User Guide

PARUS BOX

PARUS BOX

Руководство пользователя

v1.1

Оглавление

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.

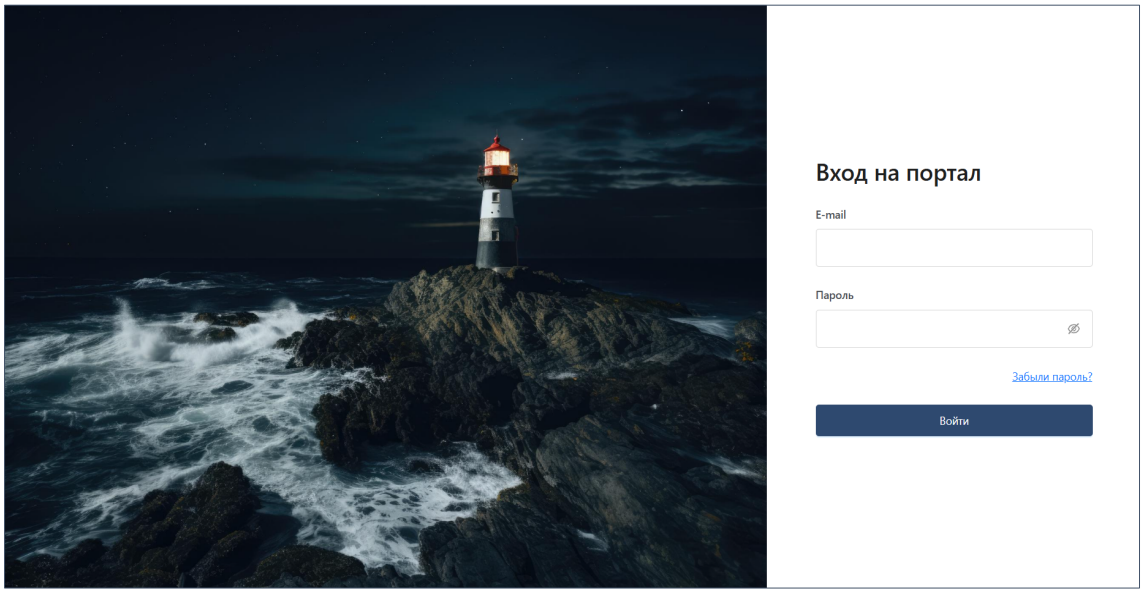

Рисунок 1 – Страница авторизации и аутентификации

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».

