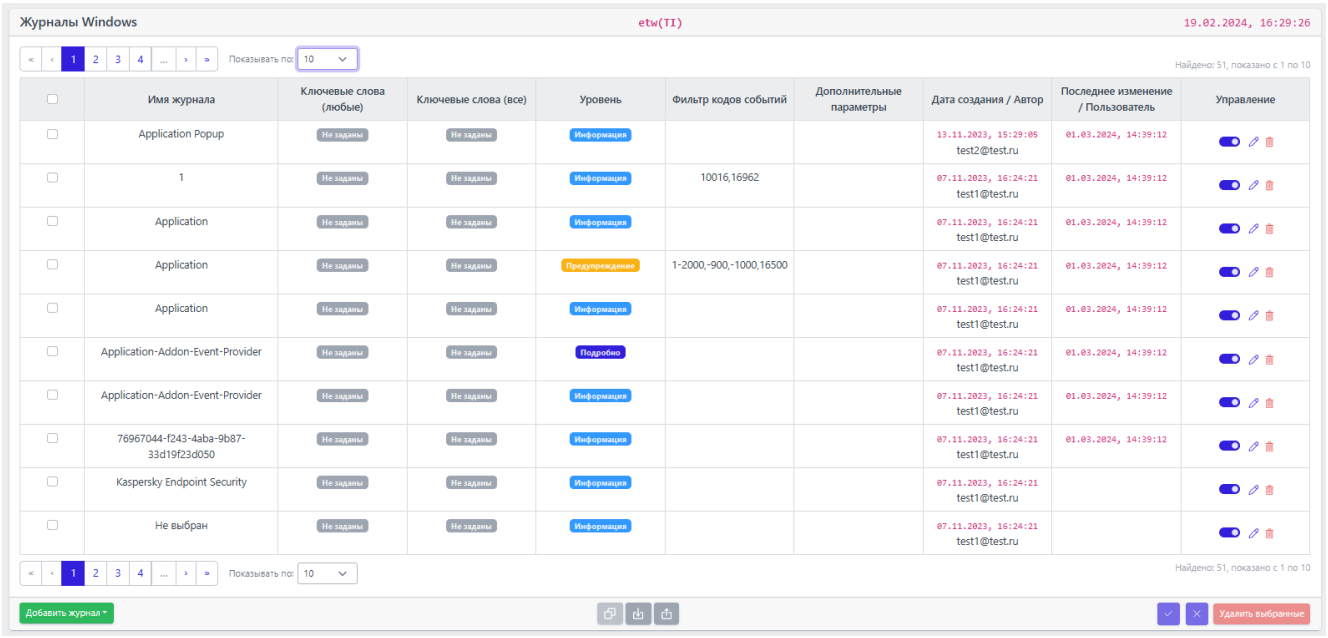



**Рисунок 129 – Страница «Журналы Windows»**

Страница «Журналы Windows»

На странице **Журналы Windows** 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 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. 130) 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.

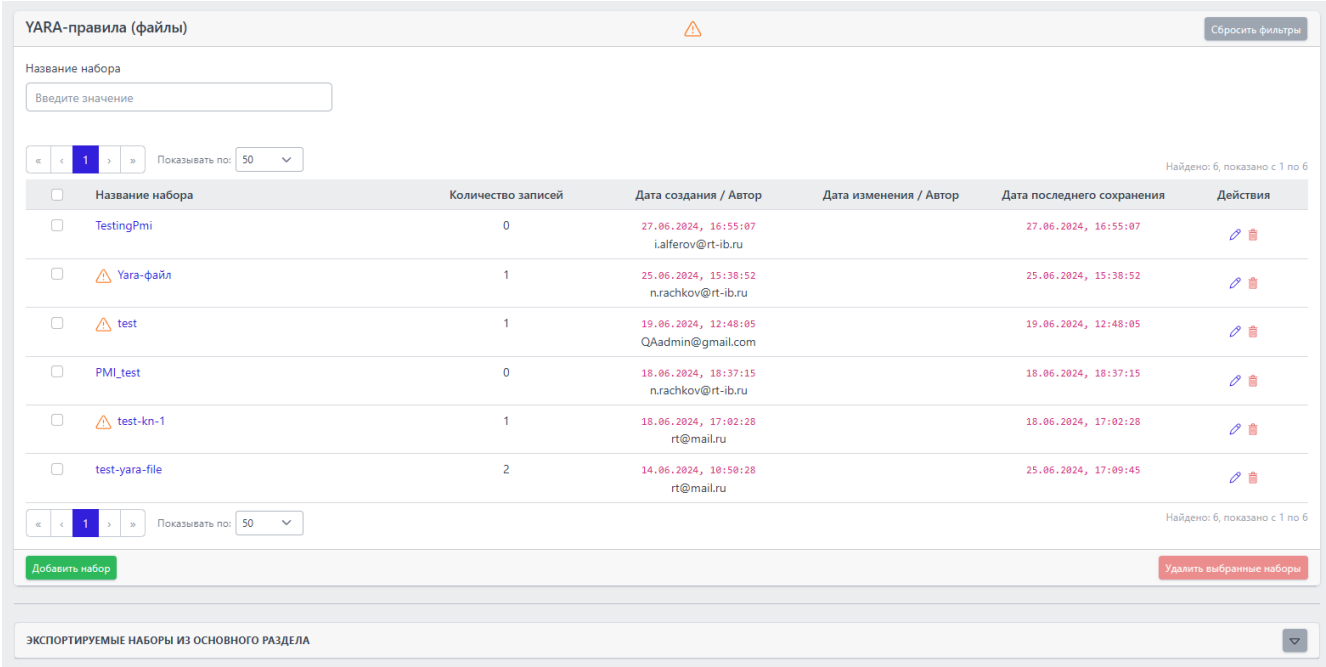



**Рисунок 130 – Наборы YARA-правил (файлы)**

Для добавления нового набора необходимо нажать кнопку **Добавить набор,** после чего в окне **Добавить набор** ввести название нового набора YARA-правил. 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. 131).

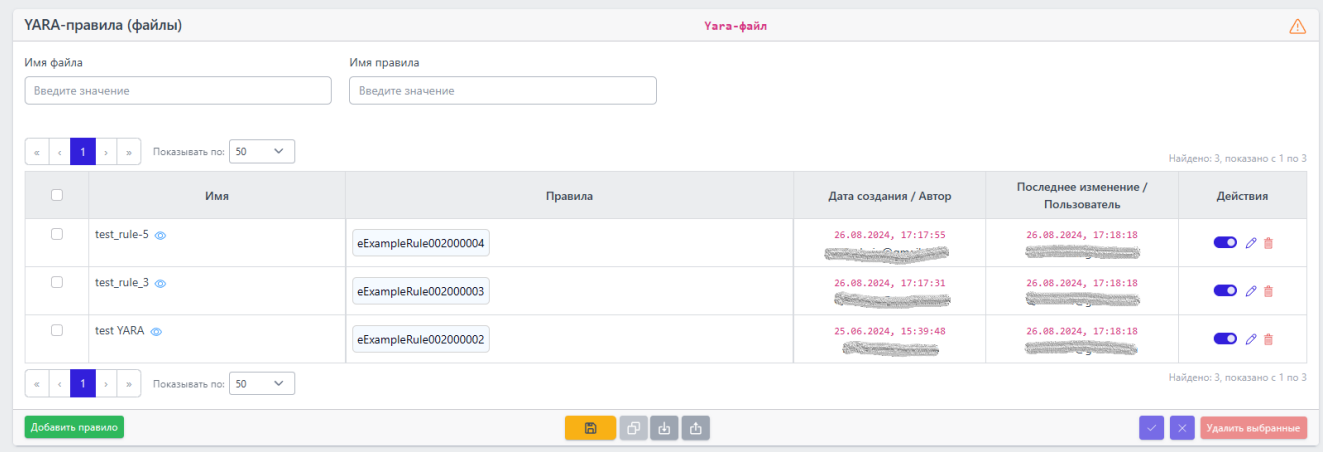



**Рисунок 131 – YARA-правила (файлы)**

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

– просматривать правила из выбранного набора;

