

RT Protect TI

Руководство администратора

Версия 1.0.35 от 19 июня 2026

Разработано компанией АО «РТ-Информационная безопасность»



1. Общие положения	5
1.1 Идентификация документа	5
1.2 Аннотация документа	5
1.3 Термины и определения	5
1.4 Условные обозначения	6
2. Общие сведения	8
2.1 Назначение и архитектура программы	8
3. Организационно-распорядительные меры.....	10
3.1 Общие сведения	10
3.2 Комплектность поставки	10
3.2.1. Процедуры и меры безопасности при распространении программы к месту назначения	10
4. Структура программы.....	11
5. Настройка программы.....	12
5.1 Требования к среде функционирования	12
5.2 Инструкция по развертыванию TI-платформы.....	12
Шаг 1. Подготовка окружения	12
Шаг 2. Создание конфигурации сервера.....	13
Шаг 3. Запуск скрипта развертывания (Ansible Playbook)	22
Шаг 4 (опциональный). Обновление сервера	23
5.3 Мониторинг состояния компонентов сервера	23
5.4 Роли	25
6. Интерфейс программы	28
6.1 Окно авторизации и общие сведения	28
6.2 Горизонтальная панель управления	30
6.2.1. Меню «Пользователь»	32
6.3 Главная страница	35

6.4 Администрирование	36
6.4.1. Пользователи.....	36
6.4.2. Организации.....	44
6.4.3. Источники данных	53
6.4.4. Теги.....	69
6.5 Аналитика	78
6.5.1. Активность.....	79
6.5.2. Заключение аналитика	91
6.5.3. Анализаторы	98
6.5.4. Граф связей	108
6.5.5. Yara-правила	111
6.5.6. Распространяемая аналитика.....	117
6.5.7. Угрозы и злоумышленники	125
6.5.8. Вредоносное ПО	126
6.5.9. Инструменты	127
6.5.10. Матрица MITRE ATT&CK	129
6.5.11. Лента угроз	129
6.5.12. Уязвимости	134
6.5.13. Алгоритм формирования оценки артефакта	146
6.5.14. ИИ агент	147
6.6 Аналитика EDR	149
6.6.1. Индикаторы атак	149
6.6.2. Индикаторы компрометации	157
6.6.3. Журналы.....	162
6.6.4. Yara-правила (файлы)	165
6.6.5. Yara-правила (память).....	169
6.7 Исключения EDR.....	172
6.7.1. Исключения для программ	172

6.7.2. Исключения для файлов.....	180
6.7.3. Сетевые исключения.....	185
6.7.4. Исключения индикаторов атак.....	189
6.8 Параметры.....	194
6.8.1. Журнал действий	194
6.8.2. Лицензия	197
7. Сообщения администратору	200
7.1 Общие сведения	200
7.2 Сообщения об ошибках	200
7.2.1. Общие сообщения.....	200
7.2.2. Специфичные сообщения	202
8. Действия после сбоя и ошибки.....	208
8.1 Общие сведения	208
9. Перечень сокращений	209
10. Заключение	210

1. Общие положения

1.1 Идентификация документа

Данное руководство кратко можно идентифицировать согласно таблице 1.

Таблица 1 – Идентификация документа

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

1.2 Аннотация документа

Документ предназначен для ознакомления администраторами 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

Термин	Описание
Backend	Программно-аппаратная часть сервиса, отвечающая за функционирование его внутренней части
JSON	Текстовый формат обмена данными, основанный на JavaScript
JSON-объект	Неупорядоченный набор пар ключ/значение. Объект начинается с открывающей фигурной скобки { и заканчивается закрывающей фигурной скобкой }. Каждое имя сопровождается двоеточием, пары ключ/значение разделяются запятой
Linux	Семейство Unix-подобных операционных систем на базе ядра Linux
Malware Bazaar	Проект сайта abuse.ch, целью которого является обмен образцами вредоносного ПО с сообществом информационной безопасности, поставщиками антивирусных программ и поставщиками информации об угрозах
SSDEEP	Алгоритм нечеткого хеширования
TCP	Один из основных протоколов передачи данных интернета. Предназначен для управления передачей данных интернета. Пакеты в TCP называются сегментами. В стеке протоколов TCP/IP выполняет функции транспортного уровня модели OSI
VirusTotal	Бесплатная служба, осуществляющая анализ подозрительных файлов и ссылок (URL) на предмет выявления вирусов, червей, троянов и всевозможных вредоносных программ
Web-сервер	Сервер, принимающий HTTP-запросы от клиентов, чаще всего веб-браузеров, и выдающий HTTP-ответы, как правило, вместе с HTML-страницей, изображением, файлом, медиа-поток или другими данными
WHOIS	Сетевой протокол прикладного уровня, базирующийся на протоколе TCP. Основное применение – получение регистрационных данных о владельцах доменных имён, IP-адресов и автономных систем
Windows	Группа семейств коммерческих операционных систем корпорации Microsoft, ориентированных на управление с помощью графического интерфейса

1.4 Условные обозначения

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

Таблица 3 – Условные обозначения

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

<table border="1"> <tr> <td data-bbox="165 185 317 349">  </td> <td data-bbox="317 185 547 349"> Примечание </td> </tr> <tr> <td colspan="2" data-bbox="165 264 547 349"></td> </tr> </table>		Примечание			Информация, требующая внимания пользователя
	Примечание				
<table border="1"> <tr> <td data-bbox="165 492 317 656">  </td> <td data-bbox="317 492 547 656"> Важно </td> </tr> <tr> <td colspan="2" data-bbox="165 571 547 656"></td> </tr> </table>		Важно			Информация, связанная с важными конфигурационными настройками и особенностями работы RT Protect TI
	Важно				

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;
- сбор информации о распространенности артефактов среди подключенных к TI-платформе клиентов;
- формирование аналитики различных форматов для распространения клиентам TI-портала через API;
- получение вердикта по анализируемым артефактам;
- формирование и содержание в актуальном состоянии базы данных уязвимостей программного обеспечения;
- 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 Модуль администрирования «RT Protect TI»	1	
	Комплект документов согласно списку: — «Руководство Администратора RT Protect TI» — «Руководство Аналитика RT Protect TI» — «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.

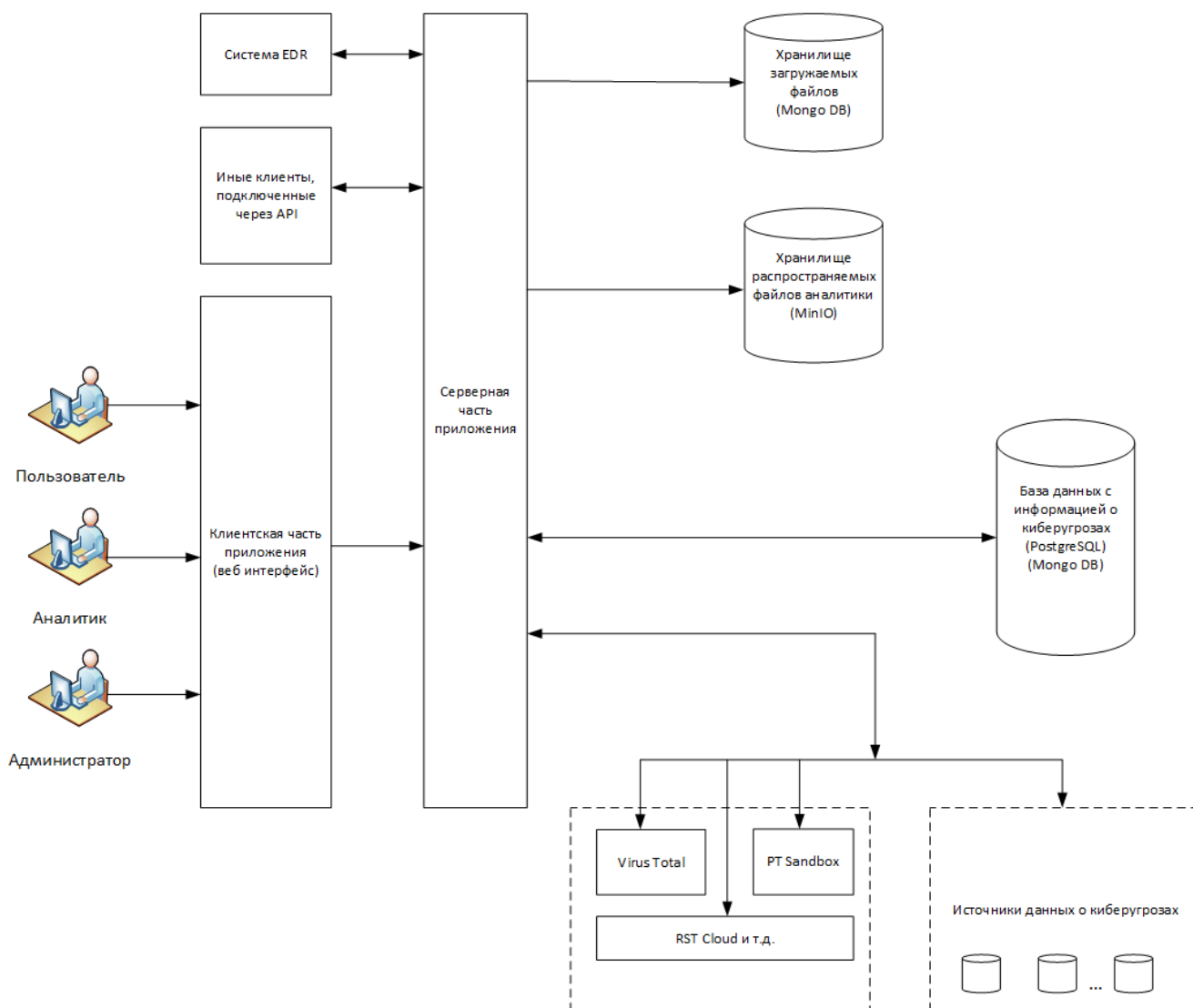


Рисунок 1 – Схема архитектуры сервиса

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 12 ядер частотой минимум 2,4 ГГц	Не менее 20 ядер частотой минимум 2,4 ГГц
Оперативная память	32 ГБ	64 ГБ
Жесткий диск	SSD:2 ТБ	SSD: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 APM, на котором разворачивается сервер TI, осуществив запрос на получение данного репозитория к контактными лицам от поставщика.

Далее необходимо перейти в корень репозитория ti-deploy.

Структура каталогов будет представлена на рисунке 2.

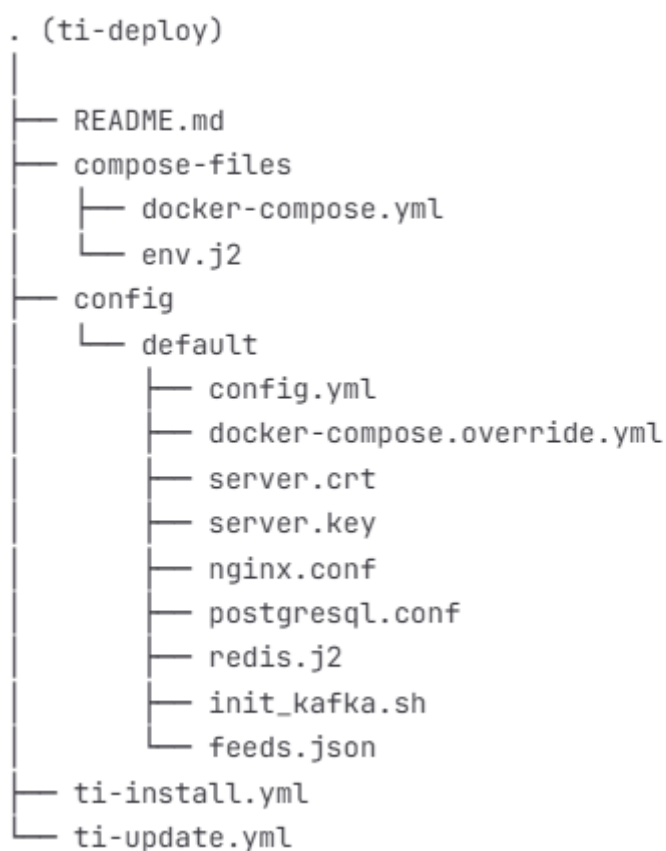


Рисунок 2 – Структура каталогов репозитория ti-deploy

В каталоге `config` хранятся конфигурации серверов. В данный каталог 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. Именовывать подкаталоги удобно, например, по IP-адресу сервера или домену. Тогда структура каталога `config` со временем примет вид, представленный на рисунке 3.

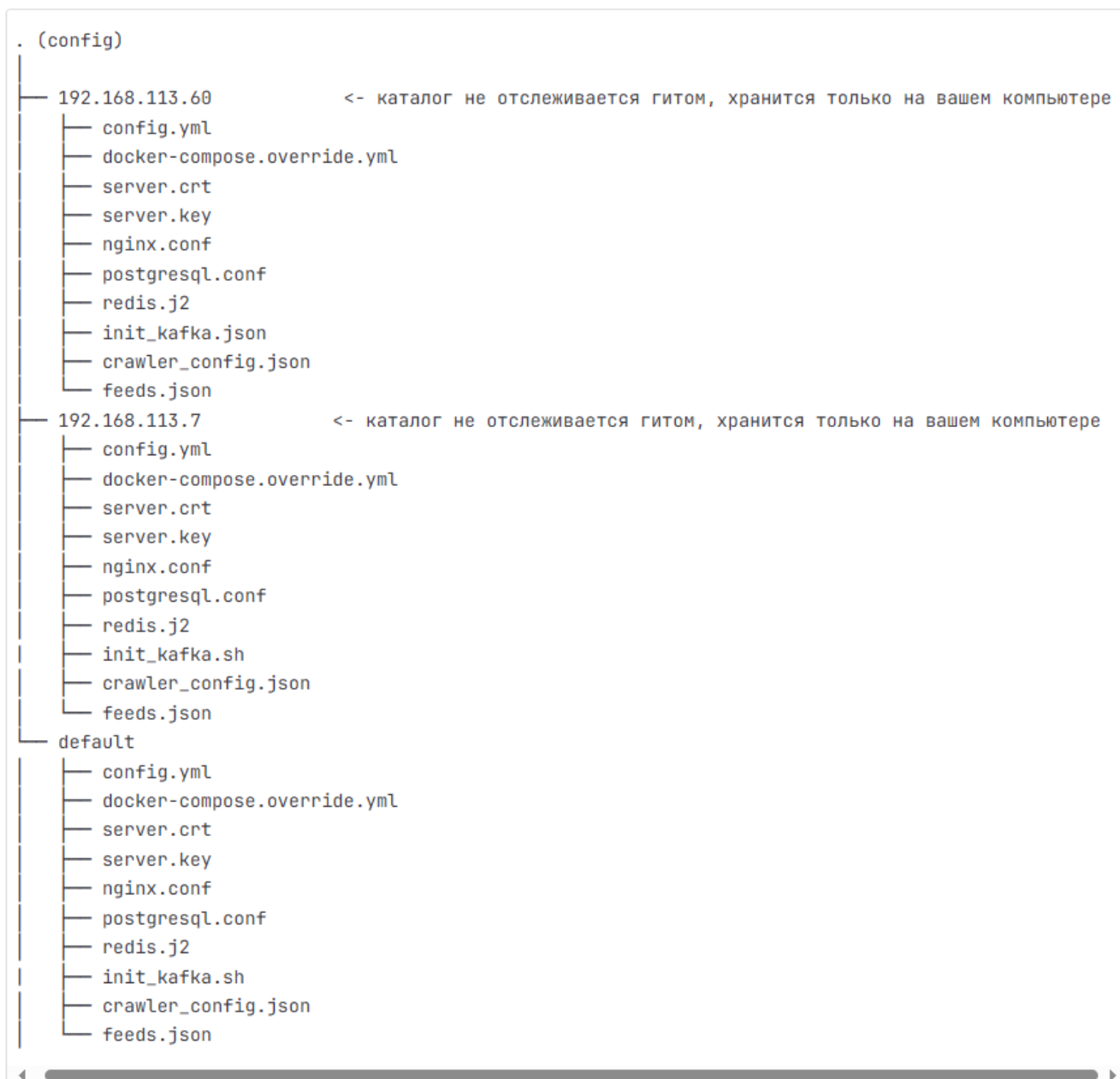


Рисунок 3 – Структура каталога `config`

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 – 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;
- feeds.json – JSON-файл с источниками данных по умолчанию для указанного сервера;
- redis.j2 – конфигурационный файл Redis (при отсутствии необходимости лучше оставить по умолчанию);
- init_kafka.sh - Скрипт для инициализации Kafka (при отсутствии необходимости лучше оставить по умолчанию);
- crawler_config.json - JSON-файл с источниками для получения статей по умолчанию для указанного сервера;
- nginx.conf – конфигурационный файл NGINX (при отсутствии необходимости лучше оставить по умолчанию);
- postgresql.conf – конфигурационный файл PostgreSQL (при отсутствии необходимости лучше оставить по умолчанию).

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

Описание конфигураций в файле config.yml приведено в следующем списке:

1) Общие конфигурации:

- config_name: "default" - Название конфигурации. Должно совпадать с названием каталога, содержащего данный конфигурационный файл.
- host_ip: "31.13.33.68" - IP-адрес целевой машины;
- home_url: "https://ti.rt-protect.ru/" - URL, по которому будет открываться главная страница приложения;

— `default_culture: "ru-RU"` – локализация сервера по умолчанию. Поддерживается 2 варианта: "ru-RU" и "en-US";

— `internal_token: "KaDDUNn4jjqd5G8JvFvtDg0VeSfyMN"`. Токен для внутренних API-вызовов.

Рекомендуется заменить строку на аналогичную случайную;

— `detect_worker_count: 10`. Количество воркеров для фиксации обнаружений. Рекомендуется оставить значение по умолчанию.

2) Настройки подключения к реестру Docker-образов.

Образы хранятся в реестре по адресу <https://docker.rt-protect.ru/containers>.

— `docker_registry: docker.rt-protect.ru`;

— `docker_registry_user: "user"`;

— `docker_registry_password: "pass"`;

3) Параметры конфигурации PostgreSQL.

Если не планируется подключения в БД извне, можно использовать любую комбинацию имени и пароля (лучше не дефолтные)

— `db_user_name: "ti_server_user"` – Имя пользователя;

— `db_user_password: "pass"` – пароль для работы с БД PostgreSQL;

— `db_files_path: "/media/ti/database"` – путь до каталога, в котором БД будет хранить данные;

— `db_backup_path: "/media/ti/db_backup"` – путь до каталога, куда будут складываться бекапы БД.

4) Параметры конфигурации JWT.

— `jwt_token_secret: "xyvfmwehpqwpkcmihyjtiaiwatbjouk"` – секрет, на основе которого будут подписываться выпущенные токены. Необходимо делать сложным и уникальным. Минимальная длина - 32 символа

— `jwt_token_issuer: "ti.rt-protect.ru"`;

— `jwt_token_audience: "ti.rt-protect.ru"`;

— `jwt_token_expiration: "120"` – Время устаревания JWT токена в минутах. Чем меньше, тем безопаснее для сервера;

— `refresh_token_expiration: "10080"` – Время устаревания refresh токена в минутах. Если не заходить на сайт в течении этого времени, потребуется повторный вход в систему.

5) Параметры конфигурации сервера.

— detect_enabled: "true" — признак включения записи "Активность". Если false, то страница "Активность" обновляться не будет.

6) Параметры конфигурации MongoDB.

— mongo_user_name: "root" — логин для инициализации MongoDB. Лучше поменять с дефолтных значений.

— mongo_user_password: "pass" — пароль инициализации MongoDB;

— storage_path: "/media/ti/storage" — путь, где MongoDB будет хранить свои данные;

— mongo_version: "7.0.5" — версия MongoDB.

7) Параметры конфигурации Redis.

— redis_password: "zWQaR1uNF8fcbI3XsQho6pIV" — пароль Redis;

— redis_path: "/media/ti/redis" — путь до хранилища Redis.

8) Параметры конфигурации внешних инструментов.

— ptms_enabled: "false" — флаг доступности модуля PT MultiScanner;

— ptms_report_lifetime: "30" — время актуальности отчета PTMS в днях

— ptms_api_key:

"IYN5nl_39oDvjKXeuf2JSn2ZPxemAEoCIEXVemX1MTEuU3LXLFWr8jpfibob_IncFPcMJgpQMkMDExuKGChro0Q" — ключ доступа до PTMS;

— ptms_api_path: "https://192.168.0.100/api/v1" Путь до API PTMS

— ptms_auto_enrichment: "false" — автоматическое обогащение из источника данных;

— ptms_sandbox: "false" — отправлять файлы на динамический анализ (если позволяет продукт);

— ptms_sandbox_image_id: "win10-1803-x64" — образ динамического анализа (если позволяет продукт);

— ptms_sandbox_duration: 180 — продолжительность динамического анализа;

— kaspersky_enabled: "true" — флаг доступности модуля KasperskyTI;

— kaspersky_api_key: "key" — ключ доступа для KasperskyTI;

— kaspersky_auto_enrichment: "true" — автоматическое обогащение из источника данных;

— vt_enabled: "true" — флаг активации модуля VT;

- vt_api_key: "key" – ключ доступа для VT;
- vt_auto_enrichment: "true" – автоматическое обогащение из источника данных;
- athena_enabled: "true" – флаг активации модуля Athena;
- athena_url: https://jupiter.avsw.ru/ – путь до API Athena;
- athena_token: "token" – ключ доступа для Athena;
- athena_ssl: "true" – флаг проверки сертификата при обращении к Athena;
- athena_auto_enrichment: "true" – автоматическое обогащение из источника данных;
- rst_cloud_enabled: "true" – флаг активации модуля RST Cloud;
- rst_cloud_token: "token" – ключ доступа для RST Cloud;
- rst_cloud_auto_enrichment: "true" – автоматическое обогащение из источника данных;
- netlas_enabled: "true" – флаг активации модуля Netlas;
- netlas_token: "tqfd90zd0g3ujlssXwdZf9aFV4Tx0qli45scWciU" – ключ доступа для Netlas;
- netlas_auto_enrichment: "false" – автоматическое обогащение из источника данных;

9) Параметры конфигурации Kafka.

- zk_data_path: "/media/ti/zk-data";
- zk_logs_path: "/media/ti/zk-txn-logs";
- kafka_data_path: "/media/ti/kafka-data".

10) Параметры конфигурации MinIO.

- minio_path: "/media/ti/minio";
- minio_access_key: "7TjqfXUAsG2eTtK2L45U";
- minio_secret_key: "rWf8E62JXi61yHDubhP5".

11) Параметры SMTP.

- smtp_host: "smtp.yandex.ru" – хост сервера SMTP;
- smtp_port: "465" – порт сервера SMTP;
- smtp_username: "username" – имя пользователя для авторизации на сервере SMTP;
- smtp_password: "password" – пароль для авторизации на сервере SMTP;
- smtp_use_ssl: true – флаг использования ssl для доступа к SMTP серверу;
- smtp_enabled: false – признак включения интеграции с сервером SMTP;

- smtp_from_name: "RT Protect TI" – имя в поле from для отправляемых сообщений;
- smtp_from_address: "ti@rt-ib.ru" – адрес отправителя сообщений.

12) Параметры работы с уязвимостями.

Лимит на количество уязвимостей из базы, с которыми будут проверяться компоненты.

Если установлено -1, значит без ограничения.

Рекомендуется оставить значение -1.

- vulnerabilities_limit: -1;
- vuln_sync_enabled: true;
- nvd_api_key: "nvd_key".

13) Параметры работы с модулем TI Reports.

- report_enabled: true - флаг активации модуля ленты угроз;
- report_worker_url: https://ml-rt-ti-reports.rt-ib.ru - URL до сервиса TI Reports;
- report_api_key: "key" - ключ для доступа к сервису TI Reports.

14) Настройки версий компонентов.

- back_version: "3.1.3"
- front_version: "1.1.43"
- detect_worker_version: "3.0.0"
- migrator_version: "2.1.19"
- feed_worker_version: "2.0.19"
- feed_downloader_worker_version: "2.0.7"
- vuln_worker_version: "2.0.2"
- vuln_downloader_worker_version: "2.0.3"
- vuln_engine_worker_version: "2.0.2"
- yara_update_worker_version: "2.0.2"
- analyzer_worker_version: "1.0.6"
- crawler_worker_version: "1.0.17"
- report_worker_version: "1.0.7"

15) Настройки подключенных анализаторов.

- kaspersky_api_key: "key";
- vt_api_key: "key";
- netlas_api_key: "key";
- rst_cloud_api_key: "key";
- pt_sandbox_api_key: "key".

16) Настройки подключенных анализаторов

- kaspersky_api_key: "key";
- vt_api_key: "key";
- netlas_api_key: "key";
- rst_cloud_api_key: "key";
- pt_sandbox_api_key: "key";

17) Адрес сервера PT Sandbox. pt_sandbox_server: "https://localhost";

- Флаг включения поведенческого анализа. pt_sandbox_enabled: true;
- Длительность выполнения поведенческого анализа (если pt_sandbox_enabled: true);
- pt_sandbox_duration: 180;
- Идентификатор образа виртуальной машины, на которой будет выполняться поведенческий анализ

(если pt_sandbox_enabled: true);

- pt_sandbox_image_id: "win7-sp1-x64";
- meta_defender_api_key: "key"
- geo_ip_login: ""
- geo_ip_password: ""
- abuse_ipdb_api_key: ""
- alien_vault_api_key: ""
- malshare_api_key: ""
- kaspersky_analyzer_version: "1.0.7"
- vt_analyzer_version: "3.0.19"
- netlas_analyzer_version: "1.0.9"
- rst_cloud_analyzer_version: "1.0.12"

- static_analyzer_version: "3.0.5"
- yara_analyzer_version: "3.0.2"
- fuzzy_family_analyzer_version: "1.0.9"
- pt_sandbox_version: "1.0.3"
- meta_defender_analyzer_version: "1.0.4"
- geo_ip_analyzer_version: "1.0.2"
- abuse_ipdb_analyzer_version: "1.0.1"
- alien_vault_analyzer_version: "1.0.6"
- malshare_analyzer_version: "1.0.1"

18) Настройки подключенных провайдеров данных

- fincert_login: "login";
- fincert_password: "password";
- fincert_base_url: "http://127.0.0.1:3456";
- pt_feeds_api_key: "api_key";

19) Названия коллекций PT Feeds.

- pt_feeds_collections: ["current-act"]
- fincert_version: "1.0.5"
- pt_feeds_version: "1.0.1"
- meta_defender_provider_version: "1.0.4"

20) Пути на сервере (на Docker-хосте).

Определяют местоположение файлов, которые передаются на сервер (менять не рекомендуется).

compose_dir: ./rt-protect/ti – путь до каталога с файлами docker-compose.yml и env.

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 конфигурация тестовая, и доступ извне будет ограничен. В этом случае сертификат будет самоподписанным.

Опционально в каталог `config` можно положить файл `feeds.json` из стандартной конфигурации, либо полученный с другого TI-сервера. Если такой файл присутствует, при выполнении `ti-install` Ansible-скрипт выполнит инициализацию таблицы источников данных тем набором источников, который содержится в файле `feeds.json`.

Вместе с файлом `feeds.json` в каталоге `config` может находиться подкаталог `feed_files`, в котором должны находиться файлы, используемые по умолчанию при инициализации списка источников данных. Имя файла должно строго совпадать с именем источника.

Также опционально в каталоге располагается файл `crawler_config.json`. Он используется для первичной инициализации страницы "Источники" внутри Ленты угроз.

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.

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-pass
```

5.3 Мониторинг состояния компонентов сервера

Администратор может просматривать состояние компонентов сервера (контейнеров) в реальном времени.

Для этого после развертывания сервера необходимо настроить сервис мониторинга Gatus и Dozzle.

Для настройки компонентов Gatus и Dozzle следует выполнить следующие действия, описанные ниже.

1) Скопировать (либо запросить у производителя) репозиторий ti-monitoring на целевую машину, где установлен сервер. Перейти в каталог репозитория.

2) Заполнить конфигурацию файла gatus.env для настройки системы мониторинга Gatus.

Параметры для заполнения:

- SCHEME=https - схема обращения к серверу TI;
- HOST=ti-dev.rt-protect.ru - Адрес сервера TI;
- INSECURE=false - Если true, обращаться без проверки сертификата;
- PRODUCT_TYPE=TI DEV - Тип продукта (используется в веб интерфейсе Gatus и в алертах);

Для того чтобы сообщения (алерты) о неисправности компонентов приходили в Telegram настроить следующие параметры:

- TELEGRAM_ENABLED=false;
- TELEGRAM_BOT_TOKEN= - Токен бота выпускается через бота @BotFather;
- TELEGRAM_USER_ID= - Идентификатор чата или канала, в который будут отправляться алерты.

Необходимо создать канал, затем добавить в него ранее созданного бота в качестве админа. После этого при помощи запроса <https://api.telegram.org/bot<токен вашего бота>/getUpdates> в браузере можно получить идентификатор группы в объекте вида `{"chat":{"id":-4880480591,"title"...``

Для того чтобы сообщения (алерты) о неисправности компонентов приходили на email, настроить следующие параметры:

- EMAIL_ENABLED=false
- EMAIL_HOST=
- EMAIL_FROM=
- EMAIL_USERNAME=
- EMAIL_PASSWORD=
- EMAIL_TO=

3) Сделать файлы run-dozzle.sh и run-gatus.sh исполняемыми выполнив команды:

```
chmod +x run-gatus.sh
```

```
chmod +x run-dozzle.sh,
```

4) Выполнить запуск с помощью команд:

