## Веб-сервис RT Protect TI

## Руководство администратора

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

# **CJ** RT **Protect**

## CJ 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	0
3.1 Общие сведения1	0
3.2 Комплектность поставки 1	0
3.2.1. Процедуры и меры безопасности при распространении программы к	
месту назначения1	0
4. Структура программы1	1
5. Настройка программы1	2
5.1 Требования к среде функционирования1	2
5.2 Роли	2
6. Интерфейс программы14	4
6.1 Окно авторизации и общие сведения14	4
6.2 Горизонтальная панель управления1	6
6.2.1. Меню «Пользователь»1	8
6.3 Главная страница1	9
6.4 Администрирование2	1
6.4.1. Пользователи	2
6.4.2. Организация	9
6.5 Аналитика	2
6.5.1. Активность	2
6.5.2. Отчеты	9

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 ТІ-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.

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
ТСР	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 НТТР-запросы от клиентов, чаще всего веб-браузеров, и выдающий НТТР-ответы, как правило, вместе с НТМL-страницей, изображением, файлом, медиа-потоком или другими данными

Таблица 2 – Термины и определения

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
Примечание	Информация, требующая внимания пользователя
Важно	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 OC Linux Ubuntu 20.04.5 LTS.

Для распространения сервиса применяется модель on-cloud (установка и развертывание сервиса осуществляется на мощностях предприятияразработчика 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 предприятияизготовителя.

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»	4	
	Руководство Администратора;	I	
	– «Веб-сервис RT Protect TI»		
	«Руководство Аналитика;		
	– «Веб-сервис RT Protect TI»		
	«Руководство Пользователя.		

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:

– ІР-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 ITинфраструктуры.

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

#### 23 RT Protect TI

Сброс пароля

θ	Введите новый пароль	$\odot$
θ	Повторите пароль	$\odot$
	Сохранить	



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).

	$\equiv$ $\square$												Ś
😡 Главная страница	Проверка артефактов												
администрирование	Введите IP-адрес, доменное имя, URL, етаїї или контрольную сумму файла для проверки											Orm	
Д. Пользователи	изедите и задиет диметлие имп, иль е нам лип киптрилелум чумму фалиа дил призедил												
🏛 Организация	СТАТИСТИКА ДОБАВЛЕНИЯ АРТЕФАКТОВ З	А МЕСЯЦ											
🖏 Теги	Файлы	Доменные имена	IP-/	Адреса			Url				•	Email	
аналитика	754563	34302	13	20392		- E	70933				⊕	21	
🖒 Активность	АКТИВНОСТЬ				<u>a</u>								
📰 Отчеты	19397		<b>-о-</b> Файлы	- <b>о-</b> IP-Адреса - <b>о-</b> Д	Іоменные имен	a 🕳 Url 🚽	► Email						
နိုင် Граф связей													
ПАРАМЕТРЫ	10000-												
🔟 Журнал действий	5000-												
👯 Интеграции	0						-						
	13:15:46 14:15:46 15:15:46 16:15:46	17:15:46 18:15:46 19:15:46 20:15:46 2	1:15:46 22:1	15:46 23:15:46 00	01:15:46 01:15:46	02:15:46	03:15:46	04:15:46	05:15:46	06:15:46	07:15:46	08:15:46	09:15:46
	ТОП 5 РАСПРОСТРАНЕННЫХ УГРОЗ (ФАЙЛЬ	ol)			топ 5 пос	ЛЕДНИХ У	ΓΡΟ3 (ΦΑ	йлы)					
		MSSS.exe (11469)							<b>3</b> c84b6	9be7eb4c	7c942efea	ad2e9c2c	3233 (4)
	31.9 %	nMirror.exe (8938) af2222204fca27c0fdabf9eefbfdb638a (6052	)			0.0 %	<b>_</b>		<ul> <li>FunMin</li> <li>KMSSS.</li> </ul>	or.exe (89 exe (11469	138) 9)		(125)
	■ f2-	4415c41d41cccc59171ace38e9bd533af (384	0)						ed01eb	fbc9eb5bb	cea545af4	d01bf5f1	0716 (1347)

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 АРІ платформы ТІ.