– добавлять новые правила в выбранный набор;

– применять наборы после изменения правил;

– копировать/перемещать выбранные правила в другой набор;

– экспортировать выбранный набор в файл;

– импортировать данные из файла в выбранный набор правил;

– активировать или деактивировать правило;

– редактировать выбранное правило;

– удалить выбранное правило из набора.

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

Подробная информация о синтаксисе YARA содержится в документе «Руководство аналитика RT Protect EDR» и официальной документации YARA. Пример правила YARA приведен на рисунке 132.

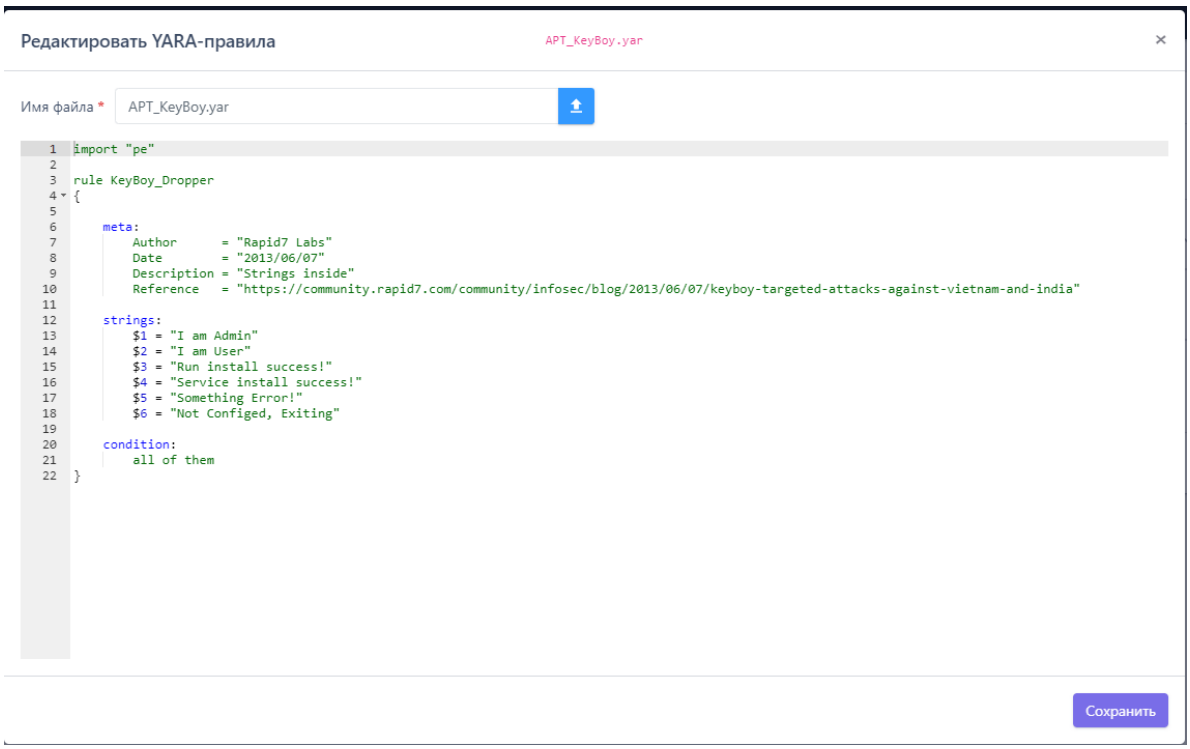



**Рисунок 132 – Пример правила YARA**

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). 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 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 .yar с помощью кнопки **Импортировать** yara-файл (  ).

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

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

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

Для экспорта набора в файл следует нажать кнопку **Экспортировать набор в файл 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 Yara-правилами, предусмотрены следующие фильтры:

– Имя файла;

– Имя правила.

### *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. 133) 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.

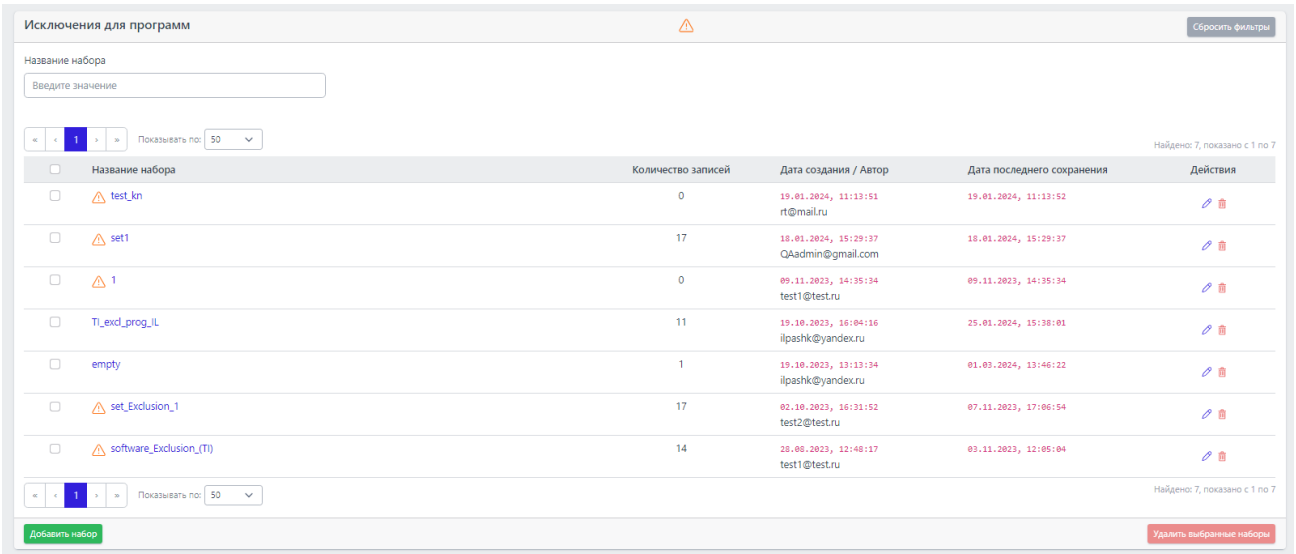



**Рисунок 133 – Наборы исключений для программ**

Наборы исключений для программ

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

– кнопка **Сбросить фильтры;**

– фильтры **Название набора** и **Показывать по**;

– таблица с наборами исключений для программ;

– кнопка **Добавить набор**;

– кнопка **Удалить выбранные наборы**.

