



О К Т О П У С

**СИСТЕМА КОМПЛЕКСНОЙ
АНТИВИРУСНОЙ ПРОВЕРКИ
ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ**

Руководство пользователя

**Москва
2021г.**

Контактная информация

127106, г. Москва, ул. Гостиничная, д.5

Тел.: +7 (495) 988-92-25

E-mail: office@avsw.ru

www.avsw.ru/about/contacts

Авторское право

ООО «АВ Софт»

www.avsw.ru

© 2010-2021 ООО «АВ Софт»

Версия документа

Декабрь 07, 2021.

Настоящий документ является собственностью ООО «АВ Софт» (далее — «АВ Софт») и защищен законодательством Российской Федерации и международными соглашениями об авторских правах и интеллектуальной собственности.

Копирование документа либо его фрагментов в любой форме, распространение, в том числе в переводе, а также их передача третьим лицам возможны только с письменного разрешения «АВ Софт».

Документ может быть изменен без предварительного уведомления.

СОДЕРЖАНИЕ

1	Термины и определения	4
2	Сокращения и значения.....	5
3	Назначение программы	6
4	Работа с серверным программным обеспечением.....	8
4.1	Элементы управления веб-интерфейсом.....	9
5	Раздел «Статистика».....	12
6	Раздел «Источники».....	14
6.1	Подраздел «WEB-трафик»	14
6.2	Подраздел «Почтовый трафик».....	15
7	Раздел «Объекты анализа».....	17
7.1	Подраздел «Файлы».....	17
7.2	Подраздел «Ссылки»	21
8	Раздел «Исследования»	22
9	Раздел «Справочники»	28

1 Термины и определения

В настоящем документе используются термины и определения, представленные в таблице 1.

Таблица 1. Термины и определения

№	Термин	Определение
1.	ExifTool	Инструмент для чтения, записи и редактирования метаданных файлов.
2.	VirusTotal	Сервис, осуществляющий анализ подозрительных файлов и ссылок (URL) на предмет выявления вирусов, червей, троянов и всевозможных вредоносных программ.
3.	JSON	Текстовый формат обмена данными, основанный на JavaScript.
4.	Автоматический режим работы	Режим работы системы, в котором файлы и приложения, поступающие на интерфейс, автоматически загружаются в систему и анализируются на предмет нелегитимного поведения.
5.	Статическая аналитика	Категория анализа формируемая на основании индикаторов, зафиксированных при исследовании программного обеспечения статическим видом анализа.
6.	Экспертный режим работы	Режим работы системы, в котором пользователь, имеющий роль аналитика, самостоятельно загружает файл или приложение для анализа в системе.

2 Сокращения и значения

В настоящем документе используется перечень сокращений, представленный в таблице 2.

Таблица 2. Сокращения и значения

№	Сокращение	Значение
1.	API	Application programming interface
2.	URL	Uniform Resource Locator
3.	APM	Автоматизированное рабочее место

3 Назначение программы

Система комплексной антивирусной проверки программного обеспечения «Октопус» (далее – система Октопус) предназначена для усиления безопасности ИТ-инфраструктуры и развития профессиональных компетенций офицеров ИБ.

Система Октопус осуществляет проверку с помощью следующих методов:

- проверка программного обеспечения в более 20 локальных антивирусах;
- статический анализ файлов по различным форматам;
- проверка во внешних аналитических ресурсах;
- анализ определенных типов файлов в соответствующих нейронных сетях.

3.1 Основные возможности

Система Октопус принимает на проверку файлы из различных типов источников, которые включают в себя:

- веб-трафик (ICAP)
- почтовый трафик (SMTP)
- сетевой трафик
- мессенджеры
- сервера и рабочие станции
- ручная загрузка
- API и др.

Система Октопус поддерживает проверку следующих типов объектов:

- файлы
- архивы
- многотомные архивы
- запароленные файлы и архивы
- веб-ссылки
- мобильные приложения

Система Октопус принимает на анализ любые типы файлов, примеры:

- исполняемые файлы (EXE, ELF, CMD)
- офисные документы (DOCX, XLSX, PPTX, PDF, RTF)
- мобильные приложения (APK)
- архивы, включая многотомные и защищенные паролем (ZIP, JAR)
- скрипты (BAT, SH) и др.

3.2 Режимы работы

Система Октопус имеет два режима работы: автоматический и экспертный. Автоматический режим заключается в перехвате и проверке файлов из интернет-трафика, почтовых вложений, мобильных устройств и API. Экспертный режим позволяет загружать вручную любые файлы в систему, в т.ч. посредством telegram-bot.

Перед началом работы с системой Октопус у администратора необходимо получить логин и пароль от учетной записи пользователя.

4 Работа с серверным программным обеспечением

Для начала работы с системой Октопус необходимо в веб-браузере в адресной строке ввести URL, полученный у администратора, и осуществить переход на страницу авторизации.

В веб-браузере откроется страница авторизации (Рисунок 1).

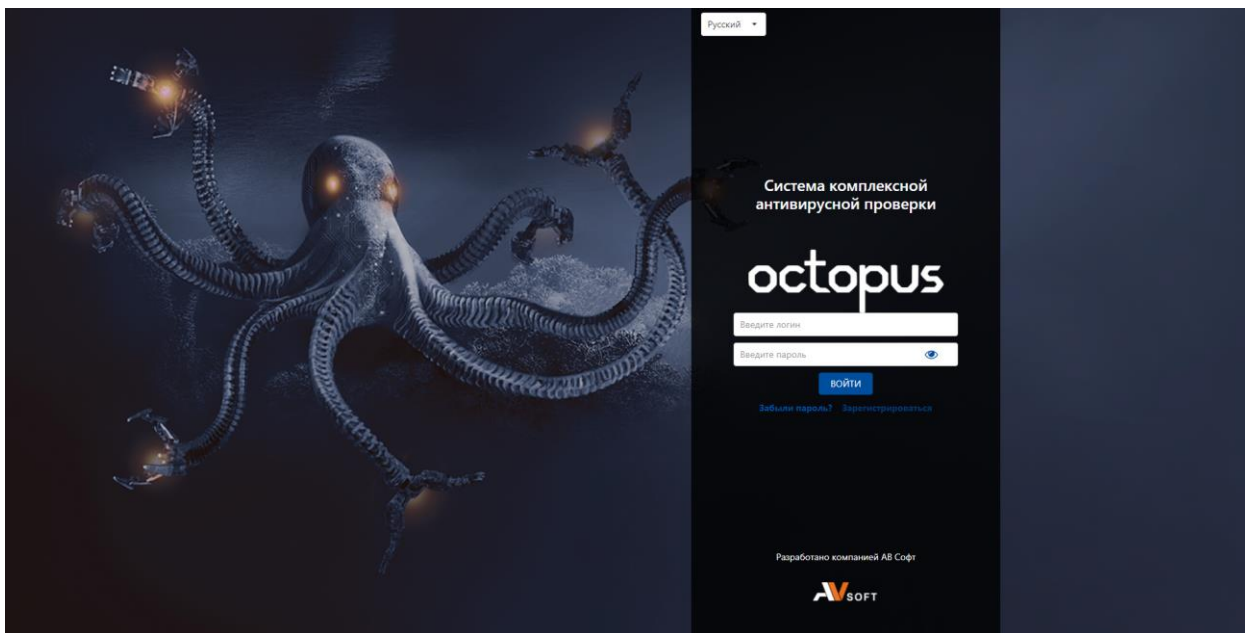


Рисунок 1. Страница авторизации пользователя в системе Октопус

Для авторизации в системе Октопус необходимо ввести логин и пароль учетной записи, полученные у администратора.

После прохождения авторизации осуществляется переход в веб - интерфейс системы, в котором присутствуют следующие разделы:

- Статистика;
- Источники;
- Объекты анализа;
- Исследования;
- Справочники;
- Настройки;
- Журналы.


Для смены языка необходимо нажать на выпадающее меню выбора языка.

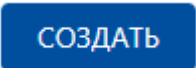




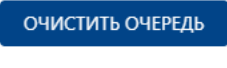
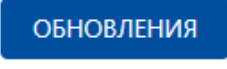
4.1 Элементы управления веб-интерфейсом

Описание, назначение и настройка по умолчанию элементов управления веб-интерфейсом системы Октопус представлены в таблице 3.