– 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 – С ртонест © 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

Проверка артефактов								
Введите IP-адрес, доменное имя	, URL, email или контрольную с	сумму файла для проверки						Отправить 📒 🕹
СТАТИСТИКА ДОБАВЛЕНИЯ АРТЕ	ФАКТОВ ЗА МЕСЯЦ							-
Файлы		Доменные имена		IP-Agpeca		Url	Email	
74324	٥	268918	•	17226416	â	127082	6	@
АКТИВНОСТЬ								Неделя День Час
16000 m				🗢 Файлы 🗢 IP-Адреса 🔶 🖊	оменные имена 🗢 Url 🔶 Email			
12000 -	$\sim$							
8000 -		$\sim$	_					
4000 -	_							
0	08:10 1438:10 15:08:10 15:38:10 16:08:10	0 163810 173810 173810 180810 183810 190810	193810 200810 203810 21:08	0 21:38:10 22:08:10 22:38:10 23:08:10 23:3	8:10 00:08:10 00:38:10 01:08:10 01:38:10 02	c0:10 02:38:10 03:08:10 03:38:10 04:08:10 04:38:10 05:38:	10 06/08/10 08/38/10 07/08/10 07/38/10 08/08/10 08/38/10 0	RGE10 093810 103810 123810 113810
[					G			
TOTTS PACIFOCTPARENHBIX 71P	ээ (файлы)				топ з последних этроз (	ФАИЛЫ)		
31.7%	KMSSS.exe (11326)     Tunkfiror.exe (6851)     26475222047ca27c0fds     winserv.exe (5665)     E24415c41641cccc5917	bt/9eefo/db638a (6052) 11ace38e9bd533af (3840)			38.0 %	<ul> <li>61:0011022380:0492240x4776545661</li> <li>001555:xxxx (1120)</li> <li>11:001000:00056551)</li> <li>11:001000:00056551)</li> <li>11:001000:00056551)</li> <li>11:001000:00057676120500000077676122</li> </ul>	083 (797) 5ec13 (2287) 5d58 (35)	
ТОП 5 РАСПРОСТРАНЕННЫХ УГР	ОЗ (ДОМЕННЫЕ ИМЕНА)				топ 5 последних угроз (	ДОМЕННЫЕ ИМЕНА)		
52.6 %	<ul> <li>proxy-sslantizepret.prox</li> <li>www.mosconguarante.</li> <li>oxbncounter.com (1100</li> <li>aro.noor.wikaba.com (6</li> <li>mail1.serviechelp.chang</li> </ul>	storpn.org (5457) com (2468) 0 579 759 Jelepus (657)			32.4 %	www.boory.com (47)     rest3.ndetschrucken (2)     eff.indetschrucken (1)     editinterschrucken (1)     editinterschrucken (1)     e62.118.138.2 (94)		

#### 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. 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).

Пользователь	
Профиль	
← Выход	

Рисунок 7 – Меню «Пользователь»

Подменю Профиль представлено на рисунке 8.

Профиль
imail
баль
Администратор
Лмя
<b>Д</b> амилия
Эрганизация
лукойл
Эписание
Сиенить пароль

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).

Руководство администратора веб-сервиса RT Protect TI СЗ Рготест Версия 1.0.20 от 17 октября 2024

Сменить пароль	$\times$
Ваш текущий пароль *	
	$\odot$
Новый пароль *	
	0
Повторите пароль *	
	0
Требования к паролю <ul> <li>Пароль должен быть не менее 8 символов.</li> <li>Должен содержать хотя бы одну заглавную букву.</li> <li>Должен содержать хотя бы одну строчную букву.</li> </ul>	
Сохранить	