Чтобы добавить новый набор с исключениями для программ, необходимо нажать кнопку **Добавить набор**, после чего ввести название нового 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. 134) 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.

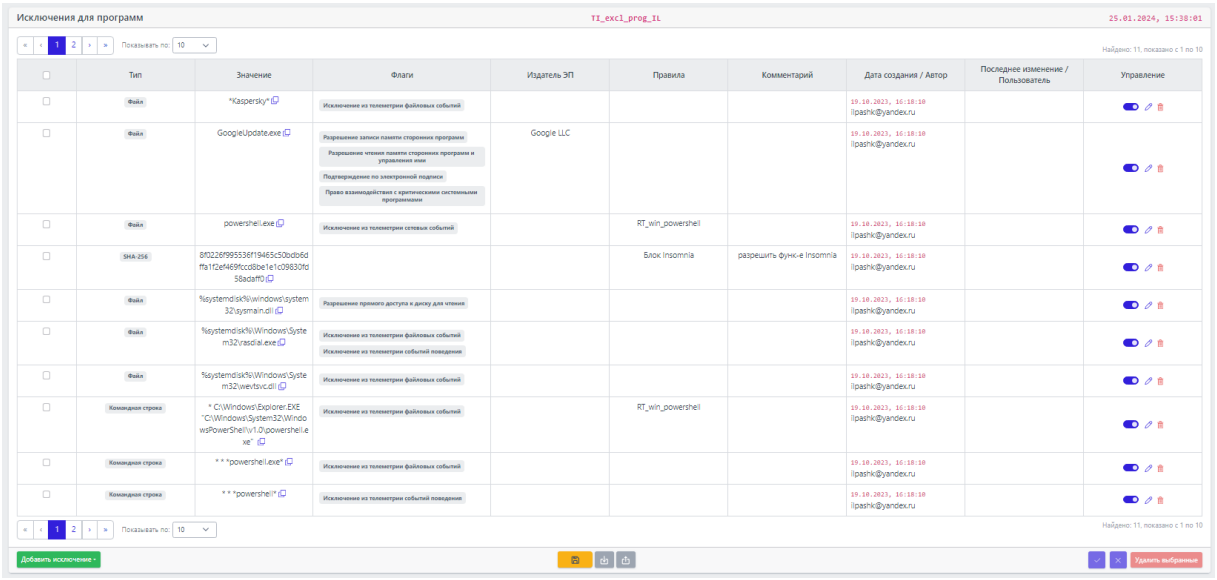



**Рисунок 134 – Исключения для программ**

Для добавления в набор нового исключения для программы необходимо нажать кнопку **Добавить исключение** и в открывшемся списке выбрать тип добавляемого исключения: **Файл, Хеш** или **Командная строка** (рис. 135).

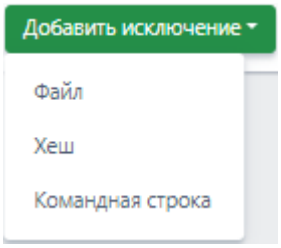



**Рисунок 135 – Добавить исключение для программ (выбор типа)**

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. 136).

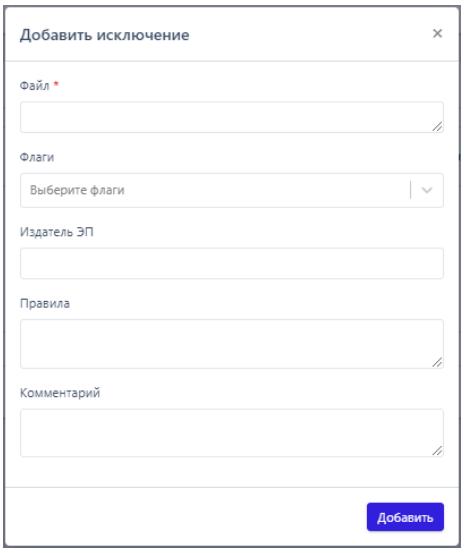



**Рисунок 136 – Добавление исключения для программы (тип «Файл»)**

Для типа исключений **Хеш** следует определить следующие параметры: **Тип хеш-суммы, Хеш-сумма, Флаги, Издатель ЭП, Правила, Комментарий** (рис. 137).

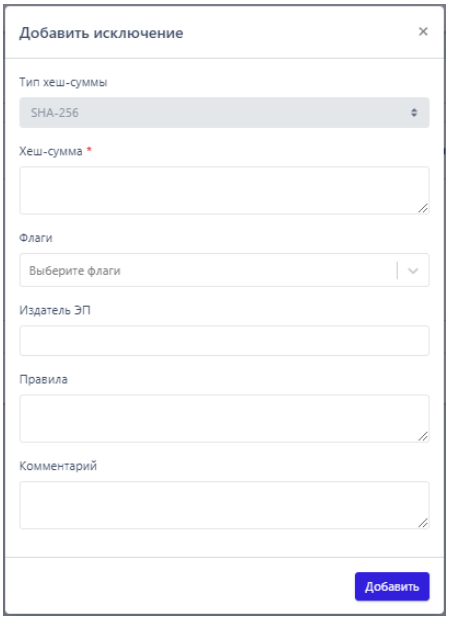



**Рисунок 137 – Добавление исключения для программы (тип «Хеш»)**

Для типа исключений **Командная строка** необходимо определить следующие параметры: **Командная строка прародителя, Командная строка родителя, Командная строка процесса, Флаги, Издатель ЭП, Правила, Комментарий** (рис. 138).

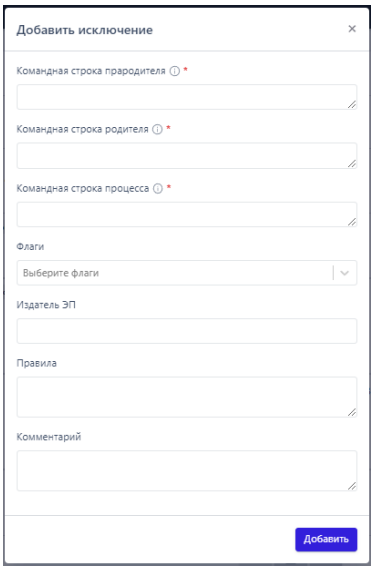



**Рисунок 138 – Добавление исключения для программы (тип «Командная строка»)**

**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 Сохранить 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. 139) содержится список файлов, исполнение которых должно быть разрешено или блокировано (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.

