Athena Sandbox

СИСТЕМА ЗАЩИТЫ ОТ ЦЕЛЕНАПРАВЛЕННЫХ АТАК

Руководство пользователя

на 77 листах

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

Версия документа

Сентябрь 16, 2021.

СОДЕРЖАНИЕ

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.	Suricata	Программное обеспечение для анализа сетевого трафика.
3.	Агент	Программный агент для контроля внешних устройств и взаимодействия с ПК ATHENA.
4.	Автоматический режим работы системы	Режим работы системы, в котором файлы и приложения, поступающие на интерфейс, автоматически загружаются в систему и анализируются на предмет нелегитимного поведения.
5.	Активное содержимое	Дополнительные функции в файле или программе, к которым относятся макросы, ссылки на электронные таблицы, надстройки, подключение к данным, элементы ActiveX.
6.	Виртуальная машина	Программная система, эмулирующая аппаратное обеспечение, используемая в системе для проведения динамических исследований.
7.	Группа индикаторов	Набор индикаторов, выпадающий в рамках одного исследования и имеющий собственный вес.

№	Термин	Определение
8.	Динамическая индикаторы	Категория анализа, формируемая на основании событий, зафиксированных в эмулируемых средах при исследовании программного обеспечения динамическим видом анализа.
9.	Имитация работы пользователя	Автоматическая имитация действий пользователя в эмулируемых средах в ходе динамического анализа, которая в зависимости от поведения исследуемого объекта выполняет нажатие клавиш клавиатуры и манипулятора типа «мышь».
10.	Категория индикаторов	Объединение индикаторов по схожим свойствам относительно объекта анализа.
11.	Песочница	Изолированная среда с контролируемым набором ресурсом, которая имитирует персональный компьютер для исполнения программного обеспечения и анализа его поведения.
12.	Сессия исследования программного обеспечения	Последовательность действий, включающая в себя запуск эмулируемой среды, загрузку и запуск в ней программного обеспечения, получение данных о поведении программного обеспечения, их последующий анализ, выгрузку программного обеспечения и остановку эмулируемой среды.
13.	События	Минимальная единица анализа, фиксируемая в эмулируемых средах при исследовании программного обеспечения динамическим видом анализа.

№	Термин	Определение
14.	Статическая аналитика	Категория анализа, формируемая на основании индикаторов, зафиксированных при исследовании программного обеспечения статическим видом анализа.
15.	Физическая машина	Физическая система, эмулирующая аппаратное обеспечение, используемая в системе для проведения динамических исследований.
16.	Экспертный режим работы системы	Режим работы системы, в котором пользователь, имеющий роль аналитика, самостоятельно загружает файл или приложение для анализа в системе.
17.	Имитационная среда	Образ операционной системы с предустановленными пользовательскими приложениями, в котором запускается и исследуется программное обеспечение.
18.	Эталон	Модель сценария исследования в виртуальной машине, на основании которой осуществляется копирование виртуальных эмулируемых сред (виртуальных машин).
19.	Шаблон	Предустановленные параметры динамического исследования.

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.	CPU	Central processing unit
3.	DNS	Domain name system
4.	HTTP	HyperText transfer protocol
5.	БД	База данных
6.	ВМ	Виртуальная машина
7.	ВПО	Вредоносное программное обеспечение
8.	ОС	Операционная система
9.	ПО	Программное обеспечение
10.	ИС	Имитационная среда

3 Назначение программы

Программный комплекс «ATHENA SANDBOX – система защиты от целенаправленных атак» (далее – ПК ATHENA) предназначен для усиления безопасности ИТ- инфраструктуры и развития профессиональных компетенций офицеров ИБ.

3.1 Общие сведения

В состав лаборатории ПК ATHENA входит множество инструментов, которые подразделяются на два направления проверки: статического анализа и динамического анализа.

Статическое направление проверки включает в себя:

- проверку в более 20 различных локальных антивирусах;
- детальный анализ структуры и содержимого файлов;
- проверку во внешних аналитических ресурсах и репутационных базах;
- анализ определенных типов файлов в нейронных сетях;
- распаковку архивов, включая многотомные и защищенные паролем.

Динамическое направление проверки дополняет статическое направление. Оно включает в себя исследование поведения ПО в изолированных виртуальных и физических средах («песочницах»). В данном типе анализа осуществляется также фиксация потребляемых ресурсов, что позволяет выявить ПО, расходующее ресурсы ОС для майнинга.

После определение вердиктов обоими видами анализа формируется общий вердикт.

В ПК ATHENA реализован прием файлов на анализ из следующих источников:

- веб-трафик;
- почтовый трафик;
- сетевой трафик;
- мобильные устройства;
- съемные носители;

– мессенджеры;
– агенты на рабочих местах;
– ручная загрузка;
– посредством API.

ПК ATHENA способен принимать любые типы файлов на проверку:

– исполняемые;
– офисные;
– мобильные приложения;
– архивы, включая многотомные и закрытые паролем;

В динамическом анализе поддерживаются следующие ОС:

– MS Windows 10 – 7;
– Windows Server (2008 R2 - 2019);
– Linux:
  – Astra Linux;
  – Debian 9.8 (Stretch);
  – openSUSE Leap 15;
  – CentOS 7.6.1810;
  – Ubuntu 18.10;
– Android (5-9).

ПК ATHENA имеет два режима работы: автоматический и экспертный.

Автоматический режим заключается в автоматической проверке всех файлов, получаемых из перечисленных выше источников, без участия пользователей системы.

Экспертный режим позволяет пользователю самому выбирать файл и «песочницу», настраивать параметры исследования, запускать файл, принимать участие в имитации работы пользователя в «песочнице», затем проводить анализ лога событий и результатов аналитического блока системы. В рамках данного режима пользователь в динамическом анализе может детально настроить эмулируемые среды по интересующим его направлениям исследования.

ПК ATHENA имеет API-интерфейс для интеграции с другими системами.

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

4 Авторизация и элементы управления

Для авторизации в ПК ATHENA необходимо ввести логин и пароль, полученный у администратора (Рисунок 1).

Рисунок 1. Страница авторизации пользователя в ПК ATHENA

После прохождения авторизации осуществляется переход в веб-интерфейс ПК ATHENA, в котором присутствуют функциональные разделы, описанные в таблице 3.

Таблица 3. Описание функциональных разделов в системе

№	Раздел	Описание
1.	Статистика	Содержит статистическую информацию.
2.	Безопасность	Содержит задания для офицеров по безопасности которые содержат источники и подозрительные/вредоносные объекты, выявленные в них.
3.	Источники	Содержит все источники, из которых поступают данные на анализ в систему.
4.	Спутники	Содержит информацию по другим системам, имеющим распределенный характер (например,

№	Раздел	Описание
		агенты на рабочие места).
5.	Объекты анализа	Содержит данные по всем загруженным в систему объектам для анализа.
6.	Исследования	Содержит все исследования, проводимые в системе, с классификацией по типам.
7.	Ресурсы	Содержит информацию по всем ресурсам, используемым в системе для динамического анализа.
8.	Справочники	Содержит гибкие справочники по системному и аналитическому направлению в системе.
9.	Настройки	Содержит настройки по всем компонентам системы.
10.	Журналы	Содержит информацию по мониторингу всех логических и физических модулей в системе, а также регистрацию действий пользователей.

4.1 Элементы управления веб-интерфейсом

Описание, назначение и настройка по умолчанию элементов управления веб-интерфейсом ПК ATHENA представлены в таблице 4.

Таблица 4. Элементы управления интерфейсом

№	Элемент	Назначение	Настройка по умолчанию	Изображение
1.	Значок «Выход»	Выполняет выход из системы	Активен	
2.	Значок «Календарь»	Выполняет переход в форму выбора даты	Активен	

№	Элемент	Назначение	Настройка по умолчанию	Изображение
3.	Значок «Профиль»	Позволяет перейти в личный аккаунт пользователя в системе	Активен	
4.	Значок «Выпадающий список»	Позволяет выбрать язык отображения интерфейса	Русский язык	
5.	Значок «Загрузить файл»	Выполняет загрузку файл на проверку	Активен	
6.	Значок «Учетная запись»	Выполняет переход в меню личного кабинета	Активен	
7.	Кнопка «Отчет»	Отображение отчета по проверке веб-ссылки	Активна	
8.	Кнопка «Копировать»	Выполняет копирование сущности	Активна	
9.	Кнопка «Обновить»	Обновление данных в таблице	Активна	
10.	Кнопка «Добавить»	Выполняет добавление новой сущности	Активна	

№	Элемент	Назначение	Настройка по умолчанию	Изображение
11.	Кнопка «Редактировать»	Выполняет редактирование	Активна	
12.	Кнопка «Фильтр»	Фильтр, который выполняет фильтрацию, если в поисковом поле таблицы введены данные	Активна	
13.	Кнопка «Экспортировать все»	Скачиваются в выбранном формате	Активна	
14.	Кнопка «Отобразить символы»	При нажатии на кнопку отобразятся введённые символы	Активна	
15.	Кнопка «Настройка лицензии»	При нажатии на кнопку отобразится форма для добавления файла лицензии	Активна	
16.	Кнопка «Загрузка сигнатур антивируса»	При нажатии на кнопку отобразится форма для добавления файла сигнатур антивируса	Активна	

№	Элемент	Назначение	Настройка по умолчанию	Изображение
17.	Кнопка «Удалить»	При нажатии на кнопку будет осуществлено удаление выбранной записи	Активна	
18.	Кнопка «Сертификат»	При нажатии на кнопку отобразится форма для загрузки сертификата	Активна	
19.	Кнопка «Настройки»	При нажатии на кнопку отобразится форма для изменения настроек	Активна	
20.	Кнопка «Отметить как выполненное»	При нажатии на кнопку отобразится форма для пометки выполненной задачи	Активна	
21.	Кнопка «Закрепить»	При нажатии на кнопку произойдет закрепление записи в таблице	Активна	

№	Элемент	Назначение	Настройка по умолчанию	Изображение
22.	Кнопка «Открепить»	При нажатии на кнопку закрепленная в таблице запись будет откреплена	Активна	
23.	Кнопка «Загрузка файла»	При нажатии на кнопку отобразится форма для подтверждения выгрузки файла на рабочую станцию	Активна	
24.	Кнопка «Печать»	При нажатии на кнопку будет осуществлена загрузка печатного отчета	Активна	
25.	Кнопка «Отправить выделенные письма»	При нажатии на кнопку будут отправлены выбранные в таблице письма	Активна	
26.	Кнопка «Информация»	При нажатии на кнопку отобразится форма содержащая информацию о машине	Активна	

№	Элемент	Назначение	Настройка по умолчанию	Изображение
27.	Кнопка «Подтвердить»	При нажатии на кнопку выбранный агент будет подтвержден	Активна	
28.	Кнопка «Отменить подтверждение»	При нажатии на кнопку снимается подтверждение с выбранного агента	Активна	
29.	Кнопка «Ловушки»	При нажатии на кнопку отобразится окно с имеющимися ловушками в системе	Активна	
30.	Кнопка «Информация»	При нажатии на кнопку отобразится окно с информацией о ловушке	Активна	
31.	Кнопка «Загрузить логи»	При нажатии на кнопку будет осуществлена выгрузка на рабочую станцию файла с логами	Активна	

№	Элемент	Назначение	Настройка по умолчанию	Изображение
32.	Кнопка «SSH»	При нажатии на кнопку будет осуществлен переход в окно консоли для подключения к удаленному серверу	Активна	
33.	Кнопка «Запустить»	При нажатии на кнопку будет осуществлен запуск машины.	Активна	
34.	Кнопка «Остановить»	При нажатии на кнопку запущенная ранее машина будет остановлена	Активна	
35.	Кнопка «Последняя динамика»	При нажатии на кнопку будет осуществлен переход на страницу с отчетом о последнем динамическом исследовании.	Активна	
36.	Кнопка «Боты»	При нажатии на кнопку отобразится окно с данными об обработчиках	Активна	

№	Элемент	Назначение	Настройка по умолчанию	Изображение
		данных ботов		
37.	Кнопка «Результаты антивирусов»	При нажатии на кнопку отобразится форма содержащая результаты антивирусов	Активна	
38.	Кнопка «Графики»	При нажатии кнопки отобразится форма для выбора типа отображаемой статистики	Активна	

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

5 Статистика

ПК ATHENA предназначена для усиления защиты в организации, ее целевой аудиторией являются офицеры по безопасности, которым необходимы для осуществления своей работы статистические данные и мониторинг инцидентов.

Статистические данные представлены в разделе «Статистика» (Рисунок 2).

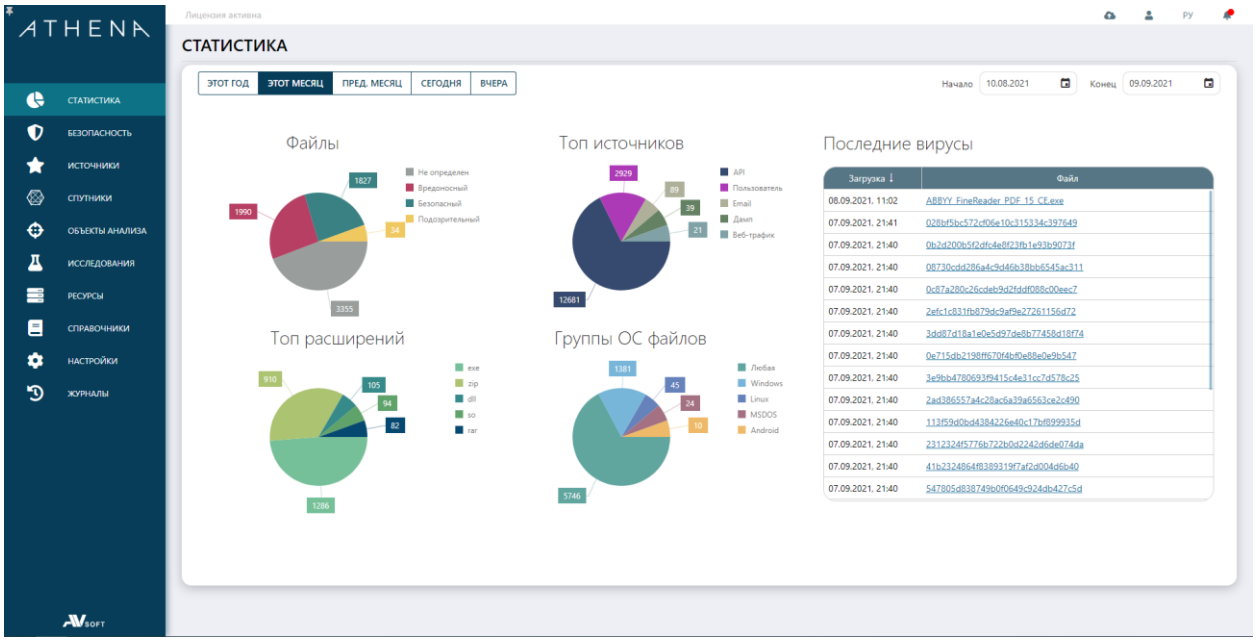


Рисунок 2. Раздел «Статистика»

Элементы на графиках являются активными, при нажатии на них происходит автоматическая фильтрация по выбранной категории. Для указания периода времени, за который требуются статистические данные, необходимо воспользоваться пейджером над схемами.

В таблице «Последние вирусы» отображаются крайние выявленные системой вирусы. Наименование каждого файла в таблице является активной ссылкой, при нажатии на которую происходит переход в отчет по файлу.

6 Безопасность

В разделе «Безопасность» консолидируются задания по безопасности, которые содержат источники и подозрительные/вредоносные объекты, выявленные в них. Задача офицера по безопасности провести проверку данных инцидентов, принимать превентивные меры по усилению защиты

ИТ-периметра и учитывать их во время проведения регулярного аудита информационной безопасности ИТ-инфраструктуры предприятия (Рисунок 3).

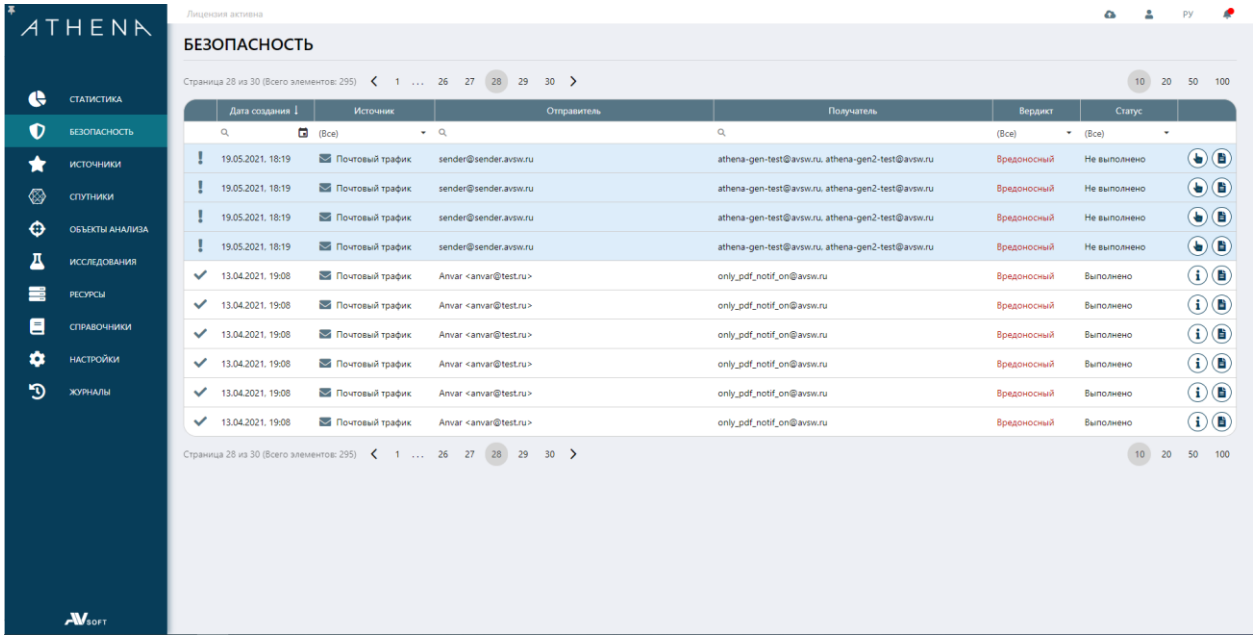


Рисунок 3. Задания по безопасности

В таблице заданий по безопасности, задания, имеющие статус «Не выполнено» отмечены голубым цветом, а задания статус которых «Выполнено» отмечены белым.