```
./run-dozzle.sh и run-gatus.sh.
```

5) После этого на порту 8888 машины где установлен сервер будет доступен интерфейс Dozzle, позволяющий просматривать логи всех запущенных на машине контейнеров в реальном времени. На порту 9090 будет запущен сервис Gatus, выполняющий healthcheck всех компонентов TI. Данный сервис также будет отправлять алерты в Telegram и на почту, если такой функционал настроен.

5.4 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).

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.

Функциональность TI-платформы зависит не только от выставленных ролей пользователей, от которых осуществлен вход, а еще и от признака – Организация владелец/ не владелец TI-платформы.

Основные функции для пользователя с ролью «Администратор» с признаком владелец платформы, можно кратко описать согласно следующему списку:

- Администрирование пользователей;
- Выпуск квот (ограничений) по использованию API-вызовов для получения отчетов по проверке файлов, проверке доменов и другой информации для пользователей и организаций в рамках организации владельца платформы;
- Добавление токенов.

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

- Добавление правил аналитики EDR;
- Добавление исключений для аналитики EDR;
- Добавление лицензий для интеграции с подключаемыми модулями и взаимодействия с другими сервисами (например, EDR).

Подробнее о функционале, доступном для администратора в рамках организации владельца платформы, описано в данном руководстве.

Функционал, доступный для других ролей для пользователей организаций владельца /не владельца платформы, описан в отдельных руководствах.

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).

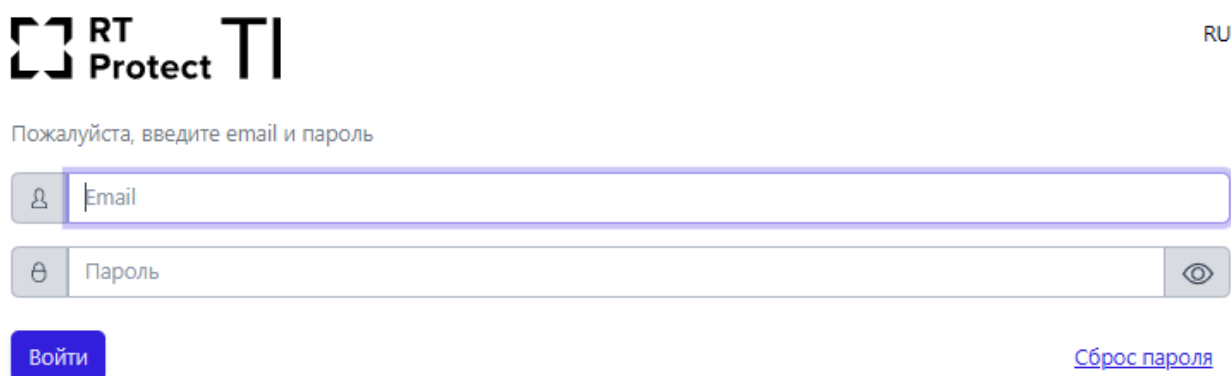


Рисунок 4 – Окно авторизации

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.

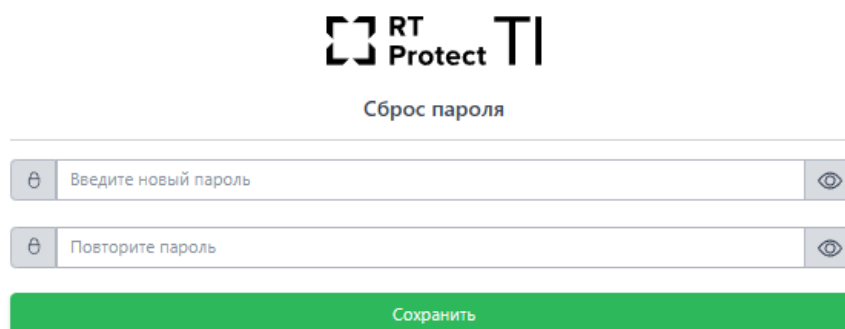


Рисунок 5 – Окно ввода параметров для сброса пароля

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).

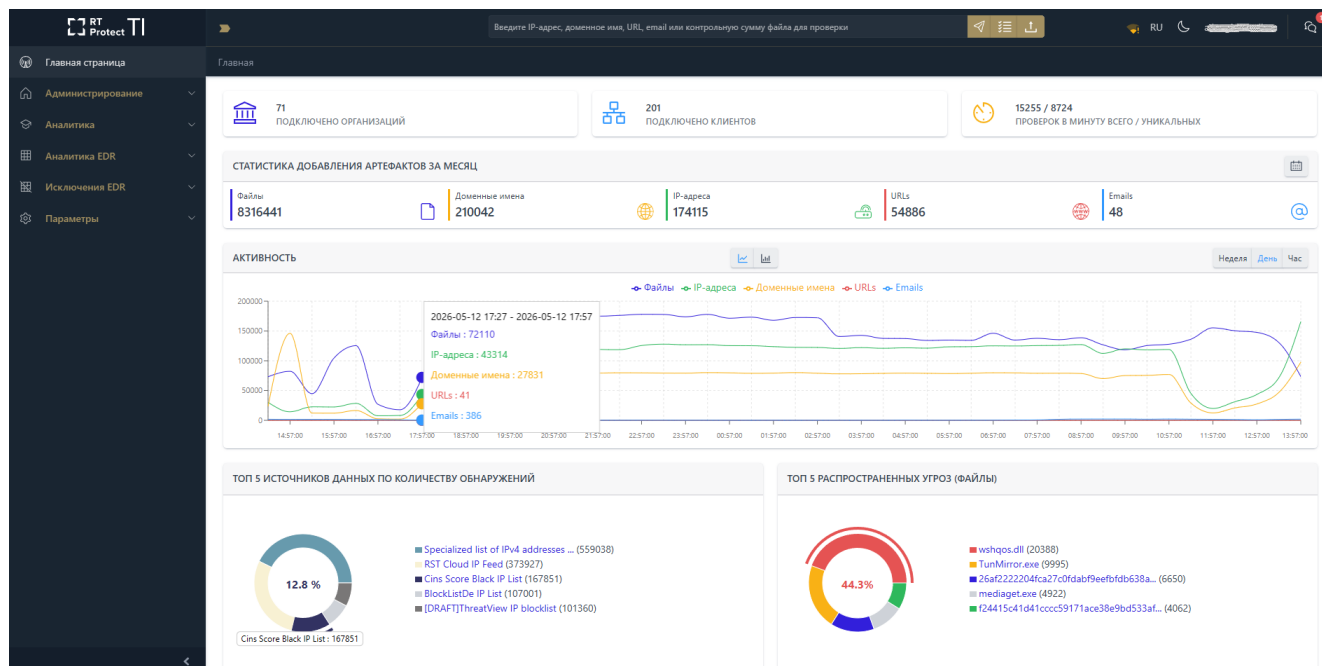


Рисунок 6 – Основное окно программы

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, уага-правила, журналы Windows, исключения для программ, исключения для файлов, сетевые исключения);
- просмотр актуальной базы данных уязвимостей и имеющейся в распоряжении TI базы данных ПО, просканированного при помощи сканера уязвимостей TI;
- просмотр действий пользователей, произведенных в модуле администрирования программы.

В левой части основного окна программы (см. рис. **Ошибка! Источник ссылки не найден.**) находится вертикальная панель управления, доступная администратору. С помощью панели управления пользователь может переходить по разделам программы для изменения настроек и просмотра информации по разделам. При выборе определенного раздела в правой части окна будет представлена информация выбранного раздела и основной инструментарий для работы пользователя программы.

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

6.2 Горизонтальная панель управления

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

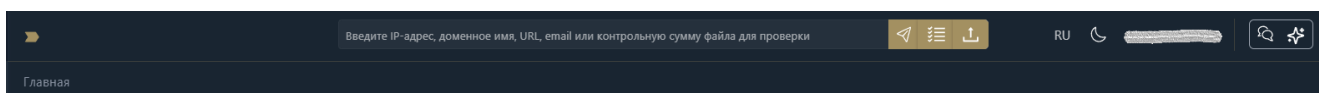
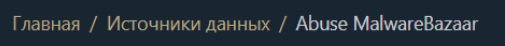


Рисунок 7 – Горизонтальная панель управления

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

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

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

При нажатии ЛКМ по иконке  появляется область, представленная на рисунке 8.

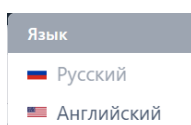


Рисунок 8 – Выбор языка

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



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



При нажатии по иконке , открывается окно для работы с ИИ агентом (подробнее см. в пункте 6.5.14).

В области представленной на рисунке 9 можно отправить артефакт, либо список артефактов на проверку.



Рисунок 9 – Область быстрой отправки артефактов на проверку

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

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

В области **Проверка артефактов** администратор также может проверить целый список артефактов, нажав по иконке , после чего откроется окно для загрузки списка артефактов, представленное на рисунке 10.

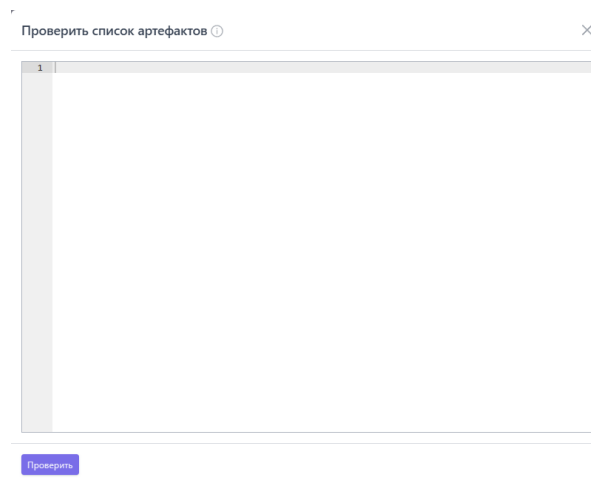


Рисунок 10 – Окно для добавления списка артефактов для проверки

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

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

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

6.2.1. Меню «Пользователь»

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

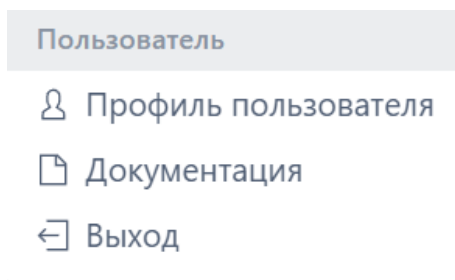


Рисунок 11 – Меню «Пользователь»

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

Подменю **Профиль пользователя** представлено на рисунке 12.

Рисунок 12 – Подменю «Профиль пользователя»

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

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

Изменять пароль возможно с помощью кнопки **Сменить пароль**. При нажатии кнопки **Сменить пароль** открывается окно для смены пароля (рис. 13).

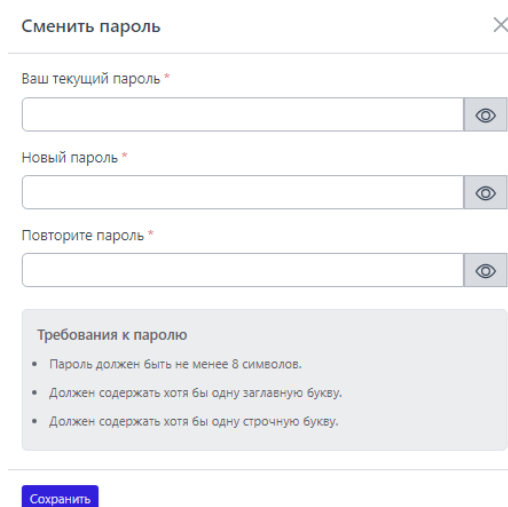


Рисунок 13 – Окно смены пароля

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 14 представлен раздел **Главная страница** модуля управления.

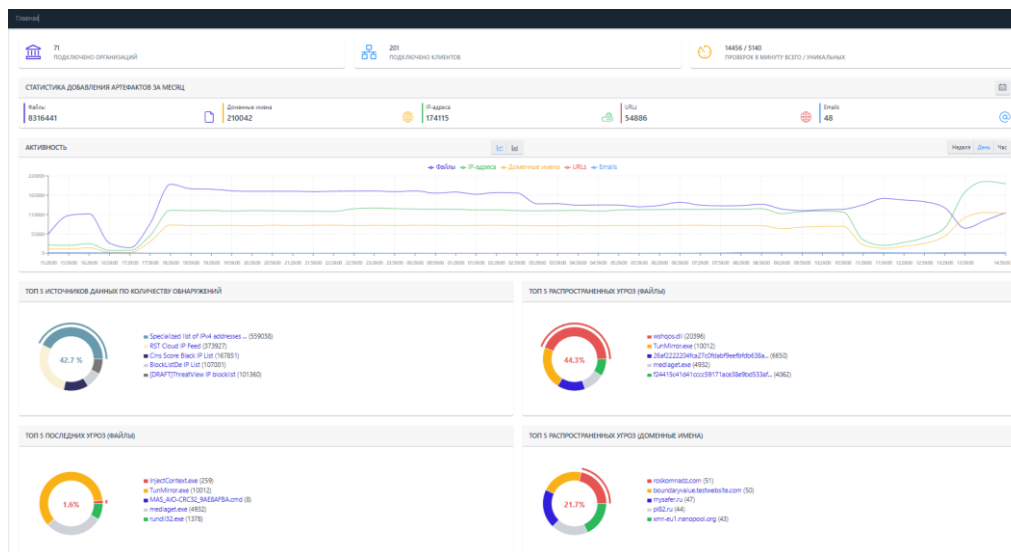


Рисунок 14 – Главная страница

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

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

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 15).

Email	Имя	Фамилия	Организация	Роль	Время создания	Управление
test-user@example.com	Test	User	тестовая	Пользователь	16.02.2026, 15:40:14	✎ ✖ 👤
test-analyst@example.com	Test	Analyst	тестовая	Аналитик	16.02.2026, 15:39:26	✎ ✖ 👤
test-admin@example.com	Test	Admin	тестовая	Администратор	16.02.2026, 15:38:27	✎ ✖ 👤
testuserqa7@gmail.com			тестовая	Администратор	28.11.2025, 13:58:09	✎ ✖ 👤
testuserqajulia@gmail.com	qa	qa	тестовая	Администратор	22.10.2025, 19:24:59	✎ ✖ 👤

Рисунок 15 – Раздел «Пользователи»

Таблица содержит следующие поля:

- 1) Email;
- 2) Имя;
- 3) Фамилия;
- 4) Организация;
- 5) Роль;
- 6) Время создания;
- 7) 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.

Организация – содержит название организации.

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

В фильтре **Дата создания/Изменения** можно выбрать параметры фильтрации из списка, представленного на рисунке 16, либо нажав по иконке **Календарь**, ввести даты.

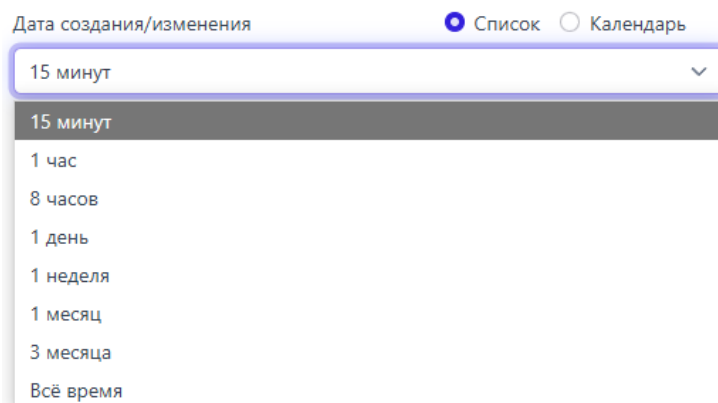


Рисунок 16 – Фильтрация по дате создания из списка

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



Рисунок 17 – Пагинатор

Ниже строки с фильтрами находится строка с элементами навигации в таблицах. В этой же строке находится элемент отображения количества найденных и показанных результатов

Найдено: 18, показано: с 1 по 10

Все элементы строки дублируются в нижней части окна программы, снизу от таблицы, для удобства просмотра и навигации. Описанные выше элементы навигации по информации на страницах являются универсальными и применяются на всех страницах. В некоторых таблицах может добавляться поле с кнопкой выбора элемента таблицы (содержит чекбокс ☐).

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



Изменение параметров учетных записей пользователей

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

При нажатии кнопки **Редактировать пользователя** открывается окно, в котором можно изменить имя и фамилию пользователя, адрес электронной почты, роль выбранного пользователя, организацию, которой принадлежит пользователь, а также изменить описание учетной записи (рис. 18).

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 18 – 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. 19).

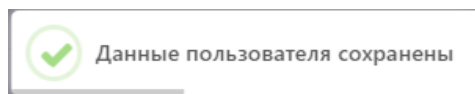


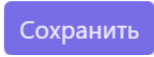
Рисунок 19 – Сообщение о сохранении данных пользователя

При нажатии кнопки **Сменить пароль** открывается окно, представленное на рисунке 20. Пароль должен соответствовать параметрам, указанным в нижней части окна:

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

Изображение окна «Смена пароля пользователя». В окне есть поля для «Новый пароль» и «Повторите пароль», флажок «Запросить смену пароля при следующем входе», блок «Требования к паролю» с перечислением правил (длина, заглавные и строчные буквы) и кнопка «Сохранить».

Рисунок 20 – 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. 21). Для отмены удаления учетной записи необходимо нажать кнопку **Отмена** или закрыть окно.

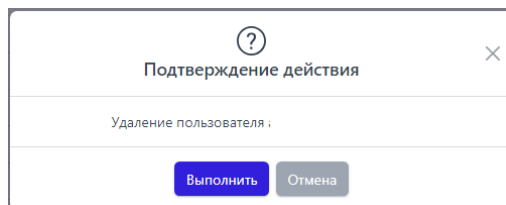


Рисунок 21 – Окно подтверждения удаления пользователя

После удаления учетной записи пользователя в нижней части основного окна программы появляется сообщение (рис. 22).

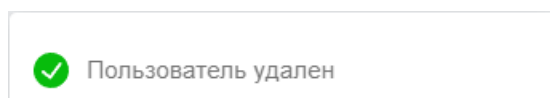


Рисунок 22 – Сообщение об удалении пользователя

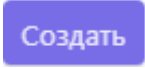
Создание учетной записи пользователя

В нижней части панели администрирования находится кнопка **Создать пользователя**. При нажатии кнопки открывается окно **Создать пользователя** (рис. 23).

Рисунок 23 – 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. 24). Такое же сообщение выводится во всех полях, требующих ввода информации.



Рисунок 24 – Сообщение о пустом поле ввода

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. 25).

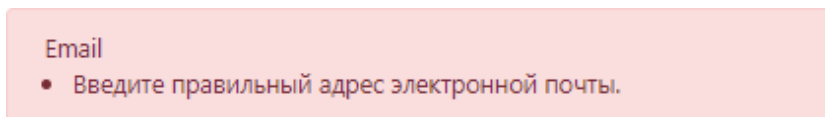


Рисунок 25 – Сообщение о неправильном адресе электронной почты

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. 26).

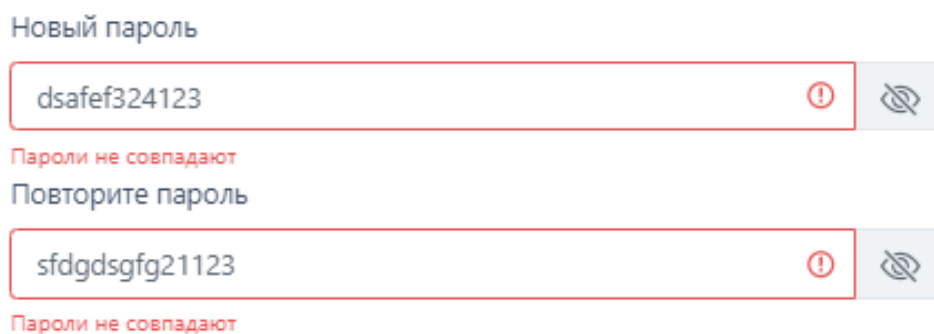


Рисунок 26 – Сообщение о несовпадении паролей

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. 27).

Организации

Название

Введите значение

Страна

Не задана

▼

Сектор

Не задан

▼

Автор / Пользователь

Не задан

▼

Признак активности

Не задано

▼

Дата создания / изменения

☒ Список

☐ Календарь

Всё время

▼

«

<

1

2

3

4

—

>

»

Показывать по 10

▼

Найдено: 71, показано с 1 по 10

☐	Название	Страна	Сектор	Количество обнаружений за месяц	Дата создания / Автор	Дата обновления / Пользователь	Управление
☒	test organization 1	Россия	Сельское хозяйство	0	16.02.2026, 15:41:40		
☒	тестовая 3			0	20.11.2025, 14:08:37	13.01.2026, 10:49:12 testuserqa@gmail.com	
☒	тестовая 2			0	20.11.2025, 14:07:23		
☒	тестовая 1			0	20.11.2025, 14:07:03		
☒	vip-test			0	16.11.2025, 18:36:37		
☒	ORG_testbud	Федеративные Штаты Микронезии	Сельское хозяйство	0	14.11.2025, 13:12:34	18.12.2025, 12:51:47	
☒	test3(ME)			0	23.10.2025, 16:51:23		
☒	test2(n_M)			0	23.10.2025, 16:50:43	23.10.2025, 16:51:02	
☒	test_1(n_M_E)			0	23.10.2025, 16:49:37	23.10.2025, 16:50:05	
☒	AlBerezin Test			0	14.10.2025, 13:20:55		

«

<

1

2

3

4

—

>

»

Показывать по 10

▼

Найдено: 71, показано с 1 по 10

Создать организацию

Удалить выбранные

Рисунок 27 – 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 предусмотрена следующая система фильтров:

- **Название**;
- **Страна**;

- Сектор;
- Автор/Пользователь;
- Признак активности;
- Дата создания/Изменения.

В полях для фильтрации **Страна**, **Сектор**, **Автор/Пользователи** предлагается выбрать из предзаполненных записей.

В поле **Дата создания/Изменения** можно указать параметры из списка, либо выбрать по календарю.

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

Название организации является активной ссылкой, при нажатии по которой ЛКМ происходит переход на страницу информации об организации, представленную на рисунке 28.

Рисунок 28 – Окно информации по выбранной организации

В окне редактирования имеются следующие области:

- Организация;
- Квоты;
- Клиенты.

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

В области **Организация** могут присутствовать следующие иконки:

—  — показывает, что организация является владельцем платформы (при наведении на данную иконку указателя мыши выводится соответствующее сообщение);

—  — показывает, что для токенов и пользователей данной организации доступ к разделам аналитики EDR разрешен.

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

При нажатии по иконке  можно скачать отчет по организации сгенерированный ИИ Агентом.

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 29).

Квоты

«

<

1

>

»

Показывать по: 10

Найдено: 1, показано с 1 по 1

☐	Путь до API	Квота в день / Использовано	Квота в месяц / Использовано	Дата создания / Автор	Дата обновления / Пользователь	Управление
☐	Получить набор коротких отчетов по Email	11 / 0	20 / 0	16.12.2024, 14:58:39 QAadmin@gmail.com		 

«

<

1

>

»

Показывать по: 10

Найдено: 1, показано с 1 по 1

Добавить квоту

Удалить выбранные

Рисунок 29 – 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;
- Управление ( – редактировать квоту,  – удалить квоту).

Для добавления новой квоты требуется нажать по иконке **Добавить квоту**, после чего откроется окно добавления информации для создания новой квоты (рисунок 30).

The screenshot shows a window titled "Добавить квоту" (Add Quota) with a close button (X) in the top right corner. Inside the window, there is a section for "API путь *" (API path) with a checkbox "Ввести путь вручную" (Enter path manually). Below this is a dropdown menu currently showing "Не выбрано" (Not selected). There is also a checkbox "Запрет вызова" (Prohibit call) which is currently unchecked. Below these are two input fields: "Максимальное количество вызовов API за день" (Maximum number of API calls per day) and "Максимальное количество вызовов API за месяц" (Maximum number of API calls per month). At the bottom, there are two checkboxes: "Без ограничений" (No restrictions) for both the daily and monthly call limits. A blue "Добавить" (Add) button is located at the bottom right of the window.

Рисунок 30 – 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.

При создании квоты и введении пути вручную можно ограничить как отдельный вызов API, так и группу вызовов, используя символ *.

Пример использования символа * при написании пути для создания квоты вызова представлен на рисунке 31.

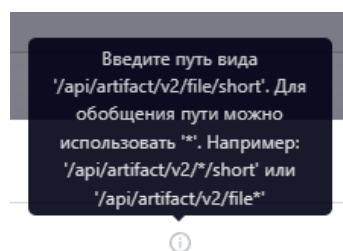


Рисунок 31 – Пример написания пути для создания квоты по API-вызову с использованием символа *

Данные пути можно взять из отдельного документа «Руководство по API RT Protect TI».

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 32.

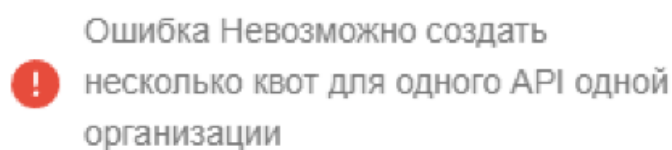


Рисунок 32 – Сообщение об ошибке при создании одинаковых квот

Для удаления выбранных кнопкой выбора квот требуется нажать по иконке  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», 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 Клиента и его значение (для его отображения необходимо нажать кнопку **Показать токен**).

Рядом с именем клиента находится иконка , при нажатии по которой открывается графическая область, показывающая активность запросов по данному клиенту (см. рисунок 33).

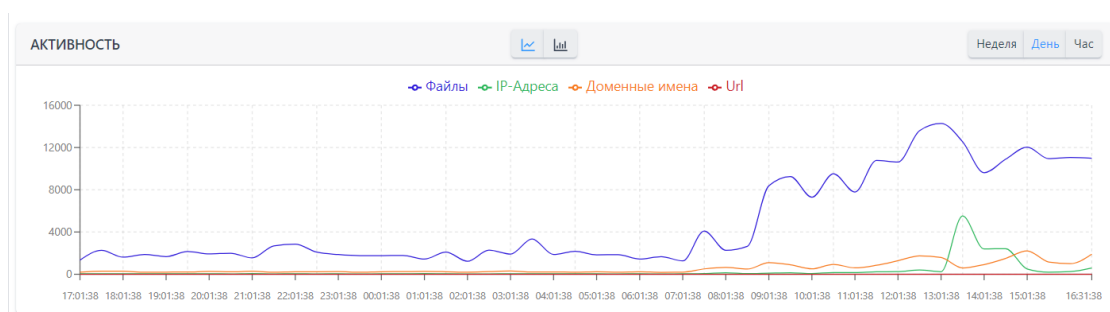


Рисунок 33 – Активность запросов по выбранному клиенту

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 .

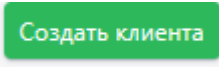
При проверке артефактов клиентом каждый артефакт будет фиксироваться в разделе «Активность» в качестве обнаружения на конкретном клиенте.



Примечание

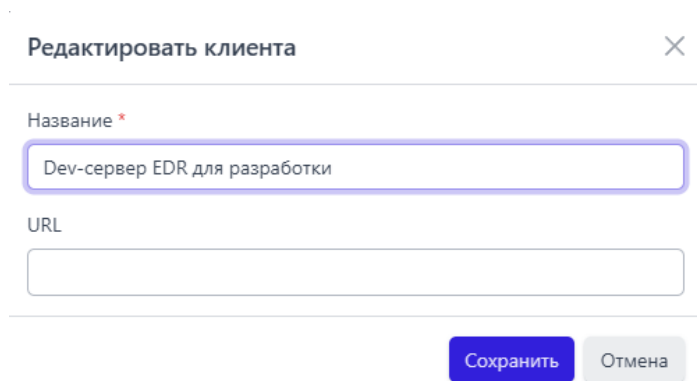
Токен представляет собой последовательность символов, передаваемую клиентом серверу при запросе, которая позволяет серверу однозначно идентифицировать инициатора запроса.

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

- удаление (иконка );
- редактирование (иконка );
- выпуск нового (иконка ).

При нажатии по иконке редактирования появляется окно редактирования, представленное на рисунке

34.



Редактировать клиента

Название *

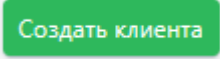
Dev-сервер EDR для разработки

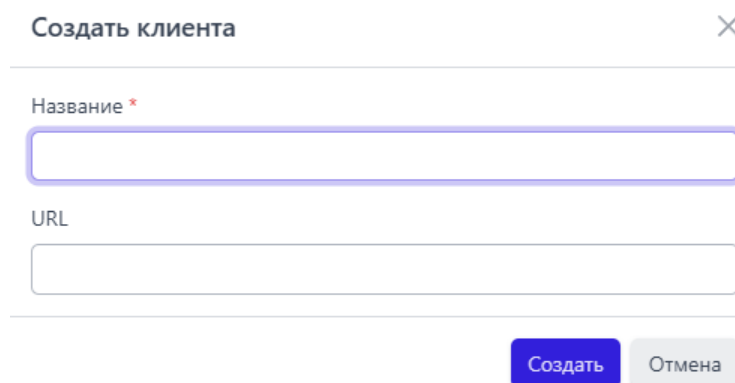
URL

Сохранить Отмена

Рисунок 34 – Окно редактирования

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

При нажатии по иконке  появляется окно, представленное на рисунке 35.



Создать клиента

Название *

URL

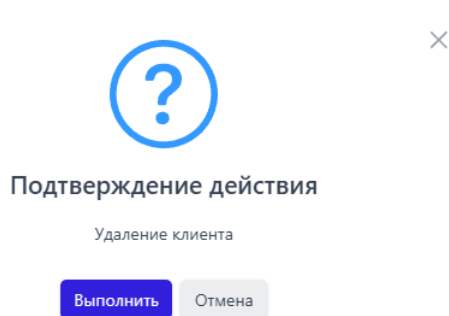
Создать Отмена

Рисунок 35 – Окно «Создать клиента»

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

Далее можно получить токен по кнопке «Показать токен», скопировать его и использовать для настройки подключаемого к TI-платформе клиента.

Для удаления клиента требуется нажать по иконке , после чего появится окно подтверждения удаления, представленное на рисунке 36.



Подтверждение действия

Удаление клиента

Выполнить Отмена

Рисунок 36 – Окно подтверждения удаления клиента

В данном окне для подтверждения удаления клиента 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. 37).

Создать организацию

Название *

Контакты

Страна

Сектор

Описание

Сайт

☐ Признак организации, владеющей данным экземпляром платформы

☐ Доступ к разделам EDR для токенов и пользователей организации

Загрузить иконку организации

Создать

Рисунок 37 – 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).

При выставлении галочки напротив поля «Доступ к разделам EDR для токенов и пользователей организации» будет возможен доступ к аналитике EDR.

После заполнения всех полей требуется нажать по иконке **Создать**, после чего будет выведено короткое сообщение (рис. 38), и информация о новой организации будет отображаться в таблице.



Рисунок 38 – Сообщение о создании организации

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

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

Для подтверждения действия по удалению организации требуется во всплывающем окне (рис. 39) нажать по иконке **Выполнить**.

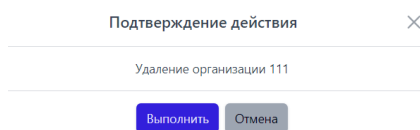


Рисунок 39 – Подтверждение удаления организации

Для редактирования информации по организации в столбце **Управление** требуется нажать по иконке  , после чего появится окно редактирования информации, представленное на рисунке 40.

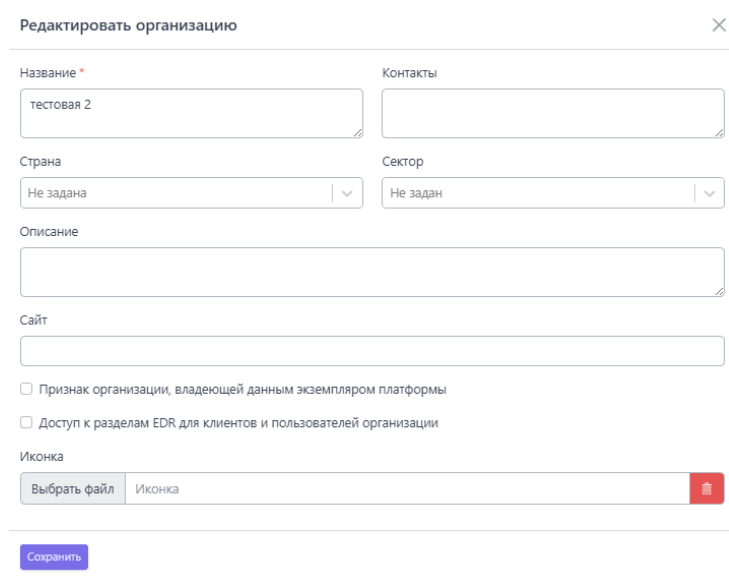
 Форма с заголовком "Редактировать организацию" и кнопкой закрытия "X". Поля для ввода: "Название *" (с текстом "тестовая 2"), "Контакты", "Страна" (с выпадающим списком "Не задана"), "Сектор" (с выпадающим списком "Не задан"), "Описание", "Сайт". Два чекбокса: "Признак организации, владеющей данным экземпляром платформы" и "Доступ к разделам EDR для клиентов и пользователей организации". Раздел "Иконка" с кнопками "Выбрать файл" и "Иконка" (красная с иконкой). Внизу кнопка "Сохранить".

Рисунок 40 – 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.

Подключена интеграция с такими источниками данных как PT-Feeds provider и FinCert.

Реализован механизм передачи ленты новостей из одного TI в другой (через stix-фид).

На TI один раз в неделю формируется фид в формате STIX, содержащий в себе перечень обогащенных через ИИ отчетов об угрозах и все имеющиеся угрозы и злоумышленники. Помимо самих сущностей, фид включает в себя все связи выгружаемых артефактов с артефактами и другими сущностями.