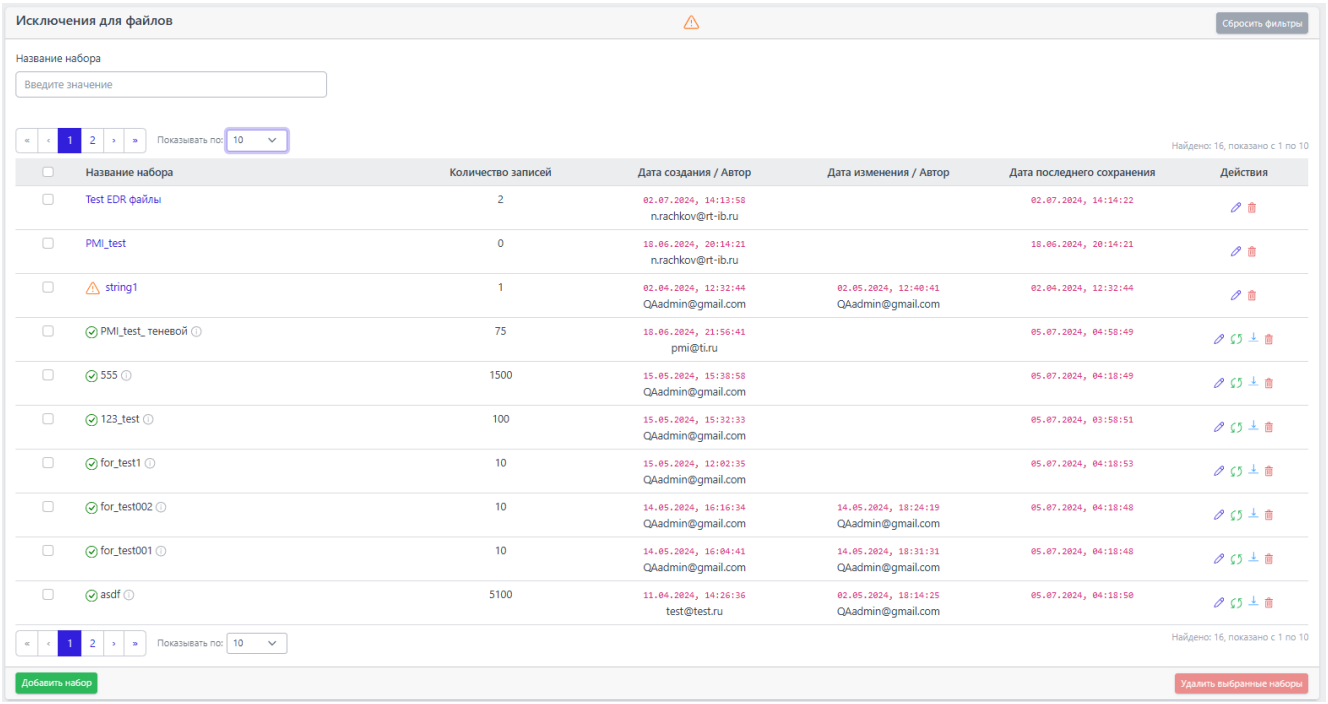



**Рисунок 139 – Наборы исключений для файлов**

Наборы исключений для файлов

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

– кнопка **Сбросить фильтры;**

– фильтры **Название набора** и **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.

При установке галочки «Теневой» будет создан набор с исключениями в концепции теневого набора. Подробнее с концепцией теневых наборов можно ознакомиться в п. 6.5.8. Для завершения операции необходимо нажать кнопку **Добавить.**

В таблице с наборами, теневые наборы в столбце названия набора имеют вид  , где  -указатель на то, что набор синхронизирован с источником данных, на основании которого создан набор,  - название набора,  - указатель, что набор обновляется автоматически.

В столбце **Действия** для теневых наборов, в отличие от обычных наборов, имеется иконка для синхронизации наборов  и для скачивания наборов  .

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. 140) 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.

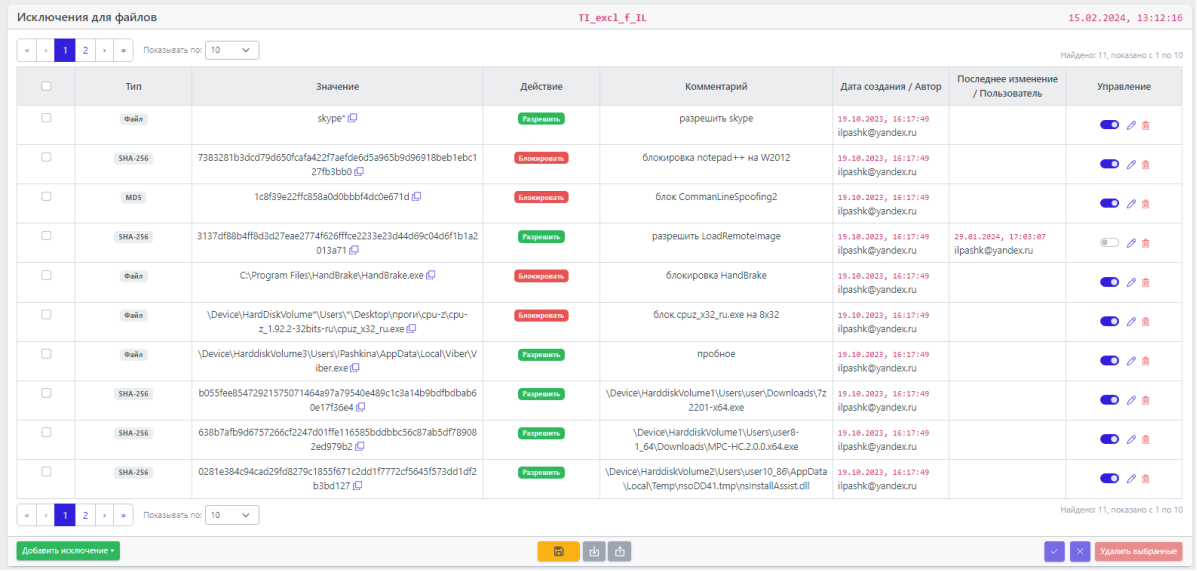



**Рисунок 140 – Исключения для файлов**

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. 141).

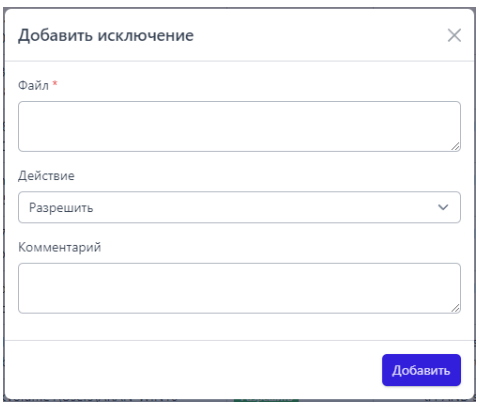



**Рисунок 141 – Добавление исключения для файла (тип «Файл»)**

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. 142).

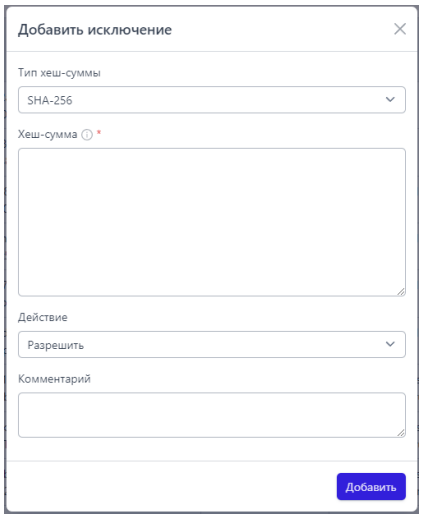



**Рисунок 142 – Добавление исключения для файла (тип «Хеш»)**

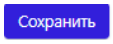
**Файл** – в поле прописываются имена исполняемых файлов, которые необходимо добавить в исключения. Имена файлов после добавления исключения будут отображаться в таблице **Исключения для файлов** в поле **Значение**, а в поле **Тип** будет указан тип исключения.

