

RT Protect TI

Руководство пользователя

Версия 1.0.35 от 19 июня 2026

Разработано компанией АО «РТ-Информационная безопасность»



1. Общие положения	2
2. Общие сведения	3
3. Назначение программы	4
3.1 Основные задачи и возможности	4
3.2 Способы отражения предметной области в программе	4
4. Роли пользователей, взаимодействующих с Сервисом	5
5. Порядок взаимодействия с сервисом	6
6. Операции, доступные пользователю программы	7
6.1 Общие сведения	7
6.2 Главная страница	8
6.3 Организации	13
6.4 Активность	14
6.5 Заявки	20
6.6 Анализаторы	21
6.7 Граф связей	25
6.8 Угрозы и злоумышленники	28
6.9 Вредоносное ПО	29
6.10 Инструменты	30
6.11 Матрица MITRE ATT&CK	31
6.12 Лента угроз	32
6.13 Уязвимости	34
6.14 Программы	37
7. Сообщения об ошибках	42
8. Термины и определения	43
9. Заключение	44

1. Общие положения

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

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

Данное руководство кратко можно идентифицировать согласно таблице 1.

Таблица 1 – Идентификация документа

Название документа	«RT Protect TI» Руководство Пользователя
Версия документа	Версия 1.0.35 (актуальна для версии продукта 3.4.0)
Идентификация программы	Сервис по предоставлению аналитики «RT Protect TI»
Идентификация разработчика	АО «РТ-Информационная безопасность»

2. Общие сведения

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

3. Назначение программы

3.1 Основные задачи и возможности

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

- 1) Широкая система администрирования пользователей сервиса (пользователи; организации; источники данных);
- 2) Проверка артефактов вредоносной активности (IP-адрес, диапазон IP адресов, доменное имя, URL, файлы);
- 3) Работа в автономном режиме и режиме интеграции с системами защиты конечных точек;
- 4) Предоставление информации о распространенных угрозах, проверенных с помощью сервиса;
- 5) Взаимодействие с иными сервисами проверки артефактов (VirusTotal, RST Cloud и другие);
- 6) Предоставление вердикта по артефактам;
- 7) Создание и хранение аналитики для предоставления во внешние сервисы (индикаторы атак, индикаторы компрометации, уага-правила, журналы Windows);
- 8) Создание и хранение наборов с исключениями (для программ и файлов);
- 9) Регистрация действий пользователей сервиса.

3.2 Способы отражения предметной области в программе

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

Сервис разворачивается на мощностях предприятия разработчика.

Сервис является облачным решением, для взаимодействия с которым пользователю предоставляется открытое API. Взаимодействие с сервисом возможно через браузер.

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

4. Роли пользователей, взаимодействующих с Сервисом

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

- пользователь;
- аналитик;
- администратор безопасности.

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

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

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

5. Порядок взаимодействия с сервисом

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

6. Операции, доступные пользователю программы

6.1 Общие сведения

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

- используя функционал главной страницы, просматривать сводную информацию по активности в организациях, подключенных к сервису;
- просматривать информацию об организациях, подключенных к сервису;
- используя функционал разделов аналитики просматривать информацию об артефактах и обнаружениях в организациях, подключенных к сервису;
- просматривать отчеты об анализе артефактов, обнаруженных в организациях;
- просматривать связи артефактов между собой в разделе **Граф связей**;
- просматривать список уязвимостей и программ для которых найдены уязвимости.

6.2 Главная страница

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

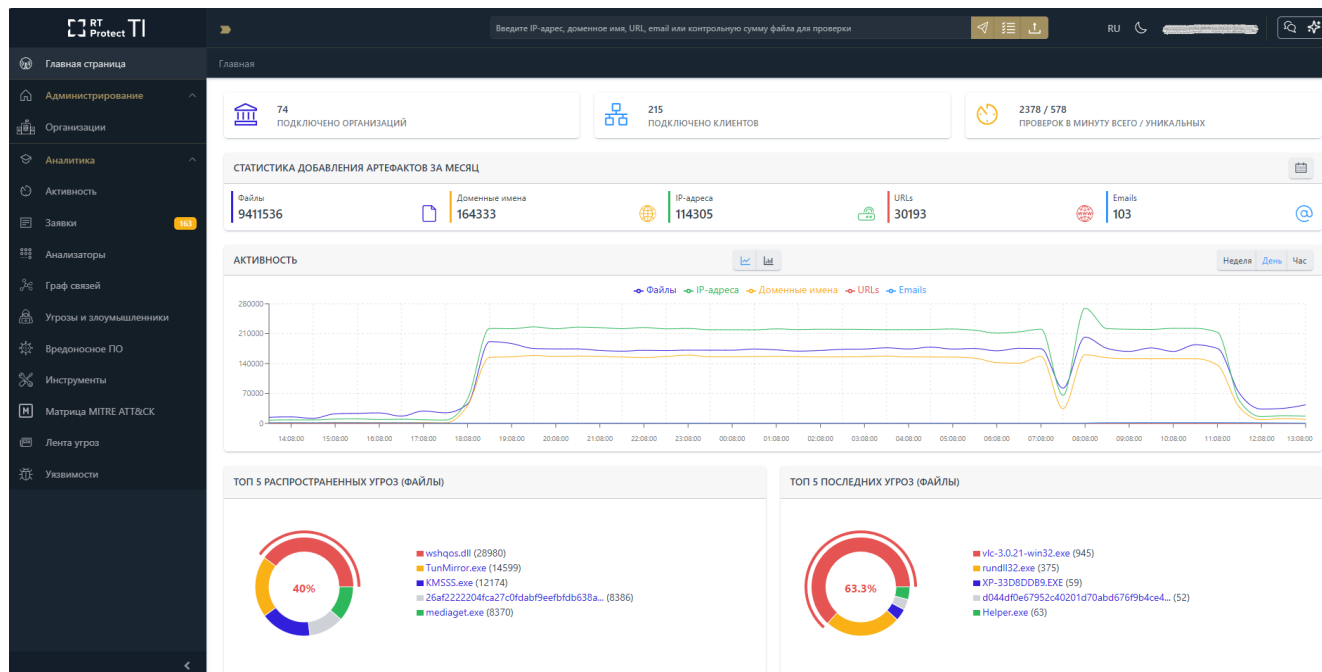


Рисунок 1 – Главная страница

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

В верхней части окна находится горизонтальная панель управления (рис. 2).

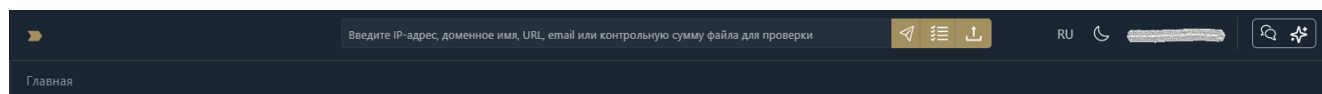


Рисунок 2 – Горизонтальная панель управления

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 по иконке  все страницы будут представлены в темной теме. Для возврата светлой темы необходимо повторно нажать на иконку.

При нажатии ЛКМ по иконке  появляется область, представленная на рисунке 3.

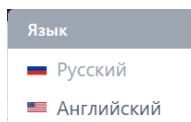


Рисунок 3 – Выбор языка

В данной области можно выбрать язык, на котором будет отображаться информация на всех страницах модуля администрирования.

При нажатии по иконке , открывается область чата, где пользователи могут оставлять сообщения и комментарии, отвечать на сообщения, оставленные другими пользователями, а также редактировать и удалять собственные комментарии.

При нажатии по иконке , открывается окно для работы с ИИ агентом.

В правом верхнем углу находится иконка с именем, идентифицирующая пользователя, который произвел вход в программу на данный момент. При нажатии по данной иконке происходит переход в окно выбора действий, представленное на рисунке 4.

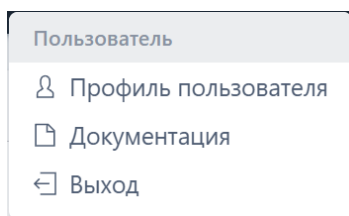


Рисунок 4 – Окно «Пользователь»

При нажатии по иконке **Документация** будет загружено руководство в формате pdf согласно роли под которой был осуществлен вход, при этом руководство будет отличаться для ролей пользователей с выставленным признаком владельца и не владельца платформы.

При нажатии по иконке **Выход** появляется окно подтверждения для выхода из профиля, представленное на рисунке 5.

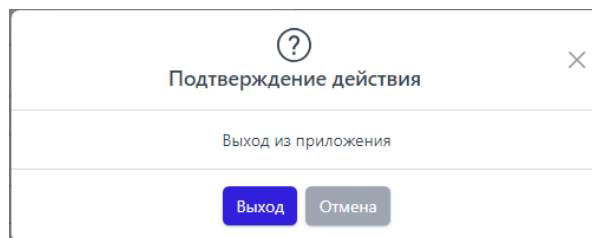


Рисунок 5 – Окно подтверждения действия выхода из приложения

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

Окно просмотра профиля пользователя представлено на рисунке 6.

Рисунок 6 – Окно просмотра профиля пользователя

В данном окне редактировать информацию о пользователе нельзя.

Для смены пароля требуется нажать по иконке **Сменить пароль**, после чего откроется окно смены пароля, представленное на рисунке 7.

Рисунок 7 – Окно смены пароля

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

В области представленной на рисунке 8 можно отправить артефакт, либо список артефактов на проверку.

Рисунок 8 – Область быстрой отправки артефактов на проверку

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

Откроется отчет TI-платформы (подробнее см. в пункте **Ошибка! Источник ссылки не найден.**).

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 9.

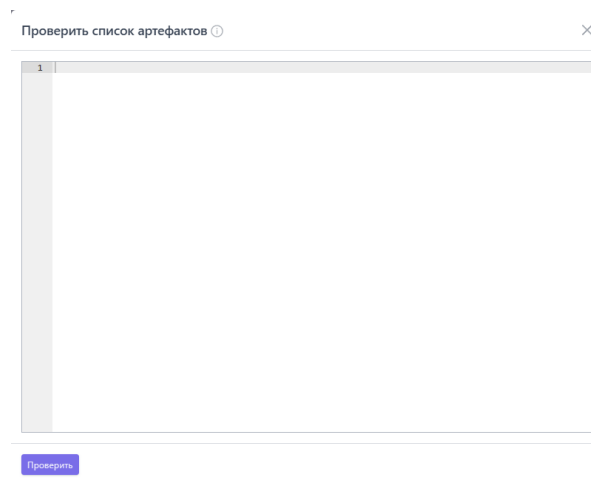


Рисунок 9 – Окно для добавления списка артефактов для проверки

В данном окне артефакт добавляется по одному в каждой строчке (строчки нумеруются). Проверка артефактов списком ограничена количеством в 1000 строк. После написания артефактов требуется нажать по иконке «Проверить».

Проверенный артефакт будет отображаться на странице **Активность** с вердиктом от TI-платформы (если артефакт уже присутствовал в базе). Можно создать заключение аналитика для одного или нескольких артефактов (создание заключения для группы артефактов).

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

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

6.3 Организации

В разделе **Организации**, представленном на рисунке 10, пользователь организации владельца платформы может просмотреть информацию обо всех организациях и клиентах, подключенных к сервису.