Загрузка фидов доступна по фиксированной ссылке <https://ti-dev.rt-protect.ru/api/Export/download/reports>. Для загрузки необходимо передать токен клиента в соответствующем заголовке HTTP-запроса.

Общий вид окна раздела **Источники данных** представлен на рисунке 41.

Источники данных

Сбросить фильтры

Название

Введите значение

Настроить

Класс артефакта

Не задан

Выбор

Дополнительно

Теги

Не заданы

Выбор

Дополнительно

Приоритет (не менее)

Не задан

Выбор

Дополнительно

Статус

Не задано

Выбор

Дата создания / изменения

Всё время

Выбор

Список

Календарь

Типы источников

Не задан

Выбор

Дополнительно

Автор / Пользователь

Не задан

Выбор

Показывать по

10

Выбор

Найдено: 170, показано с 81 по 90

☐	Название ↑	Обнаружений за месяц ↑	Элементов ↑	Актуальных ↑	STIX	Статус	Приоритет ↑	Дата создания / Автор ↑	Последнее изменение / Пользователь	Управление
☐	Habr BIZONE Articles	0	20	20	0			18.09.2025, 17:33:06 Создан автоматически	Создан автоматически	
☐	K7 SECURITY Labs	0	22	22	0			18.09.2025, 17:33:06 Создан автоматически	Создан автоматически	
☐	CYFIRMA Research	0	243	243	21			18.09.2025, 17:33:06 Создан автоматически	Создан автоматически	
☐	Proofpoint Blog	2	56	56	14			18.09.2025, 17:33:06 Создан автоматически	Создан автоматически	
☐	We Live Security	0	111	111	20			18.09.2025, 17:33:06 Создан автоматически	Создан автоматически	
☐	SECURELIST	41	581	581	8			18.09.2025, 17:33:06 Создан автоматически	Создан автоматически	
☐	SentinelOne Blog	0	39	39	5			18.09.2025, 17:33:06 Создан автоматически	Создан автоматически	
☐	Cyber Blog	1	212	212	24			18.09.2025, 17:33:06 Создан автоматически	Создан автоматически	
☐	Unit 42 Threat Research	3	627	627	17			18.09.2025, 17:33:06 Создан автоматически	Создан автоматически	
☐	Blog Malware Bytes	0	207	207	78			18.09.2025, 17:33:06 Создан автоматически	Создан автоматически	

Показывать по

10

Выбор

Найдено: 170, показано с 81 по 90

Добавить источник

Делиться

Печать

Аналитика источников

Рисунок 41 – Окно раздела «Источники данных»

Таблица имеет следующие поля:

- Кнопка выбора;
- **Название** (отображается название источника данных);
- **Обнаружений за месяц**;
- **Элементов**;
- **Актуальных**;
- **STIX**;
- **Статус** (отображается информация о статусе обновления базы);
- **Приоритет** (минимальный, Низкий, Ниже среднего, Средний, Выше среднего, Высокий);
- **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 .

В столбце Статус может присутствовать иконка, показывающая количество нераспознанных артефактов , то есть артефактов в источнике данных, которые имеют некорректную информацию. Список таких артефактов можно просмотреть, перейдя на страницу источника данных и раскрыв область **Нераспознанные артефакты**.

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.

Импортировать источники можно, нажав по иконке . Функционал импорта/экспорта позволяет переносить список источников данных между различными экземплярами TI-платформы.

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** (безопасный, вредоносный, подозрительный);
- **Тэги** (ключевые слова, которые задаются при редактировании/добавлении источника и нужны для дополнительного удобства категорирования и классификации источников);
- **Приоритет (не менее)** (не задан, минимальный, низкий, ниже среднего, средний, выше среднего, высокий);
- **Статус** (синхронизация успешна, ошибка синхронизации);
- **Автор/Пользователь**;
- **Дата создания/Изменения** (Список/Календарь);
- **Тип источника** (JSON, CSV, STIX, Провайдер, Отчет, Любой формат).

Для Приоритет источника данных 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 42.

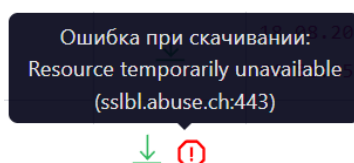


Рисунок 42 – Сообщение об ошибке при скачивании обновления источника

При нажатии по названию источника, например, [Abuse MalwareBazaar](#) откроется окно с информацией по источнику, представленное на рисунке 43.

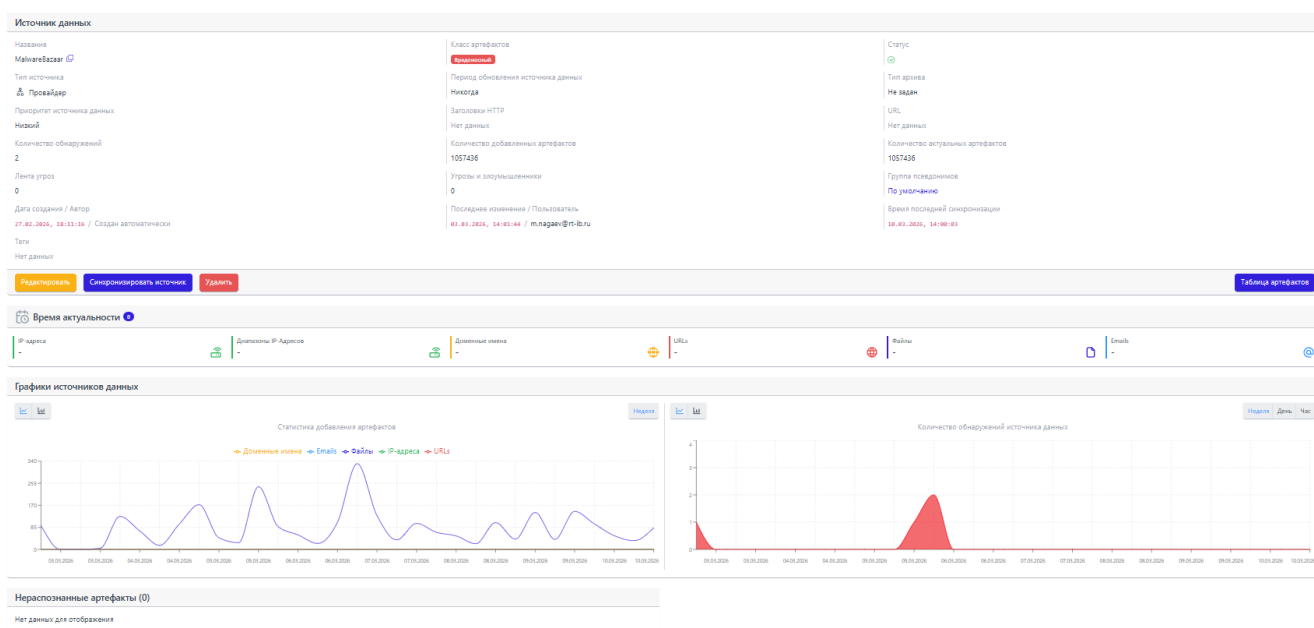


Рисунок 43 – Окно информации по источнику данных

В данном окне представлены следующие области:

- **Источник данных** (выводится информация о подключенном источнике);
- **Время актуальности** (выводится в днях время актуальности отчета по каждому артефакту из источника, а также, общее время актуальности отчета по всем источникам);
- **Графики источников данных** (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);
- **Нераспознанные артефакты.**

В области информации по источнику данных можно перейти по внешнему URL, из которого осуществляется загрузка источника данных.

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.

В поле информации о источнике данных имеются следующие иконки:

Редактировать

Синхронизировать источник

Удалить

Таблица артефактов

Редактировать

При нажатии по иконке **Редактировать** откроется окно, где можно редактировать информацию, относящуюся к настройке источника данных (см. рисунок 44).

Редактировать источник

Основные настройки

Имя *
MalwareBazaar

Приоритет источника данных *
Низкий

Группа псевдонимов
По умолчанию

Теги
Не задан

Класс артефактов *
Вредоносный

Время актуальности *
Общее время актуальности элемента источника данных *
0

IP-адреса
Введите значение

Диапазоны IP-Адресов
Введите значение

Доменные имена
Введите значение

URLs
Введите значение

Файлы
Введите значение

Emails
Введите значение

Сохранить

Рисунок 44 – Окно редактирования информации по источнику данных

В данном окне имеются вкладки с основными настройками и настройками парсинга JSON.

Синхронизировать источник

При нажатии по иконке **Синхронизировать источник** произойдет принудительная синхронизация источника данных подключенного к RT Protect TI с основным источником.

Таблица артефактов

При нажатии по иконке **Таблица артефактов** откроется страница, где в табличной форме отображается список артефактов, представленных в выбранном источнике данных (рисунок 45).

Артефакты

RST Cloud IP Feed

Артефакт

Введите значение

Дата обнаружения

начальная дата

→

конечная дата

Дата синхронизации

начальная дата

→

конечная дата

Актуальность

Не задана

Активация

Не задана

Теги

Не заданы

Надежность данных

Применить

Сбросить

Минимум 0

100 Максимум

Файлы

IP-адреса

Диапазоны IP-Адресов

Доменные имена

URLs

Emails

«

<

1

2

3

4

...

>

»

Показывать по: 50

Найдено: 4160853, показано с 1 по 50

☐	Артефакт	Надежность	Время обнаружения	Время последней синхронизации	Другие источники	Управление
☒	99.48.163.99	35	02.06.2026, 03:04:31	02.06.2026, 14:49:03		☒
☒	99.44.188.159	14	02.06.2026, 03:04:31	02.06.2026, 14:49:03	[DRAFT]ThreatView IP blocklist BlockListDe IP List Неактуальный	☒
☒	99.247.220.16	35	02.06.2026, 03:04:31	02.06.2026, 14:49:03		☒

✓

✕

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

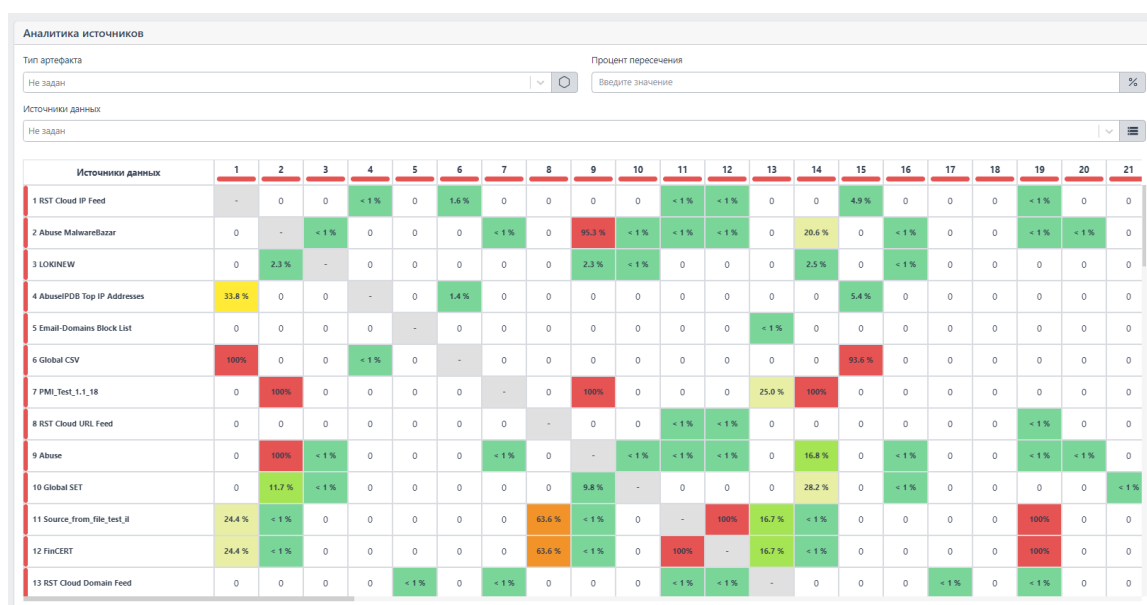
Над таблицей имеется система фильтров по различным параметрам.

— Фильтр с указанием надежности для всего источника.

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

В области **Управление** с помощью иконки  можно исключить из анализа отдельный артефакт из источника. Также в списке артефактов источника можно исключить/включить несколько артефактов из анализа с помощью иконок  / .

При нажатии на странице **Источники данных** по иконке  откроется страница, представленная на рисунке 46.



Аналитика источников

Тип артефакта: Не задан

Процент пересечения: Введите значение %

Источники данных: Не задан

Источники данных	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
1 RST Cloud IP Feed	-	0	0	< 1 %	0	1.6 %	0	0	0	0	< 1 %	< 1 %	0	0	4.9 %	0	0	0	< 1 %	0	0
2 Abuse MalwareBazar	0	-	< 1 %	0	0	0	< 1 %	0	95.3 %	< 1 %	< 1 %	< 1 %	0	20.6 %	0	< 1 %	0	0	< 1 %	< 1 %	0
3 LOKINNEW	0	2.3 %	-	0	0	0	0	0	2.3 %	< 1 %	0	0	0	2.5 %	0	< 1 %	0	0	0	0	0
4 AbuseIPDB Top IP Addresses	33.8 %	0	0	-	0	1.4 %	0	0	0	0	0	0	0	0	5.4 %	0	0	0	0	0	0
5 Email-Domains Block List	0	0	0	0	-	0	0	0	0	0	0	0	< 1 %	0	0	0	0	0	0	0	0
6 Global CSV	100 %	0	0	< 1 %	0	-	0	0	0	0	0	0	0	0	93.6 %	0	0	0	0	0	0
7 PMIL_Test_1.1_18	0	100 %	0	0	0	0	-	0	100 %	0	0	0	25.0 %	100 %	0	0	0	0	0	0	0
8 RST Cloud URL Feed	0	0	0	0	0	0	0	-	0	0	< 1 %	< 1 %	0	0	0	0	0	0	< 1 %	0	0
9 Abuse	0	100 %	< 1 %	0	0	0	< 1 %	0	-	< 1 %	< 1 %	< 1 %	0	16.8 %	0	< 1 %	0	0	< 1 %	< 1 %	0
10 Global SET	0	11.7 %	< 1 %	0	0	0	0	0	9.8 %	-	0	0	0	28.2 %	0	< 1 %	0	0	0	0	< 1 %
11 Source_from_file_test_II	24.4 %	< 1 %	0	0	0	0	0	63.6 %	< 1 %	0	-	100 %	16.7 %	< 1 %	0	0	0	0	100 %	0	0
12 FinCERT	24.4 %	< 1 %	0	0	0	0	0	63.6 %	< 1 %	0	100 %	-	16.7 %	< 1 %	0	0	0	0	100 %	0	0
13 RST Cloud Domain Feed	0	0	0	0	< 1 %	0	< 1 %	0	0	0	< 1 %	< 1 %	-	0	0	0	< 1 %	0	< 1 %	0	0

Рисунок 46 – Страница Аналитика источников

На данной странице в табличной форме представлена матрица пересечения источников данных, которая может быть использована аналитиком для понимания приоритетности источников данных. Таблица изменяется при применении фильтров, представленных выше таблицы.

В таблице показаны источники данных и процент пересечения данных, входящих в источники. Например, у источника данных в строке 7 (PMIL_Test_1.1_18) имеется 100% пересечение данных, входящих в источник 9 (Abuse).

При нажатии ЛКМ в поле с процентом пересечения открывается окно с подробной информацией по пересечению (рисунок 47).

Пересечения						
	Всего					
FinCert	246284	238879	4641	1543	1139	82
Test_PHISH_FEADS	495418	0	8200	487218	0	0
Пересечения	9	0	2	7	0	0
33.2% < 0.1% 66.79%						

Рисунок 47 – Информация по пересечению артефактов в источнике данных

Для добавления нового источника данных требуется нажать ЛКМ по иконке , после чего будет открыто окно добавления источника, представленное на рисунке 48.

Добавить источник

Основные настройки

Настройка парсинга (JSON)

Имя *

Введите значение

Приоритет источника данных *

Минимальный

Группа псевдонимов

Не задана

Теги

Не задан

Класс артефактов *

Безопасный

Время актуальности ⓘ *

Общее время актуальности элемента источника данных *

0

IP-адреса

Введите значение

Диапазоны IP-Адресов

Введите значение

Доменные имена

Введите значение

Веб-адреса

Введите значение

Файлы

Введите значение

Почтовые адреса

Введите значение

Тип источника *

JSON

Тип архива

Не задан

Источник

Выборить источник из загруженных

URL *

Введите значение

Период обновления источника данных *

Никогда

Проверка SSL-сертификата

Добавить заголовок HTTP

Ключ

Значение

+

Загрузить часть файла

Проверить настройки

Добавить

Рисунок 48 – Окно добавления источника данных

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

- 1) Основные настройки;
- 2) Настройки парсинга.

Имя источника.

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)**.

Тэги (ключевые слова для удобства категорирования и классификации).

Группа псевдонимов.

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.

Время актуальности в днях отчета по артефакту из источника (можно выставить общее время актуальности для источника, а также, время для каждого типа артефакта).

Тип источника (JSON, CSV, STIX, любой формат).

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

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.

В данном режиме работы можно выставить период обновления источника данных согласно следующих предустановленных параметров (никогда, час, 6 часов, 12 часов, день, 3 дня).

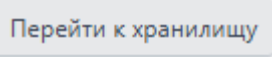
Для выбора источника данных из имеющихся загруженных источников следует сделать активной кнопку выбора **Выбрать источник из загруженных**, переведя ползунок кнопкой мыши вправо (рисунок 49), при этом становятся активны иконки  – Загрузить файл,  – Перейти к хранилищу.



Рисунок 49 – 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 50).

Хранилище источников			
« 1 » Показывать по: 50		Найдено: 9, показано с 1 по 9	
Название	Размер	Дата создания / Автор	Управление
test-kn-244.json	125 Б	18.01.2024, 13:08:19 rt@mail.ru	
file.csv	299.5 KB	12.12.2023, 16:30:44 test1@test.ru	
file_1.csv	268.15 KB	12.12.2023, 16:24:35 test1@test.ru	
file_1.csv	268.15 KB	12.12.2023, 16:19:09 test1@test.ru	
file.csv	299.5 KB	12.12.2023, 16:18:58 test1@test.ru	
test-kn-d.csv	96 Б	27.10.2023, 12:56:55 rt@mail.ru	
1.csv	134 Б	27.10.2023, 12:56:45 rt@mail.ru	
ProcessExplorer.zip	3.35 MB	13.10.2023, 16:08:38 rt@mail.ru	
Без названия (1).zip	126.16 MB	11.10.2023, 14:37:15 rt@mail.ru	
« 1 » Показывать по: 50		Найдено: 9, показано с 1 по 9	

Рисунок 50 – Страница «Хранилище источников»

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

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).

Тип источника – 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.

STIX (настройка парсинга невозможна).

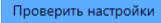
Любой формат:

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.

В поле «Добавить заголовок HTTP» 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.

Для проверки корректности настроек при добавлении источника имеется иконка  **Проверить настройки**.

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 источника имеет разные настройки и представлено на рисунках 51 - 53.

The screenshot shows the 'Добавить источник' (Add source) window with the 'Настройка парсинга (JSON)' (JSON parsing settings) tab selected. It includes a checkbox for 'JSONL - на каждой строке файла располагается JSON-объект' (JSONL - a JSON object is located on each line of the file). There are two input fields for paths: 'Путь до списка объектов с артефактами' (Path to the list of objects with artifacts) and 'Путь до артефактов в рамках элемента списка' (Path to artifacts within the list element). Below these is a section for 'Настройки дополнительных полей' (Additional field settings) with a dropdown and a 'Путь' (Path) input field, accompanied by a green '+' button. At the bottom are three buttons: 'Загрузить часть файла' (Load part of the file), 'Проверить настройки' (Check settings), and 'Добавить' (Add).

Рисунок 51 – Настройка парсинга файлов в формате JSON

The screenshot shows the 'Добавить источник' (Add source) window with the 'Настройка парсинга (CSV)' (CSV parsing settings) tab selected. It features a text input field for 'Порядковый номер колонки, в которой содержится артефакт' (Sequential column number where the artifact is located), with the value '0' entered. Below is the 'Настройки дополнительных полей' (Additional field settings) section with a dropdown and a 'Номер колонки' (Column number) input field, with a green '+' button. The bottom buttons are 'Загрузить часть файла' (Load part of the file), 'Проверить настройки' (Check settings), and 'Добавить' (Add).

Рисунок 52 – Настройка парсинга файлов в формате CSV

The screenshot shows the 'Добавить источник' (Add source) window with the 'Настройка парсинга (Любой формат)' (Any format parsing settings) tab selected. It includes a text input field for 'Регулярное выражение для разбора каждого элемента' (Regular expression for parsing each element). Below are two input fields: 'Символ разделения между элементами' (Separator symbol between elements) and 'Номер группы, содержащий артефакт' (Group number containing the artifact), with the value '0' entered. The 'Настройки дополнительных полей' (Additional field settings) section has a dropdown and a 'Номер группы' (Group number) input field, with a green '+' button. The bottom buttons are 'Загрузить часть файла' (Load part of the file), 'Проверить настройки' (Check settings), and 'Добавить' (Add).

Рисунок 53 – 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**.

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 54.

Рисунок 54 – Сообщение об ошибках при добавлении/редактировании информации об источнике

При нажатии по иконке **Загрузить часть файла** в отдельном окне ниже данной иконки будет показана часть файла, предоставленного источником данных (рисунок 55).

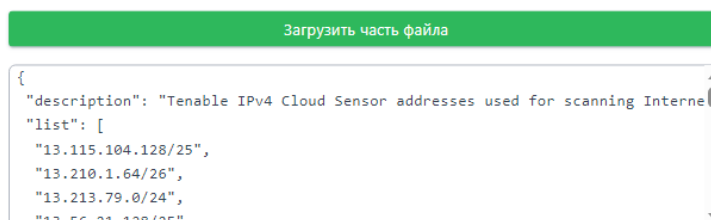


Рисунок 55 – Часть файла, предоставленного источником данных

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 56).

Note

Recent datasets ("recent additions") include hashes for the last 48 hours and are being generated every **5 minutes**. Please do not fetch them more often than that. **Full** data dumps include all hashes and are only being generated once per hour. Please do not fetch them more often than once per hour.

CSV files

The following data exports exists in CSV format:

- Recent additions ( [download](#))
- Full data dump ( [download](#) - zip compressed)

Рисунок 56 – 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 **Имя**, 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.

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.

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", "vtpersent", "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.

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 57).

Артефакт	366C3E4F90B97F849AE44A2D0F6C6D78B9DAB71582E3FBECA225180B39D589B3	Артефакт	04EE06F5A05400D75674FAE38ED7D2938468D096CEE29F2C896AA8C610FBE5BC
Время детектирования	14.03.2024, 11:47:48	Время детектирования	14.03.2024, 11:47:48
Надежность данных (от 0 до 100)	100	Надежность данных (от 0 до 100)	100
detectDate	2024-03-14 07:30:21	detectDate	2024-03-14 07:28:36
Имя файла	[External] Purchase Order from Telkomsel.exe	Имя файла	file

Рисунок 57 – 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 сразу после сохранения.

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 58.

Теги							
Группы тегов		Группы псевдонимов		Сбросить фильтры			
Название		Автор / Пользователь		Дата создания / изменения			
Введите значение		Не задан		Список Календарь			
Показывать по 50		Найдено: 3, показано с 1 по 3					
☐	Название	Префикс	Описание	Количество	Дата создания / Автор	Дата изменения / Автор	Управление
☐	Fraud	fraud	Fraud	7	17.02.2025, 17:57:43		
☐	Malware type	malware_type	Malware type	48	17.02.2025, 17:48:52		
☐	Network activity	network_activity	Network activity	18	17.02.2025, 17:55:08		
Показывать по 50		Найдено: 3, показано с 1 по 3					
Создать группу тегов		Удалить выбранные					

Рисунок 58 – 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 следующих фильтров:

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

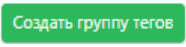
Таблица с полями для выбранной вкладки (вкладка помечена серым цветом), например, **Группы тегов** представлена полями согласно следующему списку:

- 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 .

Важно, что при удалении группы тегов следует предварительно удалить все сущности из группы.

Для создания новой группы тегов требуется нажать по иконке , после чего откроется окно создания группы тегов, представленное на рисунке 59.

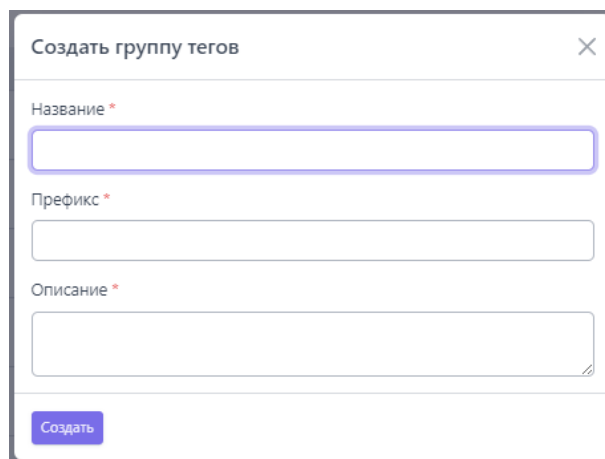


Рисунок 59 – Окно создания группы тегов

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.