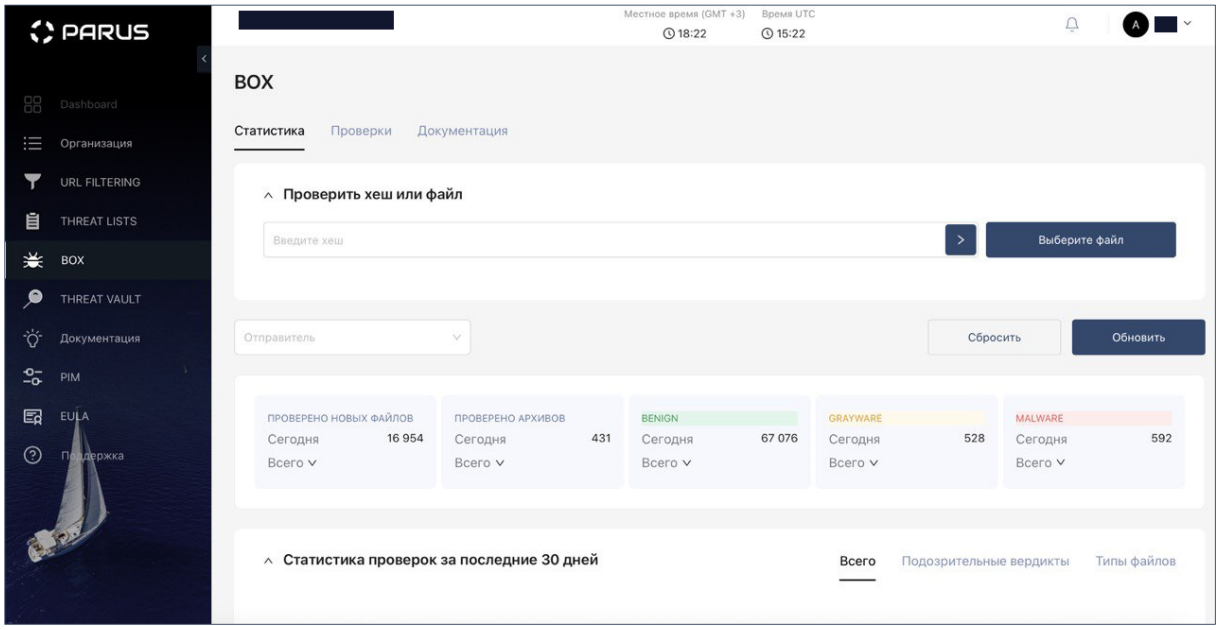

Рисунок 2 – Раздел BOX

5. В боковом меню слева найдите раздел BOX (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.

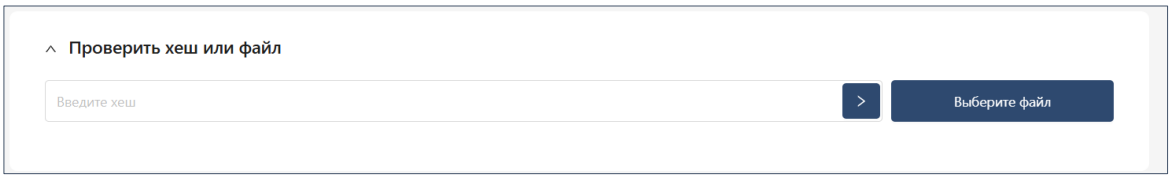

Рисунок 3 – Форма проверки контрольной суммы или файла

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).

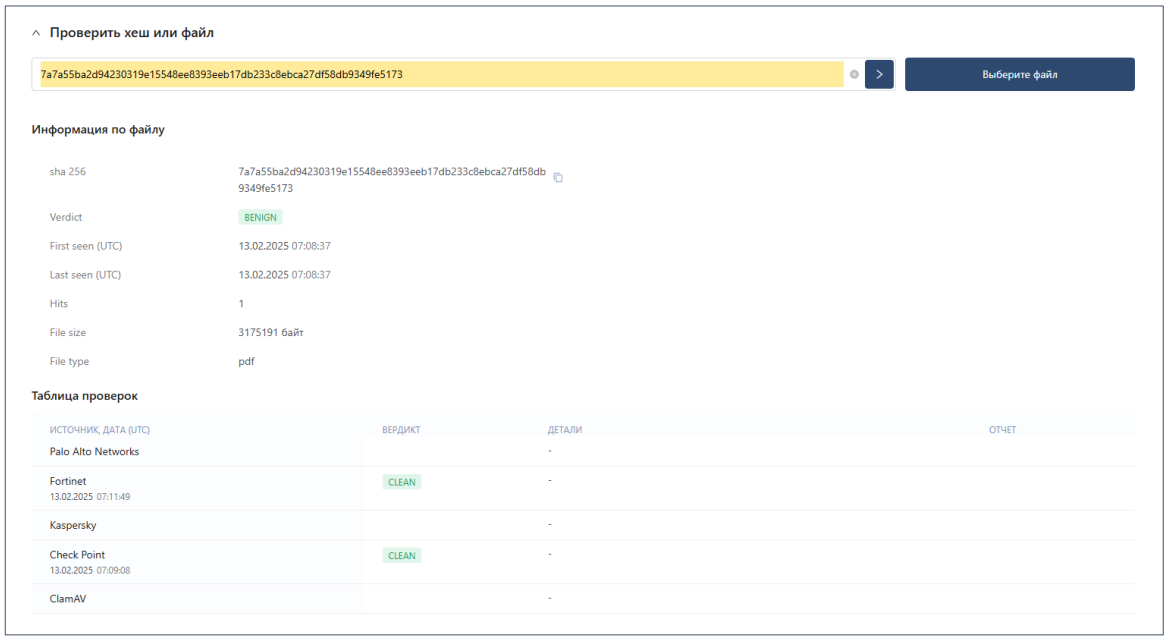

Рисунок 4 – Отчёт о проверке контрольной суммы

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).

