Веб-сервис RT Protect TI

Руководство аналитика

Версия 1.0.19 от 25 сентября 2024
Разработано компанией АО «РТ-Информационная безопасность»

RT Protect

Оглавление

1. Общие положения 4
1.1 Идентификация документа 4
1.2 Аннотация документа 4
1.3 Термины и определения 4
1.4 Условные обозначения 6
2. Общие сведения 7
2.1 Назначение и архитектура программы 7
3. Организационно-распорядительные меры 9
3.1 Общие сведения 9
3.2 Комплектность поставки 9
3.2.1. Процедуры и меры безопасности при распространении программы к месту назначения 9
4. Структура программы 10
5. Настройка программы 11
5.1 Требования к среде функционирования 11
5.2 Роли 12
6. Интерфейс программы 14
6.1 Окно авторизации и общие сведения 14
6.2 Горизонтальная панель управления 16
6.2.1. Меню «Пользователь» 17
6.3 Главная страница 20
6.4 Администрирование 22
6.4.1. Организация 22
6.4.2. Теги 23
6.5 Аналитика 24
6.5.1. Активность 24
6.5.2. Отчеты 32

6.5.3. Граф связей 34
7. Действия после сбоя и ошибки 39
7.1 Общие сведения 39
8. Перечень сокращений 40
9. Заключение 41

1. Общие положения

1.1 Идентификация документа

Данное руководство кратко можно идентифицировать согласно таблице 1.

Таблица 1 – Идентификация документа

Название документа	«Веб-сервис RT Protect TI» Руководство Аналитика
Версия документа	Версия 1.0.19 (актуальна для версии продукта frontend 0.7.13/ backend 2.8.27)
Идентификация программы	Сервис по предоставлению аналитики «RT Protect TI»
Идентификация разработчика	АО «РТ-Информационная безопасность»

1.2 Аннотация документа

Документ предназначен для ознакомления пользователей сервиса с ролью «Аналитик» (подключенных в рамках одной организации, не являющейся владельцем платформы) 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	Различные типы данных имеющие подозрительное содержимое и загружаемые на сервер для анализа (файлы, доменные имена, IP-адреса, URL)
Backend	Программно-аппаратная часть сервиса, отвечающая за функционирование его внутренней части
JSON	Текстовый формат обмена данными, основанный на JavaScript
JSON-объект	Неупорядоченный набор пар ключ/значение. Объект начинается с открывающей фигурной скобки **{** и заканчивается закрывающей фигурной скобкой **}**. Каждое имя сопровождается двоеточием, пары ключ/значение разделяются запятой
Linux	Семейство Unix-подобных операционных систем на базе ядра Linux
Malware Bazaar	Проект сайта abuse.ch, целью которого является обмен образцами вредоносного ПО с сообществом информационной безопасности, поставщиками антивирусных программ и поставщиками информации об угрозах
SSDEEP	Алгоритм нечеткого хеширования
TCP	Один из основных протоколов передачи данных интернета. Предназначен для управления передачей данных интернета. Пакеты в TCP называются сегментами. В стеке протоколов TCP/IP выполняет функции транспортного уровня модели OSI
VirusTotal	Бесплатная служба, осуществляющая анализ подозрительных файлов и ссылок (URL) на предмет выявления вирусов, червей, троянов и всевозможных вредоносных программ
Web-сервер	Сервер, принимающий HTTP-запросы от клиентов, чаще всего веб-браузеров, и выдающий HTTP-ответы, как правило, вместе с HTML-страницей, изображением, файлом, медиа-потоком или другими данными
WHOIS	Сетевой протокол прикладного уровня, базирующийся на протоколе TCP. Основное применение – получение регистрационных данных о владельцах доменных имён, IP-адресов и автономных систем

Термин	Описание
Windows	Группа семейств коммерческих операционных систем корпорации Microsoft, ориентированных на управление с помощью графического интерфейса

1.4 Условные обозначения

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

Таблица 3 – Условные обозначения

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

2. Общие сведения

2.1 Назначение и архитектура программы

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

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

– администрирование пользователей организации, взаимодействующих с сервисом;

– выпуск токенов для клиентов;

– просмотр статистической информации по обнаружениям в графическом виде;

– получение вердикта по анализируемым артефактам;

– регистрация действий пользователей организации.

Программа функционирует под управлением ОС Linux Ubuntu 20.04.5 LTS.

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

Программа предназначена для обработки информации, не являющейся секретной.

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

Пользователь – может загружать для анализа на сервисе различные артефакты, просматривать отчеты по проверке артефактов.

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

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

3. Организационно-распорядительные меры

3.1 Общие сведения

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

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

Программа поставляется заказчику согласно комплектности поставки.

3.2 Комплектность поставки

Комплектность поставки представлена в таблице 4.

Таблица 4 – Комплектность поставки

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

3.2.1. Процедуры и меры безопасности при распространении программы к месту назначения

Процедуры и меры безопасности при распространении программы к месту назначения решают следующие задачи:

– обеспечивают идентификацию и целостность программы во время пересылки;

– обеспечивают обнаружение несанкционированных модификаций программы;

– препятствуют попыткам подмены программы от имени разработчика.

4. Структура программы

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

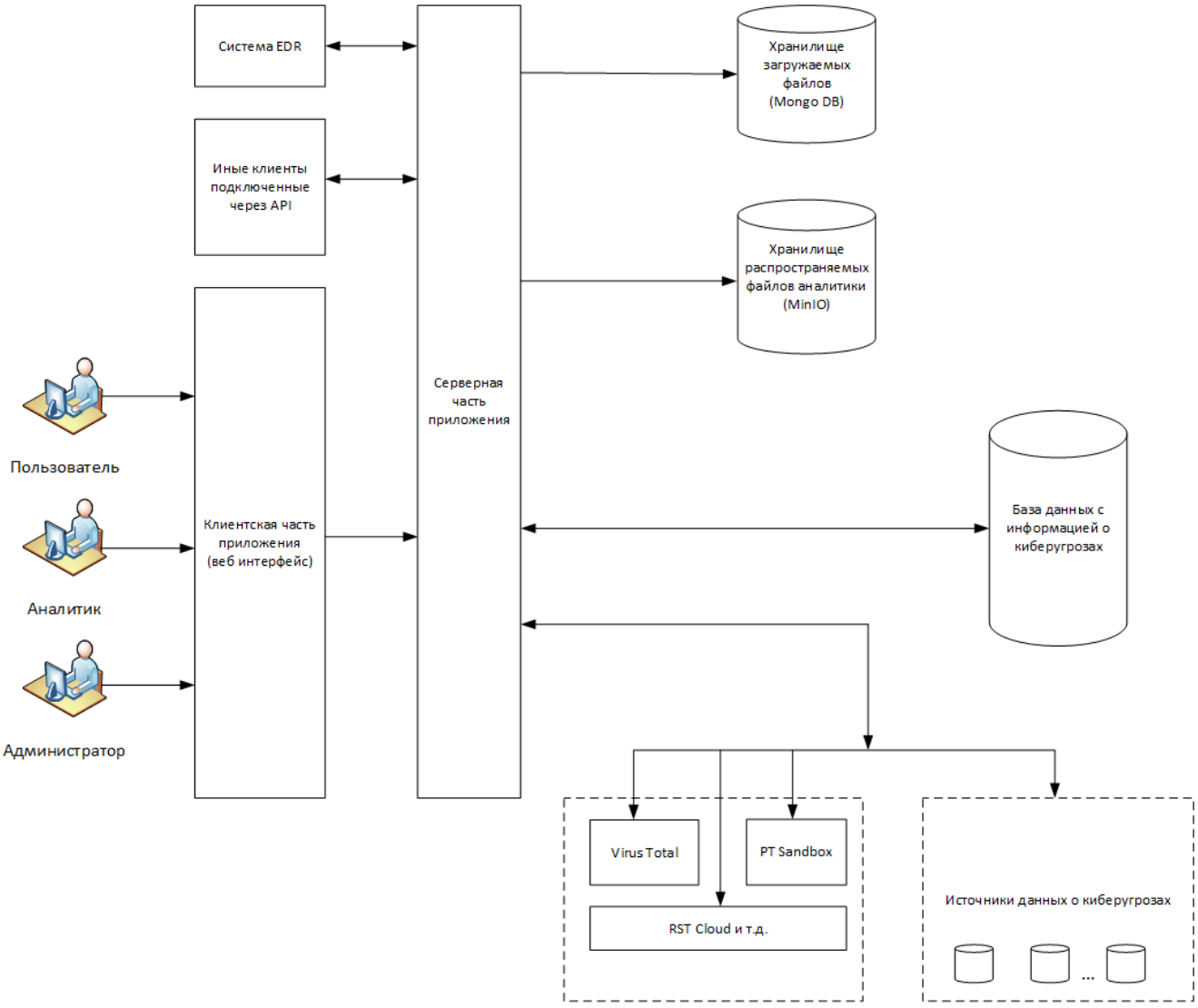


Рисунок 1 – Схема архитектуры сервиса

5. Настройка программы

5.1 Требования к среде функционирования

Программа работает на 64-х разрядной платформе семейства Linux (Ubuntu 20.04.5 LTS).