Для выполнения задания необходимо нажать на кнопку «Отметить как выполненное» (Рисунок 4).

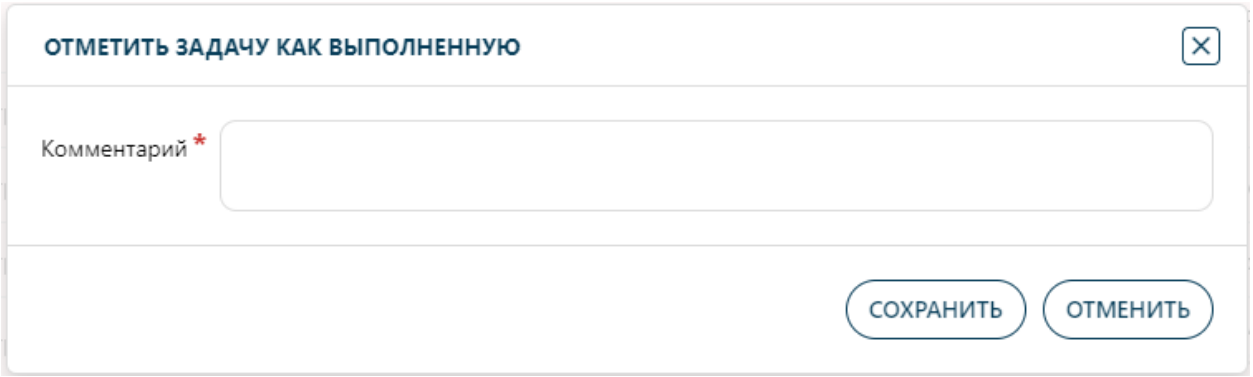


Рисунок 4. Выполнение задания по безопасности

Далее в открывшейся форме необходимо указать комментарий по нему и, по завершении ввода данных, нажать кнопку «Сохранить».

7 Проведение исследований

Цикл исследования любого объекта в системе состоит из двух блоков: статического и динамического. Инициация исследования в системе может осуществляться в ручном и автоматическом режиме.

7.1 Автоматический режим

В автоматическом режиме исследования создаются без участия пользователя по заранее заданному сценарию, который указывается в настройках администратором при интеграции источника проверки в систему.

7.2 Ручной режим

В ручном режиме пользователь самостоятельно осуществляет загрузку и запуск исследований по интересующим его параметрам. Для начала исследования необходимо загрузить объект проверки в систему одним из следующих способов:

- кнопкой «Загрузить» в верхней панели;
- кнопкой «Загрузить» по пути «Объекты анализа» → «Файлы»/«Ссылки».

После выбора способа загрузки отобразится форма «Загрузка файлов», в которой нужно нажать кнопку «Выберите файл» или просто перетащить файл в указанное поле (Рисунок 5).

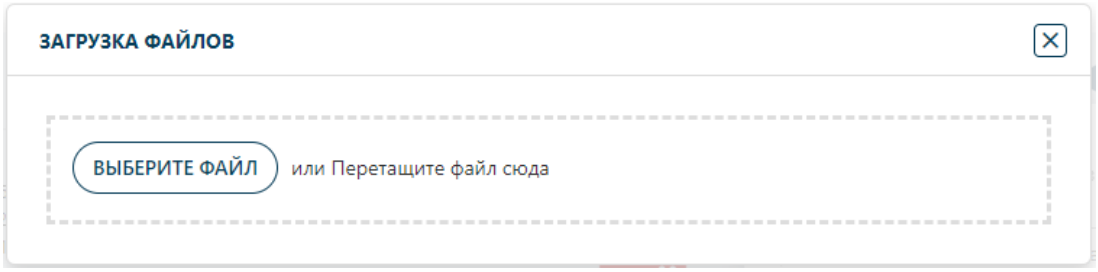


Рисунок 5. Форма загрузки файлов

По окончании выбора объектов для проверки необходимо нажать кнопку «Загрузить» (Рисунок 6).

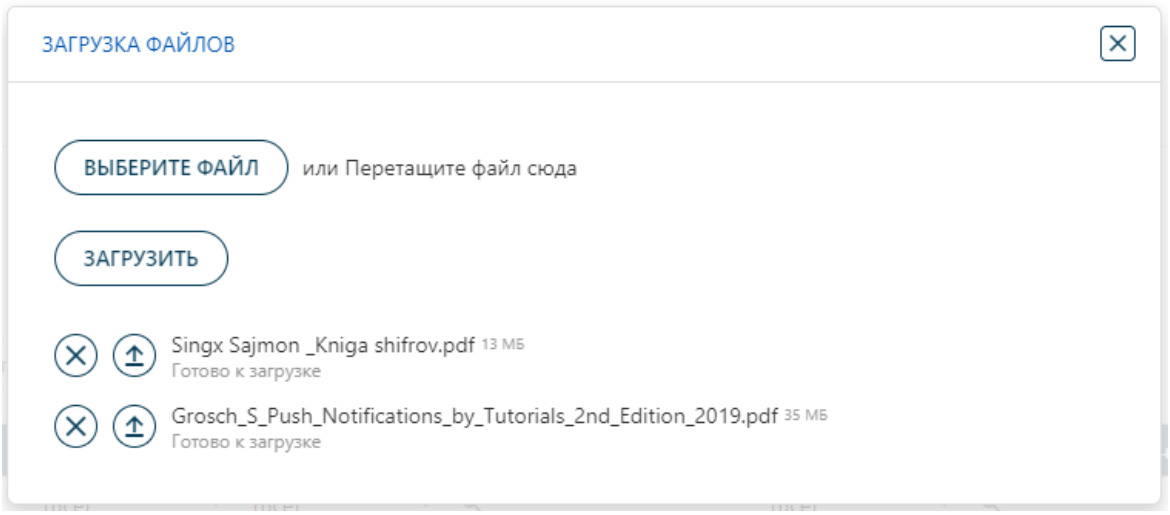


Рисунок 6. Загрузка файлов на проверку

При успешной загрузке полоса загрузки достигнет 100% и в правом верхнем углу отобразится уведомление, что загрузка выполнена успешно (Рисунок 7).

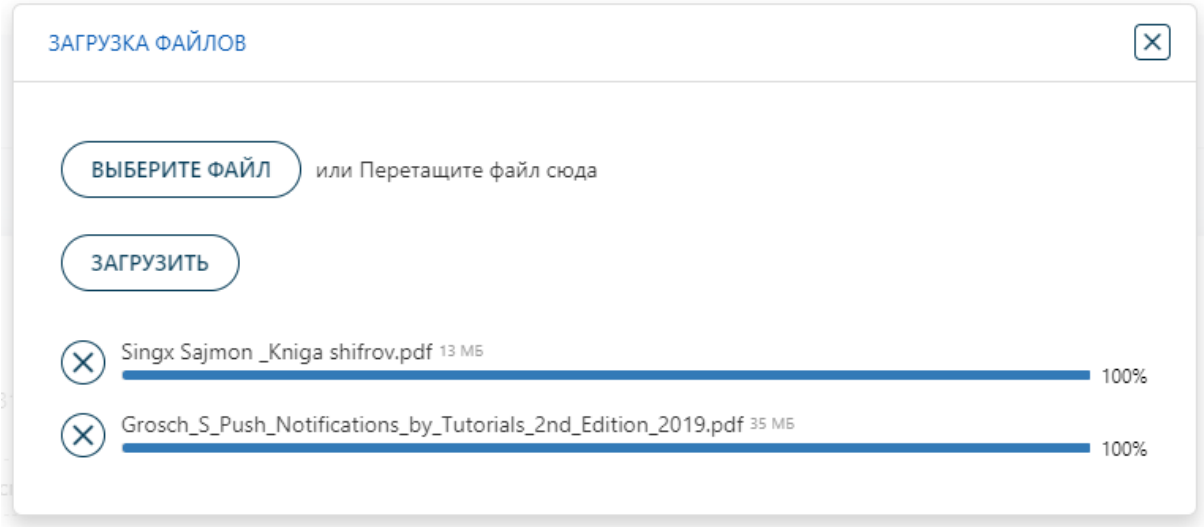


Рисунок 7. Успешная загрузка файлов на проверку в систему

Далее в таблице статических исследований, которая расположена по пути «Исследования» → «Статические», можно отслеживать статус статического исследования (Рисунок 8).

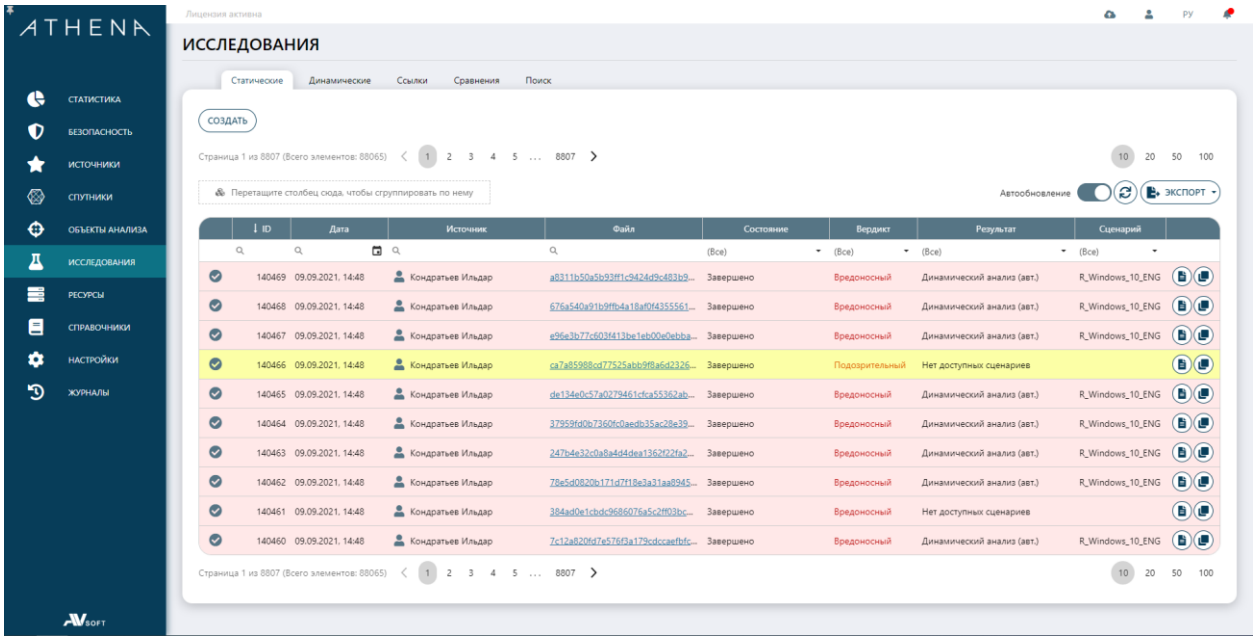


Рисунок 8. Таблица статических исследований

После завершения статической проверки файл отправится на динамическую, если получит безопасный вердикт или по принуждению вне зависимости от вердикта, если в настройках администратором выставлен соответствующий флаг.

> **!** **Статическая проверка обязательный первый шаг для любого нового объекта проверки, ранее не исследуемого системой. Динамическая проверка может быть опциональна в целях экономии ресурсов, также ее нельзя запускать до окончания статической проверки.**

В таблице динамических исследований, которая расположена по пути «Исследования» → «Динамические», можно отслеживать статус динамического исследования (Рисунок 9).

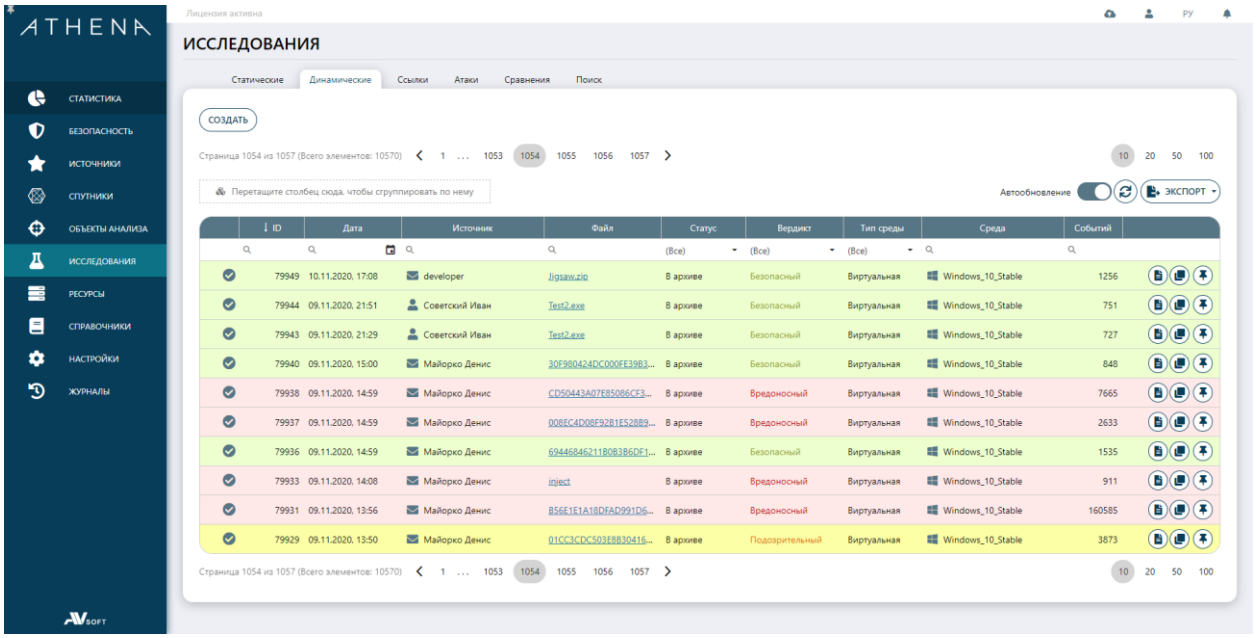


Рисунок 9. Таблица динамических исследований

В таблице ссылок, которая расположена по пути «Исследования» → «Ссылки», можно отслеживать статус анализа ссылок (Рисунок 10).

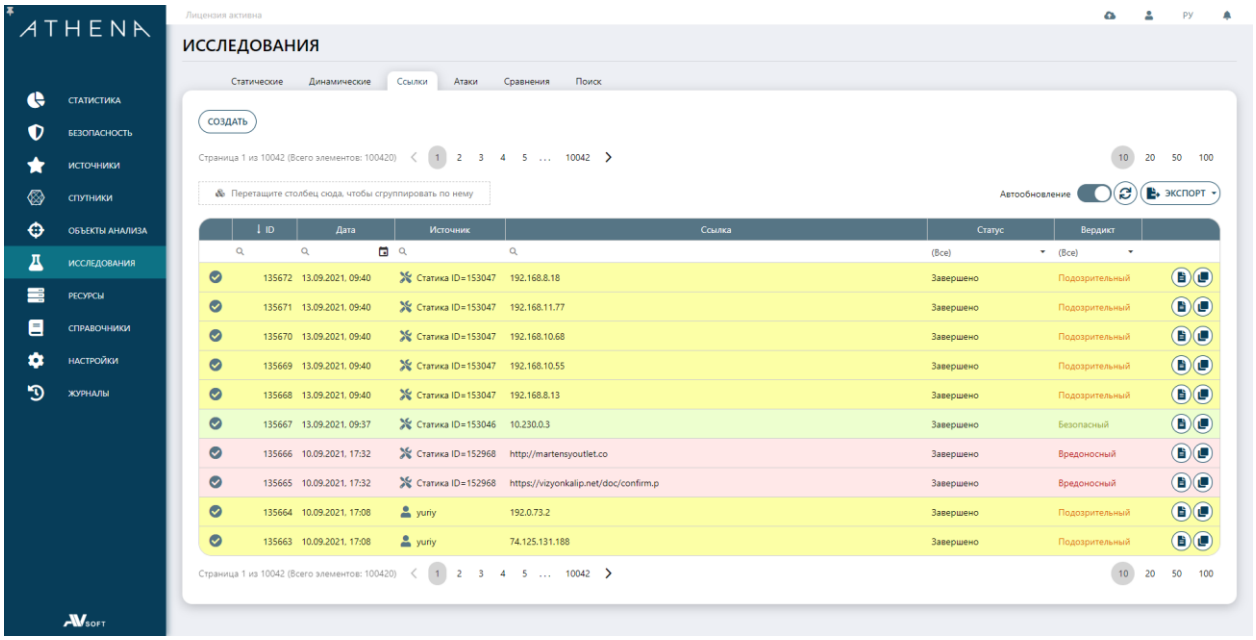


Рисунок 10. Таблица ссылок

В таблицах с результатами исследований реализована функция группировки результатов исследования по выбранному параметру. Для отображения результатов по группам необходимо, навести курсор мыши на столбец с названием параметра, далее необходимо зажать левую кнопку и

перетащить в область «Перетащите столбец сюда, чтобы сгруппировать по нему». Пример отображения результатов статического исследования с группировкой отображаемых результатов по параметру «Вердикт» представлен ниже (Рисунок 11).