Префикс – это идентификатор внутри группы тегов.

Например: `malware_type:adware`.

Для редактирования группы тегов следует в области **Управление** нажать по иконке , после чего появится окно редактирования группы, представленное на рисунке 60.

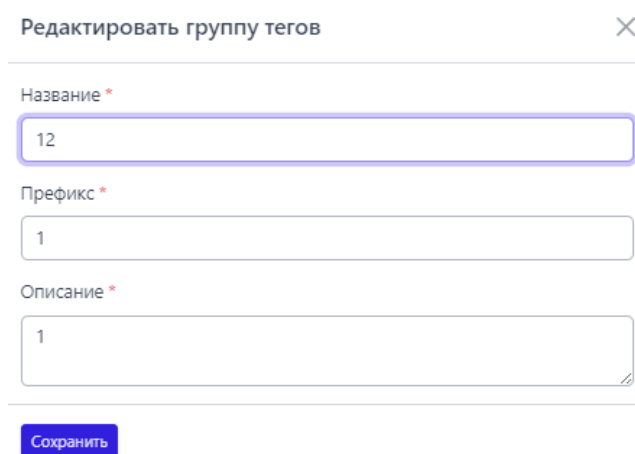


Рисунок 60 – Окно редактирования группы тегов

Название группы тегов на странице **Теги** вкладки **Группы тегов** является активной ссылкой, при нажатии по которой открывается окно с тегами данной группы (рисунок 61).

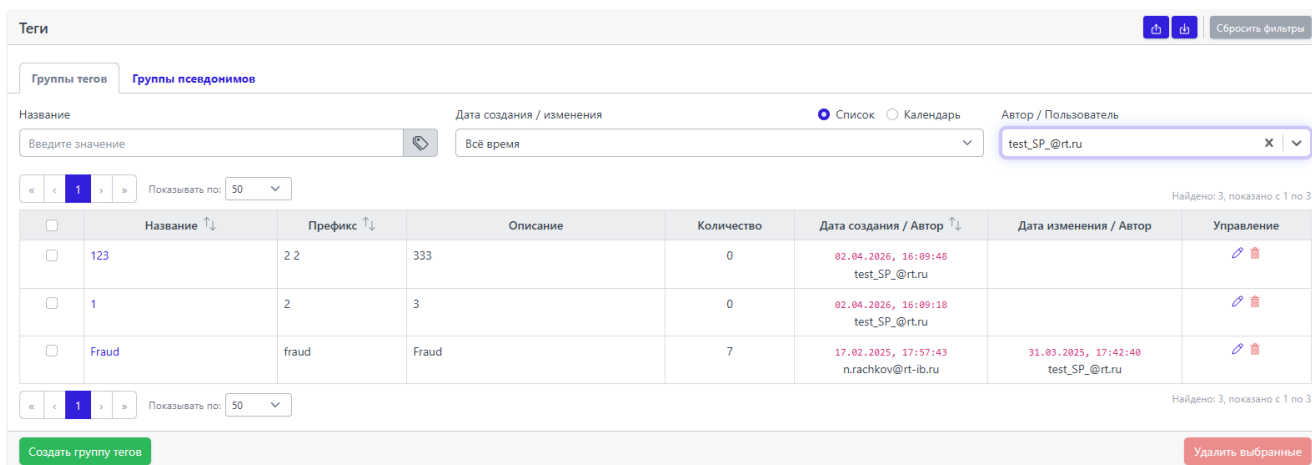


Рисунок 61 – Окно Теги в группе тегов

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

- Кнопка выбора ☐;
- Название;
- Префикс;
- Описание;
- Количество;
- Дата создания/Автор;
- Дата изменения/Автор;
- Управление (редактировать тег , удалить тег).

Фильтрация на странице **Теги** в выбранной группе осуществляется с помощью следующих фильтров:

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

Для редактирования тега следует в области **Управление** нажать по иконке , после чего появится окно редактирования тега, представленное на рисунке 62.

Редактировать тег

Название *

test_qa

Группа тегов *

test_qa

Описание *

test

Цвет *

Сохранить

Рисунок 62 – Окно редактирования информации о теге

Для создания нового тега в данной группе следует нажать по иконке , после чего откроется окно создания тега, представленное на рисунке 63.

Создать тег

Название *

Описание *

Цвет *

Создать

Рисунок 63 – 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 64.

Теги

Группы тегов

Группы псевдонимов

Название

Введите значение

Дата создания / изменения

Всё время

Список

Календарь

Автор / Пользователь

Не задан

«

1

2

3

4

...

»

Показывать по: 10

Найдено: 52, показано с 1 по 10

☐	Название	Описание	Количество	Дата создания / Автор	Дата изменения / Автор	Управление
☐	ndfgn	dfgnnq	0	28.01.2026, 11:30:00 test@test.ru		
☐	hfsf	hsdfh	0	28.01.2026, 11:29:57 test@test.ru		
☐	dsfbsdf	bsdf	0	28.01.2026, 11:29:55 test@test.ru		
☐	qrgqg	hgh	0	28.01.2026, 11:29:53 test@test.ru		
☐	gnd	dgf	0	28.01.2026, 11:29:51 test@test.ru		

Рисунок 64 – Окно вкладки Группы псевдонимов

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

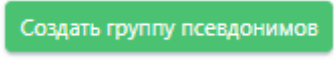
Таблица с полями для выбранной вкладки **Группы псевдонимов** представлена полями согласно следующему списку:

- 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**.

Следует отметить что для удаления группы псевдонимов следует предварительно удалить имеющиеся в группе сущности.

Для создания новой группы псевдонимов требуется нажать по иконке , после чего откроется окно создания группы, представленное на рисунке 65.

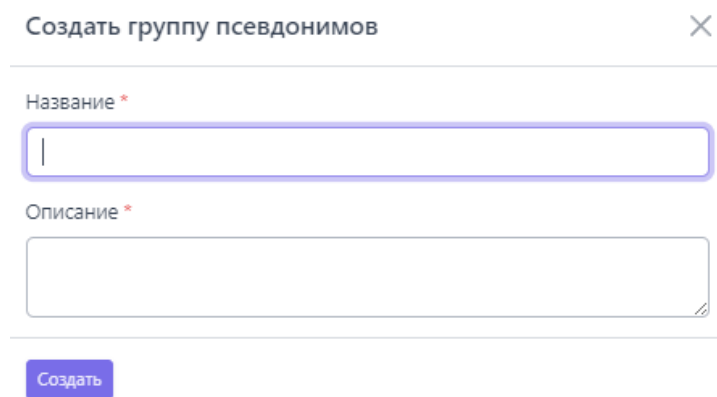


Рисунок 65 – Окно создания группы псевдонимов

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 66.

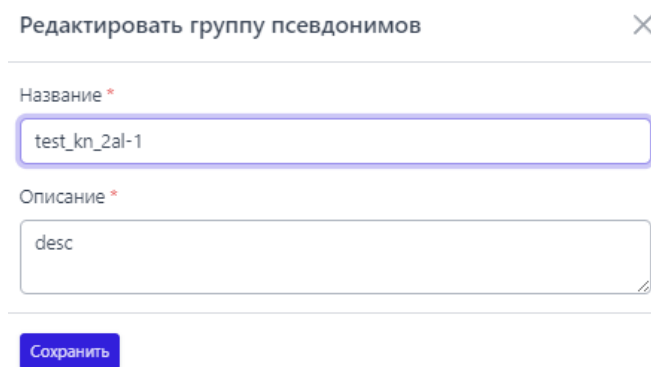


Рисунок 66 – Окно редактирования группы псевдонимов

Название группы псевдонимов на странице **Теги** вкладки **Группы псевдонимов** является активной ссылкой, при нажатии по которой открывается окно с псевдонимами данной группы (рисунок 67).

Рисунок 67 – Окно Псевдонимы в группе псевдонимов

Скриншот интерфейса "Псевдонимы" в RST Cloud. Вверху панель фильтров: "Псевдоним" (вводное поле), "Автор / Пользователь" (выпадающий список "Не задан"), "Дата создания / изменения" (выпадающий список "Всё время"). Справа кнопка "Сбросить фильтры".

В центре таблица с 6 столбцами: "Псевдоним", "Тег", "Дата создания / Автор", "Дата изменения / Автор", "Управление". В строках перечислены различные типы вредоносного ПО, такие как backdoor, badbot, badssl, banker, bootkit, bootloader, botnet, c2, clicker, cryptomining. Каждая строка имеет чекбокс в начале и иконки редактирования/удаления в конце.

Внизу панели: "Показывать по: 10" (выпадающий список), "Найдено: 10, показано с 1 по 10", кнопки "Создать псевдоним" и "Удалить выбранные".

Рисунок 67 – 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 ).

Фильтрация на странице **Псевдонимы** в выбранной группе осуществляется с помощью следующих фильтров:

- Псевдонимы;
- Автор/Пользователь;
- Дата создания/Изменения.

Для редактирования псевдонима следует в области **Управление** нажать по иконке , после чего появится окно редактирования псевдонима, представленное на рисунке 68.

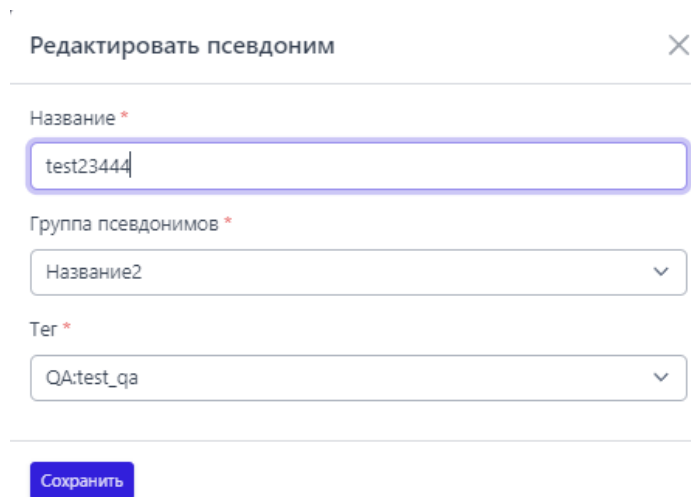


Рисунок 68 – Окно редактирования информации о псевдониме

Для создания нового тега в данной группе следует нажать по иконке , после чего откроется окно создания псевдонима, представленное на рисунке 69.

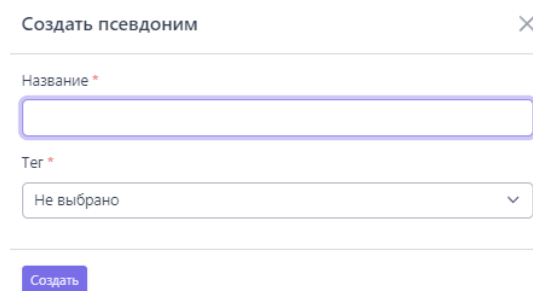


Рисунок 69 – Окно создания псевдонима

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 об 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, и в том числе известных и неизвестных АPT-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) **Анализаторы**;
- 4) **Граф связей**;
- 5) **Yara-правила**;
- 6) **Распространяемая аналитика**;
- 7) **Угрозы и злоумышленники**;
- 8) **Вредоносное ПО**;
- 9) **Инструменты**;
- 10) **Матрица MitreATT&CK**;
- 11) **Лента угроз**;
- 12) **Уязвимости**.

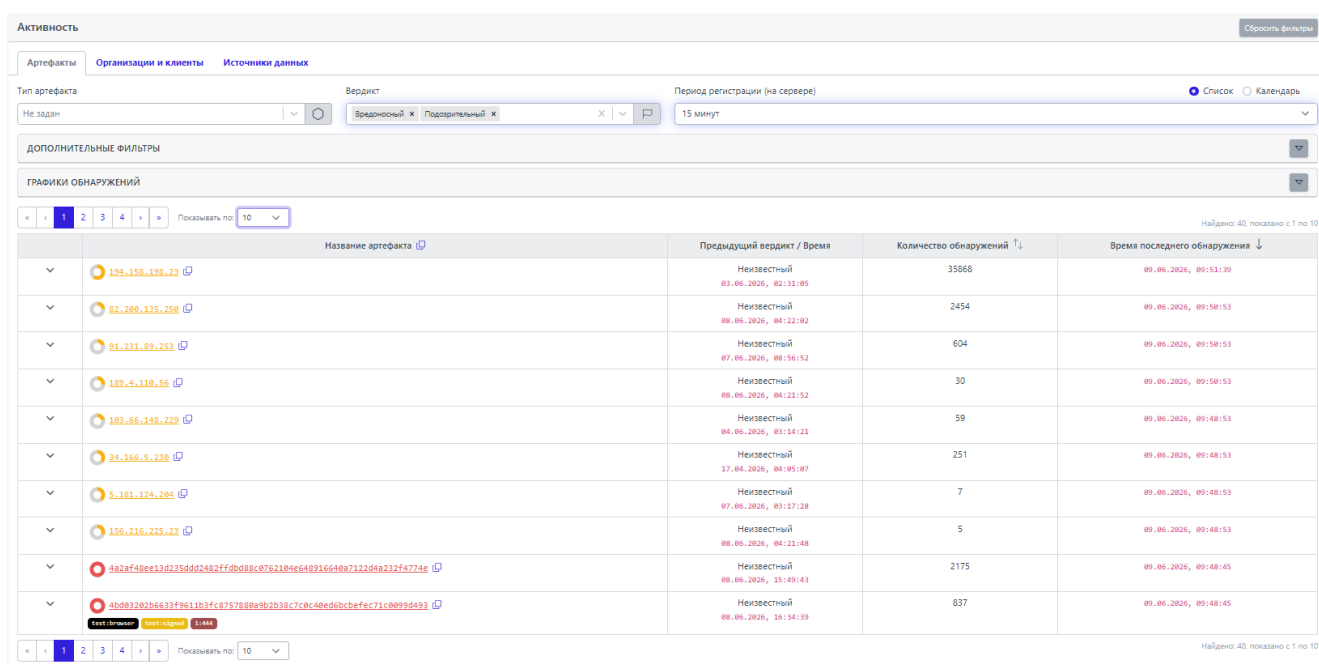
6.5.1. Активность

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 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 70 - 72.



Название артефакта	Предварительный вердикт / Время	Количество обнаружений	Время последнего обнаружения
194.156.136.23	Неизвестный 03.06.2026, 02:31:05	35868	09.06.2026, 09:51:39
82.200.135.258	Неизвестный 08.06.2026, 04:22:02	2454	09.06.2026, 09:58:53
91.231.89.253	Неизвестный 07.06.2026, 08:56:52	604	09.06.2026, 09:58:53
182.4.110.56	Неизвестный 08.06.2026, 04:21:52	30	09.06.2026, 09:58:53
103.66.149.229	Неизвестный 04.06.2026, 03:14:21	59	09.06.2026, 09:48:53
24.166.5.238	Неизвестный 17.04.2026, 04:05:07	251	09.06.2026, 09:48:53
5.181.124.296	Неизвестный 07.06.2026, 03:17:28	7	09.06.2026, 09:48:53
156.216.225.23	Неизвестный 08.06.2026, 04:21:48	5	09.06.2026, 09:48:53
4a2af48ee13d235dd2482f7fbd88c0762104e648916648a7123d4a232f4774e	Неизвестный 08.06.2026, 15:49:43	2175	09.06.2026, 09:48:45
4bd03202b633f9611b3fc8757880a9b2b38c7c8c48ed5bcbefec71c0999d493	Неизвестный 08.06.2026, 16:34:39	837	09.06.2026, 09:48:45

Рисунок 70 – Страница Активность вкладка Артефакты

Активность

Артефакты Организация и клиенты **Источники данных**

Тип артефакта: Не задан Вердикт: Любопытный, Подозрительный Период регистрации (на сервере): 15 минут Список Календарь

ДОПОЛНИТЕЛЬНЫЕ ФИЛЬТРЫ

Источники данных: ☐ Включить режим агрегации

На заданы

ПАНЕЛИ ОБОЗНАЧЕНИЙ

Название артефакта Предыдущий вердикт / Время Количество обнаружений Время последнего обнаружения

104.118.108.23 FinCert	Неизвестный	2877	09.06.2025, 09:52:39
91.231.89.253 RST Cloud IP Feed	Неизвестный	604	09.06.2025, 09:50:53
91.231.89.253 Cinc Score Black IP List	Неизвестный	604	09.06.2025, 09:50:53
91.231.89.253 [DRAFT]ThreatView IP blacklist	Неизвестный	604	09.06.2025, 09:50:53
92.209.135.259 RST Cloud IP Feed	Неизвестный	2452	09.06.2025, 09:50:53
92.209.135.259 Cinc Score Black IP List	Неизвестный	2451	09.06.2025, 09:50:53
92.209.135.259 [DRAFT]ThreatView IP blacklist	Неизвестный	2451	09.06.2025, 09:50:53
109.4.148.56 RST Cloud IP Feed	Неизвестный	30	09.06.2025, 09:50:53
109.4.148.56 Cinc Score Black IP List	Неизвестный	30	09.06.2025, 09:50:53
109.4.148.56 [DRAFT]ThreatView IP blacklist	Неизвестный	23	09.06.2025, 09:50:53

Рисунок 71 – Страница Активность вкладки Источники данных

Активность

Артефакты **Организация и клиенты** Источники данных

Тип артефакта: Не задан Вердикт: Любопытный, Подозрительный Период регистрации (на сервере): 15 минут Список Календарь

ДОПОЛНИТЕЛЬНЫЕ ФИЛЬТРЫ

Организация: Не задана Клиенты: Не заданы

ПАНЕЛИ ОБОЗНАЧЕНИЙ

Статистика обнаружений по клиентам Статистика обнаружений по организации

41 41

■ TMO - Артефакты (34) ■ IT - Информационная Безопасность (7)

■ TMO (DOR) (TMO - Артефакты) (34) ■ Тестовый сервер DOR (IT - Информационная Безопасность) (7)

Название артефакта	Предыдущий вердикт / Время	Количество обнаружений	Время последнего обнаружения
99.36.31.4 990 - информация (Тестовый сервер DOR)	Неизвестный	9	01.06.2025, 13:57:07
100.100.100.100 990 - информация (Тестовый сервер DOR)	Возвращено	2086	01.06.2025, 13:53:03
99.36.31.4 990 - информация (Тестовый сервер DOR)	Возвращено	25	01.06.2025, 13:53:03
100.100.100.100 990 - информация (Тестовый сервер DOR)	Возвращено	11	01.06.2025, 13:53:03
99.36.31.4 990 - информация (Тестовый сервер DOR)	Неизвестный	1	01.06.2025, 13:49:35
100.100.100.100 990 - информация (Тестовый сервер DOR)	Возвращено	212	01.06.2025, 13:49:35
99.36.31.4 IT - Информационная Безопасность (Тестовый сервер DOR)	Неизвестный	2176	09.06.2025, 07:50:08
100.100.100.100 IT - Информационная Безопасность (Тестовый сервер DOR)	Неизвестный	2206	09.06.2025, 07:50:08
99.36.31.4 990 - информация (Тестовый сервер DOR)	Неизвестный	1807	09.06.2025, 07:50:08
100.100.100.100 990 - информация (Тестовый сервер DOR)	Неизвестный	17	09.06.2025, 12:53:08

Рисунок 72 – Страница Активность вкладки Организация и клиенты

Таблица страницы Активность вкладки Артефакты имеет следующие поля:

- **Название артефакта** (в данном столбце в зависимости от типа артефакта отображается различная информация: контрольная сумма файла-угрозы в формате SHA-256, IP-адреса, доменные имена, URL);
- **Предыдущий вердикт/Время** (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:

— [630ae106a99ae7da5d8dd33e7704b27701f65](#) – вредоносный артефакт (шрифт красного цвета);

— [02f0c498bb4e5f62722ab5e8a63f5b3779db88ef](#) – безопасный артефакт (шрифт зеленого цвета);

— [B73753C4C69A03F9A3E09F121B6599D77B1A48E0247F9B71B56572555E1FE12B1](#) – неизвестный артефакт (шрифт серого цвета);

— [61F897ED69646E0509F6802F82D7C5E88C3E3B93C4CA86942E24D203AA878863](#) – подозрительный артефакт (шрифт оранжевого цвета).

86.25



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

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

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 73.

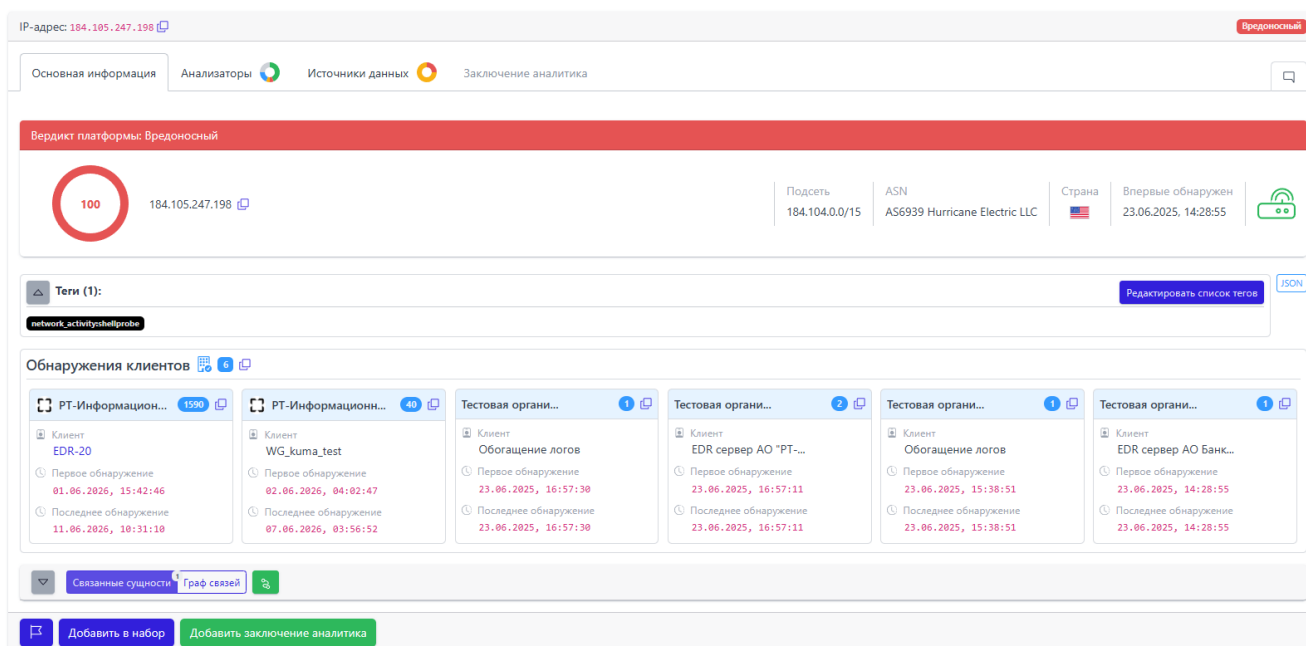


Рисунок 73 – Страница отчета сервиса по обнаруженной угрозе

Страница отчета программы об угрозе разделена на следующие области:

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

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

При наведении указателя мыши на иконку , рядом с названием вкладки, открывается окно показывающее статусы отчетов полученных для данного артефакта (рисунок 74).

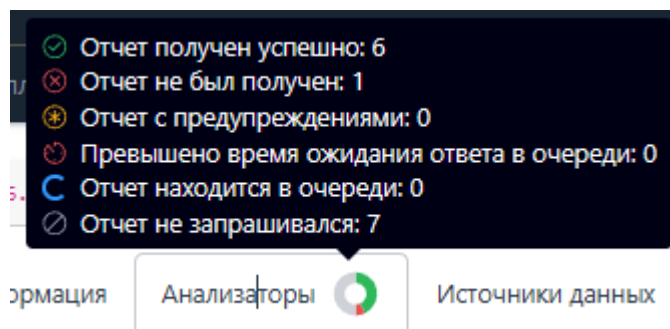


Рисунок 74 – Статусы отчетов по артефакту

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

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

В области названия вкладки **Источники данных** имеется иконка , при наведении на которую указателя мыши открывается окно с указанием вердиктов по артефакту полученных от источников данных (рисунок 75).

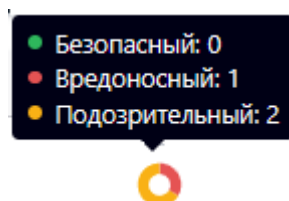
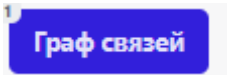


Рисунок 75 – Вердикты по артефакту

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

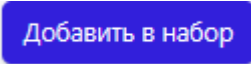
При нажатии по иконке  в поле **Связанные сущности** открывается таблица в которой показаны сущности связанные с рассматриваемым артефактом.

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

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

На странице отчета по артефакту имеется иконка для создания заявки на корректировку вердикта по

артефакту . После изменения вердикта и нажатия по кнопке «Добавить» заявка появится в разделе **Заключение аналитика** вкладки **Заявки** со статусом «Активна».

Вконка для добавления артефакта в набор .

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

В области вкладок отображается вкладка основной информации отчета ТИ-платформы, вкладки анализаторов и отчетов по артефакту от анализаторов.

В области **Источники данных** отображается отчет от источника данных по артефакту. Если запись отображается серым цветом, то анализ по артефакту в источниках данных не проводился.

Окно основной информации по результатам анализа артефакта в формате JSON представлено на рисунке 76.

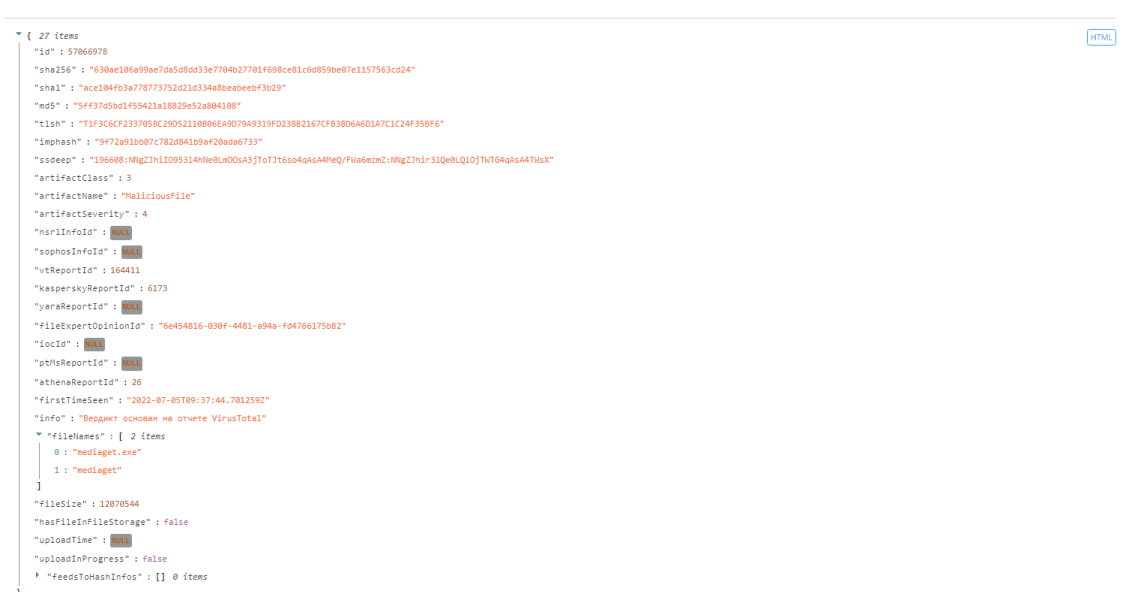
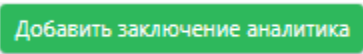
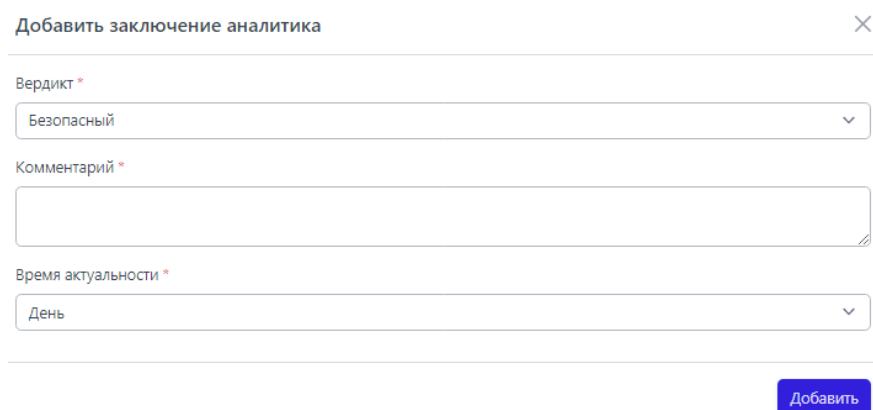


Рисунок 76 – Информация отчета об артефакте в формате JSON

В области **Обнаружения клиентов** показан список организаций, у которых обнаружен данный артефакт.

Для любого артефакта, хранящегося на TI-платформе, 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  появляется окно, в котором администратор/аналитик выносят вердикт по результатам анализа артефакта (рис. 77).



Добавить заключение аналитика

Вердикт *

Безопасный

Комментарий *

Время актуальности *

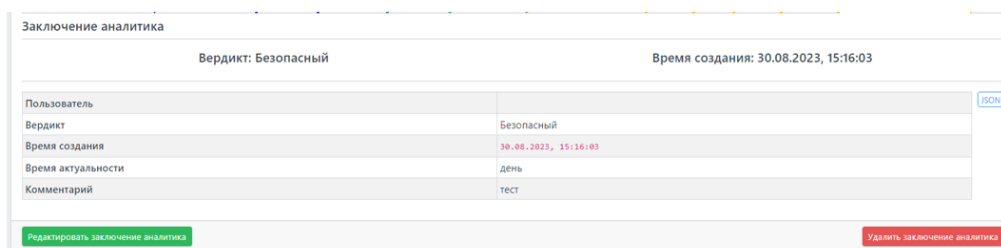
День

Добавить

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).



Заключение аналитика

Вердикт: Безопасный

Время создания: 30.08.2023, 15:16:03

Пользователь		JSON
Вердикт	Безопасный	
Время создания	30.08.2023, 15:16:03	
Время актуальности	день	
Комментарий	тест	

Редактировать заключение аналитика

Удалить заключение аналитика

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 отчета ТИ-платформы по обнаруженной угрозе требуется нажать по иконке  , после чего откроется поле добавления комментария, представленное на рисунке 79.

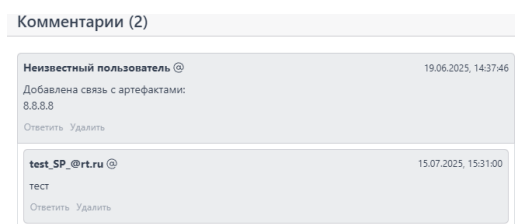
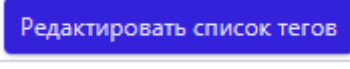


Рисунок 79 – Окно введения комментария

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 **Теги** 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**.

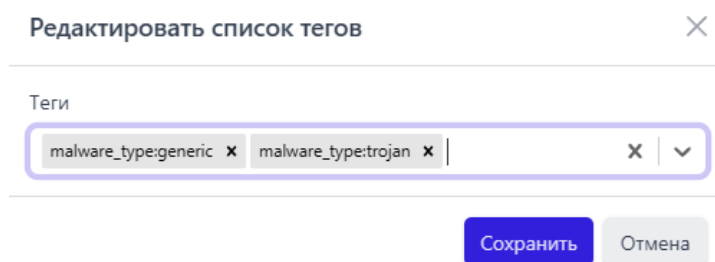


Рисунок 80 – Редактирование списка Тегов

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).

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

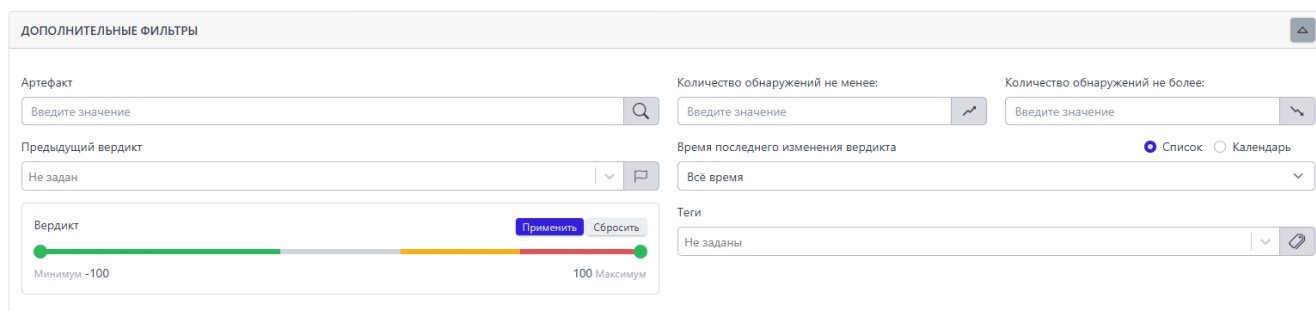


Рисунок 81 – Дополнительные фильтры на странице Активность/Артефакты

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**;

— **Вердикт**;

— **Теги**.

Фильтр по вердикту представлен в виде цветового фильтра с указанием числового значения для каждого из диапазонов оценки вредоносности артефакта. После указания диапазона, требуется нажать по иконке «Применить». При этом в таблице активности будут отображаться только те артефакты, вердикт по которым попадает в диапазон, выставленный в фильтре.

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

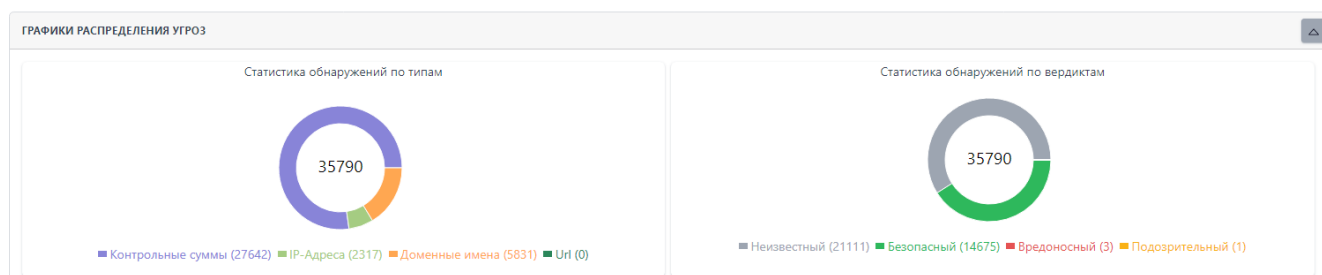


Рисунок 82 – Область графического отображения информации по обнаруженным угрозам вкладка «Артефакты»

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** на вкладке **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).

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 83).

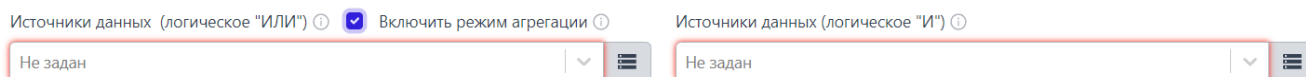


Рисунок 83 – Фильтр по источнику данных на странице Активность

Включение режима агрегации позволяет агрегировать артефакты, обнаруженные в разных источниках и искать пересечения между фидами при помощи исключающих и не исключающих условий.

То есть при указании нескольких источников данных в поле логическое «Или» будет осуществляться фильтрация артефактов по элементам, которые находятся в одном из выбранных источников.

При указании нескольких источников данных в поле логическое «И» будет осуществляться фильтрация артефактов по элементам, которые находятся в каждом из выбранных источников.

На странице **Активность** вкладки **Источники данных** имеется область с графическим отображением информации по обнаруженным угрозам (рисунок 84).

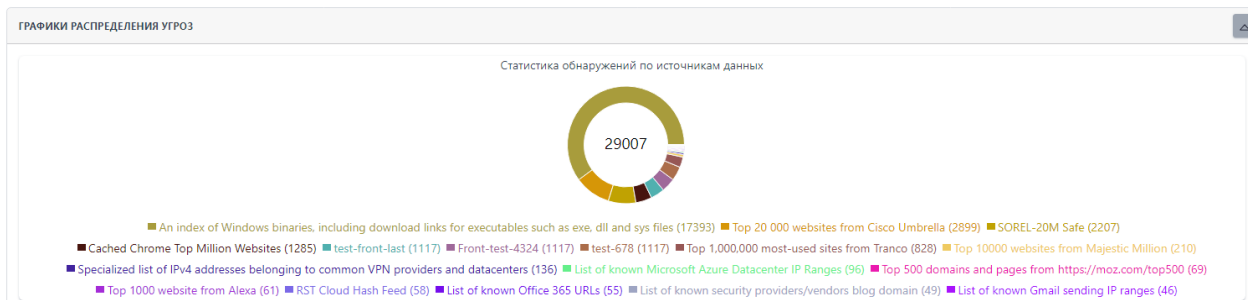


Рисунок 84 – Область графического отображения информации по обнаруженным угрозам вкладки Источники данных

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

- статистика обнаружений по источникам данных.

Для фильтрации информации на странице **Активность** вкладки **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);
- **Организация;**
- **Клиенты.**

На странице **Активность** вкладки **Организации и клиенты** имеется область с графическим отображением информации по обнаруженным угрозам (рисунок 85).



Рисунок 85 – Область графического отображения информации по обнаруженным угрозам вкладки 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. Заключение аналитика

Общие сведения

В разделе **Заключение аналитика** в табличной форме представлена информация о зарегистрированных на портале заключениях аналитика.

Заключение аналитика – это основополагающий вердикт об артефакте, который выносится аналитиком на основании анализа вердиктов, полученных от источников данных.

Проанализировав на странице **Активность** отчеты по проверке артефактов от различных вендоров, аналитик результирует общий вердикт по артефакту и, если требуется, выносит свой вердикт об опасности артефакта.

Также аналитик может поставить время актуальности, т.е. время, в течение которого вердикт по артефакту, указанный им, будет актуальным.

Общий вид страницы **Заключения аналитика** зависит от выбранной вкладки (подсвечена серым цветом).

Вкладка Заключение аналитика

Общий вид страницы **Заключения аналитика** вкладки **Заключения аналитика** представлен на рисунке 86.

Заклучения аналитика

Заклучения аналитика

Заявки

Артефакт

Введите значение

Тип артефакта

Не задан

Вердикт

Не задан

Время актуальности

Не задано

Комментарий

Введите значение

Актуальность

Не задано

Временной период

Список

Календарь

Всё время

Автор / Пользователь

Не задан

Найдено: 2100, показано с 1 по 10

Артефакт

Вердикт

Количество обнаружений

Комментарий

Время актуальности

Дата создания / Автор

Дата обновления / Пользователь

Действия

</

Рисунок 86 – Страница Заклучения аналитика

В таблице имеются следующие поля:

- Артефакт (в столбце отображается артефакт, для которого имеется заключение аналитика);
- Вердикт (в столбце отображается вердикт для артефакта);
- Количество обнаружений;
- Комментарий;
- Время актуальности (отображается время, показывающее, сколько будет актуален вердикт (заключение аналитика) по данному артефакту;
- Дата создания/Автор;
- Дата обновления/Пользователь;
- Действия (редактирование, удаление заключения аналитика).

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

- Артефакт;
- Тип артефакта (файл, ip-адрес, диапазон ip-адресов, доменное имя, URL, Email);
- Вердикт (не задано, безопасный, вредоносный, подозрительный);
- Время актуальности (не задано, день, неделя, месяц, три месяца, бесконечно);

- Комментарий;
- Актуальность.
- Временной период;
- Автор/пользователь;

86.25



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

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

- [630ae106a99ae7da5d8dd33e7704b27701f65](#) – 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 87.

Редактировать заключение аналитика

Артефакт *

Вердикт *

Комментарий *