Аппаратная платформа сервера обеспечивает возможность выполнения функциональных требований, предъявляемых к серверу, с учетом технологии его построения, критериев производительности и отказоустойчивости.

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

Таблица 5 – Программно-аппаратное обеспечение

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

Программа поддерживает работу в браузерах, представленных в таблице 6.

Таблица 6 – Список поддерживаемых браузеров

№ п/п	**Тип браузера**	**Минимальная рекомендуемая версия**
1	Google Chrome	Версия не ниже 92.0.4515.107
2	Firefox Browser	Версия не ниже 83.0

5.2 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 данных согласно списку:

– IP-адрес;

– доменное имя;

– URL;

– контрольную сумму файла (хеш-суммы);

– email.

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

3) просмотр страницы отчета по проверенному артефакту.

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

В круг типовых задач аналитика входят:

– проверка артефактов;

– анализ активности;

– просмотр отчетов об артефактах;

– просмотр программ и уязвимостей найденных в данных программах.

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

6. Интерфейс программы

6.1 Окно авторизации и общие сведения

Вход в программу производится из поддерживаемой версии браузера. Для открытия окна авторизации необходимо в строке браузера ввести имя сервера или его ip-адрес. После ввода в строке браузера корректных данных откроется окно авторизации (рис. 2).

Рисунок 2 – Окно авторизации

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

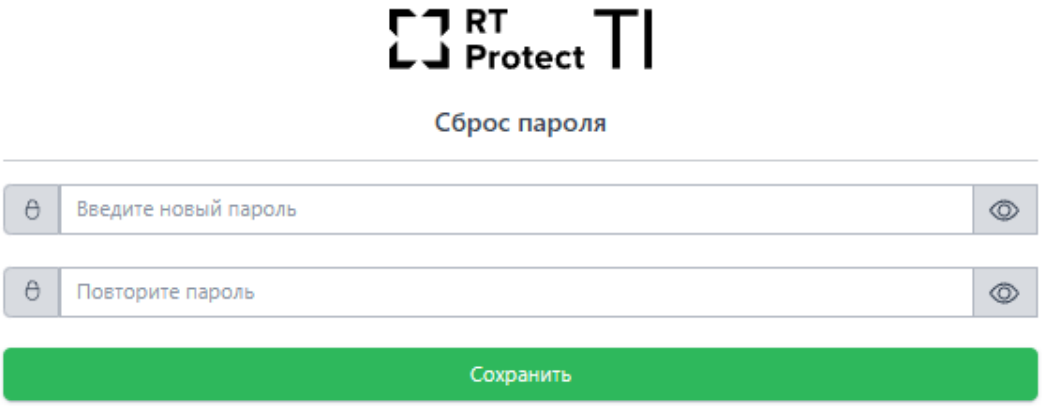


Рисунок 3 – Окно ввода параметром для сброса пароля

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

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

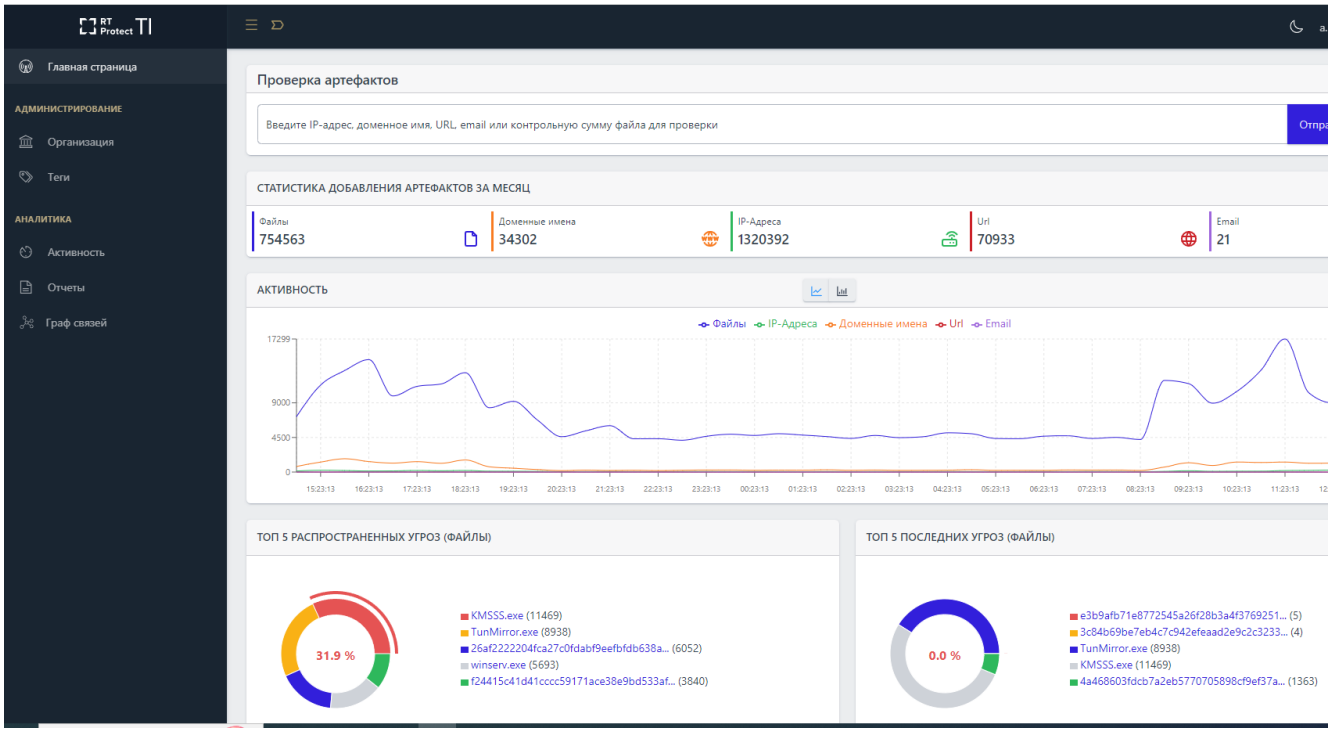


Рисунок 4 – Основное окно программы

Если в течение 5 минут пользователь выполнил 5 неудачных попыток входа, то его учетная запись будет заблокирована. В этом случае разблокировать такого пользователя сможет только администратор (подробнее см. подраздел 6.4).

Функции, доступные в интерфейсе административного модуля управления:

– анализ загруженных артефактов (IP-адресов, файлов, доменных имен, URL, email);

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

– просмотр отчетов по анализу проверенных артефактов;

– просмотр перечня программ и найденных уязвимостей.

В левой части основного окна программы (см. рис. 4) находится вертикальная панель управления, доступная аналитику. С помощью панели управления аналитик может переходить по разделам программы для изменения настроек и просмотра информации по разделам. При выборе определенного раздела в правой части окна будет представлена информация выбранного раздела и основной инструментарий для работы пользователя программы.

В нижней части страницы находится информация о товарном знаке компании – RT Protect © 2022. Справа от текущей версии программы отображается надпись о том, где «RT Protect TI» разработана – Сделано в России.

6.2 Горизонтальная панель управления

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

Рисунок 5 – Горизонтальная панель управления

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

При нажатии кнопки **Скрыть/показать панель разделов** ( ) основное окно программы приобретает вид, как показано на рисунке 6. Для возврата первоначального вида необходимо повторно нажать на кнопку .