Название	Страна	Сектор	Количество обнаружений за месяц	Дата создания / Автор	Дата обновления / Пользователь
Название_организации	ОАЭ	Строительство	0	17.09.2025, 18:19:48 QAAdmin@gmail.com	
тестовая 3			9	28.11.2025, 14:08:37 QAAdmin@gmail.com	06.09.2026, 15:58:28 test_SP@rt.ru
тестовая 2			0	28.11.2025, 14:07:23 QAAdmin@gmail.com	
тестовая 1			0	28.11.2025, 14:07:03 QAAdmin@gmail.com	
vp-test			0	16.11.2025, 18:36:37 v.pavlichuk@rt-ib.ru	
ORG_testbud	Федеративные Штаты Микронезии	Сельское хозяйство	223	14.11.2025, 13:12:34 a.budnik@rt-ib.ru	18.12.2025, 12:51:47 a.budnik@rt-ib.ru
test3(M)			0	23.10.2025, 16:51:23 QAAdmin@gmail.com	
test2(n_M)			0	23.10.2025, 16:50:43 QAAdmin@gmail.com	23.10.2025, 16:51:42 QAAdmin@gmail.com
test_1(n_M_B)			0	23.10.2025, 16:49:37 QAAdmin@gmail.com	23.10.2025, 16:50:05 QAAdmin@gmail.com

Рисунок 10 – Окно раздела «Организации»

Для фильтрации информации на странице предусмотрена система фильтров, представленная в следующем списке:

- **Название;**
- **Страна;**
- **Сектор;**
- **Признак активности;**
- **Дата создания/Изменения.**

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

иконке .

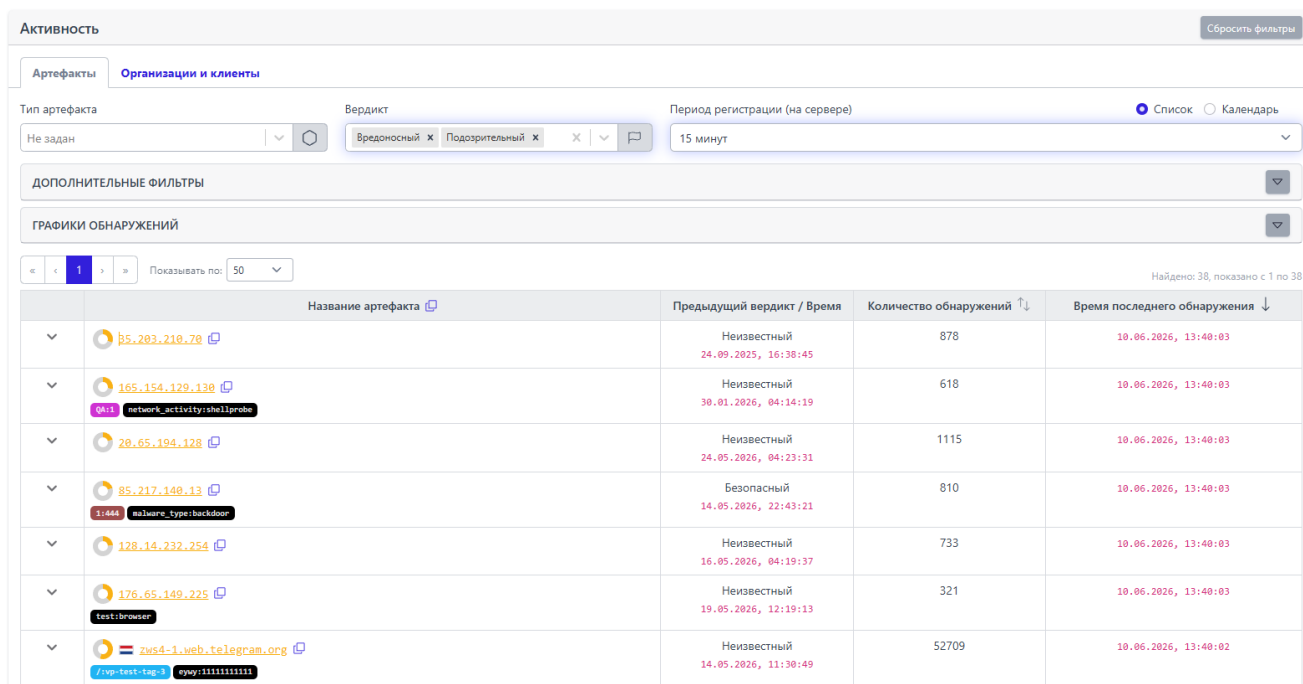
6.4 Активность

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

В верхней части страницы **Активность** имеются следующие вкладки: **Артефакты**, **Организации и клиенты**.

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

Вид страницы **Активность** в зависимости от того, по какой вкладке был произведен вход, показан на рисунках 11 - 12.



Активность				
Артефакты		Организации и клиенты		
Тип артефакта	Вердикт	Период регистрации (на сервере)		
Не задан	Вредоносный x Подозрительный x	15 минут		
ДОПОЛНИТЕЛЬНЫЕ ФИЛЬТРЫ				
ГРАФИКИ ОБНАРУЖЕНИЙ				
Показывать по: 50				
Найдено: 38, показано с 1 по 38				
	Название артефакта	Предыдущий вердикт / Время	Количество обнаружений	Время последнего обнаружения
▼	85.203.210.70	Неизвестный 24.09.2025, 16:38:45	878	10.06.2026, 13:40:03
▼	165.154.129.130 network_activity:shellprobe	Неизвестный 30.01.2026, 04:14:19	618	10.06.2026, 13:40:03
▼	20.65.194.128	Неизвестный 24.05.2026, 04:23:31	1115	10.06.2026, 13:40:03
▼	85.217.140.13 malware_type:backdoor	Безопасный 14.05.2026, 22:43:21	810	10.06.2026, 13:40:03
▼	128.14.232.254	Неизвестный 16.05.2026, 04:19:37	733	10.06.2026, 13:40:03
▼	176.65.149.225 test:browser	Неизвестный 19.05.2026, 12:19:13	321	10.06.2026, 13:40:03
▼	zws4-i.web.telegram.org /wp-test-tag-3	Неизвестный 14.05.2026, 11:30:49	52709	10.06.2026, 13:40:02

Рисунок 11 – Общий вид страницы Активность вкладки Артефакты

Активность

Сбросить фильтры

Артефакты

Организации и клиенты

Тип артефакта

Вердикт

Период регистрации (на сервере)

Список

Календарь

Не задан

Вредоносный

Подозрительный

15 минут

ДОПОЛНИТЕЛЬНЫЕ ФИЛЬТРЫ

Организация

Клиенты

Не задана

Не заданы

ГРАФИКИ ОБНАРУЖЕНИЙ

«

<

1

>

»

Показывать по:

50

Найдено: 42, показано с 1 по 42

Название артефакта	Предыдущий вердикт / Время	Количество обнаружений	Время последнего обнаружения
35.203.210.70 EDR-20		762	10.06.2026, 13:41:10
20.65.194.128 EDR-20	Неизвестный 24.05.2026, 04:23:31	999	10.06.2026, 13:41:10
128.14.232.254 EDR-20	Неизвестный 16.05.2026, 04:19:37	649	10.06.2026, 13:41:10
165.154.129.130 EDR-20		551	10.06.2026, 13:41:10
176.65.149.225 EDR-20	Неизвестный 19.05.2026, 12:19:13	305	10.06.2026, 13:41:10

Рисунок 12 – Общий вид страницы Активность вкладки Организации и клиенты

Таблица имеет следующие поля:

- **Название артефакта** (в данном столбце в зависимости от типа артефакта отображается различная информация: контрольная сумма файла-угрозы в формате SHA-256, IP-адреса, доменные имена, URL);
- **Предыдущий вердикт/Время** (предыдущий вердикт по артефакту и время внесения вердикта);
- **Количество обнаружений** (отображается общее количество обнаружений по данному артефакту);
- **Время последнего обнаружения** (отображается время последнего обнаружения файла с угрозой).

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

- 630ae106a99ae7da5d8dd33e7704b27701f6f – вредоносный артефакт (шрифт красного цвета);
- 02f0c498bb4e5f62722ab5e8a63f5b3779db88ef – безопасный артефакт (шрифт зеленого цвета);
- B73753C4C69A03F9A3E09F121B6599D7781A48E0247F9B71B56572555E1FE12B – неизвестный артефакт (шрифт серого цвета);
- 61F897ED69646E0509F6802F82D7C5E88C3E3893C4CA86942E24D203AA878863 – подозрительный артефакт (шрифт оранжевого цвета).

96.25

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.

Рисунок 13 – Клиенты и организации у которых обнаружен артефакт

Контрольная сумма файла угрозы, а также информация по другим типам артефактов является



Страница отчета программы об угрозе разделена на следующие области:

- 1) область краткой информации об угрозе;
- 2) область вкладок (Основная информация, Анализаторы, Источники данных, Заключение аналитика);
- 3) область основной информации отчета об угрозе;
- 4) область расширенной аналитики (Теги, Связанные сущности, Обнаружения клиентов, Имена файла);

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

В области вкладок отображается вкладка основной информации отчета TI-платформы, вкладки анализаторов и отчетов по артефакту от анализаторов.

В области **Источники данных** отображается отчет от источника данных по артефакту. Если запись отображается серым цветом, то анализ по артефакту в источниках данных не проводился.

Окно основной информации по результатам анализа артефакта в формате JSON представлено на рисунке 15.

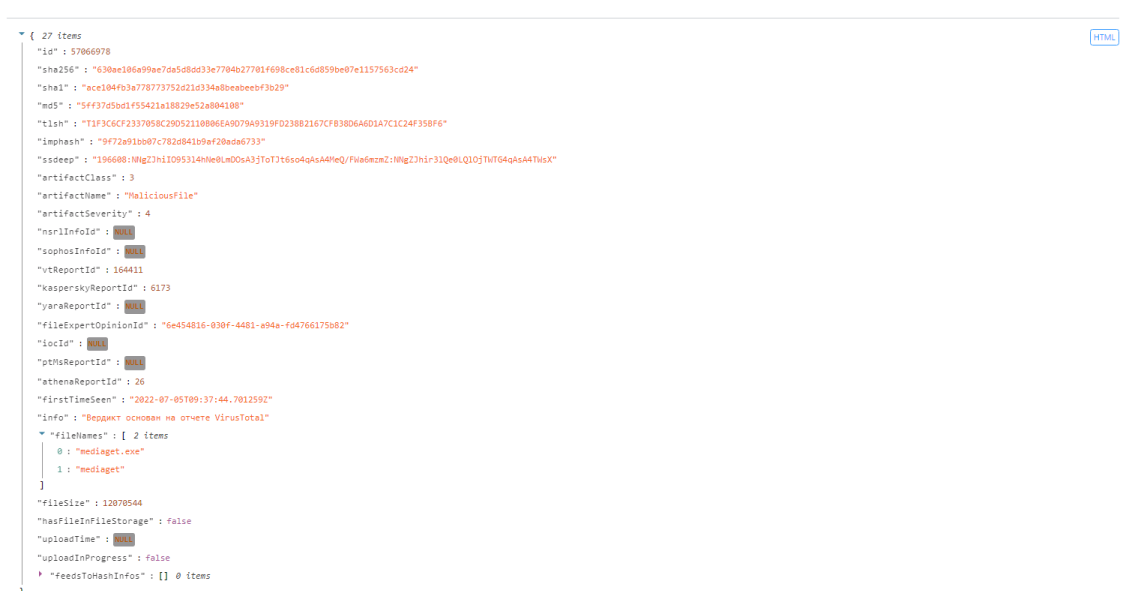


Рисунок 15 – Информация отчета об артефакте в формате JSON

В области **Связанные сущности** показывается таблица с описанием артефакта, связанного с тем артефактом, отчет по которому просматривается на данный момент.