Таблица 3. Описание элементов управления интерфейсом

№	Элемент интерфейса	Назначение	Настройка по умолчанию	Изображение
1.	Значок «Выход»	Выполняет выход из системы	Активен	
2.	Значок «Календарь»	Выполняет переход в форму выбора даты	Активен	
3.	Значок «Личный кабинет»	Позволяет перейти в личный аккаунт пользователя в системе	Активен	
4.	Значок «Фильтр»	Выполняет переход в чек-бокс	Активен	
5.	Значок «Выпадающий список»	Позволяет выбрать язык отображения интерфейса	Русский язык	
6.	Значок «Руководство пользователя»	Выполняет загрузку руководства пользователя	Активен	
7.	Значок «Загрузить файл»	Выполняет загрузку файл на проверку	Активен	

№	Элемент интерфейса	Назначение	Настройка по умолчанию	Изображение
8.	Значок «Личный кабинет»	Выполняет переход в меню личного кабинета	Активен	
9.	Иконка «Отчет»	Отображение отчета по проверке веб-ссылки	Активна	
10.	Иконка «Копировать»	Выполняет копирование сущности	Активна	
11.	Кнопка «Обновить»	Обновление таблицы	Активна	
12.	Кнопка «Добавить»	Выполняет добавление новой сущности	Активна	
13.	Кнопка «Отменить»	Выполняет отмену действия	Активна	
14.	Кнопка «Загрузить»	Выполняет загрузку файла в систему на проверку	Активна	
15.	Кнопка «Выберите файл»	Выполняет выбор файла для загрузки в систему	Активна	
16.	Кнопка «Сохранить»	Выполняет сохранение изменений в системе	Активна	

№	Элемент интерфейса	Назначение	Настройка по умолчанию	Изображение
17.	Кнопка «Создать»	Выполняет создание новой сущности	Активна	
18.	Кнопка «Добавить»	Выполняет добавление новой сущности	Активна	
19.	Кнопка «Экспорт»	Выполняет экспорт объектов или параметров из системы	Активна	
20.	Кнопка «Импорт»	Выполняет импорт объектов или параметров в систему	Активна	
21.	Кнопка «Прервать активные»	Выполняет прерывание активных исследований в системе	Активна	
22.	Кнопка «Очистить очередь»	Выполняет очищение очереди исследований в системе	Активна	
23.	Кнопка «Обновления»	Выполняет переход в сервис обновлений	Активна	

№	Элемент интерфейса	Назначение	Настройка по умолчанию	Изображение
24.	Кнопка «Фильтр»	Дополнительный фильтр, который выполняет фильтрацию, если в поисковом поле таблицы введены данные	Неактивна	
25.	Кнопка «Экспортировать все»	Скачиваются в формате Excel	Скачиваются все данные в таблице	
26.	Кнопка переключатель	Переключение параметра	Включена	

Элементы управления веб-интерфейсом имеют всплывающие подсказки, которые отображают их названия.

5 Раздел «Статистика»

После авторизации пользователя отображается по умолчанию страница раздела «Статистика» (Рисунок 2).

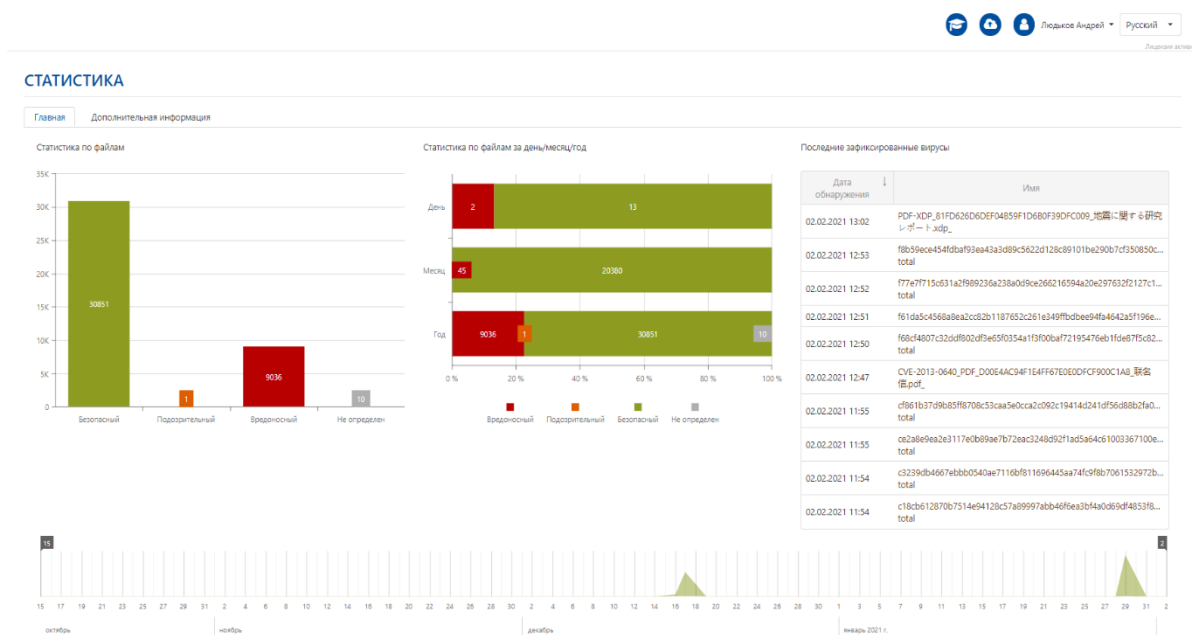


Рисунок 2. Раздел «Статистика»

Для входа в личный кабинет и выхода из системы необходимо нажать на иконку пользователя, далее отобразится выпадающее меню с общими настройками пользователя (Рисунок 3).

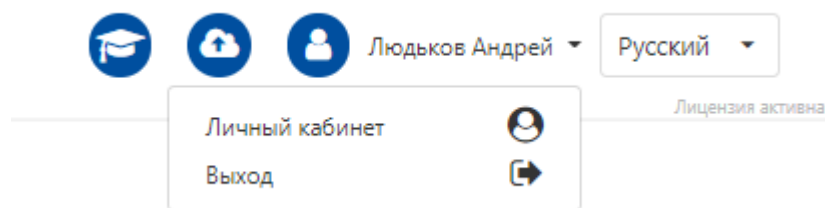


Рисунок 3. Общие настройки пользователя

Раздел «Статистика» имеет две вкладки:

- Главная;
- Дополнительная информация.

Во вкладке «Главная» (Рисунок 2) присутствует информация по следующей статистике:

- Статистика по файлам;
- Статистика по файлам за день, месяц, год;
- Последние зафиксированные вирусы.

Для задания периода необходимо переместить курсор на требуемый временной отрезок графика.

В графике «Статистика по файлам» все столбцы являются активными элементами, при нажатии на которые осуществляется переход в раздел «Файлы» с отфильтрованным списком выбранного столбца за определенный период времени, обозначенный на графике.

В таблице «Последние зафиксированные вирусы» в столбце «Имя» названия файлов являются активными ссылками, при нажатии на которые осуществляется переход в «Отчет по файлу».

Во вкладке «Дополнительная информация» (Рисунок 4) присутствуют следующие таблицы:

- Последние проверенные файлы.

СТАТИСТИКА

Главная	Дополнительная информация
---------	---------------------------

Последние проверенные файлы

Дата загрузки ↓	Имя	Вердикт
02.02.2021 11:06	52.rar	Безопасный
02.02.2021 11:06	53.rar	Безопасный
02.02.2021 11:06	51.rar	Безопасный
02.02.2021 11:06	42.rar	Вредоносный
02.02.2021 11:06	41.rar	Вредоносный
02.02.2021 11:06	43.rar	Безопасный
02.02.2021 11:06	31.rar	Безопасный
02.02.2021 11:06	32.rar	Безопасный
02.02.2021 11:06	33.rar	Безопасный
02.02.2021 11:06	12.rar	Безопасный

Рисунок 4. Вкладка «Дополнительная информация»

В таблице «Последние проверенные файлы» при нажатии на имя файла в колонке «Имя» осуществляется переход на страницу «Отчет по файлу», где отображается подробная информация по проверке выбранного файла.

6 Раздел «Источники»

6.1 Подраздел «WEB-трафик»

В разделе «WEB-трафик» (Рисунок 5) в таблице отображается вся информация по проверкам сетевого трафика в системе.