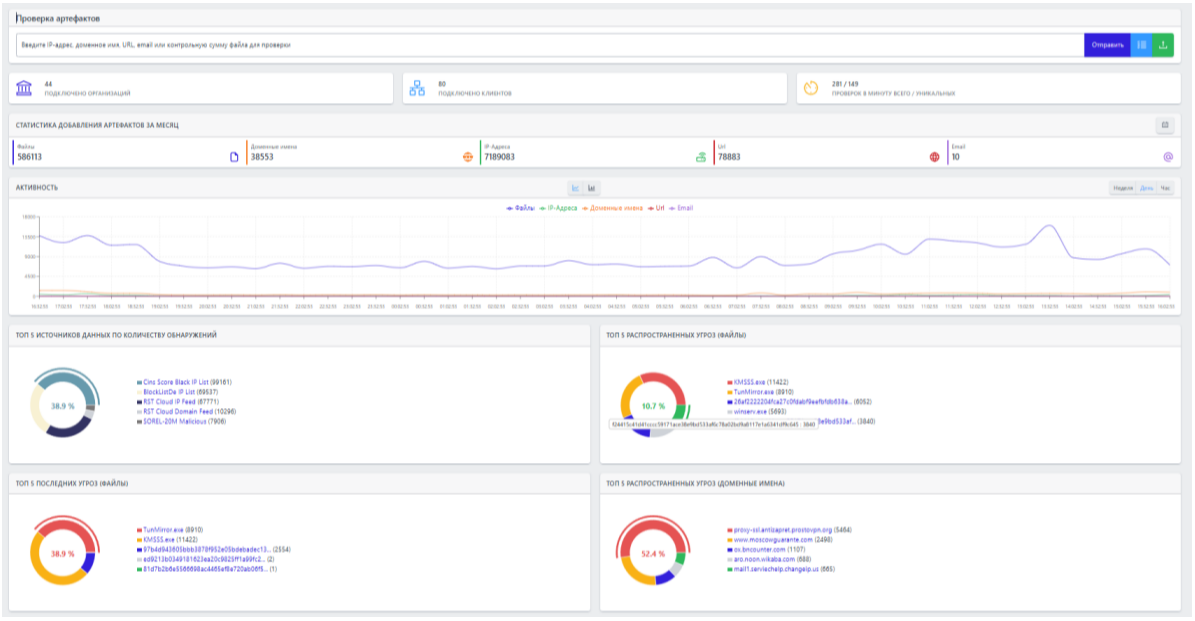
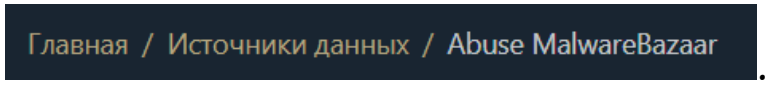


Рисунок 6 – Основное окно программы при скрытой панели разделов

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

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

6.2.1. Меню «Пользователь»

При нажатии ЛКМ на имени пользователя (логин) в правой верхней части основного окна программы открывается меню работы с учетной записью, в котором представлены подменю **Профиль** и кнопка **Выход** для выхода из программы с текущего устройства (рис. 7).

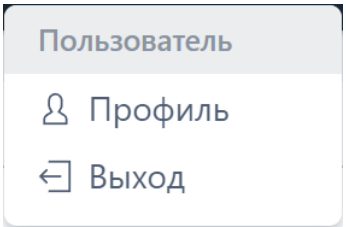


Рисунок 7 – Меню «Пользователь»

Подменю **Профиль** представлено на рисунке 8.

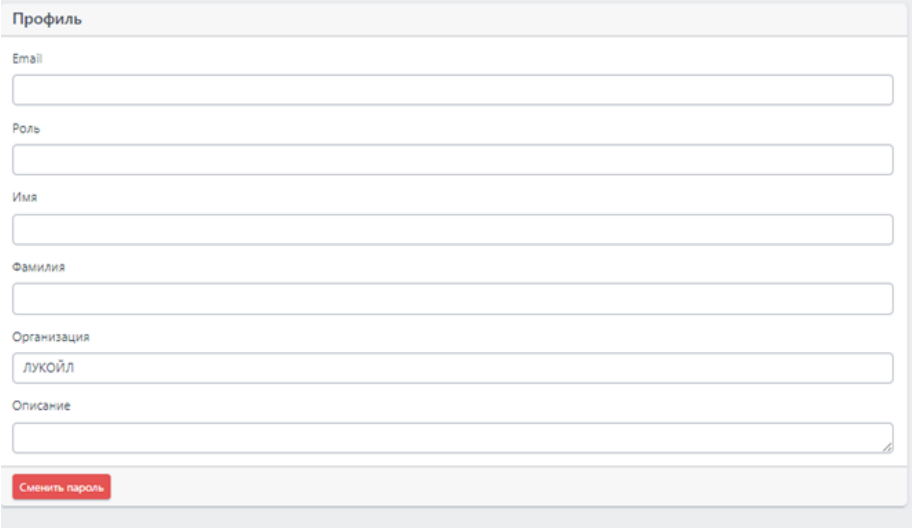


Рисунок 8 – Подменю «Профиль»

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

– адрес электронной почты для своей учетной записи;

– роль, назначенная пользователю (только аналитик);

– имя и фамилия пользователя;

– организация (в которой работает аналитик);

– поле с описанием профиля пользователя.

Изменять пароль возможно с помощью кнопки Сменить пароль. При нажатии кнопки **Сменить пароль** открывается окно для смены пароля (рис. 9).

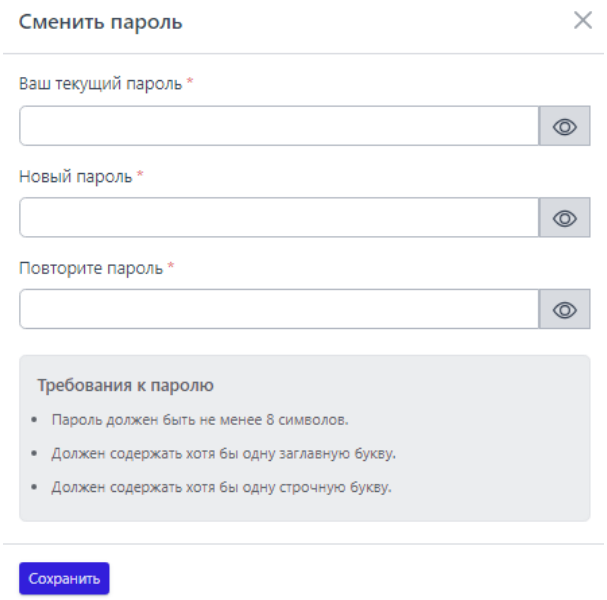


Рисунок 9 – Окно смены пароля

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

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

– область проверки артефактов;

– статистика добавления артефактов за 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, файлы).

В областях графики имеются иконки для управления размером отображения графика (50 или 100 %).

Данные иконки имеют вид :  - ширина 100%,  - ширина 50 %.

Примеры отображения области **Графики** представлены на рисунках 10 - 11.

Рисунок 10 – Области с графиками с шириной 50%

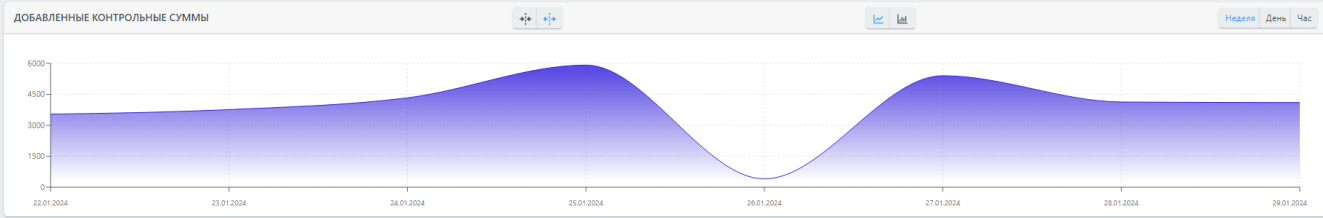


Рисунок 11 – Область с графиком с шириной 100%

В области **Проверка артефактов** Аналитик может получить вердикт для IP-адреса, домена, URL-адреса, Email или хеш-суммы. Для этого необходимо ввести данные соответствующего артефакта в строку и нажать кнопку **Отправить.** Откроется отчет сервера аналитики (подробнее см. в пункте 6.5.2).

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 сервер аналитики, а после завершения его загрузки выводится отчет с вердиктом.

В области **Проверка артефактов** администратор также может проверить целый список артефактов, нажав по иконке  , после чего откроется окно для загрузки списка артефактов, представленное на рисунке 12.

