Веб-сервис RT Protect TI

Руководство аналитика

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

CJ RT **Protect**

CJ RT J Protect

Оглавление

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

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

1. Общие положения

1.1 Идентификация документа

Данное руководство кратко можно идентифицировать согласно таблице

1.

Таблица 1 – Идентификация документа

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

1.2 Аннотация документа

Документ предназначен для ознакомления пользователей сервиса с ролью «Аналитик» (подключенных в рамках одной организации, не являющейся владельцем платформы) с технической информацией о программе «RT Protect TI» (далее по тексту программа) и содержит общие сведения о программе, организационно-распорядительные меры, сведения о структуре, описание настроек программы и тексты сообщений, выдаваемых в ходе выполнения настройки, проверки, а также о процессе функционирования программы.

1.3 Термины и определения

В настоящем документе используются термины и определения согласно ГОСТ Р ИСО/МЭК 15408 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий» и ГОСТ Р ИСО/МЭК 12207-2010 «Информационная технология. Системная и программная инженерия. Процессы жизненного цикла программных средств» согласно таблице 2.

Таблица 2 – Термины и определения

Термин	Описание		
Администратор	Уполномоченный пользователь, ответственный за установку, администрирование и эксплуатацию программы		
Артефакты	Различные типы данных имеющие подозрительное содержимое и загружаемые на сервер для анализа (файлы, доменные имена, IP-адреса, URL)		
Backend	Программно-аппаратная часть сервиса, отвечающая за функционирование его внутренней части		
JSON	Текстовый формат обмена данными, основанный на JavaScript		
JSON-объект	Неупорядоченный набор пар ключ/значение. Объект начинается с открывающей фигурной скобки { и заканчивается закрывающей фигурной скобкой }. Каждое имя сопровождается двоеточием, пары ключ/значение разделяются запятой		
Linux	Семейство Unix-подобных операционных систем на базе ядра Linux		
Malware Bazaar	Проект сайта abuse.ch, целью которого является обмен образцами вредоносного ПО с сообществом информационной безопасности, поставщиками антивирусных программ и поставщиками информации об угрозах		
SSDEEP	Алгоритм нечеткого хеширования		
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 HTML-страницей, изображением, файлом, медиа-потоком или другими данными		
WHOIS	Сетевой протокол прикладного уровня, базирующийся на протоколе TCP. Основное применение – получение регистрационных данных о владельцах доменных имён, IP- адресов и автономных систем		

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

1.4 Условные обозначения

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

Таблица 3 – Условные обозначения

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

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.

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

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

3. Организационно-распорядительные меры

3.1 Общие сведения

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

Программа и документация на нее хранятся на сервере предприятияизготовителя.

Программа поставляется заказчику согласно комплектности поставки.

3.2 Комплектность поставки

Комплектность поставки представлена в таблице 4.

Обозначение	бозначение Наименование		Примечание
	Предоставление доступа к Веб-сервису RT Protect TI	1	
	Комплект документов согласно списку:		
	– «Веб сервис RT Protect TI	4	
	Руководство Администратора»;	1	
	— «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 пригодна для функционирования на аппаратных платформах, указанных в таблице 5.

Таблица 5 – Программно-аппаратное обеспечение

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

Программа поддерживает работу в браузерах, представленных в таблице

6.

Таблица 6 – Список поддерживаемых браузеров

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

5.2 Роли

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

– пользователь;

– аналитик;

– администратор.

Пользователь – сотрудник отдела ИБ или SOC-центра.

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

– Главная страница.

Сотруднику с ролью «Пользователь» доступны следующие действия:

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

– ІР-адрес;

– доменное имя;

- URL;

– контрольную сумму файла (хеш-суммы);

– email.

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

3) просмотр страницы отчета по проверенному артефакту.

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

В круг типовых задач аналитика входят:

– проверка артефактов;

– анализ активности;

– просмотр отчетов об артефактах;

– просмотр программ и уязвимостей найденных в данных программах.

