Веб-сервис RT Protect TI

Руководство администратора

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

RT Protect

Оглавление

1. Общие положения 4
1.1 Идентификация документа 4
1.2 Аннотация документа 4
1.3 Термины и определения 4
1.4 Условные обозначения 7
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 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» 18
6.3 Главная страница 19
6.4 Администрирование 21
6.4.1. Пользователи 22
6.4.2. Организация 29
6.5 Аналитика 32
6.5.1. Активность 32
6.5.2. Отчеты 39

6.5.3. Граф связей 41
6.6 Параметры 44
6.6.1. Журнал действий 44
6.6.2. Интеграции 48
7. Сообщения администратору 49
7.1 Общие сведения 49
7.2 Сообщения об ошибках 49
7.2.1. Общие сообщения 49
7.2.2. Специфичные сообщения 51
8. Действия после сбоя и ошибки 54
8.1 Общие сведения 54
9. Перечень сокращений 55
10. Заключение 56

1. Общие положения

1.1 Идентификация документа

Данное руководство кратко можно идентифицировать согласно таблице 1.

Таблица 1 – Идентификация документа

Название документа	«Веб-сервис RT Protect TI» Руководство Администратора
Версия документа	Версия 1.0.20 (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»

1.2 Аннотация документа

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

Документ предназначен для пользователей сервиса в рамках организации, не являющейся владельцем TI-платформы, и содержит общие сведения о программе, организационно-распорядительные меры, сведения о структуре, описание настроек программы и тексты сообщений, выдаваемых в ходе выполнения настройки, проверки, а также о процессе функционирования программы.

1.3 Термины и определения

В настоящем документе используются термины и определения согласно ГОСТ Р ИСО/МЭК 15408 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных

технологий» и ГОСТ Р ИСО/МЭК 12207-2010 «Информационная технология. Системная и программная инженерия. Процессы жизненного цикла программных средств» согласно таблице 2.

Таблица 2 – Термины и определения

Термин	Описание
Администратор	Уполномоченный пользователь, ответственный за установку, администрирование и эксплуатацию программы
Артефакты	Различные типы данных имеющие подозрительное содержимое и загружаемые на сервер для анализа (файлы, доменные имена, IP-адреса, URL)
Backend	Программно-аппаратная часть сервиса, отвечающая за функционирование его внутренней части
JSON	Текстовый формат обмена данными, основанный на JavaScript
JSON-объект	Неупорядоченный набор пар ключ/значение. Объект начинается с открывающей фигурной скобки { и заканчивается закрывающей фигурной скобкой }. Каждое имя сопровождается двоеточием, пары ключ/значение разделяются запятой
Linux	Семейство Unix-подобных операционных систем на базе ядра Linux
Malware Bazaar	Проект сайта abuse.ch, целью которого является обмен образцами вредоносного ПО с сообществом информационной безопасности, поставщиками антивирусных программ и поставщиками информации об угрозах
SSDEEP	Алгоритм нечеткого хеширования
TCP	Один из основных протоколов передачи данных интернета. Предназначен для управления передачей данных интернета. Пакеты в TCP называются сегментами. В стеке протоколов TCP/IP выполняет функции транспортного уровня модели OSI
VirusTotal	Бесплатная служба, осуществляющая анализ подозрительных файлов и ссылок (URL) на предмет выявления вирусов, червей, троянов и всевозможных вредоносных программ
Web-сервер	Сервер, принимающий HTTP-запросы от клиентов, чаще всего веб-браузеров, и выдающий HTTP-ответы, как правило, вместе с HTML-страницей, изображением, файлом, медиа-потоком или другими данными

Термин	Описание
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
	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;

– просмотр информации о программах и уязвимостях, зарегистрированных для данных программ.

Программа функционирует под управлением ОС Linux Ubuntu 20.04.5 LTS.

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

Программа предназначена для обработки информации, не являющейся секретной.

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

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

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

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

3. Организационно-распорядительные меры

3.1 Общие сведения

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

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

Программа поставляется заказчику согласно комплектности поставки.

3.2 Комплектность поставки

Комплектность поставки представлена в таблице 4.

Таблица 4 – Комплектность поставки

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

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

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

– обеспечивают идентификацию и целостность программы во время пересылки;

– обеспечивают обнаружение несанкционированных модификаций программы;

– препятствуют попыткам подмены программы от имени разработчика.

4. Структура программы

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

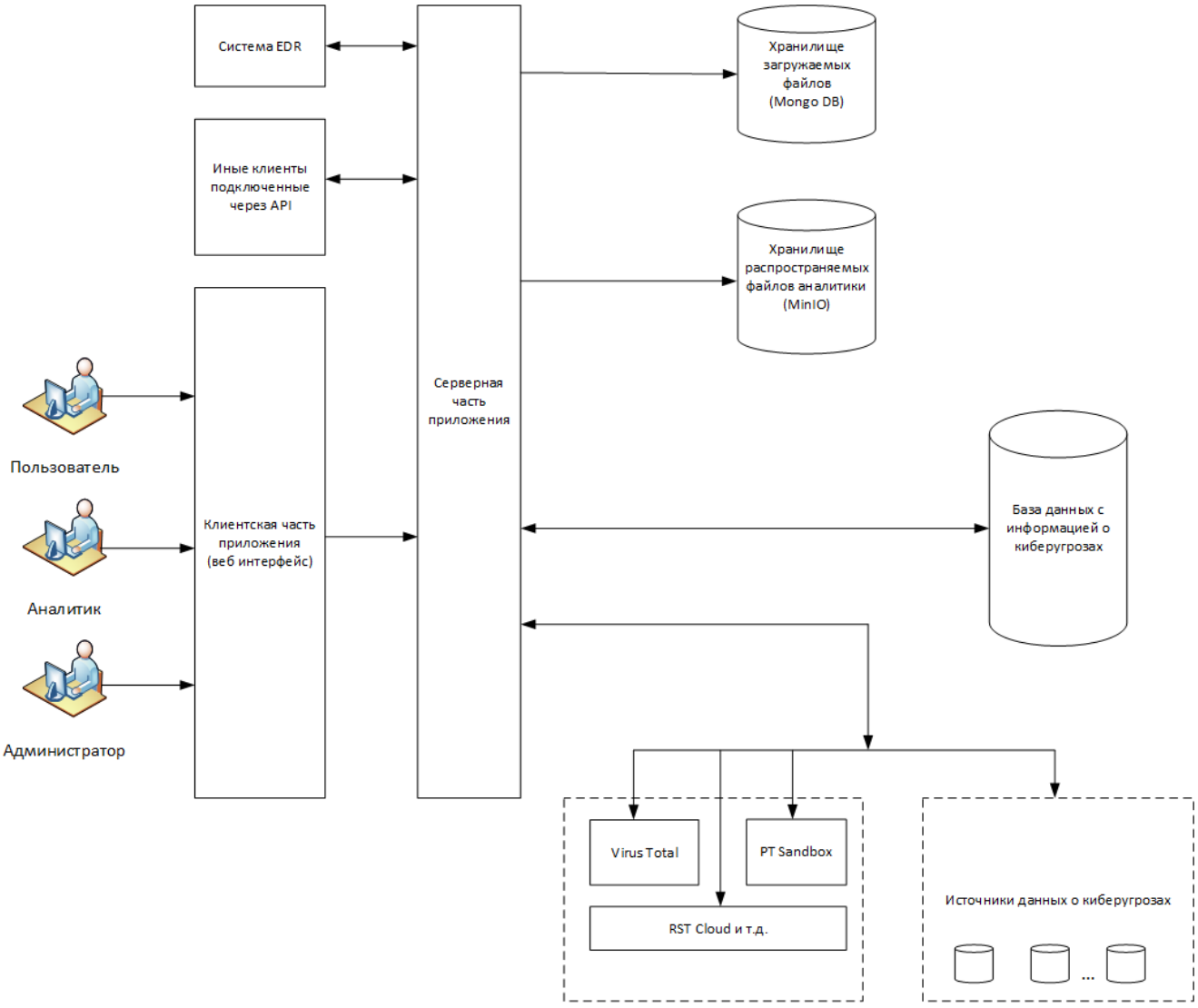


Рисунок 1 – Схема архитектуры сервиса

5. Настройка программы

5.1 Требования к среде функционирования

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

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

Программа поддерживает работу в браузерах, представленных в таблице 5.

Таблица 5 – Список поддерживаемых браузеров

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

5.2 Роли

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

– пользователь.

– аналитик;

– администратор.

Пользователь – сотрудник отдела ИБ или SOC-центра.

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

– **Главная страница;**

– **Организация;**

– **Активность;**

– **Отчеты;**

– **Граф связей.**

Сотруднику с ролью «Пользователь» доступны следующие действия:

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

– IP-адрес;

– доменное имя;

– URL;

– контрольную сумму файла (хеш-суммы).

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

3) просмотр страницы отчета по проверенному артефакту.

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

В круг типовых задач аналитика входят:

– проверка артефактов;

– анализ активности;

– просмотр отчетов об артефактах.

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

6. Интерфейс программы

6.1 Окно авторизации и общие сведения

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

Рисунок 2 – Окно авторизации

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

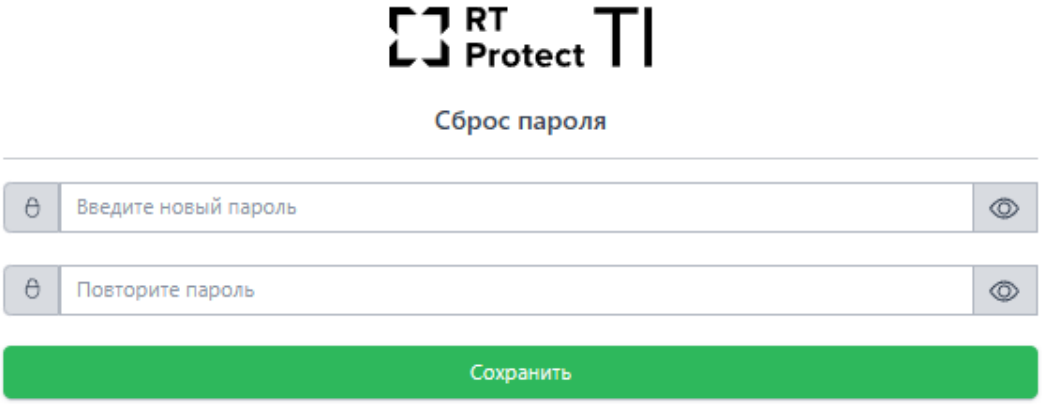


Рисунок 3 – Окно ввода параметром для сброса пароля

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 администратора открывается основное окно программы (рис. 4).