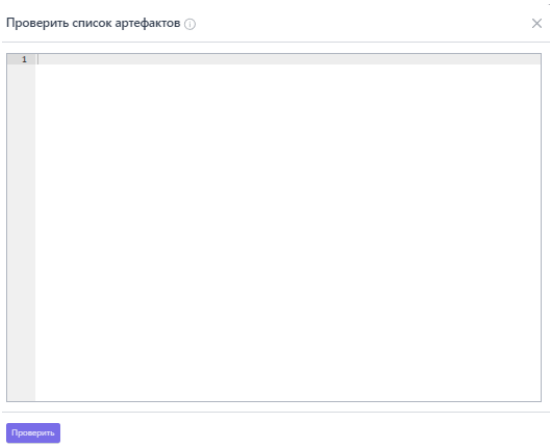


Рисунок 12 – Окно для написания списка артефактов для проверки

В данном окне артефакты добавляются по одному в каждой строчке (с нумерацией строк). Проверка артефактов списком ограничена количеством в 100 строк. После написания артефактов требуется нажать по иконке **Проверить**.

6.4 Администрирование

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

– **Организация**;

– **Теги**.

Аналитик может выполнять следующие действия:

– просматривать подробную информацию о своей организации;

– создавать и импортировать pdf-файл с общим количеством обнаружений и вредоносных обнаружений за выбранный период времени;

– просматривать названия клиентов (программ, имеющих доступ к API платформы TI);

– просмотреть квоты по использованию API вызовов для пользователей в рамках организации;

– просмотреть список тегов и псевдонимов.

6.4.1. Организация

В разделе **Организация** представлена информация об организации, в которой работают пользователи программы (рис. 13). Здесь содержатся данные о стране происхождения, сайте организации, секторе экономики. Также представлена информация по названию, контактам и описанию организации.

Имеется иконка  , при нажатии по которой можно скачать отчет за определенный период об обнаруженных в организации угрозах в формате pdf.

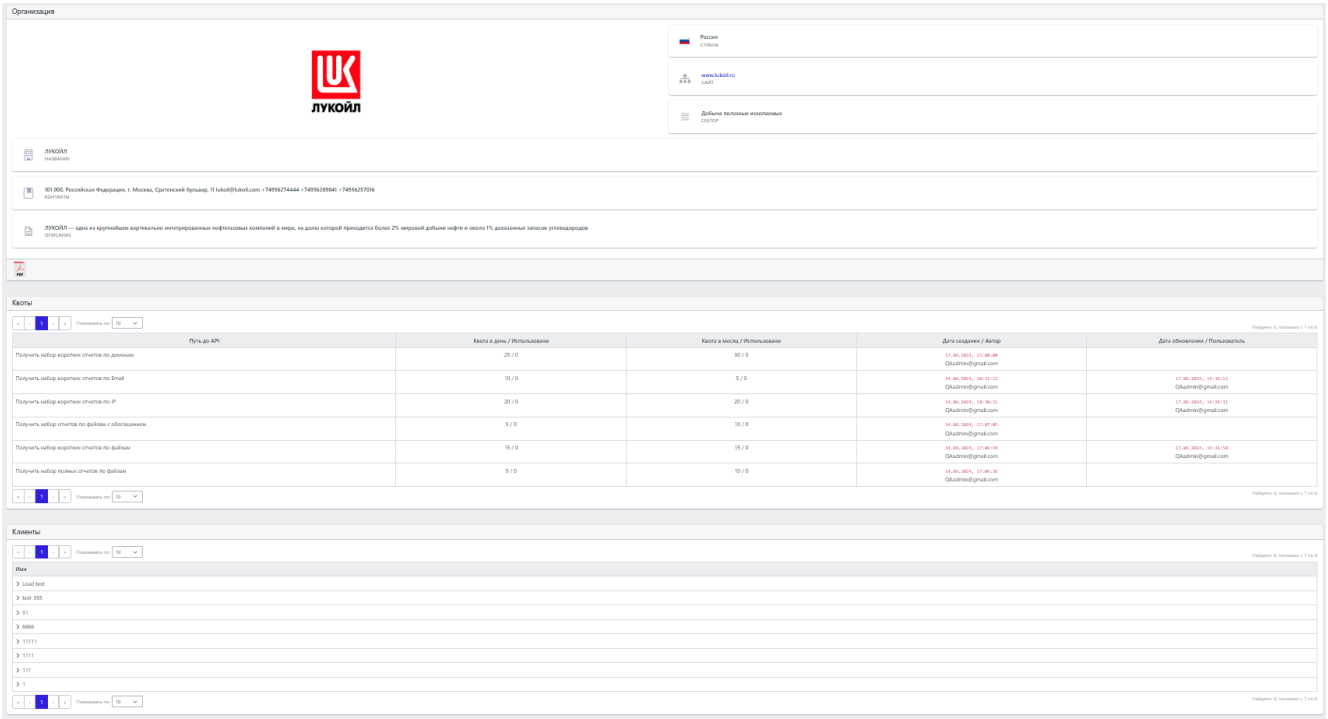


Рисунок 13 – Окно раздела «Организация»

В области **Квоты** аналитик может просмотреть квоты на использование API вызовов при обращении к серверу для пользователей в рамках своей организации.

В области **Клиенты** указывается имя клиента, соответствующее определенному токену, аналитику просмотр токена недоступен.

Примечание

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

6.4.2. Теги

На странице **Теги** аналитик может просматривать теги и псевдонимы тегов, предназначенные для ранжирования элементов активности.

Страница **Теги** представлена на рисунке 14.

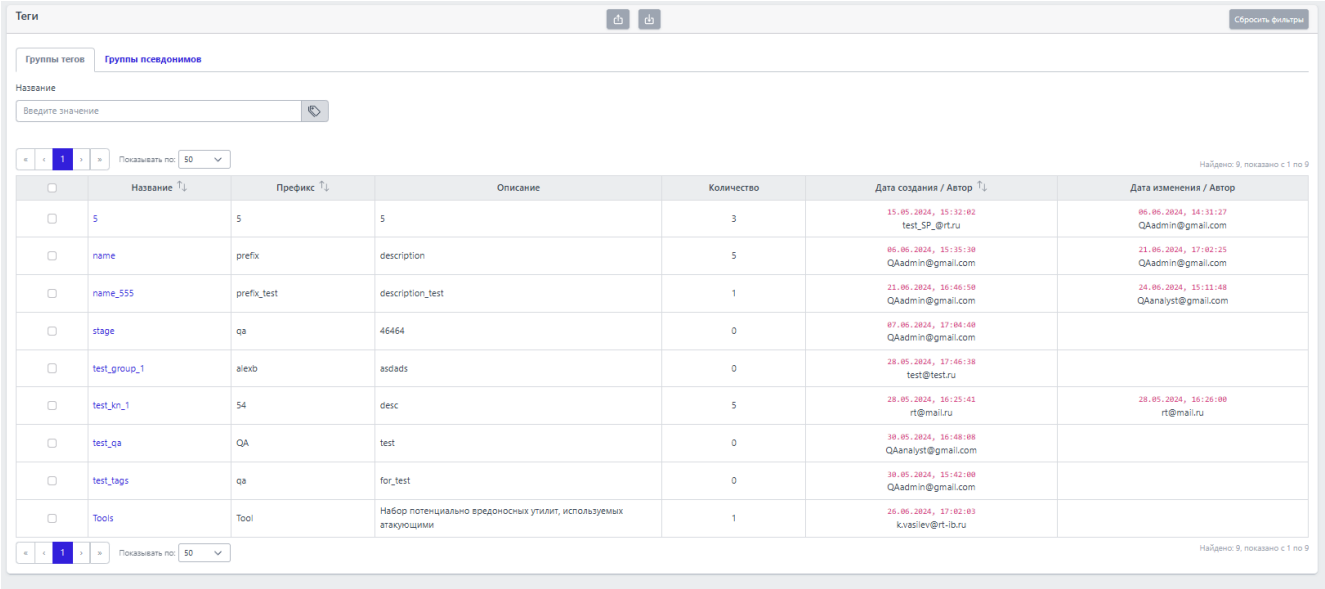


Рисунок 14 – Страница Теги

Создание, редактирование и иные действия для пользователя с ролью Аналитик (в рамках организации не владельца платформы) недоступны.

6.5 *Аналитика*

Область **Аналитика** содержит информацию об активности, происходящей в организации: обнаружениях вредоносных артефактов и отчетах по исследуемым TI-платформой артефактам. Эта информация представлена в следующих разделах:

1) **Активность;**

2) Отчеты;

3) Граф связей;

4) Угрозы и злоумышленники.

