RT Protect TI

Руководство пользователя

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

Оглавление

1. Общие положения

Настоящий документ является руководством пользователя программы «RT Protect TI».

В документе приведены общие сведения, рекомендации по использованию программы и решению типичных проблем.

Данное руководство кратко можно идентифицировать согласно таблице 1.

Таблица 1 – Идентификация документа

Название документа	«RT Protect TI» Руководство Пользователя
Версия документа	Версия 1.0.20 (актуальна для версии продукта frontend 0.8.3/backend 2.9.4)
Идентификация программы	Сервис по предоставлению аналитики «RT Protect TI»
Идентификация разработчика	АО «РТ-Информационная безопасность»

2. Общие сведения

Программа RT Protect TI – сервис компании АО «РТ-Информационная безопасность», предназначенный для сбора и анализа данных угроз информационной безопасности. Решение предоставляет актуальные сведения об угрозах, что позволяет оперативно выявлять события информационной безопасности и эффективно расследовать инциденты. Кроме того, посредством портала пользователи получают глобальные исследовательские и аналитические материалы о киберугрозах.

3. Назначение программы

3.1 *Основные задачи и возможности*

Основные задачи и возможности сервиса «RT Protect TI» можно кратко описать согласно следующему списку:

1) Широкая система администрирования пользователей сервиса (пользователи; организации; источники данных);

2) Проверка артефактов вредоносной активности (IP-адрес, доменное имя, URL, файлы);

3) Работа в автономном режиме и режиме интеграции с системами защиты конечных точек;

4) Предоставление информации о распространенных угрозах, проверенных с помощью сервиса;

5) Взаимодействие с иными сервисами проверки артефактов (VirusTotal, RST Cloud и другие);

6) Предоставление вердикта по артефактам;

7) Создание и хранение аналитики для предоставления во внешние сервисы (индикаторы атак, индикаторы компрометации, yara-правила, журналы Windows);

8) Создание и хранение наборов с исключениями (для программ и файлов);

9) Регистрация действий пользователей сервиса.

3.2 *Способы отражения предметной области в программе*

Программа предназначена для проверки артефактов вредоносной активности, полученных из различных источников.

Сервис развертывается на мощностях предприятия разработчика. Сервис является облачным решением, для взаимодействия с которым пользователю

предоставляется открытое API. Взаимодействие с сервисом возможно через браузер.

Сервис также может быть развернут на мощностях Заказчика, есть возможность установки On-Premise.

4. Роли пользователей, взаимодействующих с Сервисом

Для обеспечения эффективного функционирования Сервиса необходимо наличие следующих групп пользователей, которые взаимодействуют с Сервисом:

– пользователь;

– аналитик;

– администратор безопасности.

Пользователь – сотрудник отдела информационной безопасности (далее ИБ) или Центра обеспечения безопасности (SOC), которому предоставлен доступ для использования сервиса с целью получения информации по обнаруженным артефактам информационной безопасности.

Аналитик – сотрудник отдела информационной безопасности (далее ИБ) или Центра обеспечения безопасности (SOC), который выполняет функцию экспертной оценки артефактов, возникающих в анализируемой Сервисом IT-инфраструктуре. Аналитик с помощью доступного для него функционала Сервиса (анализа полученных артефактов сторонними сервисами, собственного анализа) выносит вердикт по артефактам, которые потенциально могут нарушить работу защищаемых устройств или защищаемой сети в целом.

Администратор безопасности – уполномоченный сотрудник организации Заказчика или Центра обеспечения безопасности. Администратор настраивает Сервис для его корректной и полнофункциональной работы.

5. Порядок взаимодействия с сервисом

Взаимодействие с Сервисом возможно по открытому API, либо через браузер, перейдя по ссылке https://ti.rt-protect.ru. При переходе по ссылке для входа на Сервис требуется пройти процедуру авторизации, описанную в документе «Руководство Администратора RT Protect TI».

6. Операции, доступные пользователю программы

6.1 Общие сведения

Интерфейс сервиса «RT Protect TI», доступный для учетных записей с ролью «Пользователь» для пользователей организации, являющейся владельцем платформы, позволяет выполнять следующие действия:

– используя функционал главной страницы, просматривать сводную информацию по активности в организациях, подключенных к сервису;

– просматривать информацию об организациях, подключенных к сервису;

– добавлять и просматривать теги для удобства категорирования источников данных;

– используя функционал разделов аналитики просматривать информацию об артефактах и обнаружениях в организациях, подключенных к сервису;

– просматривать отчеты об анализе артефактов, обнаруженных в организациях;

– просматривать связи артефактов между собой в разделе **Граф связей**.

6.2 *Главная страница*

Интерфейс главной страницы сервиса «RT Protect TI», доступный для учетных записей с ролью «Пользователь» (для организации-владельца платформы), представлен на рисунке 1.

