

User Guide

PARUS BOX



PARUS BOX

Руководство пользователя

v1.1



Оглавление

1 Введение	3
2 Вход в РВОХ	4
3 Интерфейс РВОХ	5
3.1 Раздел «Статистика»	5
3.1.1 Проверка контрольной суммы или файла	5
3.1.2 Статистика проверок.....	6
3.2 Раздел «Проверки»	8
3.2.1 Детали	11
3.3 Раздел «Документация»	12

1 Введение

PARUS BOX (далее – PBOX, Система, АИС) – это облачный сервис (SaaS), предназначенный для потоковой проверки файлов различных типов, в том числе архивов, на предмет осуществления ими вредоносной или потенциально опасной активности.

PBOX представляет собой приложение, работающее в инфраструктуре разработчика, к которому для отправки файлов и получения результатов их проверки подключаются устройства, информационные системы и пользователи конечных заказчиков. Подключение осуществляется по различным протоколам посредством сети Интернет. Система предназначена для автоматизации следующих задач компаний-заказчиков:

- потоковой проверки файлов в трафике, обрабатываемом на межсетевых экранах;
- ручной загрузки и проверки подозрительных файлов;
- проверки файлов, обрабатываемых в других информационных системах;
- осуществления статического и динамического (поведенческого) анализа файлов;
- проверки контрольных сумм файлов на наличие их в различных базах вредоносных файлов;
- предоставления вердиктов, отчетов и другой метаинформации о проверках файлов.

Настоящий документ содержит инструкции по работе с сервисом PBOX.

2 Вход в PBOX

Для входа в PBOX:

1. Перейдите по ссылке <https://cportal.parus.su>.

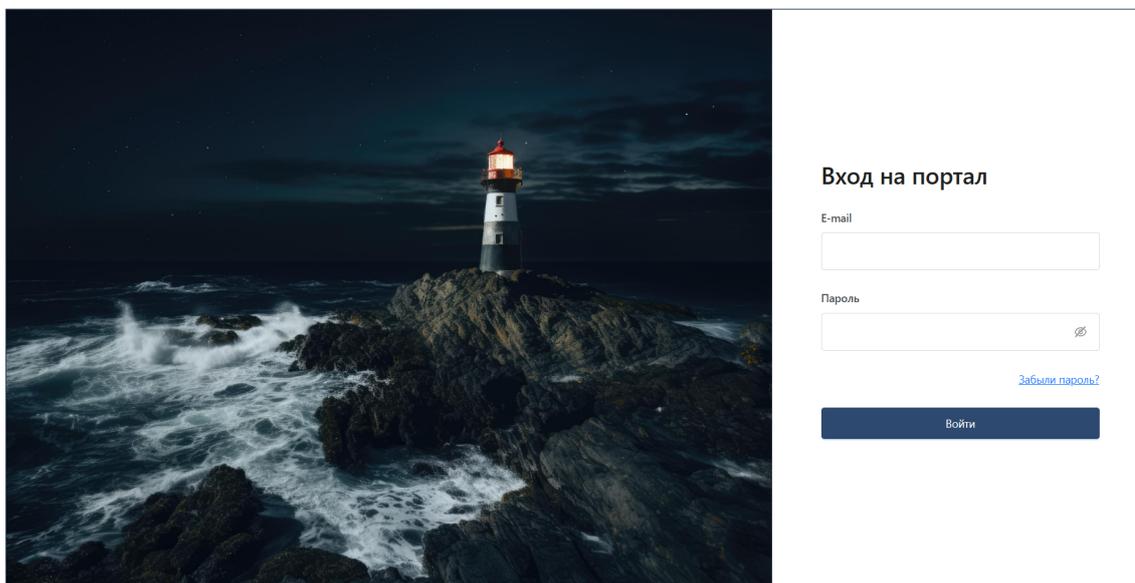


Рисунок 1 – Страница авторизации и аутентификации

2. Введите логин и пароль Вашей учётной записи в полях формы на странице авторизации и аутентификации (рисунок 1).
3. Нажмите на кнопку «Войти».
4. При успешной авторизации и аутентификации произойдёт перенаправление в раздел «Организация».