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

- **Тип артефакта** (файл, IP-адрес, доменное имя, URL);
- **Вердикт** (неизвестный, безопасный, вредоносный, подозрительный);
- **Период регистрации (на сервере)**, может задаваться в виде списка (15 минут, 1 час, 8 часов, 1 день, 1 неделя, 1 месяц, 3 месяца), либо в виде календаря (начальная и конечная даты);

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

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

- **Артефакт** (в данном фильтре можно указать любой артефакт: IP-адрес, доменное имя и т.д.);
- **Количество обнаружений не менее** (фильтрация по количеству обнаружений, не менее указанного в фильтре);
- **Количество обнаружений не более** (фильтрация по количеству обнаружений, не более указанного в фильтре);
- **Предыдущий вердикт**;
- **Время последнего изменения вердикта**;
- **Вердикт**.

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

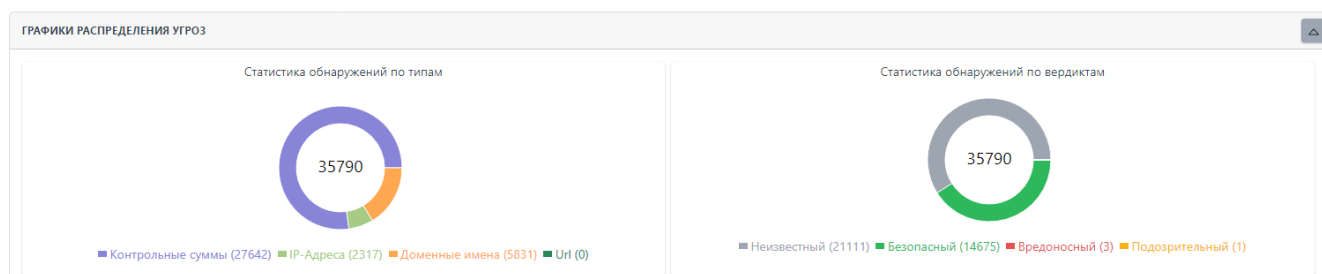


Рисунок 16 – Область графического отображения информации по обнаруженным угрозам вкладка «Артефакты»

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** вкладки **Организации и клиенты** 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);
- **Организация**;
- **Клиенты**.

А также имеется система дополнительных фильтров аналогичных фильтрам, представленным выше.

На странице **Активность** вкладки **Организации и клиенты** имеется область с графическим отображением информации по обнаруженным угрозам (рисунок 17).

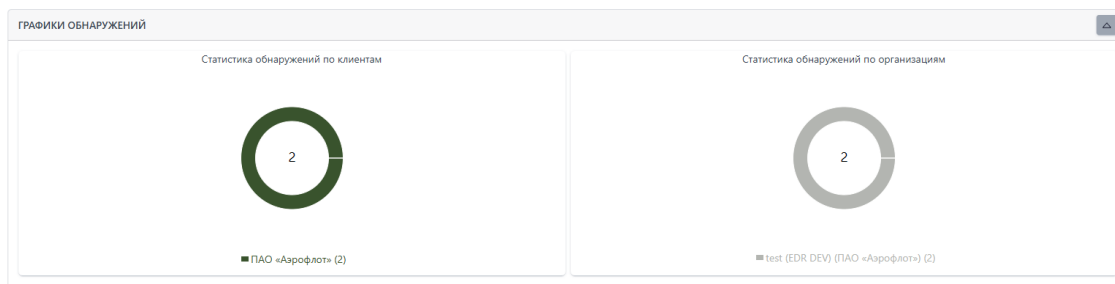


Рисунок 17 – Область графического отображения информации по обнаруженным угрозам вкладки Организации и клиенты

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

- статистика обнаружений по организациям;
- статистика обнаружений по клиентам.

6.5 Заявки

Страница Заявки представлена на рисунке 18.

Артефакт	Тип артефакта	Статус	Вердикт	Комментарий	Дата создания / Автор	Дата обновления / Пользователь
test1.ru	URL	Активна	Безопасный	какая	11.01.2026, 13:54:18 testSP@rt.ru RT-Информационная безопасность	
test1.ru	URL	Активна	Подозрительный	для теста 111	10.01.2026, 13:43:52 QA.tuser@gmail.com тестовая 1	
289vixi.mdu.ic	URL	Активна	Подозрительный	для теста 111	10.01.2026, 13:43:52 QA.tuser@gmail.com тестовая 1	
182.12.18.188	IP	Активна	Подозрительный	для теста 111	10.01.2026, 13:43:52 QA.tuser@gmail.com тестовая 1	
86.69.72.165	IP	Активна	Подозрительный	для теста 111	10.01.2026, 13:43:52 QA.tuser@gmail.com тестовая 1	
229.198.162.58	IP	Активна	Подозрительный	для теста 111	10.01.2026, 13:43:52 QA.tuser@gmail.com тестовая 1	
e0213b0c45181c23a28c8b7f7c408c138f5c7af46c1a4b170a1	File	Активна	Подозрительный	для теста 111	10.01.2026, 13:43:52 QA.tuser@gmail.com тестовая 1	
webmonocross@msk1.com	Domain	Активна	Подозрительный	для теста 111	10.01.2026, 13:43:48 QA.tanalyst@gmail.com тестовая 1	
https://holshol.ru/viss1/revalla-eroderki-kilator	URL	Активна	Подозрительный	для теста 111	10.01.2026, 13:43:48 QA.tanalyst@gmail.com тестовая 1	
test1.ru	URL	Активна	Подозрительный	для теста 111	10.01.2026, 13:43:48 QA.tanalyst@gmail.com тестовая 1	

Рисунок 18 – Страница Заявки

На данной странице пользователь может просмотреть список заявок на корректировку вердикта по артефактам.

Удаление и корректировка заявки возможна только администратором организации, создавшим заявку, либо пользователем, создавшим заявку.

Для фильтрации информации на странице предусмотрена система фильтров, представленная в следующем списке:

- Артефакт;
- Статус;
- Вердикт;
- Комментарий;
- Временной период.

6.6 Анализаторы

Анализаторы представляют собой функционал для расширения возможностей анализа артефактов с помощью программы RT Protect TI.

Процедура создания анализаторов описывается в отдельном документе.

В общем случае можно сказать, что сущность анализаторов это сложно структурированный созданный инструмент по анализу артефактов, на основе заданных при написании анализатора правил.

Общий вид страницы «Анализаторы» зависит от выбранной активной вкладки.

Общий вид страницы «Анализаторы» вкладки «Активные интеграции» представлен на рисунке 19.

Анализаторы

Сбросить фильтры

Активные интеграции

Отчеты

Название

Введите значение

Типы артефактов

Не задан

Признак активации

Не задано

«

1

2

»

Показывать по: 10

Найдено: 14, показано с 1 по 10

	Название	Приоритет	Описание	Типы артефактов
▼		« 0 0 0 0	Тестовый анализатор Analyser_QA_domain	
▼		« 0 0 0 0	Тестовый анализатор Analyser_QA_email	
▼		« 0 0 0 0	Тестовый анализатор Analyser_QA_file	
▼		« 0 0 0 0	Тестовый анализатор Analyser_QA_ip	
▼		« 0 0 0 0	Тестовый анализатор Analyser_QA_url	
▼	Fuzzy family2	« 0 0 0 0	333 меню описание	
▼		« 0 0 0 0	321	
▼	Netlas	« 0 0 0 0	Получает отчеты Netlas по артефактам	
▼		« 0 0 0 0	Получает отчеты RST Cloud по артефактам	
▼	Static File	« 0 0 0 0	Осуществляет подсчет контрольных сумм (в том числе fuzzy-хэшей) для загружаемых в хранилище TI файлов	

«

1

2

»

Показывать по: 10

Найдено: 14, показано с 1 по 10

Рисунок 19 – Общий вид страницы Анализаторы вкладки Активные интеграции

Информация на странице представлена в виде таблицы со следующими полями:

- Иконка для раскрытия информации по анализатору ();
- Название анализатора;
- Приоритет;
- Описание;
- Типы артефактов.

В поле «Типы артефактов» в виде иконок отображаются типы артефактов, проверяемые данным анализатором.

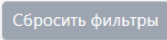
Имеются следующие иконки для обозначения типов артефактов:

-  (Email);
-  (Файл);
-  (Домен);
-  (IP адрес);
-  (URL).

Для фильтрации информации на странице имеются следующие фильтры:

- Название;
- Признак активации (не задано, активировано, не активировано);
- Типы артефактов (Файл, IP-Адрес, доменное имя, URL, Email).

На странице «Анализаторы» имеются следующие иконки:

-  (при нажатии сбрасываются выставленные фильтры на странице);

При нажатии по иконке, раскрывающей информацию по анализатору, открывается окно, представленное на рисунке 20.

^			Тестовый анализатор Analyser_QA_file	
Максимальное время анализа артефакта (в минутах)		3		
Для работы анализатора требуется загруженный файл		Нет		
Время актуальности получаемых отчетов (в днях)		1		
Автоматически запрашивать отчет по артефакту при открытии		Да		
Название группы псевдонимов		test_group2		
Дата создания		30.04.2025, 15:01:33		
Последнее изменение / Пользователь		07.05.2025, 18:37:54 / QAadmin@gmail.com		

Рисунок 20 – Информация по анализатору

В разделе «Анализаторы» вкладки «Отчеты» в табличной форме представлена информация о проверенных анализаторами артефактах.

Общий вид страницы представлен на рисунке 21.