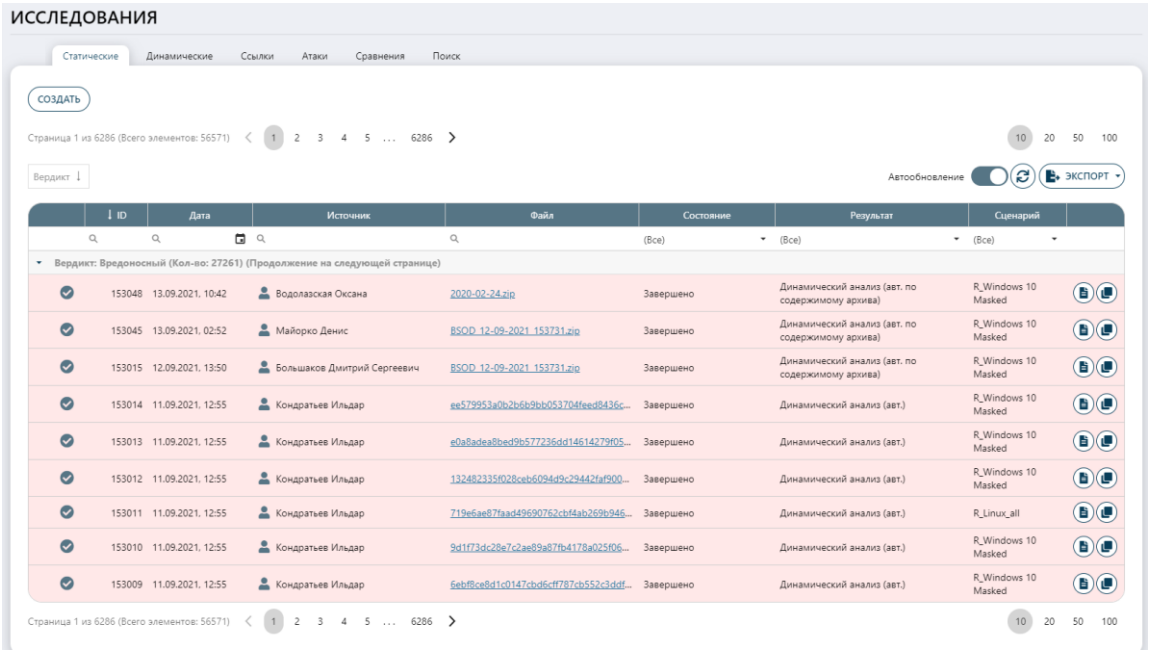


Рисунок 11. Таблица результатов исследований. Группировка по параметру «Вердикт»

Для просмотра результатов всех исследований по объекту анализа необходимо перейти в «Объекты анализа» → «Файлы»/«Ссылки» и нажать в таблице на иконку «Отчет», далее осуществится переход на страницу консолидированного отчета по файлу или ссылке (Рисунок 12).

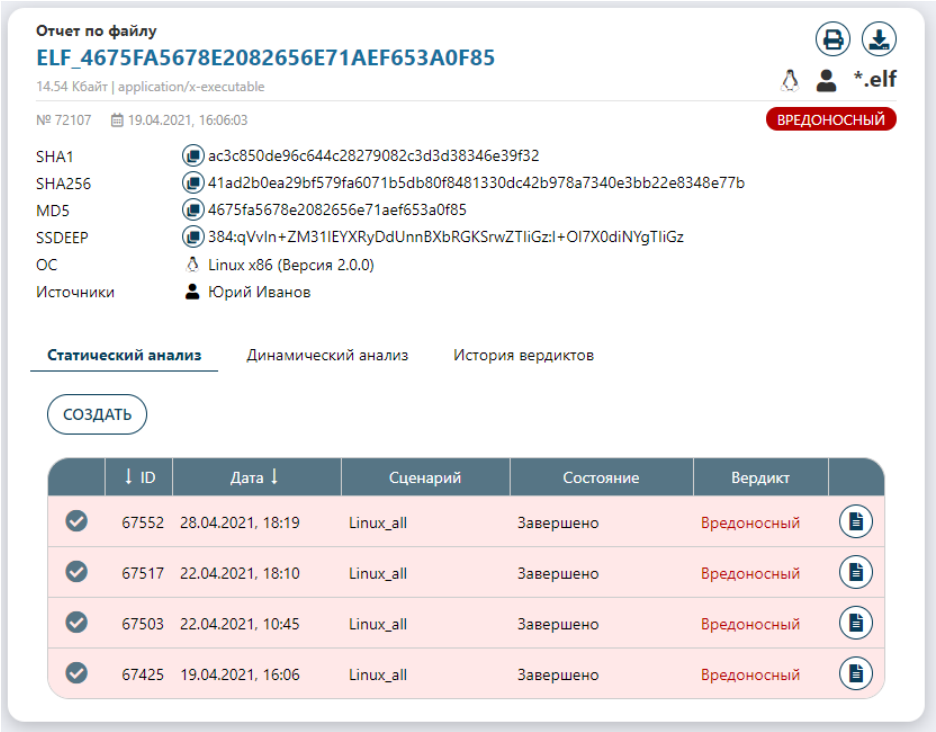


Рисунок 12. Отчет по файлу

В отчете по файлу присутствуют параметры, описанные в таблице 5.

Таблица 5. Описание параметров в общем отчете по файлу

№	Параметр	Описание
1.	Общая информация	Значимые идентификационные параметры файла: – имя; – размер; – расширение; – номер исследования; – дата и время запуска исследования.
2.	Вердикт	Общий вердикт файла на основании всех видов анализа в системе.
3.	Теги	Ассоциативные ключевые слова, которые позволяют быстро осуществлять поисковый запрос по интересующему параметру.

№	Параметр	Описание
4.	Контрольные суммы	Контрольные суммы и нечеткая контрольная сумма для определения которых используется утилита SSDeep.
5.	ОС	Операционная система с указанием версии и архитектуры для запуска и работы файла.
6.	Источники	Источники поступления файла в систему на проверку.
7.	**Статическое исследование**	
7.1.	Анализ содержимого	Анализ синтаксической структуры файла.
7.2.	VirusTotal	Внешний аналитический ресурс VirusTotal.
7.3.	Антивирусы	Проверка локальными антивирусными движками.
7.4.	Машинное обучение	Проверка различными моделями машинного обучения.
7.5.	Yara-правила	Условия идентификации и классификации вредоносных программ с точки зрения статического анализа.
8.	**Динамическое исследование**	
8.1.	Индикаторы	Условия анализа поведения на предмет вредоносной активности.
8.2.	Процессы	Список процессов, запущенных в ОС во время динамического исследования.
8.3.	Файлы	Созданные файлы в исследовательской среде динамического анализа.

№	Параметр	Описание
8.4.	Реестр	Зафиксированные изменения в реестре ОС Windows.
8.5.	Сетевой трафик	Анализ инициации сетевого взаимодействия файла с внутренней или внешней сетью Интернет.
9.	**Ход исследования**	
9.1.	Карта исследования	Графическое отображение хода исследования по основным процессам.
9.2.	MITRE	Методология классификации тактик и действий злоумышленников по основным этапам кибератаки.
9.3.	Запись исследования	Видеозапись процесса исследования файла в имитационной среде.
9.4.	События	Список поведенческих событий в исследовательской среде динамического анализа.
9.5.	IOC	Индикаторы компрометации, которые указывают на подозрительную или вредоносную активность файла.

Для перехода в какой-либо параметр необходимо нажать на иконку с его обозначением и подписью. Также возможен просмотр детального отчета по каждому направлению исследования при помощи нажатия на активную ссылку «Полный отчет».

Для проверки ссылок в ручном режиме необходимо в разделе «Объекты анализа» → «Ссылки» нажать кнопку «Проверить», далее отобразится форма для указания веб-ссылки, которую требуется проверить (Рисунок 13).

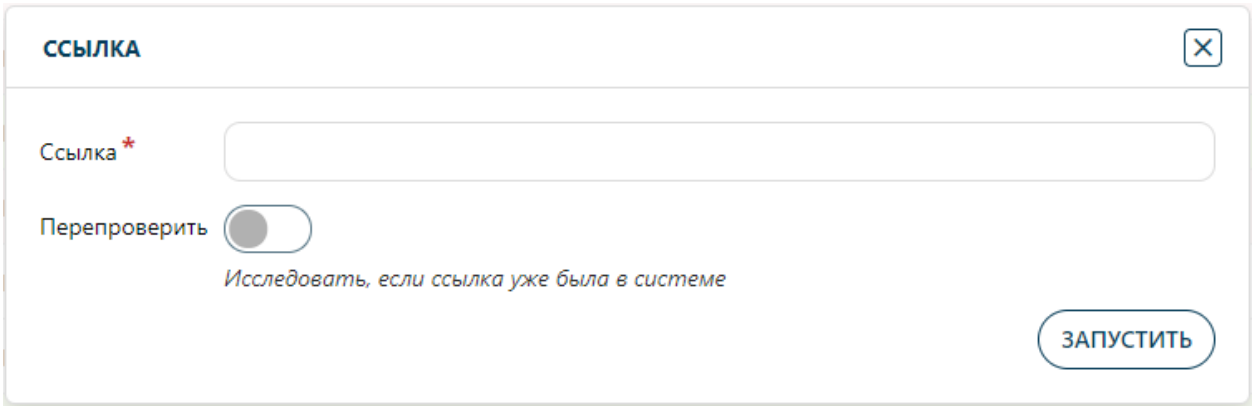


Рисунок 13. Проверка ссылки в ручном режиме

Если ссылку требуется проверить даже несмотря на то, что она уже проверялась системой, то в этом случае необходимо использовать флаг «Проверить». По окончании ввода данных необходимо нажать кнопку «Запустить». При успешном запуске веб-ссылки на проверку отобразится уведомление «Началась проверка ссылки».

В общей таблице ссылок отобразится новая ссылка, отправленная на проверку (Рисунок 14).

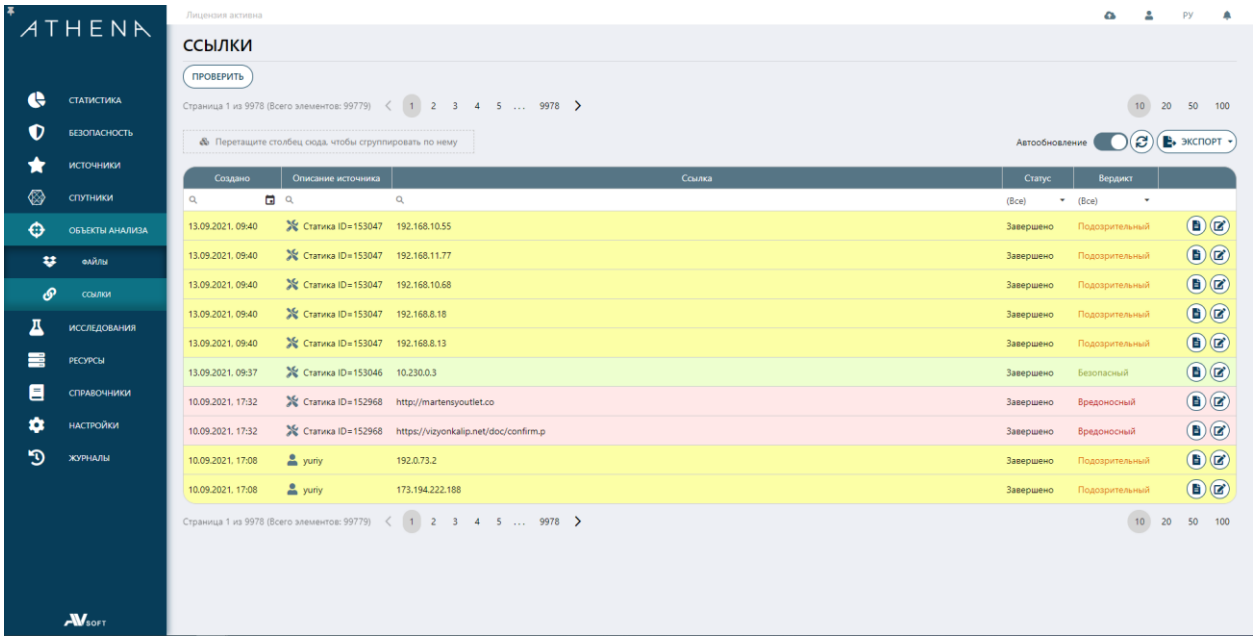


Рисунок 14. Таблица веб-ссылок

Также таблица проверяемых в системе ссылок присутствует по пути «Исследования» → «Ссылки» (Рисунок 15).

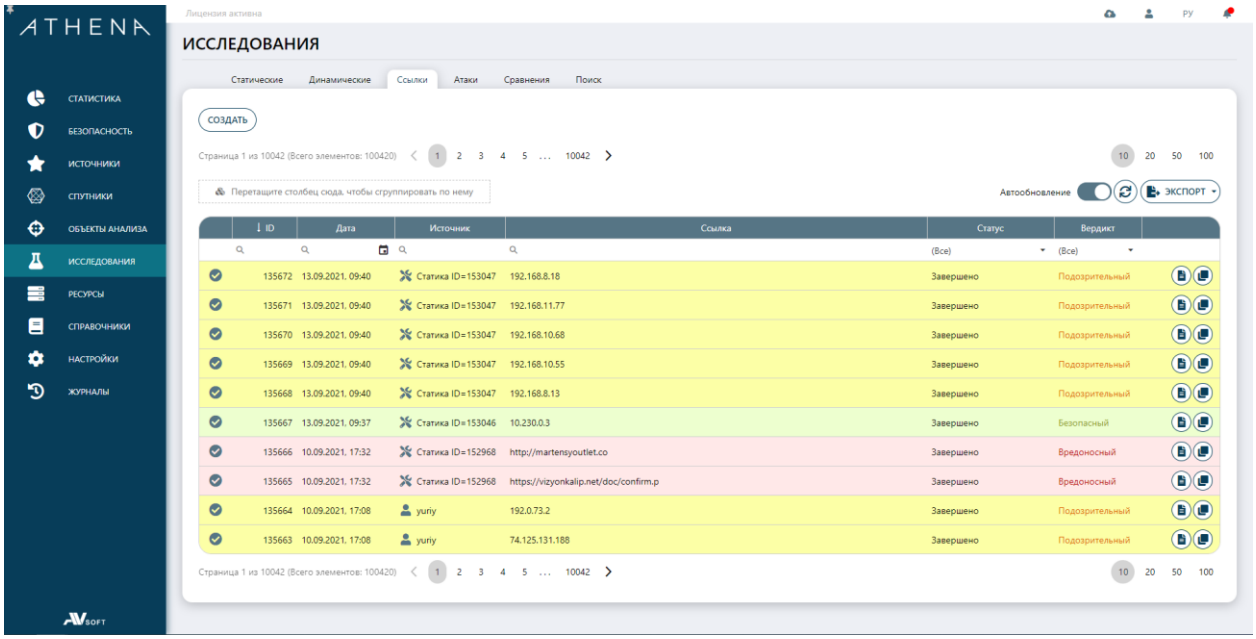


Рисунок 15. Таблица исследований веб-ссылок

Для перехода в отчет по проверке ссылки необходимо нажать иконку «Отчет» (Рисунок 16).

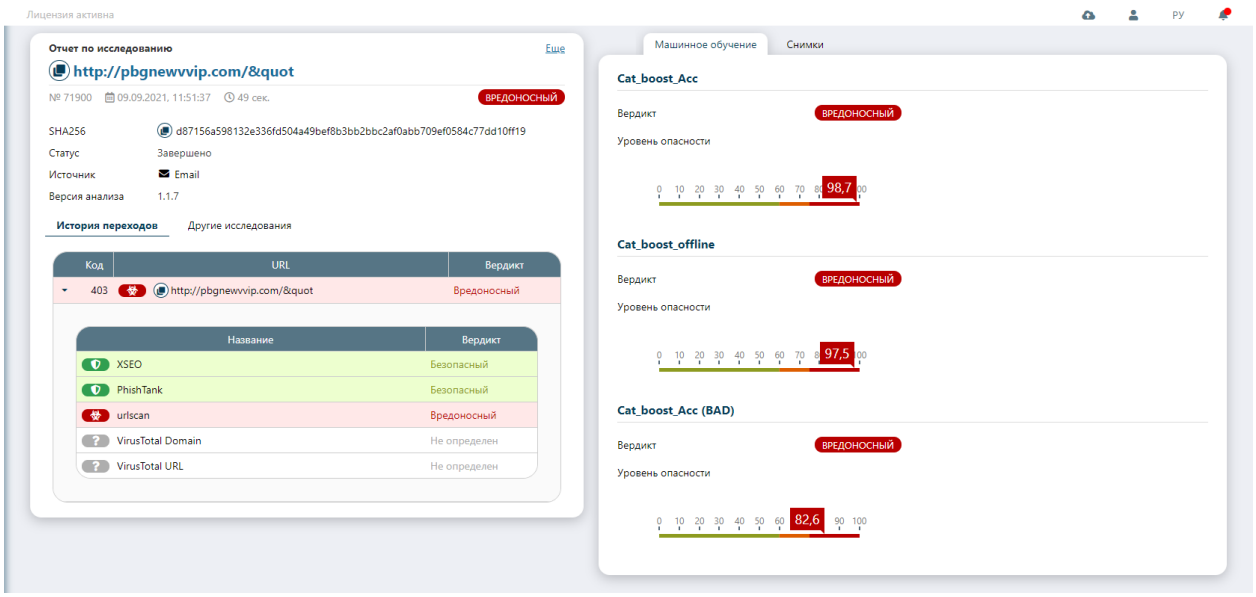


Рисунок 16. Отчет по проверке веб-ссылки

Отчет по проверке веб-ссылки включает в себя параметры, описанные, в таблице 6.