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

6. Интерфейс программы

6.1 Окно авторизации и общие сведения

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



Рисунок 2 – Окно авторизации

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

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 открывается основное окно программы (рис. 4).

E3 RT Protect TI	α Ξ				(, a.
😡 Главная страница	Проверка артефактов				
администрирование					
	оведите п-адрес, доменное имя, окс, ептан	и или контрольную сумму фаила для проверки			Ompa
🖏 Теги	СТАТИСТИКА ДОБАВЛЕНИЯ АРТЕФАКТОВ 3/	А МЕСЯЦ			
аналитика	Файлы	Доменные имена	IP-Адреса	Url	Email
🕑 Активность	/54563	34302	1320392	☐ 70933	₩ 21
🖹 Отчеты	АКТИВНОСТЬ		Lee La	4	
ွိးေ Граф связей	👁 Файлы 🐟 IP-Адреса 🐟 Доменные имена 🐟 Url 🐟 Email				
	9000-				
	15:23:13 16:23:13 17:23:13 18:23:13	19:23:13 20:23:13 21:23:13 22:23:13 23:23:1	00:23:13 01:23:13 02	23:13 03:23:13 04:23:13 05:23:13 06:23:13	8 07:23:13 08:23:13 09:23:13 10:23:13 11:23:13 12:
	ТОП 5 РАСПРОСТРАНЕННЫХ УГРОЗ (ФАЙЛЬ	(Ic		ТОП 5 ПОСЛЕДНИХ УГРОЗ (ФАЙЛЫ)	
	31.9 %	MSSS.exe (11469) nMirror.exe (0938) af2222204fca27c0fdab9eefbfdb638a (6052) servexe (6659 1415c41d41cccc59171ace38e9bd533af (3840)		0.0 %	 e3b9afb71e8772545a26f28b3a4f3769251 (5) a 3c84b59be7eb4c7c42efeaad2e9c2c3233 (4) TunMirror.exe (8938) KMSS5.exe (11469) 4a468603fdcb7a2eb5770705896cf9ef37a (1363)

Рисунок 4 – Основное окно программы

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

Функции, доступные в интерфейсе административного модуля управления:

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

– просмотр и анализ обнаружений на странице Активность;

– просмотр отчетов по анализу проверенных артефактов;

– просмотр перечня программ и найденных уязвимостей.

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

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

6.2 Горизонтальная панель управления

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



Рисунок 5 – Горизонтальная панель управления

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

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

Проверкя артефиястов							
Bergers II-Apper groupse and URL and not companying spany datas gas represent							
ана на подключено организации	ñ	е во подключено кливное		281/149 Infollition & Markotty Ecello / Viorkaniarian			
СТАТИСТИКА ДОБАВЛЕНИЯ АРТЕФА	ктов за месяц				6		
Файла 586113	40000000000000000000000000000000000000	P.Appeca 7189083		() IO	0		
АКТИВНОСТЬ		ter la			Неделя Дляь Час		
18000		-φ Фаλлы -⇔ IP-Адреса -⇔ Д	owennice vinces - Url -+ Email				
11500 6020- 4130-							
16.32.53 17.02.53 17.52.55 16.02.53	18.52.55 19.02.51 19.52.55 20.02.55 20.52.51 21.02.55 21.52.55 22.02.55 22.52.55 23.02.55 23.52.55	003253 003253 010255 013253 020253 023253 010253 033253 0402	51 043255 050255 053251 060255 065255 070255 073255 080255	08.22.53 09.02.53 09.02.53 10.02.53 10.02.53 10.02.53 10.02.53 10.02.53 10.02.53	140258 145258 150258 153258 160258		
топ 5 источников данных по к	оличеству обнаружений		топ 5 распространенных угроз (файлы)				
38.9 %	Cont Serve Back ID Lit (8919) Instatution # Unit (8919) Instatution # Unit (8917) Inst Council Server 47771 Inst Council Server 477080 IOTUL-SRM Matteries (7908)		10.7 %	14019440005114. (852) 41 (1900) Privel 114. (1840)			
топ 5 последних угроз (файлы;	1		ТОП 5 РАСПРОСТРАНЕННЫХ УГРОЗ (ДОМЕННЫЕ ИМЕНА)				
38.9 %	"Indiffuse and BFID "Indiffuse and IDED "		52.4 %	ventopa ng 1444 14 cm 2446 1971 19 19 19 19 19 19 19 19 19 19 19 19 19			

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 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).