6.5.1. Активность

В разделе **Активность** в табличной форме представлена информация о угрозах, которые обнаружены в инфраструктуре организации подключенной к сервису аналитики (рисунок 15).

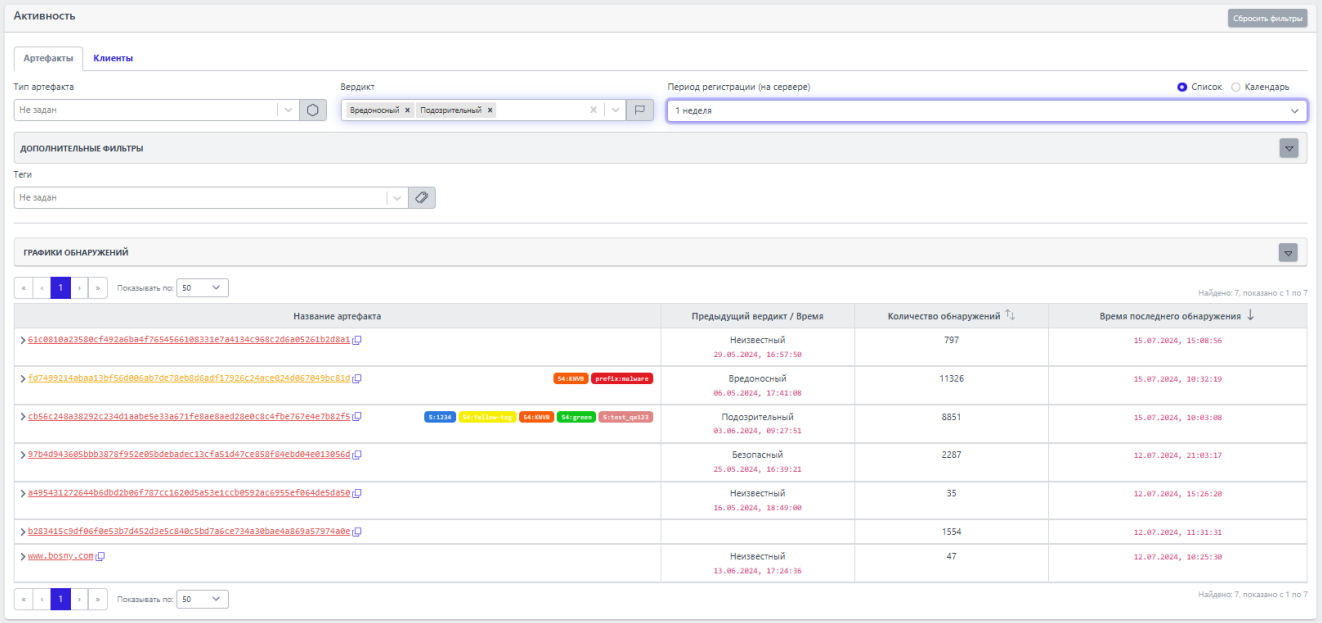


Рисунок 15 – Общий вид страницы Активность

В верхней части страницы **Активность** имеются следующие вкладки: **Артефакты, Клиенты.**

При переходе по каждой вкладке на странице **Активность** отображается информация, соответствующая данной вкладке, при этом вкладка, на которую был произведен переход, отмечается серым цветом.

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

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

– **Количество обнаружений** (отображается общее количество обнаружений по данному артефакту);

– **Время последнего обнаружения** (отображается время последнего обнаружения файла с угрозой).

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

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

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

– B73753C4C69A03F9A3E09F121B6599D77B1A4BE0247F9B71B56572555E1FE12B – неизвестный файл (шрифт серого цвета);

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

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

Также справа от названия артефакта имеются иконки с тегами для данного артефакта.

Контрольная сумма файла угрозы, а также информация по другим типам артефактов является активной ссылкой, при нажатии по которой ЛКМ открывается окно отчета TI-платформы, представленное на рисунке 16.

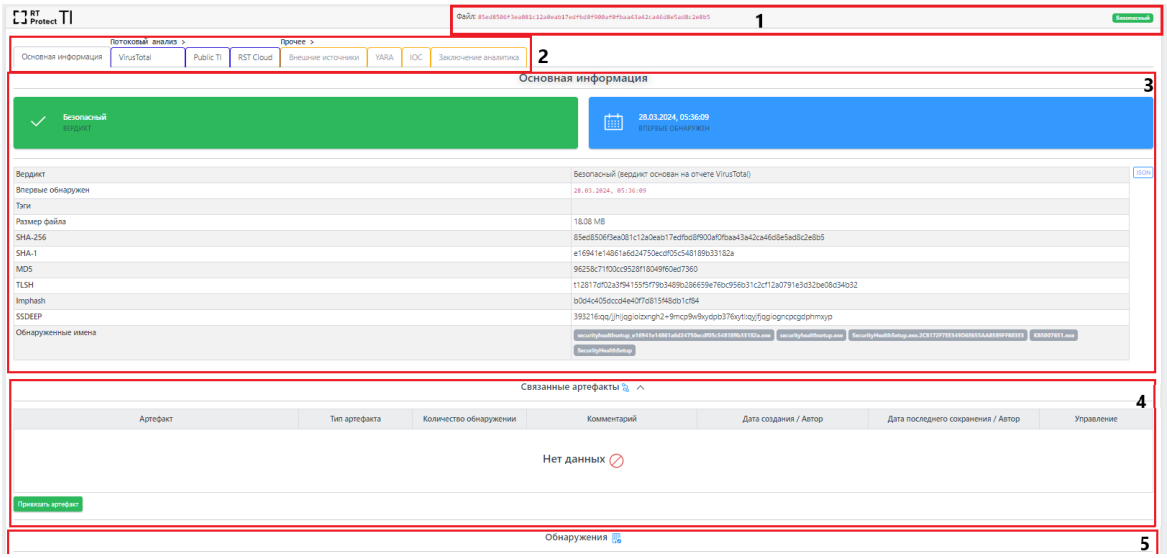


Рисунок 16 – Страница отчета сервиса по обнаруженной угрозе

Страница отчета программы об угрозе разделена на следующие области:

1) область краткой информации об угрозе;

2) область вкладок;

3) область основной информации;

4) область связанных с артефактом других артефактов;

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

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

В области 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-платформы по данной угрозе.

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

1) потоковый анализ (Virus Total, Public TI, RST Cloud);

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

Состав этих вкладок может меняться в зависимости от конфигурации сервера (какие модули подключены, какие нет).

Если в области вкладок запись отображается серым цветом, то информация по данному файлу в стороннем сервисе отсутствует. При нажатии ЛКМ по одной из вкладок появляется окно результатов по анализу артефакта (рис. 17).

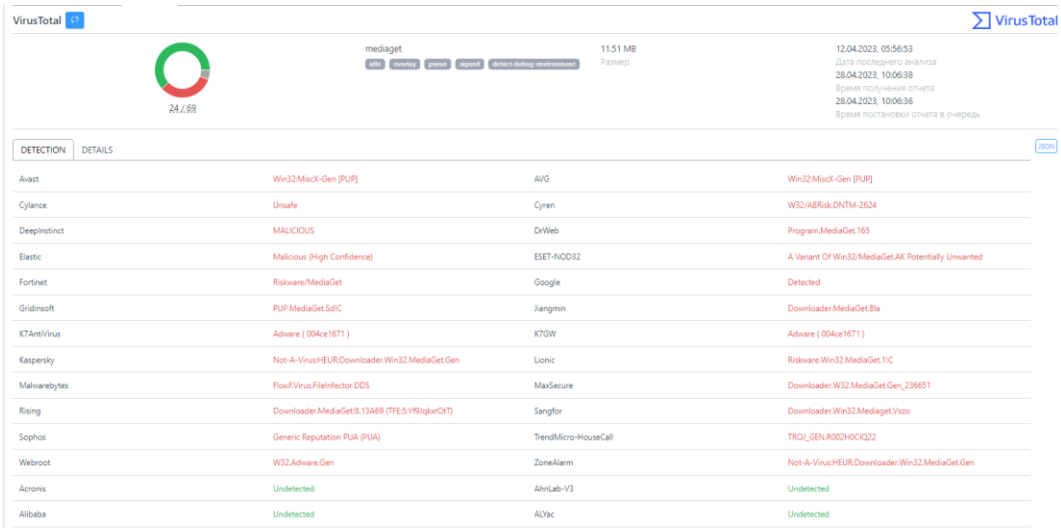
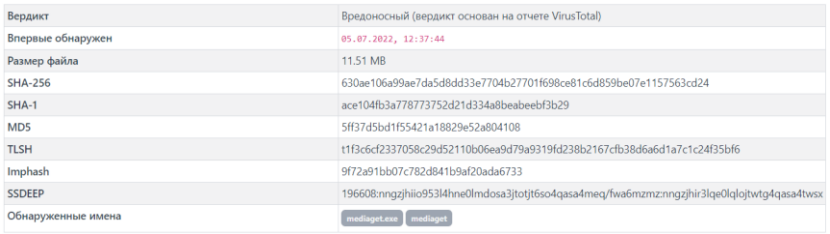


Рисунок 17 – Результаты анализа артефакта на странице Virus Total

Окно основной информации по результатам анализа артефакта в формате HTML представлено на рисунке 18.