Артефакт	Анализатор	Статус	Вердикт анализатора	Время обращения	Действия
10f11b7b3c49f76db40f2b7c1d5454177528137b-0e75cc751886c134d85	YARA	✓	100	12.09.2025, 12:00:13	Отчет
10f11b7b3c49f76db40f2b7c1d5454177528137b-0e75cc751886c134d85	YARA	✓	50	12.09.2025, 12:00:05	Отчет
00a88e275c7248819b7b7864723a5d5b88f3a318a44ba29f4f4c3a5743c	YARA	✓	50	12.09.2025, 12:00:05	Отчет
132_56_67_89	YARA	✓	100	12.09.2025, 12:00:28	Отчет
132_56_67_89	YARA	✓	100	12.09.2025, 12:00:28	Отчет
132_56_67_89	YARA	✓	100	12.09.2025, 12:00:28	Отчет
132_56_67_89	YARA	✓	50	12.09.2025, 12:00:34	Отчет
825174429e406b3a818115db6c9a9a7b5248480c1b15f5b1c9c9a93bdc12d	YARA	✓	50	12.09.2025, 12:00:14	Отчет
825174429e406b3a818115db6c9a9a7b5248480c1b15f5b1c9c9a93bdc12d	YARA	✓	50	12.09.2025, 12:00:14	Отчет
887c5933f0e1431349b78a3a14370dd18a5d411808f64c13c2a88d6f12d5	YARA	✓	50	12.09.2025, 12:00:25	Отчет
2081c8845a318a2c372b7734	YARA	✓	100	12.09.2025, 12:01:00	Отчет

Рисунок 21 – 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);
- **Анализатор** (в столбце отображается анализатор, которым был проверен артефакт);
- **Статус** (в столбце отображается информация о получении отчета (отчет получен успешно, отчет не был получен, отчет находится в очереди));
- **Вердикт отчета** (отображается вердикт по артефакту, полученный от анализатора, например , означает что артефакт безопасен на 100 %);
- **Время обращения** (время, в которое был запрошен отчет);
- **Действия** (отображается иконка для просмотра информации по отчету анализатора).

Статус отчета от анализатора отображается следующими иконками:

—  отчет по артефакту получен с ошибками (краткое описание ошибок приведено во всплывающем окне при наведении на иконку указателя мыши);

—  отчет не получен, превышено время ожидания ответа в очереди;

—  отчет не был получен (при наведении на иконку выводится статус и код ошибки);

—  отчет получен успешно.

Информация об артефакте отображается разными цветами:

— шрифт красного цвета (артефакт является вредоносным);

— шрифт зеленого цвета (артефакт является безопасным);

— шрифт серого цвета (неизвестный артефакт);

— шрифт оранжевого цвета (артефакт является подозрительным).

Над таблицей для фильтрации информации имеются следующие фильтры:

— **Анализатор** (Название анализатора);

— **Тип артефакта**;

— **Дата создания**;

— **Вердикт отчета** (Минимальное/Максимальное значения вердикта в границах от -100 (артефакт полностью безопасен), до 100 (артефакт полностью вредоносен);

— **Актуальность** (не задано, актуальный, не актуальный);

— **Признак ошибки** (не задано, не установлен, установлен).

Для просмотра отчета по артефакту нужно нажать по иконке .

Страница отчета анализатора по артефакту представлена на рисунке 22.

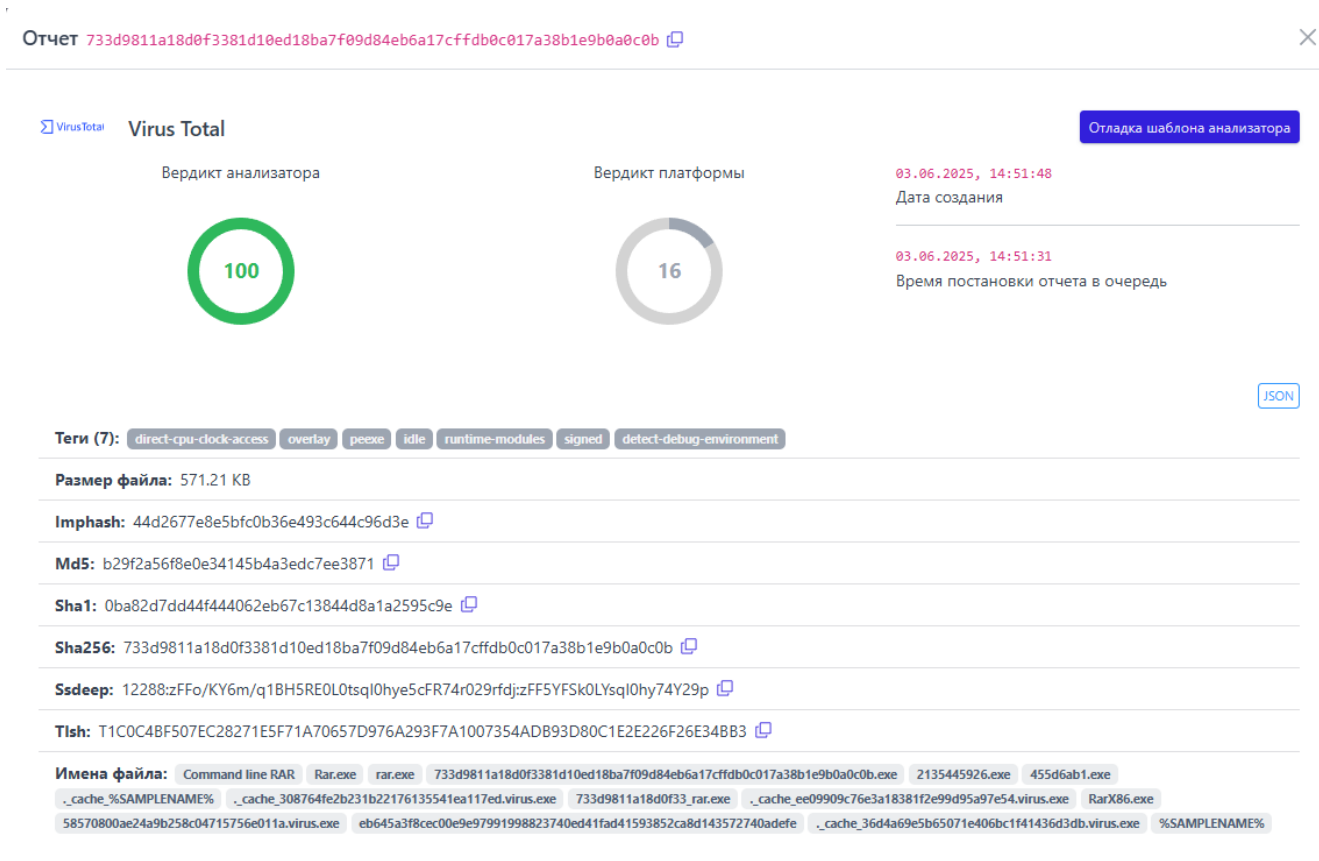


Рисунок 22 – Страница отчета по артефакту

6.7 Граф связей

Страница **Граф связей** с незаполненным полем артефакта представлена на рисунке 23.

Граф связей

Артефакт *

Введите артефакт

Показать граф

Рисунок 23 – Общий вид пустой страницы «Граф связей»

После внесения в поле «Артефакт» артефакта и нажатия по кнопке «Показать граф» откроется окно графа, показанное на рисунке 24.

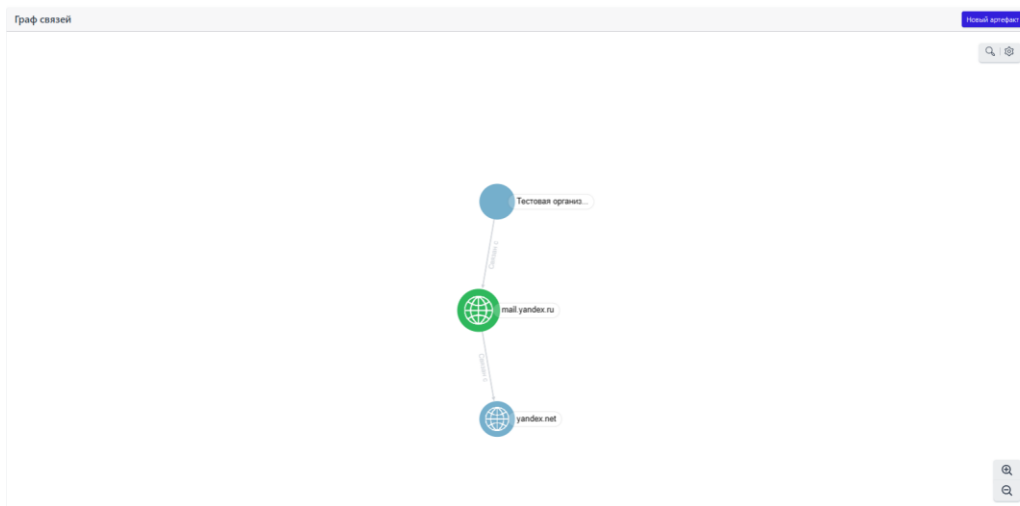


Рисунок 24 – Граф связей

В правой части окна имеются иконки для управления размером отображения графа  , и иконка  , и иконка  для возможности изменения параметров .

При нажатии по иконке изменения параметров открывается окно, представленное на рисунке 25.

Рисунок 25 – Изменение параметров отображения графа

В данном окне можно ввести артефакт, отображенный на графе изменить глубину отображения элементов (от 1 до 9), и удалить элементы и типы связей, отображенных на графе.

В основной области графа, центральным элементом показан артефакт, который был введен в поле построения графа, а от него со связями показаны артефакты, связанные с основным.

При нажатии ЛКМ на артефакт, в окне графа появиться таблица с информацией о узле представленная на рисунке 26.

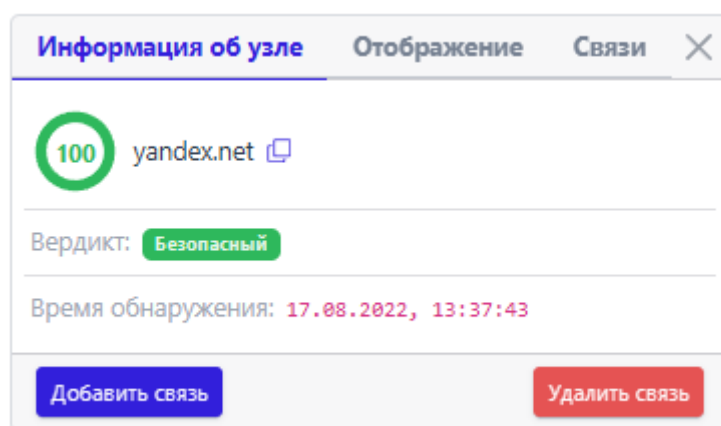


Рисунок 26 – Информация о узле

В данном окне представлены вкладки с информацией о узле.

Во вкладке **Отображение** (в данной вкладке представлены различные связи узла) можно нажав по иконке  добавить на граф связи узла с различными артефактами, а так же организациями и т.п.

С помощью различных иконок можно удалить или добавить связь. Удалить связь можно также на самом графе, наведя указатель мыши на связь, после чего откроется окно подтверждения действия по удалению. Если связь невозможно удалить, то появляется соответствующее сообщение. Связь невозможно удалить если она создана не пользователем, а автоматически.

При изменении глубины графа при нажатии на артефакт на графе отображаются связи согласно выставленного параметра (см. рисунок 27).