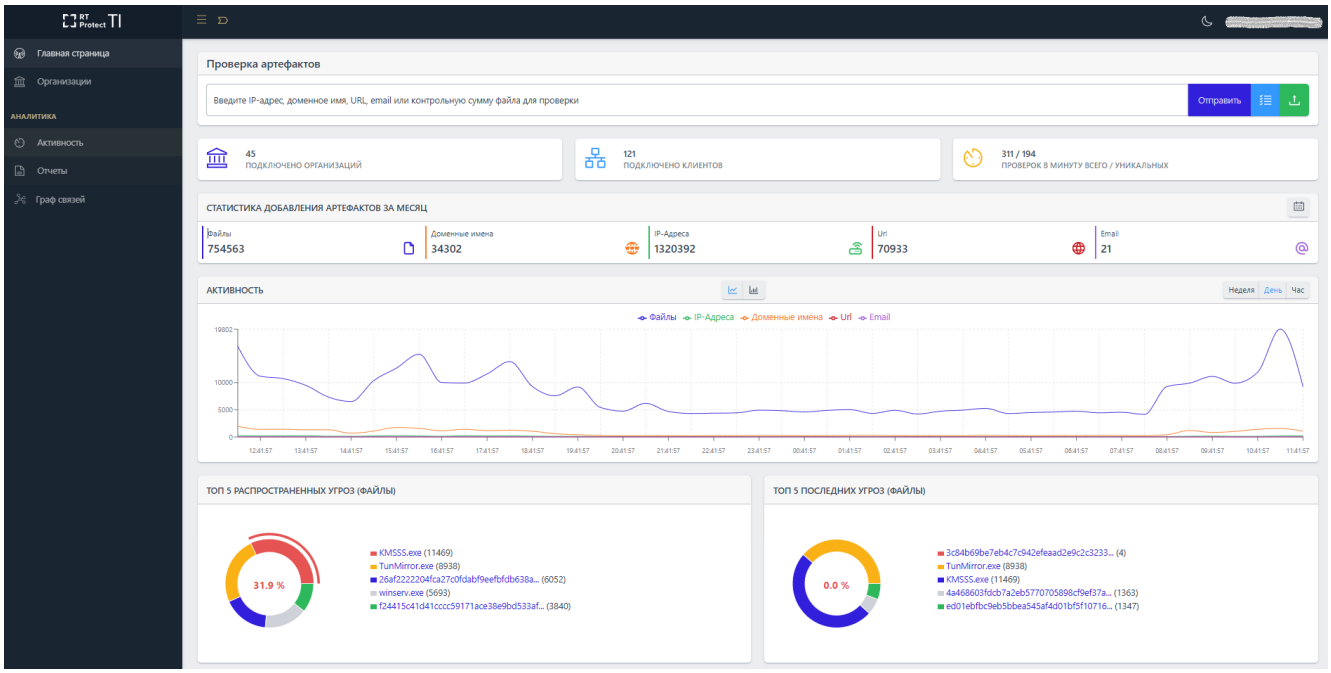


Рисунок 1 – Главная страница

Пользователь может проводить проверки артефактов (домены, ip-адреса, URL и хеш-суммы по алгоритмам SHA-256, SHA-1 и MD5, а также email). Чтобы выполнить проверку, необходимо ввести значение артефакта в строке **Проверка артефактов** и нажать кнопку **Отправить**. Кроме того, пользователь может загрузить для проверки исполняемый файл для его анализа в песочницах и с использованием сервисов, предоставляющих аналитику онлайн, по запросу (например, VirusTotal), для этого необходимо нажать кнопку **Загрузить файл** (), после чего выбрать в проводнике соответствующий файл и нажать кнопку **Отправить**.

В области **Проверка артефактов** пользователь также может проверить целый список артефактов, нажав по иконке  , после чего откроется окно для загрузки списка артефактов, представленное на рисунке 2.

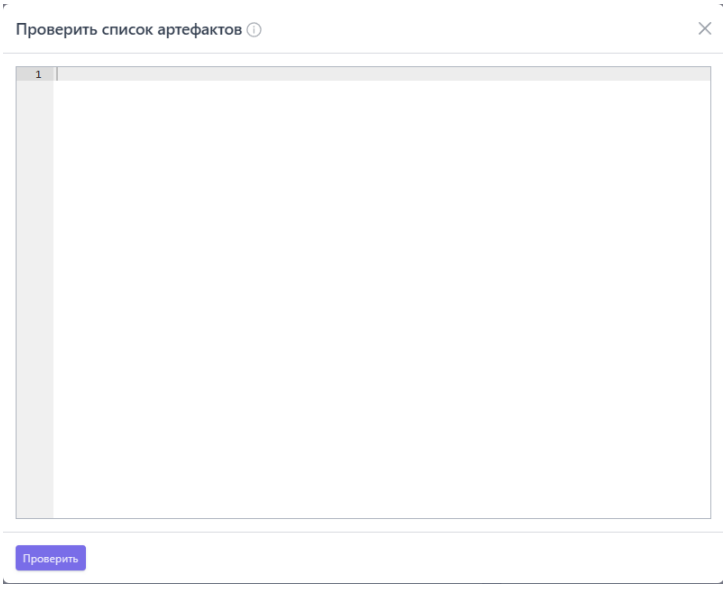


Рисунок 2 – Окно для написания списка артефактов для проверки

В данном окне артефакт добавляется по одному в каждой строчке (строчки нумеруются).

Проверка артефактов списком ограничена количеством в 100 строк.

После отправки артефактов на анализ любым из указанных способов откроется страница с отчетом. Отчет содержит несколько вкладок, которые позволяют подробно проанализировать артефакт.

В зависимости от типа артефакта список вкладок будет отличаться: это вкладки песочниц, внешних источников (например, база данных MalwareBazaar) и вкладка с данными сервиса VirusTotal.

В правом верхнем углу страницы имеются иконки  /  для смены цветовой схемы экрана (темной или светлой тем).

Также в правом верхнем углу находится иконка с именем, идентифицирующая пользователя, который произвел вход в программу на данный момент. При нажатии по данной иконке происходит переход в окно выбора действий, представленное на рисунке 3.

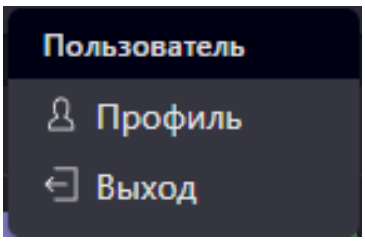


Рисунок 3 – Окно выбора действий для пользователя

В данном окне имеется возможность просмотреть профиль пользователя, либо осуществить выход из профиля.

При нажатии по иконке **Выход** появляется окно подтверждения для выхода из профиля, представленное на рисунке 4.

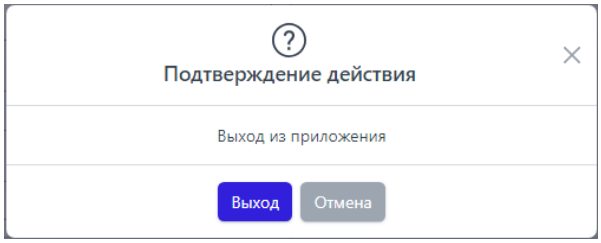


Рисунок 4 – Окно подтверждения действия выхода из приложения

Для подтверждения выхода из профиля необходимо нажать по иконке **Выход**.

Окно просмотра профиля пользователя представлено на рисунке 5.

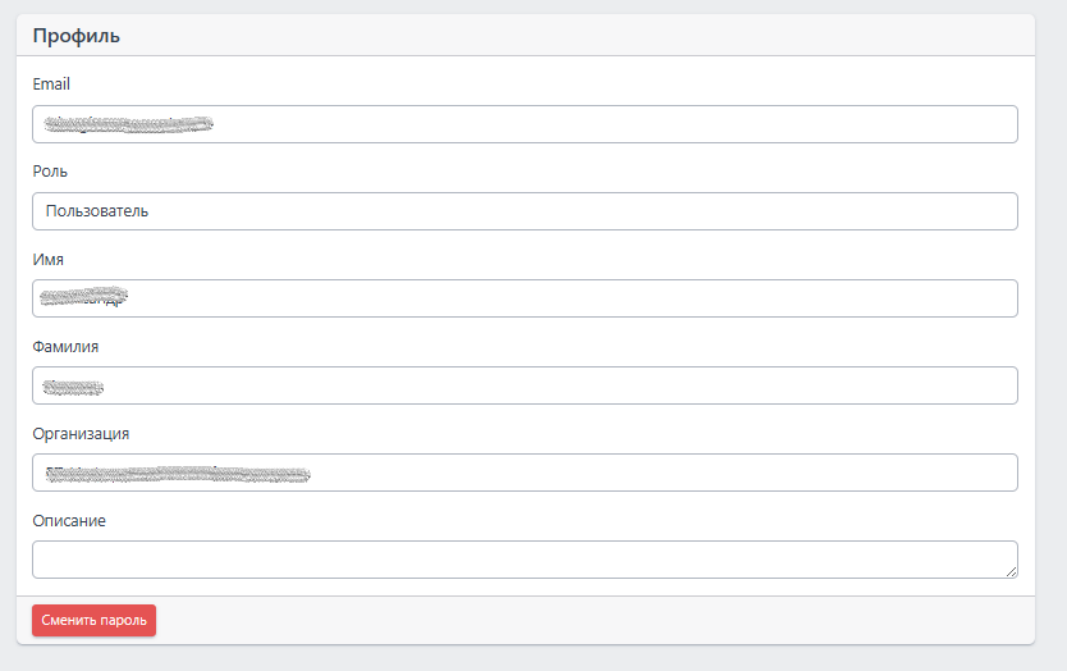


Рисунок 5 – Окно просмотра профиля пользователя

В данном окне редактировать информацию о пользователе нельзя.