Вердикт	Вредоносный (вердикт основан на отчете VirusTotal)
Впервые обнаружен	05.07.2022, 12:37:44
Размер файла	11.51 MB
SHA-256	630ae106a99ae7da5d8dd33e7704b27701f698ce81c6d859be07e1157563cd24
SHA-1	ace104fb3a778773752d21d334a8beabeebf3b29
MD5	5ff37d5bd1f55421a18829e52a804108
TLSH	t1f3c6cf2337058c29d52110b06ea9d79a9319fd238b2167cfb38d6a6d1a7c1c24f35bf6
Imphash	9f72a91bb07c782d841b9af20ada6733
SSDEEP	196608:nngzjhiio953l4hne0lmdosa3jtotjt6so4qasa4meq/fwa6mzmz:nngzjhir3lqe0lqlojtwtg4qasa4twsx
Обнаруженные имена	mediaget.exe mediaget

Рисунок 18 – Информация отчета об артефакте в формате HTML

Окно основной информации по результатам анализа артефакта в формате JSON представлено на странице 19.

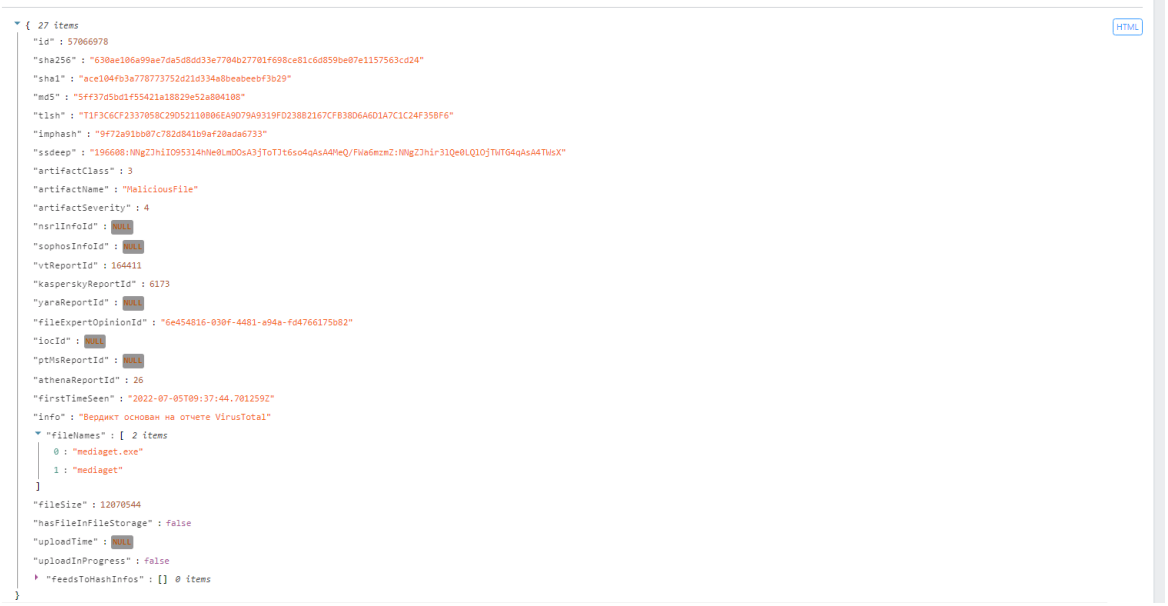


Рисунок 19 – Информация отчета об артефакте в формате JSON

В области **Связанные артефакты** показывается таблица с описанием артефакта, связанного с тем артефактом, отчет по которому просматривается на данный момент. При нажатии по иконке Привязать артефакт открывается окно для привязки артефактов друг к другу (см. рисунок 20).

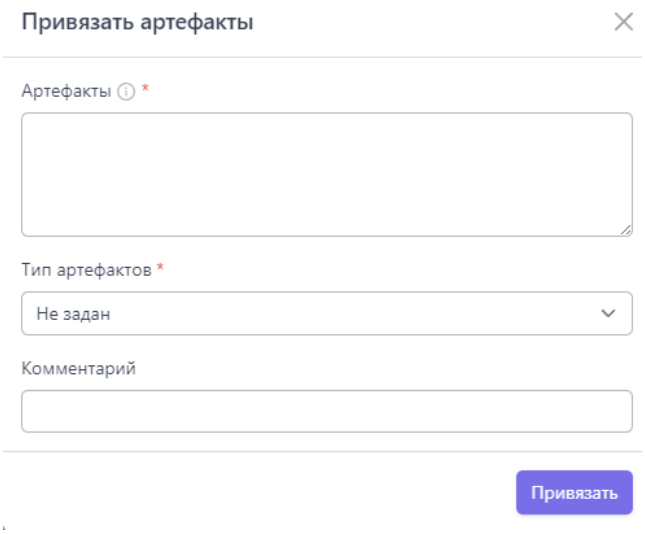


Рисунок 20 – Окно для привязки артефакта

В данном окне добавляется один или несколько артефактов, тип артефакта и комментарий. После добавления информации следует нажать по иконке **Привязать.** После привязки артефакт появится в списке связанных артефактов.

Важно

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

Для фильтрации информации на странице **Активность** вкладка **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), либо в виде календаря (начальная и конечная даты);

– Теги.

Также имеется область **Дополнительные фильтры** (скрытая по умолчанию) при активации которой открывается система дополнительных фильтров:

– **Артефакт**;

– **Количество обнаружений не менее;**

– **Количество обнаружений не более;**

– **Предыдущий вердикт;**

– **Время последнего изменения вердикта.**

На странице **Активность** вкладки **Артефакты** имеется область с графическим отображением информации по обнаруженным угрозам (рисунок 21).

Рисунок 21 – Область графического отображения информации по обнаруженным угрозам вкладка «Артефакты»

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

– статистика обнаружений по типам;

– статистика обнаружений по вердиктам;

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

– **Теги.**

Также имеется область **Дополнительные фильтры** (скрытая по умолчанию) при активации которой открывается система дополнительных фильтров:

– **Артефакт**;

– **Количество обнаружений не менее;**

– **Количество обнаружений не более;**

– **Предыдущий вердикт;**

– **Время последнего изменения вердикта;**

– **Клиенты.**

На странице **Активность** вкладки **Клиенты** имеется область с графическим отображением информации по обнаруженным угрозам для тех или иных клиентов в рамках подключенной к сервису организации.

Главным отличием вкладки **Клиенты** является то, что в ней показаны обнаружения, соответствующие организации, указанной в разделе **Организация**, а в разделе **Артефакты** показаны обнаружения, общие для всех организаций TI-платформы, но не имеющие привязки к какой-либо конкретной организации.

6.5.2. Отчеты

В разделе **Отчеты** в табличной форме представлена информация о проверенных артефактах. Общий вид страницы представлен на рисунке 22.