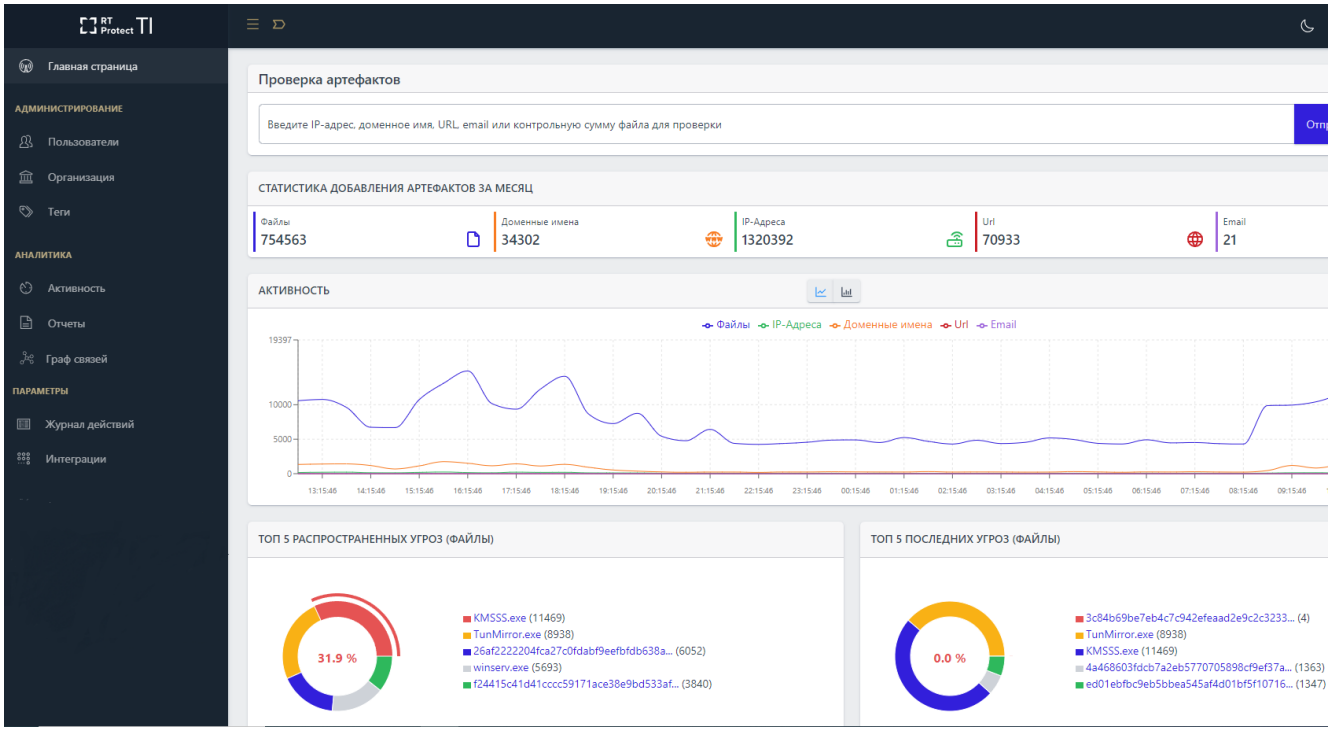


Рисунок 4 – Основное окно программы

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

Функции, доступные в интерфейсе административного модуля управления:

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

– администрирование пользователей, взаимодействующих с сервисом;

– выпуск токенов для подключения программ (например, EDR);

Важно

Клиенты с помощью токена получают доступ к API платформы TI.

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

– просмотр отчетов по анализу проверенных артефактов;

– просмотр действий пользователей, произведенных в модуле администрирования программы;

– просмотр уязвимостей и программ с найденными уязвимостями.

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

В нижней части страницы находится информация о товарном знаке компании – RT Protect © 2024. Справа от текущей версии программы отображается надпись о том, где «RT Protect TI» разработана – Сделано в России.

6.2 Горизонтальная панель управления

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

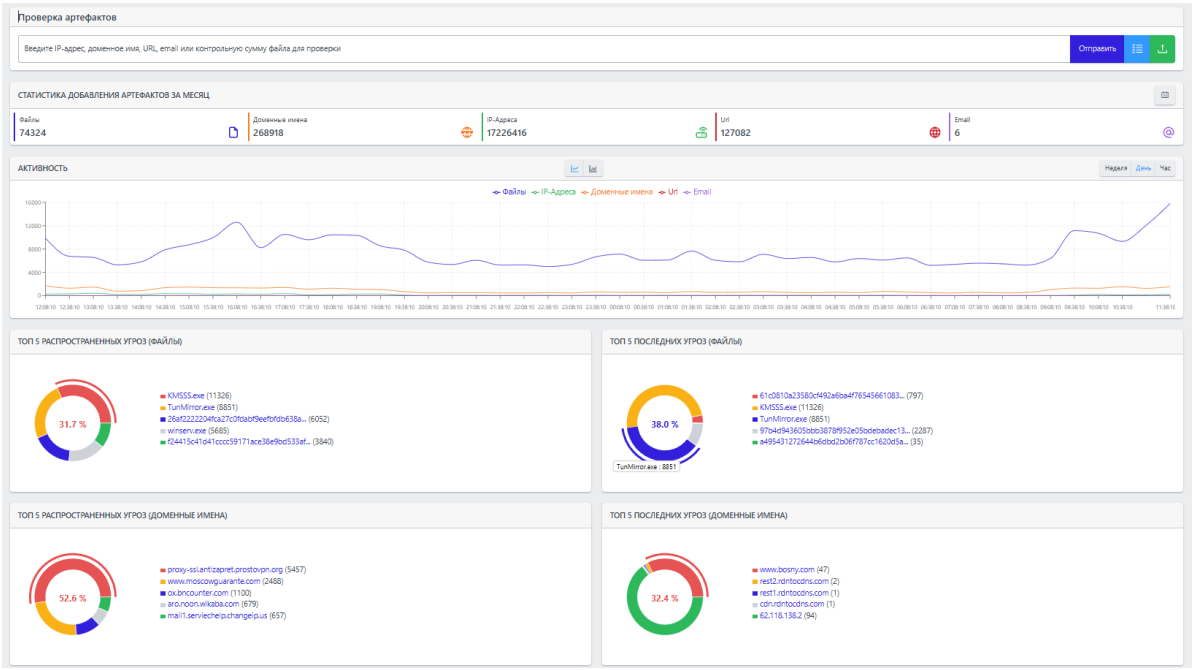


Рисунок 6 – Основное окно программы при скрытой панели разделов

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

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).

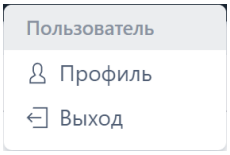


Рисунок 7 – Меню «Пользователь»

Подменю **Профиль** представлено на рисунке 8.

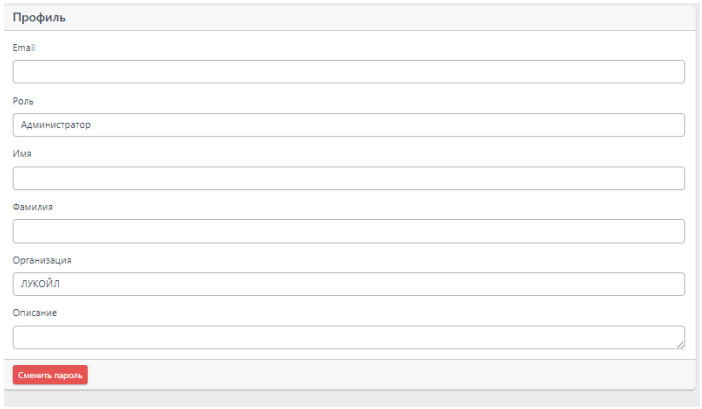


Рисунок 8 – Подменю «Профиль»

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

– адрес электронной почты для своей учетной записи;

– роль, назначенная пользователю (**Администратор**, **Пользователь**, **Аналитик**);

– имя и фамилия пользователя;

– организация;

– 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).