Для смены пароля требуется нажать по иконке **Сменить пароль,** после чего откроется окно смены пароля, представленное на рисунке 6.

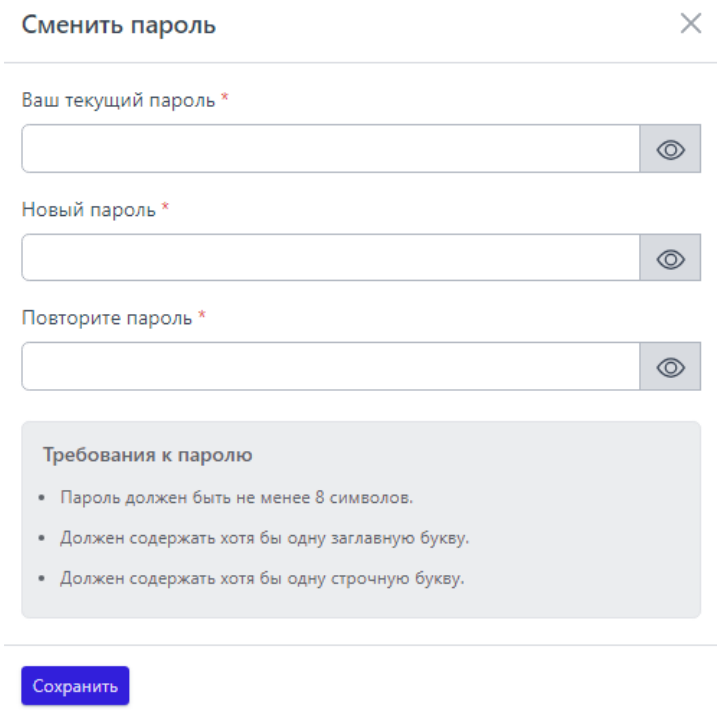


Рисунок 6 – Окно смены пароля

После смены пароля требуется нажать по иконке **Сохранить**.

На **Главной странице** пользователь имеет возможность просмотреть информацию в графическом виде об активности, распространенных и последних угрозах, а также отчеты по различным артефактам на основе источников.

6.3 *Организации*

В разделе **Организации**, представленном на рисунке 7, пользователь организации владельца платформы может просмотреть информацию обо всех организациях и клиентах, подключенных к сервису.

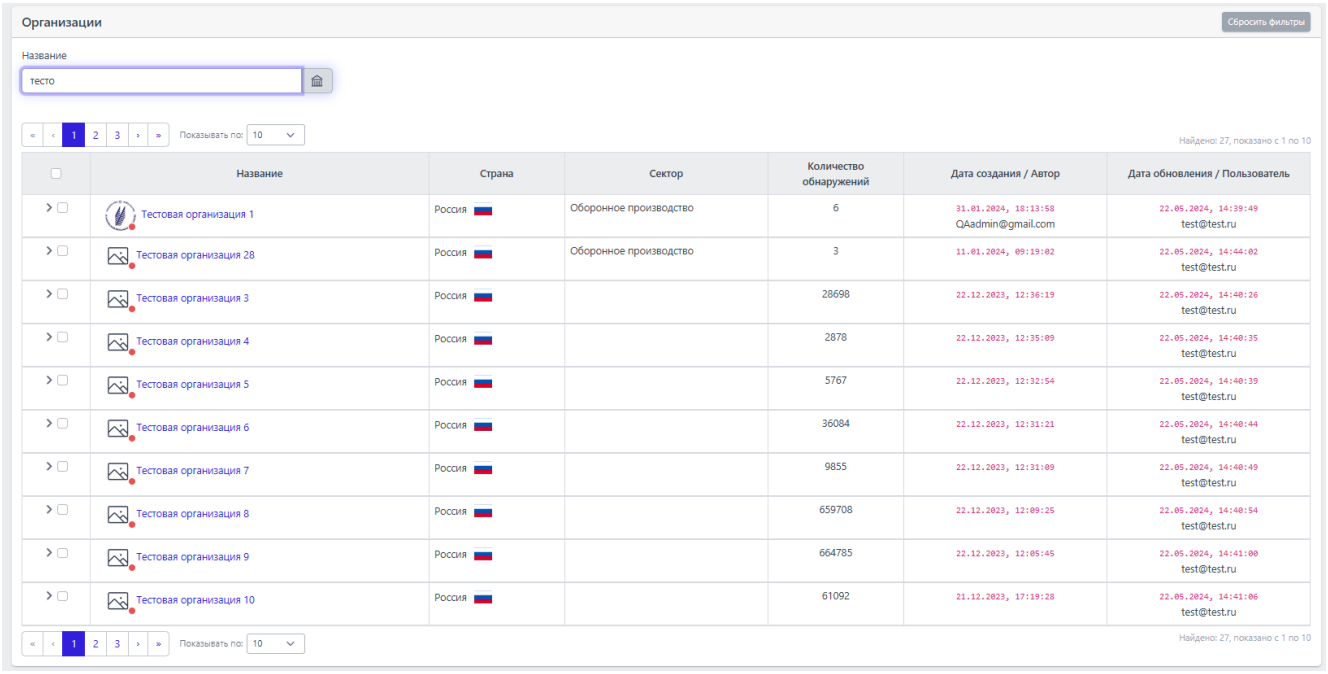


Рисунок 7 – Окно раздела «Организации»

В столбце **Название** при нажатии по имени организации пользователь может просмотреть общую информацию об организации, а также скачать отчет в формате pdf по обнаружениям в организации, нажав по иконке .

При нажатии ЛКМ по названию организации происходит переход на страницу с информацией по организации.

6.4 *Активность*

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

В верхней части страницы **Активность** имеются следующие активные вкладки Артефакты, 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 8 - 9.