Таблица 6. Описание параметров в отчете по веб-ссылке

№	Параметр	Описание
1.	Общая информация	Значимые идентификационные параметры ссылки: – имя; – номер исследования; – дата и время запуска на исследование.
2.	Контрольная сумма	Контрольная сумма ссылки, которая может использоваться в качестве ее уникального идентификатора.
3.	Статус	Статус исследования ссылки в системе.
4.	Источник	Источник поступления ссылки на проверку в систему.
5.	Версия анализа	Версия модуля анализа ссылок, используемого для анализа в системе.
6.	Вердикт	Общий вердикт по ссылке в системе на основании всех источников анализа.
7.	История переходов	Пути переходов веб-ссылки на другие адреса.
8.	Другие исследования	История исследований ссылки в системе.
9.	Машинное обучение	Модели машинного обучения, которые анализируют синтаксическую структуру файла на предмет наличия в ней вредоносных элементов.
10.	Снимки	Снимки экрана с отображением веб-страницы.

Машинное обучение включается в себя несколько моделей с разными типами алгоритмов (Рисунок 17).

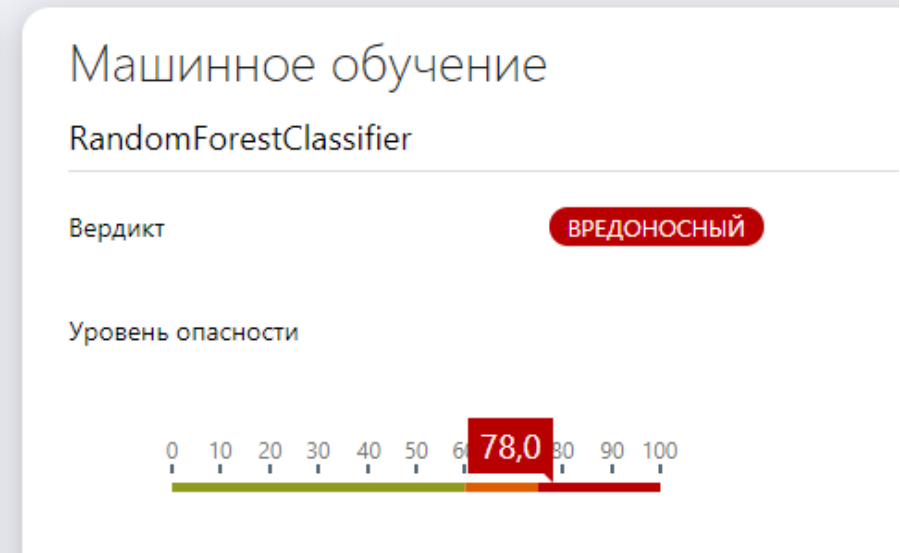


Рисунок 17. Модель машинного обучения

У каждой модели есть свой вердикт по объекту анализа и шкала с обозначением уровня опасности в процентном отношении.

8 Создание исследований

В системе возможно создание кастомизированных исследований по интересующим параметрам в ручном режиме для одного или сразу нескольких файлов (по сценарию).

Кастомизированные исследования возможны для статического и динамического типа анализа.

8.1 Статическое исследование

Для создания статического исследования по файлу необходимо воспользоваться кнопкой «Создать», которая присутствует в следующих директориях:

- «Исследования» → «Статические» → кнопка «Создать»;
- «Объекты анализа» → «Файлы» → кнопка «Отчет» → вкладка «Статический анализ» → кнопка «Создать».

Для создания статического исследования открывается форма (Рисунок 18).

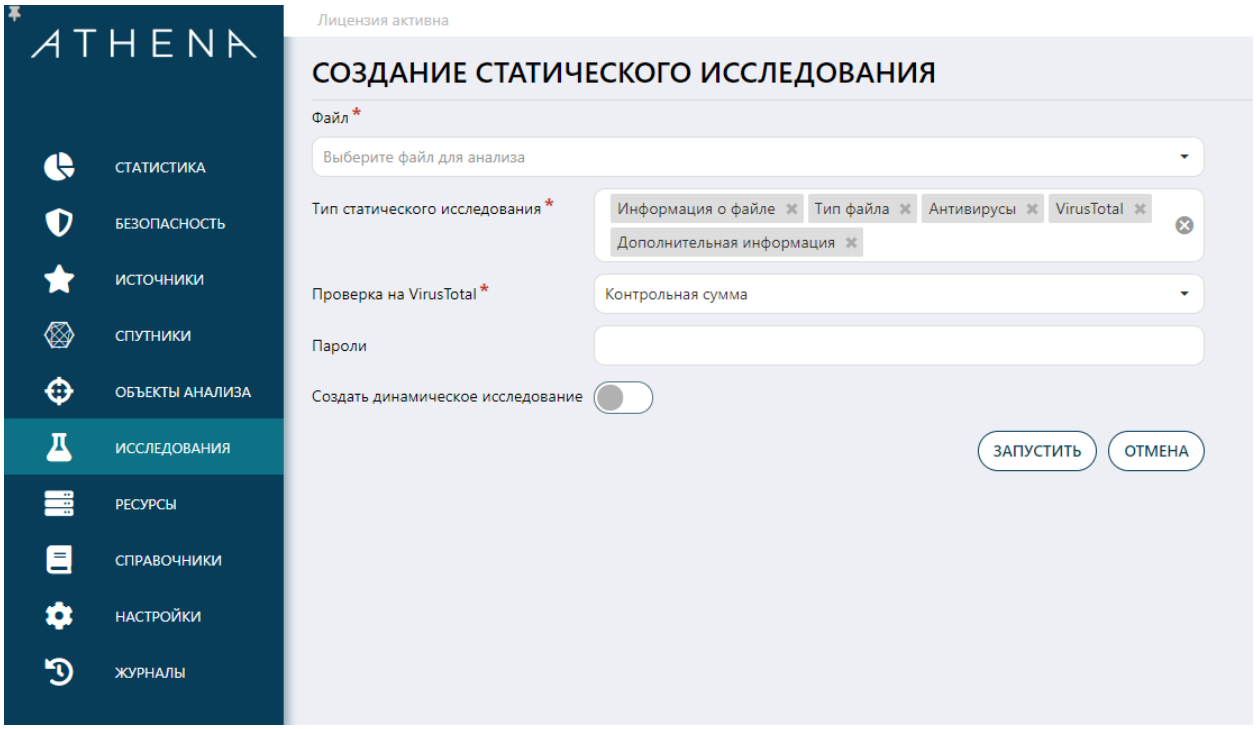


Рисунок 18. Создание статического исследования

При создании статического исследования необходимо указать параметры, описанные в таблице 7.

Таблица 7. Параметры создания статического исследования

№	Параметры	Описание
1.	Файл	Выбор файла из списка загруженных в систему.
2.	Тип статического исследования	Категории этапов и инструментов статического анализа, которые можно, при необходимости, корректировать (исключать/дополнять). По умолчанию в статический анализ включено: – Информация о файле; – Тип файла; – Антивирусы;

№	Параметры	Описание
		– VirusTotal; – Дополнительная информация.
2.1.	Информация о файле	Определение значимой идентификационной информации о файле.
2.2.	Тип файла	Определение типа файла.
2.3.	Антивирусы	Проверка файла множеством локальных антивирусных движков.
2.4.	VirusTotal	Проверка файла внешним аналитическим ресурсом VirusTotal.
2.5.	Дополнительная информация	Детальный разбор синтаксической структуры файла и структуризация ее по компонентным категориям.
3.	Проверка на VirusTotal	Выбор способа отправки на проверку во внешний аналитический ресурс VirusTotal. Доступны варианты отправки файла или только его контрольной суммы. По умолчанию отправляется контрольная сумма в целях безопасности конфиденциальных документов, которые запрещено отправлять во внешние аналитические ресурсы на анализ.
4.	Пароли	Если файл имеет пароль, который может отсутствовать в справочнике системы или просто пользователь хочет сразу его указать, то это можно сделать в данном поле.

№	Параметры	Описание
5.	Создать динамическое исследование	Флаг создания принудительного динамического исследования даже если файл получил подозрительный/вредоносный вердикт на этапе статического анализа и не имеет активного содержимого внутри себя (соответственно, теряется смысла запуска на динамический анализ в «песочнице»).

После завершения ввода данных необходимо нажать кнопку «Запустить» и удостовериться, что новое статическое исследование отобразилось в общей таблице статических исследований со статусом «В очереди». После достижения исследованием статуса «Завершено» пользователь может нажать на иконку «Отчет» и ознакомиться с результатами.

Когда в общей таблице статических исследований новому исследованию в колонке «Состояние» будет присвоен статус «Завершено», то пользователь может нажать на иконку «Отчет», чтобы ознакомиться с результатами анализа (Рисунок 19).

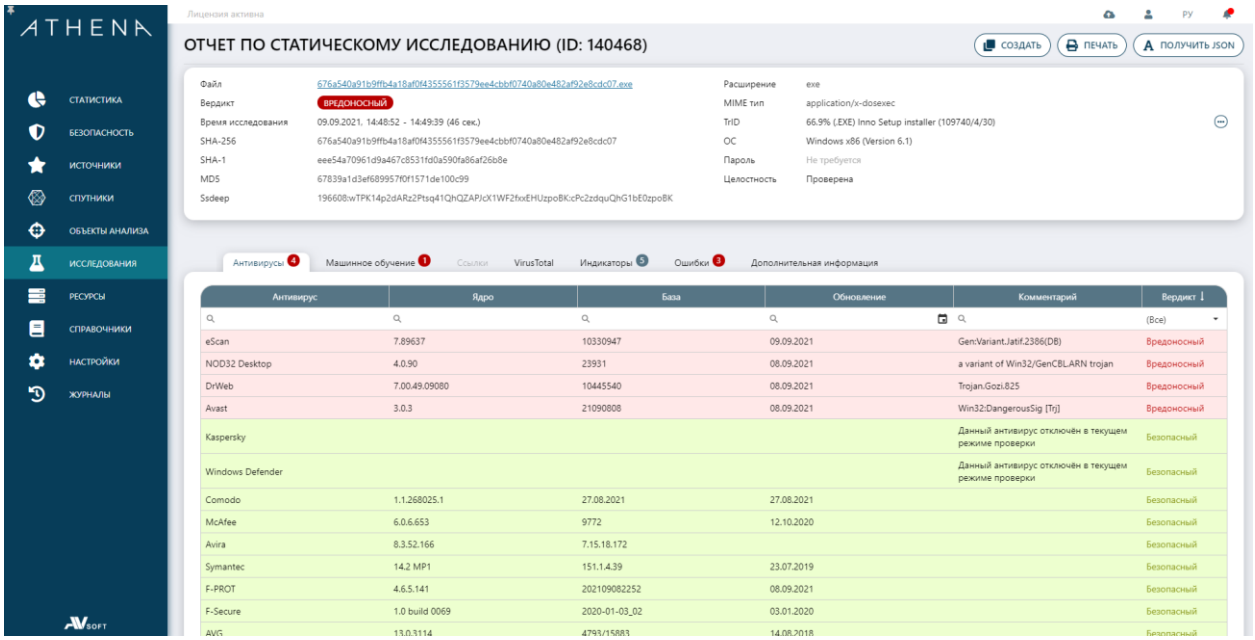


Рисунок 19. Отчет по статическому исследованию

В отчете по статическому исследованию присутствуют общие значимые параметры статического исследования, описанные в таблице 8.

Таблица 8. Параметры статического исследования

№	Параметр	Описание
1.	Наименование файла	Имя файла, которое является активной ссылкой для перехода в общий отчет по файлу, где можно найти все типы исследований, проводившихся по нему в системе.
2.	Вердикт	Вердикт файла по статическому исследованию на основании результата проверки всех инструментов, предусмотренных в данном функциональном разделе.
3.	Контрольные суммы	Уникальные идентификационные данные по файлу, которые можно использовать для поиска, как внутри системы, так и в других внешних аналитических сервисах для сравнения результатов работы системы. На

№	Параметр	Описание
		текущий момент в системе поддерживается определение следующих форматов контрольных сумм: – SHA-256; – SHA-1; – MD5.
4.	SSDeep	Утилита для вычисления нечетких контрольных сумм, которые устойчивы к небольшим изменениям в файле, что помогает вычислять схожие фрагменты в модификациях вредоносного ПО и объединять их в группы.
5.	Расширение	Расширение, которое будет определено на этапе статического анализа, влияет на выбор сценария проверки в динамическом анализе. В определении расширения участвуют поля: «MIME тип», «MIME описание», «TrID».
6.	MIME тип	Типы данных, которые могут быть переданы посредством сети Интернет с применением стандарта MIME.
7.	TrID	Утилита для определения типа файла по его бинарной сигнатуре, она показывает в процентном соотношении к какому типу больше тяготеет файл и участвует в принятии решения относительно настоящего типа файла в поле «Расширение», с которым потом файл будет отправлен на исследование в динамику (в зависимости от настроек).
8.	ОС	Операционная система для запуска и работы файла. Данная информация необходима для корректного запуска динамического анализа.

№	Параметр	Описание
9.	Пароль	Если файл или архив имеют пароль, то в данном поле будет отображаться пароль, который удалось определить системе или информация, что пароль подобрать не удалось.
10.	Целостность	Целостность файла необходимо проверять для контроля следующих параметров: – поврежден/не поврежден файл; – полный/неполный архив.

В статическом отчете присутствуют данные по проверке статическими инструментами анализа, описанные в таблице 9.

Таблица 9. Описание инструментов статического анализа

№	Параметр	Описание
1.	Антивирусы	Локальные антивирусные движки, каждый выдает отдельный вердикт по своей проверке.
2.	Virus Total	Внешний аналитический ресурс, который дает информацию по своим антивирусным вердиктам, они сегментируются в системе на доверенных и не доверенных.
3.	Ссылки	Если в файле присутствуют ссылки, то они отдельно фиксируются в данной вкладке. По каждой ссылке идет проверка и присваивается вердикт. Вердикт ссылок в файле влияет на общий вердикт по нему, если количество ссылок в файле превышает более трех.
4.	Машинное обучение	В системе есть несколько моделей машинного обучения, которые проверяют синтаксическую структуру файла на предмет вероятности наличия в ней элементов,

№	Параметр	Описание
		свойственных вредоносному программному обеспечению.
5.	Индикаторы	Статические индикаторы представляют собой синтаксическую сигнатуру или набор синтаксических сигнатур, располагающихся в теле файла или сетевого пакета, принадлежащего эксплойту.
6.	Yara-правила	Скриптовые правила идентификации вредоносных программ.
7.	Дополнительная информация	При помощи утилиты ExifTool извлекаются метаданные о файле, которые помогают идентифицировать его контент.

8.2 Динамическое исследование

Для создания динамического исследования по файлу необходимо воспользоваться кнопкой «Создать», которая присутствует в следующих директориях:

- «Исследования» → «Динамические» → кнопка «Создать»;
- «Объекты анализа» → «Файлы» → кнопка «Отчет» → вкладка «Динамический анализ» → кнопка «Создать».

Для создания динамического исследования открывается форма (Рисунок 20).

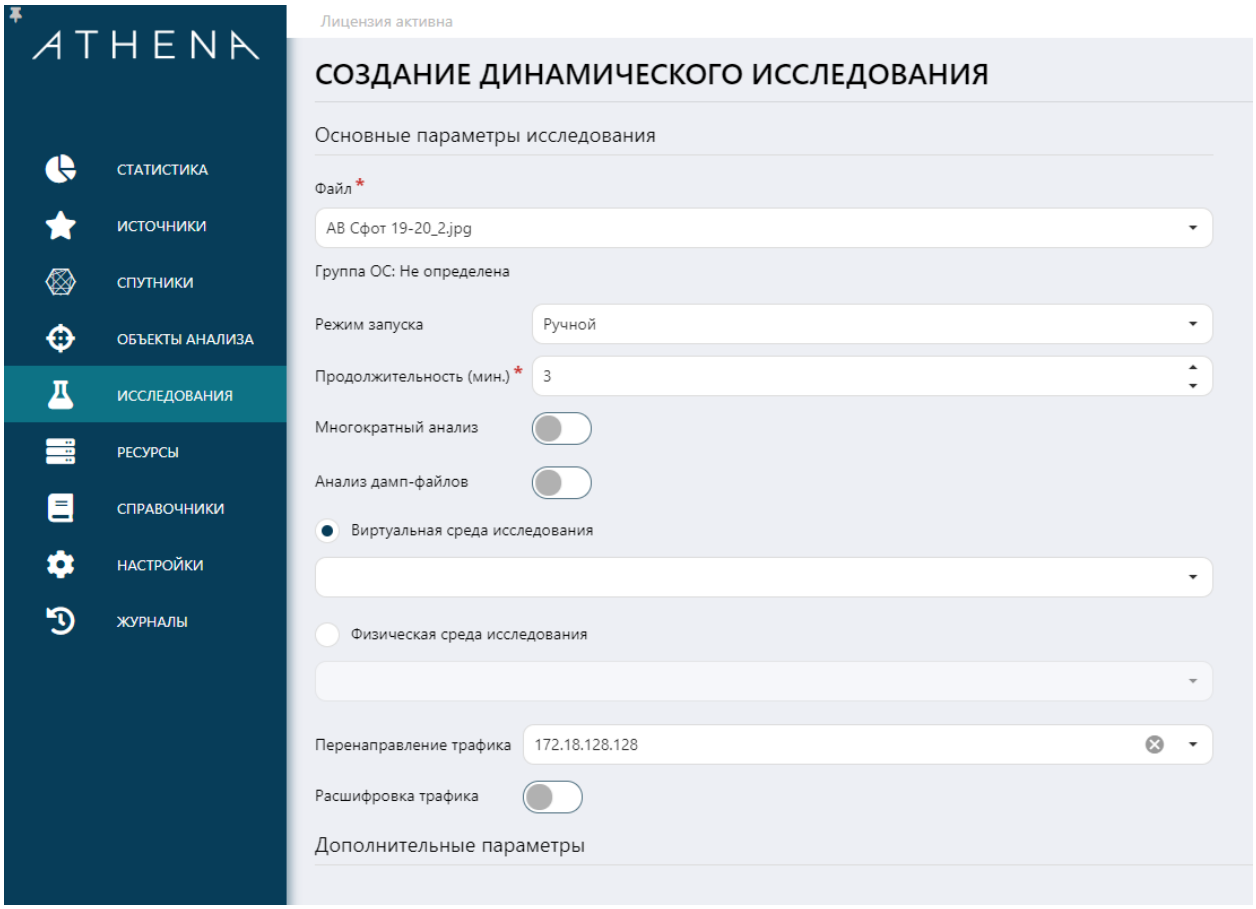


Рисунок 20. Окно создания нового динамического исследования

При создании динамического исследования необходимо указать параметры, описанные в таблице 10.