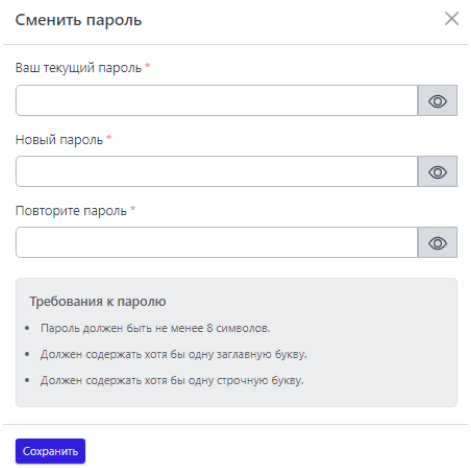


Рисунок 9 – Окно смены пароля

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

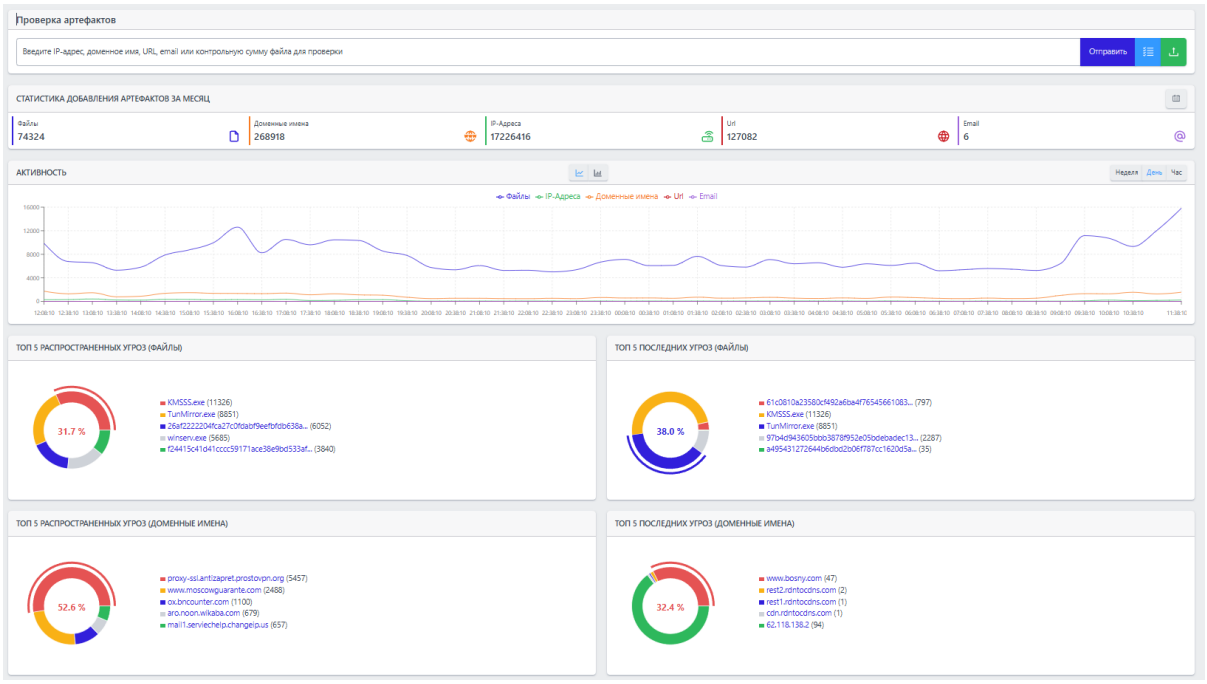


Рисунок 10 – Главная страница

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

– область проверки артефактов;

– графическое представление активности (отображение обнаружений);

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

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

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

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

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

Откроется отчет TI-платформы (подробнее см. в пункте 6.5.1). Также в области проверки артефактов с помощью кнопки **Загрузить файл** () можно проверить файлы на компьютере, с которого осуществлен доступ к TI-серверу. После нажатия кнопки  откроется проводник, в котором можно выбрать файл, нуждающийся в проверке. Далее файл загружается на TI-платформу, а после завершения его загрузки выводится отчет с вердиктом.

В области **Проверка артефактов** администратор также может проверить целый список артефактов, нажав по иконке  , после чего откроется окно для загрузки списка артефактов, представленное на рисунке 11.

Рисунок 11 – Окно для написания списка артефактов для проверки

В данном окне артефакт добавляется по одному в каждой строчке. 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:

– **Пользователи;**

– **Организация;**

– **Теги.**

Администратор может выполнять следующие действия:

– просматривать информацию о пользователях;

– создавать и удалять учетные записи пользователей;

– изменять параметры учетных записей пользователей;

– выпускать токены для клиентов в рамках организации;

– назначать квоты на использование вызовов API в рамках пользователей своей организации;

– просматривать теги и псевдонимы для ранжирования элементов активности.

6.4.1. Пользователи

В разделе **Пользователи** в табличном виде показана информация о зарегистрированных в программе пользователях принадлежащих данной организации (рисунок 12).

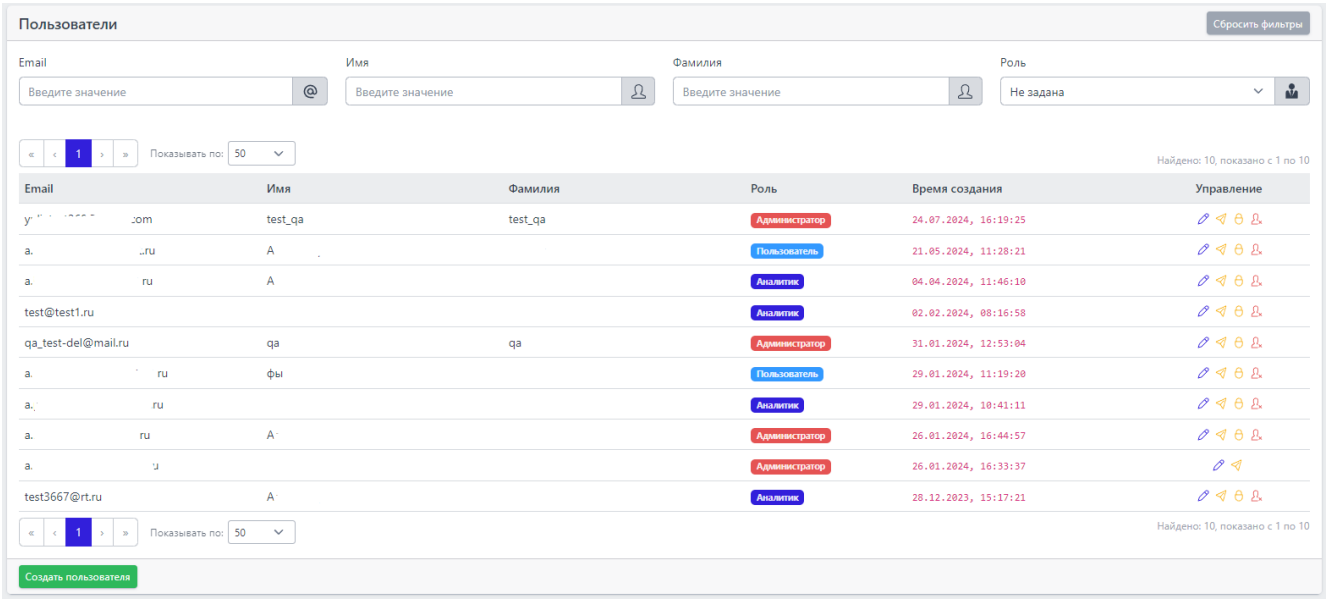


Рисунок 12 – Раздел «Пользователи»

Таблица содержит следующие поля:

1) **Email;**

2) **Имя;**

3) **Фамилия;**

4) **Роль;**

5) **Время создания;**

6) **Управление.**

Email – электронный почтовый адрес, указанный пользователем при регистрации.

Имя – содержит имя, которое пользователь указал при регистрации.

Фамилия – содержит фамилию, которую пользователь указал при регистрации.

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

Время создания – время создания пользователя.

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

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

– **Имя;**

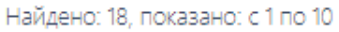
– **Фамилия;**

– **Email;**

– **Роль.**

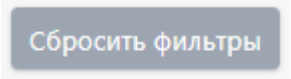
Если количество записей в таблице превышает установленное количество записей, отображаемых на странице, в верхней и нижней части таблицы отобразится пагинатор, с помощью которого можно переходить по страницам записей (рис. 13). Пагинатор является сквозным инструментом для всего модуля администрирования, то есть отображается на любой странице с фильтрами.

Рисунок 13 – Пагинатор

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

. Все элементы строки дублируются в нижней части окна программы, снизу от таблицы, для удобства просмотра и навигации.

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

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

.

Изменение параметров учетных записей пользователей

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

При нажатии кнопки **Редактировать пользователя** открывается окно, в котором можно изменить имя и фамилию пользователя, адрес электронной почты, роль выбранного пользователя, а также изменить описание учетной записи (рис. 14). 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.

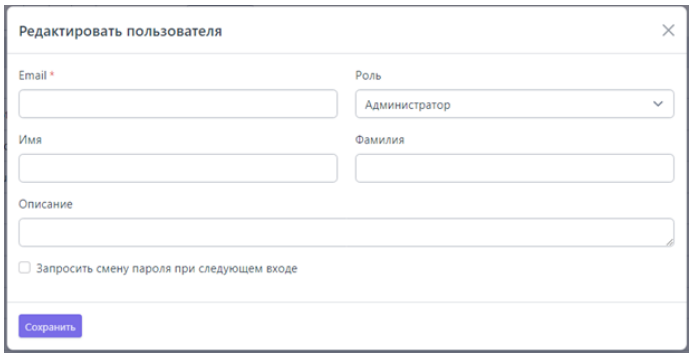


Рисунок 14 – Окно редактирования пользователя

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. 15).

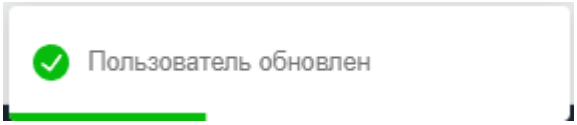


Рисунок 15 – Сообщение о сохранении данных пользователя

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

При нажатии кнопки **Сменить пароль** открывается окно, представленное на рисунке 16. Пароль должен соответствовать параметрам, указанным в нижней части окна:

1) Должен быть длиннее 8 символов;

2) Должен содержать хотя бы одну заглавную букву;

3) Должен содержать хотя бы одну строчную букву.

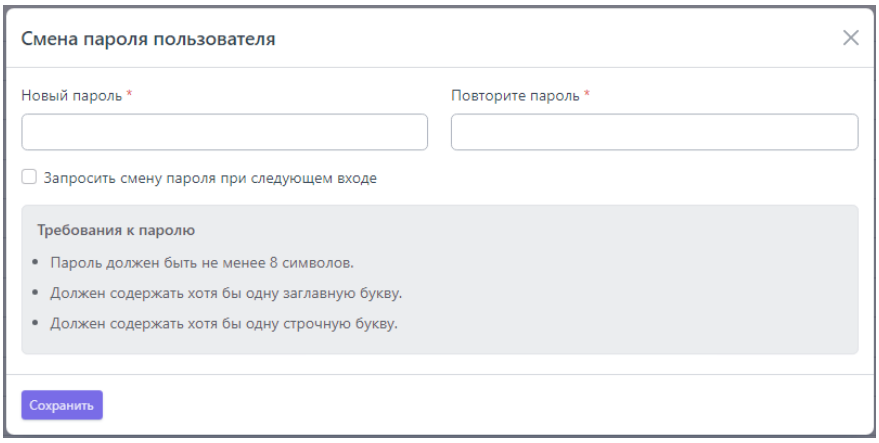
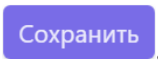


Рисунок 16 – Окно «Смена пароля пользователя»

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

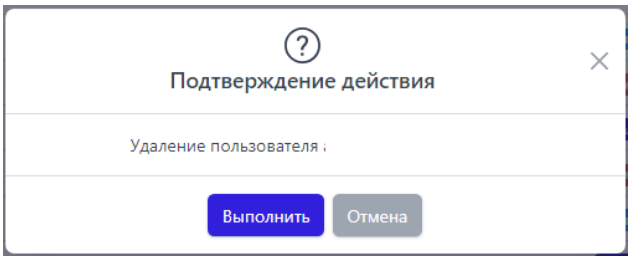


Рисунок 17 – Окно подтверждения удаления пользователя

После удаления учетной записи пользователя в нижней части основного окна программы появляется сообщение (рис. 18).