По	Пользователь								
දු	Профиль								
Ł	Выход								

Рисунок 7 – Меню «Пользователь»

Подменю Профиль представлено на рисунке 8.

Ірофиль
mail
0/6
MR
янилия
рганизация
лукойл
писание
Сменить 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 (только аналитик);
- имя и фамилия пользователя;
- организация (в которой работает аналитик);
- поле с описанием профиля пользователя.

Изменять пароль возможно с помощью кнопки Сменить пароль. При нажатии

кнопки Сменить пароль открывается окно для смены пароля (рис. 9).

Сменить пароль	×
Ваш текущий пароль *	
	\odot
Новый пароль *	
	\bigcirc
Повторите пароль *	
	\odot
Требования к паролю • Пароль должен быть не менее 8 символов. • Должен содержать хотя бы одну заглавную букву. • Должен содержать хотя бы одну строчную букву.	
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 4 представлен раздел Главная страница модуля управления.

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

– область проверки артефактов;

– статистика добавления артефактов за месяц;

– графическое представление активности (отображение обнаружений);

– графические отображения Топ 5 источников данных по количеству обнаружений;

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

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

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

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

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

Данные иконки имеют вид : 📩 - ширина 100%, 📩 - ширина 50 %. Примеры отображения области **Графики** представлены на рисунках 10 - 11.



Рисунок 10 – Области с графиками с шириной 50%



Рисунок 11 – Область с графиком с шириной 100%

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

В области Проверка артефактов администратор также может проверить

целый список артефактов, нажав по иконке 📕, после чего откроется окно для загрузки списка артефактов, представленное на рисунке 12.



Рисунок 12 – Окно для написания списка артефактов для проверки

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

6.4 Администрирование

В области Администрирование основной панели программы находятся следующие разделы:

– Организация;

– Теги.

Аналитик может выполнять следующие действия:

– просматривать подробную информацию о своей организации;

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

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

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

– просмотреть список тегов и псевдонимов.

6.4.1. Организация

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

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

Организация										
		Рассии СТЯНА	Pacar Comm.							
		www.bubal.nu	a weeklastiv esti colt							
лукойл		Добына голезных искополных сселор								
ansees and a second sec										
101 000, Рессийская Фадерация, г. Маская, Сретенский функара, 11 Інкейфіканского - 74956774444 - 74956285841 - 7495829786 всегисты	IN Bits, Processione Hypergener, C. Moores, Germscont Hypergener,									
ПОСИЛИИ С СТАТИТИКИ В СТАТИТИКИ ПО СТАТИТИКИ ПО СТАТИТИКИ С СТАТИТИКИ С СТАТИТИКИ С СТАТИТИКИ С СОЛО С СТАТИТИКИ С СТАТИТИКИ.	75 мировой добычи нефти и окало 1% доказанных запасов утлеводородов									
- file										
Keonu										
The second secon										
				Найдинас 6, посклано с 1 по 6						
пульжа ил	23 / 0	50 / 0	17.4%.3804. 15:48:58	дага обновления / пользователь						
			QAadmin@gmail.com							
Ranyverts vallop exponses orveree no Irnail	10 / 0	5/0	14.00.3804, 18.11.12 QAadmin@gmail.com	17.86.3856, 14.3612 QAadmin@gnat.com						
Tony-enu valiop reponses or verse no P	20/0	20 / 0	14.06.2004, 30:30:30:33 QAadmin@gmail.com	17.06.2804, 16:31:31 QAadmin@gnal.com						
Получить кабор отчитов по файлам с обогацияниям	5/0	10 / 0	14.86.3834, 37.87.89 QAadmin@gmail.com							
Получить кабор королиих отчетов по файкам	15 / 0	15 / 0	14.06.3094, 37286-09 QAadmin@gmail.com	17.06.2824, 16:36:58 QAadmin@gnal.com						
Получить набор полных отчетов по файлам	5/0	10 / 0	54.86.3804, 37.86.30 QAadmin@gmail.com							
x c 1 x x Excesses to 10 - V				Найданнос 6, посаланно с 1 по 6						
Клиенты										
c c t t s s fournam nu 10 v				Haligeven 8, novamen c 1 no 8						
Maa 3 Laarfaat										
> 1001 355										
> 31										
> 6666										
> 1111										
> 1111										
3 m										