Дата создания ↓	Имя	Источник	Вердикт	Ссылка	Контрольная сумма (SHA-256)	Статус
28.10.2020 13:31	Литература.docx	10.1.0.1	Безопасный	https://wdho.ru/ht1?download_token=a2c004848d638fd12afcd0631d6334ef9...	b779746cc5dcabd2ca33032c576fee907f2f5c81ac1bb...	Завершено
16.09.2020 16:27	8520.615.05_pkedjkddefpdpbcmbmeomqbeemfm.crx	192.168.1.200	Безопасный	https://dl.google.com/chromewebstore/L2Nocm9tZV9le...d0e62ace64af6334330a7ac3a2cc657914feb3211f189ae1...	d0e62ace64af6334330a7ac3a2cc657914feb3211f189ae1...	Завершено
16.09.2020 16:27	04d69f7b1931e3e806e60c36c18940e35fec327eee4cdc4...	192.168.1.200	Безопасный	https://storage.googleapis.com/update-delta/pkedjkddefpdpbcmbmeomqbeemfm/8520.615...	04d69f7b1931e3e806e60c36c18940e35fec327eee4cdc4...	Завершено
16.09.2020 16:24	unknown	192.168.1.200	Безопасный	https://www.google.com/dl/release2/chrome_componen...6f1832a8e4528538343eb0c1a540fb9712465b04db0414...	6f1832a8e4528538343eb0c1a540fb9712465b04db0414...	Завершено
16.09.2020 16:24	unknown	192.168.1.200	Безопасный	https://www.google.com/dl/release2/chrome_componen...53f121779e9d9ade49cd4eedacbc7463c086731bd66c7d0...	53f121779e9d9ade49cd4eedacbc7463c086731bd66c7d0...	Завершено
16.09.2020 16:24	unknown	192.168.1.200	Безопасный	https://www.google.com/dl/release2/chrome_componen...3077031d412e29af82ba8b7177970c7954ef00499109015...	3077031d412e29af82ba8b7177970c7954ef00499109015...	Завершено
16.09.2020 16:23	unknown	192.168.1.200	Безопасный	https://www.google.com/dl/release2/chrome_componen...818c5905d8de1bbcac106066523b82c28d06c796e3afe24...	818c5905d8de1bbcac106066523b82c28d06c796e3afe24...	Завершено
16.09.2020 16:23	unknown	192.168.1.200	Безопасный	http://www.google.com/dl/release2/chrome_componen...cd5945a3467dbd4671460257d5e92ad2000a97cfc822c1...	cd5945a3467dbd4671460257d5e92ad2000a97cfc822c1...	Завершено
16.09.2020 16:23	unknown	192.168.1.200	Безопасный	https://dl.google.com/release2/chrome_component/APV...e408c18b4d5b822f17a91e6091684a225c5233e056045e0...	e408c18b4d5b822f17a91e6091684a225c5233e056045e0...	Завершено
16.09.2020 16:23	unknown	192.168.1.200	Безопасный	https://dl.google.com/release2/chrome_component/APV...f1f6b41d7b129533565dd1493af940fa31c6edbe8205162...	f1f6b41d7b129533565dd1493af940fa31c6edbe8205162...	Завершено

Рисунок 5. Редактирование аналитики.

В таблице в колонке «Имя» все имена файлов являются активными ссылками, при нажатии на которые осуществляется переход в отчет по выбранному файлу.

! Для настройки WEB-трафика вам необходимо обратиться к администратору системы.

6.2 Подраздел «Почтовый трафик»

На странице «Почтовый трафик» (Рисунок 6) в таблице можно посмотреть информацию по всем электронным письмам с вложениями и ссылками.

Дата	Получатель	Отправитель	ID	Тема	Количество вложенных файлов	Количество вложенных ссылок	Статус	Вердикт
26.11.2020 18:49	convert_on_notif_on@avsw...	Testing <a.ludkov@avsw.ru>	c2b219420ca6832a12c07fb...	https://atfish.weebly.com/	3	1	Завершено	Вредоносный
26.11.2020 17:33	vip@avsw.ru	Testing <a.ludkov@avsw.ru>	70d1a5b3b8f227765b40b8...	!@#%'^&*()_+	3	0	Завершено	Безопасный
26.11.2020 16:24	admin2@avsw.ru	Testing <a.ludkov@avsw.ru>	07da69da800aad3b91d4c3...	tema	3	0	Завершено	Безопасный
26.11.2020 16:11	admin2@avsw.ru	Anvar <anvar@test.ru>	fec553399411d2111cc4fa...	Fwd: Re: Fwd: C вредоносным вложением	2	9	Завершено	Вредоносный
26.11.2020 15:52	admin2@avsw.ru	Anvar <anvar@test.ru>	aed51eb5424c37a476a8d1...	Fwd: Re: Fwd: C вредоносным вложением	2	9	Завершено	Вредоносный
26.11.2020 15:35	admin2@avsw.ru	Testing <a.ludkov@avsw.ru>	b336edc53cd672e7660b8b...	1m try	1	1	Завершено	Вредоносный
26.11.2020 15:31	admin2@avsw.ru	Testing <a.ludkov@avsw.ru>	6483930:153c6e2fe307cefb...	aaaaaa	3	0	Завершено	Безопасный
26.11.2020 15:23	admin2@avsw.ru	Testing <a.ludkov@avsw.ru>	f959f9c5a4904ca63558e32...	проверка	3	1	Завершено	Вредоносный
26.11.2020 15:18	admin2@avsw.ru	Testing <a.ludkov@avsw.ru>	2259f62727aca638ebd56b8...	testing	4	0	Завершено	Безопасный
25.11.2020 14:05	only_pdf_notif_on@avsw.ru	Testing <a.ludkov@avsw.ru>	1da8bd765ea8d3465af467...	123	2	0	Завершено	Безопасный

Рисунок 6. Раздел «Почтовый трафик»

В колонке «Статус» отображается статус проверки письма в системе, он может принимать следующие значения:

- В процессе (вложения или ссылки проходят проверку в системе);
- Завершено (проверка вложений или ссылок завершилась в системе).

В колонке «Вердикт» присутствует вердикт проверки письма в системе, он может принимать следующие значения:

- Не определен (необходимо обратиться к администратору системы);
- Безопасный;
- Подозрительный;
- Вредоносный.

Для просмотра информации по проверке каждого файла в письме необходимо нажать на кнопку «Отчет», далее осуществится переход на страницу «Отчет по почтовому трафику» (Рисунок 7).

ОТЧЕТ ПО ПОЧТОВОМУ ТРАФИКУ

Отправитель: Testing <a.ludkov@avsw.ru> Тема: 123

ID: d091c1a14711125d7095860f07756d26b8ef7045b41355934c08ef17b802d2 Доставлено:

Заголовки: Return-Path: <a.ludkov@avsw.ru>
X-Original-To: convert_on_notif_on@avsw.ru
Delivered-To: root@postcatcher
Received: from [192.168.10.62] (unknown [192.168.10.62])
by postcatcher (Postfix) with ESMTP id c93b72800A41
for <convert_on_notif_on@avsw.ru>; Thu, 3 Dec 2020 15:02:47 +0300 (MSK)
To: convert_on_notif_on@avsw.ru
From: Testing <a.ludkov@avsw.ru>
Subject: 123
Message-ID: <272dde24-f80-2342-ce32-2b4aee3014e8@avsw.ru>

Вложения:	Имя файла	Контрольная сумма (SHA-256)	Статус	Вердикт
	s1.docx	c03cae2a17369e06456c4437d4110ab993120f0eabd7cd1cb8358c462e...	Исследован статически	Безопасный
	s2.xlsx	082ac68eaa48828b3ee47b7ccb78a2966e3c57209f8aae30618c4a56e...	Исследован статически	Безопасный
	s3.pptx	f0cb906f4c0a93f31d3c56c5344e8dabcb930fc7362487f9157da37b63...	Исследован статически	Безопасный

Ссылки:	Ссылка	Контрольная сумма (SHA-256)	Статус	Вердикт
	https://appurl.io/cajZpjkLi	88f49e706942cd4e4cfd7b11a936a5f9f13df14d2101416537ee5882e7a...	Проверена	Вредоносный

Рисунок 7. Просмотр почтовых вложений

В отчете по почтовому трафику отображается информация по письму, а именно:

- Отправитель;
- Тема письма;
- Уникальный идентификатор письма.

В строке «Доставлено» отображается информация по доставке письма получателю, которая может иметь следующий статус:

- Доставлено;
- Не доставлено (необходимо обратиться к администратору системы).