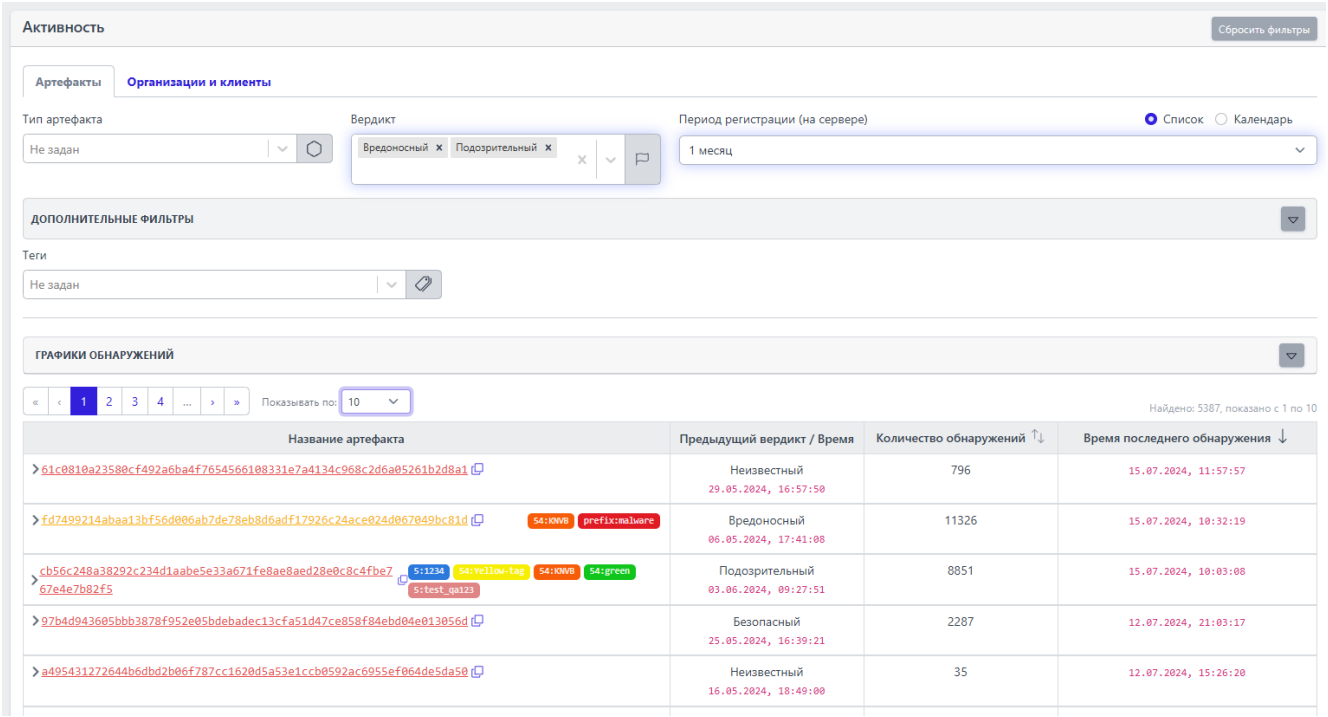


Рисунок 8 – Общий вид страницы Активность вкладки Артефакты

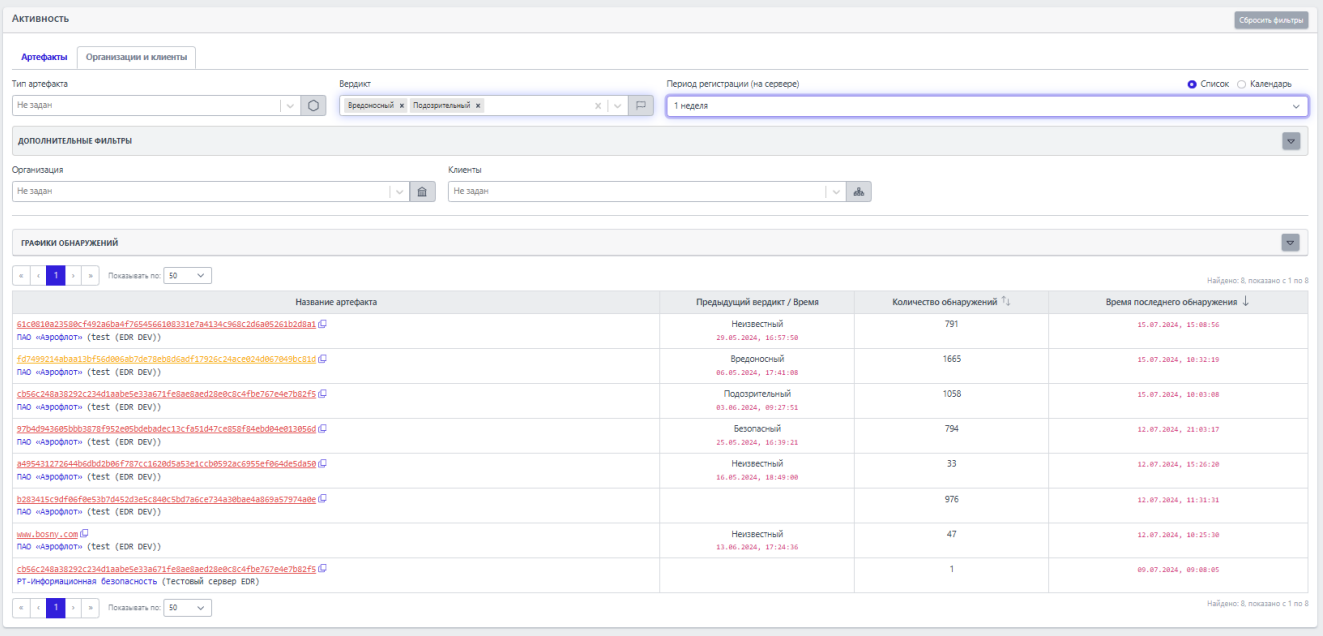


Рисунок 9 – Общий вид страницы Активность вкладки Организации и клиенты

Таблица имеет следующие поля:

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

– **Предыдущий вердикт/Время** (предыдущий вердикт по артефакту и время внесения вердикта);

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

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

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

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

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

– B73753C4C69A03F9A3E09F121B6599D77B1A4BE0247F9B71B56572555E1FE12B – неизвестный артефакт (шрифт серого цвета);

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

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

Контрольная сумма файла угрозы, а также информация по другим типам артефактов является активной ссылкой, при нажатии по которой ЛКМ открывается окно отчета TI-платформы, представленное на рисунке 10.