Рисунок 13 – Окно раздела «Организация»

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

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

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

6.4.2. Теги

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

Страница Теги представлена на рисунке 14.

Теги			۵) b			Сбросить фильтры				
Группы тегов Группы псевдонимов										
Название	Название									
Begurte shakesike 📎										
	» Показывать по: 50 🗸					Найдено: 9, показано с 1 по 9				
	Название ↑↓	Префикс ↑↓	Описание	Количество	Дата создания / Автор $\uparrow \downarrow$	Дата изменения / Автор				
	5	5	5	3	15.05.2024, 15:32:02 test_SP_@rt.ru	06.06.2024, 14:31:27 QAadmin@gmail.com				
	name	prefix	description	5	06.06.2024, 15:35:30 QAadmin@gmail.com	21.06.2024, 17:02:25 QAadmin@gmail.com				
	name_555	prefix_test	description_test	1	21.06.2024, 16:46:50 QAadmin@gmail.com	24.86.2824, 15:11:48 QAanalyst@gmail.com				
	stage	qa	46464	0	87.85.2824, 17:84:48 QAadmin@gmail.com					
	test_group_1	alexb	asdads	0	28.05.2024, 17:46:38 test@test.ru					
	test_kn_1	54	desc	5	28.05.2024, 16:25:41 rt@mail.ru	28.05.2024, 16:26:00 rt@mail.ru				
	test_qa	QA	test	0	38.85.2824, 16:48:88 QAanalyst@gmail.com					
	test_tags	qa	for_test	0	30.05.2024, 15:42:00 QAadmin@gmail.com					
	Tools	Tool	Набор потенциально вредоносных утилит, используемых атакующими	1	26.06.2024, 17:02:03 k.vasilev@rt-ib.ru					
« < 1 >	» Показывать по: 50 🗸					Найдено: 9, показано с 1 по 9				

Рисунок 14 – Страница Теги

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

6.5 Аналитика

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

- 1) Активность;
- 2) Отчеты;
- 3) Граф связей;
- 4) Угрозы и злоумышленники.

6.5.1. Активность

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

Активность			Сбросить фильтры		
Аргефакты Клиенты					
Тип артефакта Вердикт	Период регистрации (на сервере)		О Список ○ Календарь		
Не задан 🗸 🖉 Вредонорный ж Подорительный ж 🛛 Х 🗸 🖓	1 неделя		~]		
дополнительные фильтры			v		
Тем Не задан / / Ø					
Графики обнаружений					
« ← 1 → » Docasetation not 50 ♥			Найдено: 7, показано с 1 по 7		
Название артефакта	Предыдущий вердикт / Время	Количество обнаружений $\uparrow\downarrow$	Время последнего обнаружения \downarrow		
> 61c8818822588cf492a6ba4f7654566188331c7a4134c968c2d6a85261b2d8a1	Неизвестный 29.05.2024, 16:57:50	797	15.07.2024, 15:08:56		
> fd7499214abaa13bf56d006ab7dc78eb8d6adf17926c24ace024d067049bc81d	Вредоносный 05.05.2024, 17:41:08	11326	15.07.2024, 10:32:19		
> <u>cb56c248a38292c224d1aabe5e3a671fe8ae8aed28e0c8c4fbe767e4e7b82f5</u>	Подозрительный 03.06.2024, 09:27:51	8851	15.07.2024, 10:03:08		
> 97b4d943605bbb3878f952e05bdebadec13cfa51d47ce888f84ebd04e013055d	Безопасный 25.05.2024, 16:39:21	2287	12.07.2024, 21:03:17		
> <u>##95431272644b6dbd2b06f787cc1620d5as2e1ccb0592ac6955ef064de5da50</u>	Неизвестный 16.05.2024, 18:49:00	35	12.07.2024, 15:26:20		
> b283415c9df06f0e53b7d452d3e5c840c5bd7a6ce734a30bae4a869a57974a0e		1554	12.07.2024, 11:31:31		
> www.bosty.com	Неизвестный 13.06.2024, 17:24:36	47	12.07.2024, 10:25:30		
к с 3 > Показываль по: 50 ч Найдено: 7, показыно с 1 по 7					