Таблица 10. Параметры настройки запуска динамического исследования

№	Параметр	Описание
1.	Файл	Выбор файла из выпадающего меню, в котором содержатся уже загруженные в систему файлы и прошедшие статический анализ.
2.	Группа ОС	Операционная система, в которой можно осуществить запуск файла и наблюдать его работу в ней.
3.	Режим запуска	В системе поддерживаются два режима запуска динамический исследований: – ручной;

№	Параметр	Описание
		– по сценарию. Если аналитик выбирает режим «по сценарию», то ему не требуется уже выбирать тип и вид «песочницы», т.к. она уже задана в выбранном сценарии и запустится автоматически.
4.	Продолжительность	Время продолжительности динамического исследования. Оно не включает в себя время запуска виртуальной машины, ее остановки и анализа событий поведения файла в ней. Минимальное рекомендуемое время динамического исследования – 3 минуты.
5.	Многократный анализ	Флаг, который активирует длительное исследование, как правило многочасовое. если поведение файла в «песочнице» требуется наблюдать в течение продолжительного промежутка времени.
6.	Анализ дамп-файлов	Флаг, который активирует сбор созданных исследуемым файлом других файлов (дампов) и анализ их статическим анализом.
7.	Виртуальная среда исследования	В выпадающем меню есть возможность выбора операционной системы и архитектуры виртуальной «песочницы» для проведения динамического исследования.
8.	Физическая среда исследования	В выпадающем меню есть возможность выбора операционной системы и архитектуры физической «песочницы» для проведения динамического исследования.

№	Параметр	Описание
9.	Перенаправление трафика	Возможность анонимизации сетевого трафика, который будет инициировать файл в «песочнице». Опция является рекомендованной к использованию, т.к. при проверке вредоносного ПО, которое будет обращаться к не легитимным адресам в сети Интернет, есть высокий риск попасть в «черный список» IP-адресов и доменов.
10.	Расшифровка трафика	Флаг, который активирует расшифровку сетевого трафика формата SSL, т.к. в нем могут присутствовать объекты для исследования. В зашифрованном трафике их проверить невозможно, поэтому применяется его расшифровка.
11.	Дополнительные параметры	Возможность добавления дополнительных команд, которые будут исполнены в процессе динамического исследования. Добавление дополнительных параметров возможно после выбора среды исследования.

После завершения ввода данных необходимо нажать кнопку «Запустить» и удостовериться, что новое динамическое исследование отобразилось в общей таблице динамических исследований со статусом «В очереди».

После того, как статус динамического исследования в таблице изменится на «Запускается», появится возможность перейти на рабочий стол виртуальной машины, для этого необходимо нажать на кнопку «Рабочий стол» (Рисунок 21).

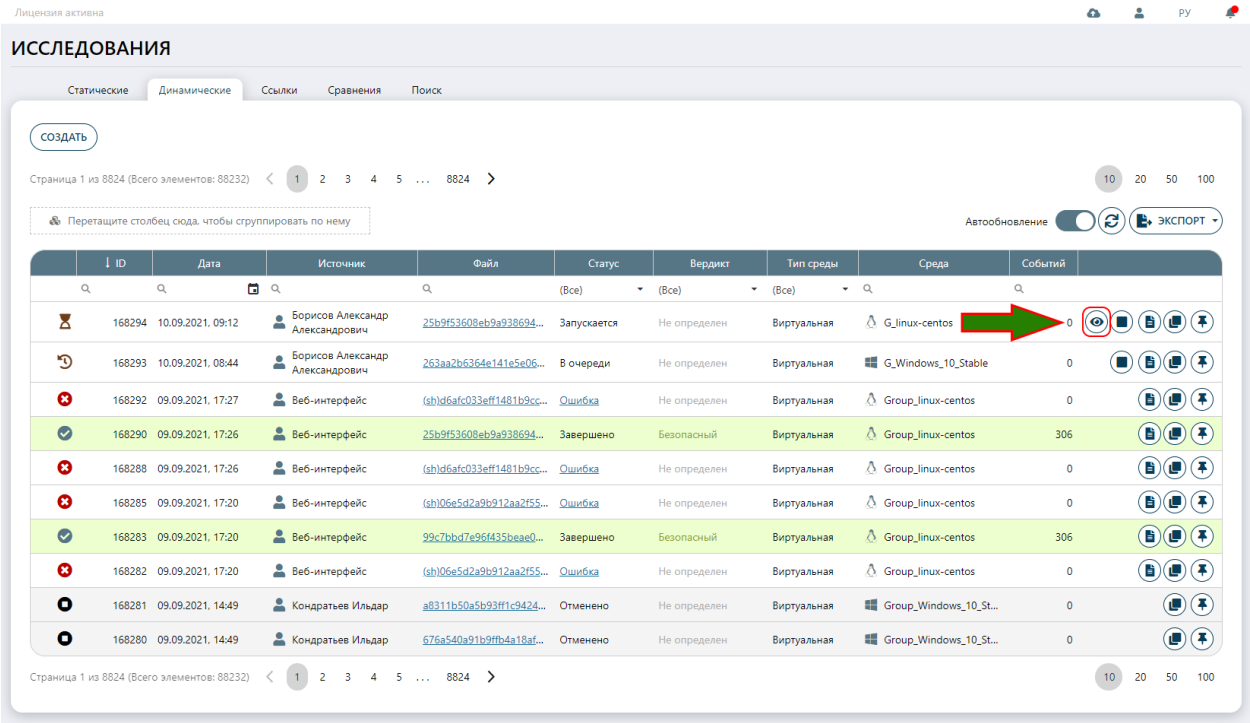


Рисунок 21. Запуск динамического исследования

Пример отображения рабочего стола виртуальной машины, в которой проводится исследование представлен ниже (Рисунок 22).

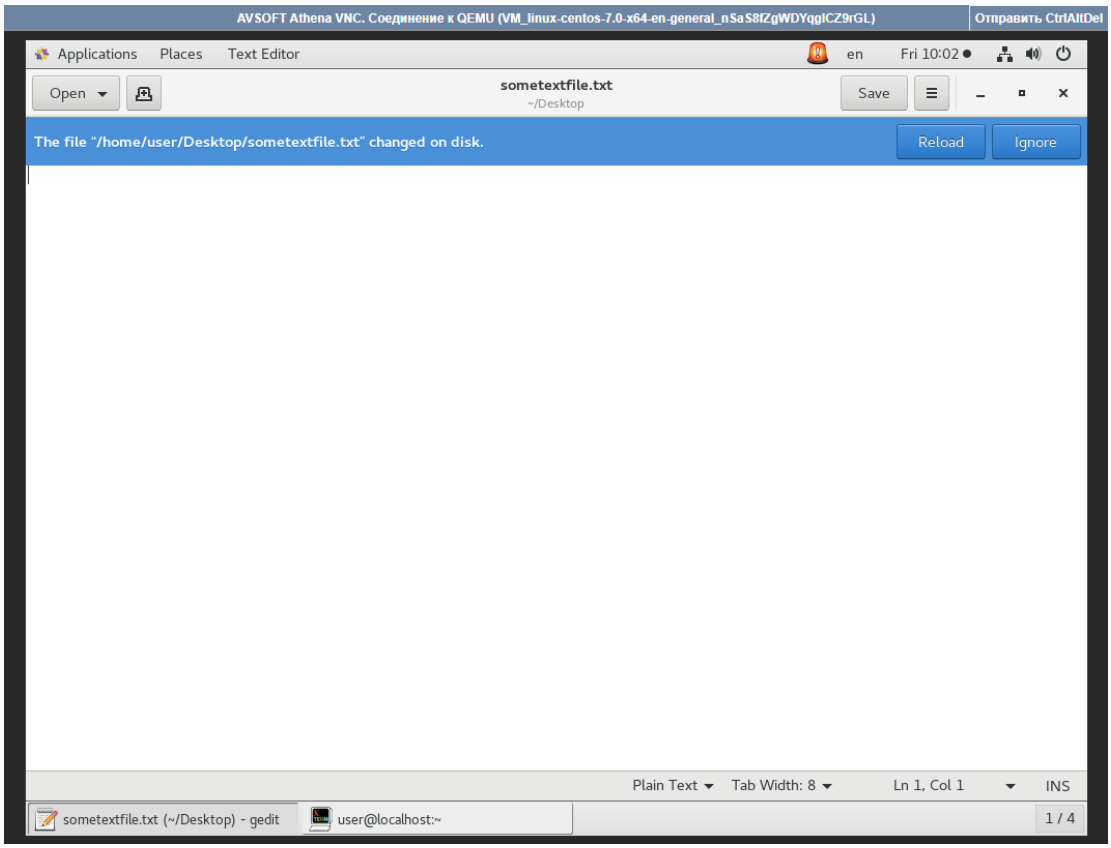


Рисунок 22. Рабочий стол виртуальной машины

В окне виртуальной машины на рабочем столе можно осуществлять действия, а также останавливать автоматическую имитацию действий пользователя при помощи сочетания клавиш «Ctrl+End».

Для остановки виртуальной машины во время исследования необходимо нажать иконку «Остановить» в таблице динамических исследований.

8.3 Сценарии исследований

В системе все динамические исследования идут по сценариям, которые определяют среду исследования с преднастроенными параметрами и правила анализа для каждого типа файла. Для запуска сразу нескольких файлов по сценарию необходимо выполнить переход «Объекты анализа» → «Файлы», далее выбрать флагом в общей таблице объекты, которые необходимо отправить на анализ (Рисунок 23).

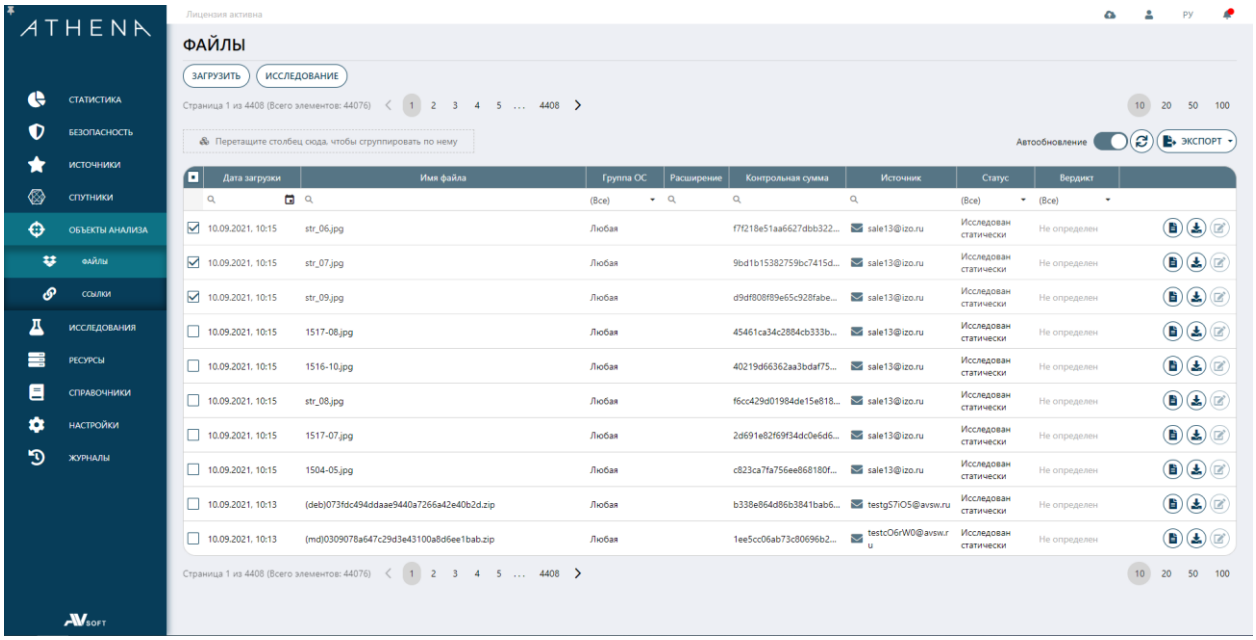


Рисунок 23. Выбор файлов для отправки на исследование по сценарию

После выбора файлов станет активна кнопка «Исследование», на которую нужно нажать, она откроет форму для выбора типа исследования «Создание исследований» (Рисунок 24).

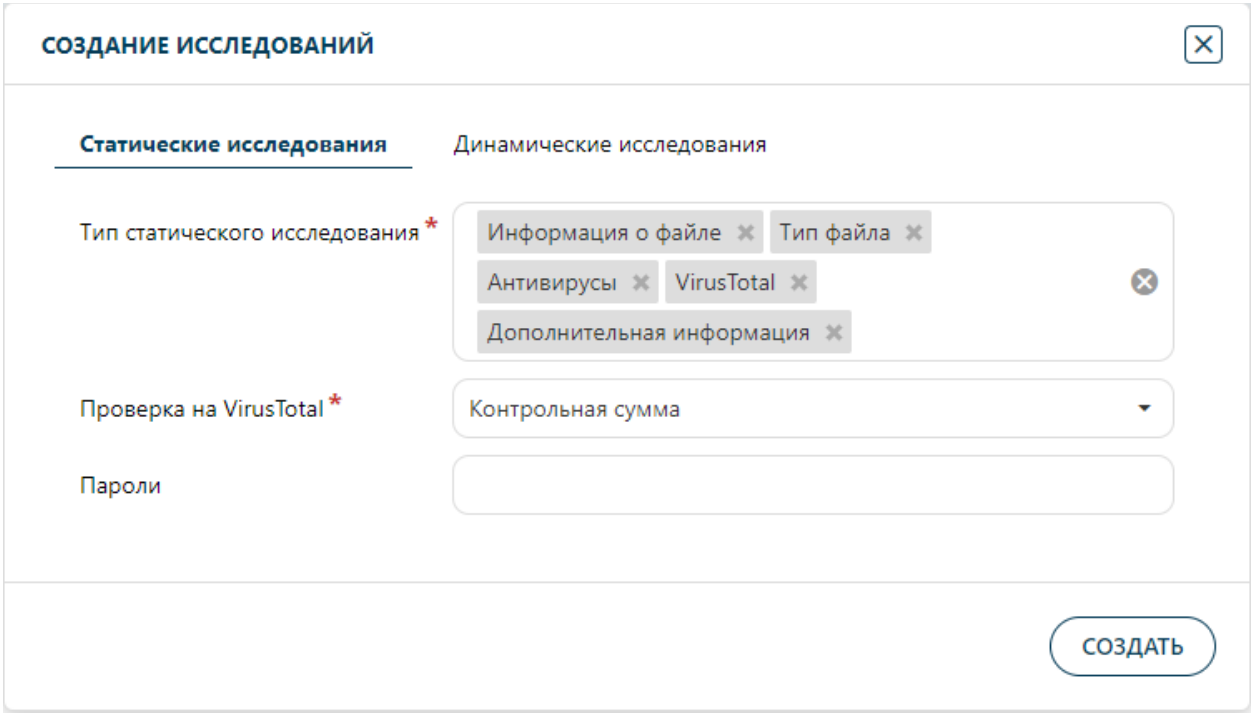


Рисунок 24. Создание исследований. Статические исследования

Перед отправкой файлов на динамическое исследование по сценарию, они должны пройти блок статической проверки. Для запуска статического исследования файлов необходимо указать параметры, описанные в таблице 7. После завершения ввода данных необходимо нажать кнопку «Создать» и удостовериться, что новое статическое исследование файлов отобразилось в таблице статических исследований.

Для выбора сценария динамического исследования файлов необходимо перейти в форме «Создание исследований» во вложенную вкладку «Динамические исследования» (Рисунок 25).