В раскрывшейся таблице отображается информация по прикрепленным файлам. В столбце «Статус» присутствует статус проверки, он может принимать следующие значения:

- Исследован статически (файл был проверен только статическим методом анализа);
- Недоступен (файл не был проверен системой, необходимо обратиться к администратору).

В столбце «Вердикт» отображается вердикт проверки в системе каждого файла, прикрепленного к письму, он может принимать следующие значения:

- Не определен (необходимо обратиться к администратору системы);
- Безопасный;
- Подозрительный;
- Вредоносный.

Для обновления таблицы почтового трафика вручную необходимо воспользоваться кнопкой «Обновить».

Для экспорта таблицы почтового трафика необходимо воспользоваться кнопкой «Экспортировать все».

Чтобы посмотреть подробную информацию по проверенному файлу необходимо нажать на иконку «Отчет», далее осуществится переход на страницу «Отчет по файлу» (Рисунок 8).

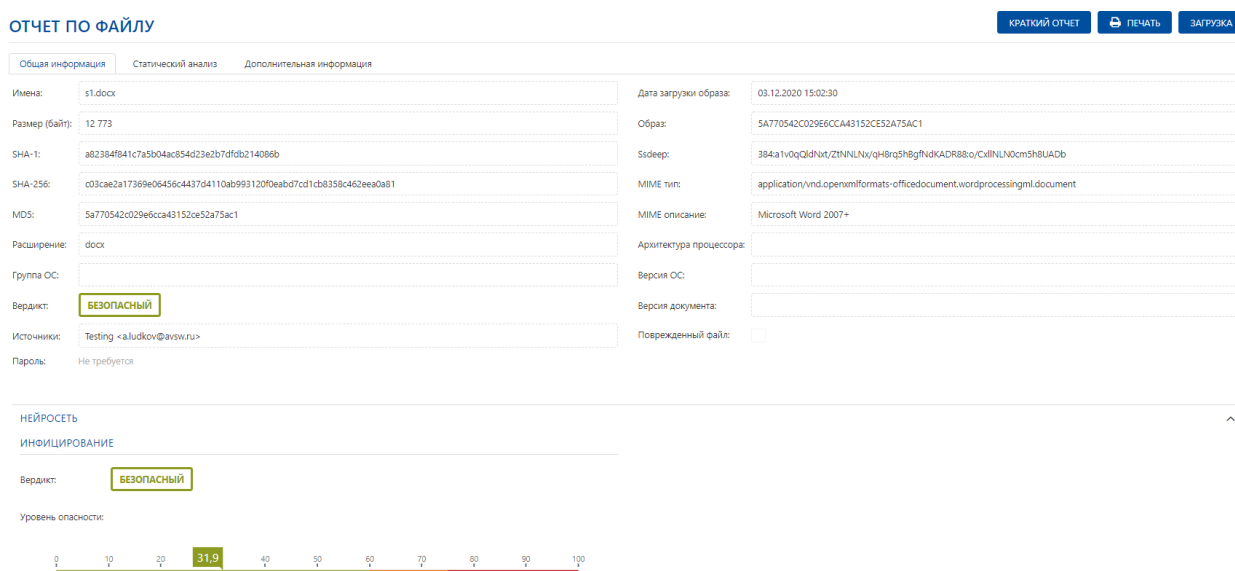


Рисунок 8. Отчет по файлу

7 Раздел «Объекты анализа»

7.1 Подраздел «Файлы»

Раздел «Файлы» (Рисунок **Error! Reference source not found.**) содержит все файлы, загруженные в систему Октопус из любых источников (веб-трафик, почтовый трафик, посредством API или вручную аналитиком).

ФАЙЛЫ

ЗАГРУЗИТЬ

Страница 1 из 3990 (Всего элементов: 39900) < 1 2 3 4 5 ... 3990 >

Перетащите столбец сюда, чтобы сгруппировать по нему

Автообновление Да

Дата загрузки	Имя	Приложение	Группа ОС	Тип	Контрольная сумма	Источник	Описание источника	Статус	Теги	Вердикт	
03.02.2021 16:30	s1.docx	Не определена	(Все)	Офисный документ	f083c54f06ac5cff6502f0c58...	Пользователь	Людков Андрей	Исследован статически		Безопасный	
03.02.2021 11:30	1.png	Не определена	(Все)	Не определен	789e05d91c03f644bbe723a...	Пользователь	ГАИ	Исследован статически		Безопасный	
02.02.2021 11:06	52.rar	Не определена	(Все)	Архив	f3c1eec00062724276821ae0...	Пользователь	Захарова Дарья	Исследован статически		Безопасный	
02.02.2021 11:06	53.rar	Не определена	(Все)	Архив	d9446ab24fceebb16dfb9ba...	Пользователь	Захарова Дарья	Исследован статически		Безопасный	
02.02.2021 11:06	51.rar	Не определена	(Все)	Архив	92155a1e6793806281f43d6...	Пользователь	Захарова Дарья	Исследован статически		Безопасный	
02.02.2021 11:06	42.rar	Не определена	(Все)	Архив	3fd54654f1410b5bc0bca934...	Пользователь	Захарова Дарья	Исследован статически	jsautolike-q [trj]	Вредоносный	
02.02.2021 11:06	41.rar	Не определена	(Все)	Архив	08270baf44ed7323056ec0...	Пользователь	Захарова Дарья	Исследован статически	win32:evogen [susp]	Вредоносный	
02.02.2021 11:06	43.rar	Не определена	(Все)	Архив	546eb30009d95974a892aed...	Пользователь	Захарова Дарья	Исследован статически		Безопасный	
02.02.2021 11:06	31.rar	Не определена	(Все)	Архив	aa855a356375460483cfa62...	Пользователь	Захарова Дарья	Исследован статически		Безопасный	
02.02.2021 11:06	32.rar	Не определена	(Все)	Архив	068603395d440013418536e...	Пользователь	Захарова Дарья	Исследован статически		Безопасный	

Страница 1 из 3990 (Всего элементов: 39900) < 1 2 3 4 5 ... 3990 >

Рисунок 9. Раздел «Файлы»

Для загрузки файла в систему необходимо нажать на кнопку «Загрузить» или иконку «Загрузить файл», которая находится рядом со входом в личный кабинет, далее появится форма «Загрузка файлов», в которой надо выбрать файл для загрузки и нажать кнопку «Загрузить» (Рисунок 10).

ЗАГРУЗКА ФАЙЛОВ

ВЫБЕРИТЕ ФАЙЛ или Перетащите файл сюда

ЗАГРУЗИТЬ

s1.docx 12 кБ
Готово к загрузке

Рисунок 10. Загрузка файла в систему

Для удаления файла из списка загрузки необходимо нажать кнопку удаления напротив конкретного файла.

Если файл уже был ранее загружен в систему, то пользователю выводится оповещение об этом (Рисунок **Error! Reference source not found.**).

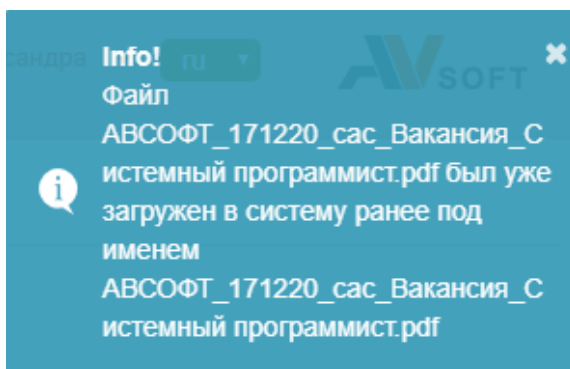


Рисунок 11. Оповещение пользователя о присутствии загружаемого файла в системе

Для просмотра информации о файле необходимо нажать на иконку «Отчет», далее осуществится переход на подробный отчет по файлу (Рисунок **Error! Reference source not found.**).