Рисунок 15 – Общий вид страницы Активность

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

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

Таблица на вкладке Артефакты имеет следующие поля:

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

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

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

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

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

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

CJ Protect TI					Файл	n asedasosfaeada	1c12a@eab	17edfbd8f908af0fbaa43a42ca46d8e5ad8c	2685		Sezonacinaŭ .	
Основная информация	Потоковый анализ > VirusTotal	Public TI	RST Cloud	внешние источники	YARA I	ОС Заключен	ие аналитика	2				
Основная информация 3												
Безопасный вердикт									28.03.2024, 05: впервые обнар	36:09 9ЖН		
Вердикт									Безопасный (вердикт основан на	otvete VirusTotal)		JSON
Впервые обнаружен									28.03.2024, 05:36:09			
Тэги												
Размер файла									18.06 MB			
SHA-256									85ed8506f5ea061c12a0eab17edfbd	8F900a101baa43a42ca46d8e5ad8c2e8b5		
MDE									e10941e14001a0024750ec0105c340	1090331028		
TISH									902000/110000902011004910080700 +1001744005200116545470b2490b20	20 16660a76bz066b21z2z412z0701a2d22ba08d24b22		
Imphash									b0d4c405dccd4e40f7d815f48db1cf	84		
SSDEEP									393216:pp/ihlippipizxnph2+9mcp9	w9xvdab376xvti:avifiaa.joancocadahmxvp		
Обнаруженные имена	Anno 252 (Balance Constant) (Bal							15007651.exe				
							Ci	зязанны	ые артефакты 🗞 \land			4
	Артефакт			Тип артефа	ікта	Количество об	бнаружении		Комментарий	Дата создания / Автор	Дата последнего сохранения / Автор	Управление
								Нет	данных ⊘			
- riposecare apreçace												
								OQH	наружения 🛄			5

Рисунок 16 – Страница отчета сервиса по обнаруженной угрозе

Страница отчета программы об угрозе разделена на следующие области:

1) область краткой информации об угрозе;

2) область вкладок;

3) область основной информации;

4) область связанных с артефактом других артефактов;

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

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

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

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

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

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

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

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

VirusTotal			∑ VirusTotal
24.68	medaget into rendry press input detect	11.51 M8 Passep	12.04.2023, 055653 Дата последнето внаниза 28.04.2023, 100588 Время получения стичта 28.04.2023, 100686 Время постановки отчета в очередь
DETECTION DETAILS			ISON
Avast	Win32:MiscX-Gen [PUP]	AVG	Win32:MiscK-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	Flowif.Virus.FileInfector.DDS	MaxSecure	Downloader.W32.MediaGet.Gen_236651
Rising	Downloader.MediaGett8.13A69 (TFE:5:Yf9)qlorrOtT)	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	ALYac	Undetected