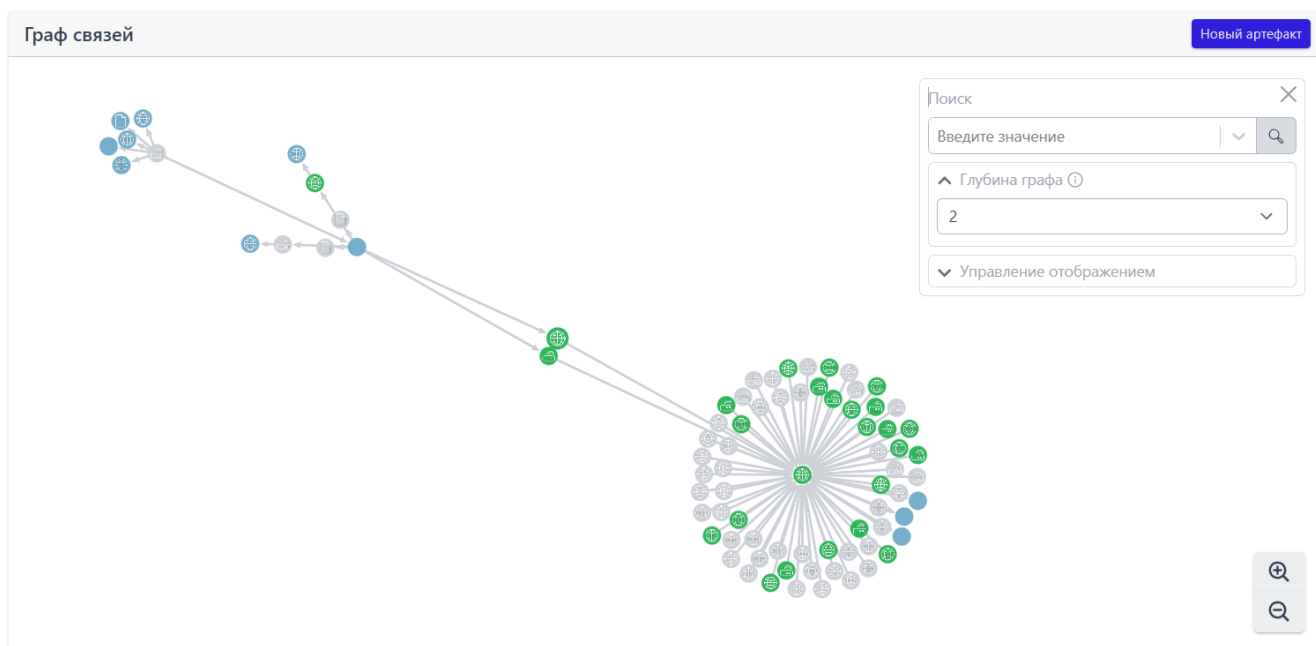


Рисунок 27 – Связи при выставленной глубине графа 2

Следует отметить что установка глубины графа более 2 затрудняет его построение и осложняет визуализацию.

6.8 Угрозы и злоумышленники

На странице угрозы и злоумышленники пользователь может просматривать информацию по злоумышленникам и угрозам (рисунок 28).

Имя	Источник данных	Страна	Страны-жертвы
test	Не задан	Не задан	Не задан
TEST_QA1	Не задан	Не задан	Не задан
APT34	Не задан	Не задан	Не задан

Рисунок 28 – Общий вид страницы Угрозы и злоумышленники

Нажав по иконке  можно перейти на страницу с описанием конкретного злоумышленника.

Так же на странице можно просмотреть граф связей артефактов из статей.

6.9 Вредоносное ПО

На странице «Вредоносное ПО» в виде таблицы представлен перечень вредоносного ПО (рисунок 29).

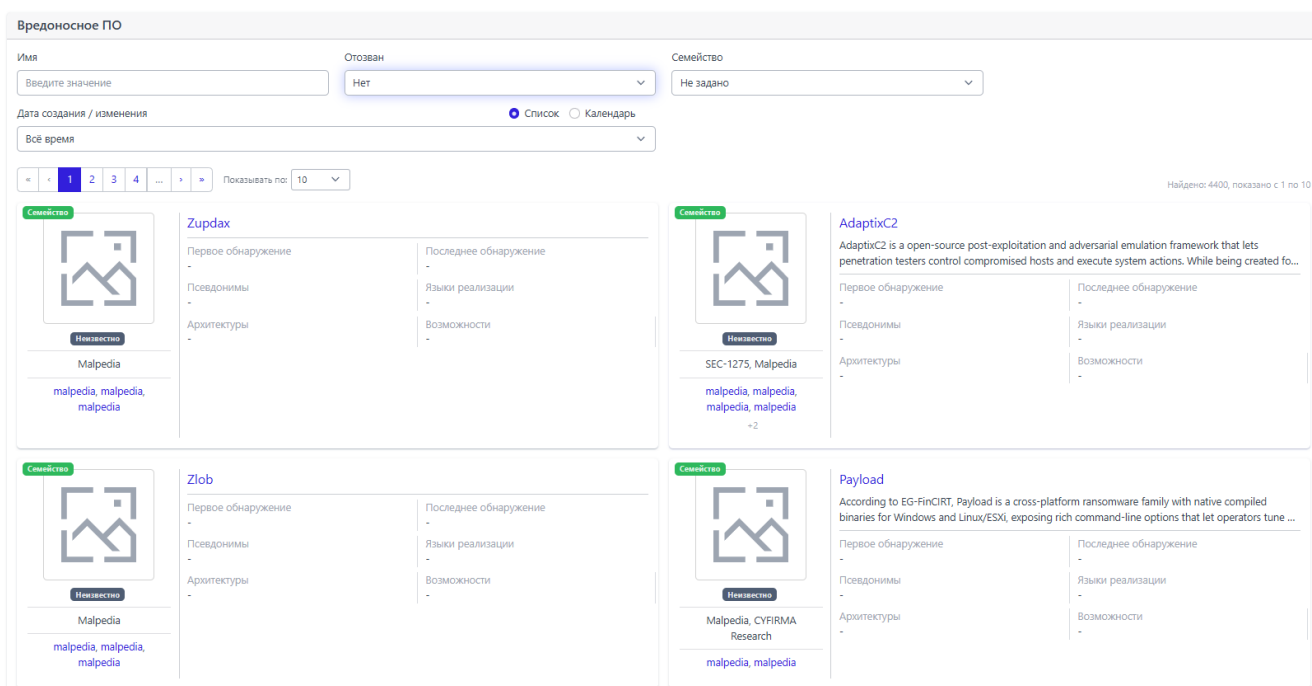


Рисунок 29 – Страница Вредоносное ПО

Информация о вредоносном ПО пополняется из источников данных типа STIX, а также, может быть добавлена вручную (данное действие доступно для администраторов владельцев платформы).

Для фильтрации информации на странице предусмотрена система фильтров, представленная в следующем списке:

- Имя;
- Отозван;
- Семейство (Не задано, Семейство, Экземпляр);
- Дата создания/Изменения (Все время, 15 минут, 1 час, 8 часов, 1 день, 1 неделя, 1 месяц, 3 месяца);

При нажатии по иконке имени вредоносного ПО (выделено синим шрифтом), открывается информация о вредоносном ПО, а также связанные сущности и граф связей.

При нажатии по имени вредоносного инструмента, которое выделено синим цветом, открывается окно с информацией о ПО.

На данной странице можно просмотреть связанные сущности и граф связей.

6.10 Инструменты

На странице «Инструменты» показана информация по вредоносным инструментам, используемым злоумышленниками при проведении вредоносных действий.

Общий вид страницы представлен на рисунке 30.

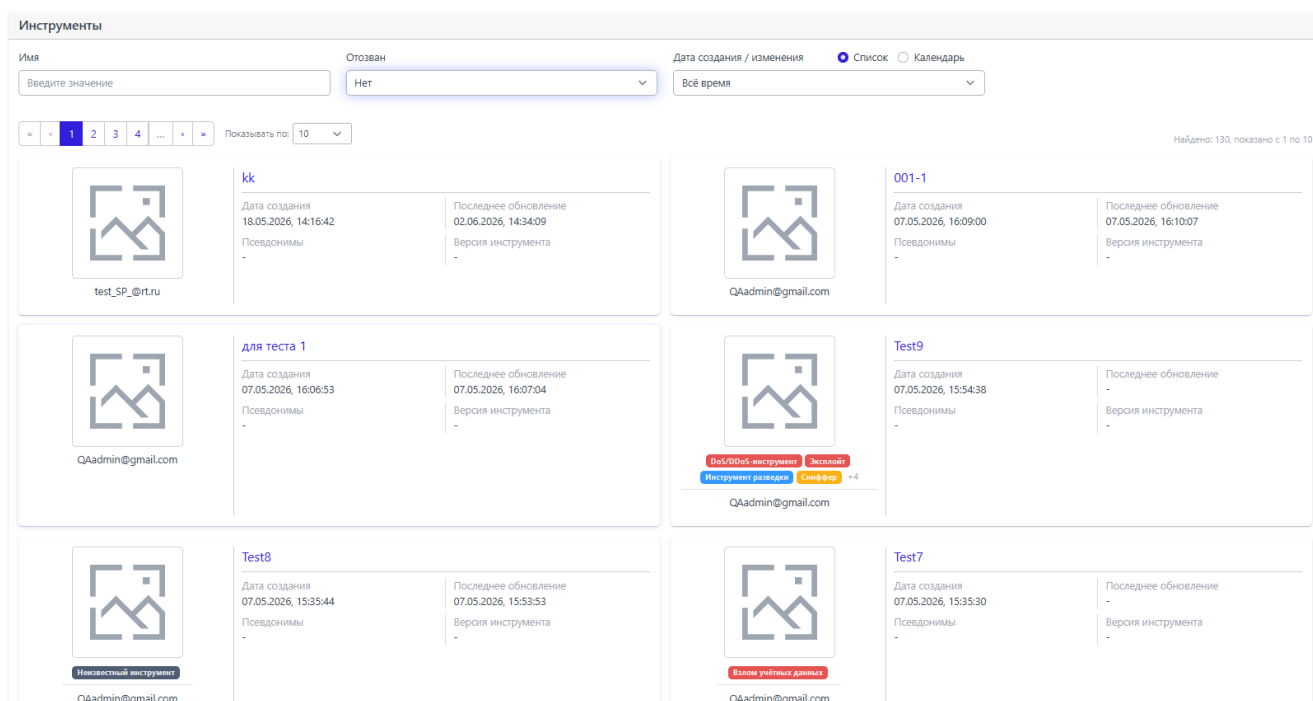


Рисунок 30 – Общий вид страницы «Инструменты»

Информация о вредоносных инструментах пополняется из источников данных типа STIX, а также, может быть добавлена вручную (данное действие доступно для администраторов владельцев платформы).

Для фильтрации информации имеется система фильтров, представленная в следующем списке:

- Имя;
- Отозван;
- Дата создания/изменения;

При наведении указателя мыши на иконку с именем инструмента и нажатии ЛКМ, открывается окно с расширенной информацией, где есть так же возможность просмотреть связанные с инструментом сущности, и просмотреть граф связей.

6.11 Матрица MITRE ATT&CK

На рисунке 31 представлен общий вид страницы Матрица MITRE ATT&CK. На данной странице приведено описание техник Mitre описывающих различные вредоносные действия. Аналитик и администратор для удобства описания и понимания вредоносных техник упоминающихся в отчетах может обратиться к странице.

Поиск

Поиск по названию или ID техники...