Время актуальности *

Редактировать

Рисунок 87 – 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**.

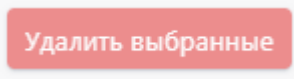
Для удаления заключения аналитика в столбце **Действия** требуется нажать по иконке , после чего появится окно, в котором следует подтвердить (либо отменить) действие удаления (рисунок 88).

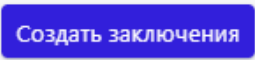
Подтверждение действия

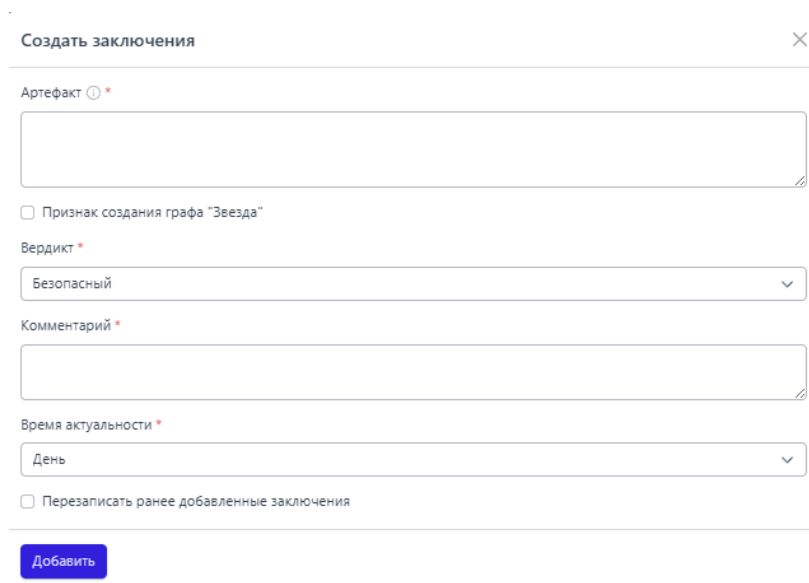
Удаление заключения аналитика

Выполнить Отмена

Рисунок 88 – 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 89.



Создать заключения

Артефакт *

☐ Признак создания графа "Звезда"

Вердикт *

Безопасный

Комментарий *

Время актуальности *

День

☐ Перезаписать ранее добавленные заключения

Добавить

Рисунок 89 – 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.

В поле артефакт можно указать диапазон ip-адресов в формате ipv4 либо ipv6.

При установке галочки в поле «Перезаписать ранее добавленные заключения», заключение, написанное в данный момент, изменится, если оно уже имелось для данного 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**.

Вкладка Заявки

На странице **Заключения аналитика** вкладка **Заявки** пользователь может принять или отклонить заявку на корректировку вердикта заключения аналитика по артефактам.

Общий вид страницы **Заключения аналитика** вкладки **Заявки** представлен на рисунке 90.

Заклучения аналитика

Заявки

Вердикт

Статус

Автор / Пользователь

Комментарий

Не задан

Не задан

Не задан

Введите значение

Артефакт

Временной период

Список Календарь

Введите значение

Всё время

<1234...>

Показывать по: 10

Найдено: 57, показано с 1 по 10

☐	Артефакт	Тип артефакта	Статус	Вердикт	Комментарий	Дата создания / Автор	Дата обновления / Пользователь	Действия
☐	13.85.16.224		Отклонена	Безопасный	01010101	06.08.2025, 10:17:41	06.08.2025, 10:18:41	
☐	sbr.ru		Одобрена	Подозрительный	test	01.08.2025, 17:57:44	06.08.2025, 17:35:14	
☐	sbr.ru		Активна	Подозрительный	для теста (удалить)	01.08.2025, 16:27:11		
☐	sbr.com		Активна	Подозрительный	для теста (удалить)	01.08.2025, 15:25:06		

Рисунок 90 – Страница Заклучения аналитика вкладка Заявки

Информация на странице представлена в виде таблицы со следующими полями:

- Кнопка выбора;
- Артефакт (отображается артефакт);
- Тип артефакта (с помощью иконок отображается тип артефакта;
- Статус (отображается статус заявки: Активна, Отклонена, Одобрена);
- Вердикт (отображается вердикт по артефакту);
- Комментарий (отображается комментарий);
- Дата создания/Автор (отображается дата создания заявки и ее автор);
- Дата обновления/Пользователь (отображается дата изменения заявки и пользователь, производивший изменения);
- Действия (отображается иконка для рассмотрения заявки).

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

- Вердикт;
- Статус;

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

Для артефактов со статусом заявки «Активна» в поле **Действие** пользователь может нажать по иконке



для того, чтобы рассмотреть заявку.

Окно рассмотрения заявки на корректировку вердикта по артефакту представлено на рисунке 91.

Заявка на корректировку вердикта

Артефакт *

cbr.com

Вердикт *

Подозрительный

Комментарий *

для теста (удалить)

Время актуальности *

День

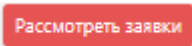
Принять

Отклонить

Рисунок 91 – Окно рассмотрения заявки на корректировку вердикта по артефакту

В данном окне пользователь может либо принять, либо отклонить заявку на корректировку вердикта.

После нажатия по соответствующей иконке статус заявки по артефакту в таблице изменится и в таблице заключения аналитика по данному артефакту будет выставлен вердикт, который указан в заявке, если заявка была принята, либо останется прежним, если заявка была отклонена.

Также действие по рассмотрению заявки можно выполнить, выбрав кнопкой выбора несколько активных заявок, и нажав по иконке .

6.5.3. Анализаторы

Общие сведения

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

Процедура создания анализаторов описывается в отдельном документе.

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

Провайдер RT Protect TI – это внешний программный модуль, который подключается к серверу TI по выделенному протоколу для передачи данных из внешних источников с целью расширения (обогащения) базы знаний TI. В качестве информации для обогащения могут выступать данные о вредоносности/безопасности артефактов, дополнительные сведения об артефактах, а также поддерживаемые в RT Protect TI объекты формата STIX.

Подробнее о формате STIX в официальной документации - <https://docs.oasis-open.org/cti/stix/v2.1/os/stix-v2.1-os.html>.

Для написания провайдеров доступен фреймворк, написанный на языке программирования Python (проект `ti_analyzer_python`).

Данный фреймворк позволяет разработчику провайдера абстрагироваться от деталей реализации протокола взаимодействия с TI и сосредоточиться только на разработке самой логики сбора артефактов из внешних источников.

Для авторизации провайдера в TI требуется также получить внутренний токен доступа, который выпускается единожды при разворачивании TI и устанавливается в его конфигурационном файле.

Имеются встроенные подключенные к сервису анализаторы и провайдеры. Так же пользователь может создавать собственные анализаторы и провайдеры. Процедура создания и подключения анализаторов и провайдеров описана в соответствующих руководствах.

Текущий список имен контейнеров анализаторов:

- 1) `static_analyzer`;
- 2) `vt_analyzer`;
- 3) `kaspersky_analyzer`;
- 4) `yara_analyzer`;

- 5) fuzzy_family_analyzer;
- 6) rst_cloud_analyzer;
- 7) netlas_analyzer;
- 8) pt_sandbox_analyzer;
- 9) meta_defender_analyzer;
- 10) geo_ip_analyzer;
- 11) abuse_ipdb_analyzer;
- 12) alien_vault_analyzer;
- 13) malshare_analyzer;
- 14) malware_bazaar_analyzer.

Текущий список имен контейнеров провайдеров:

- 1) fincert_provider;
- 2) pt_feeds_provider;
- 3) meta_defender_provider;
- 4) malware_bazaar_provider;
- 5) x_ti_provider.

Текущие списки поставляемых анализаторов и провайдеров постоянно обновляются.

Общий вид страницы **Анализаторы** зависит от вкладки, которая активна на данный момент. Страница **Анализаторы** вкладки **Активные интеграции** представлена на рисунке 92.

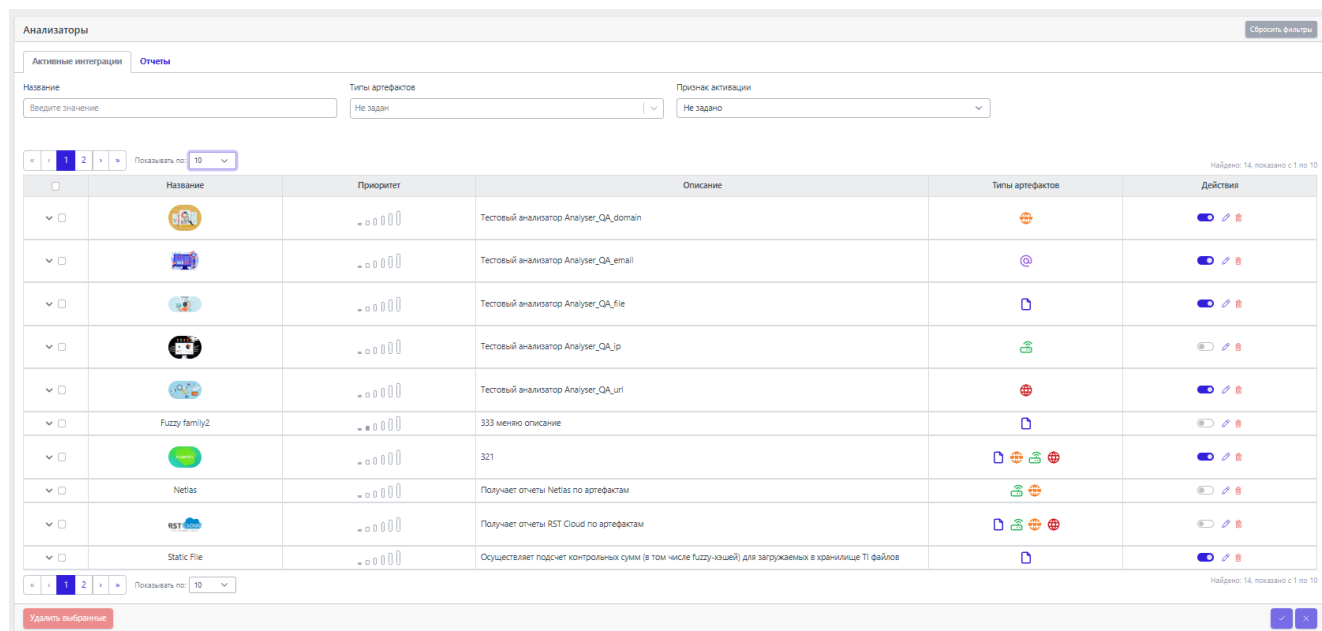


Рисунок 92 – Общий вид страницы Анализаторы вкладки Активные интеграции

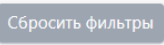
Информация на странице **Анализаторы** вкладки **Активные интеграции** представлена в виде таблицы со следующими полями:

- Иконка для раскрытия информации по анализатору ();
- Кнопка выбора (☐ / ☒);
- Название анализатора;
- Приоритет;
- Описание;
- Типы артефактов;
- Действия.

Для фильтрации информации на странице имеются следующие фильтры:

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

На странице **Анализаторы** имеются следующие иконки:

-  (при нажатии, сбрасываются выставленные фильтры на странице);
-  (после нажатия кнопки выбора напротив анализатора, происходит удаление выбранного анализатора);
-  /  (активирует/деактивирует выбранные анализаторы, т.е. делает анализ артефактов по данному анализаторам активным, или временно отключенным).

В поле «Типы артефактов» в виде иконок отображаются типы артефактов, проверяемые данным анализатором.

Имеются следующие типы артефактов:

-  (Email);
-  (Файл);
-  (Домен);
-  (IP адрес);
-  (URL).

В поле «Действия» с помощью иконок можно выполнить следующие действия:

-  (активировать/деактивировать анализ по выбранному анализатору);
-  (редактировать информацию по анализатору);
-  (удалить анализатор).

При выполнении действий по удалению анализатора, а также активации/деактивации анализатора, требуется подтвердить действие во всплывающих окнах, представленных на рисунках 93- 95.

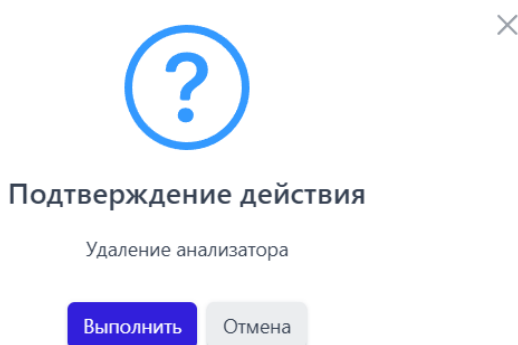


Рисунок 93 – Подтверждение действия удаления анализатора

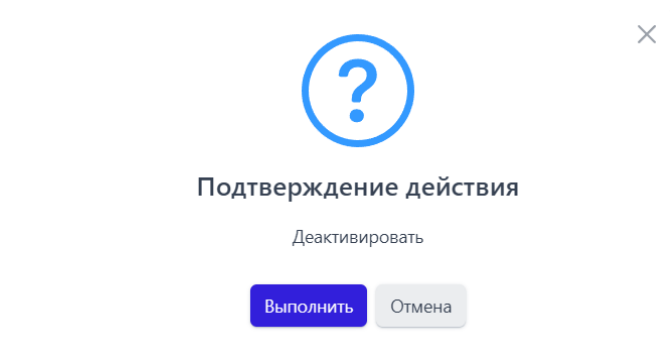


Рисунок 94 – Подтверждение действия деактивации анализатора

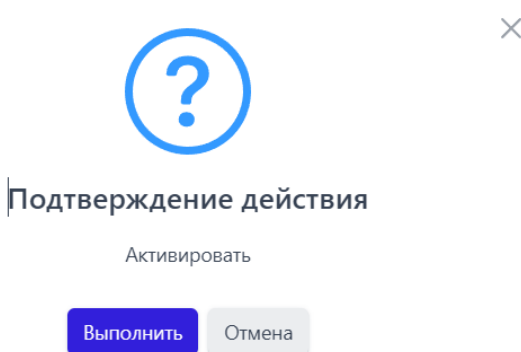


Рисунок 95 – Подтверждение действия активации анализатора

При нажатии по иконке редактирования анализатора открывается окно, представленное на рисунке

96.

Рисунок 96 – Окно редактирования информации по анализатору

В данном окне можно изменить следующие параметры работы анализатора:

- Название анализатора;
- Приоритет;
- Время актуальности получаемых отчетов в днях;
- Группу псевдонимов тегов;
- Описание анализатора;
- Загрузить или удалить иконку для анализатора;
- Автоматически запрашивать отчет по артефакту при открытии;
- Анализатор доступен только для организации владельца платформы.

После редактирования информации требуется нажать по иконке «Сохранить».

При нажатии по иконке, раскрывающей информацию по анализатору, открывается окно, представленное на рисунке 97.

☐	Название	Приоритет	Описание	Типы артефактов	Действия
^ ☐			Тестовый анализатор Analyser_QA_domain		☒  
Максимальное время анализа артефакта (в минутах)			3		
Для работы анализатора требуется загруженный файл			Нет		
Время актуальности получаемых отчетов (в днях)			1		
Автоматически запрашивать отчет по артефакту при открытии			Нет		
Название группы псевдонимов			По умолчанию		

Рисунок 97 – Информация по анализатору

На странице «Анализаторы» вкладки «Отчеты» в табличной форме представлена информация о проверенных анализаторами артефактах.

Общий вид страницы представлен на рисунке 98.

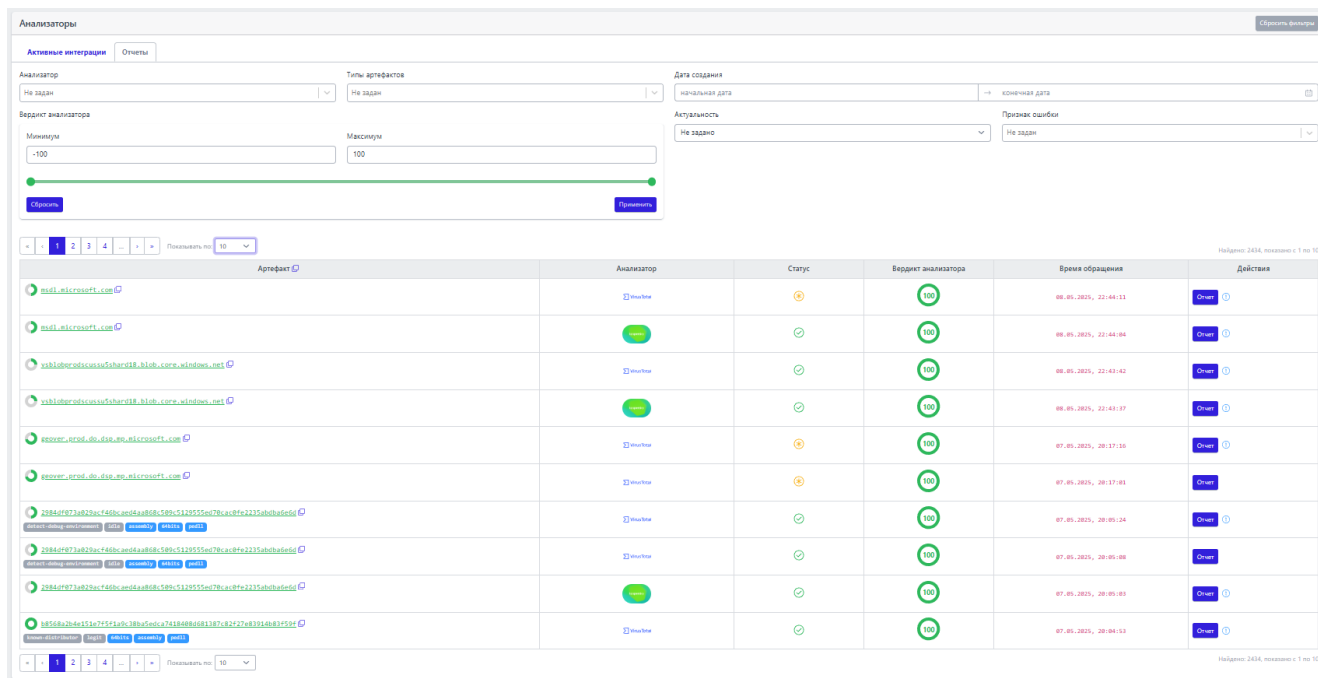


Рисунок 98 – Окно раздела Анализаторы вкладки «Отчеты»

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);

— **Анализатор** (в столбце отображается анализатор, которым был проверен артефакт);

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

— **Вердикт отчета** (отображается вердикт по артефакту, полученный от анализатора, например,  означает, что артефакт безопасен на 100 %);

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

— **Действия** (отображается иконка для просмотра информации по отчету анализатора).

Статус отчета от анализатора отображается следующими иконками:

—  отчет по артефакту получен с ошибками (краткое описание ошибок приведено во всплывающем окне при наведении на иконку);

—  отчет не получен, превышено время ожидания ответа в очереди;

—  отчет не был получен (при наведении на иконку выводится статус и код ошибки);

—  отчет получен успешно.

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).

В столбце **Артефакты** слева от информации об артефакте имеется иконка , показывающая общий вердикт платформы, характеризующий артефакт.

Т.е. в данном примере, артефакт вредоносный на 100%.

Над таблицей для фильтрации информации имеются следующие фильтры:

- **Анализатор** (Название анализатора);
- **Тип артефакта**;
- **Дата создания**;
- **Вердикт анализатора** (Минимальное/Максимальное значения вердикта в границах от -100 (артефакт полностью безопасен), до 100 (артефакт полностью вредоносен);
- **Актуальность** (не задано, актуальный, не актуальный);
- **Признак ошибки** (не задано, не установлен, установлен).

Для просмотра отчета по артефакту нужно нажать по иконке .

Справа от иконки «Отчет» имеется иконка , обозначающая, что отчет по артефакту является последним успешно полученным отчетом по данному артефакту.

Страница отчета анализатора по артефакту представлена на рисунке 99.

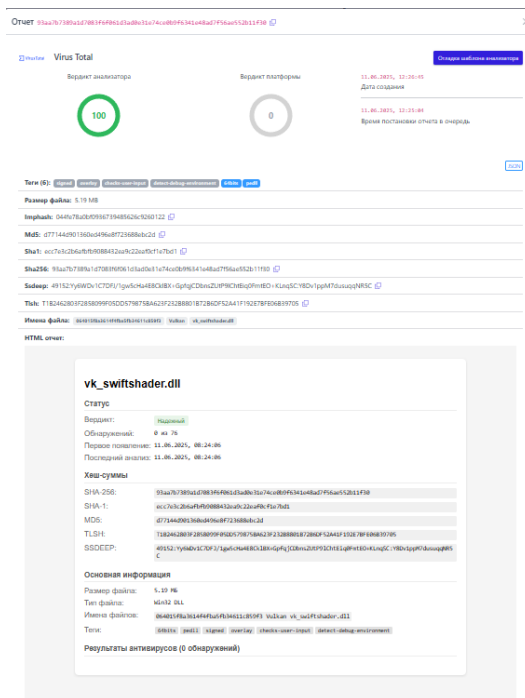


Рисунок 99 – Страница отчета по артефакту

Информацию на странице отчета можно просмотреть в форматах JSON/HTML, используя переключатель **JSON** / **HTML**.

В области **Теги** на странице отчета, полученного от анализатора, можно создать псевдоним для тега, который характерен для артефакта по данному анализатору. После нажатия в поле **Теги** на имя тега, например **assembly**, откроется окно, представленное на рисунке 100.

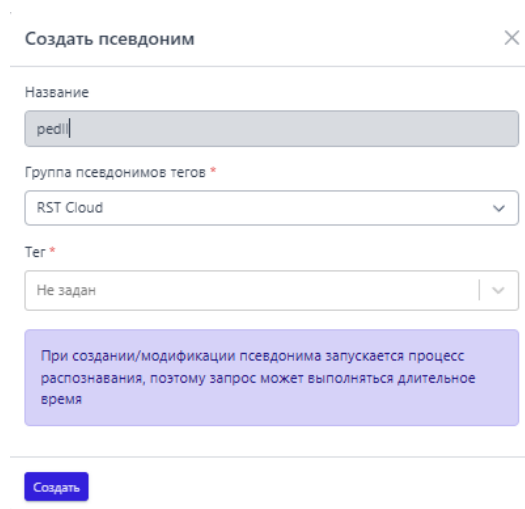
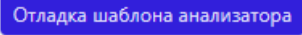


Рисунок 100 – Окно создания псевдонима для тега

После назначения псевдонима тега требуется нажать по иконке «Создать».

На странице отчета имеется иконка , после нажатия по которой откроется окно для редактирования визуального отображения полей в отчете анализатора (рисунок 101).

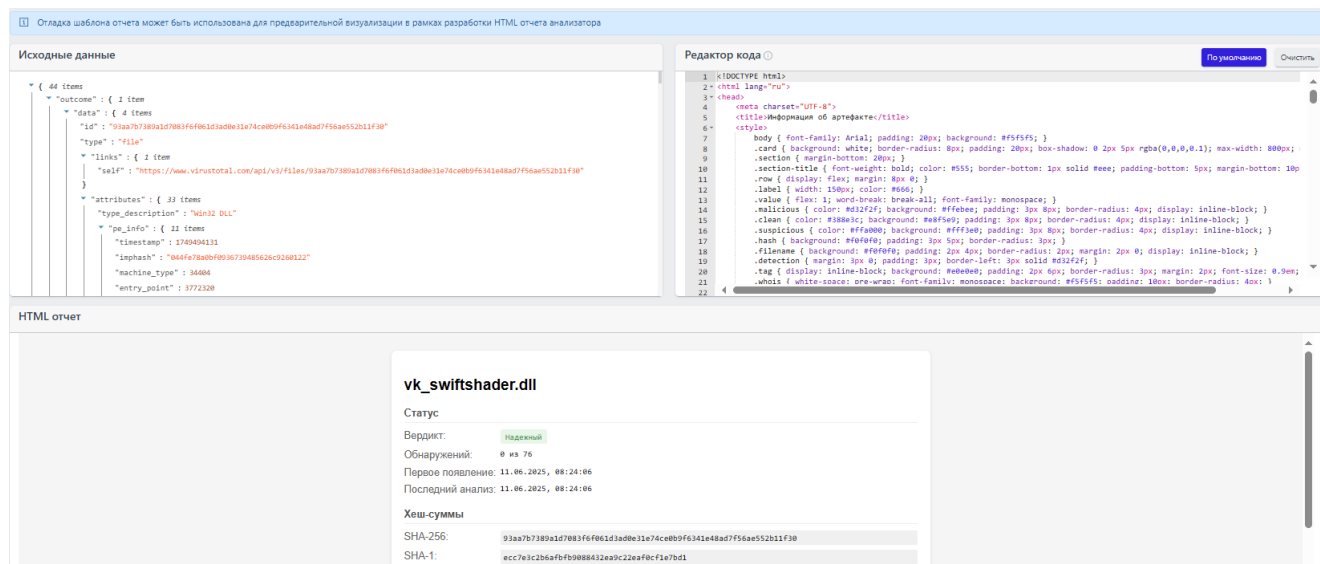


Рисунок 101 – Окно отладки шаблона анализатора

В поле **Исходные данные** показаны данные, которые приходят от анализатора (состав полей настраивается при создании анализатора).

В поле **Редактор кода** по умолчанию представлен пример шаблона для отображения HTML отчета, пришедшего от анализатора.

В поле **HTML отчет** представлено отображение HTML вида отчета по артефакту пришедшее от анализатора.

Более подробная информация по написанию анализатора, редактированию вида HTML отчета и работе с анализаторами описана в отдельном документе инструкции.

Отладка шаблона отчета может быть использована для предварительной визуализации в рамках разработки HTML-отчета анализатора.

В столбце «Артефакты» также можно перейти на страницу **Отчет TI-платформы**, нажав левой кнопкой мыши по артефакту. Описание функционала данной страницы представлено в разделе 6.5.1.

6.5.4. Граф связей

Страница **Граф связей** с незаполненным полем артефакта представлена на рисунке 102.

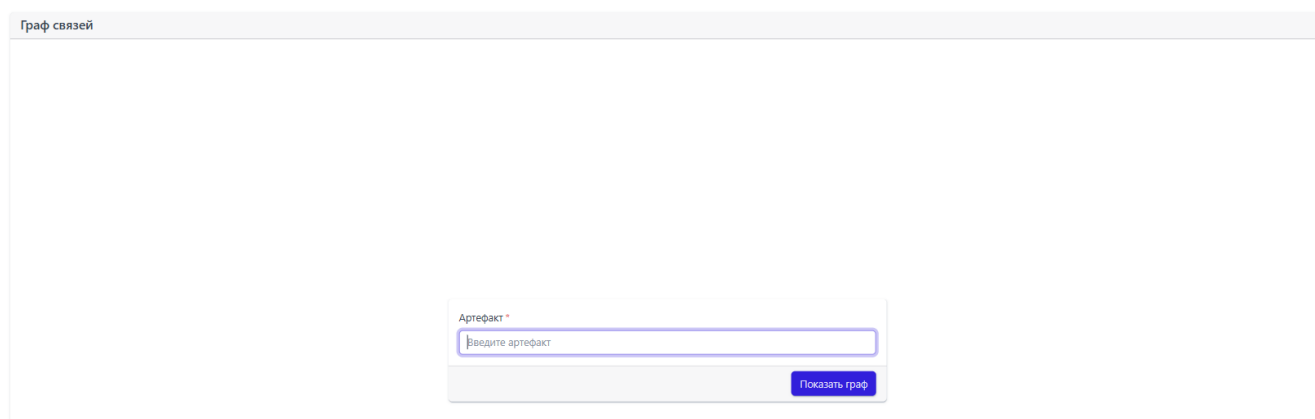


Рисунок 102 – Общий вид пустой страницы «Граф связей»

После внесения в поле «Артефакт» артефакта и нажатия по кнопке «Показать граф» откроется окно графа, показанное на рисунке 103.

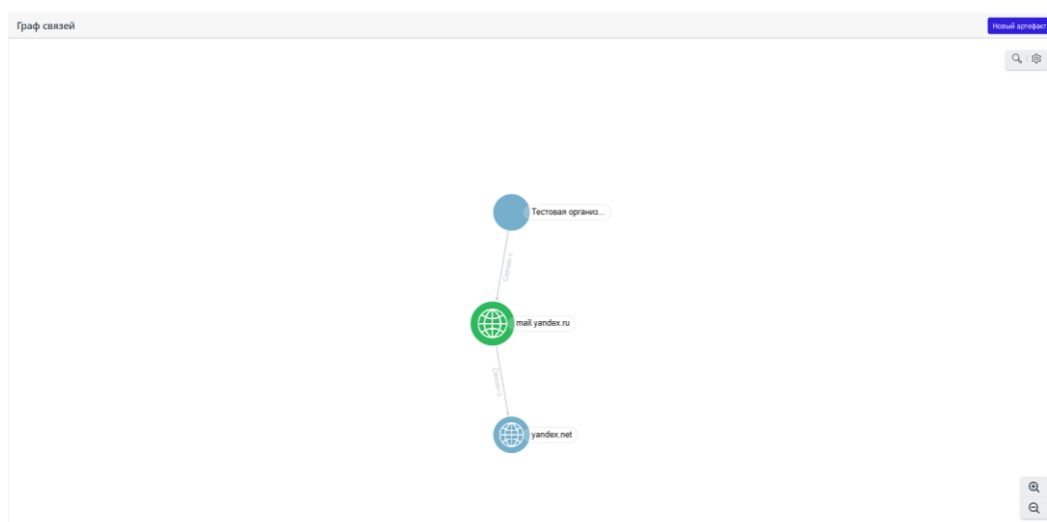


Рисунок 103 – Граф связей

В правой части окна имеются иконки для управления размером отображения графа , и



иконка для возможности изменения параметров .



При нажатии по иконке изменения параметров открывается окно, представленное на рисунке 104.

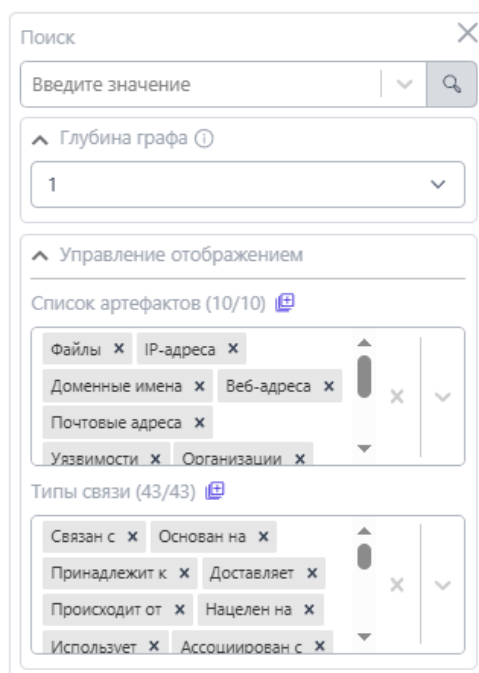


Рисунок 104 – Изменение параметров отображения графа

В данном окне можно ввести артефакт, отображенный на графе изменить глубину отображения элементов (от 1 до 9), и удалить элементы и типы связей, отображенных на графе.

В основной области графа, центральным элементом показан артефакт, который был введен в поле построения графа, а от него со связями показаны артефакты, связанные с основным.

При нажатии ЛКМ на артефакт, в окне графа появиться таблица с информацией о узле представленная на рисунке 105.

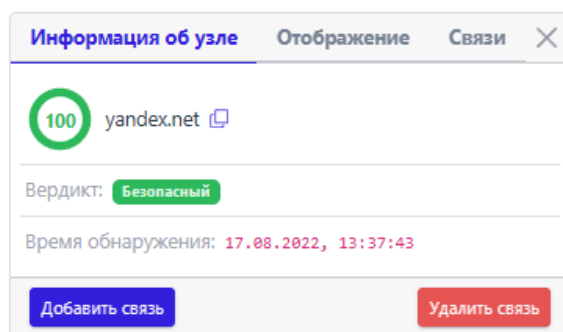


Рисунок 105 – Информация о узле

В данном окне представлены вкладки с информацией о узле.

Во вкладке Отображение (в данной вкладке представлены различные связи узла) можно нажав по иконке **+** добавить на граф связи узла с различными артефактами, а так же организациями и т.п.

С помощью различных иконок можно удалить или добавить связь. Удалить связь можно также на самом графе, наведя указатель мыши на связь, после чего откроется окно подтверждения действия по удалению. Если связь невозможно удалить, то появляется соответствующее сообщение. Связь невозможно удалить если она создана не пользователем, а автоматически.

При изменении глубины графа при нажатии на артефакт на графе отображаются связи согласно выставленного параметра (см. рисунок 106).

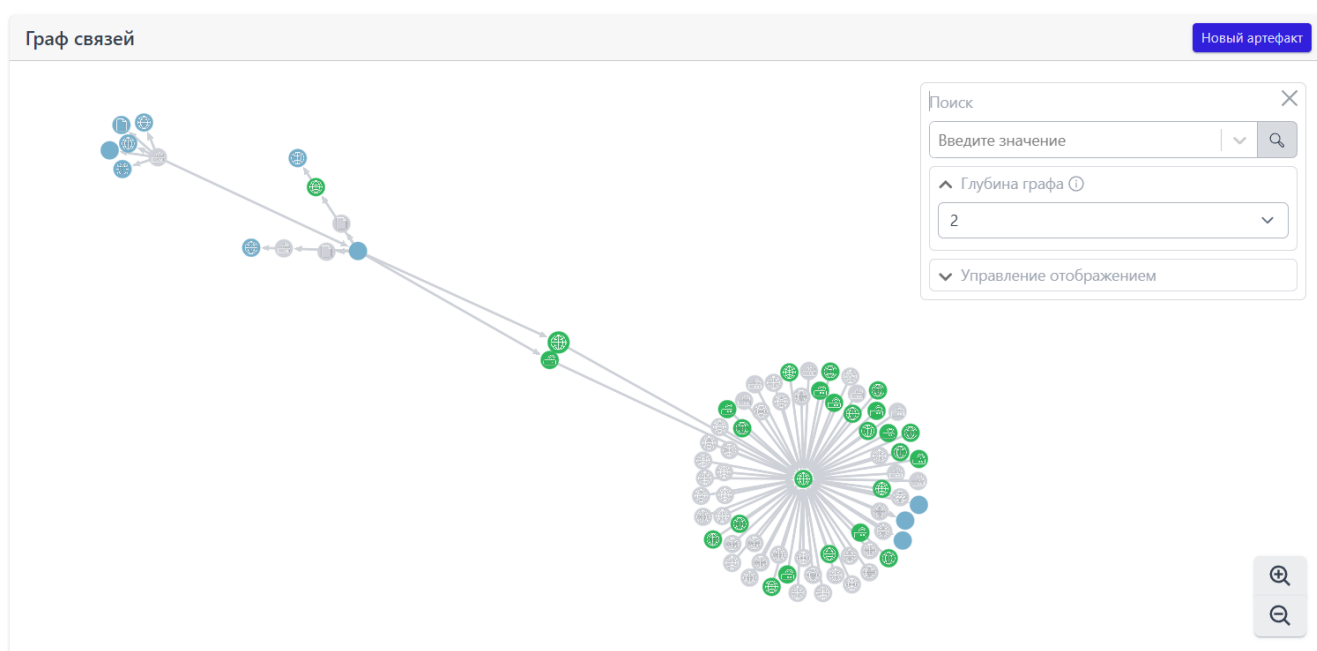


Рисунок 106 – Связи при выставленной глубине графа 2

Следует отметить что установка глубины графа более 2 затрудняет его построение и осложняет визуализацию.

6.5.5. Yara-правила

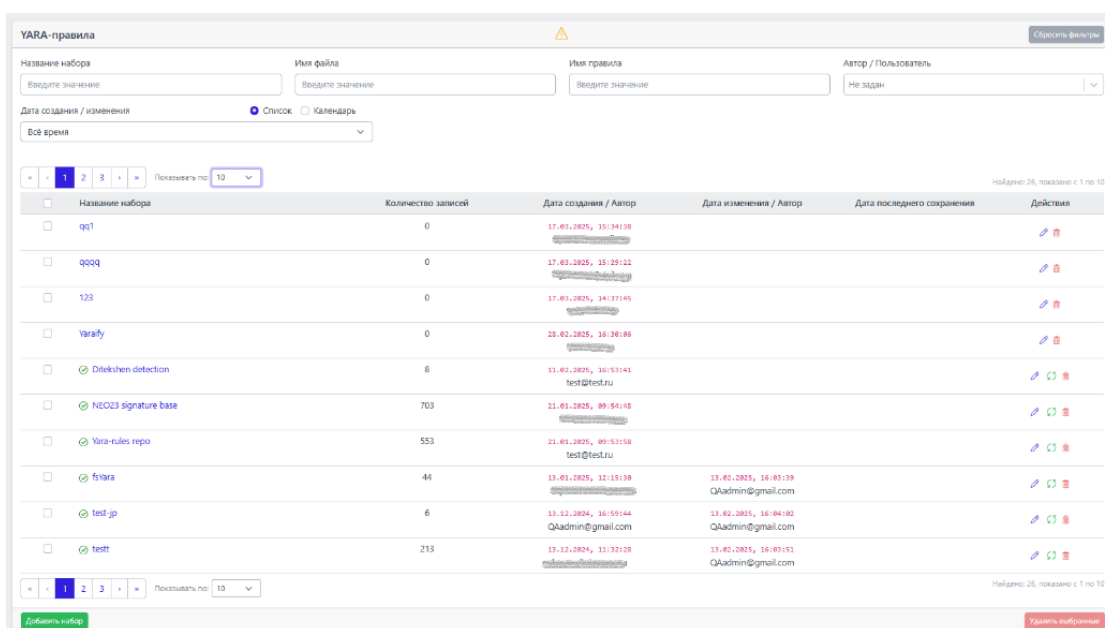
Общая информация

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 JSON и YARA-файлов, а также экспортировать в JSON или YARA-файлы. Добавляемые YARA-файлы используются движком YARA внутри TI-платформы для проверки файлов, загружаемых через главную страницу, или API-файлов.

Наборы Yara-правил

Страница с наборами YARA-правил (рис. 107) открывается при выборе на панели слева раздела **YARA-правила** и включает в себя следующие структурные элементы:

- кнопка **Сбросить фильтры**;
- таблица с наборами YARA-правил;
- кнопка **Добавить набор**;
- кнопка **Удалить выбранные наборы**;
- элементы фильтрации.



Название набора	Количество зависимостей	Дата создания / Автор	Дата изменения / Автор	Дата последнего сохранения	Действия
q1	0	17.01.2025, 15:34:38			 
q00q	0	17.01.2025, 15:29:22			 
123	0	17.01.2025, 14:37:45			 
Yarify	0	28.01.2025, 16:38:06			 
✔ Ditekhen detection	8	11.01.2025, 16:53:41 test@test.ru			 
✔ NEO23 signature base	703	21.01.2025, 09:54:48			 
✔ Yara-rules repo	553	21.01.2025, 09:53:58 test@test.ru			 
✔ fsYara	44	13.01.2025, 12:15:39	13.02.2025, 16:03:39 QAAdmin@gmail.com		 
✔ test.jp	6	13.12.2024, 16:55:44 QAAdmin@gmail.com	13.02.2025, 16:04:02 QAAdmin@gmail.com		 
✔ testt	213	13.12.2024, 11:32:28	13.02.2025, 16:03:51 QAAdmin@gmail.com		 

Рисунок 107 – Наборы YARA-правил

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

- Название набора;
- Имя файла;
- Имя правила;
- Автор/Пользователь;
- Дата создания/Изменения.

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 108) 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.

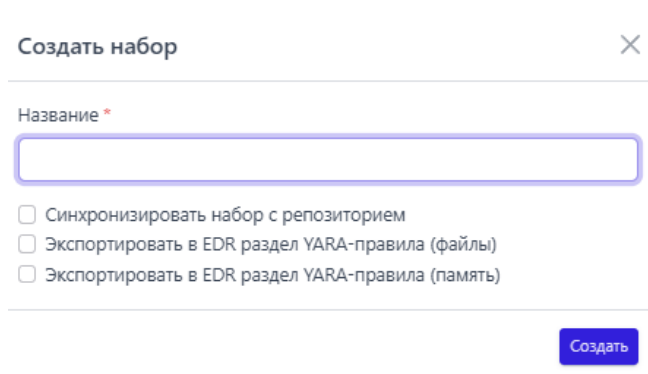


Рисунок 108 – Создать набор YARA-правил

При создании набора, после указания, что набор нужно синхронизировать с репозиторием Github, окно создания набора изменится и будет иметь вид, представленный на рисунке 109.

Создать набор

✕

Название *

Ссылка на репозиторий ⓘ *

☒ Признак рекурсивной синхронизации репозитория

Период обновления набора *

Не задан ▾

☒ Синхронизировать набор с репозиторием

☐ Экспортировать в EDR раздел YARA-правила (файлы)

☐ Экспортировать в EDR раздел YARA-правила (память)

Создать

Рисунок 109 – Создание набора синхронизированного с репозиторием

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

Пример указания адреса репозитория можно просмотреть, наведя указатель мыши на иконку ⓘ *

Также можно выставить признак рекурсивной синхронизации репозитория, который обозначает, что в ссылке на репозиторий можно указать не только корневой каталог, но и внутреннюю папку.

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. **Ошибка! Источник ссылки не найден.**).

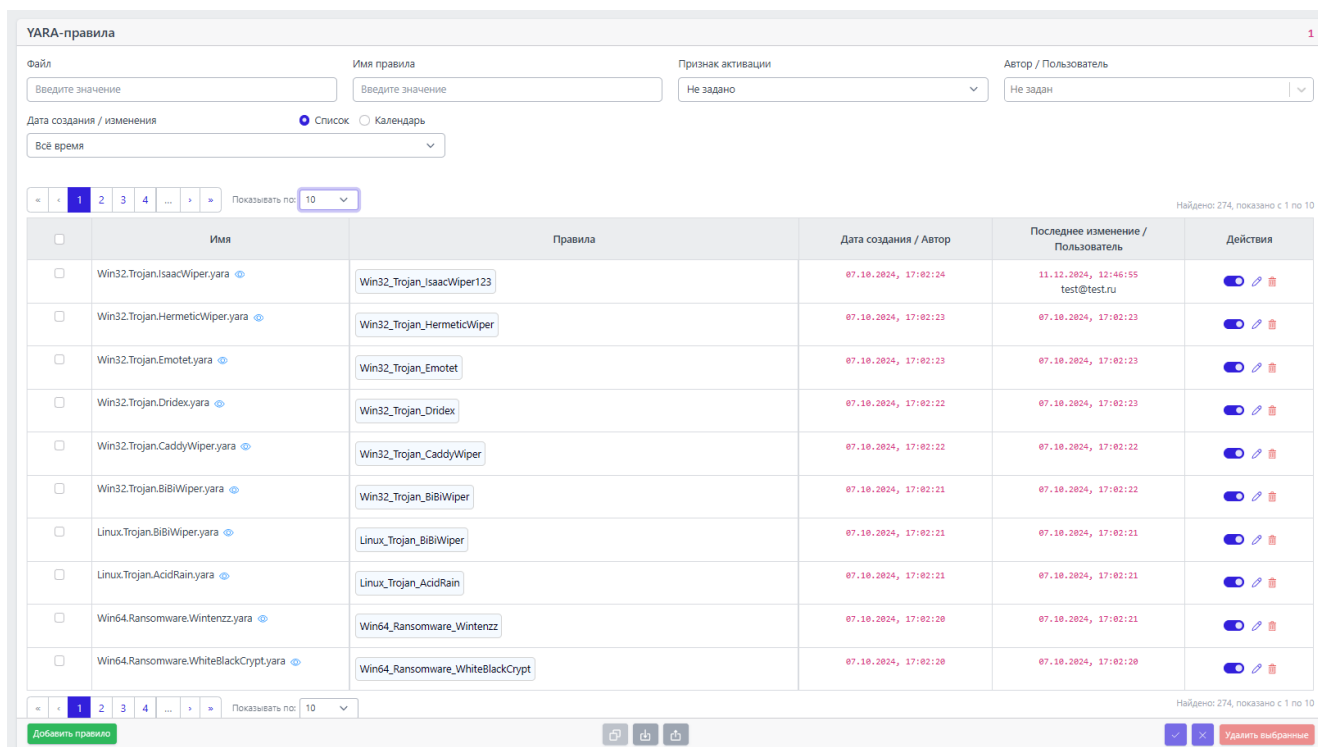


Рисунок 110 – YARA-правила

Страница «Yara-правила»

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

- просматривать правила из выбранного набора;
- добавлять новые правила в выбранный набор, при этом в синхронизируемый из репозитория набор добавлять правила нельзя;
- 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 в наборе, фильтрация осуществляется с помощью следующих фильтров:

- Файл;
- Имя файла;
- Признак активации;

- Автор/Пользователь;
- Дата создания/Изменения.

Для добавления нового правила необходимо нажать кнопку **Добавить правило**, после чего откроется окно **Добавить правило** (рисунок 111), 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 112.

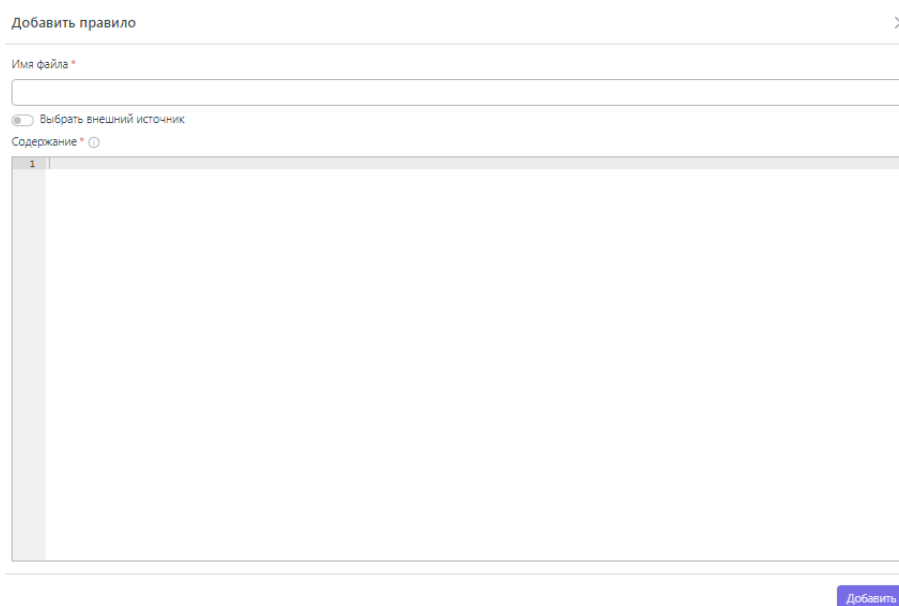


Рисунок 111 – Окно добавления правила