Рисунок 17 – Результаты анализа артефакта на странице Virus Total

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

Вердикт	Вредоносный (вердикт основан на отчете VirusTotal)
Впервые обнаружен	05.07.2022, 12:37:44
Размер файла	11.51 MB
SHA-256	630ae106a99ae7da5d8dd33e7704b27701f698ce81c6d859be07e1157563cd24
SHA-1	ace104fb3a778773752d21d334a8beabeebf3b29
MD5	5ff37d5bd1f55421a18829e52a804108
TLSH	t1f3c6cf2337058c29d52110b06ea9d79a9319fd238b2167cfb38d6a6d1a7c1c24f35bf6
Imphash	9f72a91bb07c782d841b9af20ada6733
SSDEEP	196608: nngzjhiio 95314hne0 Imdosa3 jtot jt 6 so 4 qasa 4 meq/fwa 6 mzmz: nngzjhir 3 lqe0 lqloj twtg 4 qasa 4 tws x mana 196608 mzmz: nngzjhir 3 lqe0 lqloj twtg 4 qasa 4 tws x mana 196608 mzmz: nngzjhir 3 lqe0 lqloj twtg 4 qasa 4 tws x mana 196608 mzmz: nngzjhir 3 lqe0 lqloj twtg 4 qasa 4 tws x mana 196608 mzmz: nngzjhir 3 lqe0 lqloj twtg 4 qasa 4 tws x mana 196608 mzmz: nngzjhir 3 lqe0 lqloj twtg 4 qasa 4 tws x mzmz = 196608 mzmz: nngzjhir 3 lqe0 lqloj twtg 4 qasa 4 tws x mzmz = 196608 mzmz: nngzjhir 3 lqe0 lqloj twtg 4 qasa 4 tws x mzmz = 196608 mzmz: nngzjhir 3 lqe0 lqloj twtg 4 qasa 4 tws x mzmz = 196608
Обнаруженные имена	mediaget.exe

Рисунок 18 – Информация отчета об артефакте в формате HTML

Окно основной информации по результатам анализа артефакта в формате

JSON представлено на странице 19.

{ 27 items	HTML
"id" : 57066978	_
"sha256" : "630ae106a99ae7da5d8dd33e7704b27701f698ce81c6d859be07e1157563cd24"	
"sha1" : "ace194fb3a778773752d21d334a8beabeebf3b29"	
"md5" : "5ff37d5bd1f55421a18829e52a804108"	
"t1sh": "T1F3C6CF2337058C29052110806EA9079A9319FD23882167CF83806A6D1A7C1C24F358F6"	
"imphash" : "9f72a91bb07c782d841b9af20ada6733"	
"ssdeep" : "196608:NWgZJhiI095334NWe8LmD0sA3jToTJt6so4qAsA4WeQ/FWa6mzmZ:NWgZJhir31Qe8LQ10jTWT64qAsA4TWsX"	
"artifactClass" : 3	
"artifactName": "MaliciousFile"	
"artifactSeverity": 4	
"nsrlinfold" : NULL	
"sophosInfold": NULL	
"vtReportId" : 164411	
"kasperskyReportId" : 6173	
"yaraReportId" : Mull	
"fileExpertOpinionId": "6e454816-030f-4481-s94a-f04766175b82"	
"iocld" : Matt	
"ptMsReportId" : MULL	
"athenaReportId" : 26	
"firstTimeSeen": "2022-07-05T09:37:44.7012592"	
"info": "Вердикт основан на отчете VirusTotal"	
* "fileNames" : [2 items	
0 : "mediaget.exe"	
1: "mediaget"	
1	
"fileSize" : 12070544	
"hasFileInFileStorage" : false	
"uploadTime" : Mall	
"uploadInProgress" : false	
* "feedsToHashInfos" : [] 0 items	
}	

Рисунок 19 – Информация отчета об артефакте в формате JSON

В области Связанные артефакты показывается таблица с описанием артефакта, связанного с тем артефактом, отчет по которому просматривается на

данный момент. При нажатии по иконке Привязать артефакт открывается окно для привязки артефактов друг к другу (см. рисунок 20).