Reconnaissance	12	Resource Development	9	Initial Access	11	Execution	24	Persistence	25	Privilege Escalation	14	Stealth	33
T1589 Gather Victim Identity L...	1	T1583 Acquire Infrastructure	1	T1078 Valid Accounts	4	T1047 Windows Management Inst...		T1034 Path Interception		T1034 Path Interception		T1006 Direct Volume Access	
T1590 Gather Victim Network...	1	T1584 Compromise Infrastruct...	1	T1091 Replication Through Remov...		T1053 Scheduled Task/Job	1	T1037 Boot or Logon Initializat...	1	T1037 Boot or Logon Initializat...	1	T1014 Rootkit	
T1591 Gather Victim Org Infor...	1	T1585 Establish Accounts	1	T1133 External Remote Services		T1059 Command and Scriptin...	11	T1053 Scheduled Task/Job	1	T1053 Scheduled Task/Job	1	T1027 Obfuscated Files or Inf...	11
T1592 Gather Victim Host Info...	1	T1586 Compromise Accounts	1	T1189 Drive-by Compromise		T1061 Graphical User Interface		T1062 Hypervisor		T1055 Process Injection	11	T1036 Masquerading	11
T1593 Search Open Websites/...	1	T1587 Develop Capabilities	1	T1190 Exploit Public-Facing Applic...		T1064 Scripting		T1078 Valid Accounts	1	T1068 Exploitation for Privilege Es...		T1055 Process Injection	11
T1594 Search Victim-Owned Webs...		T1588 Obtain Capabilities	1	T1195 Supply Chain Comprom...	1	T1072 Software Deployment Tools		T1098 Account Manipulation	1	T1078 Valid Accounts	1	T1064 Scripting	
T1595 Active Scanning	1	T1608 Stage Capabilities	1	T1199 Trusted Relationship		T1106 Native API		T1108 Redundant Access		T1098 Account Manipulation	1	T1070 Indicator Removal	1
T1596 Search Open Technical ...	1	T1650 Acquire Access		T1200 Hardware Additions		T1127 Trusted Developer Utilit...	1	T1112 Modify Registry		T1134 Access Token Manipulat...	1	T1078 Valid Accounts	1
T1597 Search Closed Sources	1	T1683 Generate Content	1	T1566 Phishing	1	T1129 Shared Modules		T1133 External Remote Services		T1484 Domain or Tenant Polic...	1	T1108 Redundant Access	
T1598 Phishing for Information	1			T1659 Content Injection		T1153 Source		T1136 Create Account	1	T1543 Create or Modify Syste...	1	T1127 Trusted Developer Utilit...	1
T1681 Search Threat Vendor Data				T1669 Wi-Fi Networks		T1175 Component Object Model a...		T1137 Office Application Start...	1	T1546 Event Triggered Execut...	11	T1134 Access Token Manipulat...	1
T1682 Query Public AI Services						T1197 BITS Jobs		T1176 Software Extensions	1	T1547 Boot or Logon Autosta...	14	T1140 Deobfuscate/Decode Files ...	
						T1203 Exploitation for Client Execu...		T1197 BITS Jobs		T1548 Abuse Elevation Control...	1	T1149 LC_MAIN Hijacking	
						T1204 User Execution	1	T1205 Traffic Signaling	1	T1611 Escape to Host		T1197 BITS Jobs	
						T1559 Inter-Process Communi...	1	T1505 Server Software Compo...	1			T1202 Indirect Command Execution	
						T1569 System Services	1	T1525 Implant Internal Image				T1205 Traffic Signaling	1
						T1574 Hijack Execution Flow	11	T1542 Pre-OS Boot	1			T1211 Exploitation for Stealth	
						T1609 Container Administration C...		T1543 Create or Modify Syste...	1			T1216 System Script Proxy Exe...	1
						T1610 Deploy Container		T1546 Event Triggered Execut...	11			T1218 System Binary Proxy Ex...	11
						T1648 Serverless Execution		T1547 Boot or Logon Autosta...	11			T1220 XSL Script Processing	
						T1651 Cloud Administration Com...		T1554 Compromise Host Software...				T1221 Template Injection	
						T1674 Input Injection		T1556 Modify Authentication ...	1			T1480 Execution Guardrails	1

Рисунок 31 – Общий вид страницы Матрица MITRE ATT&CK

6.12 Лента угроз

На данной странице представлены статьи, касающиеся информационной безопасности, в которых имеются упоминания об угрозах и вредоносных артефактах.

Информация на странице представлена в виде списка статей с кратким описанием.

Статьи получены из различных источников.

Для фильтрации информации на странице имеется система фильтров, представленная в следующем списке:

- Название;
- Отозван;
- Информация получена из ИИ;
- Артефакт;
- Уязвимость;
- Источник;
- Тип отчета (не задано, отчет об угрозе, другое).
- Дата создания/Изменения.

Общий вид страницы **Лента угроз** представлен на рисунке 32.

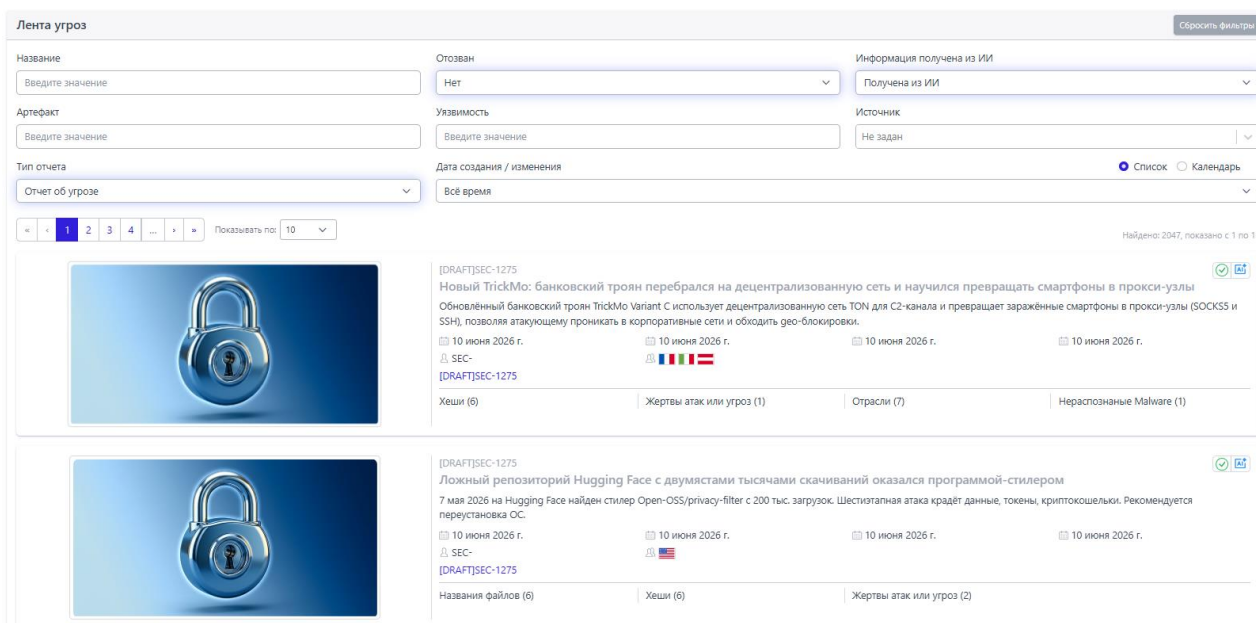


Рисунок 32 – Общий вид страницы Лента угроз

При нажатии по имени статьи ЛКМ откроется страница с более подробной информацией о статье и об артефактах, которые упоминаются в статье (рисунок 33).

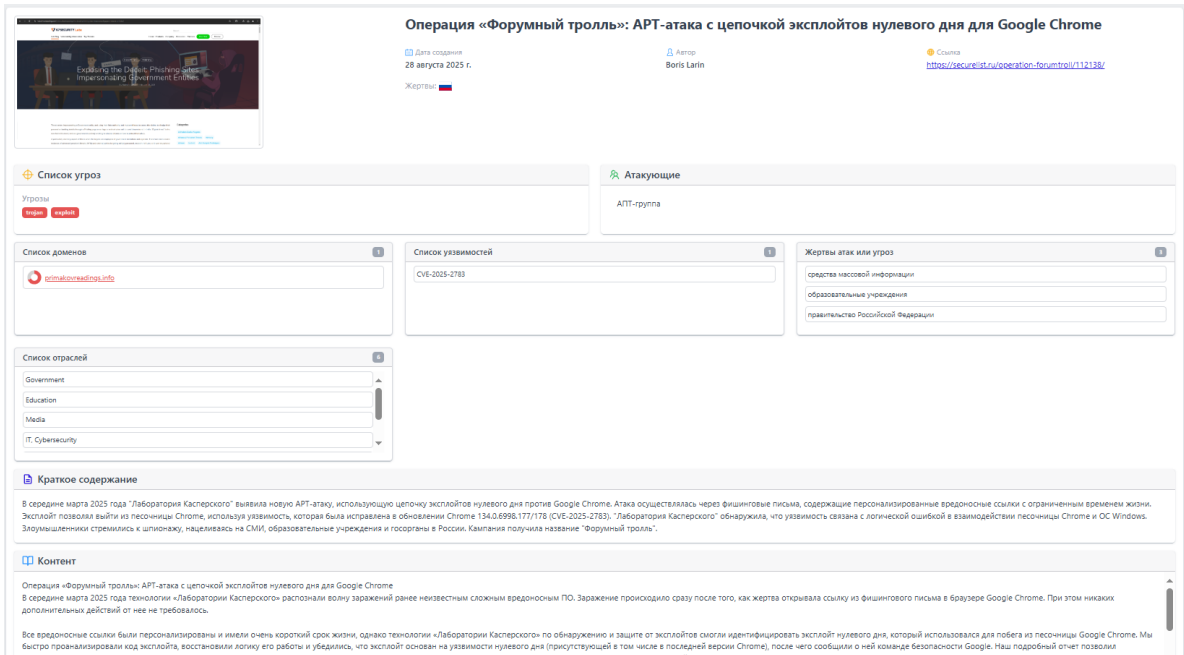


Рисунок 33 – Подробная информация о статье

На странице отображается информация из статьи, а также, угрозы упоминающиеся в статье, например, найденные вредоносные артефакты.

В нижней части окна отображается область с графом связей артефактов.

6.13 Уязвимости

Общий вид страницы «Уязвимости» представлен на рисунке 34.