#### 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.

Проверка артефактов								
Введите IP-адрес, доменное имя, UP	L, email или контрольную і	сумму файла для проверки						Отправить
СТАТИСТИКА ДОБАВЛЕНИЯ АРТЕФА	КТОВ ЗА МЕСЯЦ							
<sup>одйлы</sup> 74324	٥	Доменные имена 268918	(P-Appeca 17226416		â	uri 127082	Email 6	@
АКТИВНОСТЬ				E F				Неделя День Час
	64810 10810 10810 K0810	1 161810 179810 17380 180810 181810 1		еса - Доме		10 COLOR TO C		40 100610 102410 113410
ТОП 5 РАСПРОСТРАНЕННЫХ УГРОЗ (	ФАЙЛЫ)				ТОП 5 ПОСЛЕДНИХ УГРОЗ (Ф	АЙЛЫ)		
31.7 %	<ul> <li>KMSSS.exe (11326)</li> <li>TunMirror.exe (8851)</li> <li>26af2222204fca27c0fdz</li> <li>winserv.exe (5685)</li> <li>f24415c41d41cccc5917</li> </ul>	br/Seefordb638a (6052) 1ace38e9bd533af (3840)			38.0 %	<ul> <li>€1-0610x23580c449</li> <li>KMSSS.exe (11326)</li> <li>■ Turhimoraek (851</li> <li>97b40494505bb633</li> <li>■ 8495431272644b6di</li> </ul>	2a6coa776545661032(797) ) ) ) ) (2827) (2	
ТОП 5 РАСПРОСТРАНЕННЫХ УГРОЗ (	ДОМЕННЫЕ ИМЕНА)				топ 5 последних угроз (д	ОМЕННЫЕ ИМЕНА)		
52.6 %	<ul> <li>proy-sslantizapret.pro</li> <li>www.moscowguarante</li> <li>ox.bnoourcom (110</li> <li>aro.noon.wikaba.com (6</li> <li>mail1.serviecheip.chang</li> </ul>	istorph.org (5457) com (2458) 0) 7579) pelpus (657)			32.4 %	■ www.bosny.com (47 ■ rest2.rdntocdns.com = cst1.rdntocdns.com = cdnruntocdns.com = 62.118.138.2 (54)	) (a (n (n	

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 ТІ-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 ТІ-серверу. После нажатия кнопки откроется проводник, в котором можно выбрать файл, нуждающийся в проверке. Далее файл загружается на ТІ-платформу, а после завершения его загрузки выводится отчет с вердиктом.

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

Проверить список артефактов 🕦	>
Проверить	

#### 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.

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

Пользователи							Сбросить фильтры
Email Введите значение	@	Имя Введите значение	٩	Фамилия Введите значение	£	Роль Не задана	~ 1
≪ < 1 → » Пока	зывать по: 50 🗸	Фамилия		Роль	Время создан	<b>4</b> 9	Найдено: 10, показано с 1 по 1 Управление
y the second som	test ga	test ga		Администратор	24.07.2024, 16	:19:25	/ <b>√</b> € L
aru	A .			Пользователь	21.05.2024, 11	:28:21	⊘ ⊲ ⊖ &
a. ru	А			Аналитик	04.04.2024, 11	:46:10	0 1 8 2
test@test1.ru				Аналитик	02.02.2024, 08	:16:58	<i>0</i> ⊲ θ &
qa_test-del@mail.ru	qa	qa		Администратор	31.01.2024, 12	:53:04	Ø ◀ θ &
a. <sup>.</sup> ru	фы			Пользователь	29.01.2024, 11	:19:20	0 1 8 B
a.; ru				Аналитик	29.01.2024, 10	:41:11	1 d b b
a. ru	A-			Администратор	26.01.2024, 16	:44:57	0 🕫 8 B
a. u				Администратор	26.01.2024, 16	: 33: 37	0 1
test3667@rt.ru	A			Аналитик	28.12.2023, 15	:17:21	0 🕫 O &
« < 1 > » Пока	зывать по: 50 🗸						Найдено: 10, показано с 1 по 10
Создать пользователя							

#### 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 <sup>Найдено: 18, показано: с 1 по 10</sup>. 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 П).

Для отмены фильтрации информации на странице в правом верхнем углу

предусмотрена иконка

Сбросить фильтры

Изменение параметров учетных записей пользователей

В поле Управление находятся кнопки Редактировать пользователя 🖉,

Отправить пользователю ссылку для сброса пароля ( I ), Сменить пароль  $\Theta$  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.