```
1 rule CobaltStrike__Resources_Artifact32_and_Resources_Dropper_v1_49_to_v3_14
2 {
3   meta:
4     desc="Cobalt Strike's resources/artifact32{.exe,.dll,big.exe,big.dll} and resources/dropper.exe signature for versions 1.49 to 3.14"
5     rs1 = "40fc605a8b95bbd79a3bd7d9af73fbeebe3fada577c99e7a111f6168f6a0d37a"
6     author = "gssincla@google.com"
7
8   strings:
9     // Decoder function for the embedded payload
10    $payloadDecoder = { 8B [2] 89 ?? 03 [2] 8B [2] 03 [2] 0F B6 18 8B [2] 89 ?? C1 ?? 1F C1 ?? 1E 01 ?? 83 ?? 03 29 ?? 03 [2] 0F B6 00 31 ?? 88 ?? 8F
11
12
13
14   condition:
15     any of them
16 }
```

Рисунок 112 – 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 113.

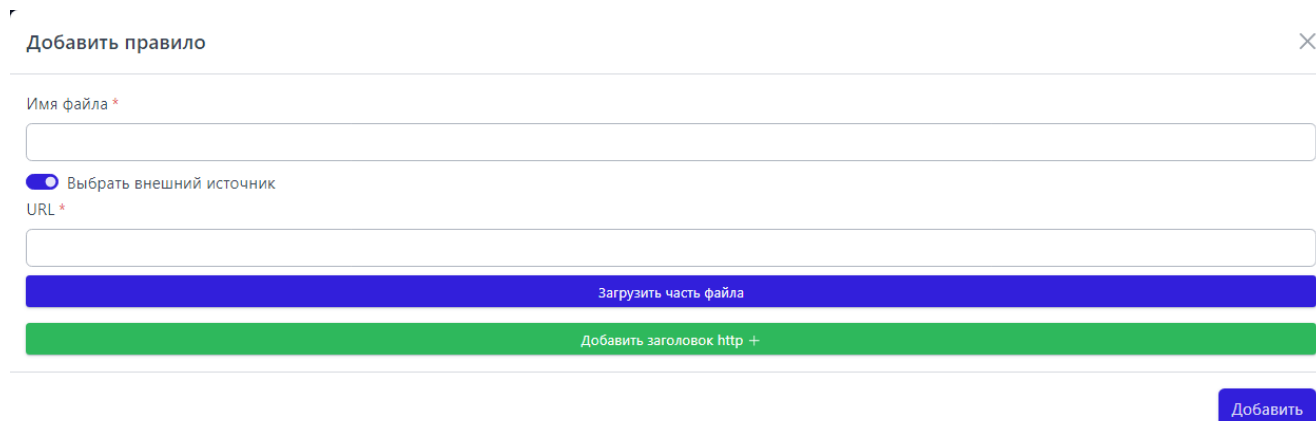


Рисунок 113 – Окно добавления правила из внешнего источника

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/JSON** (). Набор будет сохранен в папке **Загрузки** в указанном формате. Для импорта правил из файла требуется нажать кнопку **Импортировать YARA-файл** (). При этом импорт правил из файла поддерживается также в форматах **YARA/JSON**. 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

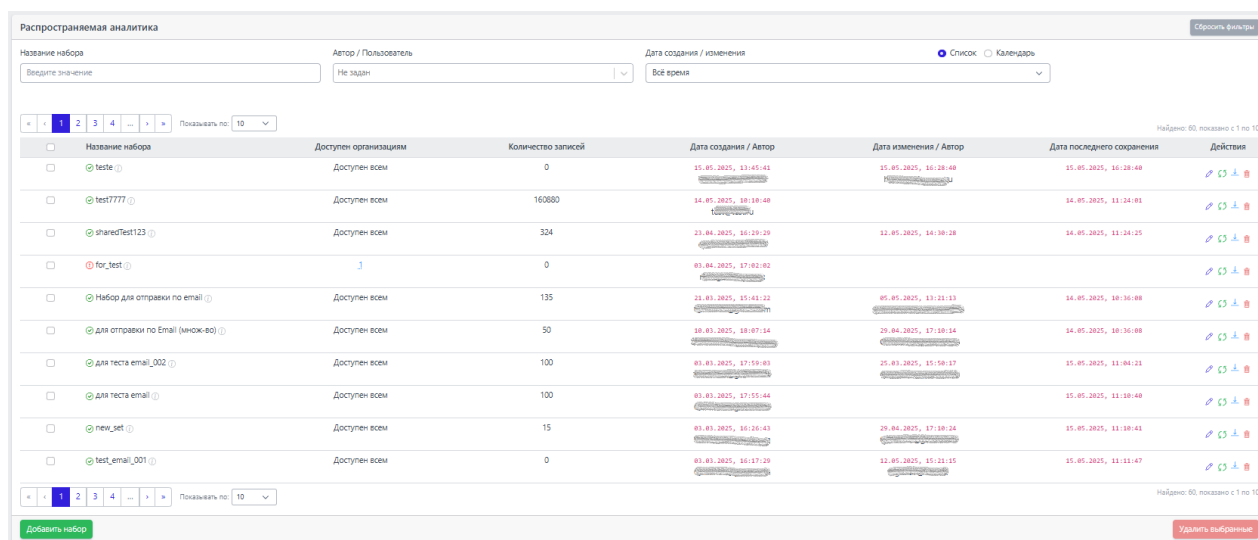
Общие сведения

Распространяемая аналитика позволяет определить артефакты, в автоматическом режиме распространяемые на клиентов, взаимодействующих с ТИ, если они поддерживают соответствующий формат данных.

На странице раздела **Распространяемая аналитика** пользователь сервиса RT Protect ТИ, 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 114.



Название набора	Доступен организациям	Количество записей	Дата создания / Автор	Дата изменения / Автор	Дата последнего сохранения	Действия
teste	Доступен всем	0	15.05.2025, 13:45:41	15.05.2025, 16:18:49	15.05.2025, 16:18:49	  
test7777	Доступен всем	163880	14.05.2025, 18:18:48	14.05.2025, 18:18:48	14.05.2025, 13:14:01	  
sharedTest123	Доступен всем	334	21.04.2025, 16:29:29	22.05.2025, 14:18:28	14.05.2025, 13:14:25	  
for_test	3	0	01.04.2025, 17:02:02			  
Набор для отправки по email	Доступен всем	135	21.03.2025, 15:43:22	05.05.2025, 13:21:13	14.05.2025, 18:16:08	  
для отправки по Email (много-во)	Доступен всем	50	18.03.2025, 18:07:14	25.04.2025, 17:10:14	14.05.2025, 18:16:08	  
для теста email_002	Доступен всем	100	01.03.2025, 17:19:03	25.03.2025, 15:10:17	15.05.2025, 13:04:21	  
для теста email	Доступен всем	100	01.03.2025, 17:15:44		15.05.2025, 13:04:48	  
new_set	Доступен всем	15	01.03.2025, 16:16:43	29.04.2025, 17:10:14	15.05.2025, 13:04:41	  
test_email_001	Доступен всем	0	01.03.2025, 16:17:19	22.05.2025, 15:14:15	15.05.2025, 13:11:47	  

Рисунок 114 – Страница раздела «Распространяемая аналитика»

Страница представлена в виде таблицы с наборами аналитических данных.

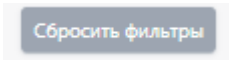
В таблице имеются следующие поля:

— Название набора;

- Доступен организациям;
- Количество записей;
- Дата создания/автор;
- Дата изменения/автор;
- Дата последнего сохранения;
- Действия.

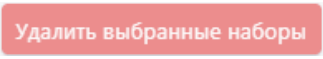
Для фильтрации информации в таблице имеются следующие фильтры:

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

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

Для навигации на странице имеется стандартный элемент пагинатор.

Действия, возможные над наборами:

-  (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 115.

Создать набор

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

Название *

☐ Доступен организациям ☐ Недоступен организациям

Не заданы

Почтовый адрес для получения обновлений ⓘ

Введите значение, разделитель ,

Период обновления набора *

Никогда

Тип создаваемого архива

Без архивации

Формат создаваемого файла

CSV

Настройки экспорта ⓘ

Не задано

☐ Признак автоматического сохранения после синхронизации

Создать

Созданные конфигурации

Рисунок 115 – Окно создания набора

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

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

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

Выбранная вкладка подсвечивается синим цветом. Поля с настройками по выбранной вкладке **Источники данных** представлены на рисунке 116.

Создать набор

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

Источник данных:

Тип артефакта:

Количество:

Актуальность:

Надежность (Минимум):

Сортировка:

Направление сортировки:

Дата добавления: ☒ Список ☐ Календарь

Дата синхронизации: →

Активация:

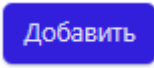
Добавить

Создать

Рисунок 116 – Настройка полей выбранной вкладки «Источники данных»

В данной вкладке можно настроить следующие параметры:

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

После выставления настроек требуется нажать по иконке , после чего появится поле с зафиксированными настройками конфигурации источника данных (рисунок 117).

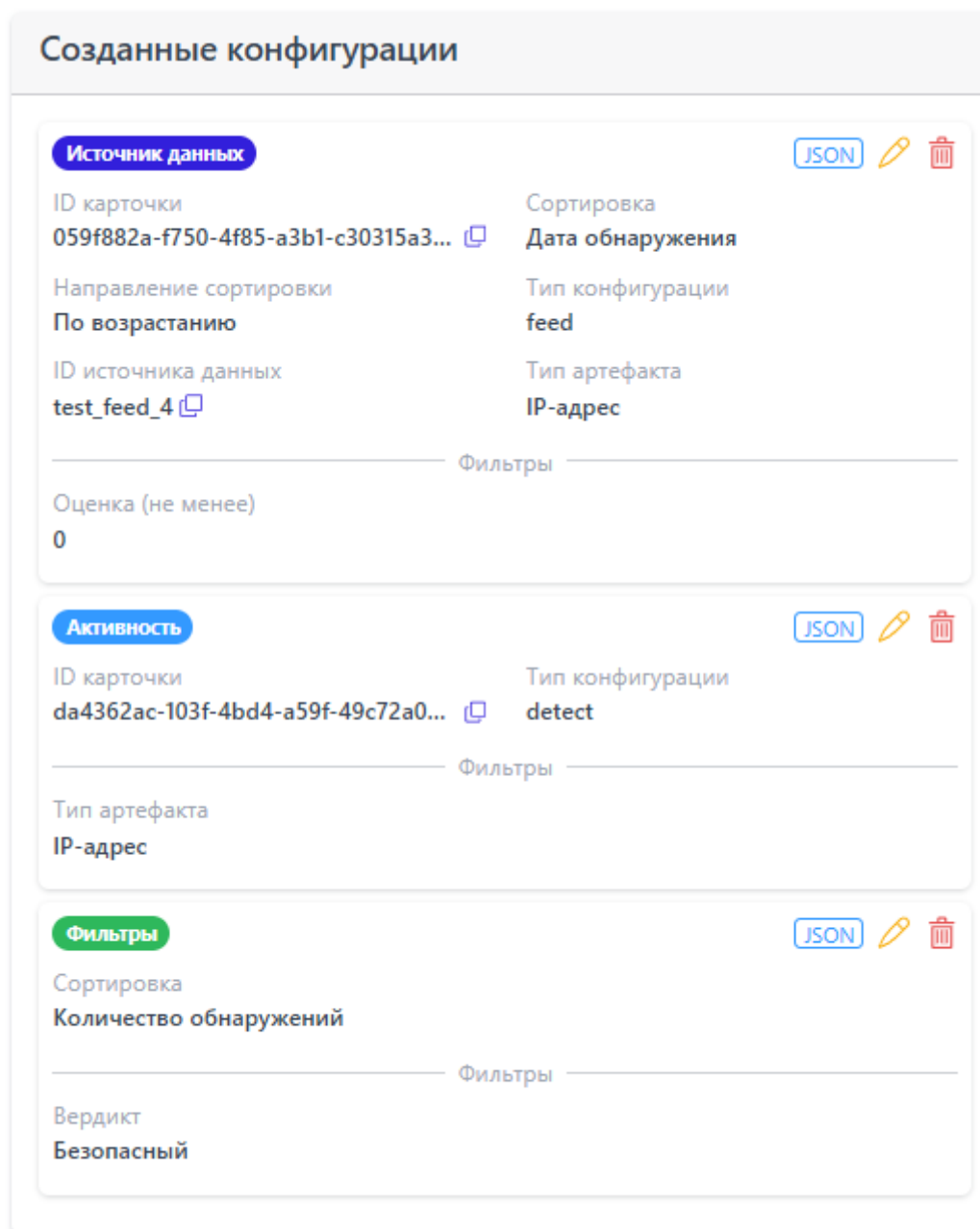


Рисунок 117 – Создание конфигурации набора распространяемой аналитики

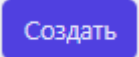
В области настроенной конфигурации имеются кнопки, не зависящие от конфигурации и являющиеся общими для всех вкладок.

При нажатии по иконке  имеется возможность редактирования настроенной конфигурации.

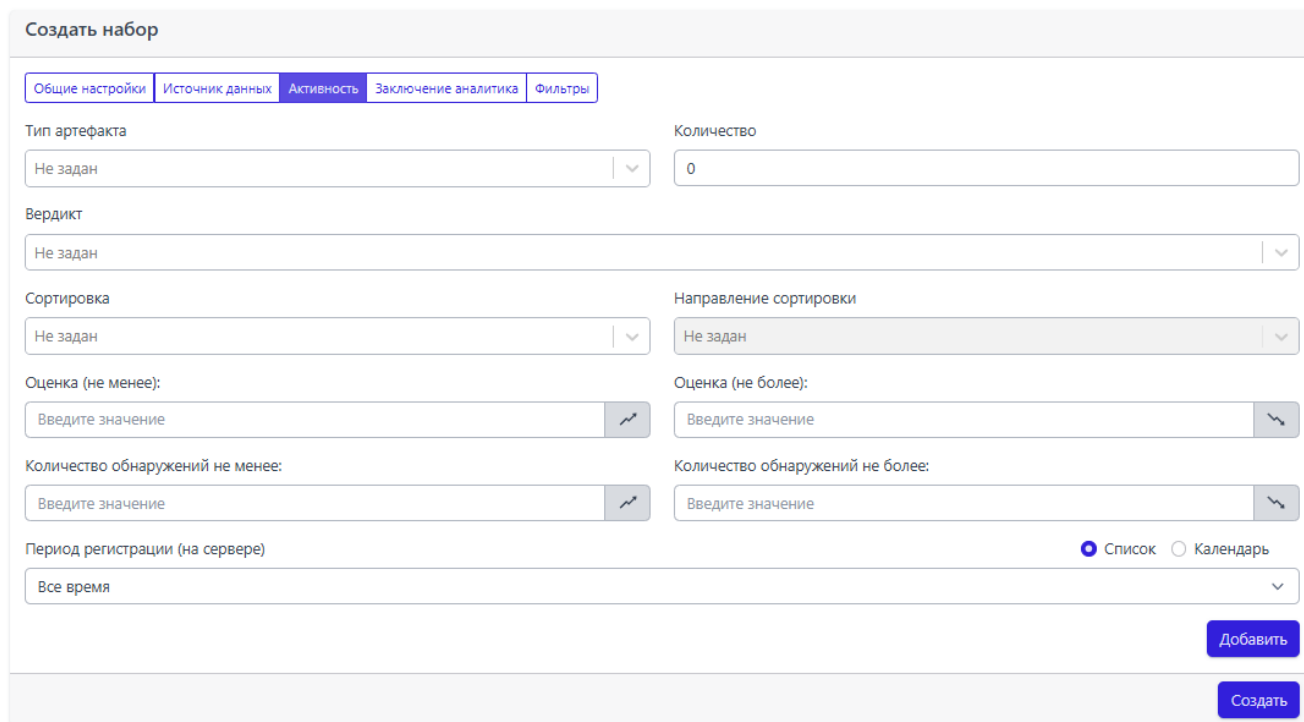
При нажатии по иконке , имеется возможность просмотра настроенной конфигурации в соответствующем формате.

При нажатии по иконке  происходит удаление настроек параметров в конфигурации.

После редактирования настроек конфигурации для сохранения измененных настроек требуется

нажать по иконке .

Поля настройки по выбранной вкладке **Активность** представлены на рисунке 118.



Создать набор

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

Тип артефакта: Не задан | Количество: 0

Вердикт: Не задан

Сортировка: Не задан | Направление сортировки: Не задан

Оценка (не менее): Введите значение | Оценка (не более): Введите значение

Количество обнаружений не менее: Введите значение | Количество обнаружений не более: Введите значение

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

Добавить

Создать

Рисунок 118 – 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 возрастантию/убыванию);
- количество обнаружений не менее;
- количество обнаружений не более;
- Период регистрации (на сервере) (начальная и конечная даты);
- Оценка (от -100 до 100).

Поля настройки по выбранной вкладке **Заключения аналитика** представлены на рисунке 119.

Рисунок 119 – 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 аналитика);

- Тип артефакта (Файл, IP-адрес; доменное имя; URL, EMAIL);

- Вердикт (Неизвестный, безопасный, вредоносный, подозрительный);

- Сортировка (по количеству обнаружений, по времени последнего обнаружения, по возрастанию/убыванию);

- Время актуальности (день, неделя, месяц, 3 месяца, бесконечно);

- Время создания (начальная и конечная дата),

- Актуальность.

Поля настройки по выбранной вкладке **Фильтры** представлены на рисунке 120.

Создать набор

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

Вердикт

Безопасный

Дата изменения вердикта:

Все время

Сортировка

Количество обнаруже...

Направление сортировки

Не задан

Оценка (не менее):

Не задана

Оценка (не более):

Не задана

Первое обнаружение

☒ Список ☐ Календарь

Все время

Последнее обнаружение

☒ Список ☐ Календарь

Все время

Количество обнаружений не менее:

Не задано

Количество обнаружений не более:

Не задано

Количество

Не задано

Теги

Не задан

Отмена

Сохранить

Создать

Рисунок 120 – Настройка полей выбранной вкладки «Фильтры»

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

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

6.5.7. Угрозы и злоумышленники

На данной странице отображаются данные по угрозам и злоумышленникам полученные от различных источников, например, данных MISP.

Источники данных возможно загрузить как с помощью сервера RT Protect TI, так и на этапе деплоя сервера добавим необходимую информацию в файл:

ti-deploy/config/default/feeds.json

Данный раздел может использоваться аналитиками и администраторами в качестве аналитической информации.

Общий вид страницы представлен на рисунке 121.

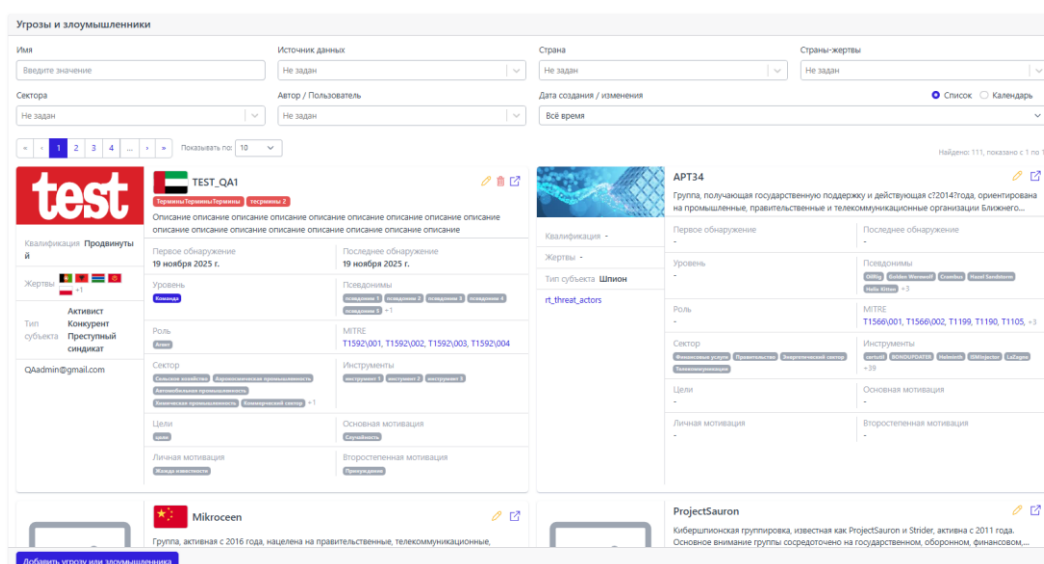


Рисунок 121 – Страница Угрозы и злоумышленники

На данной странице имеется возможность добавить информацию о злоумышленнике или угрозе нажав по иконке «Добавить угрозу или злоумышленника».

Имеется возможность редактировать информацию о злоумышленнике, удалить поле с описанием, либо перейти на страницу с описанием угрозы.

Так же можно просмотреть граф связей упоминаемых в статье артефактов.

6.5.8. Вредоносное ПО

На странице Вредоносное ПО в виде таблицы представлен перечень вредоносного ПО (рисунок 122).

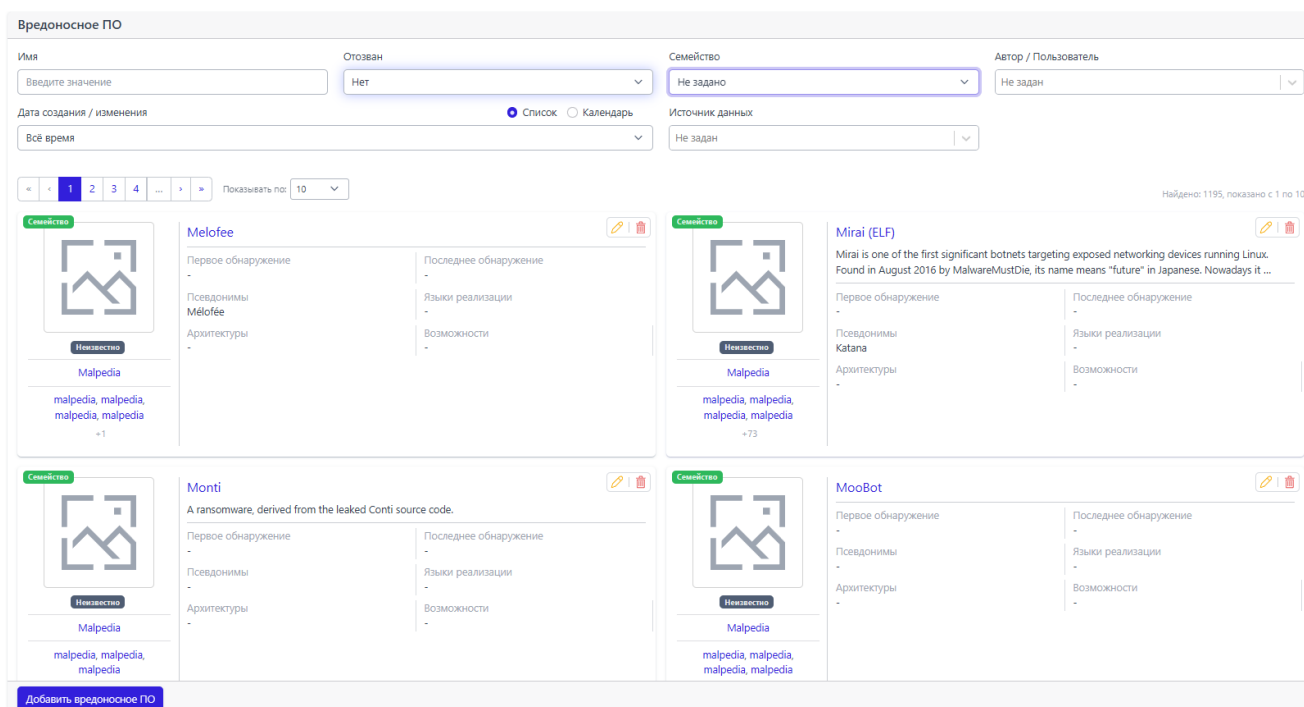


Рисунок 122 – Страница Вредоносное ПО

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

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

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

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

Добавить вредоносное ПО

При нажатии по иконке , можно добавить информацию о новом вредоносном ПО.

После нажатия по иконке открывается страница добавления информации о ПО представленная на рисунке 123.

The screenshot shows a web form titled "Добавить вредоносное ПО" (Add Malware) with a close button (X) in the top right corner. The form contains several input fields and dropdown menus:

- Имя *** (Name): A text input field with placeholder "Введите значение".
- Тип вредоносного ПО *** (Type of malware): A dropdown menu with "Не задан" (Not specified) selected.
- Дата обнаружения *** (Date of discovery): A date picker input field.
- Дата последнего обнаружения *** (Date of last discovery): A date picker input field.
- Псевдонимы** (Aliases): A text input field with placeholder "Введите значение, разделитель ;".
- Термины** (Terms): A text input field with placeholder "Введите значение, разделитель ;".
- Описание** (Description): A large text area with placeholder "Введите значение".
- Языки реализации** (Implementation languages): A dropdown menu with "Не задана" (Not specified) selected.
- Архитектуры** (Architectures): A dropdown menu with "Не задана" (Not specified) selected.
- Возможности** (Capabilities): A dropdown menu with "Не задана" (Not specified) selected.
- Семейство** (Family): A checkbox.
- Отозван** (Revoked): A checkbox.
- Иконка** (Icon): A section with a "Выбрать файл" (Choose file) button and a preview area labeled "Иконка" with a red delete icon.

At the bottom right of the form are two buttons: "Создать" (Create) in blue and "Отмена" (Cancel) in grey.

Рисунок 123 – Ручное добавление информации о вредоносном ПО

При установке галочки «Отозвать» дальнейший учет данного вредоносного инструмент исключается

В области дополнительной информации можно указать дату обнаружения, дату последнего обнаружения, языки реализации, Архитектуры, возможности.

При нажатии по иконке «Создать» информация о новом вредоносном ПО появится в общем списке.

6.5.9. Инструменты

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

Общий вид страницы представлен на рисунке 124.

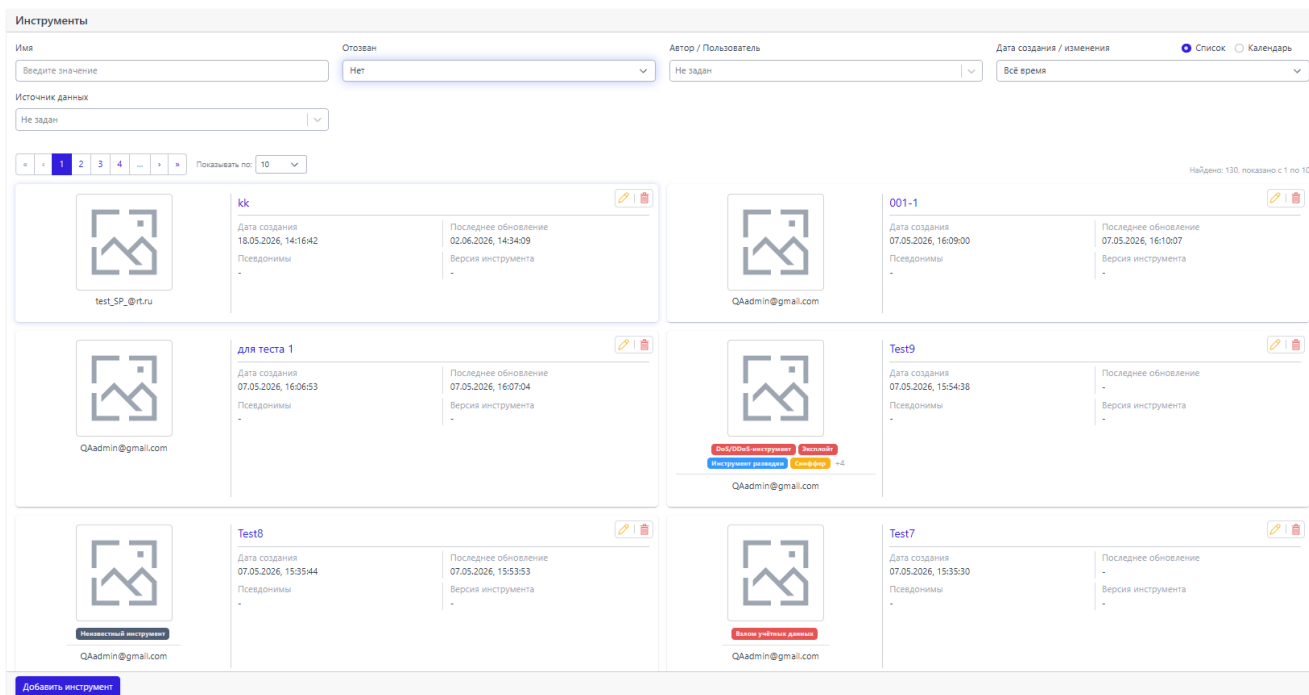
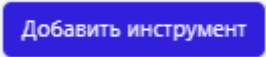


Рисунок 124 – Общий вид страницы «Инструменты»

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

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

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

Для добавления информации о инструменте вручную, требуется по иконке , после чего в открывшемся окне добавить информацию и нажать по иконке «Создать», после чего инструмент появиться в общем списке.

При наведении указателя мыши на иконку с именем инструмента и нажатии ЛКМ, открывается окно с расширенной информацией, где есть так же возможность просмотреть связанные с инструментом сущности, и просмотреть граф связей.

6.5.10. Матрица MITRE ATT&CK

На рисунке 125 представлен общий вид страницы Матрица MITRE ATT&CK. На данной странице приведено описание техник Mitre описывающих различные вредоносные действия. Аналитик и администратор для удобства описания и понимания вредоносных техник упоминающихся в отчетах может обратиться к странице.

Поиск

Поиск по названию или ID техники...

Reconnaissance12	Resource Development9	Initial Access11	Execution24	Persistence25	Privilege Escalation14	Stealth33
T1589 Gather Victim Identity I...	T1583 Acquire Infrastructure	T1078 Valid Accounts	T1047 Windows Management Inst...	T1034 Path Interception	T1034 Path Interception	T1006 Direct Volume Access
T1590 Gather Victim Network ...	T1584 Compromise Infrastruct...	T1091 Replication Through Remov...	T1053 Scheduled Task/Job	T1037 Boot or Logon Initializat...	T1037 Boot or Logon Initializat...	T1014 Rootkit
T1591 Gather Victim Org Infor...	T1585 Establish Accounts	T1133 External Remote Services	T1059 Command and Scriptin...	T1053 Scheduled Task/Job	T1053 Scheduled Task/Job	T1027 Obfuscated Files or Inf...
T1592 Gather Victim Host Info...	T1586 Compromise Accounts	T1189 Drive-by Compromise	T1061 Graphical User Interface	T1062 Hypervisor	T1055 Process Injection	T1036 Masquerading
T1593 Search Open Websites/...	T1587 Develop Capabilities	T1190 Exploit Public-Facing Applic...	T1064 Scripting	T1078 Valid Accounts	T1068 Exploitation for Privilege Es...	T1055 Process Injection
T1594 Search Victim-Owned Webs...	T1588 Obtain Capabilities	T1195 Supply Chain Comprom...	T1072 Software Deployment Tools	T1098 Account Manipulation	T1078 Valid Accounts	T1064 Scripting
T1595 Active Scanning	T1608 Stage Capabilities	T1199 Trusted Relationship	T1106 Native API	T1108 Redundant Access	T1098 Account Manipulation	T1070 Indicator Removal
T1596 Search Open Technical ...	T1650 Acquire Access	T1200 Hardware Additions	T1127 Trusted Developer Utilit...	T1112 Modify Registry	T1134 Access Token Manipulat...	T1078 Valid Accounts
T1597 Search Closed Sources	T1683 Generate Content	T1566 Phishing	T1129 Shared Modules	T1133 External Remote Services	T1484 Domain or Tenant Polic...	T1108 Redundant Access
T1598 Phishing for Information		T1659 Content Injection	T1153 Source	T1136 Create Account	T1543 Create or Modify Syste...	T1127 Trusted Developer Utilit...
T1681 Search Threat Vendor Data		T1669 Wi-Fi Networks	T1175 Component Object Model a...	T1137 Office Application Start...	T1546 Event Triggered Execut...	T1134 Access Token Manipulat...
T1682 Query Public AI Services			T1197 BITS Jobs	T1176 Software Extensions	T1547 Boot or Logon Autosta...	T1140 Deobfuscate/Decode Files ...
			T1203 Exploitation for Client Execu...	T1197 BITS Jobs	T1548 Abuse Elevation Control...	T1149 LC_MAIN Hijacking
			T1204 User Execution	T1205 Traffic Signaling	T1611 Escape to Host	T1197 BITS Jobs
			T1559 Inter-Process Commun...	T1505 Server Software Compo...		T1202 Indirect Command Execution
			T1569 System Services	T1525 Implant Internal Image		T1205 Traffic Signaling
			T1574 Hijack Execution Flow	T1542 Pre-OS Boot		T1211 Exploitation for Stealth
			T1609 Container Administration C...	T1543 Create or Modify Syste...		T1216 System Script Proxy Exe...
			T1610 Deploy Container	T1546 Event Triggered Execut...		T1218 System Binary Proxy Ex...
			T1648 Serverless Execution	T1547 Boot or Logon Autosta...		T1220 XSL Script Processing
			T1651 Cloud Administration Com...	T1554 Compromise Host Software...		T1221 Template Injection
			T1674 Input Injection	T1556 Modify Authentication ...		T1480 Execution Guardrails

Рисунок 125 – Общий вид страницы Матрица MITRE ATT&CK

6.5.11. Лента угроз

На данной странице представлены статьи, касающиеся информационной безопасности, в которых имеются упоминания об угрозах и вредоносных артефактах.

Информация на странице представлена в виде списка статей с кратким описанием.

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

- Название;
- Отозван;
- Информация получена из ИИ;
- Артефакт;
- Уязвимость;
- Источник;

- Источник данных;
- Дата создания/Изменения;
- Тип отчета (не задано, отчет об угрозе, другое).

Общий вид страницы **Лента угроз** представлен на рисунке 126.

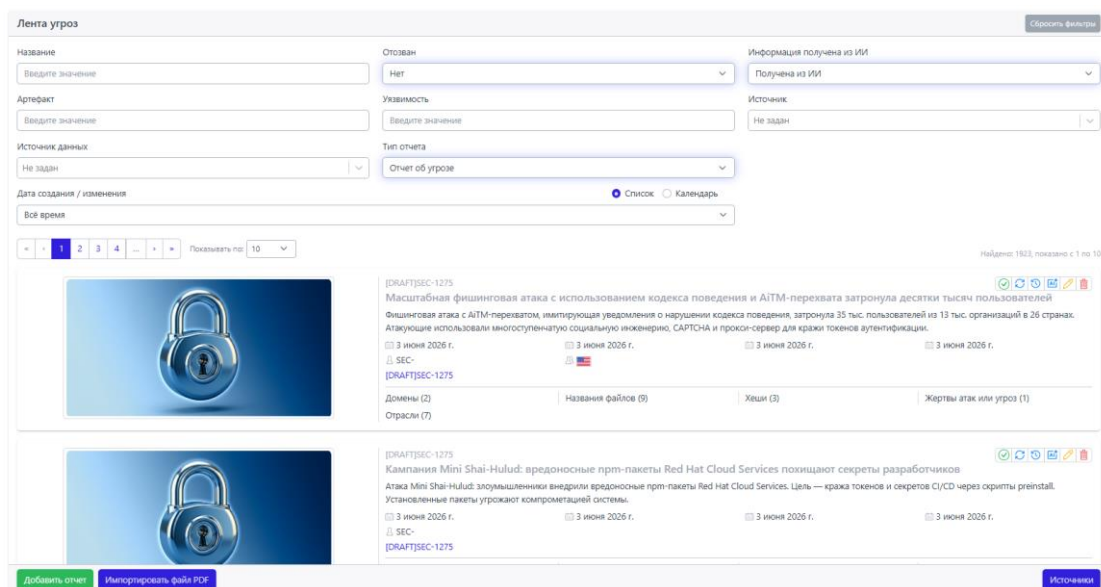


Рисунок 126 – Общий вид страницы Лента угроз

При нажатии по имени статьи ЛКМ откроется страница с более подробной информацией о статье и об артефактах, которые упоминаются в статье (рисунок 127).

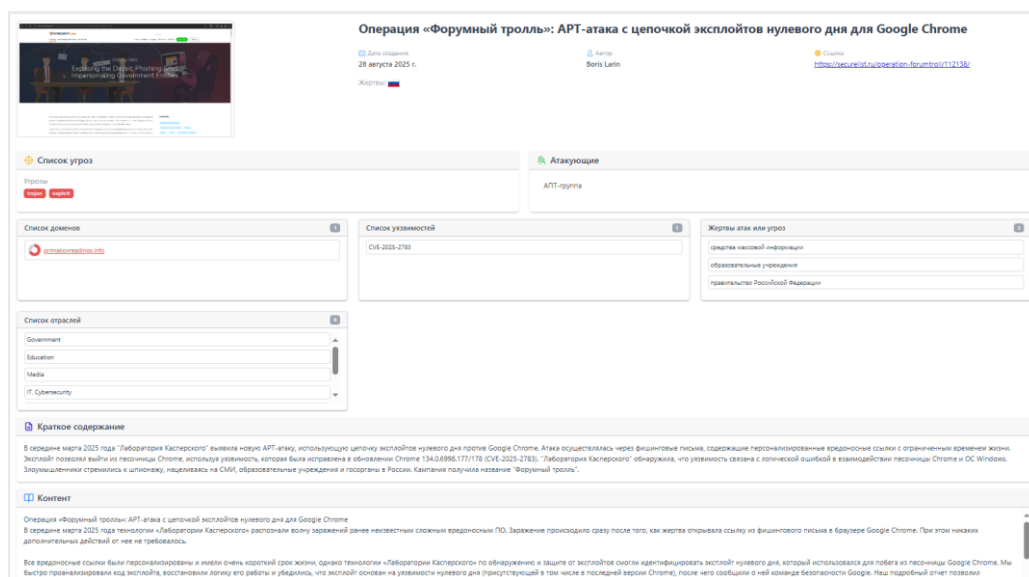


Рисунок 127 – Подробная информация о статье

На странице отображается информация из статьи, а также, угрозы упоминающиеся в статье, например, найденные вредоносные артефакты.

В нижней части окна отображается область с графом связей артефактов.

При нажатии по иконке **Источники** на странице «Лента угроз» происходит переход на страницу со списком источников из которых были получены представленные на странице статьи (рисунок 128).

☐	Название	URL	Источник данных	Дата создания / Автор	Действия
☐	SECURELIST_test_QA	https://securelist.com/	SECURELIST_test_QA	05.03.2026, 17:52:47 QAAdmin@gmail.com	
☐	Blog Malware Bytes_forrest_other_org	https://www.malwarebytes.com/blog	Blog Malware Bytes_forrest_other_org	05.03.2026, 17:48:39 forrest2@yandex.ru	
☐	Telegram APT Reports_test_QA	https://t.me/s/aptreports	Telegram APT Reports_test_QA1	03.03.2026, 18:29:25 QAAdmin@gmail.com	
☐	Blog Malware Bytes_test_qa	https://www.malwarebytes.com/blog	Blog Malware Bytes_test_qa	03.03.2026, 18:22:54 QAAdmin@gmail.com	
☐	Google Cloud	https://cloud.google.com/blog/topics/threat-intelligence/	Google Cloud	26.02.2026, 18:28:40 test@test.ru	
☐	AnyRun	https://any.run/cybersecurity-blog/category/malware-analysis/	asdadf	25.02.2026, 15:53:24 test@test.ru	
☐	vp-test	http://vp-test.ru	vp-test	20.02.2026, 13:51:35 v.pavlichuk@rt-ib.ru	
☐	Telegram APT Reports	https://t.me/s/aptreports	Telegram APT Reports	11.02.2026, 17:49:09 d.yudanov@rt-ib.ru	
☐	Expert Blog Solar 4RAYS TEST QA	https://rt-solar.ru/solar-4rays/blog/	Expert Blog Solar 4RAYS TEST QA	22.10.2025, 19:17:52 QAAdmin@gmail.com	

Рисунок 128 – Список источников

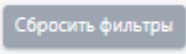
Информация на странице представлена в таблице со следующими полями:

- Кнопка выбора;
- Название;
- URL;
- Источник данных;
- Дата создания/Автор;
- Действия (Редактировать, проверить обновления, обновить целиком).

Для фильтрации информации предусмотрены следующие фильтры:

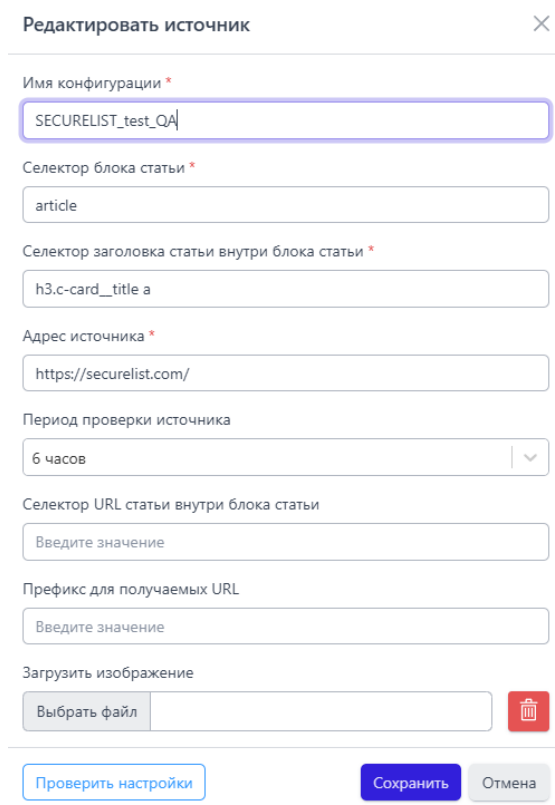
- Автор/пользователь;
- Дата создания/Изменения.

На странице представлены следующие иконки:

-  ;
-  (импортировать источники);
-  (экспортировать выбранные источники);
-  (создать источник).

При нажатии ЛКМ по названию источника происходит переход на страницу источника.

При нажатии в поле «Действия» по иконке редактирования источника открывается окно представленное на рисунке 129.



Редактировать источник

Имя конфигурации *

SECURELIST_test_QA

Селектор блока статьи *

article

Селектор заголовка статьи внутри блока статьи *

h3.c-card_title a

Адрес источника *

https://securelist.com/

Период проверки источника

6 часов

Селектор URL статьи внутри блока статьи

Введите значение

Префикс для получаемых URL

Введите значение

Загрузить изображение

Выбрать файл

Проверить настройки Сохранить Отмена

Рисунок 129 – Редактирование источника

В данном окне можно изменить параметры источника, проверить настройки, после чего сохранить изменения нажав по иконке «Сохранить».

На странице Источники в поле «Название» иконкой  показано что источник синхронизирован с данными полученными из источника данных взятого из статьи.

Иконка  показывает что синхронизация выполнена с ошибками, при этом при наведении указателя мыши на иконку. Во всплывающем окне приведен список ошибок синхронизации.

В области «Граф связей» можно просмотреть связи артефактов, упоминаемых в статье с другими артефактами.

При нажатии по иконке  на странице Лента угроз, открывается окно представленное на рисунке 130.

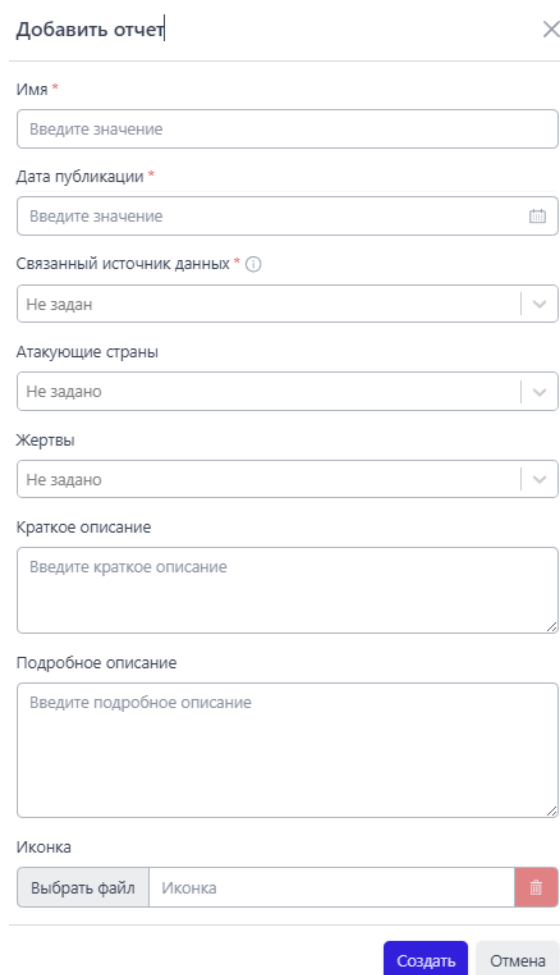
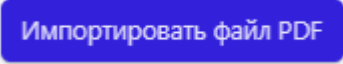


Рисунок 130 – Добавление отчета по источнику данных

После заполнения данных в данном окне требуется нажать по иконке «Создать», после чего обогащенный с помощью AI отчет по артефактам из указанного источника данных появиться в списке Лента угроз.

При нажатии по иконке , открывается окно представленное на рисунке 131.

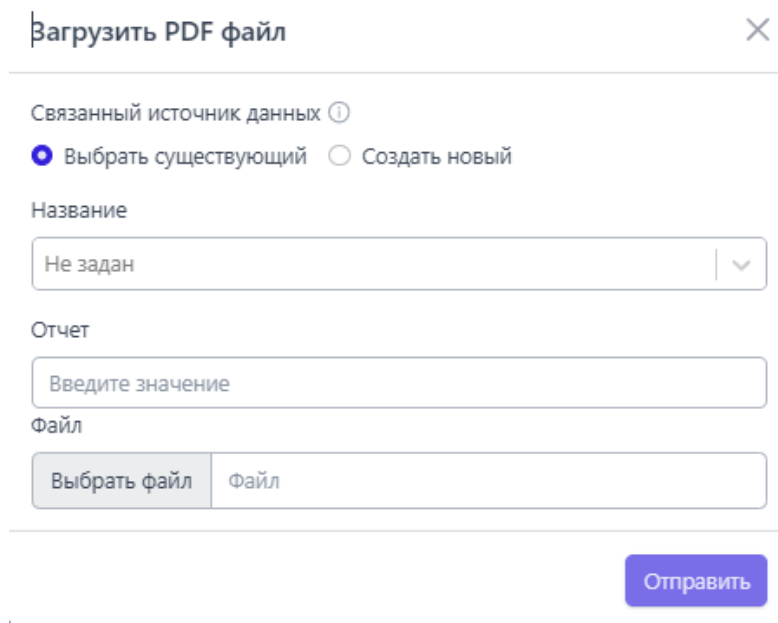


Рисунок 131 – Окно для указания информации при загрузке PDF файла

В данном окне можно выбрать источник данных, либо создать новый, к которому подкрепить PDF-файл с отчетом по артефактам, после нажатия по иконке отправить, обновиться запись в ленте угроз. В данной записи будет информация по артефактам упоминающимся в pdf-файле и отчет по ним.

6.5.12. Уязвимости

Общие сведения

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

Функционал включается/выключается лицензией.

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

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

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

Оценка серьезности уязвимости представлена по классификации CVSS (Common Vulnerability Scoring System) и на основе собственной системы оценки, на основе которой формируется критичность.

Уязвимости

Общий вид страницы зависит от выбранной вкладки (Уязвимости/Программы).

Общий вид страницы «Уязвимости» представлен на рисунке 132.

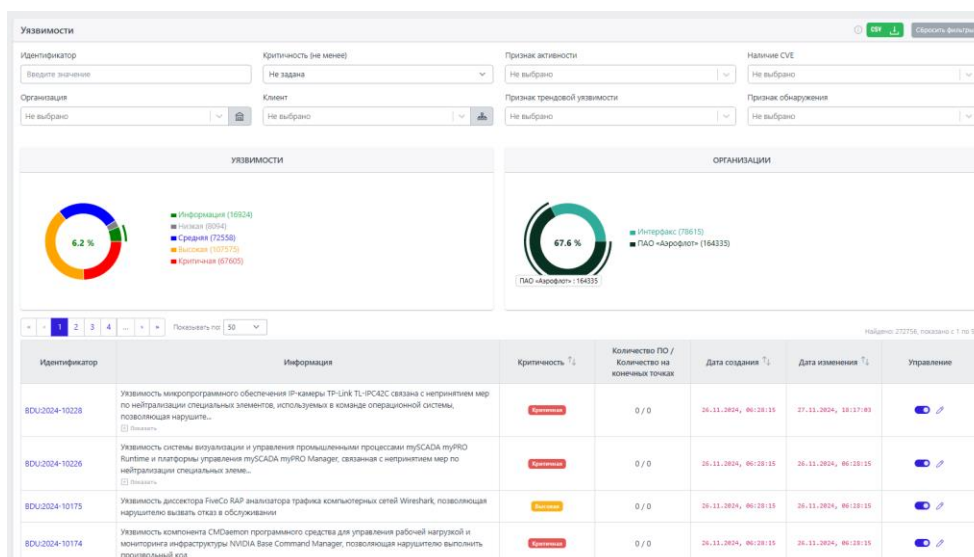


Рисунок 132 – Страница Уязвимости

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

Информация об уязвимостях берется из источников БДУ ФСТЭК и NIST, с которыми настроена постоянная синхронизация. Настройка параметров синхронизации с источниками прописываются при разворачивании портала RT Protect TI в конфигурационных файлах.

Таблица имеет следующие поля:

- Идентификатор (идентификация уязвимости по CVE);
- Информация (описание уязвимости);
- Критичность уязвимости;

— Количество ПО/Количество на конечных точках (в таблице отображается количество программ, в которых найдена данная уязвимость и количество конечных точек, на которых зарегистрировано ПО с данной уязвимостью);

- Дата создания;
- Дата изменения;
- Управление.

Для фильтрации информации в таблице имеются следующие фильтры:

- Идентификатор (в фильтре указывается идентификатор уязвимости в формате CVE или BDU);
- Критичность (низкая, ниже среднего, средняя, высокая, критичная);
- Признак активности (активирована, деактивирована);
- Наличие CVE (имеется, отсутствует);
- Организация;
- Клиент;
- Признак трендовой уязвимости (обычная уязвимость, трендовая уязвимость);
- Признак обнаружения (не обнаружено, обнаружено).

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

В столбце **Управление** можно деактивировать/активировать уязвимость, т.е. исключить из анализа программ. Данное действие производится с помощью иконок  / . Деактивация/активация уязвимости производится аналитиком/администратором на основании анализа информации об уязвимости.

В столбце **Управление** при нажатии по иконке редактирования  открывается окно, представленное на рисунке 133.

Редактировать уязвимость BDU:2024-07259

Критичность *

Средняя

Признак трендовой уязвимости *

Обычная уязвимость

Краткое описание уязвимости

Введите краткое описание

Подробное описание уязвимости

Введите подробное описание

Редактировать

Рисунок 133 – Окно редактирования информации по уязвимости

В данном окне можно изменить критичность уязвимости, выставить признак наличия трендовой уязвимости, а также добавить краткое и подробное описание уязвимости.

После добавления информации требуется нажать по иконке «Редактировать».

На странице **Уязвимости** представлена графическая область с отображением количества уязвимостей с распределением по критичности и организаций, в которых обнаружены программы с уязвимостями (рисунок 134).

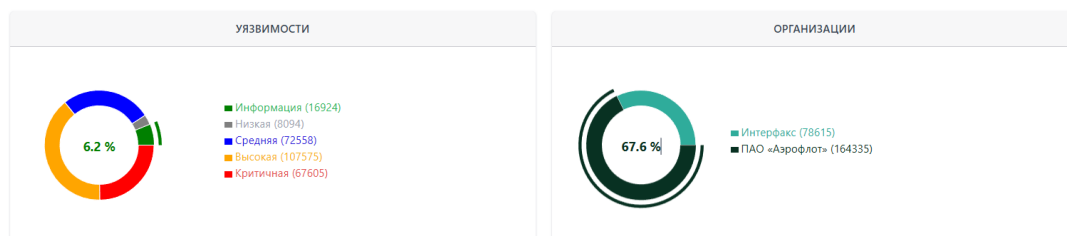
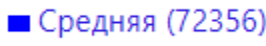


Рисунок 134 – Отображение обнаруженных уязвимостей и организаций

В данной области надписи с уровнями критичности уязвимости, а также указатели того, что уязвимости найдены или не найдены, являются активными ссылками, при нажатии по которым происходят переходы к соответствующим страницам.

Например, при нажатии по уровню критичности уязвимости  , на странице с уязвимостями отображаются только уязвимости с критичностью **Средняя**.

Также на странице **Уязвимости** можно выполнить сортировку по уязвимостям, нажав по иконкам:

-  сортировка по убыванию уровня критичности уязвимости (от более критичной к менее критичной);
-  сортировка по возрастанию уровня критичности (от менее критичной до более критичной).

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

При нажатии в столбце **Идентификатор** по CVE-идентификатору уязвимости открывается информация об уязвимости, представленная на рисунке 135.

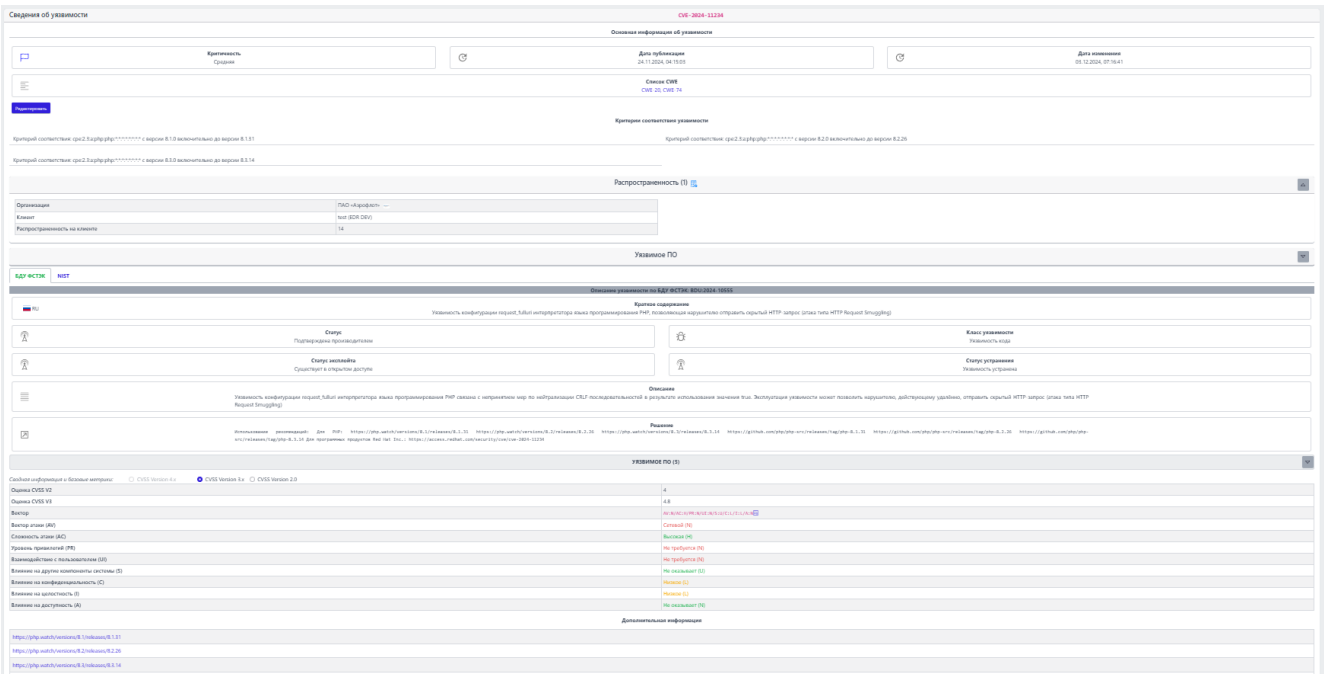


Рисунок 135 – Информация по уязвимости

На странице имеются следующие области с информацией по уязвимости:

- Основная информация по уязвимости;
- Критерии соответствия уязвимости;
- Распространенность;
- Уязвимое ПО;
- Описание уязвимости по БДУ ФСТЭК и NIST;
- Дополнительная информация.