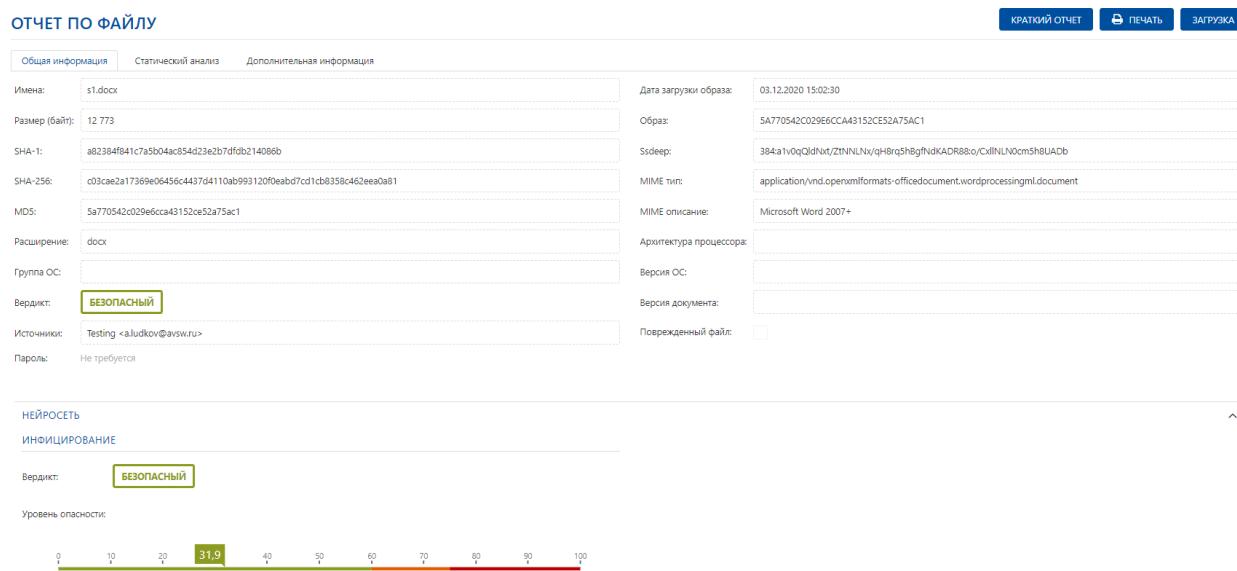


Рисунок 12. Отчет по файлу

Для печати и экспортирования данных в отчете по файлу необходимо нажать кнопку «Печать».

Для загрузки файла из системы необходимо нажать кнопку «Загрузить» на странице отчета.

В отчете по файлу присутствуют следующие вкладки:

- Общая информация;
- Статистический анализ;
- Дополнительная информация.

Во вкладке «Общая информация» присутствуют общие данные по файлу, вердикт и история вердиктов (Рисунок 12).

Во вкладке «Статический анализ» присутствует информация по всем статическим проверкам файла, а также кнопка запуска статического исследования (**Error! Reference source not found.**).

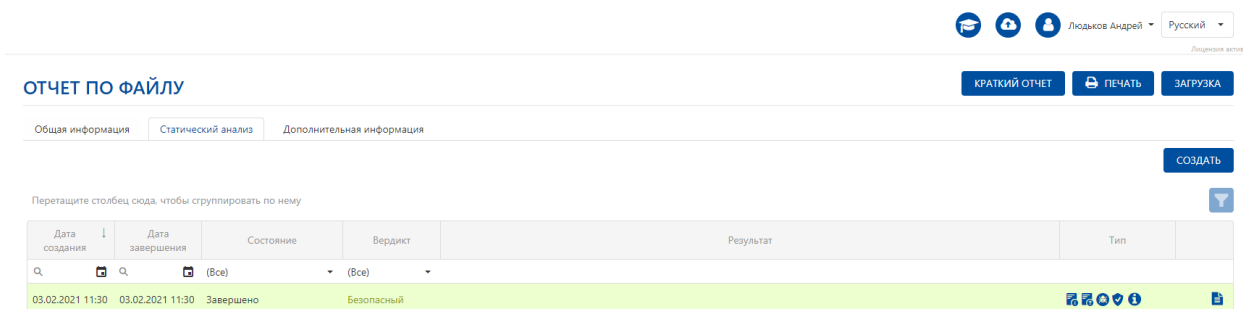


Рисунок 13. Вкладка «Статический анализ» в отчете по файлу

В таблице статического анализа присутствует информация о состоянии конкретной сессии статической проверки в колонке «Состояние», которая может принимать следующие статусы:

- В очереди;
- Выполняется;
- Анализ данных;
- Ошибка;
- Завершено;
- Отменено;
- Архивируется;
- В архиве;
- Анализ YARA-правил;
- Анализ ссылок.

Также в таблице статического анализа присутствует информация по вердикту конкретной статической проверки в колонке «Вердикт», который может принимать следующие значения:

- Не определен (необходимо обратиться к администратору системы);
- Безопасный;
- Подозрительный;
- Вредоносный.

Во вкладке «Дополнительная информация» присутствует полная информация по файлу (Рисунок 14).

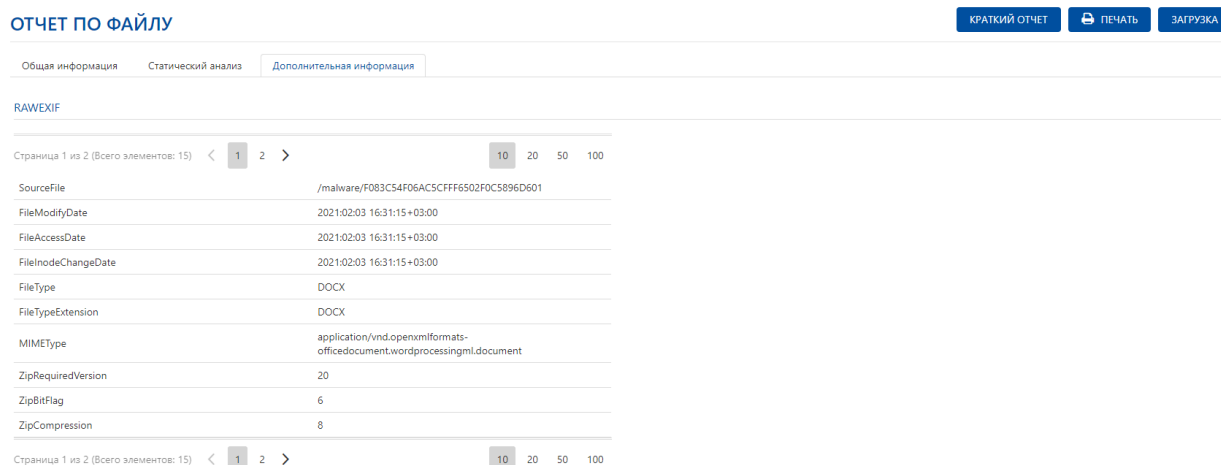


Рисунок 14. Вкладка «Дополнительная информация» в отчете по файлу

7.2 Подраздел «Ссылки»

Раздел «Ссылки» содержит все ссылки, которые были добавлены в систему на проверку (Рисунок 15).

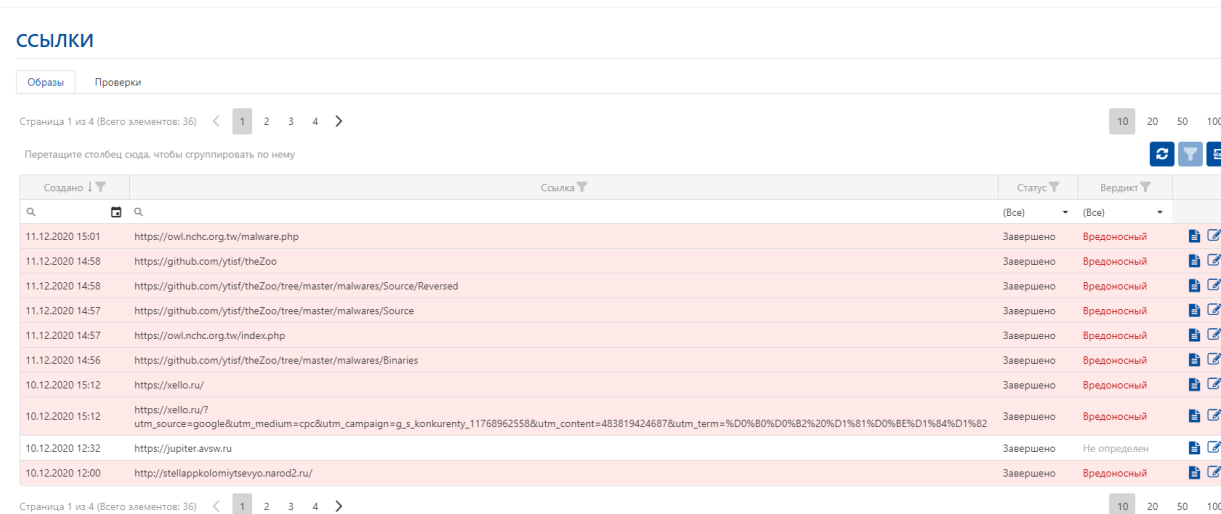


Рисунок 15. Страница «Ссылки»

Для экспорта таблицы ссылок необходимо воспользоваться кнопкой «Экспортировать все».