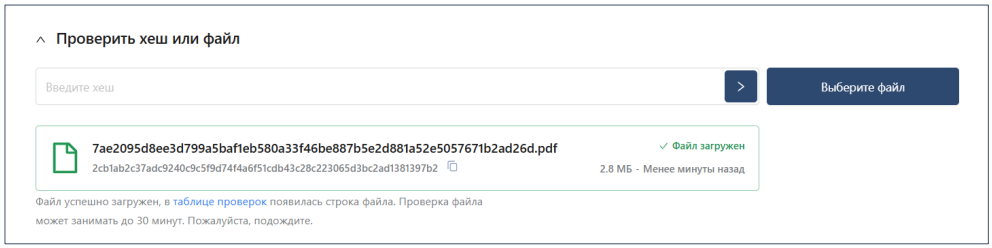

Рисунок 6 – Успешная загрузка файла на проверку

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

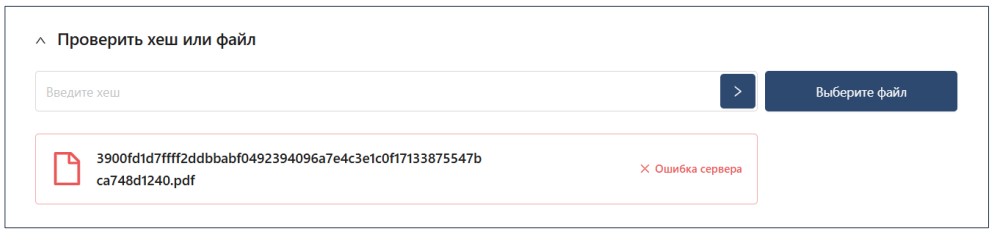

Рисунок 7 – Неуспешная загрузка файла на проверку

3.1.2 Статистика проверок

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

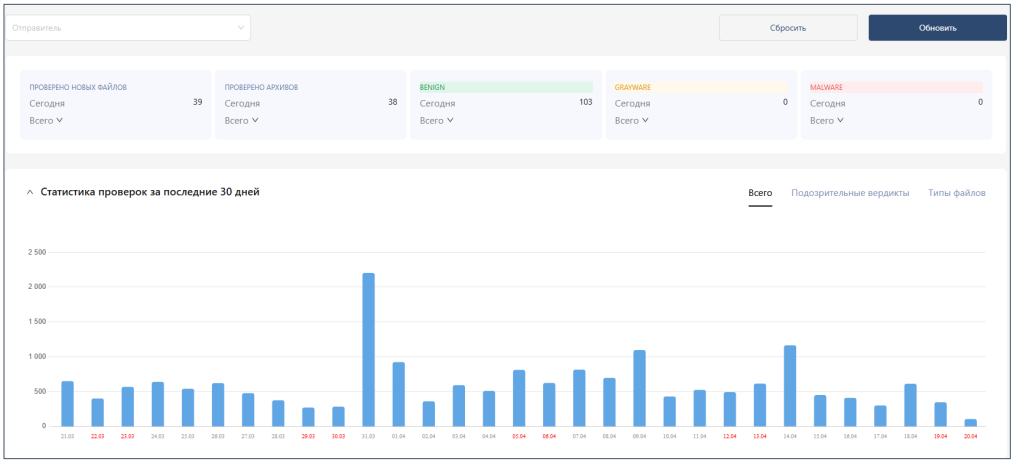