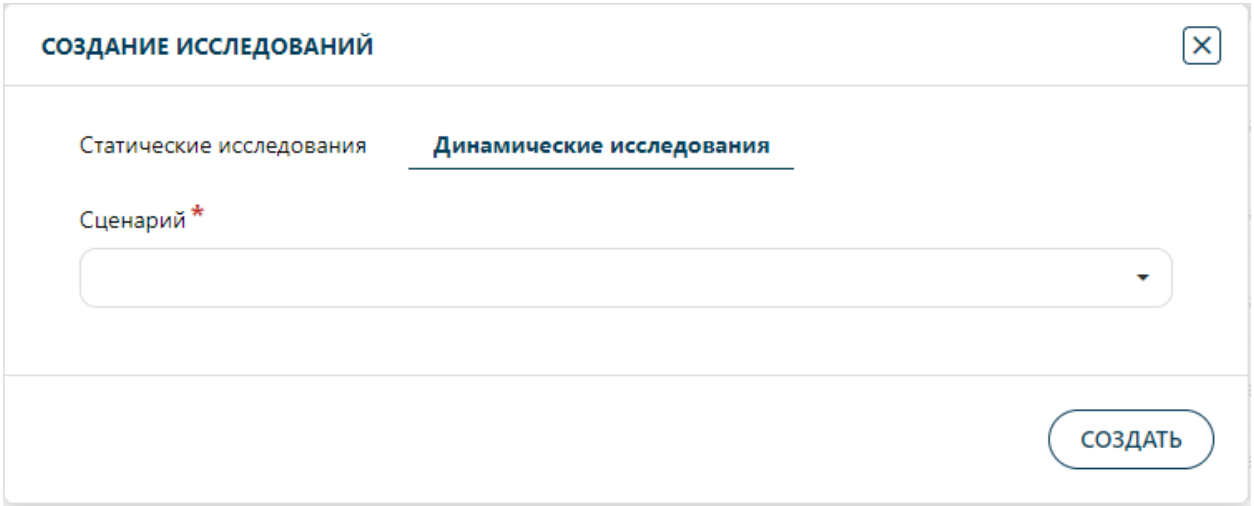


Рисунок 25. Создание исследований. Динамические исследования

После выбора сценария в выпадающем меню, необходимо нажать кнопку «Создать» и удостовериться, что новое динамическое исследование файлов отобразилось в общей таблице по пути «Исследования» → «Динамические».

8.4 Краткий отчет

Когда в общей таблице динамических исследований новому исследованию в колонке «Состояние» будет присвоен статус «Завершено», то пользователь может нажать на иконку «Отчет», чтобы ознакомиться с результатами анализа в кратком отчете (Рисунок 26).

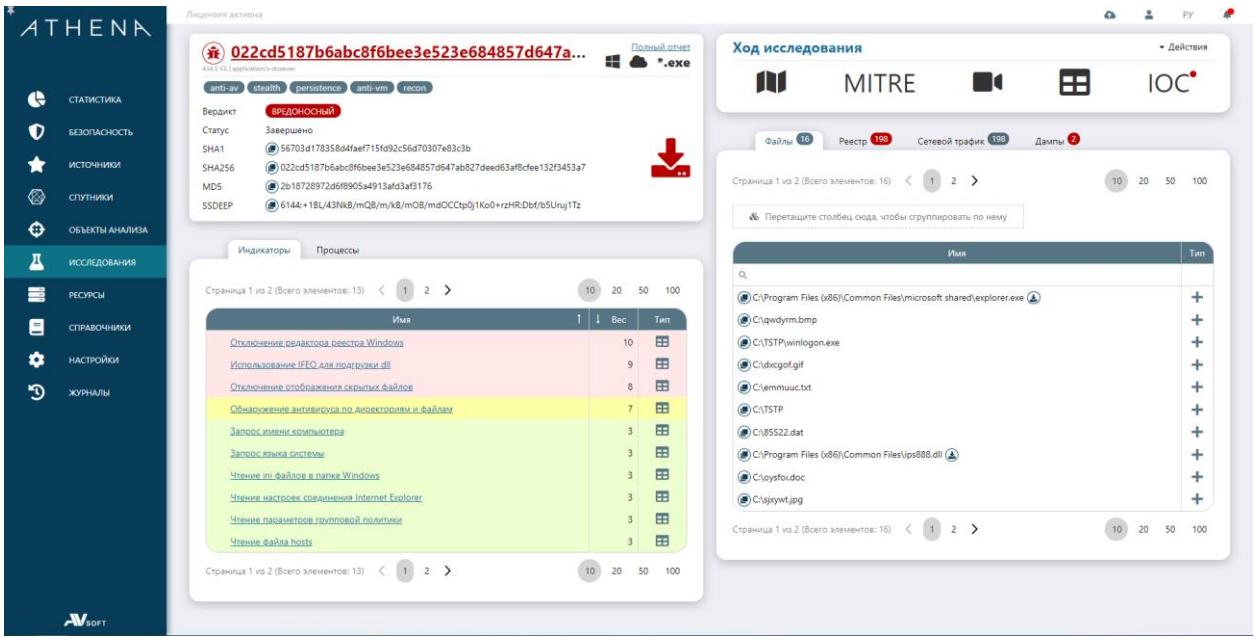


Рисунок 26. Отчет по динамическому исследованию

В отчете по динамическому анализу присутствуют параметры исследования, описанные в таблице 11.

Таблица 11. Описание параметров динамического отчета

№	Параметры	Описание
1.	Имя файла	Наименование файла, окрашенное в цвет его вердикта согласно правилам проверки системы.
2.	Теги	Ключевые ассоциативные компоненты поиска

№	Параметры	Описание
		значимой с точки зрения вредоносного поведения файла информации.
3.	Контрольные суммы	Уникальные идентификационные параметры файла.
4.	Скачать файл	Функция загрузки и сохранения файла на рабочую станцию.
5.	Действия	В данном функциональном разделе можно выполнить копирование динамического исследования для повторного запуска, а также выполнить печать отчета.
6.	Карта исследования	Графические отображение хода исследования по значимым для исследования процессам в операционной системе.
7.	MITRE	Методология декомпозиции основных этапов реализации кибератаки в ИТ-инфраструктуре с привязкой к тактикам и методам на каждом этапе реализации.
8.	Видео	Видео запись исследования файла в «песочнице».
9.	События	Таблица событий, собранных в процессе исследования файла в «песочнице».
10.	IOC	Индикаторы компрометации вредоносного поведения файла по результатам его проверки в динамическом анализе.
11.	Файлы	Созданные в процессе исследования файлы в «песочнице».
12.	Реестр	События в реестре операционной системы Windows.

№	Параметры	Описание
13.	Сетевой трафик	Взаимодействие файла в процессе исследования в «песочнице» с внутренней и внешней сетью Интернет.
14.	Дампы	Собранная информация о состоянии операционной системы и созданных объектов в ней на протяжении анализа файла в «песочнице».

В функциональном разделе «Действия» присутствуют следующие функции:

– Копировать исследования;

– Печать.

8.5 Полный отчет

В кратком отчете по динамическому анализу возможен переход в его полную, более детальную версию, при помощи нажатия на активную ссылку «Полный отчет» (Рисунок 27).

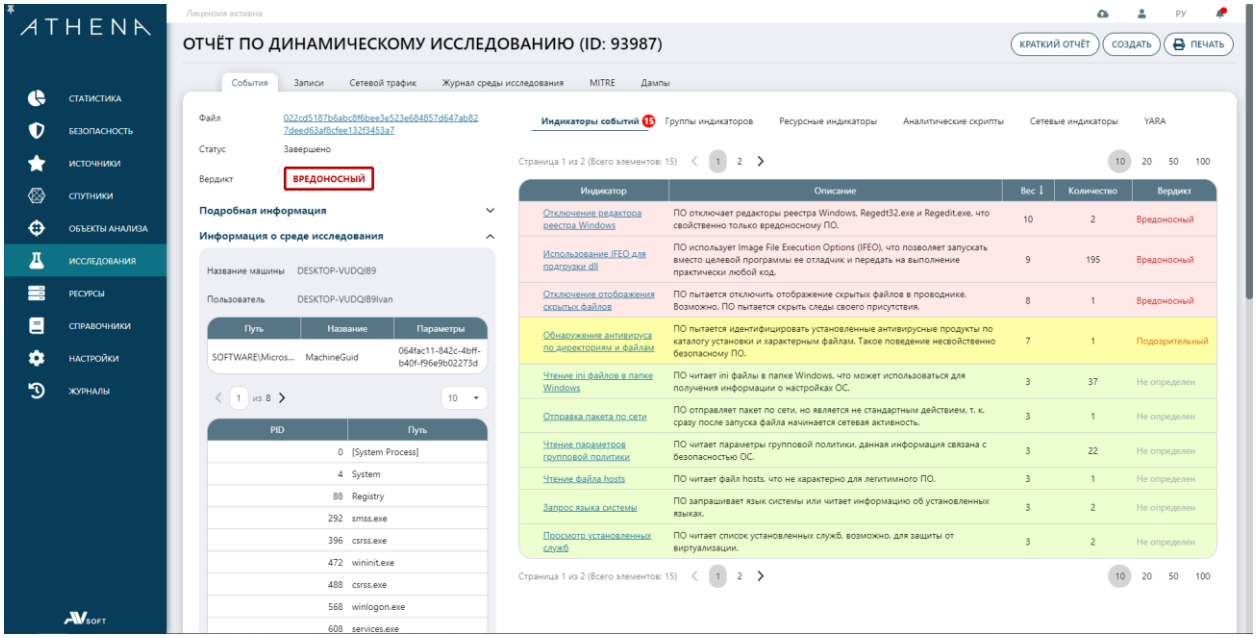


Рисунок 27. Полный отчет по динамическому исследованию

В полном отчете можно получить подробную информацию по параметрам исследования, описанным в таблице 12.

Таблица 12. Описание параметров подробного отчета

№	Параметры	Описание
1.	События	
1.1	Среда исследования	Подробная информация о среде исследования, ее параметрах запуска и детальном времени работы.
1.2	Индикаторы событий	Логические правила индикации легитимности действий файла в исследуемой среде на основании собранных событий в «песочнице».
1.3	Группы индикаторов	Логические правила индикации легитимности действий файла на основании индикаторов событий.
1.4	Ресурсные индикаторы	Логические правила индикации повышенного использования ресурсов исследовательской среды.
1.5	Аналитические скрипты	Последовательность команд для выполнения операций по индикации не легитимных действий файла в исследовательской среде.
1.6	Сетевые индикаторы	Логические правила индикации легитимности сетевого взаимодействия файла в процессе его работы в исследовательской среде.
1.7	YARA	Скриптовые логические индикаторы на базе формирования yara-правил.
1.8	Таблица событий	Событий, собранные в процессе исследования файла в «песочнице».
1.9	Процессы	Этапы выполнения программы на уровне процессов в операционной

№	Параметры	Описание
		системе.
1.10	Карта исследований	Наглядное отображение хода исследования, связи процессов между собой и результатов их выполнения.
2.	Записи	
2.1	Видео	Видеозапись всего исследования в «песочнице» для наглядного ознакомления с ходом запуска и работы файла в «песочнице».
2.2	Снимки	Скриншоты экрана исследования файла в «песочнице» для быстрого и наглядного ознакомления с результатами его работы.
3.	Сетевой трафик	
3.1	Соединения	Внутренние и внешние сетевые соединения, инициированные файлом в процессе своей работы в «песочнице».
3.2	Дамп сетевого трафика	В дампах содержится весь сетевой трафик, зафиксированный в «песочнице» в формате *pcap.
3.3	Дамп расшифрованного сетевого трафика	В дампах содержится расшифрованный в «песочнице» сетевой трафик в формате *pcap.
3.4	DNS	Перечень доменных имен и соответствующих им ip-адресов.
3.5	HTTP(S)-запросы	Перечень HTTP и HTTPS запросов.
3.6	Suricata	Внешний аналитический сервис для анализа сетевого трафика.

№	Параметры	Описание
3.7	Moloch	Внешний аналитический сервис для анализа сетевого трафика.
4.	Журнал среды исследований	Запись системных событий исследовательской среды.
5.	MITRE	Методология, позволяющая проследить полный жизненный цикл кибератаки в ИТ-инфраструктуре.
6.	Дампы	Собранная информация о состоянии операционной системы и созданных объектов в ней на протяжении анализа файла в «песочнице».

8.6 Визуальные компоненты

В динамическом отчете большое значение имеют наглядные визуальные компоненты, которые могут в различных функциональных категориях продемонстрировать процесс исследования файла в «песочнице».

Карта исследований по основным процессам, запущенным в операционной системе доступна к просмотру при выполнении перехода «Исследования» → «Динамические» → «Отчет» → «Карта исследования» (Рисунок 28).

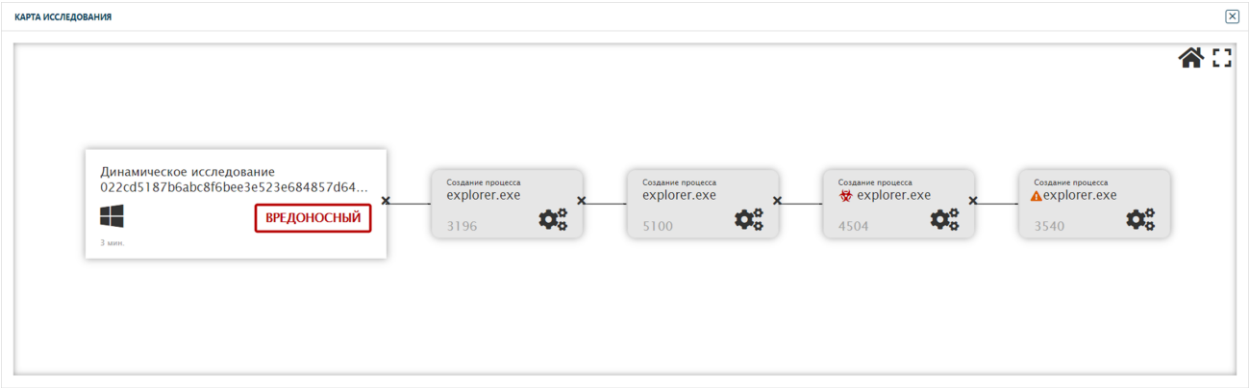


Рисунок 28. Карта динамического исследования

На карте исследований процессы с подозрительными и вредоносными действиями имеют специальные отметки, если процесс не имеет специальной

отметки – он признан безопасным. Описание отметок процессов динамического исследования представлено в таблице 13.

Таблица 13. Описание отметок процессов динамического исследования

№	Вид отметки	Описание
1.		Данный значок обозначает процесс с подозрительными действиями.
2.		Данный значок обозначает процесс с вредоносными действиями.

Для просмотра записи всего исследования файла в «песочнице» необходимо выполнить переход «Исследования» → «Динамические» → «Отчет» → «Видео» (Рисунок 29).

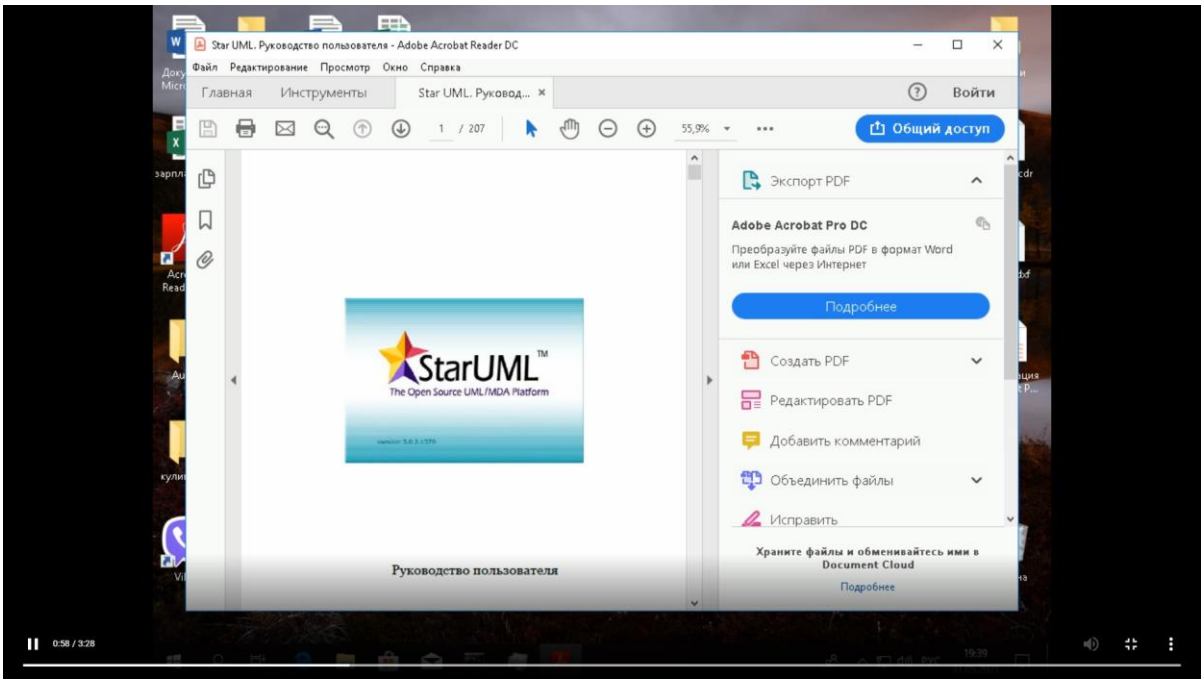


Рисунок 29. Видеозапись исследования файла в «песочнице»

Видеозапись имеет формат *mp4, для ее скачивания и сохранения на рабочей станции необходимо нажать на троеточие в нижнем правом углу и выбрать опцию «Скачать». Также присутствует функция просмотра записи сразу в окне отчета, для этого необходимо при нажатии на троеточие выбрать опцию «Картинка в картинке».

Снимки экрана исследования в «песочнице» для оперативного ознакомления с ходом исследования в «песочнице» можно найти по пути «Исследования» → «Динамические» → «Отчет» → «Полный отчет» → «Записи» → «Снимки» (Рисунок 30).