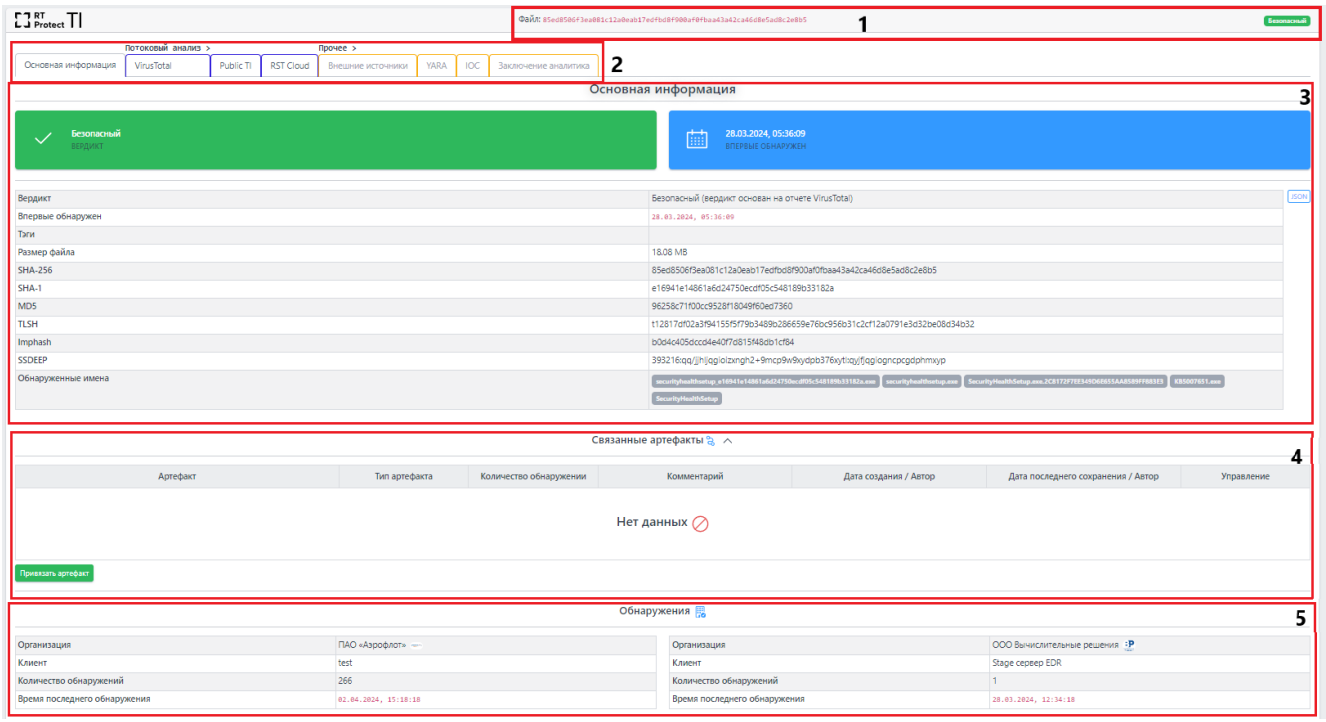


Рисунок 10 – Страница отчета сервиса по обнаруженной угрозе

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

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

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

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

Если в области вкладок запись отображается серым цветом, запрос информации по данному артефакту в том или ином сервисе недоступен. При нажатии ЛКМ по одной из вкладок появляется окно результатов по анализу артефакта (рис. 11).

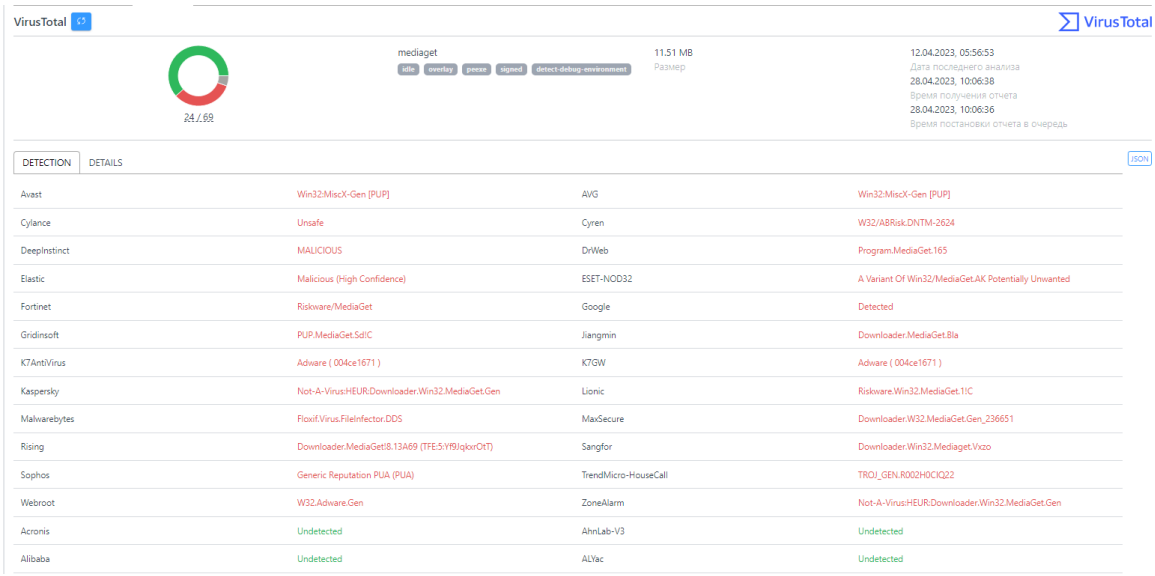


Рисунок 11 – Результаты анализа артефакта на странице Virus Total

Окно основной информации по результатам анализа артефакта в формате HTML представлено на рисунке 12.

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 12 – Информация отчета об артефакте в формате HTML

Окно основной информации по результатам анализа артефакта в формате JSON представлено на рисунке 13.

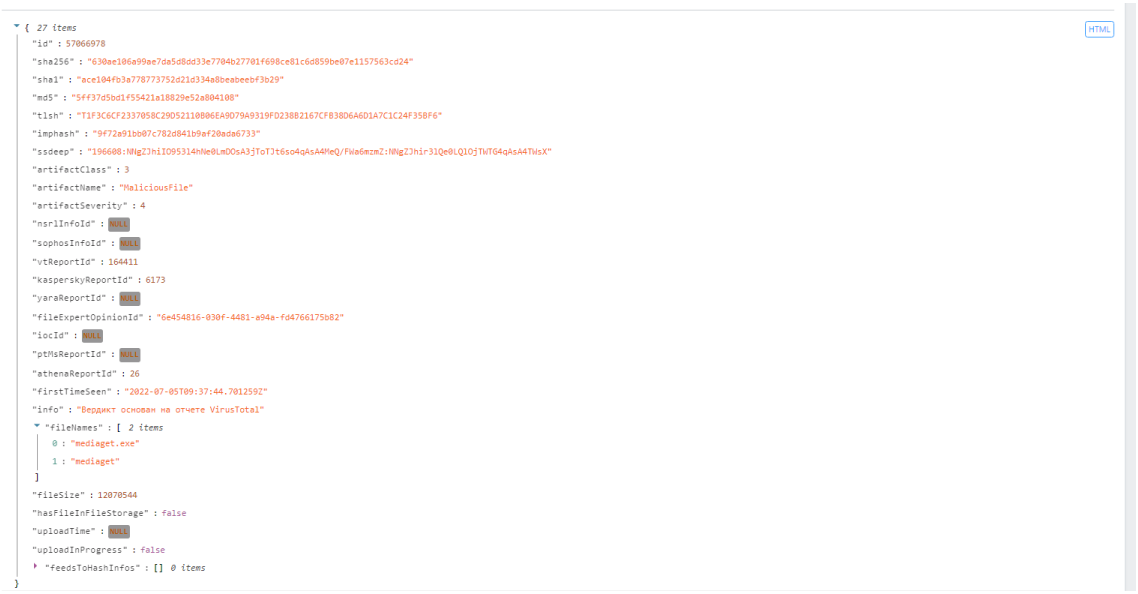


Рисунок 13 – Информация отчета об артефакте в формате JSON

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 14).

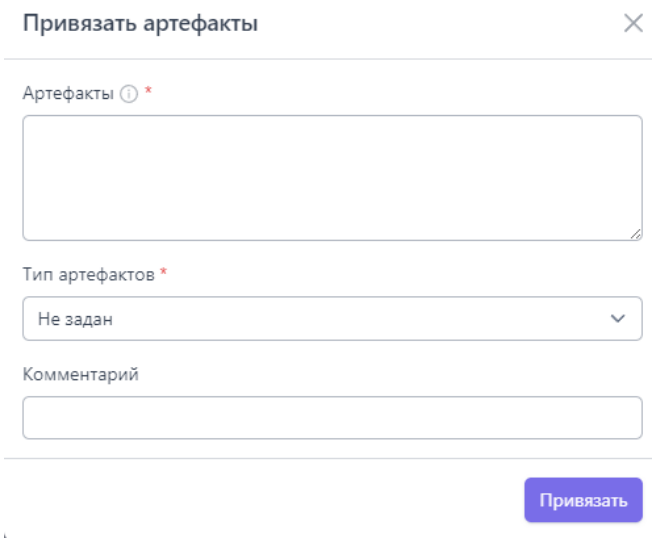


Рисунок 14 – Окно для привязки артефакта

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** вкладки **Артефакты** предусмотрена система основных фильтров, представленная в следующем списке:

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

– **Вердикт** (неизвестный, безопасный, вредоносный, подозрительный);

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

– **Теги** (теги для удобства идентификации элементов активности).