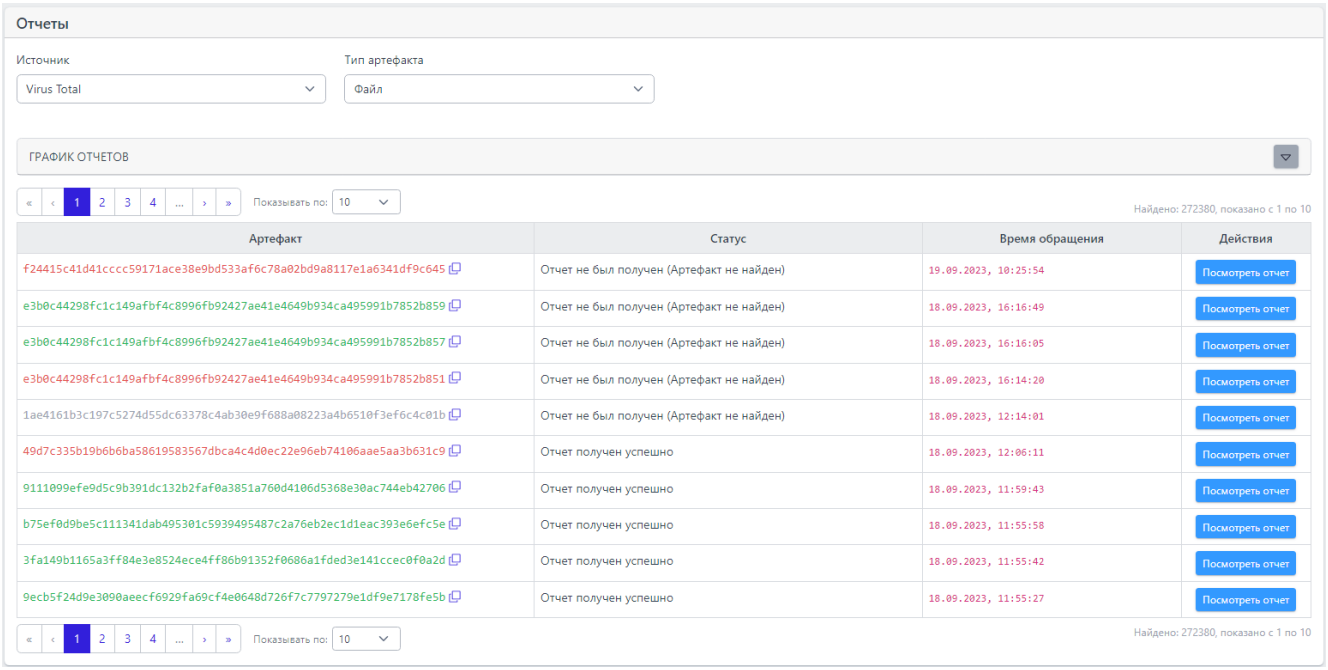


Рисунок 22 – Окно раздела «Отчеты»

В таблице имеются следующие поля:

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

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

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

– **Действия** (получить отчет).

Информация об артефакте отображается разными цветами:

– шрифт красного цвета (артефакт является вредоносным);

– шрифт зеленого цвета (артефакт является безопасным).

Над таблицей для фильтрации информации имеются следующие фильтры:

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

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

Над таблицей для отображения визуальной информации имеется область с графиком полученного числа отчетов за определенный период в зависимости от установленного в фильтре источника данных (рисунок 23).

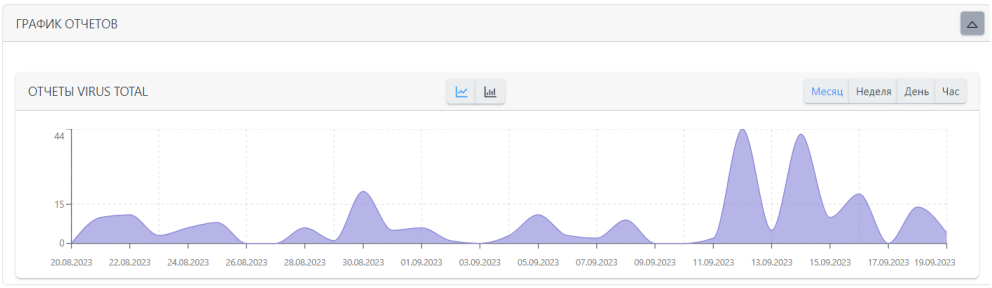


Рисунок 23 – Отчеты Virus Total

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

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

Страница отчета по артефакту представлена на рисунке 24.

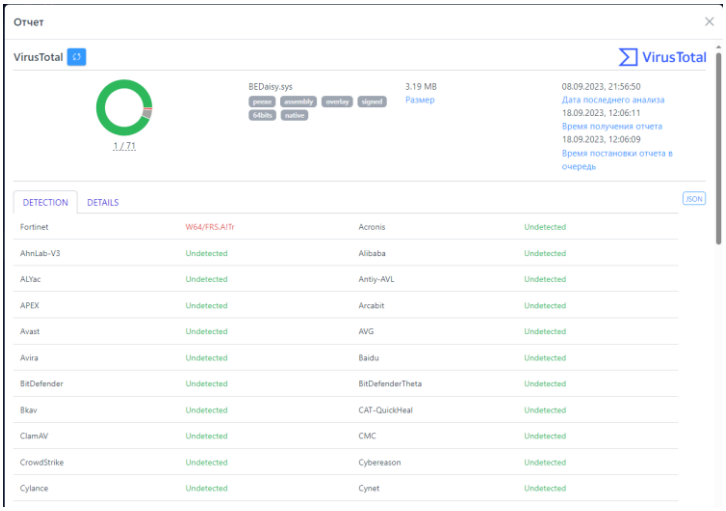


Рисунок 24 – Страница отчета по артефакту от источника Virus Total

6.5.3. Граф связей

Страница «Граф связей» с незаполненным полем артефакта представлена на рисунке 25.

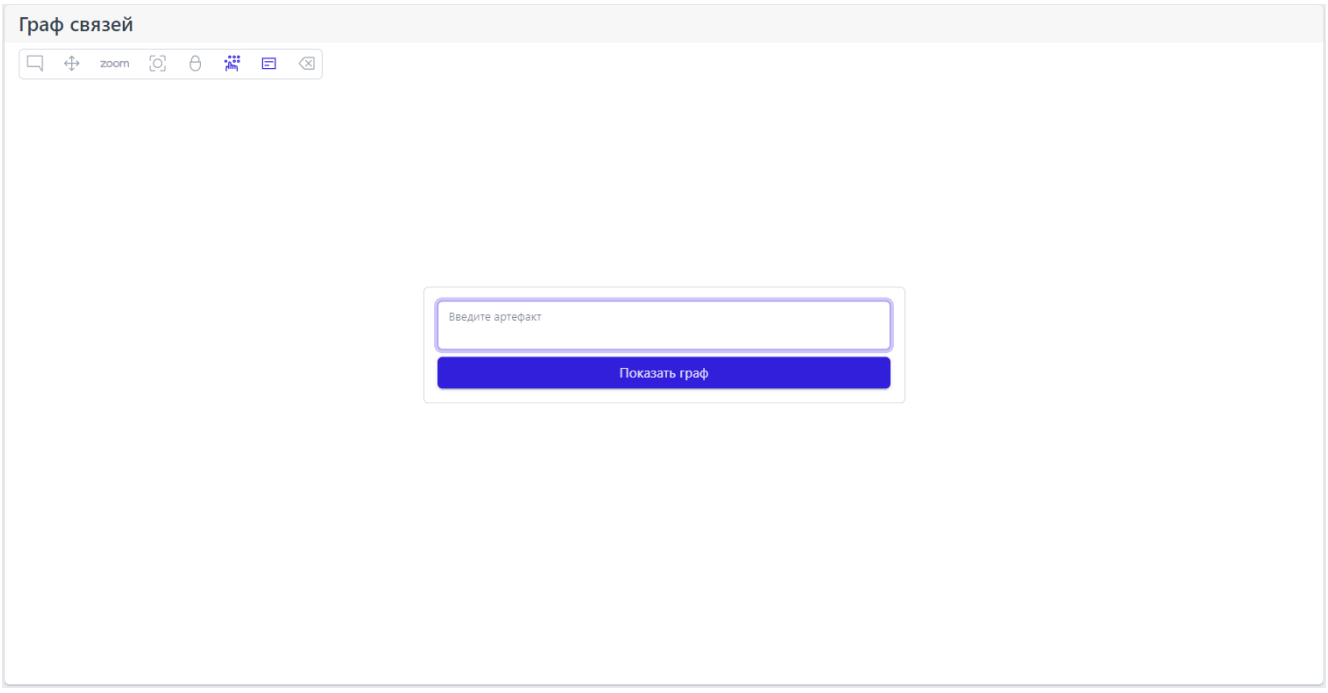


Рисунок 25 – Общий вид пустой страницы «Граф связей»

На странице имеется две области:

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

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

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

Пример отображения графа после заполнения поля артефакта в виде ip-адреса представлен на рисунке 26.