Рисунок 8 – Статистика проверок

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

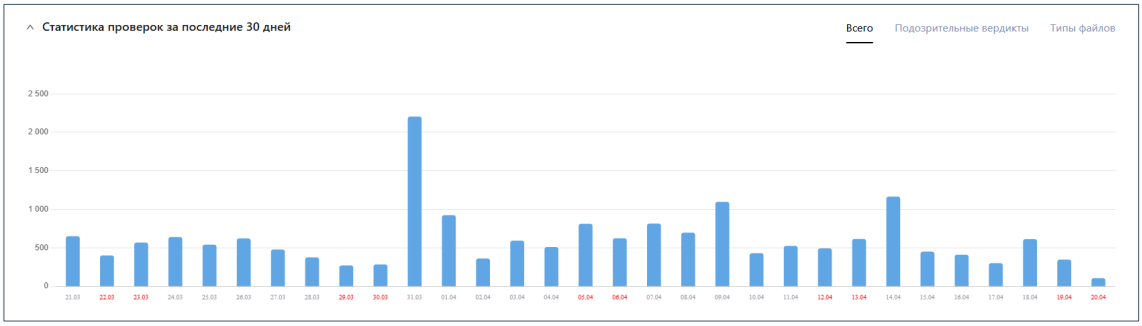

Рисунок 10 – График проверок

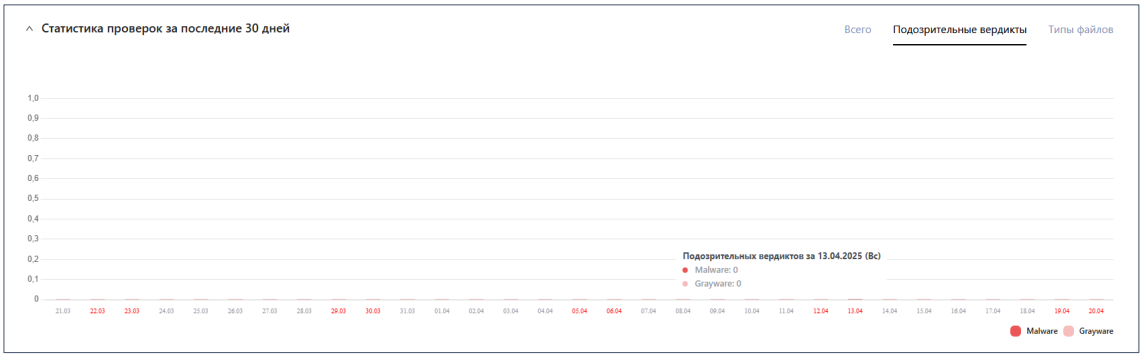

Рисунок 11 – График подозрительных вердиктов

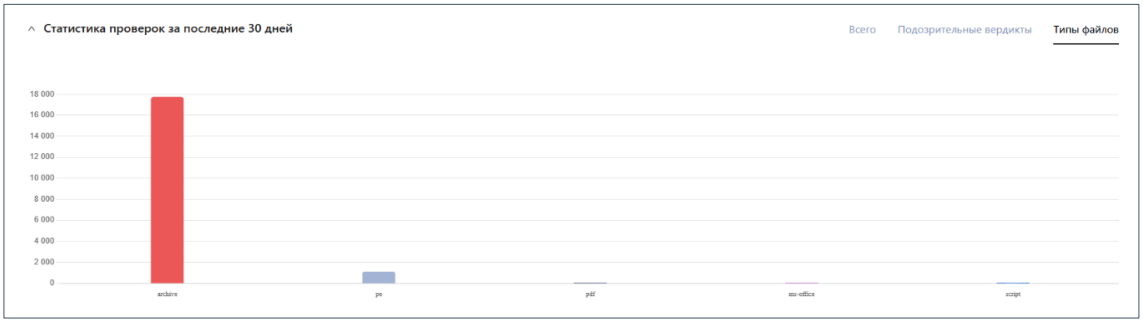

Рисунок 12 – График типов проверенных файлов

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.