Для обновления таблицы ссылок вручную необходимо воспользоваться кнопкой «Обновить».

Для загрузки ссылки в систему необходимо перейти во вкладку «Проверки» и нажать на кнопку «Добавить ссылку» (Рисунок **Error! Reference**

source not found.), далее появится форма «Ссылка», в которой надо выбрать ссылку для загрузки и нажать кнопку «Сохранить».

ССЫЛКА

Ссылка: *

Принудительное исследование: Нет

СОХРАНИТЬ

Рисунок 16. Добавление новой ссылки

8 Раздел «Исследования»

Раздел «Исследования» (Рисунок 17) содержит следующие вкладки:

- Статические;
- Ссылки.

ИССЛЕДОВАНИЯ

Статические Ссылки

СОЗДАТЬ

Страница 1 из 20132 (Всего элементов: 201314) < 1 2 3 4 5 ... 20132 >

Перегадите столбец сюда, чтобы сгруппировать по нему

Автообновление

ID	Дата проверки	Дата завершения	Источник	Файл	Режим	Состояние	Вердикт	Результат	Сценарий	Тип
252991	03.02.2021 17:36	03.02.2021 17:53	Debug file checker	conf_board.pdf	Молния	Завершено	Безопасный	Динамический анализ неактивен		
252990	03.02.2021 17:36	03.02.2021 17:53	Debug file checker	conenza.pdf	Молния	Завершено	Безопасный	Динамический анализ неактивен		
252989	03.02.2021 17:36	03.02.2021 17:53	Debug file checker	connectad.pdf	Молния	Завершено	Безопасный	Динамический анализ неактивен		
252988	03.02.2021 17:36	03.02.2021 17:53	Debug file checker	condydca.pdf	Молния	Завершено	Безопасный	Динамический анализ неактивен		
252987	03.02.2021 17:36	03.02.2021 17:53	Debug file checker	conduitusa.pdf	Молния	Завершено	Безопасный	Динамический анализ неактивен		
252986	03.02.2021 17:36	03.02.2021 17:53	Debug file checker	conduit.pdf	Молния	Завершено	Безопасный	Динамический анализ неактивен		
252985	03.02.2021 17:36	03.02.2021 17:53	Debug file checker	CONDUIT_I804.pdf	Молния	Завершено	Безопасный	Динамический анализ неактивен		
252984	03.02.2021 17:36	03.02.2021 17:53	Debug file checker	condizioni-general-di-servizio-posteD-1-9.pdf	Молния	Завершено	Безопасный	Динамический анализ неактивен		
252983	03.02.2021 17:36	03.02.2021 17:53	Debug file checker	conditions_reduction_grat...	Молния	Завершено	Безопасный	Динамический анализ неактивен		
252982	03.02.2021 17:36	03.02.2021 17:53	Debug file checker	Conditions.pdf	Молния	Завершено	Безопасный	Динамический анализ неактивен		

Страница 1 из 20132 (Всего элементов: 201314) < 1 2 3 4 5 ... 20132 >

Рисунок 17. Раздел «Исследования»

Раздел «Исследования» содержит все статические исследования в системе Октопус из любых источников (почтовый трафик, веб-трафик, посредством API или созданные вручную аналитиком).

Для автообновления таблицы статических исследований необходимо воспользоваться переключателем «Автообновление».

Для обновления таблицы статических исследований вручную необходимо воспользоваться кнопкой «Обновить».

Для экспорта таблицы статических исследований необходимо воспользоваться кнопкой «Экспортировать все».

Для создания статического исследования в системе необходимо выполнить следующие шаги:

1. Нажать кнопку «Создать».
2. Выбрать необходимый файл для исследования (Рисунок 18).

СОЗДАНИЕ ИССЛЕДОВАНИЯ

Файл

s1.docx

Тип статического исследования: *

Информация о файле × Тип файла × Антивирусы × VirusTotal ×
Дополнительная информация ×

Проверка на VirusTotal: *

Контрольная сумма × Файл ×

Пароли:

ЗАПУСТИТЬ

Рисунок 18. Окно создания нового статического исследования

3. Выбрать тип статического исследования.
4. Выбрать тип проверки на ресурсе «VirusTotal».
5. После выбора всех параметров нажимаем на кнопку «Запустить».

Созданное исследование отобразится в таблице статических исследований.

Для просмотра отчета по статическому исследованию необходимо нажать на иконку «Отчет» в таблице исследований. Далее осуществится переход на страницу «Отчет по статическому исследованию» (Рисунок 19).

ОТЧЕТ ПО СТАТИЧЕСКОМУ ИССЛЕДОВАНИЮ (ID: 51373) ПЕЧАТЬ ПОЛУЧИТЬ JSON

Общая информация | Аналитики | Yara-правила | Антивирусы | Нейронная сеть | Ошибки | **Дополнительная информация 2**

Файл:	0042C6A5421AEF9D81C05FDA62C55500	Версия документа:	
Вердикт:	ВРЕДНОСНЫЙ	Вердикт Wildfire:	ВРЕДНОСНЫЙ
MIME тип:	application/x-dosexec	SHA-256:	652e886d4d40cca927c7c50f698208c186dda12287c524ff91d4bbe280448675
MIME описание:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows	SHA-1:	09c70b7e429518806c4cb6850dcb7bdd8ad2d75e
Расширение:	dll	MD5:	0042c6a5421aef9d81c05fda62c55500
Язык:	0409	Группа ОС:	Windows
Ssdeep:	6144:ST5ArblGreJAItMSjGy3PSTRdFDWoblYbRbP0S4:c5UIGrelMstE7H	Версия ОС:	5.2
TrID:	82.0% (.EXE) Win64 Executable (generic) (27624/17/4),6.0% (.EXE) OS/2 Executabl	Архитектуры:	x64
Теги:	Исполняемый файл	Режим системы:	Полный анализ
Пароль:	Не требуется		

Рисунок 19. Отчет по статическому исследованию

В «Отчете по статическому исследованию» присутствуют вкладки:

- Общая информация;
- Аналитики;
- YARA- правила;
- Антивирусы;
- Нейронная сеть;
- Ошибки;
- Дополнительная информация.

Во вкладке «Аналитики» показаны аналитики, которые сработали при проверке файла (Рисунок 20).

ОТЧЕТ ПО СТАТИЧЕСКОМУ ИССЛЕДОВАНИЮ (ID: 51373) ПЕЧАТЬ ПОЛУЧИТЬ JSON

Общая информация | **Аналитики** | Yara-правила | Антивирусы | Нейронная сеть | Ошибки | **Дополнительная информация 2**

Перетяните столбец сюда, чтобы сгруппировать по нему ▼

Аналитика	Описание	Вес	Вердикт ↓
Импорты: Функции снимка экрана	Присутствуют функции способные делать снимки экрана	0	Не определен
Импорты: Работа с реестром	Импорты: Работа с реестром	0	Не определен

Рисунок 20. Вкладка «Аналитики» в отчете по статическому анализу файла

Во вкладке «Yara-правила» присутствует информация по сработавшим Yara-правилам (Рисунок 21).

ОТЧЕТ ПО СТАТИЧЕСКОМУ ИССЛЕДОВАНИЮ (ID: 51373) ПЕЧАТЬ ПОЛУЧИТЬ JSON

Общая информация Аналитики **Yara-правила** Антивирусы Нейронная сеть Ошибки Дополнительная информация ²

Перетащите столбец сюда, чтобы сгруппировать по нему ▼

Аналитика	Описание	Вердикт ↓
(Все) ▼		
Нет данных		

Рисунок 21. Вкладка «Yara-правила» в отчете по статическому исследованию

Во вкладке «Антивирусы» присутствует информация по вердиктам всех локальных антивирусов, зарегистрированных в системе (Рисунок 22).