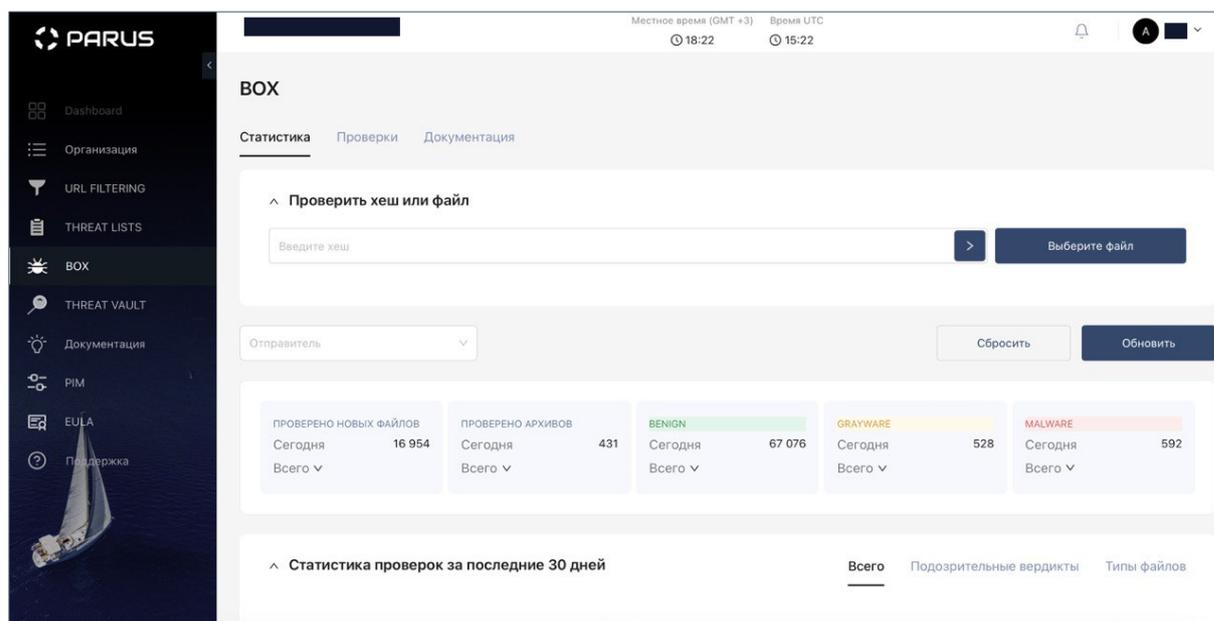


Рисунок 2 – Раздел VOX

5. В боковом меню слева найдите раздел VOX (рисунок 2) и перейдите в него.

3 Интерфейс PBOX

3.1 Раздел «Статистика»

3.1.1 Проверка контрольной суммы или файла

В форме проверки контрольной суммы (алгоритм SHA-256) или файла (рисунок 3) осуществляется проверка файла или архива на наличие угроз безопасности.

Проверка файла выполняется:

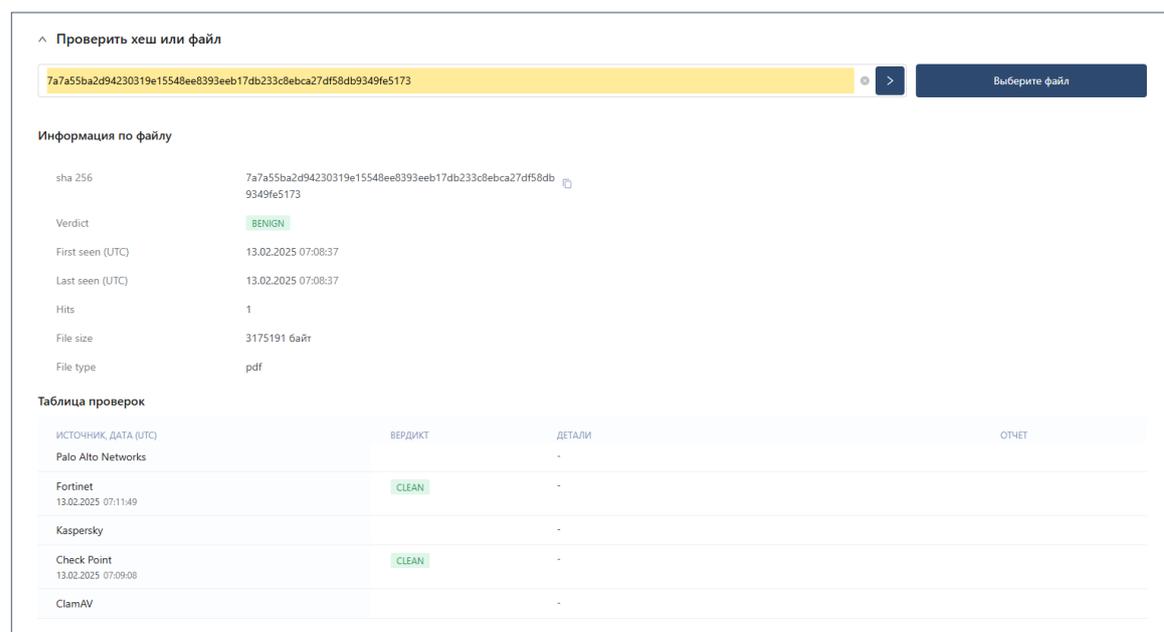
- по контрольной сумме;
- по файлу, загружаемому с устройства.