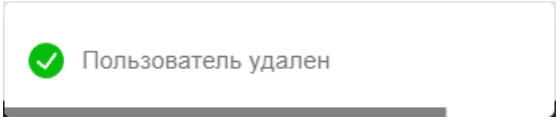


Рисунок 18 – Сообщение об удалении пользователя

В нижней части панели администрирования находится кнопка **Создать пользователя.** При нажатии кнопки открывается окно **Создать пользователя** (рис. 19).

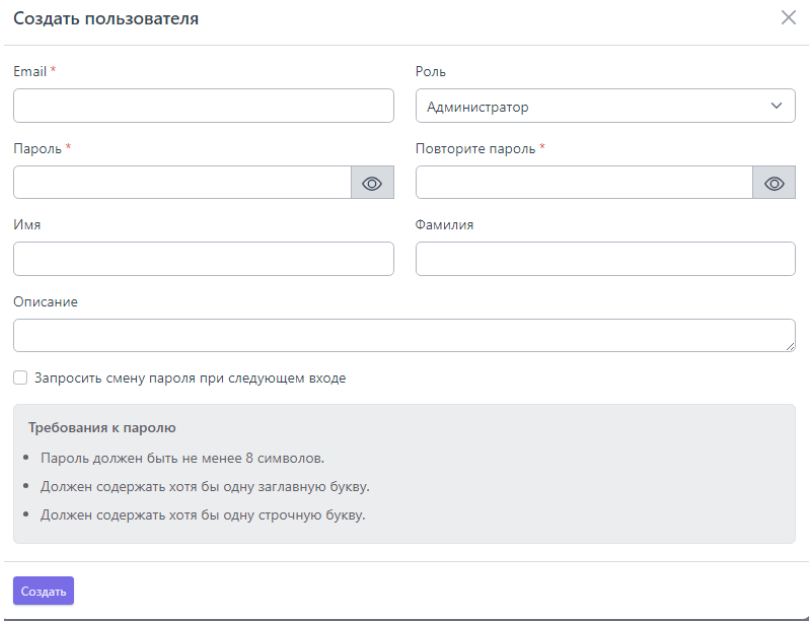


Рисунок 19 – Окно создания нового пользователя

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

– **Email;**

– **Роль;**

– **Пароль;**

– **Повторить пароль;**

– **Имя;**

– **Фамилия;**

– **Описание.**

При установке галочки в строке **Запросить смену пароля при следующем входе** пользователь устанавливает функцию смены пароля при следующем входе пользователя с данным именем. Для завершения регистрации нового пользователя следует заполнить все поля ввода.

В поле ввода **Адрес электронной почты** необходимо ввести адрес электронной почты вида login@domain. Чтобы отобразить/скрыть символы, вводимые в поля **Новый пароль** и **Повторите пароль**, следует нажать кнопки / . В нижней части окна **Создать пользователя** приведены правила формирования пароля. Для подтверждения значений, установленных для новой учетной записи пользователя, необходимо нажать кнопку Создать.

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

Рисунок 20 – Сообщение о пустом поле ввода

При написании в поле ввода **Имя пользователя** значения имени пользователя, идентичного уже сохраненному в программе, выводится сообщение о том, что пользователь с таким именем уже существует (рис. 21).

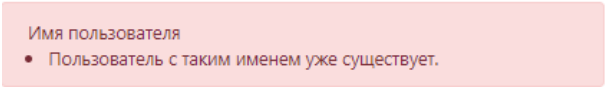


Рисунок 21 – Сообщение о совпадении имени пользователя

При вводе пользователем некорректного адреса электронной почты в поле ввода **Email** в нижней части окна **Редактировать пользователя** или **Создать**

пользователя выводится сообщение о необходимости ввода правильного адреса электронной почты (рис. 22).

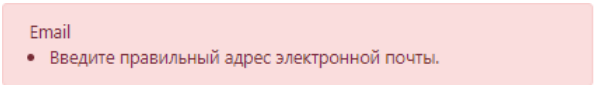


Рисунок 22 – Сообщение о неправильном адресе электронной почты

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. 23).

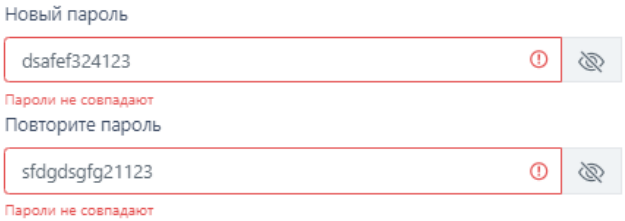


Рисунок 23 – Сообщение о несовпадении паролей

Сообщения об ошибках, которые выдает программа при вводе некорректных значений пароля, будут идентичны тем, которые могут возникнуть при вводе пароля и его подтверждения в окне **Создать пользователя.**

6.4.2. Организация

В разделе **Организация** представлена информация об организации, в которой работают пользователи программы (рис. 24). Здесь содержатся данные о стране происхождения, сайте организации, секторе экономики. Также представлена информация по названию, контактам и описанию организации.

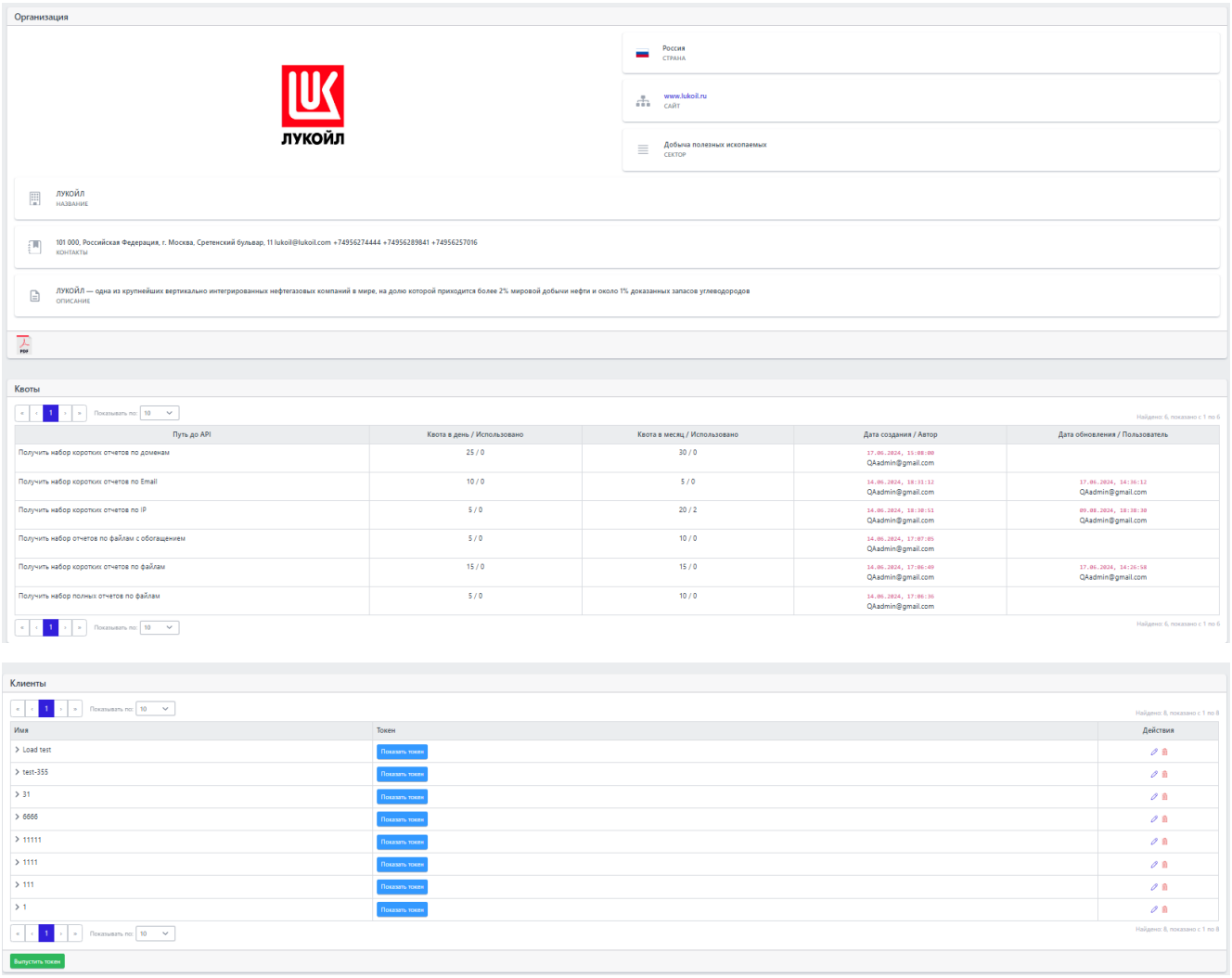


Рисунок 24 – Окно раздела «Организация»

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

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

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

Примечание

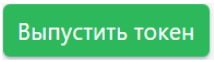
Токен представляет собой зашифрованную последовательность символов, передаваемую клиентом серверу при запросе, которая

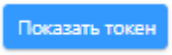
позволяет серверу однозначно идентифицировать инициатора запроса.