Редактировать пользоват	еля	×
Email *	Роль	
	Администратор	~
Имя	Фамилия	
Описание		
Запросить смену пароля при	следующем входе	
Сохранить		

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.

Смена пароля пользователя	×
Новый пароль *	Повторите пароль *
<ul> <li>Требования к паролю</li> <li>Пароль должен быть не менее 8 символов.</li> <li>Должен содержать хотя бы одну заглавную букву.</li> <li>Должен содержать хотя бы одну строчную букву.</li> </ul>	
Сохранить	

Рисунок 16 – Окно «Смена пароля пользователя»

После указания нового пароля, требуется нажать по иконке <sup>Сохранить</sup>. 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.

? Подтверждение действия	×
Удаление пользователя :	
Выполнить Отмена	

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

Создание учетной записи пользователя

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

Создать пользователя	×
Email *	Роль
Пароль *	Повторите пароль *
Имя	Фамилия
Описание	le la
Запросить смену пароля при следующем входе	
<ul> <li>Требования к паролю</li> <li>Пароль должен быть не менее 8 символов.</li> <li>Должен содержать хотя бы одну заглавную букву.</li> <li>Должен содержать хотя бы одну строчную букву.</li> </ul>	
Создать	

#### 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.

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.

Имя	
Имя	()
Необходимо заполнить данное поле	

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).

њзователя						
зователь с т	таким и	именем	і уже с	ишестви	ет.	
2	льзователя зователь с	льзователя зователь с таким і	льзователя зователь с таким именем	льзователя зователь с таким именем уже с	льзователя зователь с таким именем уже существу	льзователя зователь с таким именем уже существует.

#### 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).

Email • Введите правильный адрес электронной почты.

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).

Новый пароль		
dsafef324123	()	Ø
Пароли не совпадают Повторите пароль		
sfdgdsgfg21123	0	Ø
Пароли не совпадают		

#### 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.

Организация	
Process C7201A	
ЛУКОЙЛ 🗮 Аббила полемые ассоленные	
III INCEANSE	
ISI 2008. Proceedicase Φερεραμικε, r. Mocesa, Cpretencené dynasap, 11 lukol@kukol.com +74555274444 +7455528941 +74555257016 Icoltar/lar	
ДУКОЙЛ — одна их врутнейщих вертикально интерированных нефтехзовых компаний в кире, на доло которой приходите более 2% кировой добичи нефти и около 1% доказанных запасов узлеводородов Отоссност	
_	
<u>고</u>	
Keona	
Kerns	Найдено: 6, показано с 1 по 6
Keons         Keons and the second of th	Найдено: 6, показано с 1 по 6 ения / Пользователь
Kerns         Kerns and an an an and an	Найденся 6, посазано с 1 по 6 ения / Пользователь
Korus         Karus	Найдено (, посазно с 1 по 6 ения / Пользователь 2004, 34:36:12 nin@gmail.com
Normaling logicity of the mean regime of the mean regimes of the mean regime of the mean reg	Halgano E. mozzano I. I no E. ever / Rozzostera 2014, 14114-12 2024, 141110 2024, 141110 2024, 141110 2024, 141110
Korna         Korna <th< td=""><td>Valgens 6. macroso 1 fm 6 ever / Rozzoszetens 2004, 1419-12 2004, 1419-12 2004, 1419-13 2004, 1419-1</td></th<>	Valgens 6. macroso 1 fm 6 ever / Rozzoszetens 2004, 1419-12 2004, 1419-12 2004, 1419-13 2004, 1419-1
Korne         Composition of the state	Italyane 6. mozano 1 i no 6 exer / Rotatosetta 2024, 54:34:12 2024, 54:34:12 2024, 54:34:12 2024, 54:34:12 2024, 54:34:14 2024, 54:34:14 2024, 54:34:14
Normal         Normal         Normal         Area codese         Area cod	Holgens 6, mozano 1 i no 6 eeer / Ronaposaren. 2000, 1418-131 mäginat Loon andig praticon 2000, 1418-134 andig praticon
Image: constraint on galaxies         Second on galaxies	Halagen (; measies 1 in 6 exert / Rokassaters exert / Rokassaters ) 2004, 14:34:12 minggmal.com ) 2004, 14:34:13 Minggmal.com ) Halagen (; measies 1 in 6
Image: constraint on the state of	Halageo & mussion 1 to 6 exert / Robasoaters exert / Robasoaters andgmat (cm 2004, 14:14:12 andgmat (cm 2004, 14:14:14 andgmat (cm Halageo & mussion 1 to 6
Construction         Construction<	Halapen & encases i t es 6 exer / Totascearca exer / Totascearca Ming gnal com 2005, 18 19 10 2005, 18 10 20 Ang gnal com 2006, 18 10 20 2007, 18 10 20 2007
Construint         Constru	Halgens & measure of 1 m 6 event / fischardearten fischer / f
	Halgens & macases i t es 6 exers / Danadoareze 2004, 15: 10: 10 2004, 15: 20: 10; 20: 10; 20: 10; 20: 10; 20: 10; 20: 10; 20: 10; 20: 10; 20: 10; 20: 10; 20: 10; 20: 10; 20: 10; 20: 10; 20: 10; 20: 10; 20: 10;
Constrained         Constrained <thconstrained< th=""> <thconstrained< th=""></thconstrained<></thconstrained<>	Halapon & macanes 1 m 6 mmr / Danabaaren 2005, 12 milio 2007, 12 m
	Halayers & macanes 1 ar 6 exert / Doassoarten 2001, 10 (A112) 2001, 10 (A112)
Kersa         Contract on the Direction of Directio	Halagen & receiver i 1 no 6 ever / Reascaster. and gmal.com 2009, 10:10:10 2009, 10:10:10 2009, 10:10:10 2009, 10:10:10 2009, 10:10:10 Halagen & receiver i 1 no 6 Reference Phalagen & receiver