ОТЧЕТ ПО СТАТИЧЕСКОМУ ИССЛЕДОВАНИЮ (ID: 51373) ПЕЧАТЬ ПОЛУЧИТЬ JSON

Общая информация Аналитики Yara-правила **Антивирусы** Нейронная сеть Ошибки Дополнительная информация ²

Перетащите столбец сюда, чтобы сгруппировать по нему ▼

Антивирус ▼	Версия ▼	Версия вирусной базы ▼	Дата вирусной базы ▼	Комментарий ▼	Вердикт ↓ ▼
Windows Defender	1.1.16500.1	1.305.3321.0	04.12.2019, 00:00		Безопасный
Avira	8.3.52.166	7.15.18.172		Adware/BrowseFox.aox	Вредоносный
F-Secure	1.0 build 0069	2020-09-01_08	01.09.2020, 00:00		Безопасный
ClamAV	0.102.3	25955	12.10.2020, 00:00	Win.Adware.Swiftbrowse-346	Вредоносный
Avast	3.0.3			Win32:BrowseFox-EA [PUP]	Вредоносный
NOD32 Endpoint Security	4.5.3			Срок действия лицензии истёк	Не определен
Zoner	1.3.0	3107100	18.10.2018, 00:00		Безопасный
Sophos	3.79.0	5.78	08.09.2020, 00:00		Безопасный
DrWeb	7.00.33.06080	7304508	13.10.2020, 00:00	Срок действия лицензии истёк	Не определен
Trend Micro				Срок действия лицензии истёк	Не определен
Panda					Безопасный
Symantec	14.2 MP1	151.14.39	23.07.2019, 00:00	PUA.Yontoo.C	Вредоносный
AVG	13.0.3114	4793/15883	14.08.2018, 00:00		Безопасный
Kaspersky				not-a-virus:AdWare.Win32.SwiftBrowse....	Вредоносный
F-PROT	4.6.5.141	202010121930	12.10.2020, 00:00		Безопасный
eScan	7.86229	11611051	12.10.2020, 00:00	Adware.SwiftBrowse.CN(DB)	Вредоносный
Comodo				ApplicUnwnt	Вредоносный
McAfee	6.0.6.653	9772	12.10.2020, 00:00		Безопасный
NOD32 Desktop	4.0.90	20644	09.01.2020, 00:00	Win64/Adware.BrowseFox.D application	Вредоносный
BitDefender	7.86228	11611156	12.10.2020, 00:00	Сканирование не удалось, вероятно срок действия лицензии истёк	Не определен

Рисунок 22. Вкладка «Антивирусы» в отчете по статическому анализу файла

В таблице локальных антивирусов присутствует информация по вердикту каждого антивируса в колонке «Вердикт», который может принимать следующие значения:

- Не определен (необходимо обратиться к администратору системы);

- Безопасный;
- Подозрительный;
- Вредоносный.

Во вкладке «Нейронная сеть» указан вердикт файла после прохождения проверки с помощью нейронных сетей (Рисунок 23).

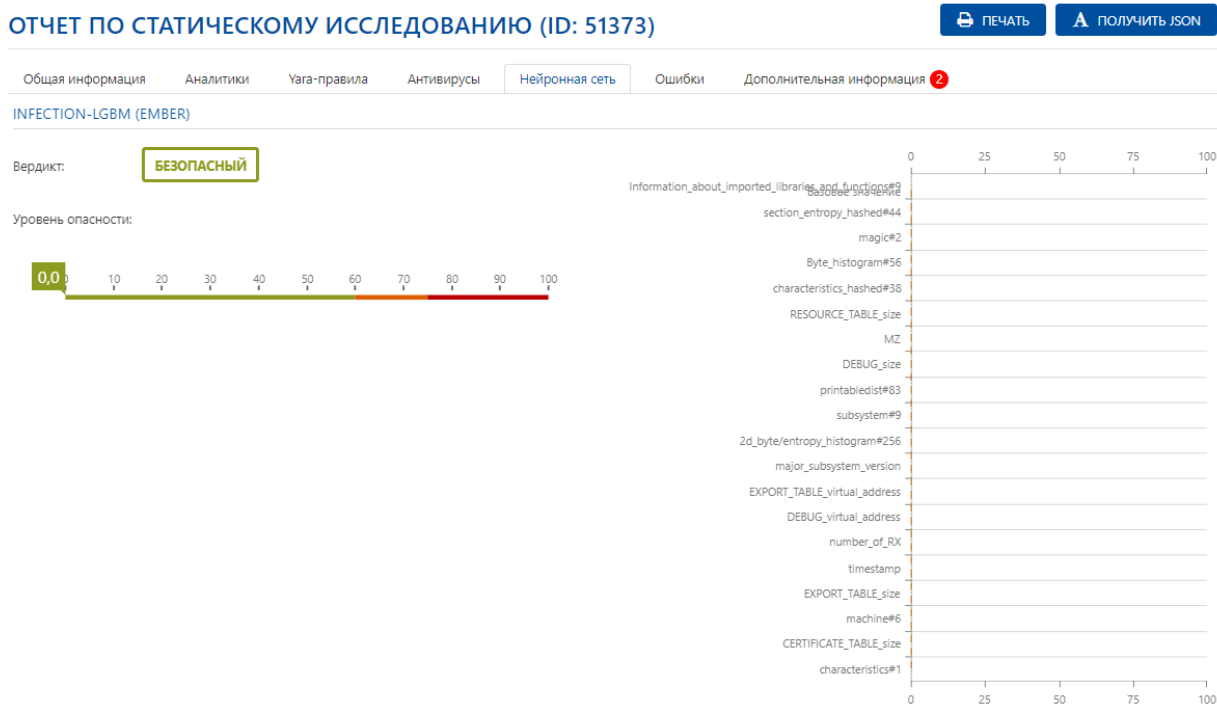


Рисунок 23. Вкладка «Нейронная сеть» в отчете по статическому анализу файла

Во вкладке «Ошибки» присутствует информация по ошибкам в работе антивирусных лицензий (Рисунок 24).

ОТЧЕТ ПО СТАТИЧЕСКОМУ ИССЛЕДОВАНИЮ (ID: 51373) ПЕЧАТЬ ПОЛУЧИТЬ JSON

Общая информация Аналитики Яга-правила Антивирусы Нейронная сеть **Ошибки** **Дополнительная информация 2**

Модуль	Сообщение
bitdefender	Сканирование не удалось, вероятно срок действия лицензии истёк
nod32_2	Срок действия лицензии истёк
drweb	Срок действия лицензии истёк
trendmicro	Срок действия лицензии истёк

Рисунок 24. Вкладка «Ошибки» в отчете по статическому анализу файла

Если во вкладке «Ошибки» отображаются ошибки по работе антивирусов, то необходимо обратиться к администратору системы.

Во вкладке «Дополнительная информация» присутствует подробная информация по соответствующему типу файла, включая результаты работы утилиты ExifTool (Рисунок 25).

ОТЧЕТ ПО СТАТИЧЕСКОМУ ИССЛЕДОВАНИЮ (ID: 51373) [ПЕЧАТЬ] [ПОЛУЧИТЬ JSON]

Общая информация | Аналитики | Yara-правила | Антивирусы | Нейронная сеть | Ошибки | **Дополнительная информация** 2

ИНФОРМАЦИЯ О РЕЗУЛЬТАТЕ

Резюме | Информация заголовков | Импорты/Экспорты | Секции | Ресурсы | Строки | Плагины | Цифровая подпись

Imphash: d559cb5fa36cd7eb2b80c182b04e6e25

Резюме:

Страница 1 из 2 (Всего элементов: 11) < 1 2 > 10 20 50 100

Архитектура	IMAGE_FILE_MACHINE_AMD64
Дата компиляции	2014-Oct-22 12:30:34
Обнаруженные языки	English - United States
Имя компании, которая создала файл	TODO: <Company name>
Файловый дескриптор	TODO: <File description>
Версия файла	3.1.0.6
Внутреннее имя	XTLS.dll
Копирайт	TODO: (c) <Company name>. All rights reserved.
Имя, с которым создали файл	XTLS.dll
Название продукта, с которым распространяется файл	XVRNT

Страница 1 из 2 (Всего элементов: 11) < 1 2 > 10 20 50 100

Рисунок 25. Вкладка «Дополнительная информация» в отчете по статическому анализу файла

Для печати и экспортирования данных в отчете по файлу необходимо нажать кнопку «Печать».

Для получения информации о файле в формате JSON необходимо нажать кнопку «Получить JSON».