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

– удаление токена (иконка );

– редактирование имени токена (иконка );

– выпуск нового токена (иконка );

– просмотр токена (иконка );

– копирование токена в буфер обмена (иконка ).

При нажатии по иконке редактирования имени токена появляется окно редактирования, представленное на рисунке 25.

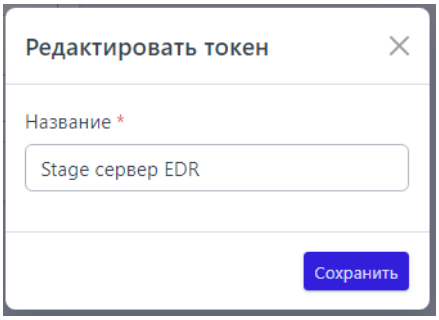
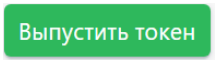


Рисунок 25 – Окно редактирования названия токена

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

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

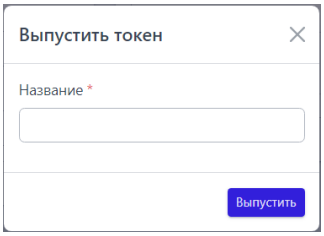


Рисунок 26 – Окно «Выпустить токен»

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

Для удаления токена требуется нажать по иконке , после чего появится окно подтверждения удаления, представленное на рисунке 27.

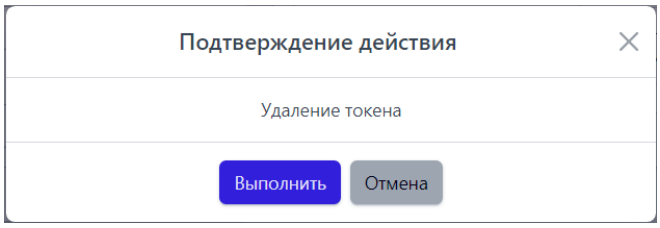


Рисунок 27 – Окно подтверждения удаления токена

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

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.

6.5.1. Активность

В разделе **Активность** в табличной форме представлена информация о последних угрозах, которые обнаружены в инфраструктуре, подключенной к сервису аналитики (рисунок 28).

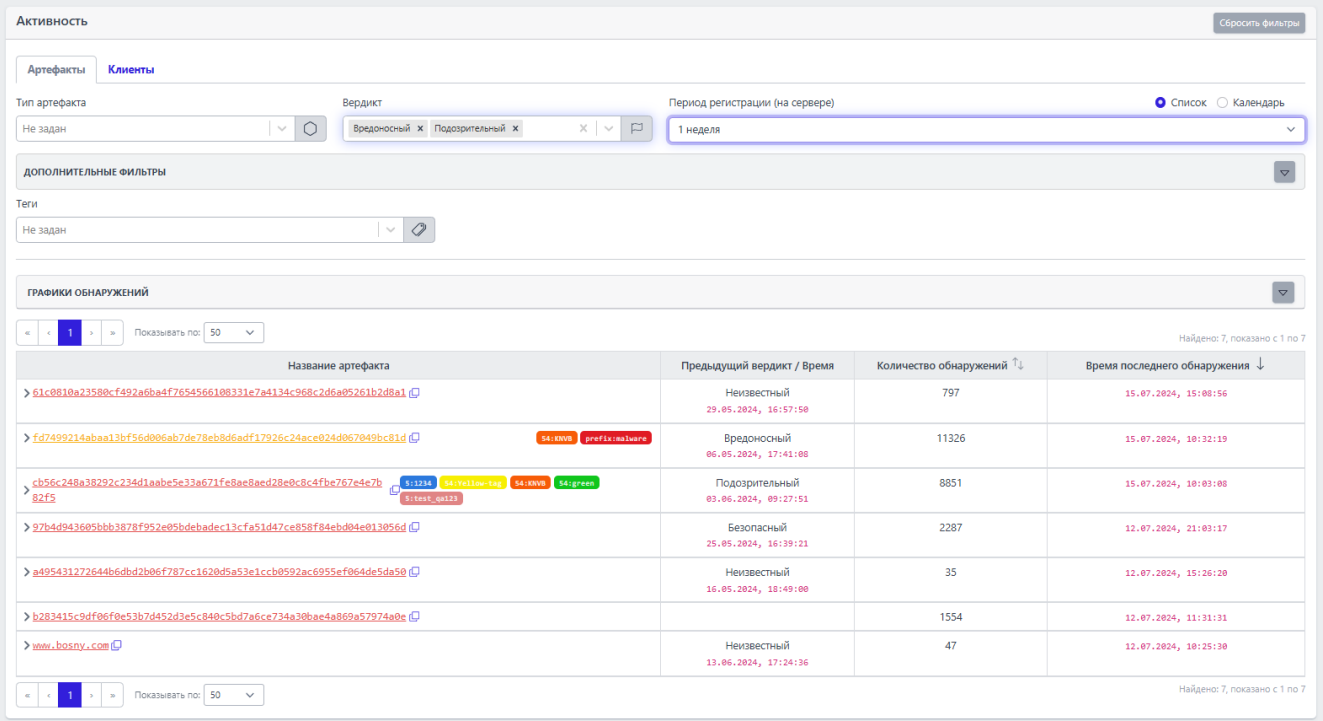


Рисунок 28 – Общий вид страницы Активность

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

Важно

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

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

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

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

– **Предыдущий вердикт/Время** (отображается вердикт и время вынесения вердикта);

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

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

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

– 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, а также иконка тега для артефакта.

Контрольная сумма файла угрозы, а также информация по другим типам артефактов является активной ссылкой, при нажатии по которой ЛКМ открывается окно отчета TI-платформы, представленное на рисунке 29.

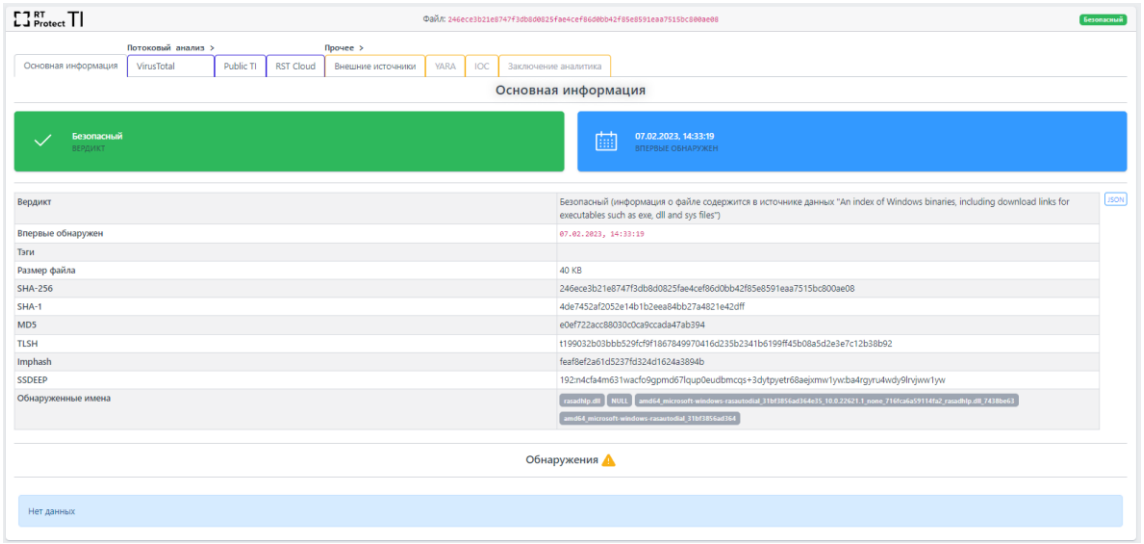


Рисунок 29 – Страница отчета сервиса по обнаруженной угрозе

Страница отчета программы об угрозе разделена на следующие области:

– область краткой информации об угрозе;

– область вкладок;

– область основной информации;

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. 30).

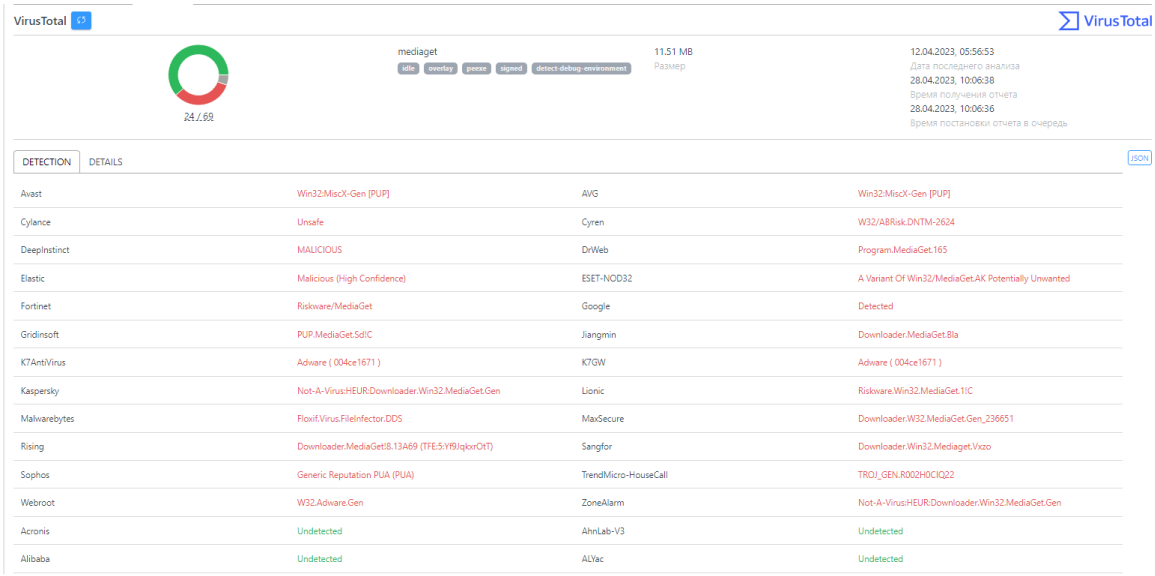


Рисунок 30 – Результаты анализа артефакта на странице Virus Total

Окно основной информации по результатам анализа артефакта в формате HTML представлено на странице 31.