Для поиска по контрольной сумме введите контрольную сумму файла в форму и нажмите на кнопку «>» или Enter.



Рисунок 3 – Форма проверки контрольной суммы или файла

После отправки контрольной суммы на проверку, при наличии её в базе, пользователь получит отчёт о проверке (рисунок 4). При отсутствии контрольной суммы в базе будет получено сообщение «Хеш не найден» (рисунок 5).



7a7a55ba2d94230319e15548ee8393eeb17db233c8ebca27df58db9349fe5173

Выберите файл

Информация по файлу

sha 256	7a7a55ba2d94230319e15548ee8393eeb17db233c8ebca27df58db9349fe5173
Verdict	BENIGN
First seen (UTC)	13.02.2025 07:08:37
Last seen (UTC)	13.02.2025 07:08:37
Hits	1
File size	3175191 байт
File type	pdf

Таблица проверок

ИСТОЧНИК, ДАТА (UTC)	ВЕРДИКТ	ДЕТАЛИ	ОТЧЕТ
Palo Alto Networks		-	
Fortinet 13.02.2025 07:11:49	CLEAN	-	
Kaspersky		-	
Check Point 13.02.2025 07:09:08	CLEAN	-	
ClamAV		-	

Рисунок 4 – Отчёт о проверке контрольной суммы

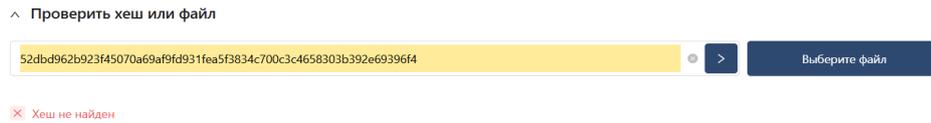


Рисунок 5 – Сообщение о необнаружении контрольной суммы

Для поиска по файлу нажмите на кнопку «Выберите файл» и загрузите файл с устройства.

После отправки файла на проверку будет получена информация об успешной загрузке файла с указанием объема файла и ссылкой на таблицу проверок (раздел «Проверки») (рисунок 6).

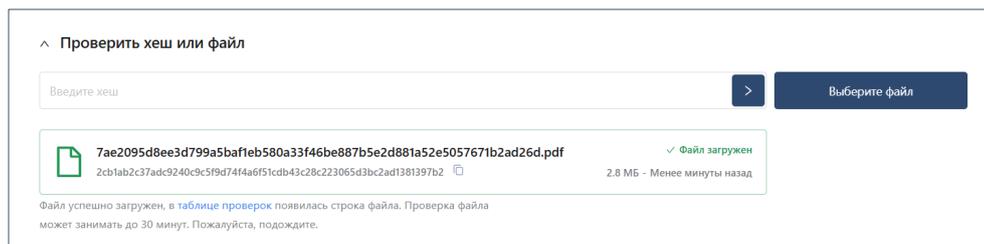


Рисунок 6 – Успешная загрузка файла на проверку

Если при загрузке файла произошла ошибка, то появится сообщение о ней с текстом ошибки (рисунок 7).

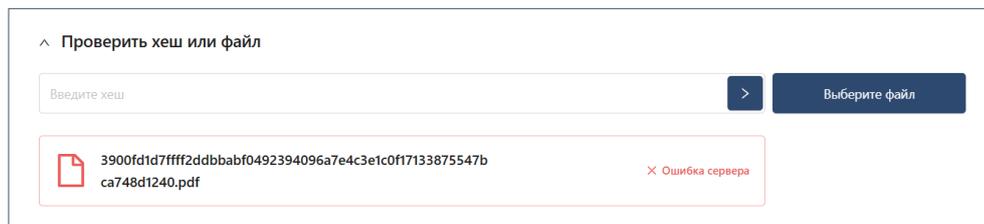


Рисунок 7 – Неуспешная загрузка файла на проверку

3.1.2 Статистика проверок

Статистика проверок (рисунок 8) содержит информацию о количестве проверок за текущий день и всё прошедшее время.