В области основной информации по уязвимости указана критичность уязвимости, дата публикации и дата изменения, а также представлена ссылка, касающаяся уязвимости, перейдя по которой осуществляется вход на сайт <https://cwe.mitre.org>.

В области «Критерии соответствия уязвимости» указаны характеристики программы в CPE-формате, в которой найдены определенные уязвимости.

В области «Распространенность» показаны организации и клиенты, на которых установлены программы с найденными уязвимостями.

В области уязвимое ПО в табличном виде приведены программы, в которых найдена уязвимость.

Информация по уязвимости представлена в двух вкладках **БДУ ФСТЭК** и **NIST**.

Оценка уязвимости описана по стандартам CVSS v2 и CVSS v3. По данным стандартам имеются разные метрики оценки уязвимости.

CVSS предлагает простой инструментарий для расчета числового показателя по десятибалльной шкале, который позволяет специалистам по безопасности оперативно принимать решение о том, как реагировать на ту или иную уязвимость. Чем выше значение метрики, тем более оперативная реакция требуется.

Система оценки CVSS состоит из 3 метрик: базовая метрика, временная метрика и контекстная метрика. Каждая метрика представляет собой число (оценку) в интервале от 0 до 10 и вектор – краткое текстовое описание со значениями, которые используются для вывода оценки. Базовая метрика отображает основные характеристики уязвимости. Временная метрика соответствует таким характеристикам уязвимости, которые изменяются со временем, а контекстная метрика – характеристикам, которые уникальны для среды пользователя.

CVSS является понятным, прозрачным и общепринятым способом оценки IT-уязвимостей для руководителей, производителей приложений и средств поддержания информационной безопасности, исследователей и др.

Подробнее: <https://www.securitylab.ru/analytics/355336.php?ysclid=m4i5x7mbmb44314431>

Программы

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

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

В первом варианте название программы и их модификации отображаются по группам в формате CPE (см. рис 136).

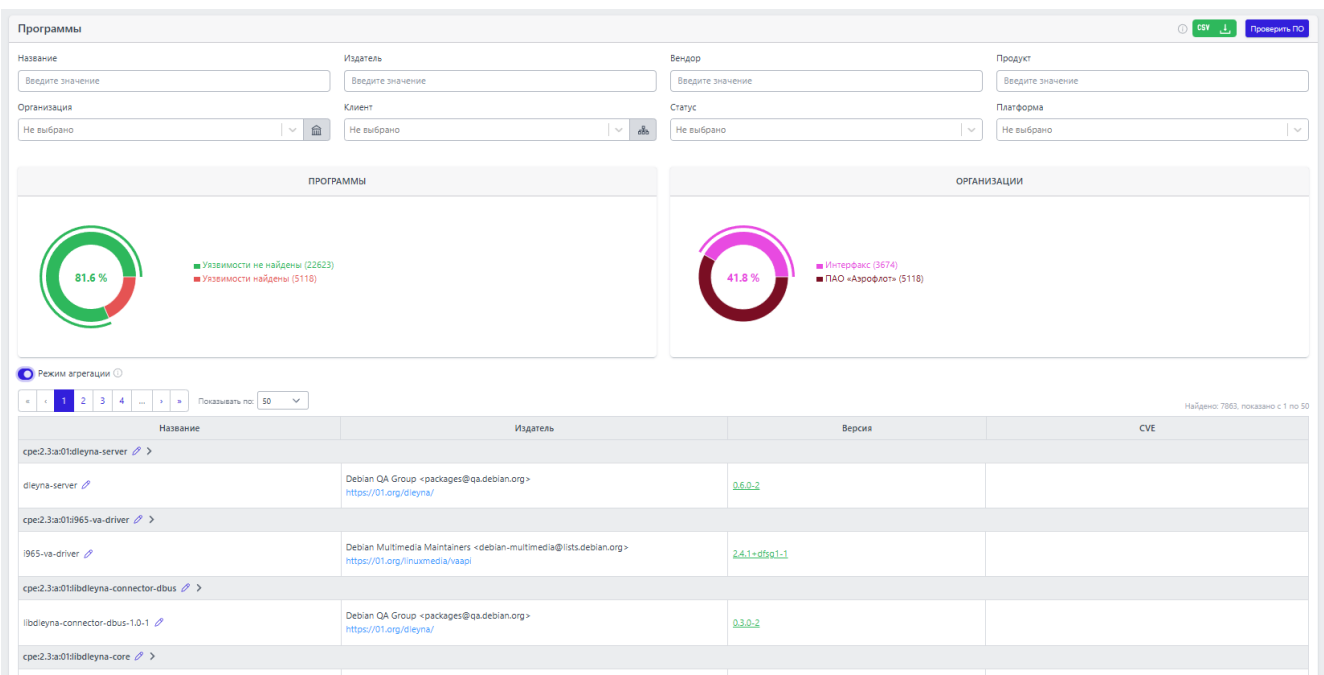


Рисунок 136 – Отображение страницы Программы
(название программы в формате CPE)

На странице имеются следующие области:

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

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

Таблица имеет следующие поля:

- Название (указывается идентификация программы в формате CPE);
- Издатель;
- Версия (версия ПО);
- CVE (описание уязвимостей, найденных для программы в формате CVE с указанием критичности);
- CPE (описание программ по стандарту для машиночитаемого именования и идентификации всех видов программного обеспечения (софта) и устройств).

В таблице **Программы**, если программа имеет несколько версий, в столбце CVE отображаются все уязвимости в формате CVE, найденные для программы (рисунок 137).

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

Рисунок 137 – Пример отображения таблицы с уязвимостями для версий программы

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

Во втором режиме отображения таблицы с проанализированными программами название программы отображается в обычном виде (рисунок 138).

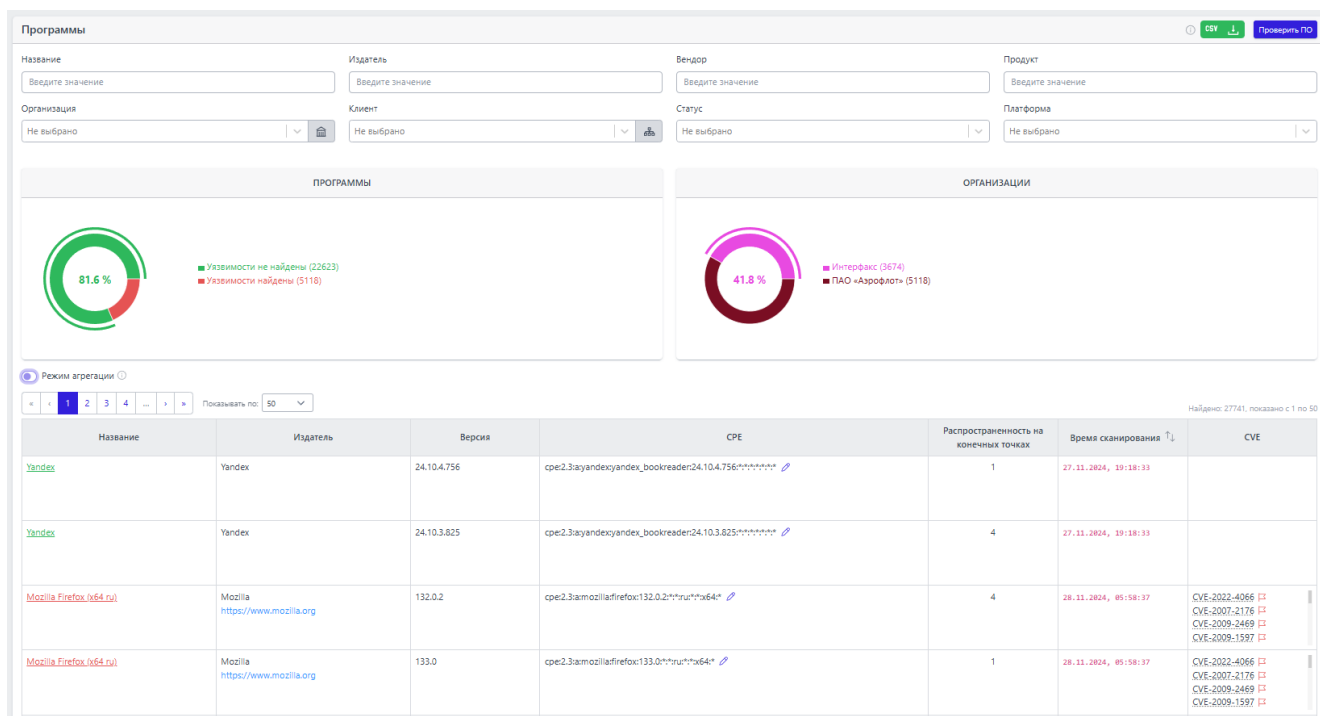


Рисунок 138 – Отображение страницы программы (название программы в обычном формате)

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

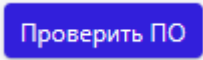
- Программы, в которых имеются уязвимости (шрифт красного цвета, например **Microsoft Edge**);
- Программы, в которых отсутствуют уязвимости (шрифт зеленого цвета, например **Windows SDK**).

Таблица имеет следующие поля:

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

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

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

В правом верхнем углу страницы **Программы** имеется иконка , при нажатии по которой отрывается окно для задания параметров для проверки новой программы, отсутствующей в списке (рисунок 139).

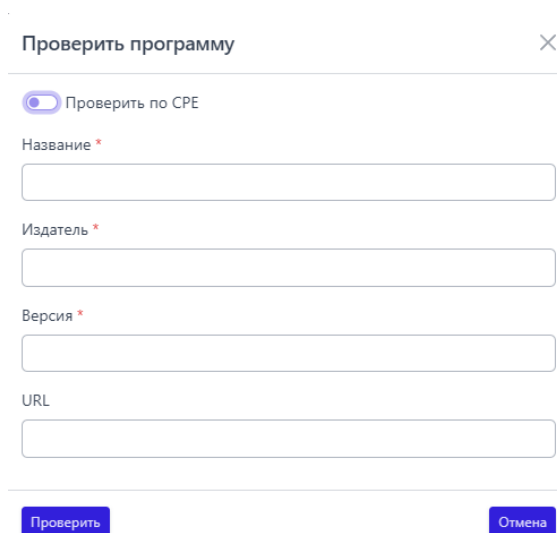


Рисунок 139 – Окно задания параметров проверяемой программы

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

Окно задания параметров для проверки программы при нажатии по иконке  Проверить по CPE имеет вид, представленный на рисунке 140.

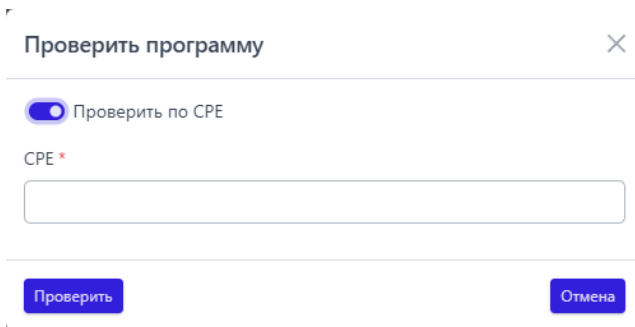
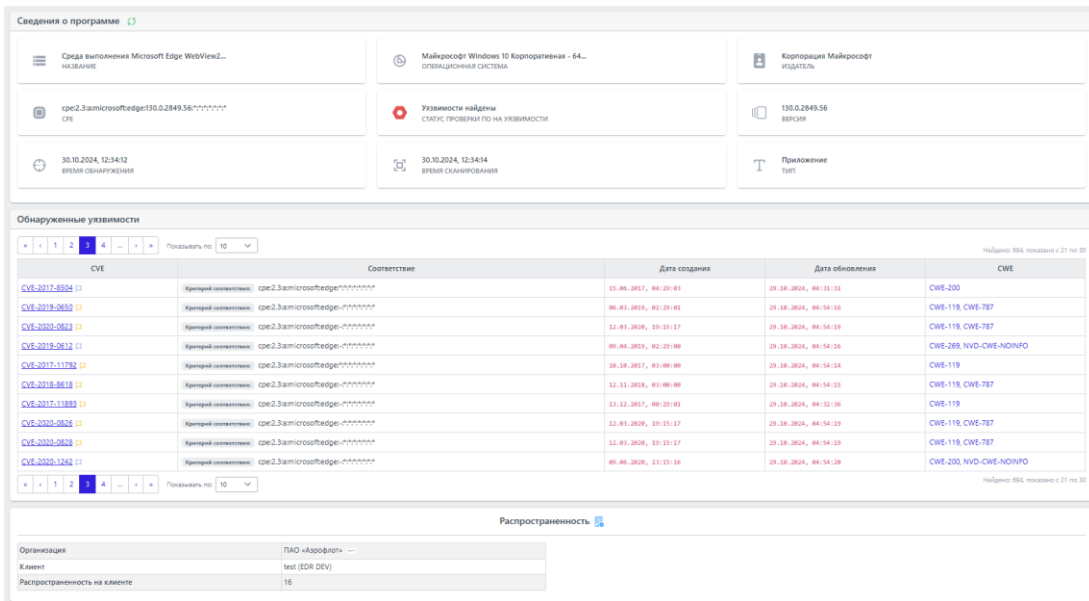


Рисунок 140 – Проверка программы, заданной в формате CPE

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

При нажатии по иконке с названием программы на странице **Программы**, происходит переход на страницу сведений о программе, представленную на рисунке 141.



CVE	Соответствие	Дата создания	Дата обновления	CWE
CVE-2017-8504	Критерий соответствия: cpe2.3:microsoftedge:*****	05.06.2017, 00:20:03	29.10.2024, 00:11:02	CWE-200
CVE-2019-2650	Критерий соответствия: cpe2.3:microsoftedge:*****	06.03.2019, 02:20:03	29.10.2024, 00:14:08	CWE-119, CWE-787
CVE-2020-2623	Критерий соответствия: cpe2.3:microsoftedge:*****	22.03.2020, 23:11:17	29.10.2024, 00:14:09	CWE-119, CWE-787
CVE-2019-2612	Критерий соответствия: cpe2.3:microsoftedge:*****	09.04.2019, 02:20:00	29.10.2024, 00:14:08	CWE-269, NVD-CWE-NONFO
CVE-2017-11792	Критерий соответствия: cpe2.3:microsoftedge:*****	28.10.2017, 03:00:00	29.10.2024, 00:14:04	CWE-119
CVE-2018-8618	Критерий соответствия: cpe2.3:microsoftedge:*****	22.11.2018, 03:00:00	29.10.2024, 00:14:05	CWE-119, CWE-787
CVE-2017-11992	Критерий соответствия: cpe2.3:microsoftedge:*****	23.12.2017, 00:20:03	29.10.2024, 00:12:06	CWE-119
CVE-2020-2626	Критерий соответствия: cpe2.3:microsoftedge:*****	22.03.2020, 23:11:17	29.10.2024, 00:14:09	CWE-119, CWE-787
CVE-2020-2628	Критерий соответствия: cpe2.3:microsoftedge:*****	22.03.2020, 23:11:17	29.10.2024, 00:14:09	CWE-119, CWE-787
CVE-2020-1242	Критерий соответствия: cpe2.3:microsoftedge:*****	09.06.2020, 23:11:16	29.10.2024, 00:14:08	CWE-200, NVD-CWE-NONFO

Рисунок 141 – Сведения о программе

На данной странице сведения о программе представлены в следующих областях:

- Общие сведения о программе;
- Таблица с обнаруженными уязвимостями;

— Распространенность (показывается распространенность программы с уязвимостями у различных клиентов).

В верхней части страницы сведений о программе имеется иконка , при нажатии по которой ЛКМ будет отправлена команда на повторное сканирование экземпляра ПО.

В столбце CPE имеется иконка  для редактирования названия программы в CPE-формате.

Идентификатор уязвимости в CVE-формате является активной ссылкой, при нажатии по которой открывается страница с описанием уязвимости, представленная на рисунке 142.

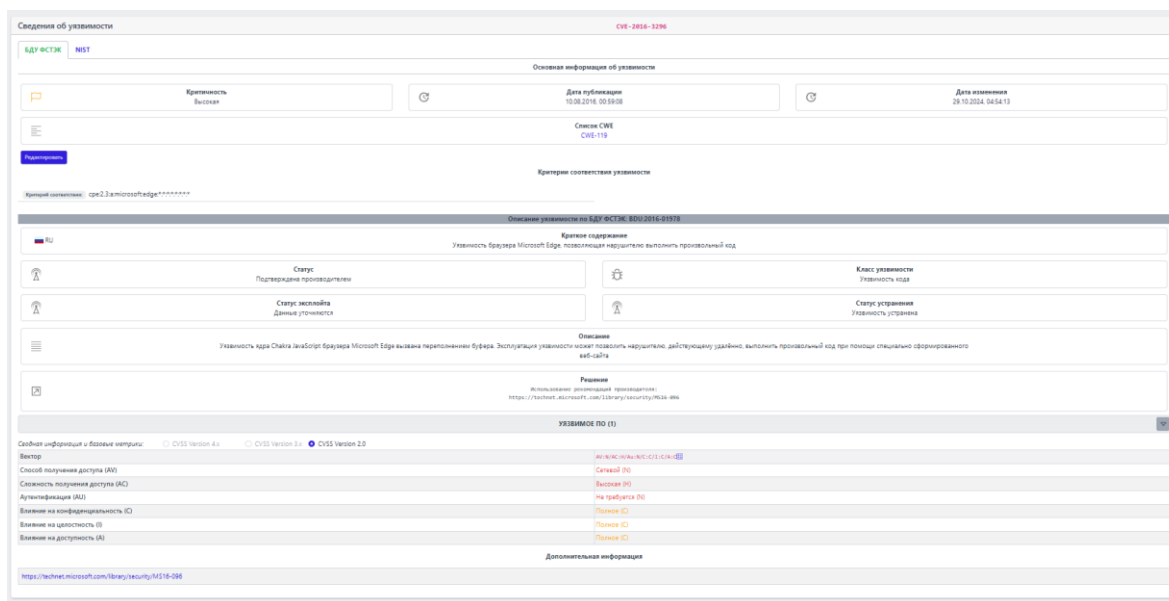
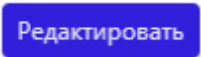


Рисунок 142 – Сведения о уязвимости

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

Для редактирования информации об уязвимости требуется нажать по иконке  , после чего откроется окно редактирования, представленное на рисунке 143.

Редактировать уязвимость BDU:2016-01978, CVE-2016-3296

Критичность *

Высокая

Признак трендовой уязвимости *

Обычная уязвимость

Краткое описание уязвимости

Введите краткое описание

Подробное описание уязвимости

Введите подробное описание

Редактировать

Рисунок 143 – Окно редактирования информации об уязвимости

На странице информации об уязвимости при нажатии по иконке [CWE-119](#) происходит переход на страницу с описанием уязвимости в CWE-формате.

6.5.13. Алгоритм формирования оценки артефакта

Алгоритм вычисления вердикта представляет собой сложную формулу, в которой присутствуют данные о вредоносности артефакта от различных источников.

Алгоритму вычисления вердикта по артефакту на вход передается следующий набор данных:

- заключение аналитика;
- список актуальных записей об артефакте во всех подключенных в TI-фидах;
- список актуальных отчетов по артефакту из всех анализаторов.

На выход алгоритм возвращает число, являющееся количественным показателем вредоносности оценки артефакта в диапазоне от -100 (гарантированно безопасен) до 100 (гарантированно вредоносен).

На основании полученной оценки высчитывается строгий вердикт по артефакту:

- от -100 до -20: вердикт - "Безопасный".
- от -20 до 20: вердикт - "Неизвестный".
- от 20 до 60: вердикт - "Подозрительный".

— от 60 до 100: вердикт - "Вредоносный".

Если источник локальный и загружается из файла, то устаревание для элементов сразу после загрузки файла начинает применяться. А если источник скачивается по ссылке, устаревание начинает работать в момент, когда артефакт пропадает из источника данных при очередном скачивании.

6.5.14. ИИ агент

Для ускорения и облегчения работы пользователей в программе RT Protect TI в версии программы 3.3.0 появилась возможность использовать ИИ агента.

ИИ агент реализован в виде отдельного сервиса, разворачиваемого при деплое RT Protect TI.

С помощью конфигуратора при создании файла config.yml необходимого для разворачивания сервиса RT Protect TI, возможно отметить в разделе «Параметры работы с модулем TI Reports» флаг включения интеграции с сервисами AI, после чего указать URL на котором развернут сервис AI-агента и ключ доступа к сервису (URL и ключ при On-Premise установке запрашиваются заказчиком у поставщика).

ИИ агент доступен для всех пользователей RT Protect TI в рамках ролевой модели.

Запросы к агенту и получение ответов ограничены ролевой моделью пользователя под которой был осуществлен доступ к RT Protect TI.

Сервис ИИ агента для формирования запросов и ответов, касающихся работы в RT Protect TI использует API RT Protect TI.

Пользователем при формировании запросов к ИИ агенту создается сессий которая видна только для данного пользователя.

Одновременно можно создавать несколько сессий.

Общий вид страницы чата с ИИ агентом представлен на рисунке 144.

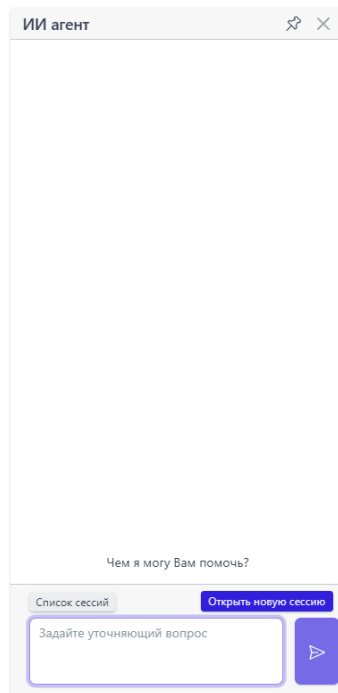


Рисунок 144 – Начало работы с ИИ агентом

Пример запроса к ИИ агенту и полученного ответа представлен на рисунке 145.

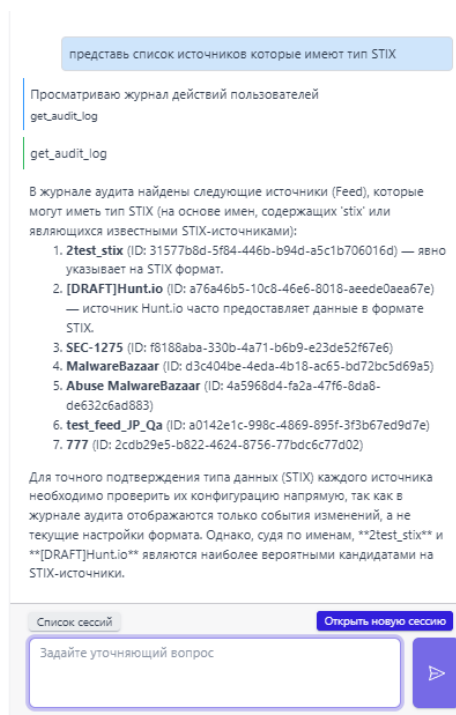


Рисунок 145 – Пример ответа от ИИ агента

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.

Функционал раздела **Аналитика EDR** может быть ограничен лицензией.



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 развиваться, однако ограничен рамками событий только одного агента.

Второй вариант не позволяет выполнить противодействие в режиме реального времени, т.к. требуется какое-то время, чтобы события, возникающие на агенте, были доставлены до сервера и обработаны им, перед тем как сервер сможет выполнить корреляцию.

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

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

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

Наборы индикаторов атак

Страница с наборами индикаторов атак (рис. 146) включает в себя следующие структурные элементы:

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

- применить изменения выбранного набора;
- удалять выбранные наборы.

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

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

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

Для добавления нового набора с индикаторами атак требуется нажать по иконке , после чего появиться окно представленное на рисунке 147.

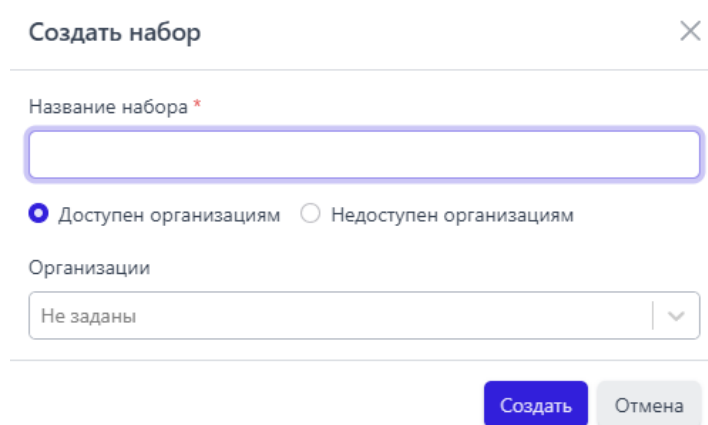


Рисунок 147 – Окно создания набора

В данном окне требуется ввести название набора с индикаторами атак и указать будет ли набор доступен всем, или только организациям, указанным при создании 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. 148).

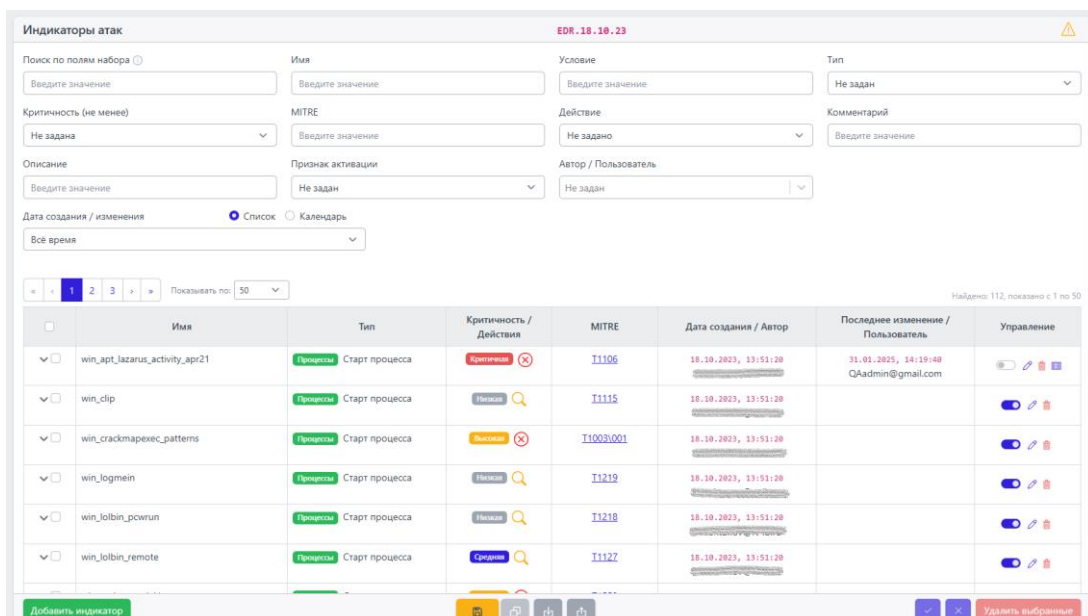


Рисунок 148 – Индикаторы атак

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;
- просмотреть историю изменений.

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

- **Поиск по полям набора** (Поиск осуществляется по подстроке без учета регистра в текстовых полях);
- **Имя;**

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

Для добавления нового индикатора атаки необходимо нажать кнопку **Добавить индикатор** в нижней части страницы. В открывшемся окне **Добавить индикатор** (рис. 149) следует прописать условия, на основании которых будет срабатывать правило.

Рисунок 149 – Добавление индикатора

После написания условия необходимо нажать кнопку **Добавить**. В нижней части страницы появится сообщение о добавлении нового правила (рис. 150).

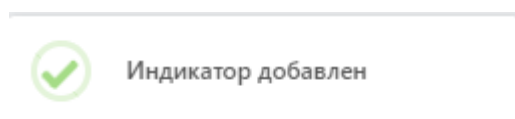


Рисунок 150 – Сообщение о добавлении индикатора атаки

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.151).

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

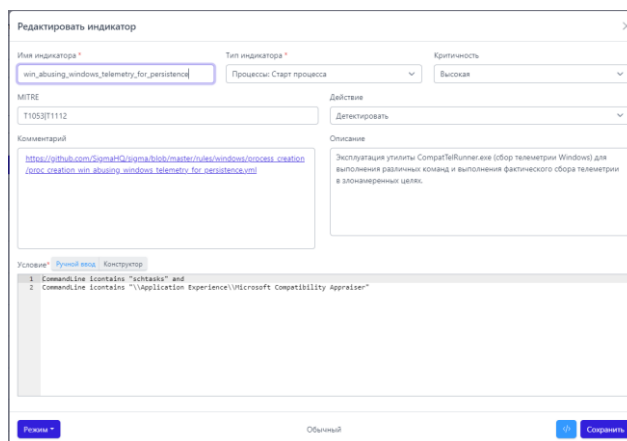


Рисунок 151 – Редактирование индикатора атаки

Для сохранения внесенных изменений необходимо нажать кнопку **Сохранить**, после чего в нижней части страницы появится сообщение об изменении правила (рис. 152).

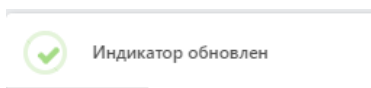


Рисунок 152 – Сообщение об обновлении индикатора атаки

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**.

Для просмотра истории изменений в правиле в наборе можно нажать по иконке , после чего происходит переход в окно «История изменений», где можно просмотреть историю изменений элементов аналитики (рисунок 153).

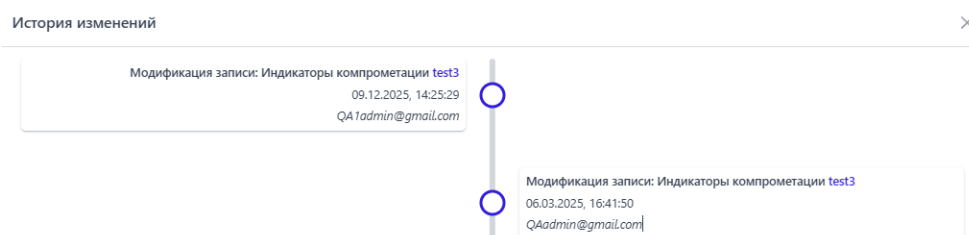


Рисунок 153 – История изменений

Для просмотра изменения требуется нажать левой кнопкой мыши в окошке «Модификация записи». После чего иконка  изменится на  и появится окошко с описанием измененного параметра.

Просмотр истории изменений предусмотрен для всех элементов аналитики и исключений.

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».

Наборы индикаторов компрометации

Страница **Индикаторы компрометации** представлена на рисунке 154. На странице отображаются наборы с индикаторами компрометации, сохраненные на сервере аналитики.

☐	Название набора	Доступен организациям	Количество записей	Дата создания / Автор	Дата изменения / Автор	Дата последнего сохранения	Действия
☐	string	Доступен всем	0	07.05.2025, 15:16:55		07.05.2025, 15:16:55	
☐	teteeteet	Доступен всем	2	15.04.2025, 16:10:30		15.04.2025, 16:10:30	
☐	qwefqwef	Доступен всем	9	17.03.2025, 14:54:12		17.03.2025, 14:54:12	
☐	asfbsdfb	Доступен всем	0	17.03.2025, 14:54:09		17.03.2025, 14:54:09	
☐	ewvqewv	Доступен всем	0	17.03.2025, 14:54:07		17.03.2025, 14:54:07	
☐	erfwereh	Доступен всем	0	17.03.2025, 14:54:03		17.03.2025, 14:54:03	
☐	vqewvqewv	Доступен всем	0	17.03.2025, 14:54:01		17.03.2025, 14:54:01	
☐	asdfasdf	Доступен всем	0	17.03.2025, 14:53:58		17.03.2025, 14:53:58	
☐	for_test_3	Доступен всем	0	22.04.2025, 17:22:36			
☐	for_test_2	Доступен всем	0	22.04.2025, 17:15:12			

Рисунок 154 – 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) Доступен организациям;
- 4) Количество записей;
- 5) Дата создания/Автор (показывает, когда и кто создал набор);
- 6) Дата изменения/Автор (показывает, когда и кто производил последние изменения с набором);
- 7) Дата последнего сохранения;
- 8) Действие (содержит кнопки **Редактировать** (позволяет редактировать название набора) и **Удалить**).

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

Удалить выбранные наборы.

Для фильтрации информации на странице предусмотрена следующая система фильтров:

- **Название набора;**
- **Поиск по полям набора** (Поиск осуществляется по подстроке без учета регистра в текстовых полях);
- **Автор/Пользователь;**
- **Дата создания/изменения.**

Для добавления нового набора индикаторов компрометации необходимо нажать кнопку **Добавить набор**, после чего в открывшемся окне **Создать набор** (рис. 155) в строке **Название** ввести название нового набора, выбрать если необходимо параметр будет ли набор являться теневым, и указать будет ли набор доступен всем организациям, или только организациям указанным при создании набора.

Рисунок 155 – Окно «Создать набор»

Для завершения операции добавления необходимо нажать кнопку **Создать**, после чего в нижней части страницы появится сообщение о добавлении набора (рис. 156), а строка с новым набором появится в таблице.



Рисунок 156 – Сообщение о добавлении набора

Для удаления одного или нескольких наборов индикаторов компрометации следует отметить флажками соответствующие им кнопки выбора , после чего нажать кнопку **Удалить выбранные наборы**.

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

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

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

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

- **Поиск по полям набора** (Поиск осуществляется по подстроке без учета регистра в текстовых полях);
- **Имя индикатора**;
- **Артефакт**;
- **Тип индикатора** (Не задан, Файл, SHA-256, IP адрес, Доменное имя, Сетевая сигнатура, SHA-1, MD 5, URL);
- **Комментарий**;
- **Признак активации** (на задано, Активировано, не активировано);
- **Автор/Пользователь**;
- **Дата создания/Изменения**.

Шапка таблицы с индикаторами содержит следующие поля:

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

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

В нижней части таблицы индикаторов находятся кнопки операций с индикаторами:

- 1) **Добавить индикатор** ;
- 2) Импортировать CSV-файл –  ;
- 3) Экспортировать набор в файл формата CSV;
- 4) Удалить индикатор или индикаторы **Удалить выбранные** .

Для добавления индикатора в области **Индикаторы компрометации** необходимо нажать кнопку **Добавить индикатор** . Далее в открывшемся окне **Добавить индикатор** (рис. 157) следует заполнить поля, обязательными для заполнения из которых являются поля **Имя индикатора**, **Тип артефакта** и **Артефакт**, после чего нажать кнопку **Добавить** .

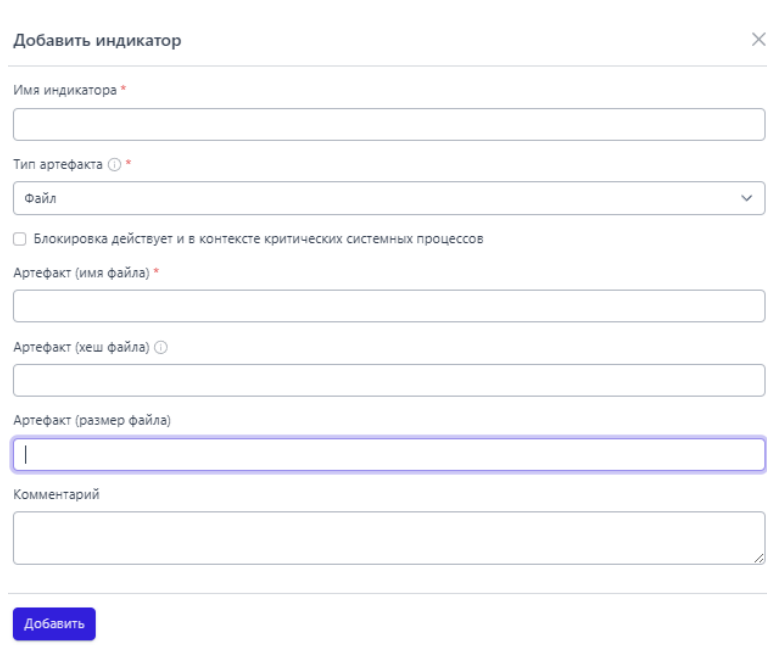


Рисунок 157 – Окно «Добавить индикатор»

В нижней части страницы появится сообщение о добавлении индикатора компрометации (рис. 158).

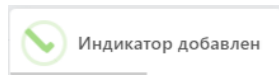


Рисунок 158 – Сообщение о добавлении индикатора

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

Для импорта данных из файла с индикаторами следует нажать кнопку  **Импортировать CSV или json-файл**. После нажатия кнопки открывается окно файлового менеджера, в котором необходимо выбрать импортируемый файл, после чего импортировать данные из файла в выбранный набор индикаторов компрометации. После завершения операции импорта индикаторы компрометации из импортируемого файла добавятся в выбранный набор индикаторов компрометации.

6.6.3. Журналы

Общая информация

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

Наборы с журналами

Страница с наборами журналов (рис. 159) открывается при выборе на панели слева раздела **Журналы** и включает в себя следующие структурные элементы:

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

Журналы

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

Дата создания / изменения: ☒ Список ☐ Календарь

Всё время

Показывать по: 10

Название набора	Доступен организациям	Количество записей	Дата создания / Автор	Дата изменения / Автор	Дата последнего сохранения	Действия
1111	Доступен всем	2	17.03.2025, 15:40:00		17.03.2025, 15:40:00	
21312	Доступен всем	1	17.03.2025, 15:37:43		17.03.2025, 15:37:43	
Irina_Test	Доступен всем	1	18.03.2025, 16:49:19		18.03.2025, 16:49:19	
123	Доступен всем	5	17.02.2025, 17:47:20		03.03.2025, 18:19:43	
test-qa	Доступен всем	4	30.01.2025, 11:50:42		03.03.2025, 18:20:15	
test_api	Доступен всем	3	19.11.2024, 17:33:19		19.11.2024, 17:33:19	
PMI_Test_1.1	Доступен всем	2	11.11.2024, 19:24:32		19.11.2024, 17:13:50	
WinEvt-Test	Доступен всем	0	03.09.2024, 17:58:33		03.09.2024, 17:58:33	
test_QA1	Доступен всем	3	09.08.2024, 17:27:05	29.01.2025, 17:33:38	30.01.2025, 10:54:42	
tgntg	Доступен всем	0	17.07.2024, 14:06:56		17.07.2024, 14:06:56	

Найдено 20, показано с 1 по 10

Добавить набор Удалить выбранные

Рисунок 159 – Наборы с журналами

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

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

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

При нажатии ЛКМ на имени набора открывается страница **Журналы** для выбранного набора (рис. 160).

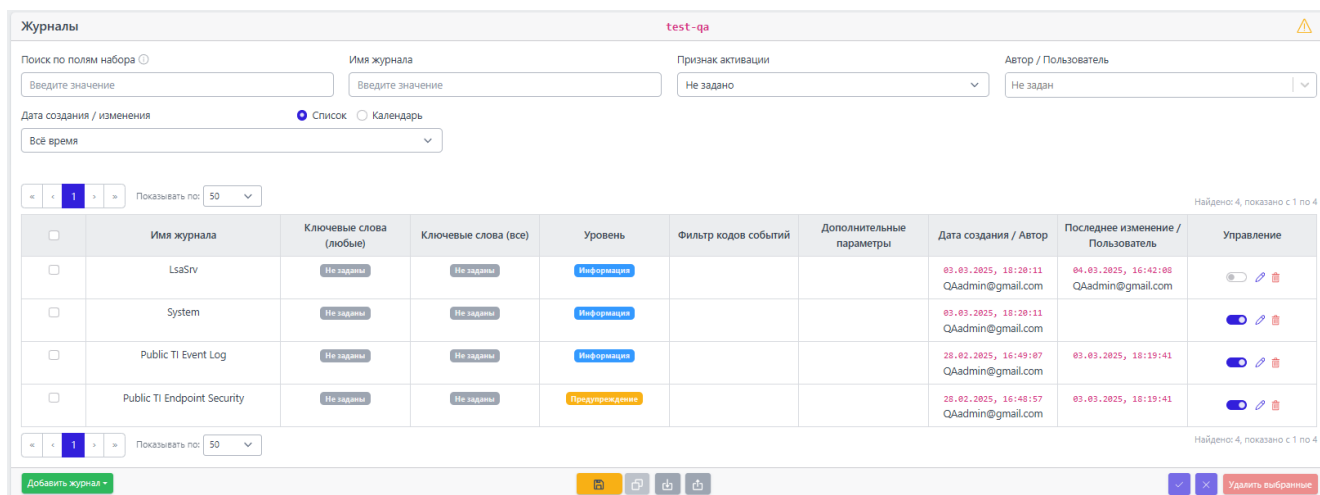


Рисунок 160 – Страница «Журналы» выбранного набора

Страница «Журналы»

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

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

Для фильтрации информации на странице используется следующая система фильтров:

- **Поиск по полям набора** (Поиск осуществляется по подстроке без учета регистра в текстовых полях);
- **Имя журнала**;
- **Признак активации**;
- **Автор/Пользователь**;
- **Дата создания/изменения**.

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

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

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

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

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

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

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

6.6.4. Yara-правила (файлы)

Общая информация

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

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

Наборы YARA-правил (файлы)

Страница с наборами YARA-правил для файлов (рис. 161) включает в себя следующие структурные элементы:

— таблица с наборами YARA-правил;

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

YARA-правила (файлы)

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

Дата создания / изменения: ☒ Список ☐ Календарь

Всё время

Показывать по: 10

Название набора	Доступен организациям	Количество записей	Дата создания / Автор	Дата изменения / Автор	Дата последнего сохранения	Действия
☐ set_sk	Доступен всем	9	22.04.2025, 17:01:03		22.04.2025, 17:02:26	
☐ Irlng_Test	Доступен всем	0	10.03.2025, 16:53:43		10.03.2025, 16:53:43	
☐ проверка_2	Доступен всем	1	24.01.2025, 12:06:04		24.01.2025, 12:11:48	
☐ Проверка	Доступен всем	28	24.01.2025, 11:59:39		28.02.2025, 16:55:55	
☐ ABC	Доступен всем	1	20.11.2024, 14:11:26		14.04.2025, 16:59:00	
☐ abcd	Доступен всем	0	12.11.2024, 17:25:54	18.11.2024, 14:15:44	03.03.2025, 18:22:14	
☐ test	Доступен всем	1	12.11.2024, 17:24:11		12.11.2024, 17:24:12	
☐ PMI_Test_1.1	Доступен всем	1	11.11.2024, 19:50:40		11.11.2024, 19:52:52	
☐ 111	Доступен всем	0	06.11.2024, 14:17:03		06.11.2024, 14:17:16	
☐ new_name	Доступен всем	0	06.11.2024, 12:10:22	06.11.2024, 12:10:39	06.11.2024, 12:10:22	

Добавить набор

Удалить выбранные

Экспортируемые наборы из основного раздела

Рисунок 161 – Наборы YARA-правил (файлы)

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

- **Название набора**;
- **Поиск по полям набора** (Поиск осуществляется по подстроке без учета регистра в текстовых полях);
- **Автор/Пользователь**;
- **Дата создания/Изменения**.

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

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

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

Страница «YARA-правила (файлы)»

При нажатии ЛКМ по имени набора открывается страница **YARA-правила (файлы)** для выбранного набора (рис. 162).

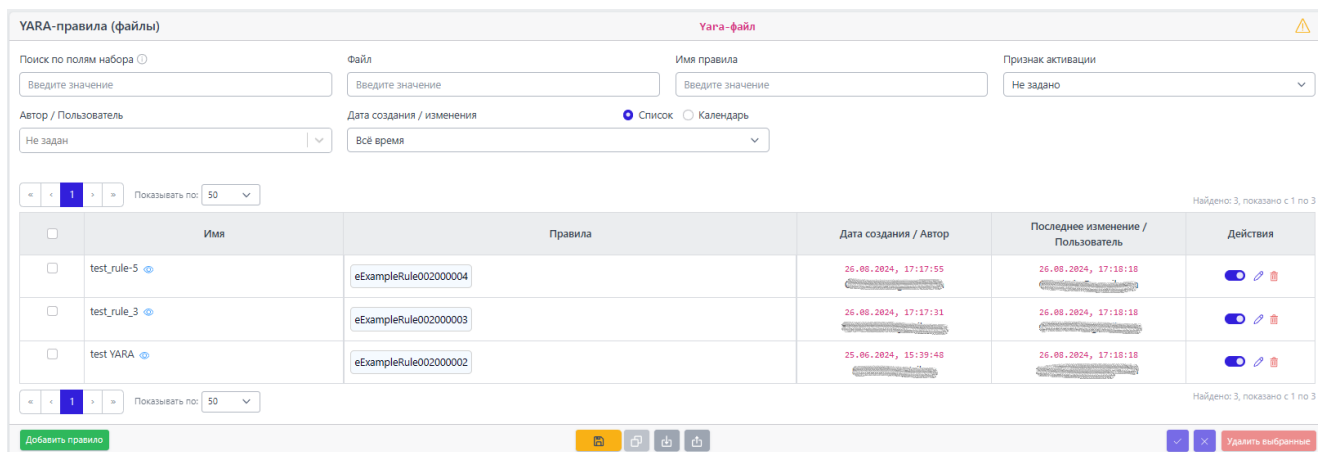


Рисунок 162 – YARA-правила (файлы)

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

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

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

- **Поиск по полям набора** (Поиск осуществляется по подстроке без учета регистра в текстовых полях);
- **Файл**;
- **Имя правила**;
- **Признак активации**;

- Автор/Пользователь;
- Дата создания/изменения.

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

Подробная информация о синтаксисе YARA содержится в документе «Руководство аналитика RT Protect EDR» и [официальной документации YARA](#). Пример правила YARA приведен на рисунке 163.

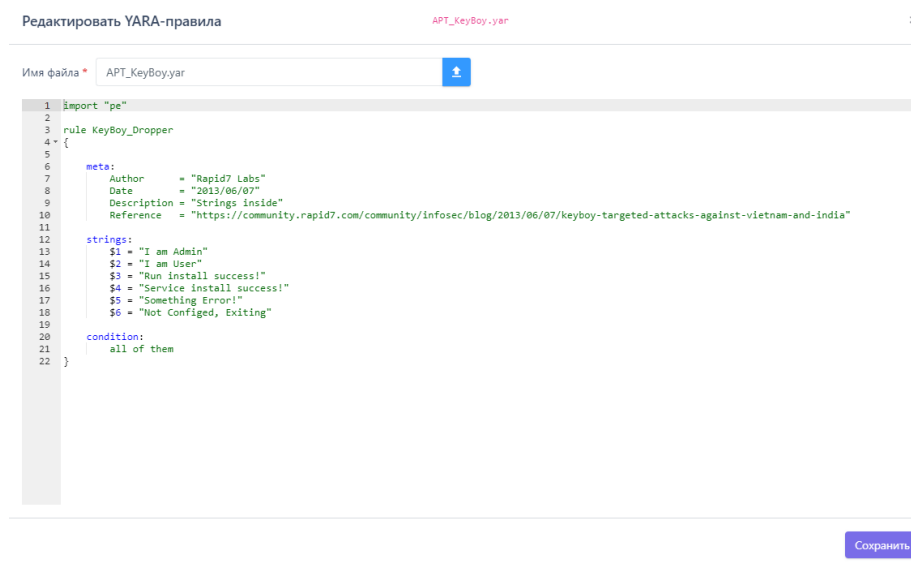


Рисунок 163 – Пример правила YARA

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

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

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

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

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

Для удаления правил из набора необходимо удалить правила по отдельности с помощью кнопки **Удалить** (🗑️).

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

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

- Имя файла;
- Имя правила.

6.6.5. Yara-правила (память)

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

Наборы YARA-правил (память)

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

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

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

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 (память), предусмотрены следующие фильтры:

- **Поиск по полям набора** (Поиск осуществляется по подстроке без учета регистра в текстовых полях);
- **Файл**;
- **Имя правила**;
- **Признак активации**;
- **Автор/Пользователь**;
- **Дата создания/Изменения**.

6.7 Исключения EDR

В области **Исключения EDR** содержатся разделы:

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

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