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 31 – Информация отчета об артефакте в формате HTML

Окно основной информации по результатам анализа артефакта в формате JSON представлено на странице 32.

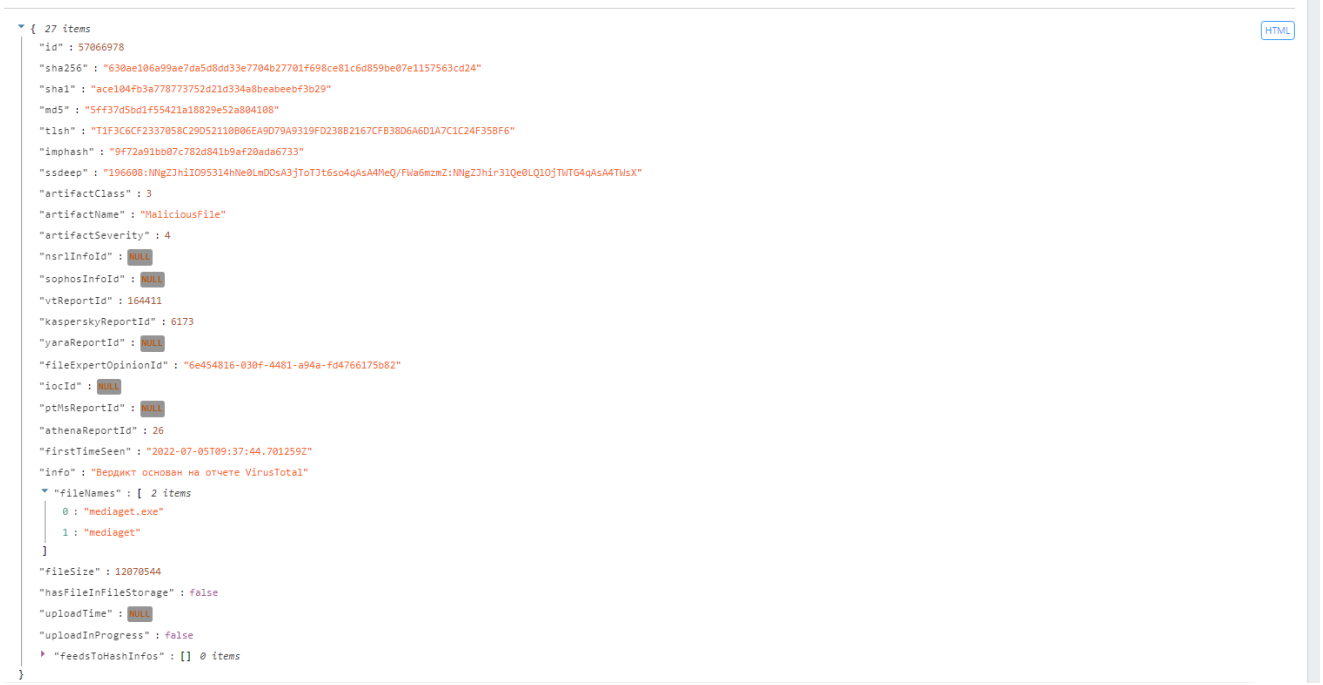


Рисунок 32 – Информация отчета об артефакте в формате JSON

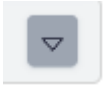
Для фильтрации информации на странице **Активность** вкладка **Артефакты** предусмотрена система основных фильтров, представленная в следующем списке:

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

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

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

– **Теги.**

Также имеется система дополнительных фильтров, которая по умолчанию скрыта. Для открытия поля с дополнительными фильтрами требуется нажать по иконке  в области **Дополнительные фильтры**.

Имеются следующие дополнительные фильтры:

– **Артефакт;**

– **Количество обнаружений не менее;**

– **Количество обнаружений не более;**

– **Предыдущий вердикт;**

– **Время последнего изменения вердикта.**

На странице **Активность** вкладки **Клиенты** имеется область с графическим отображением информации по обнаруженным угрозам (рисунок 33).

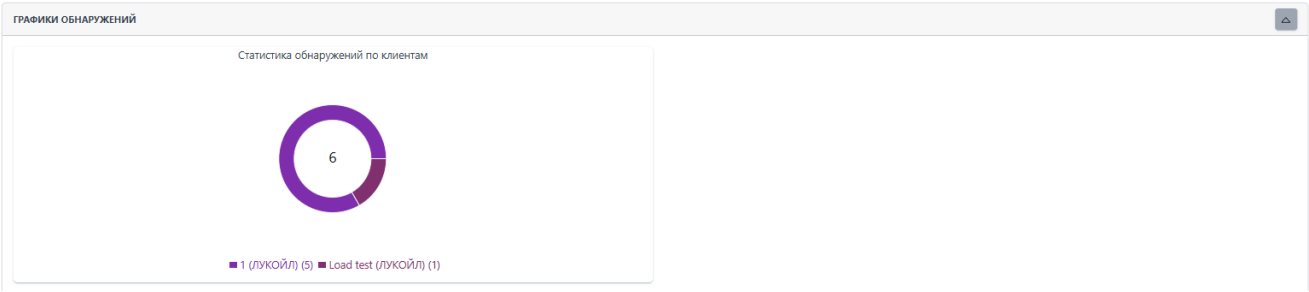


Рисунок 33 – Область графического отображения информации по обнаруженным угрозам вкладка «Артефакты»

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

– статистика обнаружений по клиентам в рамках организации.

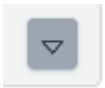
Для фильтрации информации на странице **Активность** вкладка **Клиенты** предусмотрена система фильтров, представленная в следующем списке:

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

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

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

– **Клиенты.**

Также имеется система дополнительных фильтров, которая по умолчанию скрыта. Для открытия поля с дополнительными фильтрами требуется нажать по иконке  в области **Дополнительные фильтры**.

Имеются следующие дополнительные фильтры:

– **Артефакт;**

– **Количество обнаружений не менее;**

– **Количество обнаружений не более;**

– **Предыдущий вердикт;**

– **Время последнего изменения вердикта;**

На странице **Активность** вкладки **Клиенты** имеется область с графическим отображением информации по обнаруженным угрозам для тех или иных клиентов.

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 34.

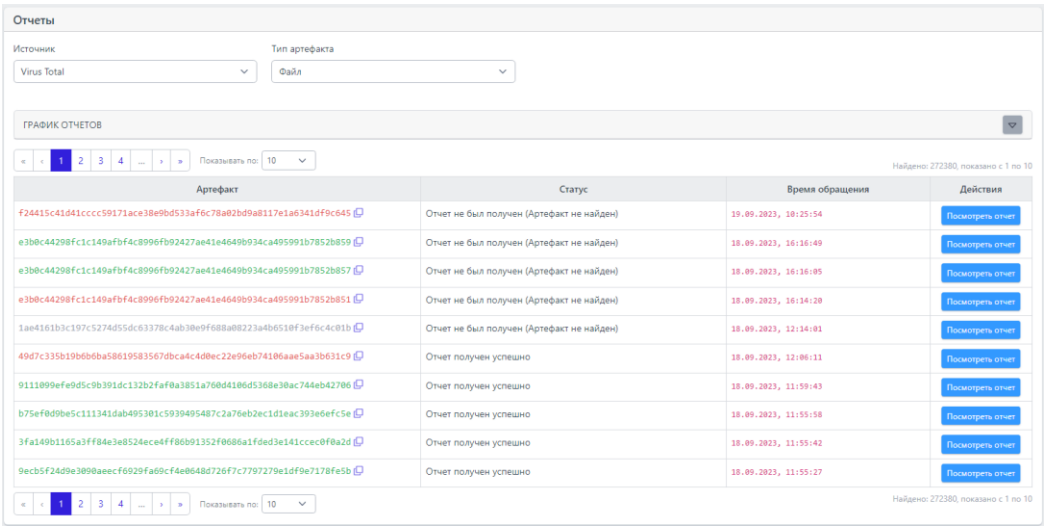


Рисунок 34 – Окно раздела «Отчеты»

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).

Над таблицей для фильтрации информации имеются следующие фильтры:

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

– **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 35).

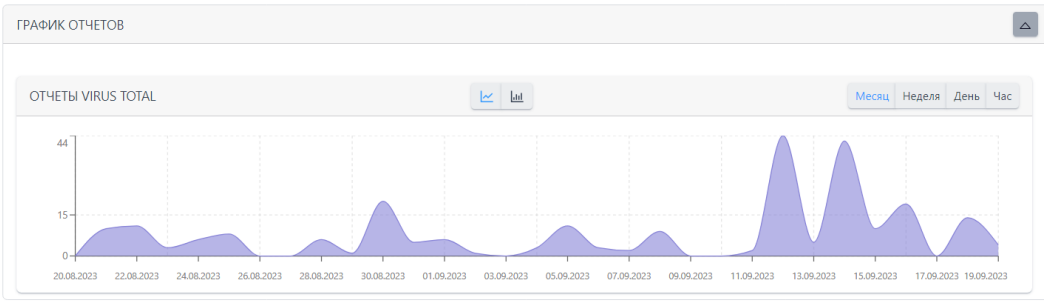


Рисунок 35 – Отчеты Virus Total

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 36.

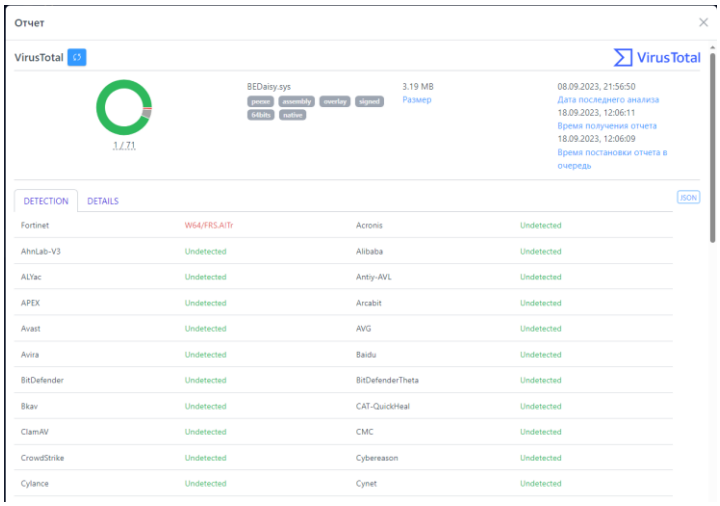


Рисунок 36 – Страница отчета по артефакту от источника Virus Total

6.5.3. Граф связей

Страница **Граф связей** с незаполненным полем артефакта представлена на рисунке 37.