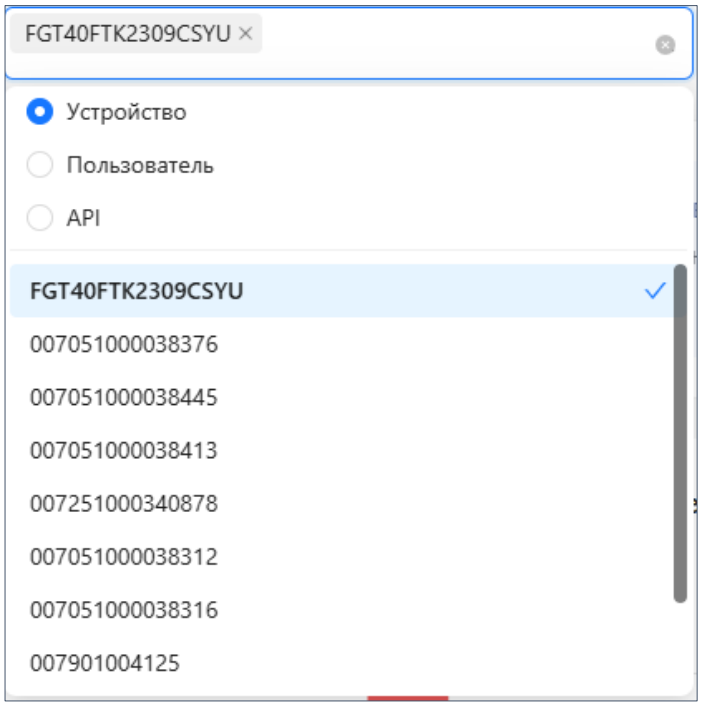

Рисунок 13 – Фильтр «Отправитель»

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)».

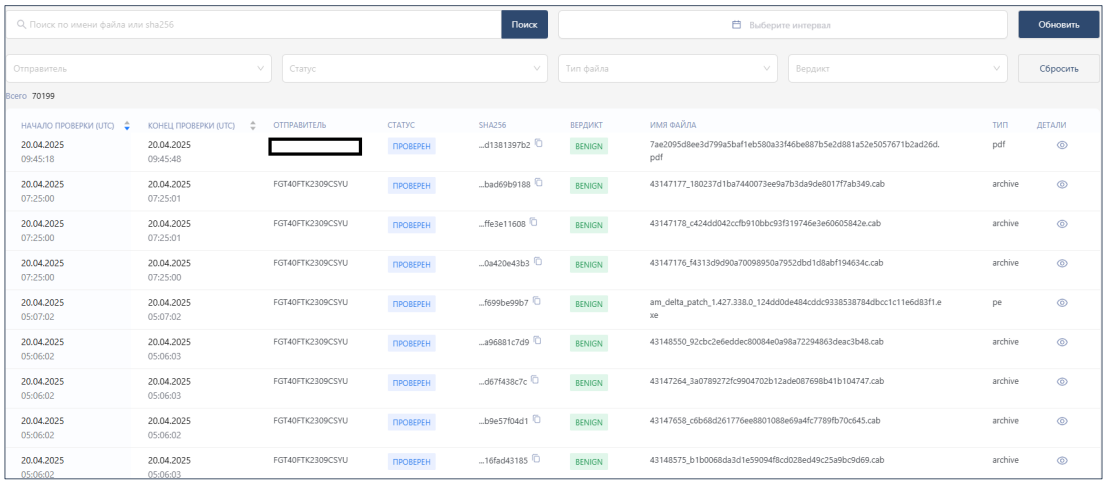

Рисунок 14 – Раздел «Проверки»

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.