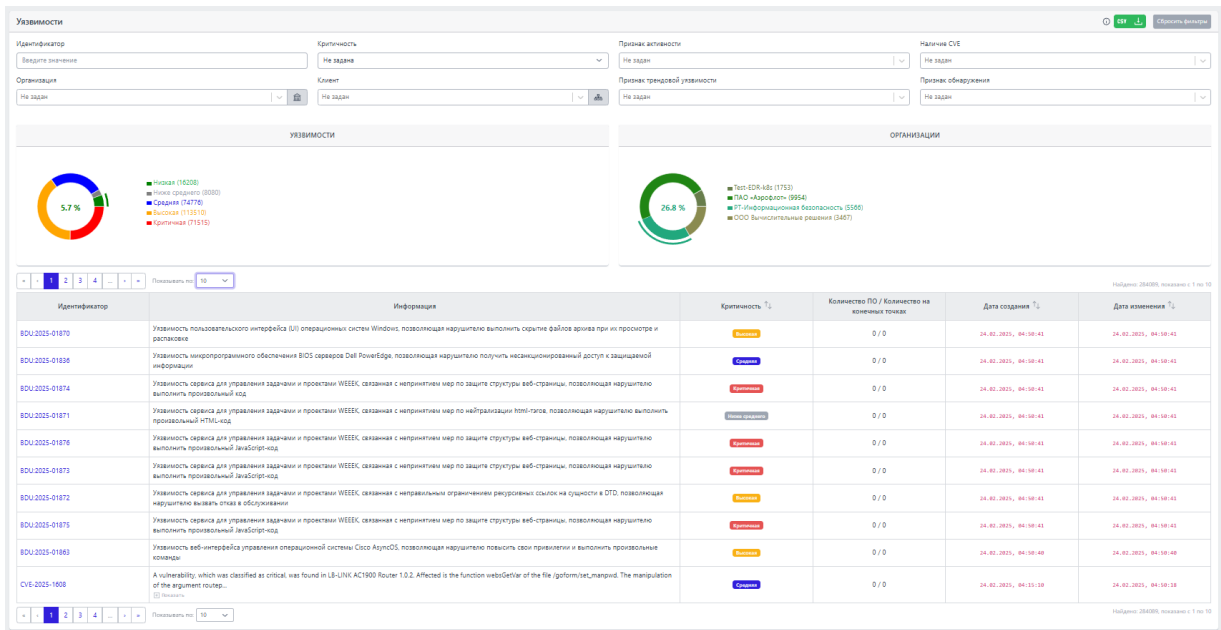


Рисунок 34 – Страница Уязвимости

На данной странице в виде таблицы представлена информация по найденным уязвимостям.

Таблица имеет следующие поля:

- Идентификатор (идентификация уязвимости по CVE);
- Информация (описание уязвимости);
- Критичность уязвимости;
- Количество ПО/Количество на конечных точках (в таблице отображается количество программ, в которых найдена данная уязвимость и количество конечных точек, на которых зарегистрировано ПО с данной уязвимостью);
- Дата создания;
- Дата изменения.

Для фильтрации информации в таблице имеются следующие фильтры:

- Идентификатор (в фильтре указывается идентификатор уязвимости в формате CVE);
- Критичность (не менее) (низкая, средняя, высокая, критичная);
- Признак активности (активирована, деактивирована);

- Наличие CVE (имеется, отсутствует);
- Организация;
- Клиент;
- Признак трендовой уязвимости (обычная уязвимость, трендовая уязвимость);
- Признак обнаружения (не обнаружено, обнаружено).

В столбце **Идентификатор** трендовая уязвимость отмечена иконкой . Признак выставляется аналитиком/администратором на основании анализа информации об уязвимости.

При нажатии в столбце **Идентификатор** по CVE-идентификатору уязвимости открывается информация об уязвимости, представленная на рисунке 35.

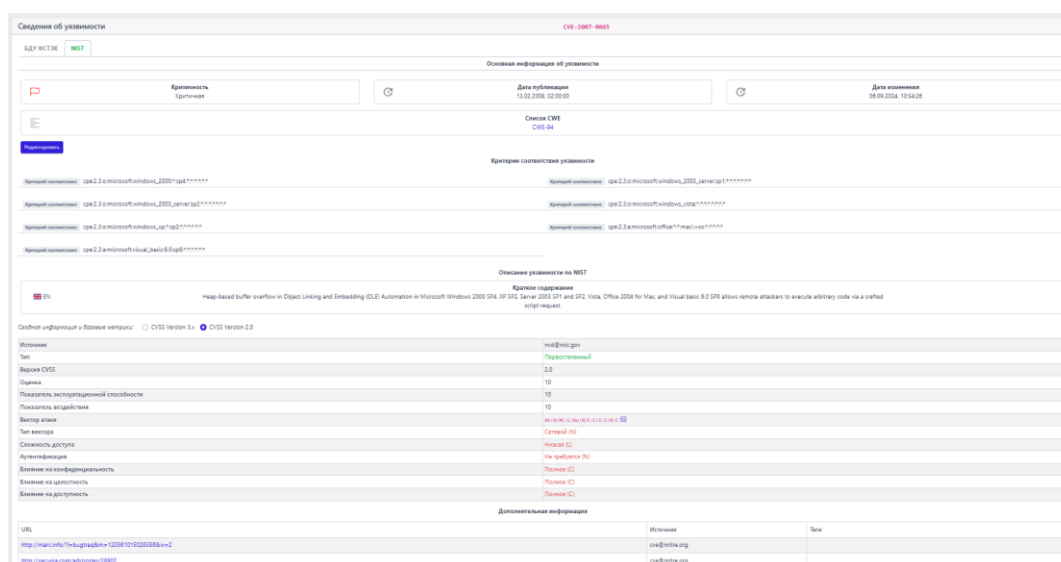


Рисунок 35 – Информация по уязвимости

На данной странице информация по уязвимости представлена в двух вкладках БДУ ФСТЭК и NIST.

Также по уязвимости можно просмотреть информацию по описанию CVE, перейдя по активной ссылке, подсвеченной синим цветом ([Список CVE: CVE-259](#)).

Данная ссылка находится в поле рядом с полем, где указывается дата публикации и изменения информации по уязвимости.

На странице «Уязвимости» имеется графическая область с отображением найденных уязвимостей по категории критичности, а также организации в которых были выявлены уязвимости. Данная область представлена на рисунке 36.

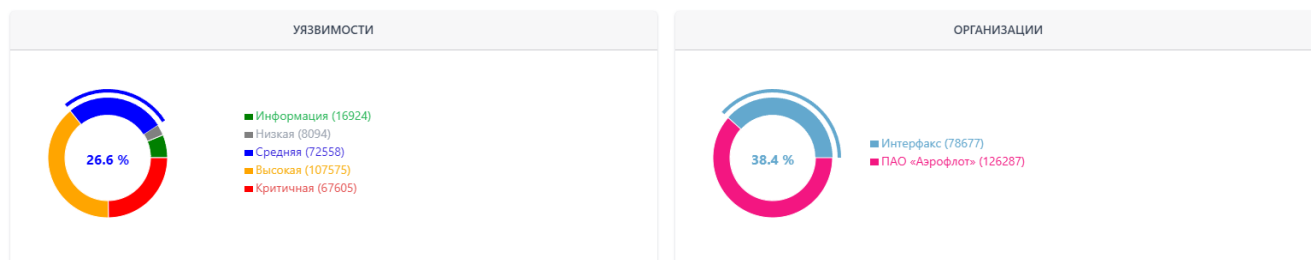


Рисунок 36 – Область с графическим отображением уязвимостей по критичности и организациям в которых обнаружены уязвимости

В области «Уязвимости» при нажатии на уровни критичности найденных уязвимостей, например **■ Средняя (72558)**, в таблице найденных уязвимостей будут отображаться уязвимости с уровнем критичности **Средняя** и выше.

В области «Организации» при нажатии по имени организации будут отображаться уязвимости, которые обнаружены только в программах, установленных в данной организации.

При нажатии по иконке  пользователь загружает на компьютер, с которого осуществлен вход в модуль администрирования RT Protect TI, информацию о всех найденных уязвимостях в организации в Excel формате.

6.14 Программы

Страница Программы при выключенном режиме агрегации

( Режим агрегации ) представлена на рисунке 37.

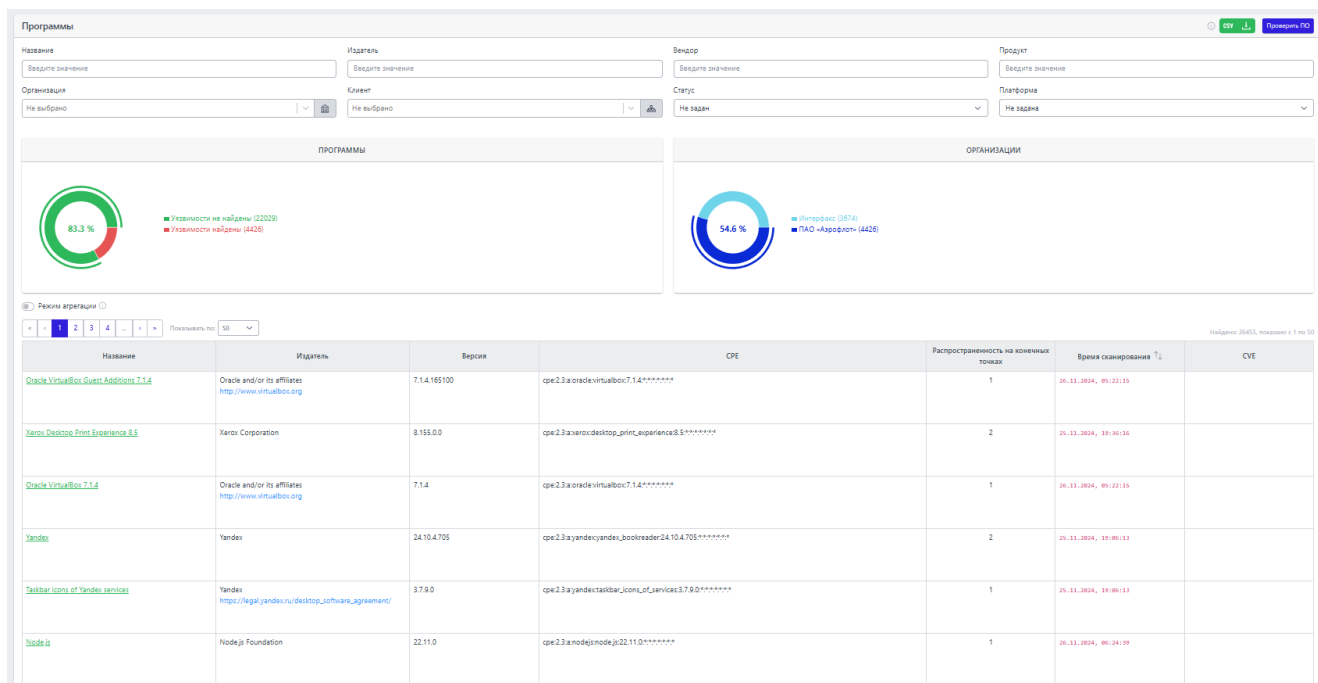


Рисунок 37 – Страница Программы при выключенном режиме агрегации

На странице в табличной форме представлена информация о программах, которые проанализированы на предмет уязвимостей.

Таблица имеет следующие поля:

- Название (указывается название программы);
- Издатель;
- Версия;
- CPE (описание программ по стандарту для машиночитаемого именования и идентификации всех видов программного обеспечения (софта) и устройств);
- Распространенность на конечных точках;
- Время сканирования;
- CVE (описание уязвимостей, найденных для программы в формате CVE с указанием критичности).

В таблице для удобного представления и быстрого анализа названия программ выделены различными цветами:

- Программы, в которых имеются уязвимости (шрифт красного цвета, например, **Microsoft Edge**);
- Программы, в которых отсутствуют уязвимости (шрифт зеленого цвета, например, **Windows SDK**).