А также имеется система дополнительных фильтров, представленная 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;**

– **Предыдущий вердикт** (период регистрации на сервере);

– **Время последнего изменения вердикта.**

На странице **Активность** вкладки **Артефакты** имеется область с графическим отображением информации по обнаруженным угрозам (рисунок 15).

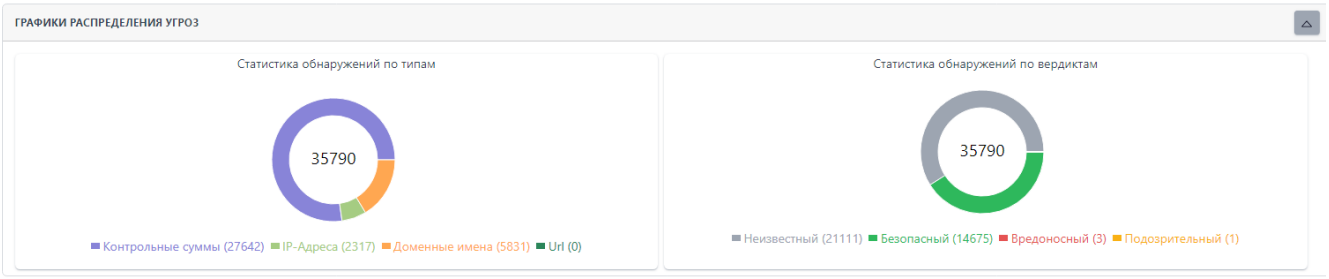


Рисунок 15 – Область графического отображения информации по обнаруженным угрозам вкладка «Артефакты»

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 **Организации и клиенты** предусмотрена система основных фильтров, представленная в следующем списке:

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

– **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**.

А также имеется система дополнительных фильтров, представленная согласно следующему списку:

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

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

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

– **Предыдущий вердикт;**

– **Время последнего изменения вердикта**;

На странице **Активность** вкладки **Организации и клиенты** имеется область с графическим отображением информации по обнаруженным угрозам (рисунок 16).

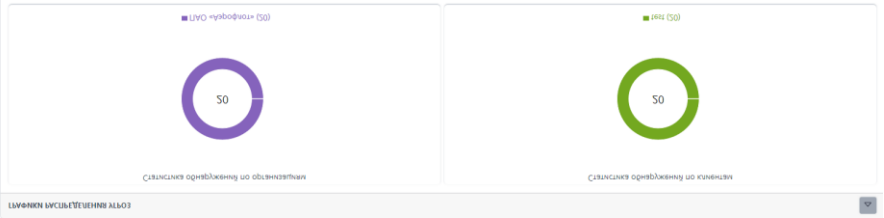


Рисунок 16 – Область графического отображения информации по обнаруженным угрозам вкладка Организации и клиенты

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

– статистика обнаружений по организациям;

– статистика обнаружений по клиентам.

6.5 *Отчеты*

В разделе **Отчеты** в табличной форме представлена информация о проверенных внешними анализаторами, для которых настроена интеграция, артефактах. Общий вид страницы представлен на рисунке 17.

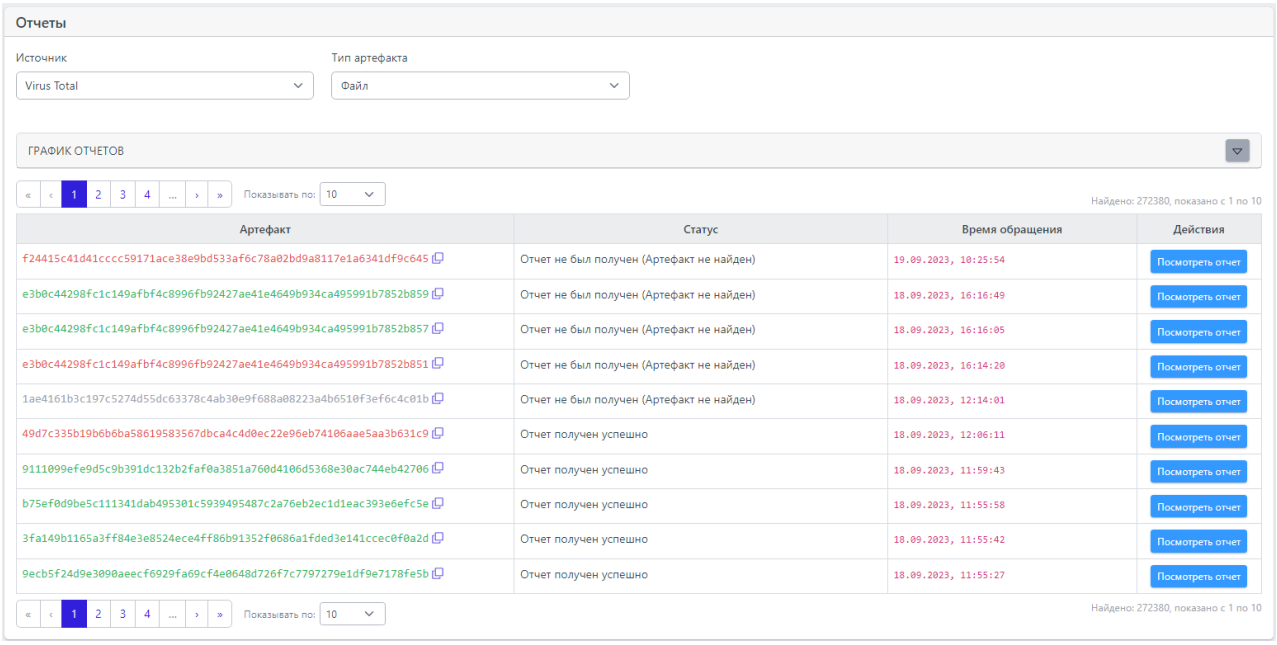


Рисунок 17 – Окно раздела «Отчеты»

В таблице имеются следующие поля:

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

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

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

– **Действия** (получить отчет).

Информация об артефакте отображается разными цветами:

– шрифт красного цвета (артефакт является вредоносным);

– шрифт зеленого цвета (артефакт является безопасным);

– шрифт серого цвета (неизвестный артефакт);

– шрифт оранжевого цвета (артефакт является подозрительным).

Над таблицей для фильтрации информации имеются следующие фильтры:

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

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

Над таблицей для отображения визуальной информации имеется область с графиком полученного числа отчетов за определенный период в зависимости от установленного в фильтре источника данных (рисунок 18).