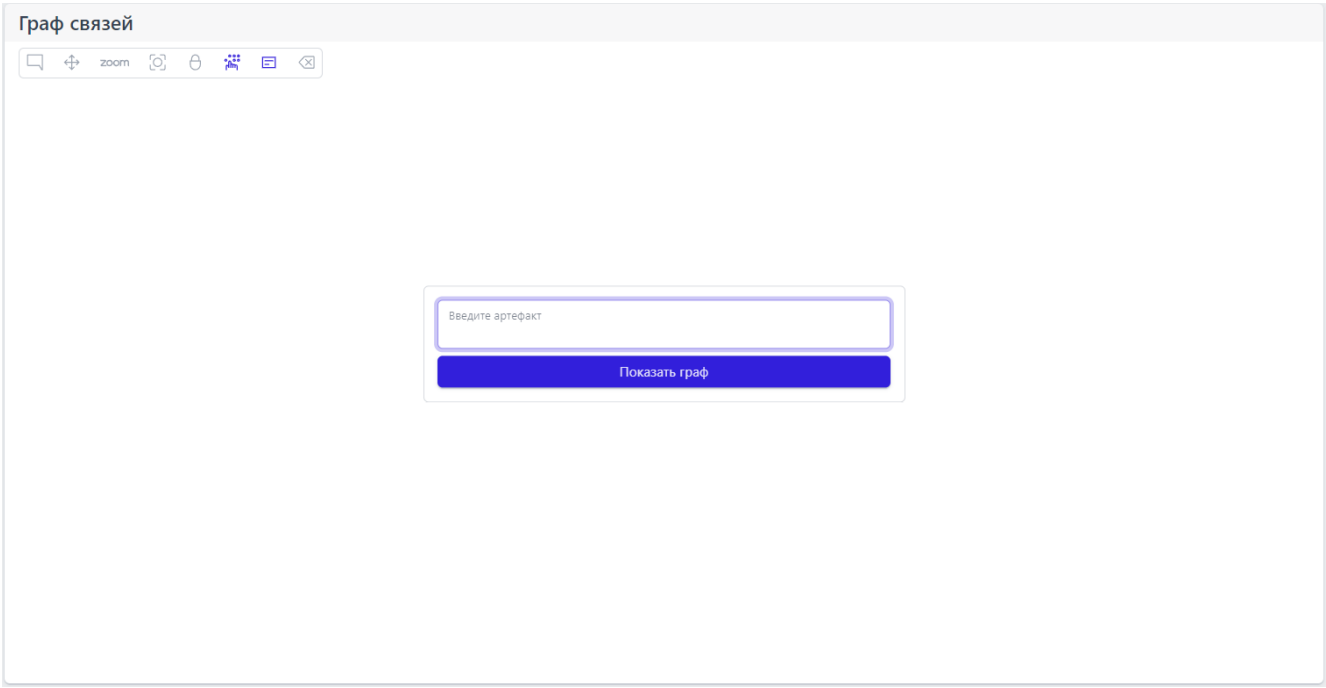


Рисунок 37 – Общий вид пустой страницы «Граф связей»

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 38.

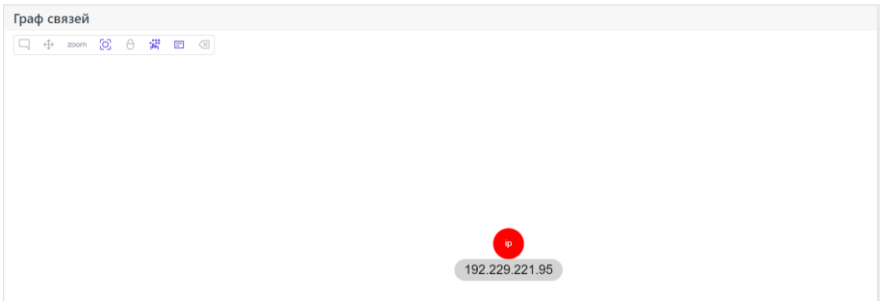


Рисунок 38 – Отображение графа связей для артефакта типа ip-адрес

Пример отображения графа связей для артефакта типа домен с привязанными артефактами представлен на рисунке 39.

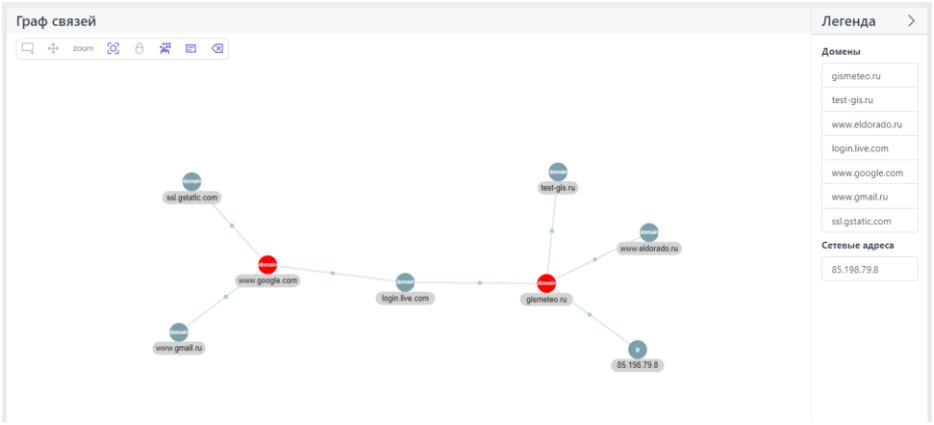


Рисунок 39 – Отображения графа связей для артефакта типа домен с привязанными артефактами

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 40).

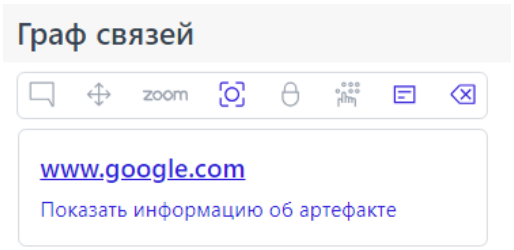


Рисунок 40 – Краткая информация по артефакту

При нажатии в данной области по иконке **Показать информацию об артефакте** появляется окно, представленное на рисунке 41.

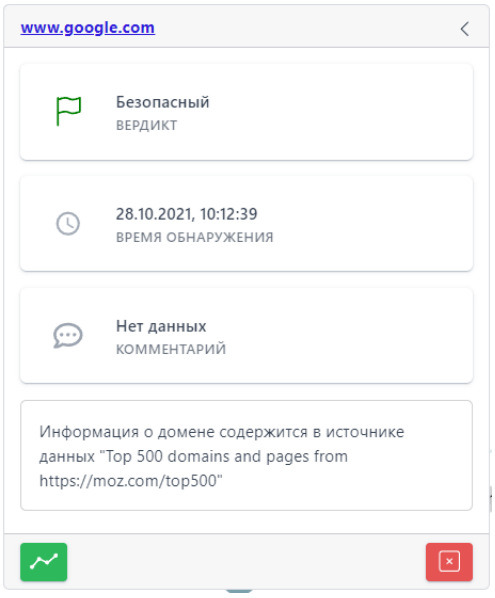


Рисунок 41 – Информация об артефакте

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 42.

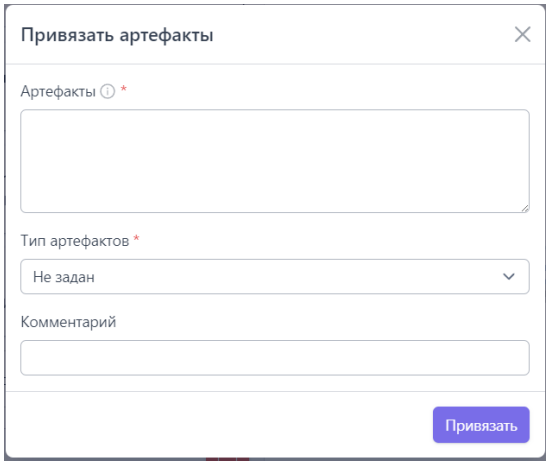


Рисунок 42 – Окно добавления информации для привязывания артефакта

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  .

6.6 Параметры

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

6.6.1. Журнал действий

На странице **Журнал действий пользователей** в табличном виде представлена информация о действиях пользователей (в рамках организации, указанной в разделе **Организации**) (рис. 43).