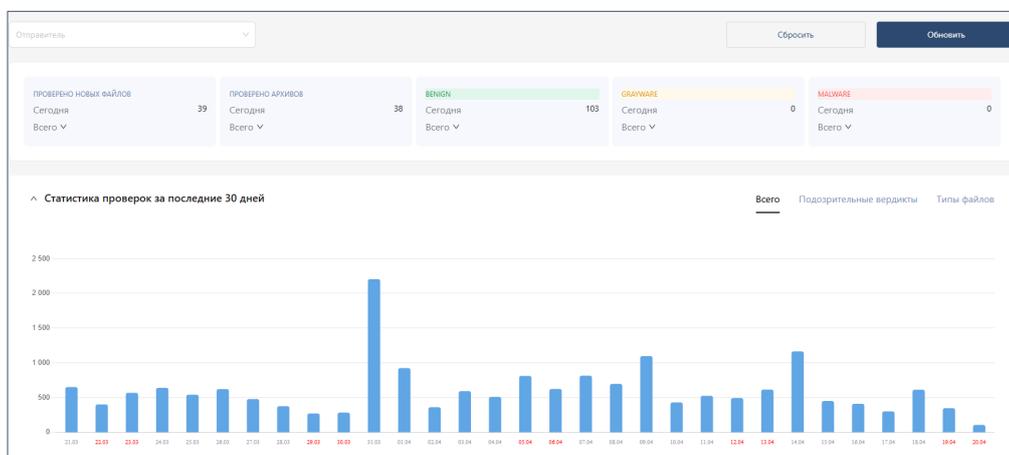


Рисунок 8 – Статистика проверок

Данные представлены в виде карточек с данными по вердиктам и типам проверяемых объектов (файлов или архивов) (рисунок 9), а также в трех графиков с данными за последние 30 календарных дней, отражающими количество проверок по датам (рисунок 10), количество подозрительных вердиктов из проверенных файлов и архивов по датам (рисунок 11) и количество файлов и архивов по типам (рисунок 12).