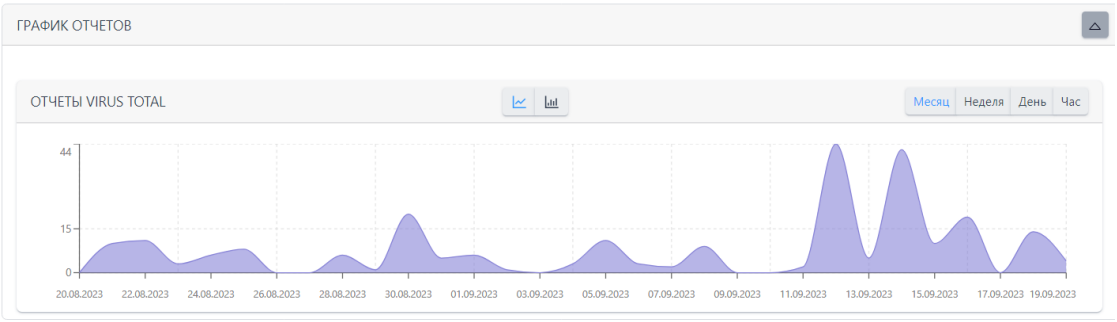
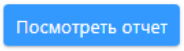


Рисунок 18 – Отчеты Virus Total

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

Для просмотра отчета по артефакту нужно нажать по иконке 

.

Страница отчета по артефакту представлена на рисунке 19.

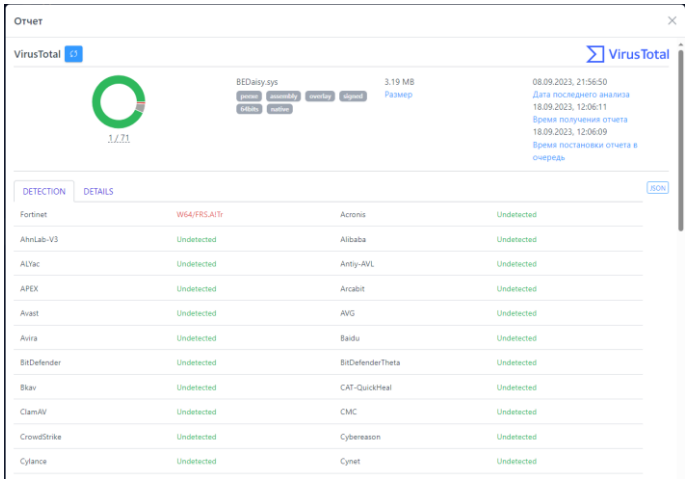


Рисунок 19 – Страница отчета по артефакту от источника Virus Total

6.6 *Граф связей*

Страница **Граф связей** с незаполненным полем артефакта представлена на рисунке 20.

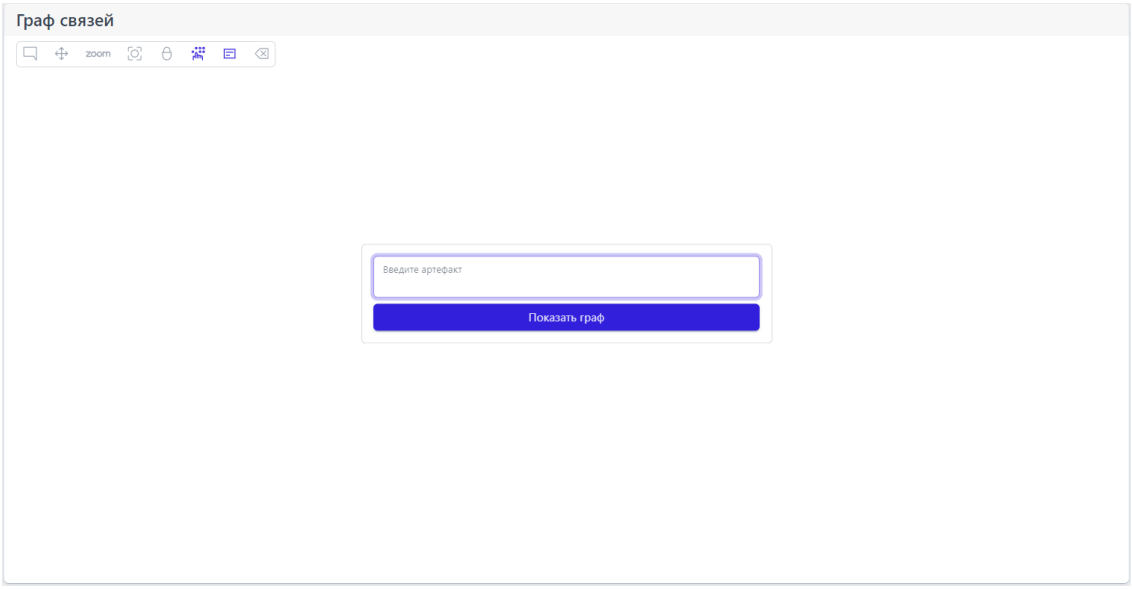


Рисунок 20 – Общий вид пустой страницы «Граф связей»

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 21.

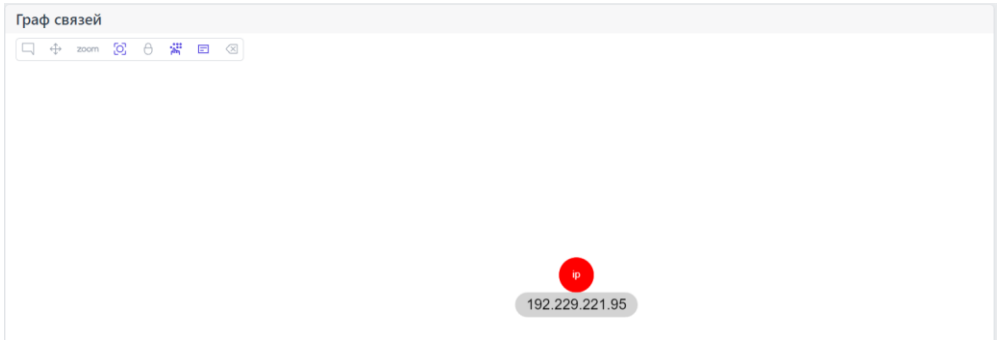


Рисунок 21 – Отображение графа связей для артефакта типа ip-адрес

Пример отображения графа связей для артефакта типа домен, с привязанными артефактами представлен на рисунке 22.