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

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

6.7.1. Исключения для программ

Общая информация

На странице с наборами исключений для программ (рис. 164) 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.

Исключения для программ

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

Дата создания / изменения: ☒ Список ☐ Календарь

Всё время

Показывать по: 10

☐	Название набора	Доступен организациям	Количество записей	Дата создания / Автор	Дата изменения / Автор	Дата последнего сохранения	Действия
☐	test	Доступен всем	5	14.03.2025, 14:18:18		14.03.2025, 14:18:18	✎ ✖
☐	testff	Доступен всем	22	14.03.2025, 12:23:44		14.03.2025, 12:23:44	✎ ✖
☐	лимиты полей	Доступен всем	6	06.03.2025, 18:02:33		06.03.2025, 18:09:42	✎ ✖
☐	vp-test	Доступен всем	4	28.02.2025, 20:23:51		28.02.2025, 20:23:51	✎ ✖
☐	test	Доступен всем	151	19.02.2025, 18:28:52	19.02.2025, 18:29:14	03.03.2025, 18:24:27	✎ ✖
☐	test_set1	Доступен всем	20	19.02.2025, 17:21:45		26.02.2025, 16:45:17	✎ ✖
☐	test_flags	Доступен всем	7	19.02.2025, 11:57:50		19.02.2025, 14:59:38	✎ ✖
☐	123	Доступен всем	11	12.02.2025, 15:01:27		03.03.2025, 18:24:11	✎ ✖
☐	for-test	Доступен всем	27	05.02.2025, 12:21:49		19.02.2025, 15:01:50	✎ ✖
☐	1	Доступен всем	13	05.02.2025, 10:19:55		19.02.2025, 15:12:30	✎ ✖

Добавить набор

Удалить выбранные

Рисунок 164 – Наборы исключений для программ

Наборы исключений для программ

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

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

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

- **Название набора**;
- **Поиск по полям набора** (Поиск осуществляется по подстроке без учета регистра в текстовых полях);
- **Автор/Пользователь**;
- **Дата создания/Изменения**.

Чтобы добавить новый набор с исключениями для программ, необходимо нажать кнопку **Добавить набор**, после чего ввести название нового набора, а так же указать будет ли доступен набор всем организациям, или только организациям указанным при создании набора. Для завершения операции необходимо нажать кнопку **Добавить**.

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

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

Для перехода к странице Исключения для программ необходимо нажать ЛКМ на имени набора в поле Название набора.

Страница «Исключения для программ»

На странице **Исключения для программ** (рис. 165) можно выполнять следующие операции:

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

Исключения для программ

for-test

Поиск по полям набора

Введите значение

Признак активации

Не задано

Автор / Пользователь

Не задан

Дата создания / изменения

Всё время

Список

Календарь

«

1

»

Показывать по:

50

Найдено: 27, показано с 1 по 27

☐	Тип	Значение	Флаги	Издатель ЭП	Правила	Комментарий	Дата создания / Автор	Последнее изменение / Пользователь	Управление
☐	Командная строка	schtasks.exe /Create /tn "Microsoft\Office\Office ClickToRun Service Monitor" /XML "\C:\Program Files\Common Files\Microsoft Shared\ClickToRun\Service Watcher\Schedule.xml" /schtas ks.exe /Create /tn "Microsoft\Office\Office ClickToRun Servi * [img alt="lock icon" data-bbox="238 645 248 655"/>	Исключение из телеметрии файловых событий				27.02.2025, 18:23:23 QAdmin@gmail.com		
☐	Командная строка	* * * [img alt="lock icon" data-bbox="215 680 225 690"/>	Исключение из телеметрии файловых событий				27.02.2025, 17:55:17 QAdmin@gmail.com		
☐	Командная строка	* * * [img alt="lock icon" data-bbox="215 740 225 750"/>	Исключение из телеметрии файловых событий	Microsoft Windows Hardware Compatibility Publisher_Microsoft Windows Hardware Compatibility Publisher_Microsoft Windows Hardware Compatibility Publisher_Microsoft Windows Hardware Compatibility Publisher_Microsoft Windows Hardware Compatibility Publisher1			27.02.2025, 17:41:31 QAdmin@gmail.com		

Рисунок 165 – Исключения для программ определенного набора

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

- Поиск по полям набора (Поиск осуществляется по подстроке без учета регистра в текстовых полях);
- Признак активации;
- Автор/Пользователь;
- Дата создания/Изменения.

Для добавления в набор нового исключения для программы необходимо нажать кнопку **Добавить исключение** и в открывшемся списке выбрать тип добавляемого исключения: **Файл**, **Хеш** или **Командная строка** (рис. 166).

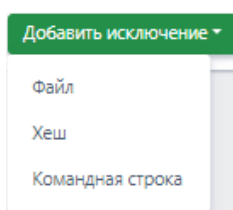


Рисунок 166 – Добавить исключение для программ (выбор типа)

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. 167).

Рисунок 167 – 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. 168).

Рисунок 168 – 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. 169).

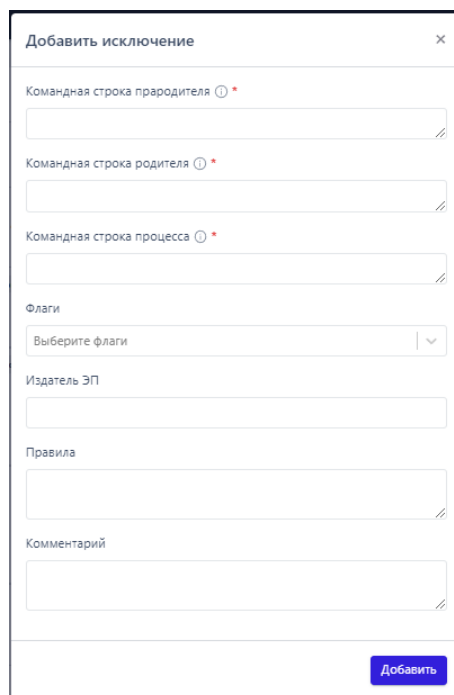


Рисунок 169 – Добавление исключения для программы (тип «Командная строка»)

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

Исключения для файлов

Сбросить фильтры

Название набора

Поиск по полям набора

Автор / Пользователь

Введите значение

Введите значение

Не задан

Дата создания / изменения

Список

Календарь

Всё время

«

1

2

3

4

»

Показывать по: 10

Найдено: 34, показано с 1 по 10

☐	Название набора	Доступен организациям	Количество записей	Дата создания / Автор	Дата изменения / Автор	Дата последнего сохранения	Действия
☐	itina	Доступен всем	1	04.04.2025, 12:00:13		04.04.2025, 12:00:13	
☐	для импорта	Доступен всем	6	06.03.2025, 17:39:14		06.03.2025, 17:39:46	
☐	test_0011	Доступен всем	7	19.02.2025, 16:14:22	19.02.2025, 16:38:53	06.03.2025, 17:27:36	
☐	test_ip+_1	Доступен всем	8	13.02.2025, 16:38:20		13.02.2025, 16:38:20	
☐	test_ip	Доступен всем	10922	13.02.2025, 16:16:25		03.03.2025, 18:25:46	
☐	test_ip	Доступен всем	18	15.01.2025, 18:53:57		04.03.2025, 18:53:01	
☐	test	Доступен всем	6	13.01.2025, 17:51:11		13.01.2025, 17:51:11	
☐	test#903	Доступен всем	0	05.03.2025, 15:22:22		16.05.2025, 15:10:07	
☐	TestFileExcl_123	Доступен всем	10	03.03.2025, 17:40:06	29.04.2025, 17:13:03	16.05.2025, 15:06:30	
☐	set(shadow)	Доступен всем	100	20.12.2024, 16:22:00		14.05.2025, 23:00:38	

«

1

2

3

4

»

Показывать по: 10

Найдено: 34, показано с 1 по 10

Добавить набор

Удалить выбранные

Рисунок 170 – Наборы исключений для файлов

Наборы исключений для файлов

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

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

Чтобы добавить новый набор с исключениями для файлов, необходимо нажать кнопку **Добавить набор**, после чего ввести название нового набора, указать признак будет ли набор теневым, а так же указать будет ли доступен набор всем организациям, или только организациям указанным при создании набора.

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

- **Название набора**;
- **Поиск по полям набора** (Поиск осуществляется по подстроке без учета регистра в текстовых полях);
- **Автор/Пользователь**;
- **Дата создания/Изменения**.

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

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 **Исключения для файлов** необходимо нажать ЛКМ на имени набора в поле **Название набора**.

Страница «Исключения для файлов»

На странице **Исключения для файлов** (рис. 171) можно выполнять следующие операции:

- просматривать исключения для файлов в выбранном наборе;
- добавлять новое исключение по имени файла;

- Исключения для файлов**

Поиск по полнм набору Значение Тип Комментарий

Введите значение Введите значение Не задано Введите значение

Действие Признак активации Автор / Пользователь

Не задан Не задано Не задан

Дата создания / изменения ☒ Список ☐ Календарь

Все время

Показывать по 10

	Тип	Значение	Действие	Флаги	Комментарий	Дата создания / Автор	Последнее изменение / Пользователь	Управление
☐	файл	test005.exe	Безопасность	Не останавливать службу Безопасность действует и в режиме критического состояния системы		05.03.2025, 14:15:25 QAdmin@gmail.com		☒ <input type="edit"/>
☐	MDX	03a2d54d310a43ce548f2acc32b91	Результат		test	05.03.2025, 14:15:25 QAdmin@gmail.com		☒ <input type="edit"/>
☐	файл	test2.exe	Безопасность	Не останавливать службу Безопасность действует и в режиме критического состояния системы		05.03.2025, 14:15:25 QAdmin@gmail.com		☒ <input type="edit"/>
☐	файл	test1.exe	Безопасность	Не останавливать службу Безопасность действует и в режиме критического состояния системы		05.03.2025, 14:15:25 QAdmin@gmail.com		☒ <input type="edit"/>
☐	файл	test3.exe	Безопасность	Не останавливать службу Безопасность действует и в режиме критического состояния системы		05.03.2025, 14:15:25 QAdmin@gmail.com		☒ <input type="edit"/>
☐	файл	test4.exe	Безопасность	Не останавливать службу Безопасность действует и в режиме критического состояния системы		05.03.2025, 14:15:25 QAdmin@gmail.com		☒ <input type="edit"/>
☐	SHA-1	02963557677bdca3ef6d7715c731a31ed713307a	Результат		test	05.03.2025, 14:15:25 QAdmin@gmail.com		☒ <input type="edit"/>
☐	SHA-256	070be6415923ae6ec04466a2b94616de1fdd53e107aed2ebcf5f9a74ee33700	Безопасность	Не останавливать службу Безопасность действует и в режиме критического состояния системы	test	05.03.2025, 14:15:25 QAdmin@gmail.com	04.03.2025, 17:27:23 QAdmin@gmail.com	☒ <input type="edit"/>
☐	MDX	03a2d54d310a43ce548f2acc32b91	Результат		test	04.03.2025, 14:12:04 QAdmin@gmail.com	04.03.2025, 14:51:30 QAdmin@gmail.com	☒ <input type="edit"/>
☐	SHA-1	02963557677bdca3ef6d7715c731a31ed713307a	Результат		test	04.03.2025, 14:13:32 QAdmin@gmail.com		☒ <input type="edit"/>

Показывать по 10

Добавить исключение

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

- Руководство администратора RT Protect TI
Версия 1.0.35 от 19 июня 2026

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. 172).

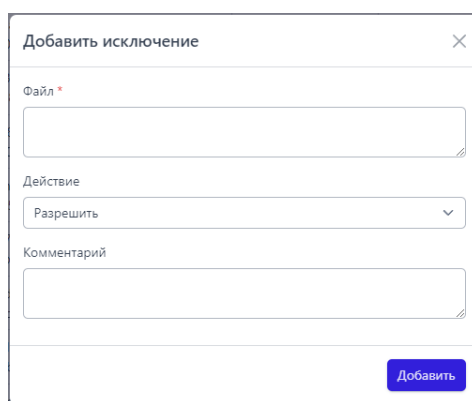
The screenshot shows a dialog box titled "Добавить исключение" (Add exception) with a close button (X) in the top right corner. Inside the dialog, there are three main sections: "Файл *" (File) with a text input field, "Действие" (Action) with a dropdown menu currently set to "Разрешить" (Allow), and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

Рисунок 172 – 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. 173).

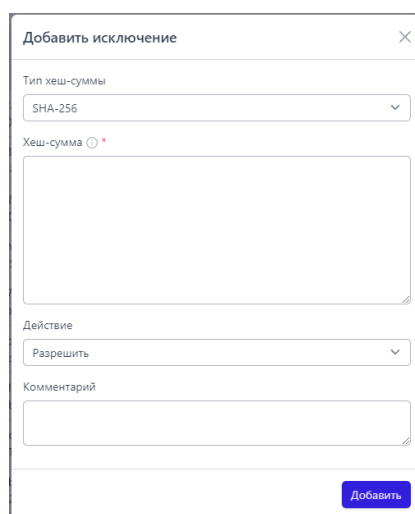
The screenshot shows a dialog box titled "Добавить исключение" (Add exception) with a close button (X) in the top right corner. Inside the dialog, there are four main sections: "Тип хеш-суммы" (Hash type) with a dropdown menu set to "SHA-256", "Хеш-сумма" (Hash) with a large text input field, "Действие"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

Рисунок 173 – Добавление исключения для файла (тип «Хеш»)

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

Имена файлов после добавления исключения будут отображаться в таблице **Исключения для файлов** в поле **Значение**, а в поле **Тип** будет указан тип исключения.

Тип хеш-суммы — в поле устанавливается тип хеш-суммы исполняемого файла. В программе предусмотрены следующие типы хеш-сумм для добавления файлов в исключения: **SHA-256, SHA-1 и MD5**.

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

Комментарий — в поле прописывается произвольный комментарий. Для добавления новой программы-исключения по имени файла или хеш-сумме комментарий не является обязательным параметром. Комментарий после добавления исключения будет отображаться в таблице **Исключения для программ** в поле **Комментарий**.

Для завершения операции добавления исключения для программы необходимо после ввода информации в окне **Добавить исключение** нажать кнопку **Добавить**.

Чтобы удалить исключение для файла, необходимо отметить одно или несколько исключений, установив флажок в кнопке выбора, и нажать кнопку **Удалить выбранные**. Также можно удалить исключение из набора с помощью кнопки **Удалить** (). Для внесения изменений в исключение для файла необходимо нажать кнопку **Редактировать** ( в соответствующей строке таблицы **Исключения для файлов** и в открывшемся окне **Редактировать исключение** изменить необходимую информацию. Для завершения редактирования необходимо нажать кнопку **Сохранить** ( после внесения изменений в редактируемый элемент.

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

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

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

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

6.7.3. Сетевые исключения

Общая информация

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

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

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

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

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

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

Наборы сетевых исключений

Страница **Сетевые исключения** содержит наборы с сетевыми исключениями и включает в себя следующие структурные элементы (рис. 174):

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

Рисунок 174 – Страница наборов сетевых исключений

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

- **Название набора**;
- **Поиск по полям набора** (Поиск осуществляется по подстроке без учета регистра в текстовых полях);
- **Автор/Пользователь**;
- **Дата создания/Изменения**.

Чтобы добавить новый набор с сетевыми исключениями, необходимо нажать кнопку **Добавить набор**, после чего ввести название нового набора, указать признак будет ли набор теневым, а так же указать будет ли доступен набор всем организациям, или только организациям указанным при создании набора.

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. 175) 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.

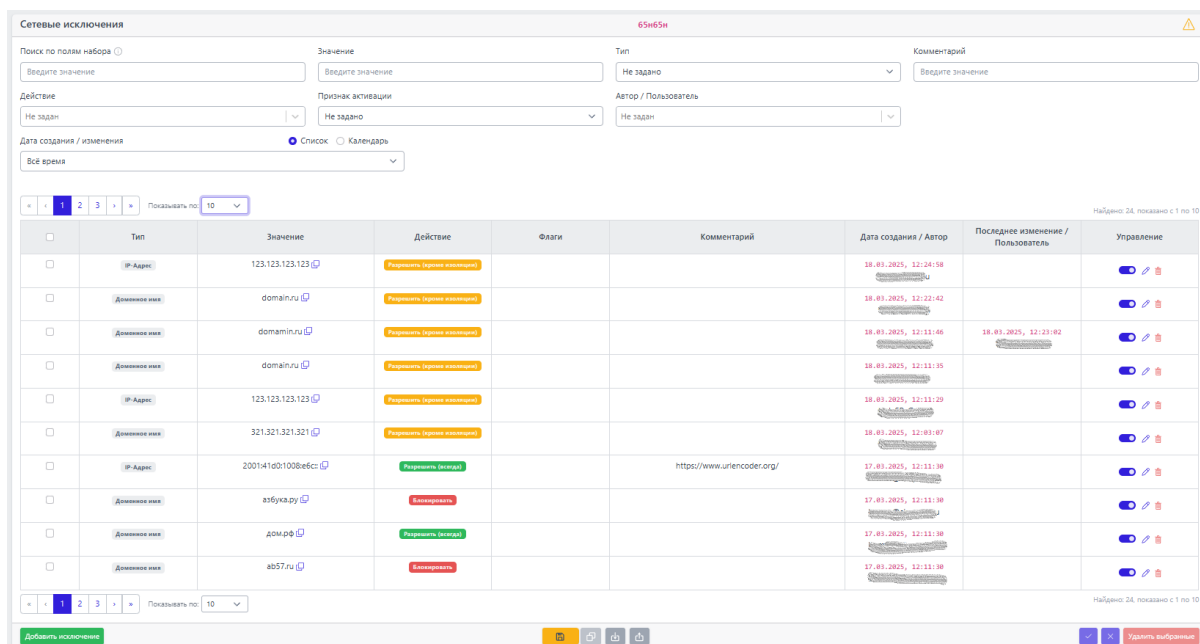


Рисунок 175 – Страница «Сетевые исключения»

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

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

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

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

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

Далее выбрать формат, в котором будет экспортироваться набор (csv или json). Набор будет сохранен в папке **Загрузки** в выбранном формате.

Для импорта исключений из файла требуется нажать кнопку **Импортировать файл** (). Далее выбрать на компьютере файл соответствующего формата, содержащий нужные правила, и нажать кнопку **Открыть**.

Чтобы активировать или деактивировать исключение из выбранного набора, необходимо нажать кнопку **Деактивировать сетевое исключение/Активировать сетевое исключение** .

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

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

6.7.4. Исключения индикаторов атак

Общая информация

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

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

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

Наборы исключений индикаторов атак

Страница **Наборы исключений индикаторов атак** включает в себя следующие структурные элементы (рис. 176):

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

Рисунок 176 — Страница «Наборы исключений индикаторов атак»

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

- **Название набора**;
- **Поиск по полям набора** (Поиск осуществляется по подстроке без учета регистра в текстовых полях);
- **Автор/Пользователь**;
- **Дата создания/Изменения**.

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

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

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

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

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.

Общий вид страницы с исключениями для выбранного набора представлен на рисунке 177.

Исключения индикаторов атак 55

Поиск по полям набора (🔍) Имя Условие Тип

Введите значение Введите значение Введите значение Не задан

Комментарий Описание Признак активации Автор / Пользователь

Введите значение Введите значение Не задано Не задан

Дата создания / изменения ☒ Список ☐ Календарь

Всё время

Показывать по: 50

	Имя	Тип	Дата создания / Автор	Последнее изменение / Пользователь	Управление
☒	блок_создания_btl_на_рабочем_столе	Создание нового файла	18.03.2025, 13:13:28 QAadmin@gmail.com		
☒	блок_добавления_ключа	Создание нового ключа	18.03.2025, 13:13:28 QAadmin@gmail.com		
☒	блок_индекс_музыки	Исходящее подключение	18.03.2025, 13:13:28 QAadmin@gmail.com		

Показывать по: 50

Найдено 3, показано с 1 по 3

Добавить исключение

Удалить выбранные

Рисунок 177 – Страница исключений индикаторов атак для выбранного набора

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

- Поиск по полям набора (Поиск осуществляется по подстроке без учета регистра в текстовых полях);
- Имя;
- Условие;
- Тип;
- Комментарий;
- Описание;
- Признак активации;
- Автор/Пользователь;
- Дата создания/Изменения.

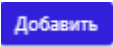
Для добавления исключения в выбранный набор необходимо нажать кнопку **Добавить исключение**, после чего откроется одноименное окно. Далее в открывшемся окне **Добавить исключение** следует заполнить поля с параметрами исключения. Поле, отмеченное значком звездочки (*), является обязательным для заполнения.



Важно

Имя исключения должно соответствовать имени исключаемого индикатора.

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

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

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 . Для отмены изменений следует нажать кнопку **Заккрыть 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. 178).

Время ↑↓	Событие	Имя пользователя	Статус
07.03.2025, 11:27:10	Вход в систему	test_SP_@rt.ru	✓
07.03.2025, 11:27:00	Выход из системы	test_SP_@rt.ru	✓
06.03.2025, 18:57:12	Вход в систему	QA1admin@gmail.com	✓
06.03.2025, 18:57:08	Выход из системы	QAadmin@gmail.com	✓
06.03.2025, 18:57:02	Вход в систему	QAadmin@gmail.com	✓
06.03.2025, 18:56:58	Выход из системы	QAadmin@gmail.com	✓
06.03.2025, 18:50:10	Вход в систему	QAadmin@gmail.com	✓
06.03.2025, 18:49:31	Выход из системы	test_user1@gmail.com	✓
06.03.2025, 18:49:29	Вход в систему	test_user1@gmail.com	✓
06.03.2025, 18:49:25	Выход из системы	test_user@gmail.com	✓

Рисунок 178 – 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) Статус (успешно/неудачно);

4) Пользователь;

5) Временной период.

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

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

На рисунке 179 отображается информация о событии в формате HTML.

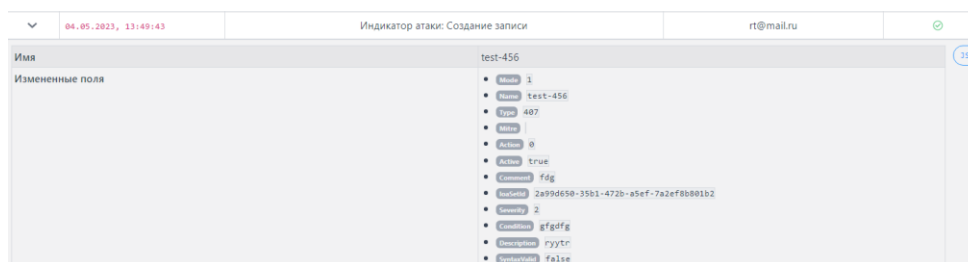


Рисунок 179 – Отображение информации о событии в формате HTML

На рисунке 180 отображается информация в формате JSON.

Время	Событие	Имя пользователя	Статус
04.09.2025, 15:49:43	Индикатор атаки: Создание записи	rt@mail.ru	🟢
<pre> { "id": "2025-09-04T15:49:43-07:00", "userId": "d0c9d0b0-43d0-40de-80de-030057367676", "username": "rt@mail.ru", "type": 1, "tableName": "Log", "time": "2025-09-04T15:49:43-07:00", "oldValues": {}, "newValues": { "Name": "test-456", "Type": 487, "Hit": "", "Action": 0, "Comment": "Flag", "Severity": 2, "Condition": "ifFlag", "Description": "Trybe", "SyntaxValid": false }, "affectedColumns": [], "primaryKey": "Name", "name": "test-456", "success": true, "collectionChanged": false } </pre>			

Рисунок 180 – Отображение информации о событии в формате JSON

В верхней части страницы Журнал действий пользователя можно скачать информацию из журнала действий пользователя в формате CSV с помощью иконки , и в формате JSON с помощью иконки .

Можно скачать как весь журнал действий, так и действия, отображенные согласно выставленным фильтрам на странице.

6.8.2. Лицензия

Страница подраздела **Лицензия** представлена на рисунке 181.

Информация о лицензии

Название компании
rt-ib

Статус
Активна

Дата начала действия
27.07.2025

Дата окончания действия
26.07.2027

Остаток дней действия
677

Комментарий
test

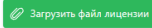
Ограничения лицензии

- Пользователи: 206
- Организации: 62
- Клиенты: 168
- Анализаторы: 14

EDR: Интеграция включена

VM: Интеграция включена

Загрузка лицензии

Загрузка в формате файла
 Загрузить файл лицензии

Лицензия была загружена на сервер пользователем QAadmin@gmail.com 11.09.2025, 14:52:51

Рисунок 181 – 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,**
- **Ограничения лицензии** (Ограничения по количеству пользователей, организаций, клиентов и организаций).

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

1. 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.

2. Если достигнуты пределы, выставленные в ограничениях по лицензии, то создание организации выше порога невозможно. При этом кнопка будет заблокирована и будет выводиться информационное сообщение о невозможности создания в связи с ограничением лицензии.

В нижней части поля «Информация о лицензии» показано, что включены интеграции со следующими модулями:

- EDR;
- VM (менеджер уязвимостей).

7. Сообщения администратору

7.1 Общие сведения

Диалоговые окна, используемые для оповещения, различаются в зависимости от категории информации, которая в них содержится.

Предусмотрены следующие категории информации:

- 1) ошибка;
- 2) обнаружение;
- 3) предупреждение;
- 4) успешно.

Сообщения администратору выводятся в виде диалоговых окон.

7.2 Сообщения об ошибках

Можно выделить два типа сообщений об ошибках:

- 1) общие сообщения – выводятся в приложении в том случае, если возникшая ошибка не была обработана специальным образом, и использовался общий обработчик;
- 2) специфичные сообщения – выводятся в конкретных местах приложения и содержат детальное описание ошибки.

7.2.1. Общие сообщения

Общие сообщения – универсальные сообщения, которые выводятся в тех ситуациях, когда ошибка была обработана особым образом. Эти сообщения используются почти всегда.

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

- 1) экран ошибки;
- 2) всплывающее сообщение об ошибке.

Пример сообщения в виде экрана ошибки представлен на рисунке 182.

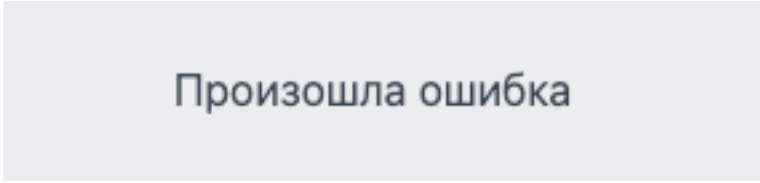


Рисунок 182 – Сообщение об ошибке типа «Экран ошибки»

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 183.

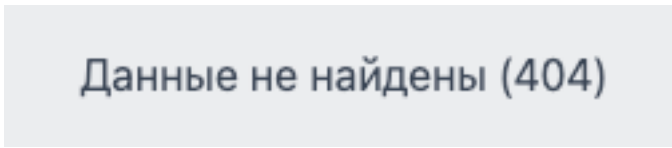


Рисунок 183 – Сообщение об ошибке

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 184.

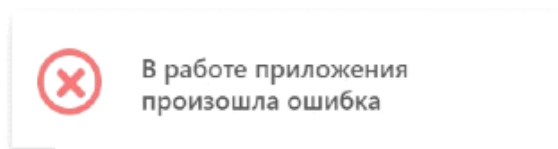


Рисунок 184 – Всплывающее сообщение об ошибке

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 185).

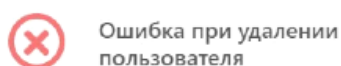


Рисунок 185 – Ошибка при удалении пользователя

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 186).



Ошибка сброса пароля

Рисунок 186 – 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 187.

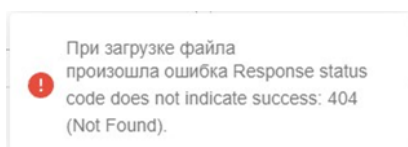


Рисунок 187 – Ошибка при загрузке файла

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 188.

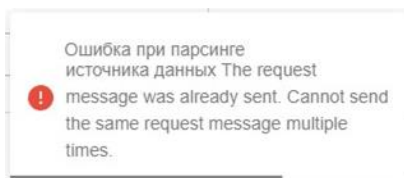


Рисунок 188 – Окно ошибки при парсинге источника данных

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 189.

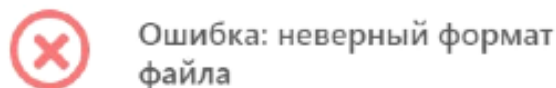


Рисунок 189 – Неверный формат файла

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 190.

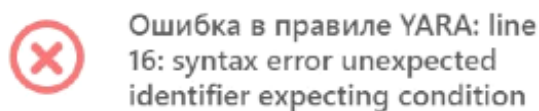


Рисунок 190 – Ошибка в правиле YARA

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 191.

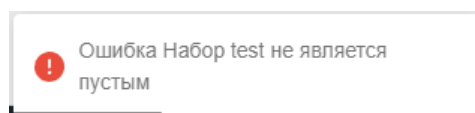


Рисунок 191 – Сообщение об ошибке при попытке удаления не пустого набора

- 1) Сообщение об ошибке при вводе неправильных учетных данных представлено на рисунке 192.

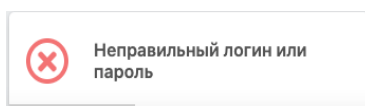


Рисунок 192 – Сообщение об ошибке при вводе неправильных учетных данных

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 193.

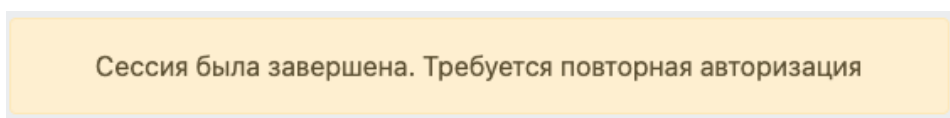


Рисунок 193 – Уведомление о завершении сессии пользователя

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.

- 1) Сообщение в хедере об отсутствии лицензии приведено на рисунке 194.

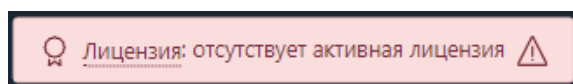


Рисунок 194 – Отсутствует лицензия

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 195.

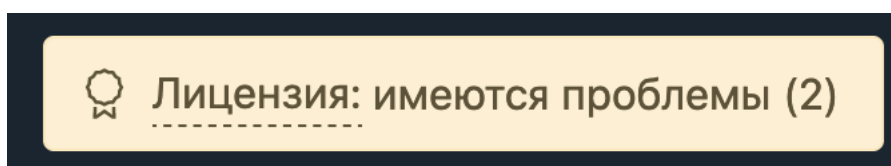


Рисунок 195 – Сообщение о проблемах с лицензией

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 196 - 197 .

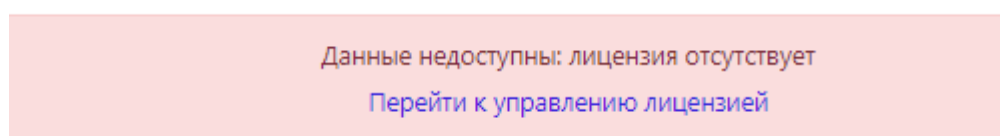


Рисунок 196 – Сообщение при отсутствии лицензии

Для начала работы требуется загрузить файл лицензии
Для управления лицензиями требуется роль "Администратор сервера"

Рисунок 197 – 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 198.

Проблемы с лицензией
• Лицензия отсутствует

Рисунок 198 – 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 действия со стороны пользователя/администратора;
- критические ошибки.

2) ошибки оборудования:

- выход из строя аппаратных средств, на которых установлена программа;
- выход из строя сервера (или компонентов на сервере), с которыми взаимодействуют компоненты программы, установленные на оборудовании пользователя;
- перебои питания со стороны клиентской или серверной части.

Для устранения ошибки требуется переконфигурировать программу либо восстановить 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».