Рисунок 9 – Карточки со статистикой проверок

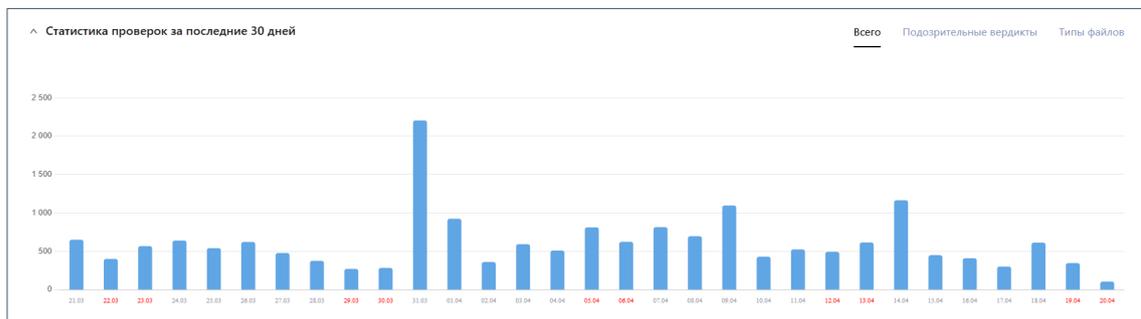


Рисунок 10 – График проверок

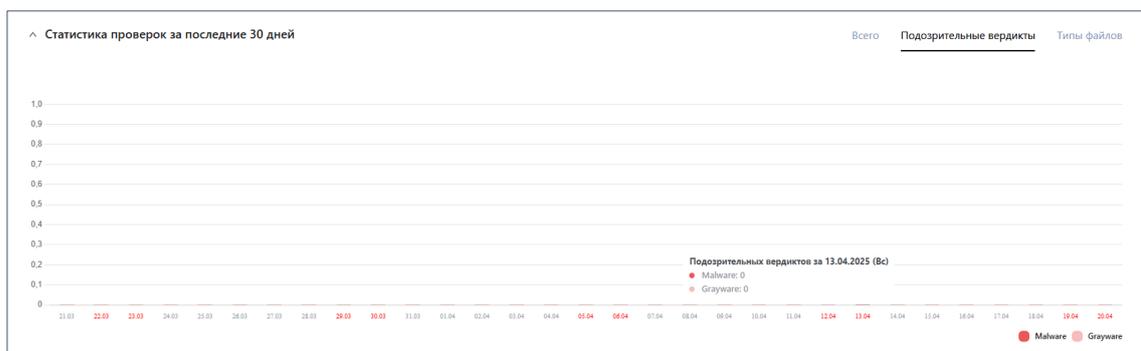


Рисунок 11 – График подозрительных вердиктов

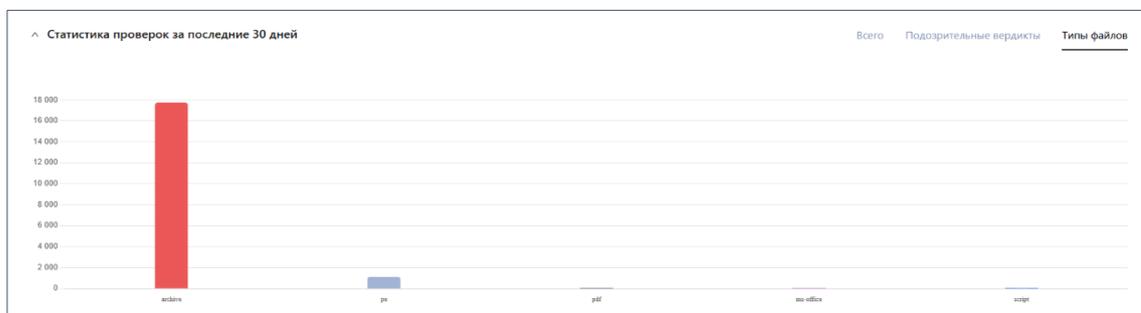


Рисунок 12 – График типов проверенных файлов

Данные можно отфильтровать по отправителю (рисунок 13). Для применения фильтра выберите один из трех типов отправителя: «Устройство», «Пользователь» или «API».

Для пунктов «Пользователь» и «Устройство» выберите из выпадающего списка конкретные устройства.

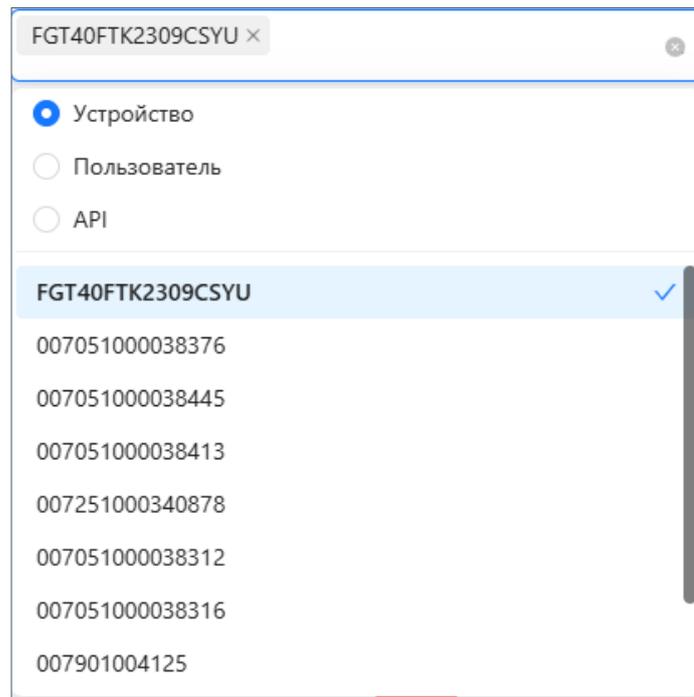


Рисунок 13 – Фильтр «Отправитель»

3.2 Раздел «Проверки»

В разделе «Проверки» в табличном виде представлены данные о проверяемых файлах и архивах (рисунок 14). Записи в таблице могут быть отсортированы по столбцам «Начало проверки (UTC)» и «Конец проверки (UTC)».