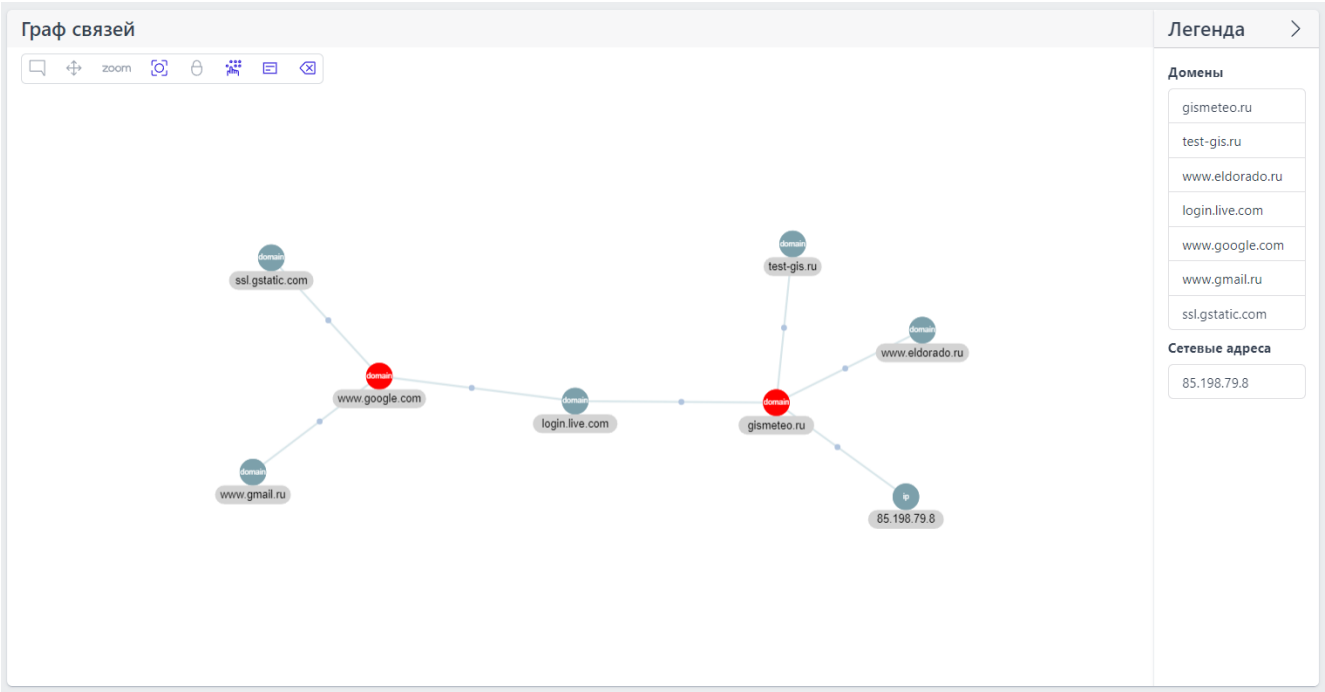


Рисунок 22 – Отображения графа связей для артефакта типа домен, с привязанными артефактами

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

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

При нажатии ЛКМ по круглой области отрисовки графа отображается информация об артефакте (смотри рисунок 23).

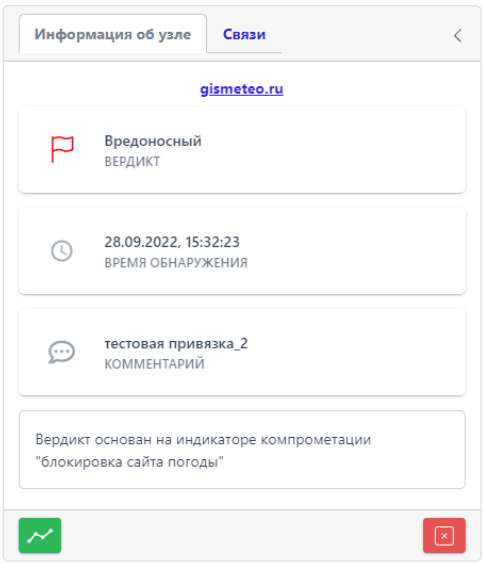


Рисунок 23 – Информация по артефакту

При нажатии по активной области **Связи** появится окно, показывающее список связей данного артефакта (рисунок 24).

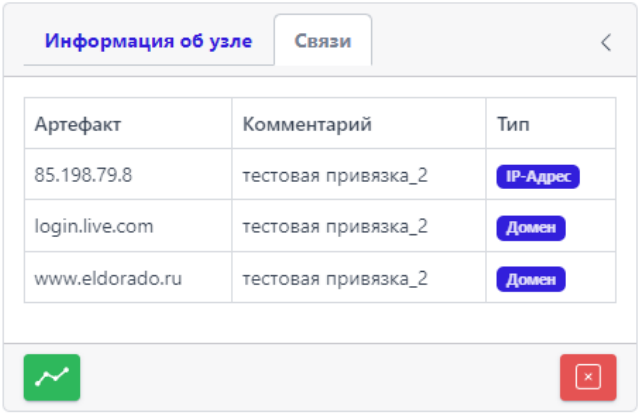


Рисунок 24 – Связи по данному артефакту

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

Для привязки нового артефакта к выбранному артефакту следует нажать по иконке  , после чего появляется окно для внесения информации по привязанному артефакту, представленное на рисунке 25.

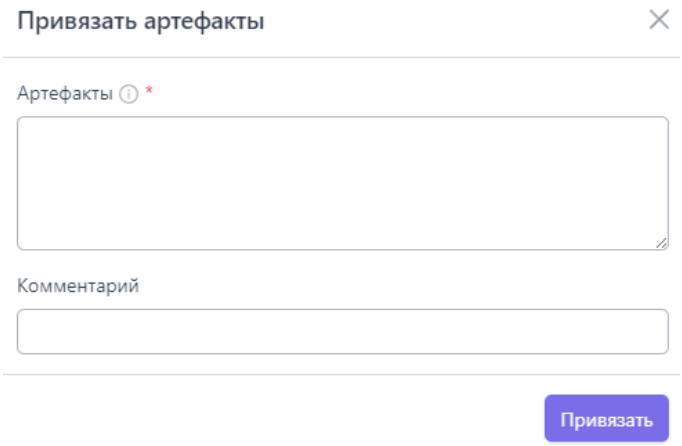


Рисунок 25 – Окно добавления информации для привязывания артефакта

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

Для удаления связи между двумя артефактами из привязанных артефактов следует нажать по иконке  , после чего появится окно указания того, какую связь и для какого узла требуется удалить (рисунок 26).

Рисунок 26 – Удаление связей между артефактами

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

7. Сообщения об ошибках

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 Изделия, установленные на оборудовании пользователя;

– перебои питания со стороны клиентской или серверной части.

При возникновении ошибки пользователю не следует самостоятельно заниматься устранением ошибки. Пользователь обращается к администратору, который согласно процедурам, описанным в документе «Руководство администратора RT Protect TI», устраняет выявленные ошибки.

8. Термины и определения

Перечень терминов и определений указан в таблице 2.

Таблица 2 – Термины и определения

Информационная безопасность (ИБ)	Сфера науки и техники, охватывающая совокупность проблем, связанных с обеспечением защищенности объектов информационной сферы в условиях существования угроз. Под информационной безопасностью также понимают защищенность информации от несанкционированного ознакомления, преобразования и уничтожения, защищенность информационных ресурсов от воздействий, направленных на нарушение их работоспособности
Инцидент ИБ	Нарушение или угроза нарушения ИБ компании
URL	Унифицированный указатель ресурса
API	Интерфейс прикладного программирования
SOC	Центр обеспечения компьютерной безопасности
ОС	Операционная система
Событие ИБ	Любое идентифицированное явление в системе или сети
Угроза ИБ	Потенциально возможное событие, действие (воздействие), процесс или явление, создающее опасность возникновения инцидента ИБ
Уязвимость информационной системы (ИС)	Недостаток в ИС, используя который внешний злоумышленник может намеренно реализовать угрозу ИБ

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».