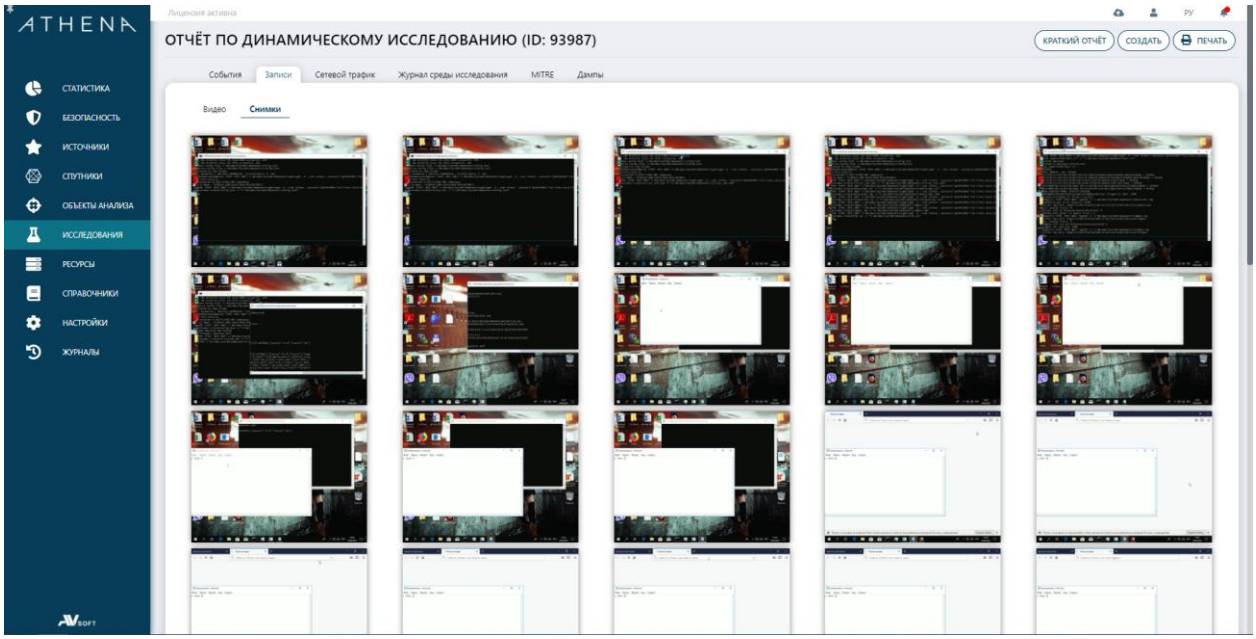


Рисунок 30. Снимки экрана исследования файла в «песочнице»

Каждый снимок можно увеличить при нажатии на него.

Графики использование ресурсов «песочницы» на протяжении анализа можно посмотреть выполнив переход «Исследования» → «Динамические» → «Отчет» → «Полный отчет» → «События» → «Процессы» (Рисунок 31).

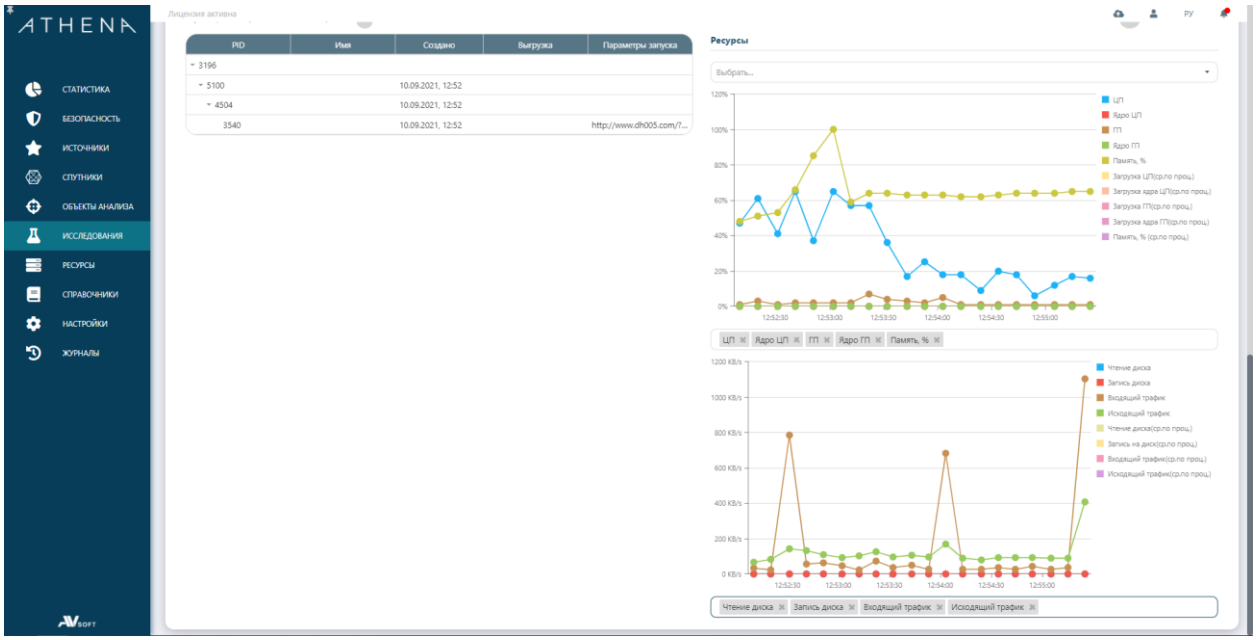


Рисунок 31. Графики нагрузки на ресурсы «песочницы»

Взаимодействие файла по сети можно посмотреть на карте, на которой наглядно видна директория подключения (Рисунок 32).

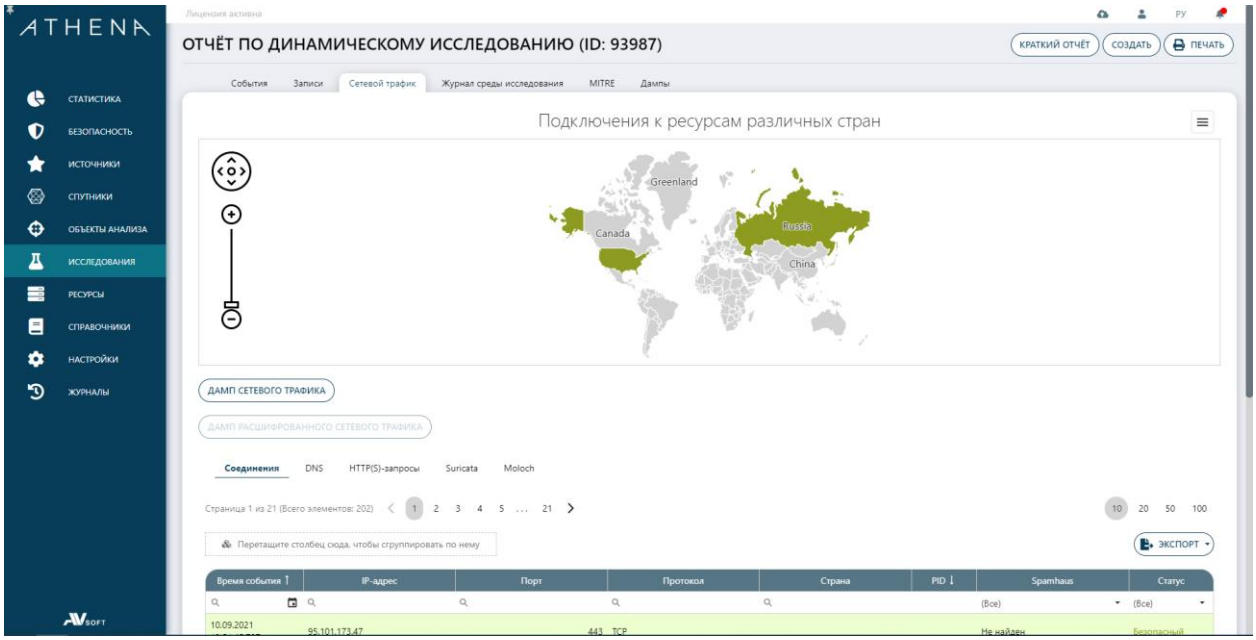


Рисунок 32. Карта взаимодействия файла по сети в «песочнице»

При нажатии на конкретную страну осуществляется фильтрация адресов и сетевых запросов в таблице.

В данном функциональном разделе можно скачать для дальнейшего анализа дампы следующих типов:

- Дамп сетевого трафика;
- Дамп расшифрованного сетевого трафика.

9 Мониторинг источников

9.1 Веб-трафик

Во вкладке «Веб-трафик» содержится информация по проверяемым объектам, с которыми сталкивается пользователь, работая в глобальной сети Интернет (Рисунок 33).

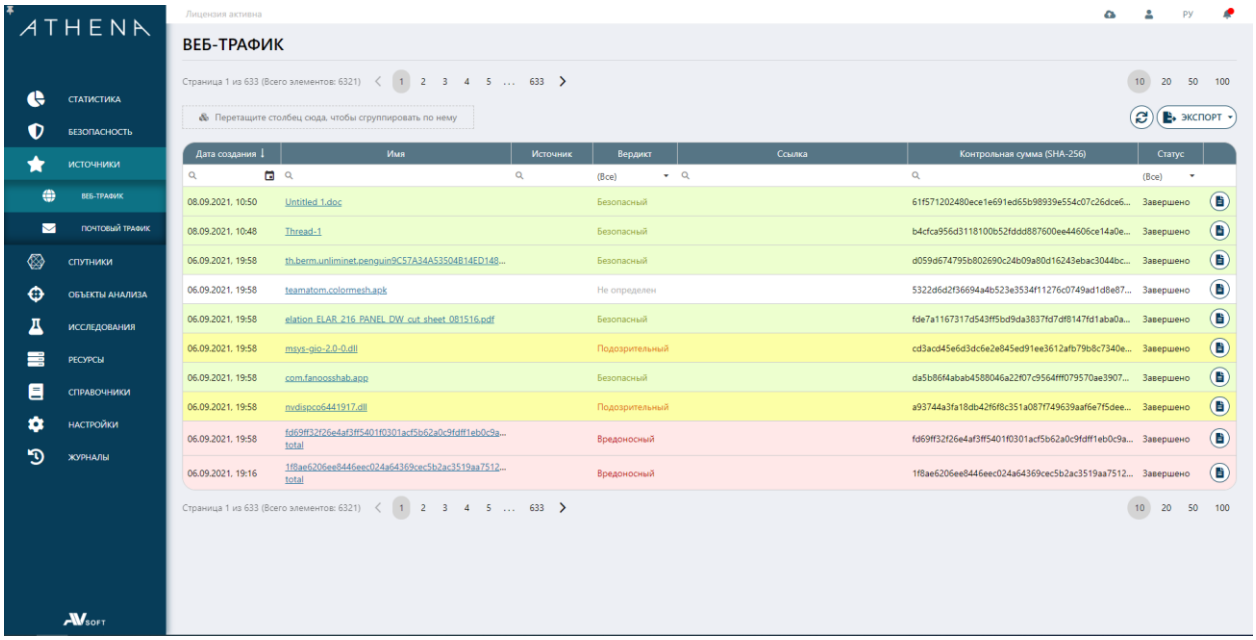


Рисунок 33. Раздел «Веб-трафик»

Все объекты, которые пользователь пытается скачать посредством браузера, сначала проходят проверку в системе, а потом уже допускаются к скачиванию пользователем на свою рабочую станцию.

При нажатии на иконку «Отчет» будет отображаться общий отчет по файлу, скаченному по веб-ссылке.

Для настройки веб-трафика вам необходимо обратиться к администратору ПК ATHENA.

9.2 Почтовый трафик

Во вкладке «Почтовый трафик» содержится информация по всем письмам, имеющим вложения и ссылки, которые проходят проверку в системе (Рисунок 34).

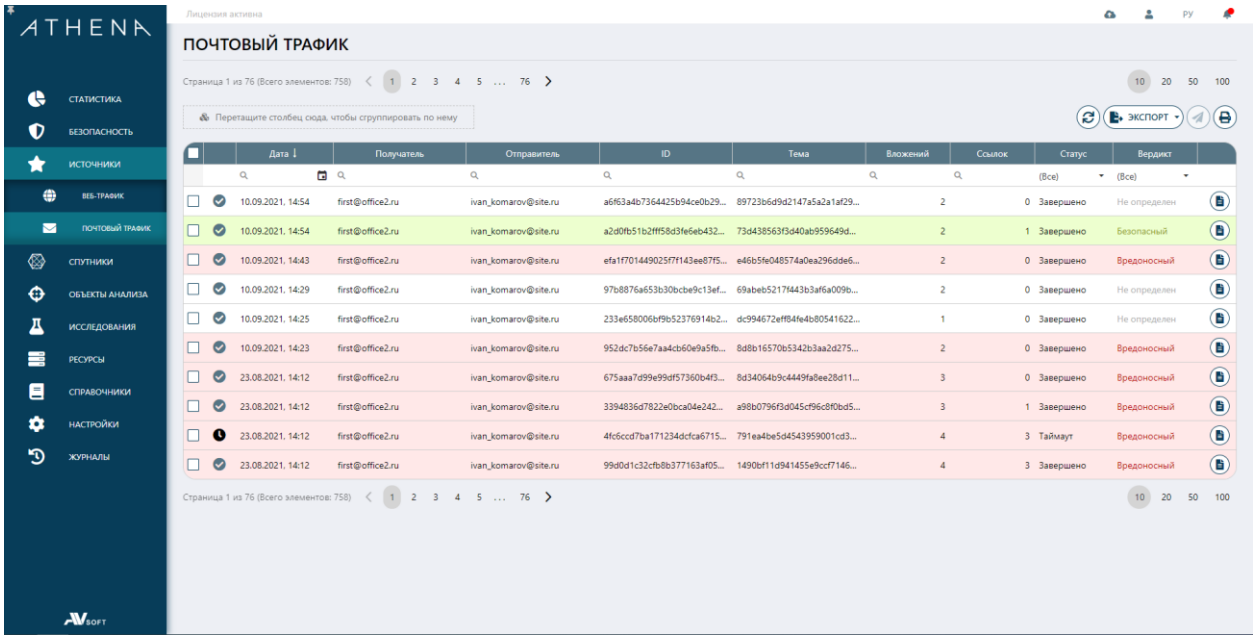


Рисунок 34. Раздел «Почтовый трафик»

> **! Для настройки почтового трафика вам необходимо обратиться к администратору ПК ATHENA.**

Для перехода в отчет по проверке письма необходимо нажать на иконку «Отчет» (Рисунок 35).

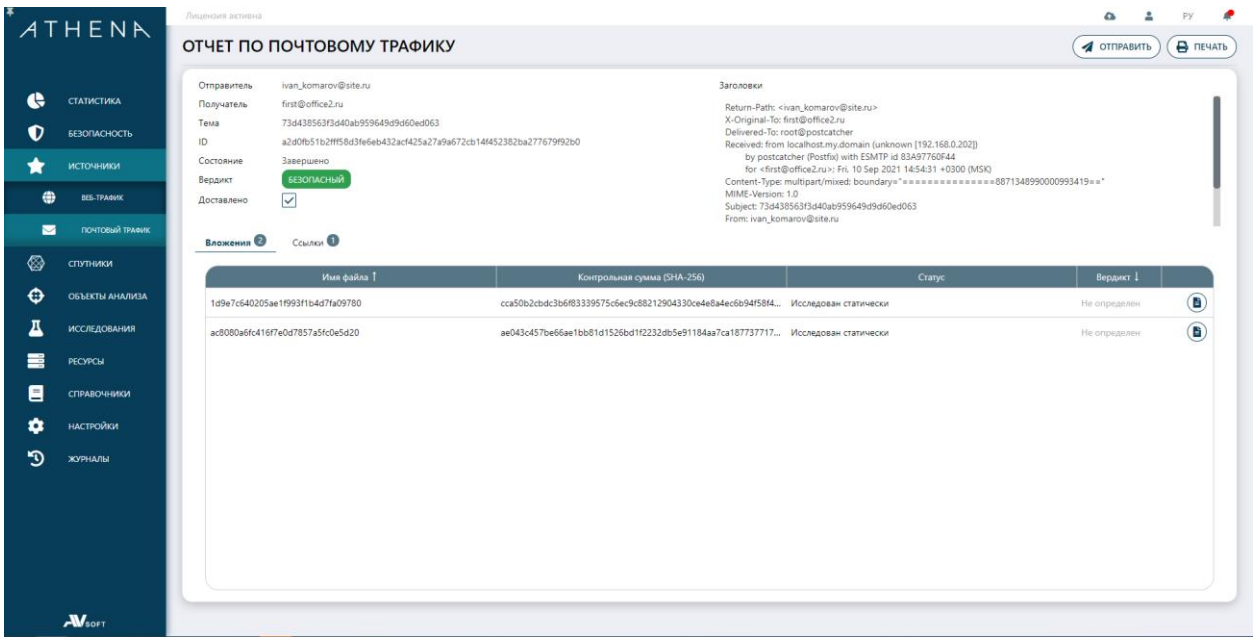


Рисунок 35. Отчет по почтовому трафику

В отчете по проверке письма отображается идентифицирующая информация по письму, результаты проверки вложений в нем и ссылок, также можно получить информацию по заголовкам электронного письма.

10 Спутники

10.1 Агенты

В разделе «Агенты» присутствует информация по агентам на рабочие места, подробная информация по работе с ними содержится в руководстве по работе с агентами ПК ATHENA (Рисунок 36).