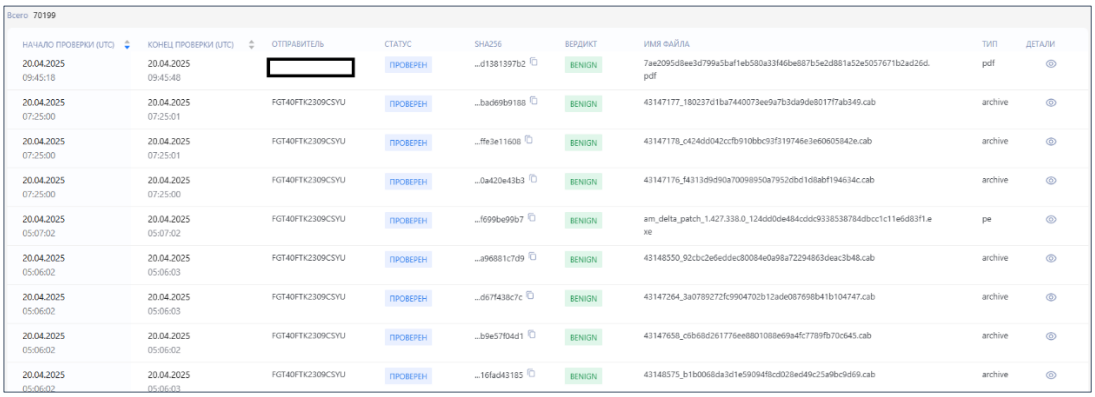

Рисунок 15 – Таблица проверок

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).

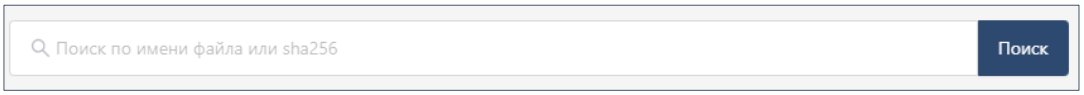

Рисунок 16 – Поиск по контрольной сумме или имени файла

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.

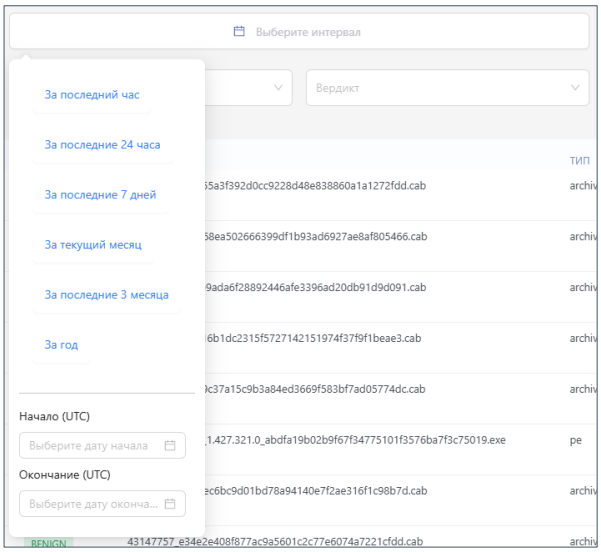

Рисунок 17 – Фильтр выбора временного интервала

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

Для фильтрации по статусу проверки (рисунок18), 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.

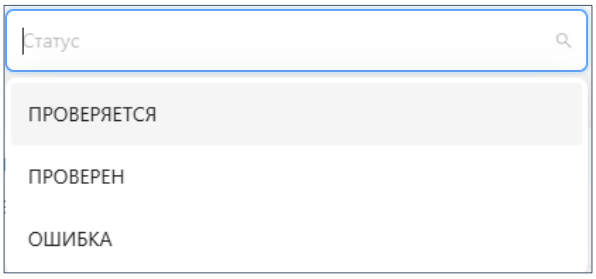

Рисунок 18 – Фильтр статуса проверки

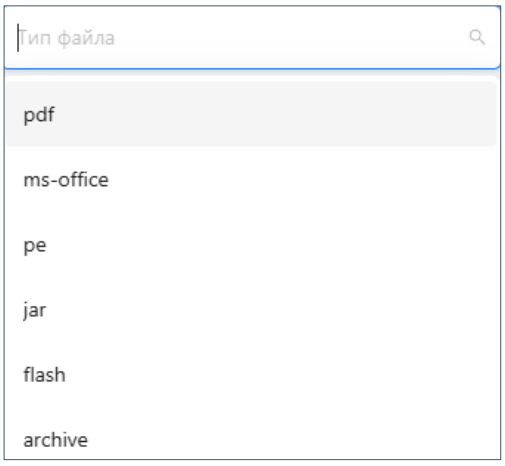

Рисунок 19 – Фильтр типа файла или архива

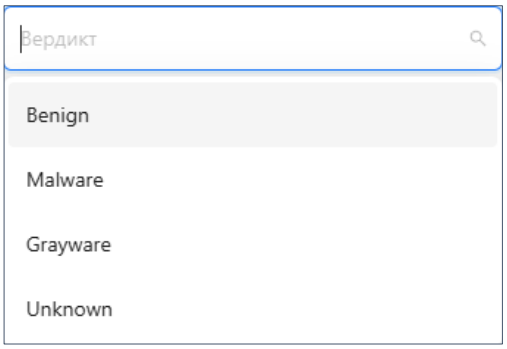

Рисунок 20 – Фильтр вердикта

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).