НАЧАЛО ПРОВЕРКИ (UTC)	КОНЕЦ ПРОВЕРКИ (UTC)	ОТПРАВИТЕЛЬ	СТАТУС	SHA256	ВЕРДИКТ	ИМЯ ФАЙЛА	ТИП	ДЕТАЛИ
20.04.2025 09:45:18	20.04.2025 09:45:48		ПРОВЕРЕН	...d1381397b2	BENIGN	7ae2095d8ee3d799a5baf1eb580a33146eb87b5e2d881a52e5057671b2ad26d.pdf	pdf	
20.04.2025 07:25:00	20.04.2025 07:25:01	FGT40FTK2309CSYU	ПРОВЕРЕН	...bad696f188	BENIGN	43147177_180237d1ba7440073ee9a7b3d99de801777ab349.cab	archive	
20.04.2025 07:25:00	20.04.2025 07:25:01	FGT40FTK2309CSYU	ПРОВЕРЕН	...ffe3e11608	BENIGN	43147178_c424d042ccfb910bbc93f19746e3e660605842e.cab	archive	
20.04.2025 07:25:00	20.04.2025 07:25:00	FGT40FTK2309CSYU	ПРОВЕРЕН	...0420e43b3	BENIGN	43147176_54513d9d90a70089050a7552dbd1d8abf194634c.cab	archive	
20.04.2025 05:07:02	20.04.2025 05:07:02	FGT40FTK2309CSYU	ПРОВЕРЕН	...f699be99b7	BENIGN	am_delta_patch_1.427.338.0_124dd0de484cddc9338538784dbcc1c1e6d831e xe	pe	
20.04.2025 05:06:02	20.04.2025 05:06:03	FGT40FTK2309CSYU	ПРОВЕРЕН	...a96881c7d9	BENIGN	43148550_92cbe2feddec80084e0a98a72294963deac3b48.cab	archive	
20.04.2025 05:06:02	20.04.2025 05:06:03	FGT40FTK2309CSYU	ПРОВЕРЕН	...d67f438c7c	BENIGN	43147264_3a0789272c9904702b12ade087698b41b104747.cab	archive	
20.04.2025 05:06:02	20.04.2025 05:06:02	FGT40FTK2309CSYU	ПРОВЕРЕН	...b9e57704c1	BENIGN	43147658_cb68d261776ee8801088e69a4fc7789fb70c645.cab	archive	
20.04.2025 05:06:02	20.04.2025 05:06:03	FGT40FTK2309CSYU	ПРОВЕРЕН	...16fd43185	BENIGN	43148575_b1b0068da3d1e59094f8cd028e49c25a9bc9d69.cab	archive	

Рисунок 14 – Раздел «Проверки»

В таблице проверок (рисунок 15) отражены следующие данные:

- время начала и конца проверки;
- отправитель;
- статус проверки;

- контрольная сумма проверяемого файла или архива;
- вердикт;
- имя файла или архива;
- тип файла или архива;
- общее количество проверок.

НАЧАЛО ПРОВЕРКИ (UTC)	КОНЕЦ ПРОВЕРКИ (UTC)	ОТПРАВИТЕЛЬ	СТАТУС	SHA256	ВЕРДИКТ	ИМЯ ФАЙЛА	ТИП	ДЕТАЛИ
20.04.2025 09:45:18	20.04.2025 09:45:48	[REDACTED]	ПРОВЕРЕН	...d1381397b2	BENIGN	7ae2095d9ee3d799a5ba1eb580a33f46be887b5e2d881a52e5057671b2ad26d.pdf	pdf	
20.04.2025 07:25:00	20.04.2025 07:25:01	FGT40FTK2309CSYU	ПРОВЕРЕН	...bad9989188	BENIGN	43147172_180237d1b47440073ee9a7b3da9d80177fab349.cab	archive	
20.04.2025 07:25:00	20.04.2025 07:25:01	FGT40FTK2309CSYU	ПРОВЕРЕН	...ffe3e11608	BENIGN	43147178_c424d042ccfb910bcb93f919746a3e6065842e.cab	archive	
20.04.2025 07:25:00	20.04.2025 07:25:00	FGT40FTK2309CSYU	ПРОВЕРЕН	...0a420e43b3	BENIGN	43147176_34113d9490a70098950a7952db108abf194634c.cab	archive	
20.04.2025 05:07:02	20.04.2025 05:07:02	FGT40FTK2309CSYU	ПРОВЕРЕН	...f099be9907	BENIGN	am_delta_patch_1427.338.0_124d000e484c0dc9338538784dbcc1c1e6d831f.exe	pe	
20.04.2025 05:06:02	20.04.2025 05:06:03	FGT40FTK2309CSYU	ПРОВЕРЕН	...a98881c709	BENIGN	43148550_92bc2e6ed9ec80084e0a98a722948630eac3b48.cab	archive	
20.04.2025 05:06:02	20.04.2025 05:06:03	FGT40FTK2309CSYU	ПРОВЕРЕН	...d61f43bc7c	BENIGN	43147264_3a0789272c9904702b12ade087898b41b104747.cab	archive	
20.04.2025 05:06:02	20.04.2025 05:06:02	FGT40FTK2309CSYU	ПРОВЕРЕН	...b9e57f0d41	BENIGN	43147858_e8b68d261778ee8801088e69a4c7789fb70c645.cab	archive	
20.04.2025 05:06:02	20.04.2025 05:06:03	FGT40FTK2309CSYU	ПРОВЕРЕН	...16fa943185	BENIGN	43148575_b1b0068da3d1e590448cc8028e49c25a98c9459.cab	archive	