Чтобы посмотреть информацию об исследовании ссылки, в разделе «Исследования» переходим во вкладку «Ссылки» после чего необходимо нажать на иконку «Отчет». Далее осуществится переход на страницу «Отчет по исследованию ссылки» (Рисунок 26).



Рисунок 26. Отчет по исследованию ссылки

В отчете по исследованию ссылки отображается таблица с результатами проверок на нескольких ресурсах, а также присутствует вердикт от нейронных сетей.

9 Раздел «Справочники»

В разделе «Справочники» (Рисунок 27) присутствуют следующие подразделы справочников:

- Системные;
- Аналитические.

СПРАВОЧНИКИ

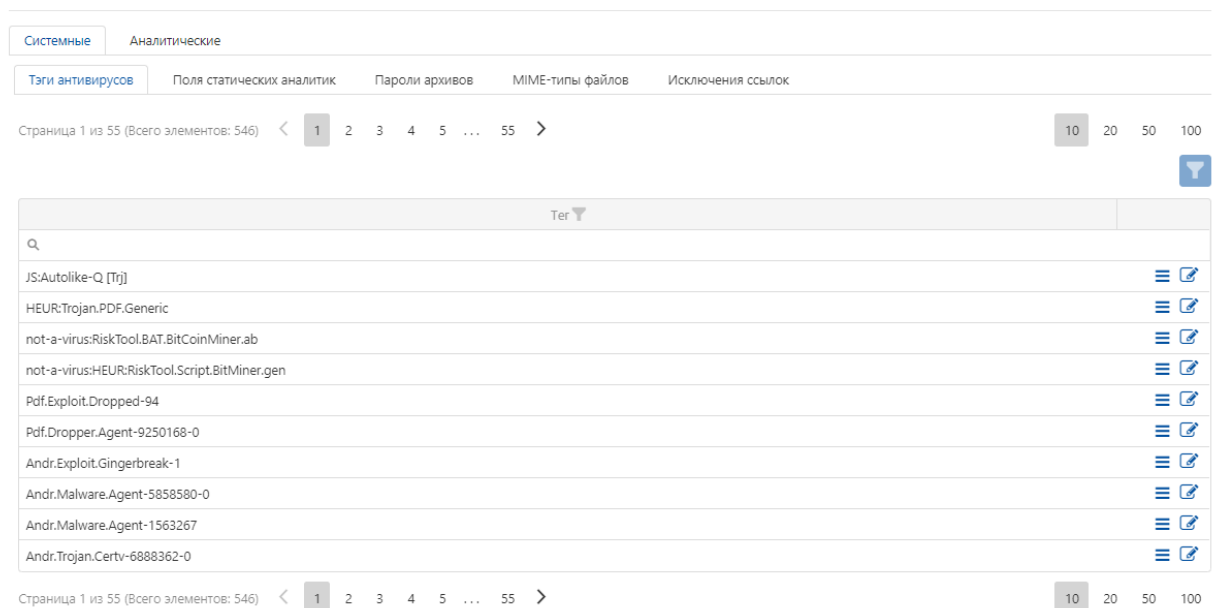


Рисунок 27. Раздел «Справочники-Системные»

В группе системных справочников (Рисунок 27) присутствуют следующие общесистемные справочники:

- Тэги антивирусов (список сигнатур вирусов);
- Поля статических аналитик;
- Пароли архивов (пароли, используемые для загружаемых архивов);
- MIME-типы файлов;
- Исключения (список исключений ссылок).

В группе аналитических справочников присутствуют следующие справочники, используемые для анализа:

- Статические аналитики (содержит аналитики, которые определяют вердикт файла в статическом анализе);
- Правила Yara.

Для добавления новой статической аналитики необходимо нажать кнопку «Добавить строку» в разделе Справочники-Аналитические-Статические аналитики, далее осуществится форма для заполнения «Создание статической аналитики» (Рисунок 28).

СОЗДАНИЕ СТАТИЧЕСКОЙ АНАЛИТИКИ

Название: * Вес: * 1

Вердикт: * Описание: *

Фильтр: * И +

Фильтр: *

ОБНОВИТЬ ФИЛЬТР

СОХРАНИТЬ

Рисунок 28. Форма добавления статической аналитики

В разделе создания аналитики необходимо указать следующие параметры:

- Название (наименование аналитики);
- Вес (уровень опасности аналитики от 1 до 10);
- Описание (краткое описание аналитики с обоснованием веса);
- Вердикт (принудительное определение типа угрозы для аналитики).

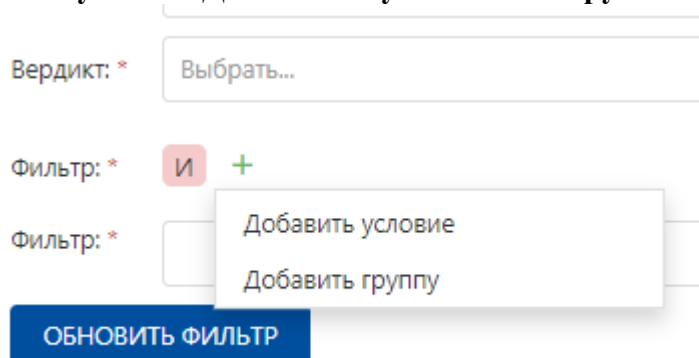
Фильтр представлен в виде древовидной структуры данных. В данной структуре узлами являются логические условия, её ветвями являются операции над данными.

Возможные значения узлов:

- И;
- ИЛИ;
- НЕ И;
- НЕ ИЛИ.

Создание фильтра начинается с выбора логической операции для корневого узла. После выбора предоставляется возможность добавить условие или группу. (Рисунок 29)

Рисунок 29. Добавление условия или группы



При добавлении условия необходимо выбрать нужное поле, задать условие поиска путём выбора нужной операции и ввести данные для сравнения (Рисунок 30).

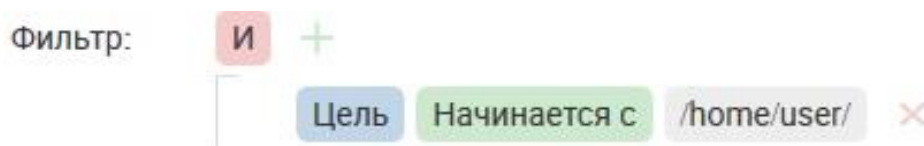


Рисунок 30. Пример добавления одного условия фильтра

При добавлении группы, необходимо сначала выбрать логическую операцию для создаваемого узла. После этого, используя операции, необходимо добавить ветвь (Добавить условие) или добавить узел (Добавить группу), продолжить построение дерева аналитик (Рисунок 31).

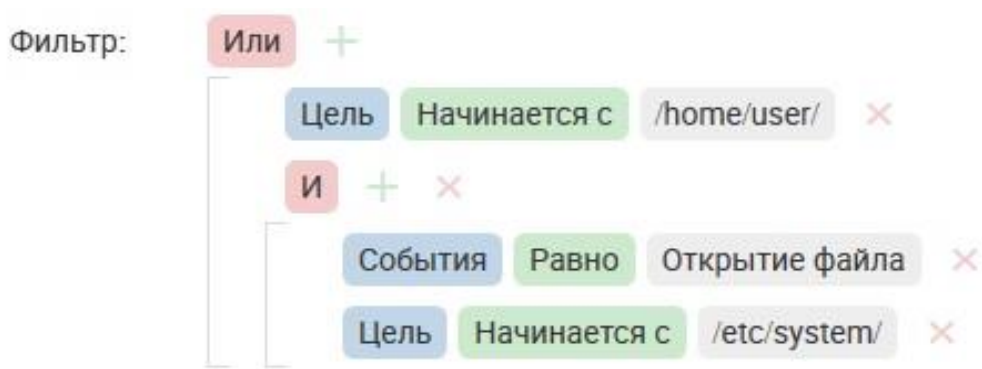


Рисунок 31. Пример добавления группы в фильтр

Исключение необходимо добавлять, как отдельную группу «НЕ ИЛИ» к основной группе правил. Для правил, где нет исключения, перед добавлением исключения необходимо все правила включить в группу. (Это также возможно сделать во вкладке фильтра «Текст», заключив необходимое в скобки).

Для обновления фильтра необходимо воспользоваться кнопкой «Обновить фильтр».

По окончании ввода данных необходимо нажать кнопку «Сохранить».