**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 

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. 143):

– таблица с наборами сетевых исключений;

– кнопка **Добавить набор**;

– кнопка **Удалить выбранные наборы**.

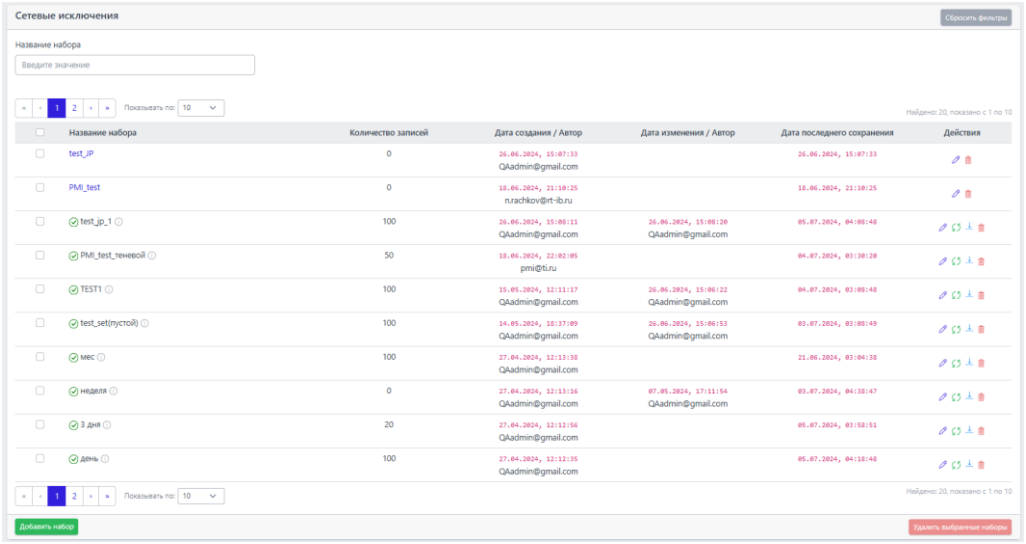



**Рисунок 143 – Страница наборов сетевых исключений**

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

При необходимости можно создать теневой набор, указав галочку после названия набора. Подробнее с концепцией теневых наборов можно ознакомиться в п. 6.5.8 данного руководства.

В таблице с наборами теневые наборы в столбце названия набора имеют вид test_jp_1, где -указатель на то, что набор синхронизирован с источником данных, на основании которого создан набор, test_jp_1 - название набора, - указатель, что набор обновляется автоматически.

В столбце **Действия** для теневых наборов, в отличие от обычных наборов, имеется иконка для синхронизации наборов и для скачивания наборов .

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. 144) 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.

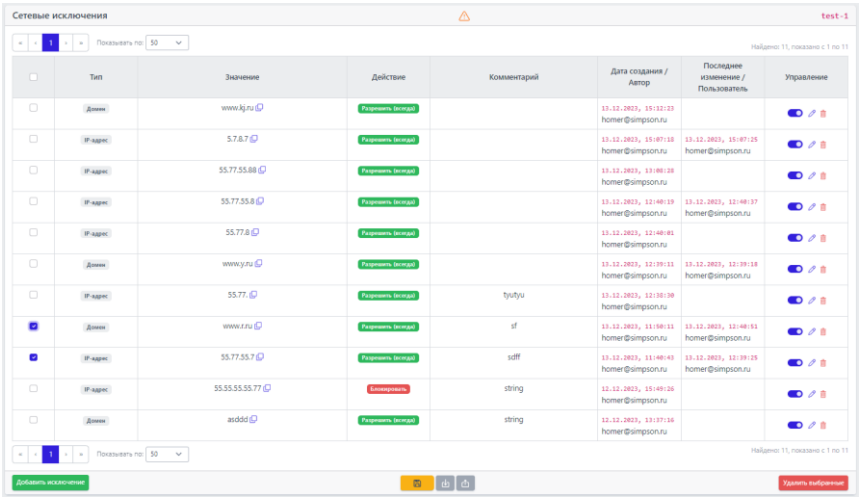



**Рисунок 144 – Страница «Сетевые исключения»**

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

Чтобы завершить операцию, после ввода параметров в окне **Добавить исключение** следует нажать кнопку Добавить. 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 Сохранить. Для отмены изменений следует нажать кнопку **Закрыть 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. 145):

– таблица с наборами исключений для индикаторов атак;

– кнопка **Добавить набор**;

– кнопка **Применить набор**;

– кнопка **Удалить выбранные наборы**.

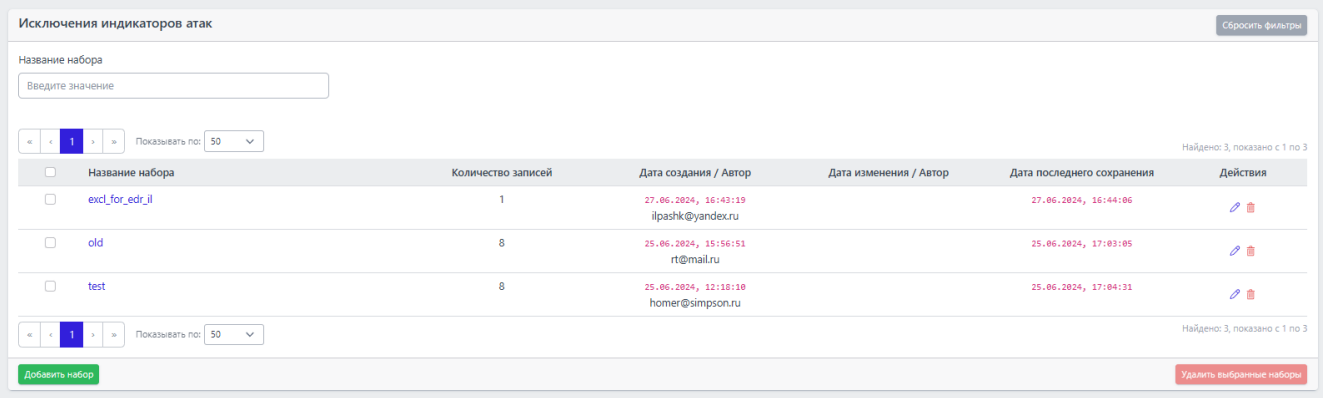



**Рисунок 145 – Страница «Наборы исключений индикаторов атак»**

Чтобы добавить новый набор с сетевыми исключениями, необходимо нажать кнопку **Добавить набор**. 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**.

Страница «Исключения индикаторов атак»

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.

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 Параметры*

В области **Параметры** имеются следующие разделы **Журнал действий, Интеграции, Лицензия**.

6.8.1. Журнал действий

На странице **Журнал действий пользователей** в табличном виде представлена информация о действиях пользователей: аналитиков и администраторов (рис. 146).