Рисунок 15 – Таблица проверок

Фильтры, применяемые к таблице, позволяют отфильтровать записи по:

- имени или контрольной сумме файла (алгоритм SHA-256);
- дате проверки;
- отправителю;
- статусу проверки.

Для фильтрации по имени или контрольной сумме файла (алгоритм SHA-256) введите искомый текст в строку поиска нажмите на кнопку «Поиск» (рисунок 16).

Поиск

Рисунок 16 – Поиск по контрольной сумме или имени файла

Для фильтрации по дате проверки используйте фильтр «Выберите интервал» (рисунок 17). Нажмите на кнопку фильтра и либо выберите искомое из предложенных стандартных временных интервалов, либо введите интересующий интервал в специальных полях самостоятельно.

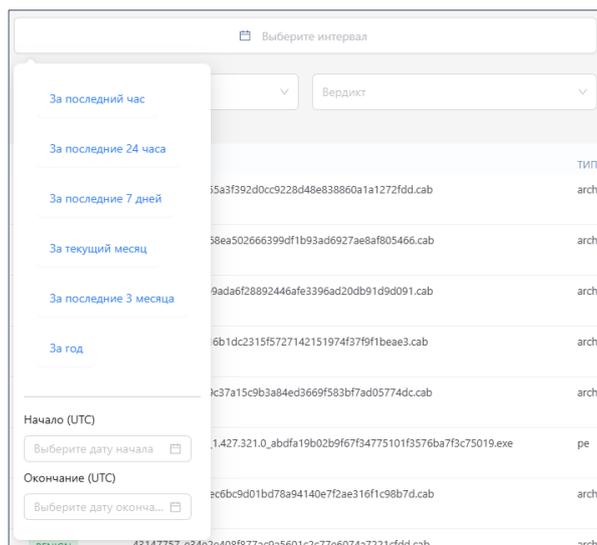


Рисунок 17 – Фильтр выбора временного интервала

Для фильтрации по отправителю используйте алгоритм, описанный в п. 3.1.2 настоящего руководства (рисунок 13).

Для фильтрации по статусу проверки (рисунок 18), типу проверяемого файла или архива (рисунок 19) и вердикту (рисунок 20) нажмите на соответствующий фильтр и выберите из выпадающего меню интересующие параметры (один или несколько). При вводе значения в строку поиска внутри фильтра будет осуществляться поиск по выпадающему меню.