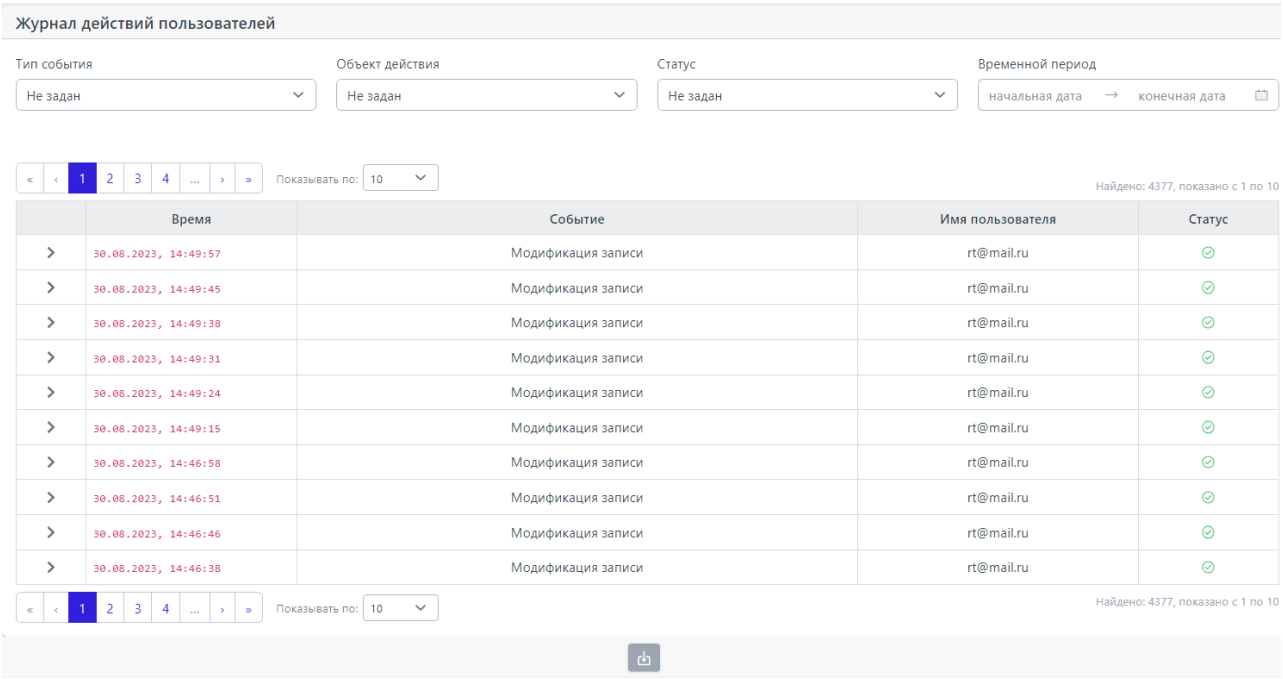


Рисунок 43 – Журнал действий

Таблица представлена следующими полями:

– иконка > (при нажатии отображается информация о событии);

– **Время** (отображается время регистрации события);

– **Событие** (отображаются события в формате «Объект действия: Тип события», например, «Индикатор атаки: Создание записи»);

– **Имя пользователя** (отображается имя пользователя, который произвел определенное действие);

– **Статус** (отображается статус действия или события).

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

1) Тип события:

– Создание записи;

– Модификация записи;

– Удаление записи;

– Вход в систему;

– Выход из системы.

2) Объект действия:

– Пользователь;

– Индикатор компрометации;

– Yara-правило;

– Индикатор атаки;

– Организация;

– Токен;

– Заключение аналитика по IP;

– Заключение аналитика по файлу;

– Заключение аналитика по домену;

– Заключение аналитика по URL;

– Отчет Public TI по файлу;

– Отчет Public TI по IP;

– Отчет Public TI по домену;

– Отчет Public TI по URL;

– Отчет VT по файлу;

– Отчет VT по IP;

– Отчет VT по домену;

– Отчет VT по URL;

– Отчет Athena по файлу;

– Отчет Yara;

– Отчет Netlas по IP;

– Отчет Netlas по домену;

– Журнал Windows;

– Исключения для файлов;

– Исключения для программ.

3) Временной период (начало);

4) Временной период (окончание);

5) Статус (успешно/неудачно).

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

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

На рисунке 44 отображается информация о событии в формате HTML.

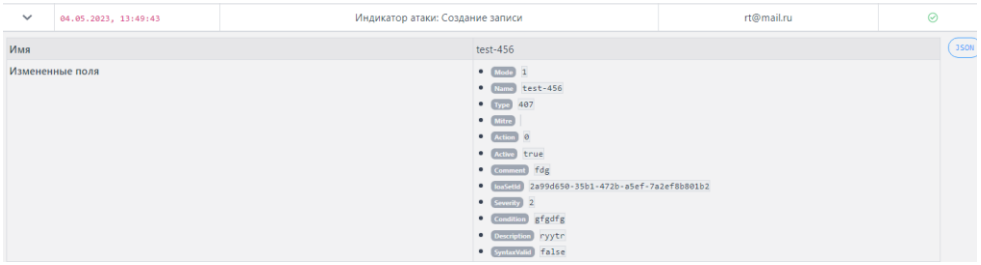


Рисунок 44 – Отображение информации о событии в формате HTML

На рисунке 45 отображается информация в формате JSON.

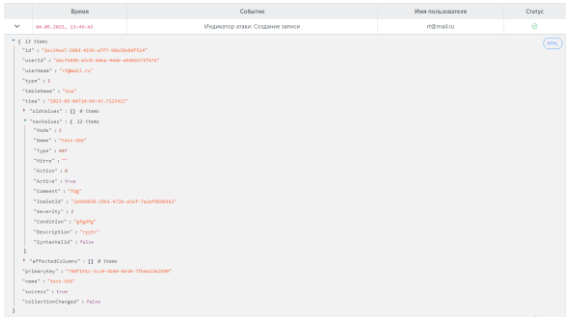


Рисунок 45 – Отображение информации о событии в формате Json

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

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

6.6.2. Интеграции

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

Страница **Интеграции** представлена на рисунке 46.

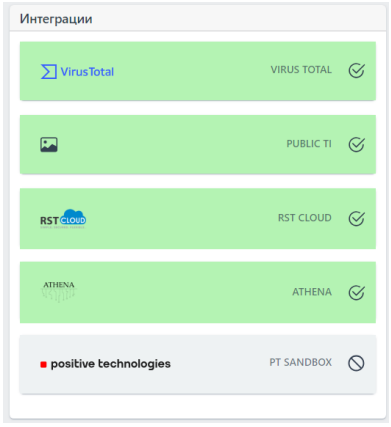


Рисунок 46 – Страница «Интеграции»

7. Сообщения администратору

7.1 Общие сведения

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

Предусмотрены следующие категории информации:

1) ошибка;

2) обнаружение;

3) предупреждение;

4) успешно.

Сообщения администратору выводятся в виде диалоговых окон.

7.2 Сообщения об ошибках

Можно выделить два типа сообщений об ошибках:

1) общие сообщения – выводятся в приложении в том случае, если возникшая ошибка не была обработана специальным образом, и использовался общий обработчик;

2) специфичные сообщения – выводятся в конкретных местах приложения и содержат детальное описание ошибки.

7.2.1. Общие сообщения

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

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

1) экран ошибки;

2) всплывающее сообщение об ошибке.

Пример сообщения в виде экрана ошибки представлен на рисунке 47.

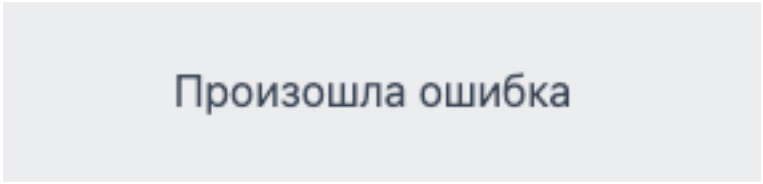


Рисунок 47 – Сообщение об ошибке типа «Экран ошибки»

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 48.

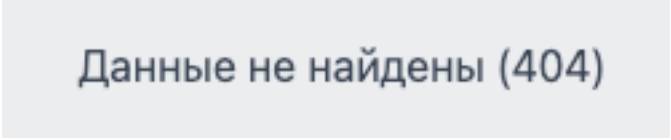


Рисунок 48 – Сообщение об ошибке

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 49.

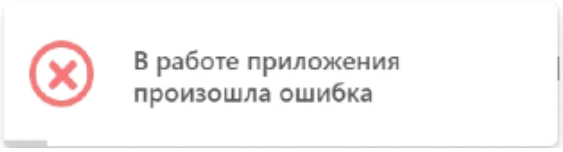


Рисунок 49 – Всплывающее сообщение об ошибке

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 50).

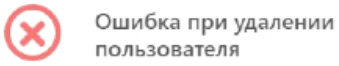


Рисунок 50 – Ошибка при удалении пользователя

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 51).

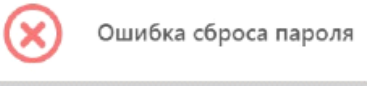


Рисунок 51 – Ошибка сброса пароля

Возможная причина: некорректный ответ сервера.

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

Страницы раздела «Аналитика».

1) Ошибка: неверный формат файла.

Выводимое сообщение представлено на рисунке 52.

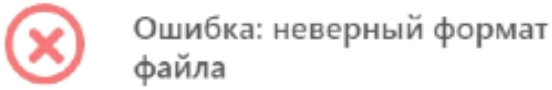


Рисунок 52 – Неверный формат файла

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

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

Экран авторизации

1) Сообщение об ошибке при вводе неправильных учетных данных представлено на рисунке 53.

Рисунок 53 – 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 54.

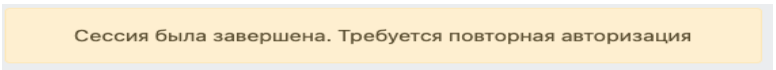


Рисунок 54 – Уведомление о завершении сессии пользователя

Данная ситуация не является ошибкой.

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

Действия по устранению: осуществить повторный вход в систему.

8. Действия после сбоя и ошибки

8.1 Общие сведения

Большинство ошибок можно разделить на следующие типы:

1) ошибки конфигурации:

– некорректные настройки параметров безопасности;

– некорректная установка компонентов программы;

– некорректные действие со стороны пользователя/администратора;

– критические ошибки.

2) ошибки оборудования:

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

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

– перебои питания со стороны серверной части.

Для устранения ошибки требуется обратиться к поставщику программы.

9. Перечень сокращений

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

Таблица 6 – Перечень сокращений

ИС	Информационная система
ИТ	Информационная технология
ЛКМ	Левая кнопка мыши
ПКМ	Правая кнопка мыши
ПО	Программное обеспечение
ФСТЭК	Федеральная служба по техническому и экспортному контролю
ЦП	Центральный процессор
APT	Advanced Persistent Threat (постоянная серьезная угроза)
ID	Identifier (идентификатор)
IT	Information Technology (информационные технологии)
NSRL	National Software Reference Library (Национальная справочная библиотека программного обеспечения)
PID	Process Identifier (идентификатор процесса)
PPID	Parent Process Identifier (идентификатор родительского процесса)
RPC	Remote Procedure Call (удалённый вызов процедур)
SID	Security Identifier (идентификатор безопасности)
TGS	Ticket Granting Server (служба выдачи билетов)
URL	Uniform Resource Locator

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