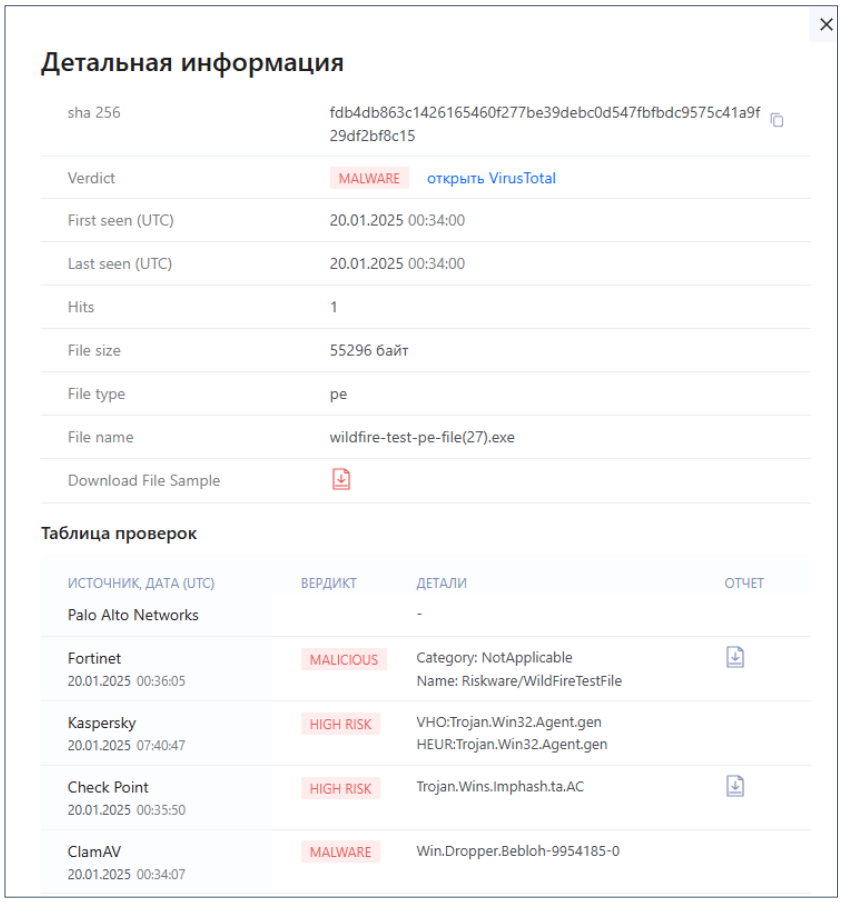

Рисунок 22 – Детали проверки

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.

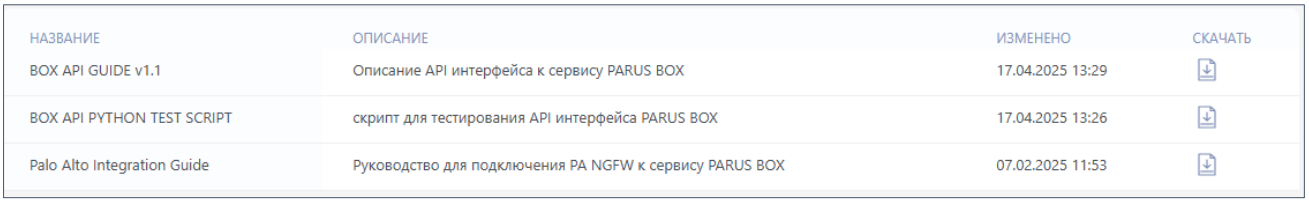

Рисунок 23 – Раздел «Документация»