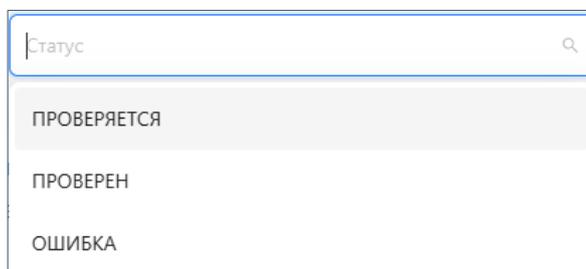


Рисунок 18 – Фильтр статуса проверки

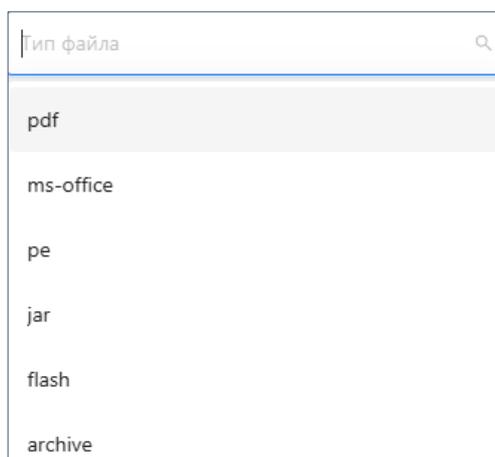


Рисунок 19 – Фильтр типа файла или архива

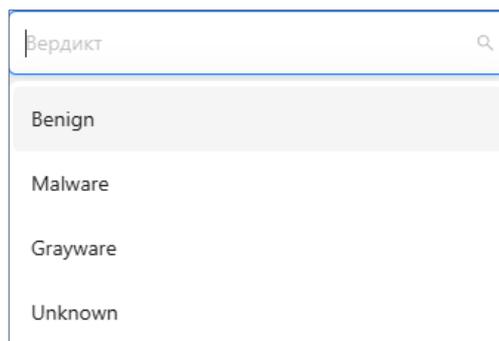


Рисунок 20 – Фильтр вердикта

Если в фильтре «Вердикт» выбран только пункт «Malware», то становится доступен фильтр «Уникальные Malware» (рисунок 21).

При включении этого фильтра в таблице будут отображаться только уникальные записи с Malware вердиктами. Все остальные фильтры также будут применены.

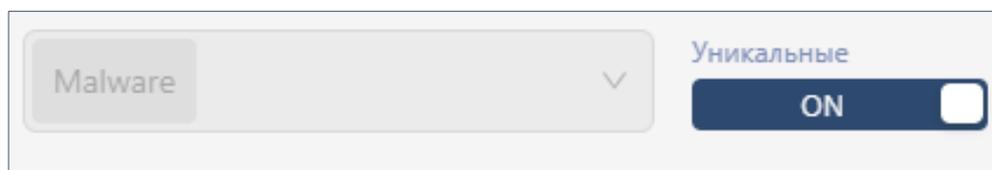


Рисунок 21 – Фильтр «Уникальные Malware»

Для обновления данных в таблице нажмите на кнопку «Обновить».

Для сброса всех примененных фильтров нажмите на кнопку «Сбросить».

3.2.1 Детали

В столбце «Детали» таблицы проверок можно ознакомиться с подробными деталями каждой проверки (информация о файле или архиве, вердикты Palo Alto Networks, Kaspersky, Check Point, ClamAV и Fortinet), а также скачать отчеты Palo Alto Networks, Fortinet и Check Point (доступно только для Malware вердиктов), скачать сэмпл вредоносного файла или архива (доступно только для Malware вердиктов), получить ссылку на проверку VirusTotal (только для Malware вердиктов).

Для просмотра деталей нажмите на иконку  в строке интересующей проверки. Данные будут представлены во всплывающем окне (рисунок 22).

Детальная информация X

sha 256	fdb4db863c1426165460f277be39debc0d547fbfdbc9575c41a9f29df2bf8c15
Verdict	MALWARE открыть VirusTotal
First seen (UTC)	20.01.2025 00:34:00
Last seen (UTC)	20.01.2025 00:34:00
Hits	1
File size	55296 байт
File type	pe
File name	wildfire-test-pe-file(27).exe
Download File Sample	

Таблица проверок

ИСТОЧНИК, ДАТА (UTC)	ВЕРДИКТ	ДЕТАЛИ	ОТЧЕТ
Palo Alto Networks		-	
Fortinet 20.01.2025 00:36:05	MALICIOUS	Category: NotApplicable Name: Riskware/WildFireTestFile	
Kaspersky 20.01.2025 07:40:47	HIGH RISK	VHO:Trojan.Win32.Agent.gen HEUR:Trojan.Win32.Agent.gen	
Check Point 20.01.2025 00:35:50	HIGH RISK	Trojan.Wins.Imphash.ta.AC	
ClamAV 20.01.2025 00:34:07	MALWARE	Win.Dropper.Bebloh-9954185-0	

Рисунок 22 – Детали проверки

3.3 Раздел «Документация»

В разделе «Документация» (рисунок 23) представлена вся существующая документация к PARUS BOX.

Для скачивания файла документа на устройство нажмите на иконку в строке интересующего документа.

НАЗВАНИЕ	ОПИСАНИЕ	ИЗМЕНЕНО	СКАЧАТЬ
BOX API GUIDE v1.1	Описание API интерфейса к сервису PARUS BOX	17.04.2025 13:29	
BOX API PYTHON TEST SCRIPT	скрипт для тестирования API интерфейса PARUS BOX	17.04.2025 13:26	
Palo Alto Integration Guide	Руководство для подключения PA NGFW к сервису PARUS BOX	07.02.2025 11:53	

Рисунок 23 – Раздел «Документация»