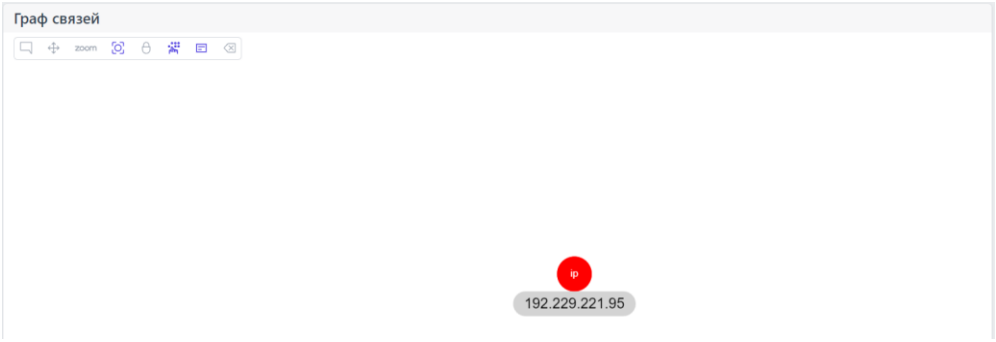


Рисунок 26 – Отображение графа связей для артефакта типа ip-адрес

Пример отображения графа связей для артефакта типа домен с привязанными артефактами представлен на рисунке 27.

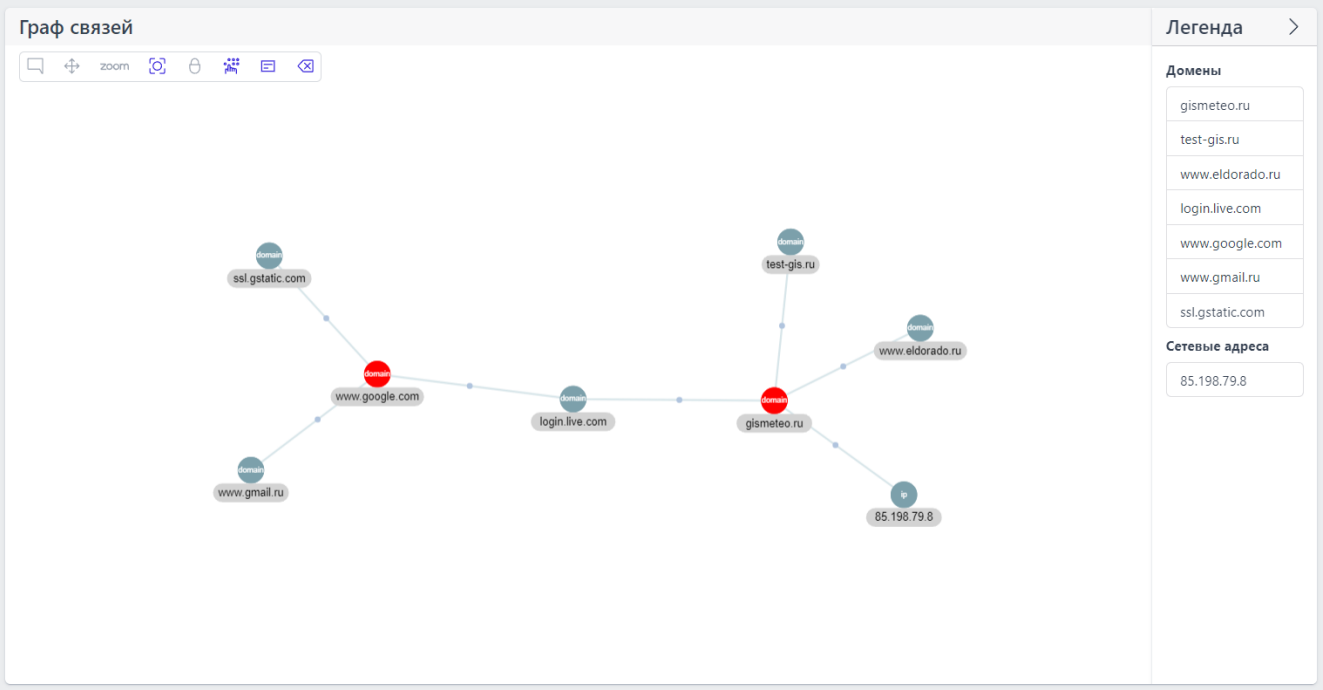


Рисунок 27 – Отображения графа связей для артефакта типа домен с привязанными артефактами

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

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

При нажатии ЛКМ по круглой области отрисовки графа отображается краткая информация об артефакте (смотри рисунок 28).

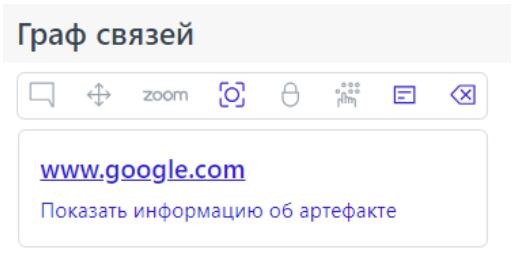


Рисунок 28 – Краткая информация по артефакту

При нажатии в данной области по иконке **Показать информацию об артефакте** появляется окно, представленное на рисунке29.

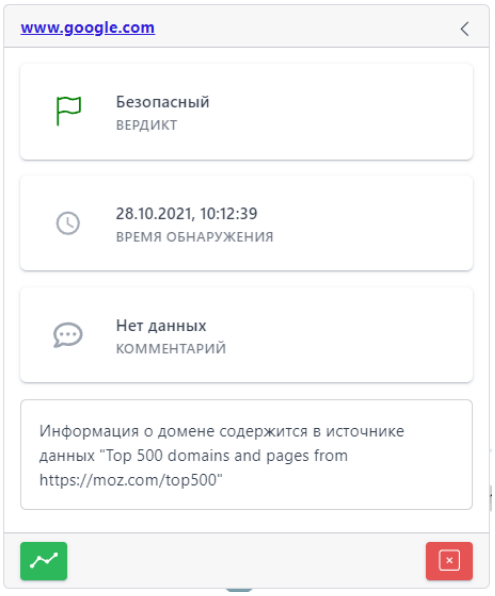


Рисунок 29 – Информация о артефакте

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

Для привязки нового артефакта следует нажать по иконке  , после чего появляется окно для внесения информации по привязанному артефакту, представленное на рисунке 30.

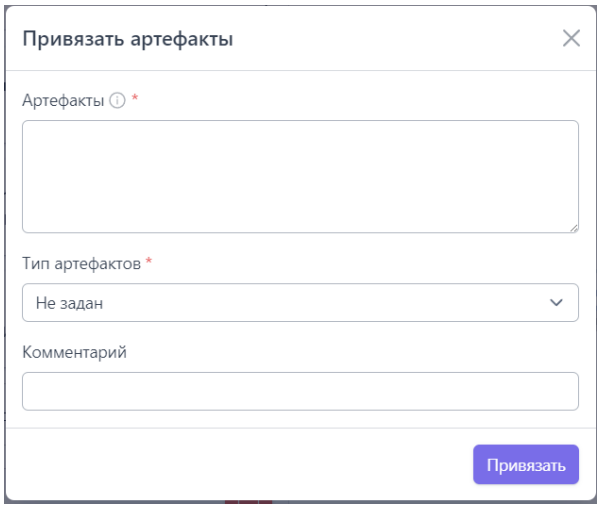


Рисунок 30 – Окно добавления информации для привязывания артефакта

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

Для удаления узла графа из привязанных артефактов следует нажать по иконке  .

7. Действия после сбоя и ошибки

7.1 Общие сведения

Большинство ошибок можно разделить на следующие типы:

1) ошибки конфигурации:

– некорректные настройки параметров безопасности;

– некорректная установка компонентов программы;

– некорректные действие со стороны пользователя/администратора;

– критические ошибки.

2) ошибки оборудования:

– выход из строя аппаратных средств, на которых установлена программа;

– выход из строя сервера (или компонентов на сервере) с которыми взаимодействуют компоненты программы, установленные на оборудовании пользователя;

– перебои питания со стороны серверной части.

Для устранения ошибки требуется обратиться к поставщику программы.

8. Перечень сокращений

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

Таблица 7 – Перечень сокращений

ЛКМ	Левая кнопка мыши
ПКМ	Правая кнопка мыши
ПО	Программное обеспечение
ФСТЭК	Федеральная служба по техническому и экспортному контролю
URL	Uniform Resource Locator