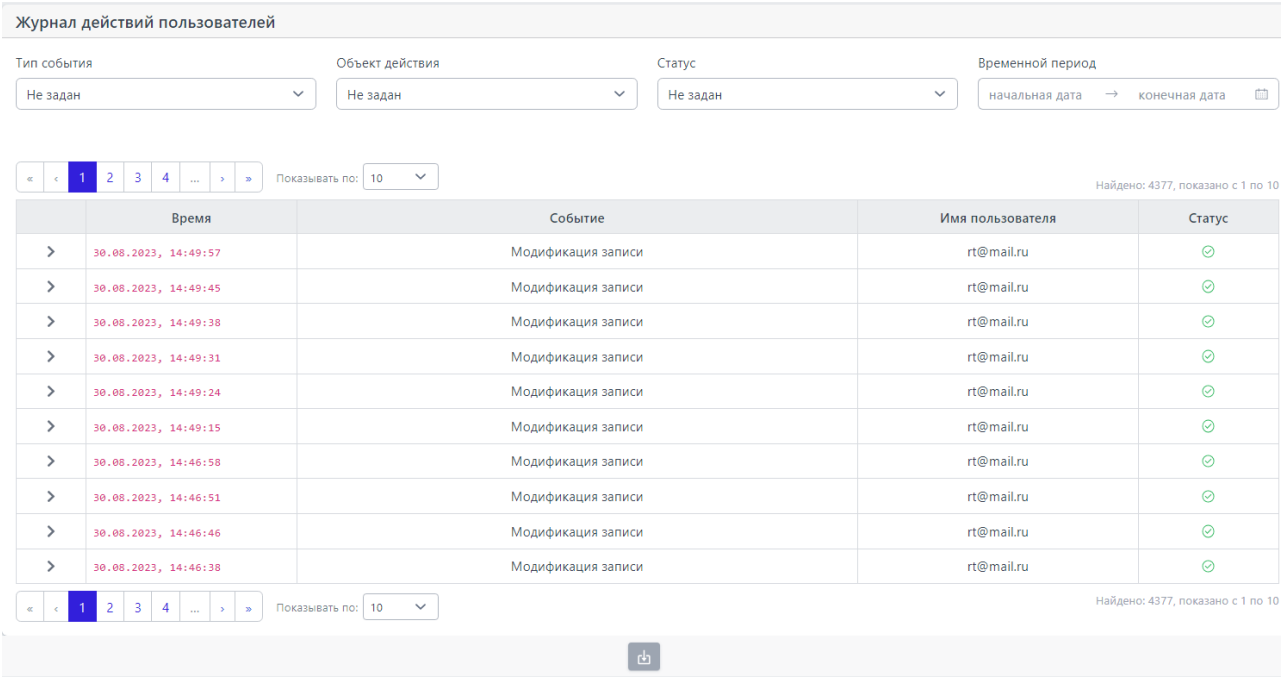



**Рисунок 146 – Журнал действий**

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:

– Пользователь;

– Индикатор компрометации;

– Yara-правило;

– Индикатор атаки;

– Организация;

– Токен;

– Заключение аналитика по IP;

– Заключение аналитика по файлу;

– Заключение аналитика по домену;

– Заключение аналитика по URL;

– Отчет Public TI по файлу;

– Отчет Public TI по IP;

– Отчет Public TI по домену;

– Отчет Public TI по URL;

– Отчет VT по файлу;

– Отчет VT по IP;

– Отчет VT по домену;

– Отчет VT по URL;

– Отчет Athena по файлу;

– Отчет Yara;

– Отчет Netlas по IP;

– Отчет Netlas по домену;

– Журнал Windows;

– Исключения для файлов;

– Исключения для программ.

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 HTML / JSON.

На рисунке 147 отображается информация о событии в формате HTML.

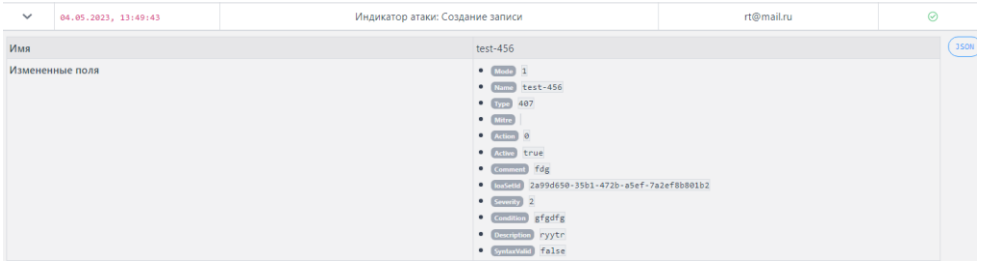



**Рисунок 147 – Отображение информации о событии в формате HTML**

На рисунке 148 отображается информация в формате JSON.

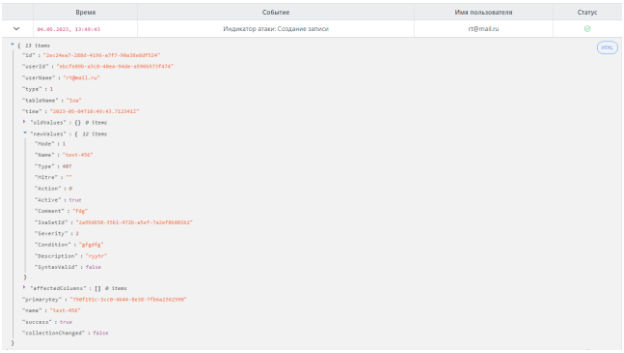


**Рисунок 148 – Отображение информации о событии в формате Json**

В нижней части страницы **Журнал действий** у администратора имеется возможность выгрузить часть журнала, касающуюся модификации аналитики за определенный период. Информация в скачиваемом файле представлена в формате CSV.

Для скачивания файла требуется нажать ЛКМ по иконке . Далее в выпадающем окне следует выбрать временной интервал (месяц/ квартал). Загруженный файл будет находиться в папке **Загрузки**.

6.8.2. Интеграции

На странице **Интеграции** в табличной форме показаны сервисы, с которыми настроена интеграция модуля администрирования сервиса аналитики.

Страница **Интеграции** представлена на рисунке 149.

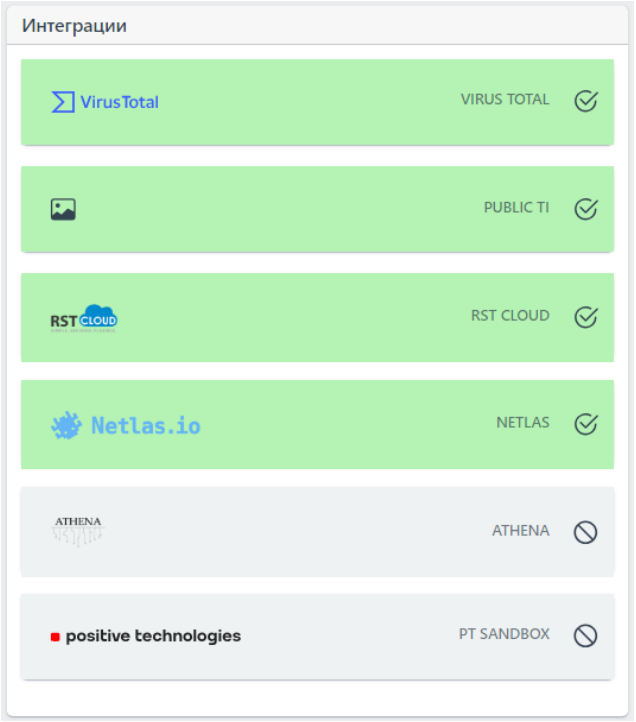



**Рисунок 149 – Страница «Интеграции»**

Все интеграции настраиваются с помощью конфигурационных файлов при развертывании модуля администрирования.