Для фильтрации информации на странице используются следующие фильтры:

- **Название** (в области фильтра задается имя программы);
- **Издатель**;
- **Вендор**;
- **Продукт**;
- **Организация**;
- **Клиент**;
- **Статус** (не задан, уязвимости не найдены, уязвимости найдены, в процессе анализа, ошибка при формировании CPE, ошибка при сканировании);
- **Платформа**.

При нажатии по иконке с названием программы происходит переход на страницу сведений о программе, представленную на рисунке 38.

Мozilla Firefox (x64 en-US)

НАЗВАНИЕ

mozilla

ПРОИЗВОДИТЕЛЬ ПРОДУКТА

https://www.mozilla.org

URL

cpe2.3:mozilla:firefox:128.0:*:*en*...

CPE

firefox

НАЗВАНИЕ ПРОДУКТА

Microsoft Windows 11 Pro - 64 bit

ОПЕРАЦИОННАЯ СИСТЕМА

Вредоносный

СТАТУС ПРОВЕРКИ ПО НА УЯЗВИМОСТИ

07.09.2024, 05:14:52

ВРЕМЯ СКАНИРОВАНИЯ

Mozilla

ИЗДАТЕЛЬ

128.0

ВЕРСИЯ

T

а

ТИП ПО

02.09.2024, 14:46:33

ВРЕМЯ ОБНОВЛЕНИЯ

Обнаруженные уязвимости

1

2

3

4

Показывать по 10

CVE	Соответствие	Дата создания	Дата обновления	CWE
CVE-2024-7521	Критичный соответствием: cpe2.3:mozilla:firefox:***** Отсутствует в уязвимой и последующих версиях: 129.0	06.09.2024, 01:00:00	06.09.2024, 11:00:10	CWE-755, CWE-416
CVE-2024-7528	Критичный соответствием: cpe2.3:mozilla:firefox:***** Отсутствует в уязвимой и последующих версиях: 129.0	06.09.2024, 01:00:00	06.09.2024, 11:00:10	CWE-416
CVE-2024-1492	Критичный соответствием: cpe2.3:mozilla:firefox:*****	11.12.2023, 00:00:00	06.09.2024, 10:51:57	CWE-59
CVE-2024-43113	Критичный соответствием: cpe2.3:mozilla:firefox:*****iphone_* Отсутствует в уязвимой и последующих версиях: 129	06.09.2024, 10:13:49	06.09.2024, 11:04:02	CWE-79
CVE-2024-7529	Критичный соответствием: cpe2.3:mozilla:firefox:*****	06.09.2024, 01:00:00	06.09.2024, 11:00:10	CWE-328
CVE-2024-7527	Критичный соответствием: cpe2.3:mozilla:firefox:***** Отсутствует в уязвимой и последующих версиях: 129.0	06.09.2024, 01:00:00	06.09.2024, 11:00:10	CWE-416
CVE-2024-7529	Критичный соответствием: cpe2.3:mozilla:firefox:***** Отсутствует в уязвимой и последующих версиях: 129.0	06.09.2024, 01:00:00	06.09.2024, 11:00:10	NVD-CWE-NONINFO, CWE-451
CVE-2024-8382	Критичный соответствием: cpe2.3:mozilla:firefox:***** Отсутствует в уязвимой и последующих версиях: 130.0	09.01.2024, 01:00:00	07.09.2024, 05:15:07	NVD-CWE-NONINFO, CWE-479
CVE-2024-4066	Критичный соответствием: cpe2.3:mozilla:firefox:*****	29.11.2022, 22:15:10	06.09.2024, 11:00:10	CWE-404
CVE-2024-1970	Критичный соответствием: cpe2.3:mozilla:firefox:*****	11.04.2007, 14:19:00	06.09.2024, 10:50:02	NVD-CWE-OTHER

Показывать по 10

Распространенность

Организация

ПАО «Аэрофлот»

Клиент

test (EOR DEV)

Распространенность на клиенте

1

Рисунок 38 – Сведения о программе

На данной странице сведения о программе представлены в следующих областях:

- Общие сведения о программе;
- Таблица с обнаруженными уязвимостями;
- Распространенность (показывается распространенность программы с уязвимостями у различных клиентов).

Общий вид страницы «Программы» при переключении режима агрегации в состояние «Включен» ( Режим агрегации) представлен на рисунке 39.

Включенный режим агрегации позволяет сгруппировать программы по полям «Вендор» и «Продукт» из сгенерированного представления программы в формате CPE.

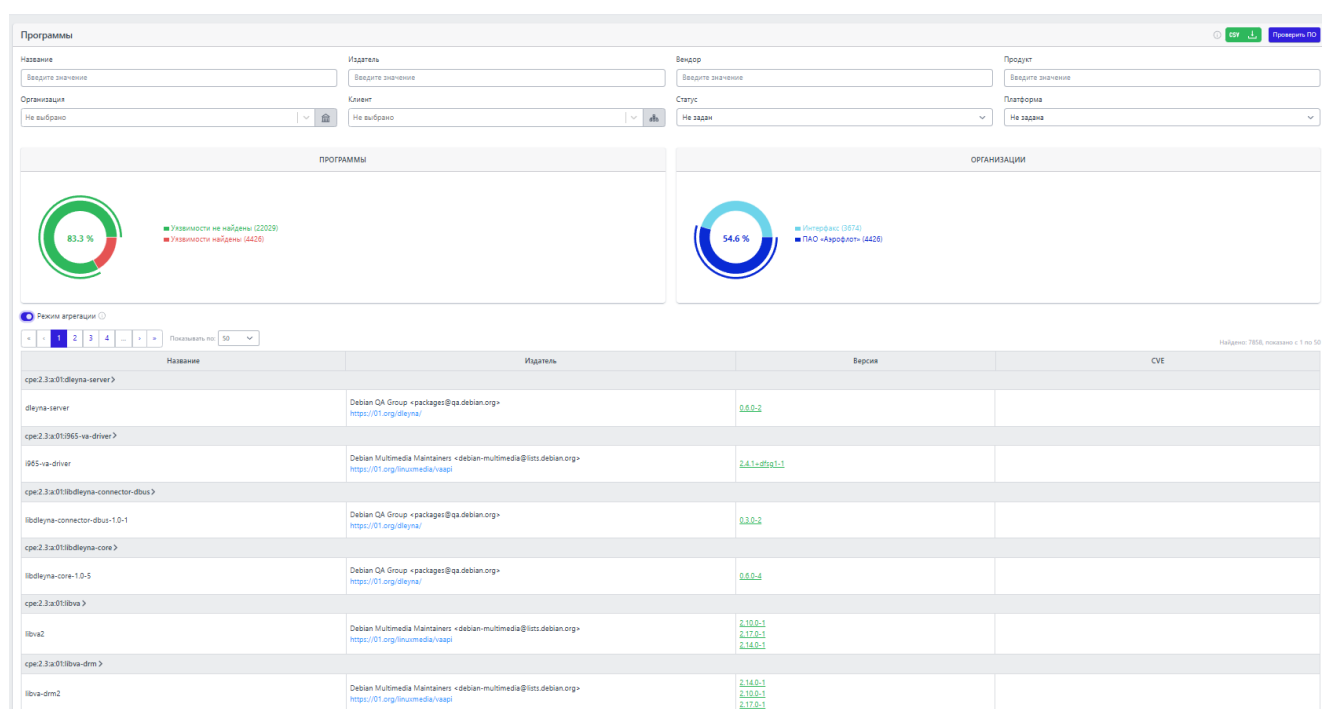


Рисунок 39 – Общий вид страницы программы при включенном режиме агрегации

В данной таблице в столбце «Версия» имеется иконка , при нажатии по которой уязвимости в CVE-формате отображаются только для данной версии программы.

На странице **Программы** имеется область с графическим отображением по программам и организациям, в которых найдены уязвимости.

Данная область представлена на рисунке 40.

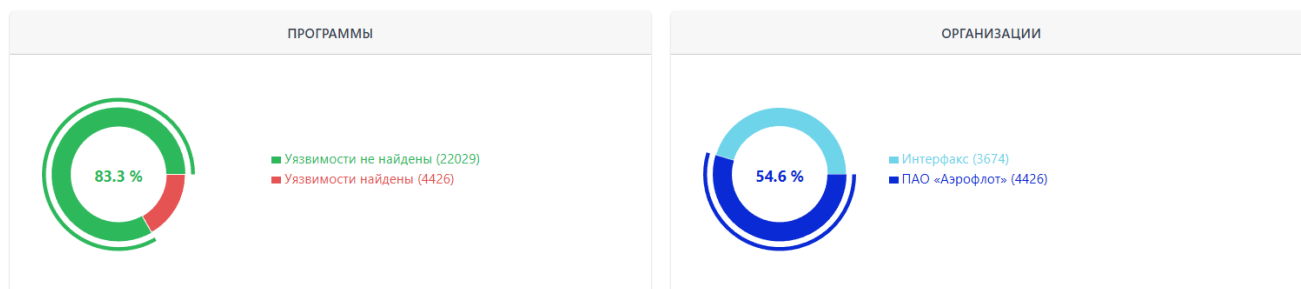


Рисунок 40 – Графическая область

На странице «Программы» имеется возможность, нажав по иконке **Проверить ПО**, проверить программу на наличие уязвимостей.

При нажатии по данной иконке открывается окно, в котором требуется заполнить поля для проверки программы (рисунок 41).

Проверить программу

☒ Проверить по CPE

Название *

Издатель *

URL

Версия *

Тип

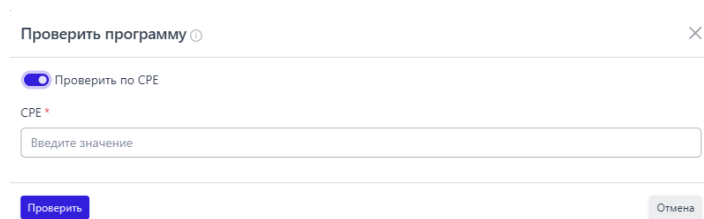
Приложение

Проверить Отмена

Рисунок 41 – Окно задания параметров проверяемого ПО

В данном окне с помощью ползунка **Проверить по CPE** можно задать представление программы в виде CPE.

CPE – это структурированная схема именования систем информационных технологий, программного обеспечения и пакетов. Основанный на общем синтаксисе унифицированных идентификаторов ресурсов (URI), CPE включает в себя формальный формат имени, метод проверки имен по системе и формат описания для привязки текста и тестов к имени.



Проверить программу

☒ Проверить по CPE

CPE *

Введите значение

Проверить Отмена

Рисунок 42 – Окно задания представления программы в CPE формате

После заполнения полей в окне проверки программы требуется нажать по иконке **Проверить**.

7. Сообщения об ошибках

Большинство ошибок можно разделить на следующие типы:

1) Ошибки конфигурации:

- некорректные настройки параметров безопасности;
- некорректная установка компонентов программы;
- некорректные действие со стороны пользователя/администратора;
- критические ошибки.

2) Ошибки оборудования:

- выход из строя аппаратных средств, на которых установлена программа;
- выход из строя сервера (или компонентов на сервере), с которыми взаимодействуют компоненты

Изделия, установленные на оборудовании пользователя;

- перебои питания со стороны клиентской или серверной части.

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

8. Термины и определения

Перечень терминов и определений указан в таблице 2.

Таблица 2 – Термины и определения

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

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