#### Рисунок 24 – Окно раздела «Организация»

В области **Организация** имеется иконка <sup>2</sup>, 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 🥟 ); Выпустить токен – выпуск нового токена (иконка Показать токен – просмотр токена (иконка
- копирование токена в буфер обмена (иконка 🖳 ).

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

):

Редактировать токен	×
Название * Stage сервер EDR	
	Сохранить

Рисунок 25 – Окно редактирования названия токена

После редактирования названия токена требуется нажать по иконке

#### Сохранить.

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

Выпустить токен	×
Название *	
	Выпустить

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.

Подтверждение действия			
Удаление токена			
Выполнить Отмена			

#### 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).

Активность			Сбросить фильтры
Артефакты Клиенты			
Тип артефакта Вердикт	Период регистрации (на сервере)		🔕 Список 🔘 Календарь
Не задан 🛛 🗸 🖓 Вредоносный х Подозрительный х 🛛 Х 🗸 🖓	1 неделя		~
дополнительные фильтры			
Теги Не задан 🗸 🖉			
ГРАФИКИ ОБНАРУЖЕНИЙ			
(c)     1     >     Discussion     50     V			Найдено: 7, показано с 1 по 7
Название артефакта	Предыдущий вердикт / Время	Количество обнаружений $\uparrow\downarrow$	Время последнего обнаружения $\downarrow$
> <u>61c0810a23588cf492a6ba4f7654566108331e7a4134c368c2d6a05261b2d8a1</u>	Неизвестный 29.05.2024, 16:57:50	797	15.07.2024, 15:08:56
> <u>fd7499214abaa13bf56d006ab7dc78eb8d6adf17926c24ace024d067049bc81d</u>	Вредоносный 06.05.2024, 17:41:08	11326	15.07.2024, 10:32:19
> 2556248a38292c234d1aabe5e33a671fe8ae8aed28e0c8c4fbe767e4e7b 82f5	Подозрительный 03.06.2024, 09:27:51	8851	15.07.2024, 10:03:08
> 97b4d943605bbb3878f952e05bdebadec13cfa51d47ce858f84ebd04e013056d	Безопасный 25.05.2024, 16:39:21	2287	12.07.2024, 21:03:17
> a495431272644b6dbd2b06f787cc1620d5a53e1ccb0592ac6955ef064de5da50	Неизвестный 16.05.2024, 18:49:00	35	12.07.2024, 15:26:20
> b283415c9df06f0e53b7d452d3e5c840c5bd7a6ce734a30bae4a869a57974a0e		1554	12.07.2024, 11:31:31
> www.boxny.com ()	Неизвестный 13.06.2024, 17:24:36	47	12.07.2024, 10:25:30
e     c     1     >     >     Nocasultants not     50     V			Найдено: 7, показано с 1 по 7