Интеграции разделены на категории:

– Потоковый анализ (Сервис Virus Total, Public TI, RST Cloud);

– Анализ в песочницах (Athena, PT Sandbox);

– Netlas.io.

Таким образом при получении отчета RT Protect TI по какому либо из артефактов, можно перейти по вкладке к инструменту подключенному в рамках интеграции и получить отчет по артефакту от данного сервиса.

6.8.3. Лицензия

Страница подраздела **Лицензия** представлена на рисунке 150.

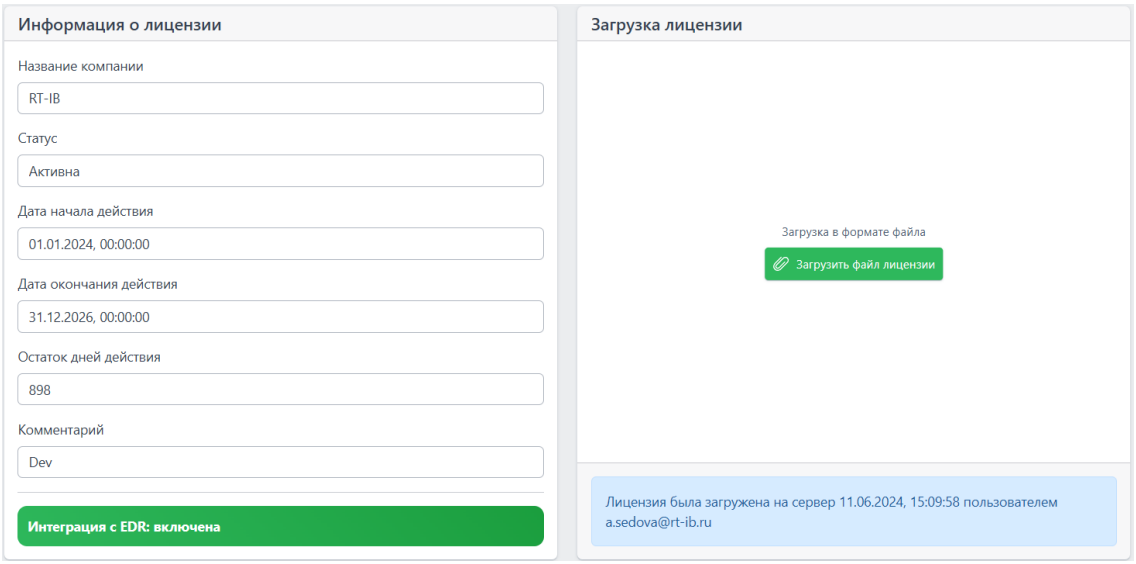



**Рисунок 150 – Страница подраздела «Лицензия»**

На странице имеются две области:

– **Информация о лицензии;**

– **Загрузка лицензии.**

В области **Информация о лицензии** представлена следующая информация:

– **Название компании;**

– **Статус лицензии** (активна/не активна);

– **Дата начала действия лицензии;**

– **Дата окончания действия лицензии;**

– **Остаток дней действия лицензии;**

– **Комментарий.**

В области **Загрузка лицензии** пользователь имеет возможность загрузить файл лицензии.

Также в области **Загрузка лицензии** в нижней части окна представлена информация, когда и каким пользователем была загружена лицензия.

**Важно**

Если лицензия отсутствует или ее срок действия истек, то в модуле администрирования доступны для просмотра следующие страницы:

– **Главная страница** (с возможностью добавления артефактов для проверки с помощью интерфейса, а также через API);

– **Пользователи**;

– **Журнал действий**,

– **Лицензия**;

– **Активность**.

При просмотре отчета по артефакту в модуле администрирования, когда лицензия отсутствует или ее срок действия истек, имеется возможность посмотреть только вкладку **Основная информация**, остальные вкладки будут недоступны.

# 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 особенным образом. Эти сообщения используются почти всегда.

Из-за технологий, используемых в приложении фронтенда, общие сообщения бывают двух типов:

1) экран ошибки;

2) всплывающее сообщение об ошибке.

Пример сообщения в виде экрана ошибки представлен на рисунке 151.

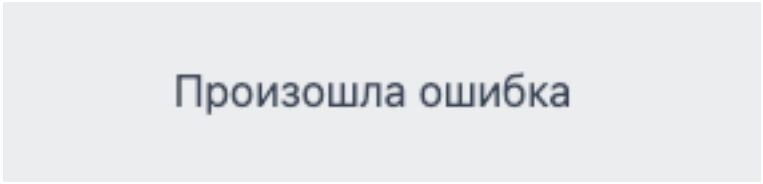



**Рисунок 151 – Сообщение об ошибке типа «Экран ошибки»**

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 152.

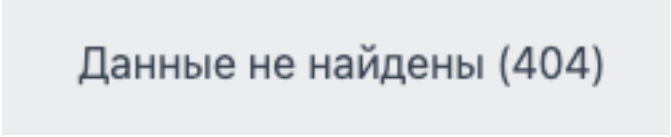



**Рисунок 152 – Сообщение об ошибке**

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 153.

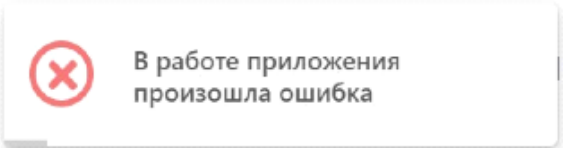



**Рисунок 153 – Всплывающее сообщение об ошибке**

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 154).

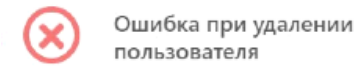



**Рисунок 154 – Ошибка при удалении пользователя**

**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 155).

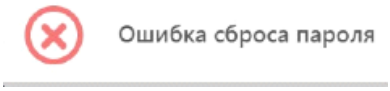



**Рисунок 155 – Ошибка сброса пароля**

**Возможная причина:** некорректный ответ сервера.

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

Страница «Источники данных»

1) Сообщение ошибки при загрузке части файла (создать или редактировать источник данных) представлено на рисунке 156.

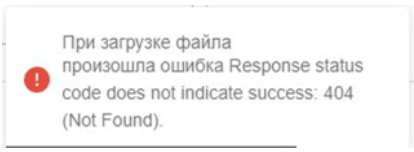



**Рисунок 156 – Ошибка при загрузке файла**

**Возможные причины:** некорректный URL.

**Действия по устранению:** ввести верный URL для источника данных (feed).

2) Сообщение об ошибке при проверке настроек (создать или редактировать источник данных) представлено на рисунке 157.