Привязать артефакты	×
Артефакты 访 *	
Тип эптефактор *	
Не задан	~
Комментарий	
	Привязать

Рисунок 20 – Окно для привязки артефакта

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

Важно

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

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

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

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

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

– Теги.

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

- Артефакт;
- Количество обнаружений не менее;
- Количество обнаружений не более;
- Предыдущий вердикт;
- Время последнего изменения вердикта.

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



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

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

– статистика обнаружений по типам;

– статистика обнаружений по вердиктам;

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

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

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

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

– Теги.

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

- Артефакт;
- Количество обнаружений не менее;
- Количество обнаружений не более;
- Предыдущий вердикт;
- Время последнего изменения вердикта;
- Клиенты.

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

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

6.5.2. Отчеты

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

Отчеты				
Источник Тип артефакта				
Virus Total v Файл	~			
ГРАФИК ОТЧЕТОВ				
		Найде	ено: 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	
e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b857 📮	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	
« <		Найде	ено: 272380, показано с 1 по 10	

Рисунок 22 – Окно раздела «Отчеты»

В таблице имеются следующие поля:

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

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

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

– Действия (получить отчет).

Информация об артефакте отображается разными цветами:

– шрифт красного цвета (артефакт является вредоносным);

– шрифт зеленого цвета (артефакт является безопасным).

Над таблицей для фильтрации информации имеются следующие фильтры:

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

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

Над таблицей для отображения визуальной информации имеется область

с графиком полученного числа отчетов за определенный период в зависимости от установленного в фильтре источника данных (рисунок 23).



Рисунок 23 – Отчеты Virus Total

Для сворачивания области График отчетов требуется нажать по иконке

Для просмотра отчета по артефакту нужно нажать по иконке

Страница отчета по артефакту представлена на рисунке 24.

Отчет			
/irusTotal 🖸			Virus Tota
	BEDaisy. receive 64bits	sys 3.19 M8 executly signed Passep name	08.09.2023, 21:56-50 Дата последнего анализа 18.09.2023, 1:206611 Время получения стчета 18.09.2023, 1:20669 Время постановки отчета в очередь
DETECTION DETAILS			ISO
Fortinet	W64/FRS.AITr	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 24 – Страница отчета по артефакту от источника Virus Total

6.5.3. Граф связей

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

Граф связей	
🗆 🕂 zoom 🖸 🖯 🐹 🖃 🔇	
	Введите артефакт
	Показать граф

Рисунок 25 – Общий вид пустой страницы «Граф связей»

На странице имеется две области:

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

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

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

Пример отображения графа после заполнения поля артефакта в виде ipадреса представлен на рисунке 26.



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

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



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

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

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

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

Грас	ф св	язей					
	\Leftrightarrow	zoom	0	θ	្រំព័	E	
wv	<u>vw.g</u>	oogle.c	:om				
По	казать	инфори	иацию	обар	отефак	те	

Рисунок 28 – Краткая информация по артефакту

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



Рисунок 29 – Информация о артефакте

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

Для привязки нового артефакта следует нажать по иконке ²⁰⁰, после чего появляется окно для внесения информации по привязанному артефакту, представленное на рисунке 30.

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

Рисунок 30 – Окно добавления информации для привязывания артефакта

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

Для удаления узла графа из привязанных артефактов следует нажать по



7.1 Общие сведения

Большинство ошибок можно разделить на следующие типы:

1) ошибки конфигурации:

– некорректные настройки параметров безопасности;

– некорректная установка компонентов программы;

– некорректные действие со стороны пользователя/администратора;

– критические ошибки.

2) ошибки оборудования:

выход из строя аппаратных средств, на которых установлена программа;

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

– перебои питания со стороны серверной части.

Для устранения ошибки требуется обратиться к поставщику программы.

8. Перечень сокращений

Основные сокращения, указанные в документе, представлены в таблице

7.

Таблица 7 – Перечень сокращений

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

9. 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».