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 файлаугрозы 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:

\_ <u>630ae106a99ae7da5d8dd33e7704b27701f6</u> – вредоносный файл (шрифт

красного цвета);

\_ <u>02f0c498bb4e5f62722ab5e8a63f5b3779db88ef</u> – безопасный файл (шрифт зеленого цвета);

- в73753С4С69А03F9А3E09F121B6599D77B1A4BE0247F9B71B56572555E1FE12BI- НЕИЗВЕСТНЫЙ ФАЙЛ (ШРИФТ

серого цвета);

— <u>61F897ED69646E0509F6802FB2D7C5E88C3E3B93C4CA86942E24D203AA878863</u> — 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.

C3 Protect TI					Файл: 246е	ce3b21e8	8747f3db8d0825fae	4cef86d8bb42f	8568591eaa75150c000ae08	езопасный
	Потоковый анализ >			Прочее >						
Основная информация	VirusTotal	Public TI	RST Cloud	Внешние источники	YARA	IOC	Заключение а	налитика		
							Основная і	информа	ция	
Безопасный вердикт									07.62.2023, 1433.39 BRI2954J COMAPYXEN	
Вердикт							6 e	езопасный (ин recutables sud	формация о файле содержится в источнике данных. "An index of Windows binaries, including download links for as exe, dll and sys files"	JSON
Впервые обнаружен							0	7.02.2023, 14:	33:19	
Тэги										
Размер файла							4	ОКВ		
SHA-256							2	46ece3b21e87	47f3db8d0825fae4cef86d0bb42f85e8591eaa7515bc800ae08	
SHA-1							4	de7452af2052e	14b1b2eea84bb27a4821e42dff	
MD5							e	Def722acc8803	0c0ca9ccada47ab394	
TLSH							t	99032b03bbb	529fcf9f1867849970416d235b2341b6199ff45b08a5d2e3e7c12b38b92	
Imphash							fe	af8ef2a61d523	37fd324d1624a3894b	
SSDEEP							1	92:n4cfa4m631	wacfo9gpmd67lqup0eudbmcqs+3dytpyetr68aejxmw1yw:ba4rgyru4wdy9lrvjww1yw	
Обнаруженные имена							0	asadhip.dll NU Imd64_microsoft.s	ll and Ed. microsoft windows reasonabil. 31H1856ad364435_18.8.22N211_noses_71H0x46a5511H4x2yzaadhip.ml_741Be63 ekdows reasonabil.91H2956ad34	
							Обнару	жения 🛕		
Нет данных										

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).

VirusTotal 🤨			∑ VirusTotal
24/69	mediaget Ide overlap prees Bjind (detectd	11.51 MB dag environment Passep	12.04.2023, 055653 Дата последнито анализа 28.04.2023, 100628 Времи получения отчета 28.04.2023, 100628 Времи постановки отчета в очередь
DETECTION DETAILS			1501
Avast	Win32:MiscX-Gen [PUP]	AVG	Win32:MiscX-Gen (PUP)
Cylance	Unsafe	Cyren	W32/ABRisk.DNTM-2624
DeepInstinct	MALICIOUS	DrWeb	Program.MediaGet.165
Elastic	Malicious (High Confidence)	ESET-NOD32	A Variant Of Win32/MediaGet.AK Potentially Unwanted
Fortinet	Riskware/MediaGet	Google	Detected
Gridinsoft	PUP.MediaGet.SdlC	Jiangmin	Downloader:MediaGet.Bla
K7AntiVirus	Adware ( 004ce1671 )	K7GW	Adware ( 004ce1671 )
Kaspersky	Not-A-Virus:HEUR:Downloader.Win32.MediaGet.Gen	Lionic	Riskware.Win32.MediaGet.11C
Malwarebytes	Floxif.Virus.FileInfector.DDS	MaxSecure	Downloader.W32.MediaGet.Gen_236651
Rising	Downloader.MediaGet!8.13A69 (TFE:5:Yf9JqlorOtT)	Sangfor	Downloader.Win32.Mediaget.Vxzo
Sophos	Generic Reputation PUA (PUA)	TrendMicro-HouseCall	TROJ_GEN.R002H0CIQ22
Webroot	W32.Adware.Gen	ZoneAlarm	Not-A-Virus:HEUR:Downloader:Win32.MediaGet.Gen
Acronis	Undetected	AhnLab-V3	Undetected
Alibaba	Undetected	ALVac	Undetected