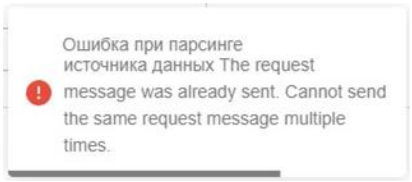



**Рисунок 157 – Окно ошибки при парсинге источника данных**

**Возможные причины:** неправильно заполнены поля (настройка парсинга CSV, JSON, любой формат).

**Действия по устранению:** правильно произвести настройку парсинга для источника данных (feed).

Страницы раздела «Аналитика».

1) Ошибка: неверный формат файла.

Выводимое сообщение представлено на рисунке 158.

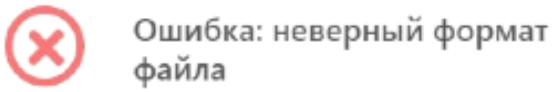



**Рисунок 158 – Неверный формат файла**

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

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

Страницы «Индикаторы атак» и «Yara-правила».

1) Ошибка в правиле.

Выводимое сообщение «Ошибка в правиле YARA» представлено на рисунке 159.

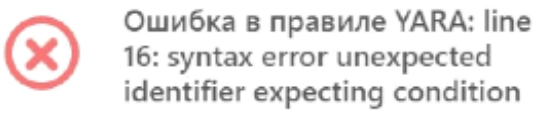



**Рисунок 159 – Ошибка в правиле YARA**

**Возможная причина**: неверное написание YARA-правила, некорректный ответ сервера.

**Возможные действия по устранению**: убедиться в правильности написания YARA-правила, убедиться в наличии связи с сервером, перезагрузить страницу, повторить действие.

2) Ошибка при удалении не пустого набора.

При попытке удаления не пустого набора правил выводится сообщение, представленное на рисунке 160.

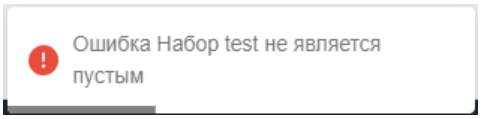



**Рисунок 160 – Сообщение об ошибке при попытке удаления не пустого набора**

Экран авторизации

1) Сообщение об ошибке при вводе неправильных учетных данных представлено на рисунке 161.


**Рисунок 161 – 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 162.


**Рисунок 162 – 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.

Экран лицензии и сообщения об ошибках лицензии на других экранах

1) Сообщение в хедере об отсутствии лицензии приведено на рисунке 163.

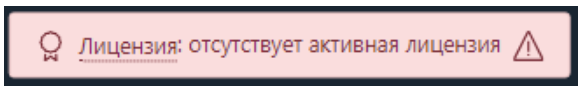



**Рисунок 163 – Отсутствует лицензия**

Данное сообщение отображается на всех экранах приложения в хедере в том случае, если лицензия не была загружена.

Если роль пользователя «Администратор сервера», то слово «Лицензия» является ссылкой, ведущей на экран «Лицензии». Если роль пользователя «Администратор безопасности», то при наведении курсора на слово «Лицензии»

отображается поясняющий текст «Для управления лицензиями требуется роль «Администратор сервера».

**Возможные причины:** лицензия не была загружена.

**Действия по устранению:** сообщить администратору, перейти к лицензии, загрузить файл лицензии.

2) Сообщение в хедере о наличии проблем с лицензией представлено на рисунке 164.


**Рисунок 164 – Сообщение о проблемах с лицензией**

Данное сообщение отображается на всех экранах приложения в хедере в том случае, если лицензия была загружена, но выполнены не все её условия. Число в скобках означает количество нарушенных требований (это может быть срок действия и допустимое количество агентов).

Если роль пользователя «Администратор сервера», то слово «Лицензия» является ссылкой, ведущей на экран «Лицензии». Если роль пользователя «Администратор безопасности», то при наведении курсора на слово «Лицензии» отображается поясняющий текст «Для управления лицензиями требуется роль «Администратор сервера».

**Возможные причины**: закончился срок действия лицензии или было превышено количество агентов.

**Действия по устранению**: сообщить администратору, перейти к лицензии, устранить проблемы.

3) Сообщения о функциональных ограничениях вследствие отсутствия лицензии представлены на рисунках 165 - 166 .

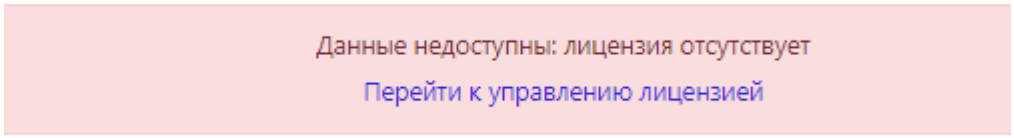



**Рисунок 165 – Сообщение при отсутствии лицензии**

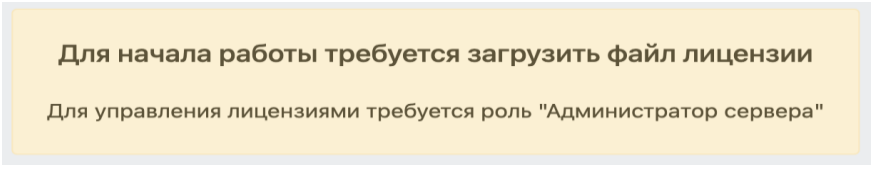



**Рисунок 166 – Сообщение при отсутствии лицензии**

Данное сообщение отображается на всех экранах приложения (кроме экрана **Лицензии**). Оно свидетельствует о том, что лицензия не была загружена на сервер, поэтому функционал приложения ограничен.

**Возможные причины:** лицензия не была загружена.

**Действия по устранению:** сообщить администратору, перейти к лицензии, загрузить файл лицензии.

4) Сообщение о проблемах с лицензией на экране **Лицензии** представлено на рисунке 167.

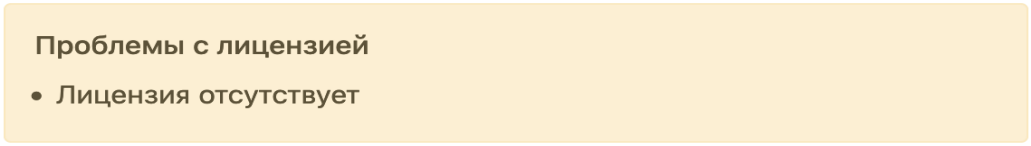



**Рисунок 167 – Сообщение об отсутствии лицензии**

Данное сообщение отображается на экране **Лицензии**. Данный экран доступен только пользователям с ролью «Администратор сервера».

**Возможные причины:** лицензия не была загружена, истек срок действия лицензии, было превышено допустимое кол-во агентов.

**Действия по устранению:** сообщить администратору, загрузить новый файл лицензии.

# 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 клиентской или серверной части.

Для устранения ошибки требуется переконфигурировать программу либо восстановить ее из ранее сделанной резервной копии, либо восстановить программу с установочного носителя согласно рекомендациям настоящего руководства.

# 9. Перечень сокращений

Основные сокращения, указанные в документе, представлены в таблице 7.

**Таблица 7 – 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».