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: nng zjhii o 953 l4hne 0 lm dosa 3 jtot jt 6 so 4 qasa 4 meq/f wa 6 mz mz: nng zjhir 3 lqe 0 lq loj twtg 4 qasa 4 tw sx a stat 100 ms s 10
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).

ГРАФИКИ ОБНАРУЖЕНИЙ	۵
Статистика обнаружений по клиентам	
6	
■ 1 (ЛУКОЙЛ) (5) ■ Load test (ЛУКОЙЛ) (1)	

## 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.

Отчеты			
Источник Тип артефакта			
Virus Total V Файл	~		
ГРАФИК ОТЧЕТОВ			~
		Найдено	: 272380, показано с 1 по 10
Артефакт	Статус	Время обращения	Действия
f24415c41d41cccc59171ace38e9bd533af6c78a02bd9a8117e1a6341df9c645 🕒	Отчет не был получен (Артефакт не найден)	19.09.2023, 10:25:54	Посмотреть отчет
e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b859	Отчет не был получен (Артефакт не найден)	18.09.2023, 16:16:49	Посмотреть отчет
e3b8c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b857 💭	Отчет не был получен (Артефакт не найден)	18.09.2023, 16:16:05	Посмотреть отчет
e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b851 🗗	Отчет не был получен (Артефакт не найден)	18.09.2023, 16:14:20	Посмотреть отчет
1ae4161b3c197c5274d55dc63378c4ab30e9f688a08223a4b6510f3ef6c4c01b 🗗	Отчет не был получен (Артефакт не найден)	18.09.2023, 12:14:01	Посмотреть отчет
49d7c335b19b6b6ba58619583567dbca4c4d0ec22e96eb74106aae5aa3b631c9 💭	Отчет получен успешно	18.09.2023, 12:06:11	Посмотреть отчет
9111099efe9d5c9b391dc132b2faf0a3851a760d4106d5368e30ac744eb42706 🗗	Отчет получен успешно	18.09.2023, 11:59:43	Посмотреть отчет
b75ef0d9be5c111341dab495301c5939495487c2a76eb2ec1d1eac393e6efc5e 🗗	Отчет получен успешно	18.09.2023, 11:55:58	Посмотреть отчет
3fa149b1165a3ff84e3e8524ece4ff86b91352f0686a1fded3e141ccec0f0a2d	Отчет получен успешно	18.09.2023, 11:55:42	Посмотреть отчет
9ecb5f24d9e3090aeecf6929fa69cf4e0648d726f7c7797279e1df9e7178fe5b 🖸	Отчет получен успешно	18.09.2023, 11:55:27	Посмотреть отчет
«         <		Найдено	: 272380, показано с 1 по 10



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.

Отчет					
/irusTotal 🗭				∑ Virus	Tota
		BEDaisy.sys prees assembly overlay 64bits native	3.19 MB signed Passep	08.09.2023, 21:56:50 Дата последнего анализа 18.09.2023, 12:06:11 Время получения отчета 18.09.2023, 12:06:09 Время постановки отчета в очередь	
DETECTION DETAILS					JSON
Fortinet	W64/FRS.AlTr		Acronis	Undetected	
AhnLab-V3	Undetected		Alibaba	Undetected	
ALYac	Undetected		Antiy-AVL	Undetected	
APEX	Undetected		Arcabit	Undetected	
Avast	Undetected		AVG	Undetected	
Avira	Undetected		Baidu	Undetected	
BitDefender	Undetected		BitDefenderTheta	Undetected	
Bkav	Undetected		CAT-QuickHeal	Undetected	
ClamAV	Undetected		CMC	Undetected	
CrowdStrike	Undetected		Cybereason	Undetected	
Cylance	Undetected		Cynet	Undetected	

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.

Гра	ф св	язей													
	$\Leftrightarrow$	zoom	[0]	θ	<sup>1</sup> nni	F	$\bigotimes$								
									ſ	Введите арт	тефакт				
												Показать	граф		

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 IPадреса представлен на рисунке 38.

pad	ф св	язей					
	$\oplus$	zoom	0	θ	23	=	$\otimes$

Рисунок 38 – Отображение графа связей для артефакта типа ір-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.

ww.goog	<u>jle.com</u>
P	<b>Безопасный</b> вердикт
0	28.10.2021, 10:12:39 ВРЕМЯ ОБНАРУЖЕНИЯ
$\overline{\cdots}$	<b>Нет данных</b> комментарий
Информ данных https://r	ация о домене содержится в источнике "Top 500 domains and pages from noz.com/top500"

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

чего появляется окно для внесения информации по привязанному артефакту, представленное на рисунке 42.

Привязать артефакты	×
Артефакты 🕕 *	
Тип артефактов *	
Не задан	~
Комментарий	
	Привязать

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



#### 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).

Журнал действий пользователей								
Тип событи	19	Объект действия		Статус		Временной период		
Не задан	,	✓ Не задан	~	Не задан	~	начальная дата →	конечная дата 🔛	
« c	2 3 4 > » Пок	казывать по: 10 💙				Найден	о: 4377, показано с 1 по 10	
	Время		Событие		Имя	пользователя	Статус	
>	30.08.2023, 14:49:57	Μ	одификация записи		1	rt@mail.ru	$\odot$	
>	30.08.2023, 14:49:45	М	одификация записи		1	rt@mail.ru	$\odot$	
>	30.08.2023, 14:49:38	M	одификация записи		I	$\odot$		
>	30.08.2023, 14:49:31	М	одификация записи		I	rt@mail.ru	$\odot$	
>	30.08.2023, 14:49:24	М	одификация записи		I	rt@mail.ru	$\odot$	
>	30.08.2023, 14:49:15	М	одификация записи			rt@mail.ru	$\odot$	
>	30.08.2023, 14:46:58	М	одификация записи		I	rt@mail.ru	$\odot$	
>	30.08.2023, 14:46:51	М	одификация записи		I	rt@mail.ru	$\odot$	
>	30.08.2023, 14:46:46	М	одификация записи		I	rt@mail.ru	$\odot$	
>	30.08.2023, 14:46:38	М	одификация записи		I	rt@mail.ru	$\odot$	
« «	2 3 4 > » Пок	казывать по: 10 🗸				Найден	о: 4377, показано с 1 по 10	
			Ŀ					

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

На рисунке 44 отображается информация о событии в формате HTML.

$\sim$	04.05.2023, 13:49:43	Индикатор атаки: Создание записи	1	rt@mail.ru	$\odot$
Имя		test-456			JSON
Изменен	ные поля		1 test-456 407 0 true ) 766 ) 2a99d650-3551-472b-a5ef-7 ) 2 g staffs ryytr	a2ef8b801b2	

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.

Интеграции						
VirusTotal	VIRUS TOTAL	$\otimes$				
	PUBLIC TI	$\otimes$				
RSTCIOUD	RST CLOUD	$\otimes$				
ATHENA	ATHENA	$\otimes$				
positive technologies	PT SANDBOX	$\otimes$				

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.

## Произошла ошибка

#### 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.

Данные не найдены (404)

#### 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.



В работе приложения произошла ошибка

#### 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.



Ошибка: неверный формат файла

#### 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.

Сессия была завершена. Требуется повторная авторизация

#### 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.

53

## 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.

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

#### Таблица 6 – Перечень сокращений

## 10. Заключение



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».