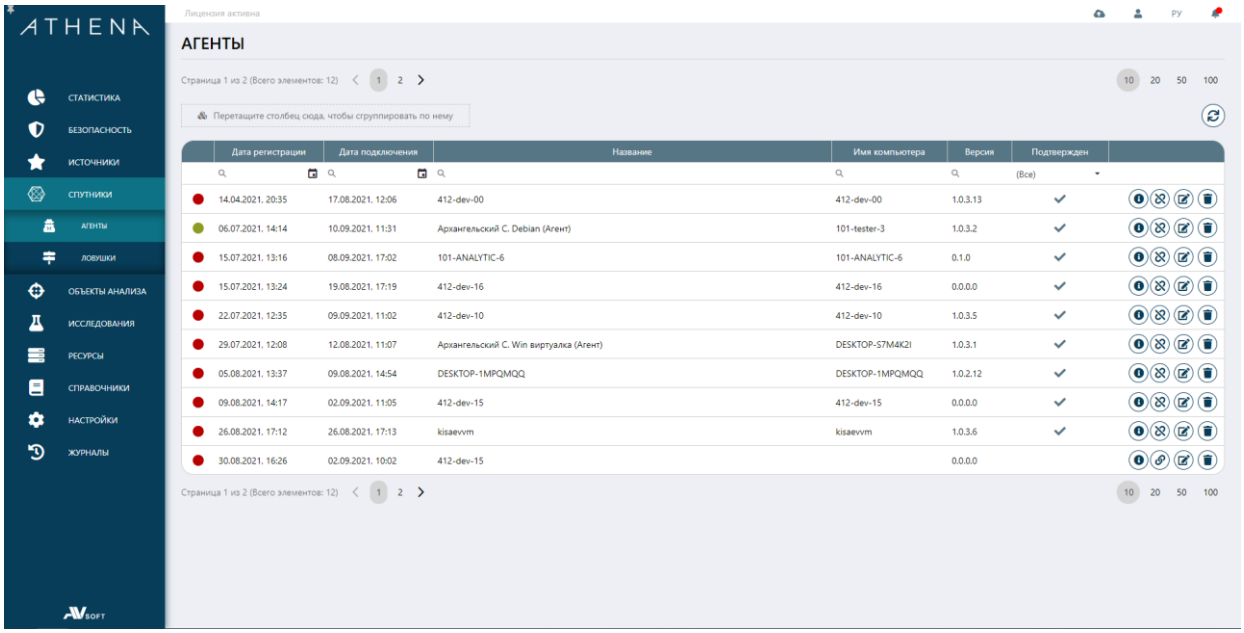


Рисунок 36. Раздел «Агенты»

> **! Для настройки агентов на рабочие места необходимо обратиться к администратору ПК ATHENA.**

10.2 Ловушки

В разделе «Ловушки» присутствует информация о ловушках, предусмотренных в ПК ATHENA, по умолчанию при переходе в раздел ловушки отображается вложенная вкладка «Хосты» (Рисунок 37).

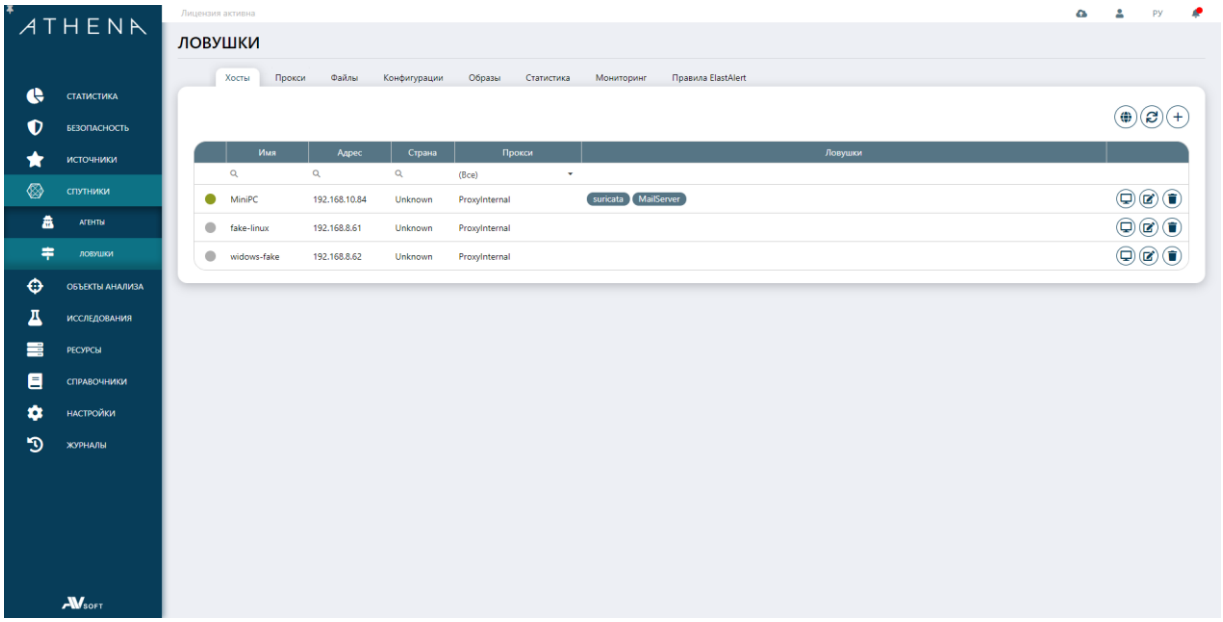


Рисунок 37. Раздел «Ловушки» вложенная вкладка «Хосты»

11 Ресурсы

В системе присутствует отдельный раздел, связанный с ресурсами динамического анализа, который называется «Ресурсы». В нем присутствует идентификационная информация и статусы о состоянии всех исследовательских сред (Рисунок 38).

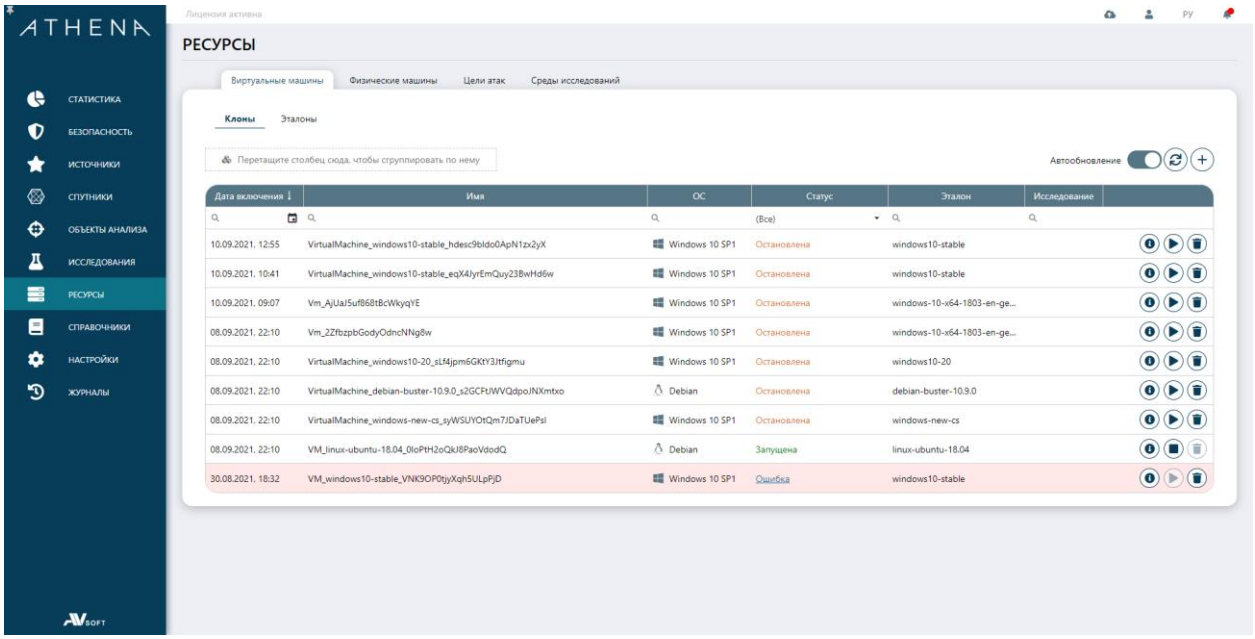


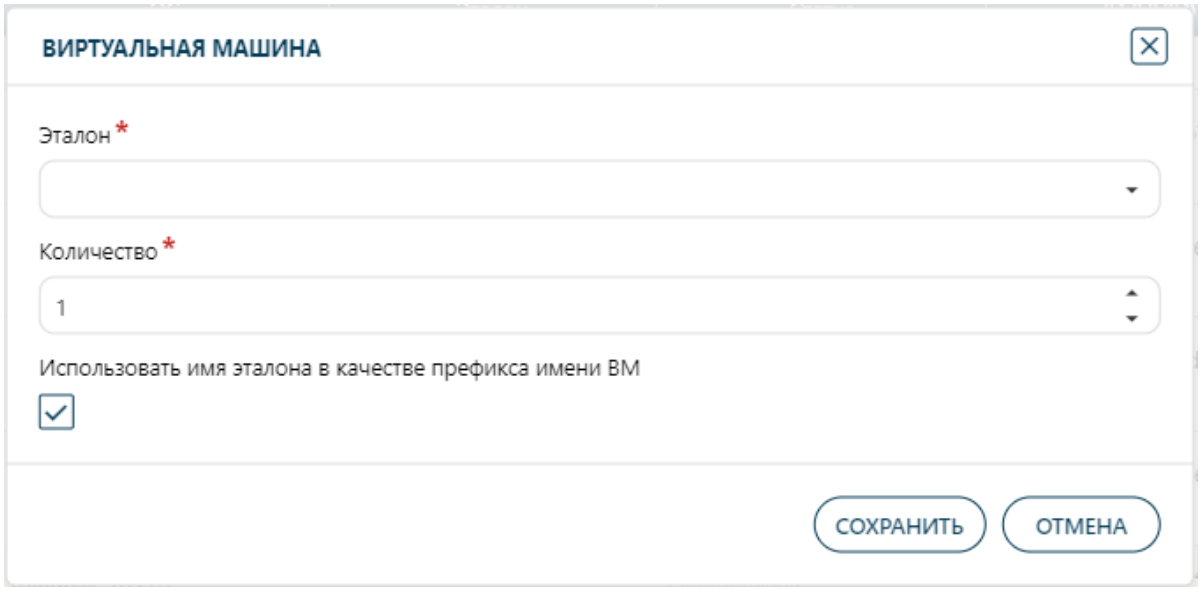
Рисунок 38. Раздел «Ресурсы» вкладка «Виртуальные машины»

Во вкладке «Виртуальные машины» присутствует общая информационная таблица по всем виртуальным ресурсам, используемым для запуска в них файлов и отслеживания поведения.

Виртуальные машины могут быть клонированы, что позволяет проводить в них параллельно сразу несколько динамических исследований. Процесс клонирования осуществляется на базе эталона – шаблонного образца, который не изменяется и не используется в исследованиях, а служит только для целей создания новых клонов.

Пользователь может увеличить количество клонов виртуальных машин, если позволяют физические ресурсы сервера, на котором развернута система. При попытке добавления избыточного количества клонов, которое может привести к дестабилизации работы динамического анализа, система заблокирует эту попытку и отобразит предупреждающее сообщение.

Для добавления нового клона необходимо нажать на кнопку «Добавить» в разделе «Виртуальные машины» вкладка «Клоны», которая отобразит форму для заполнения «Виртуальная машина» (Рисунок 39).



39. Добавление нового клона виртуальной машины

В поле «Эталон» необходимо выбрать эталон, на базе которого будет создаваться новый клон виртуальной машины. В поле «Количество» необходимо указать требуемое количество клонов. Флаг «Использовать имя эталона в качестве префикса имени ВМ» является рекомендуемым для привязки к эталону созданных клонов и удобного поиска. После завершения

ввода данных необходимо нажать кнопку «Сохранить» и удостовериться в том, что созданный клон отобразился в общей таблице клонов.

> **!** **Кастомизация и добавление эталона осуществляется инженерами ПК ATHENA.**

Если клон не отрабатывает штатно, то он будет отмечен системой, как неработоспособный и исследования с него будут переброшены на другие. Пример присвоения системой статуса неработоспособного клона представлен на рисунке 40.

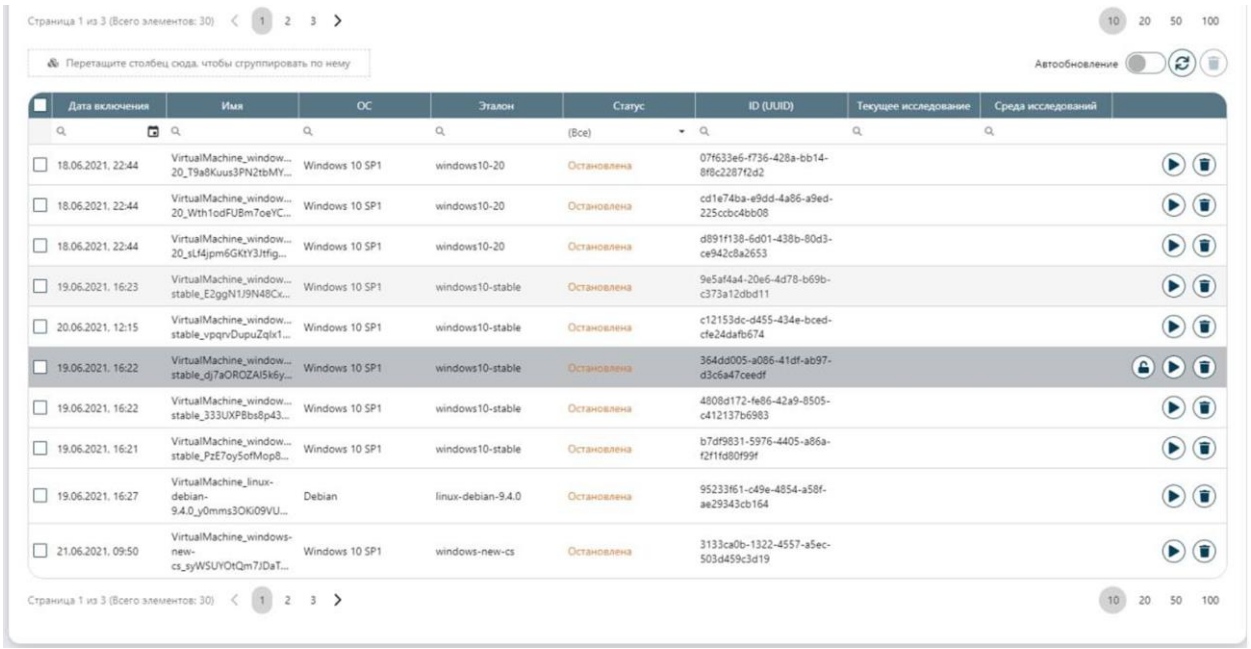


Рисунок 40. Отметка системой неработоспособного клона

Во вложенной вкладке «Эталоны» собрана информация по всем имеющимся в системе эталонным виртуальным средам.

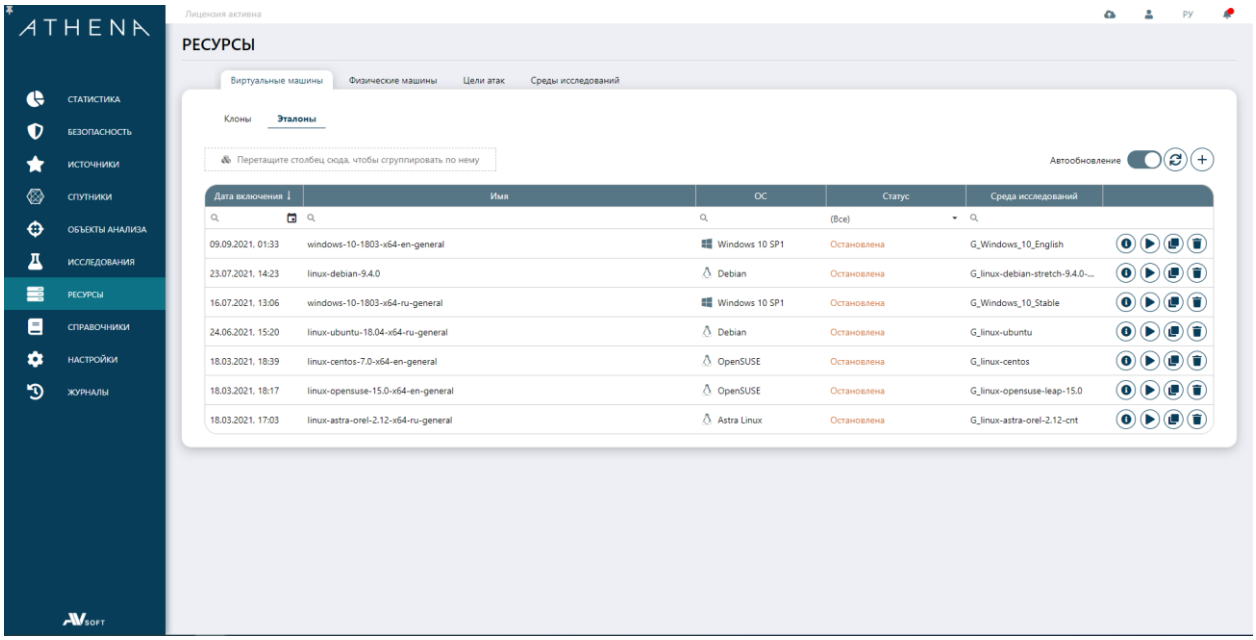


Рисунок 41. Вкладка «Виртуальные машины» вложенная вкладка «Эталоны»

Для добавления новой эталонной виртуальной среды необходимо нажать кнопку «Добавить». После этого на экране отобразится форма «Эталон» (Рисунок 42).

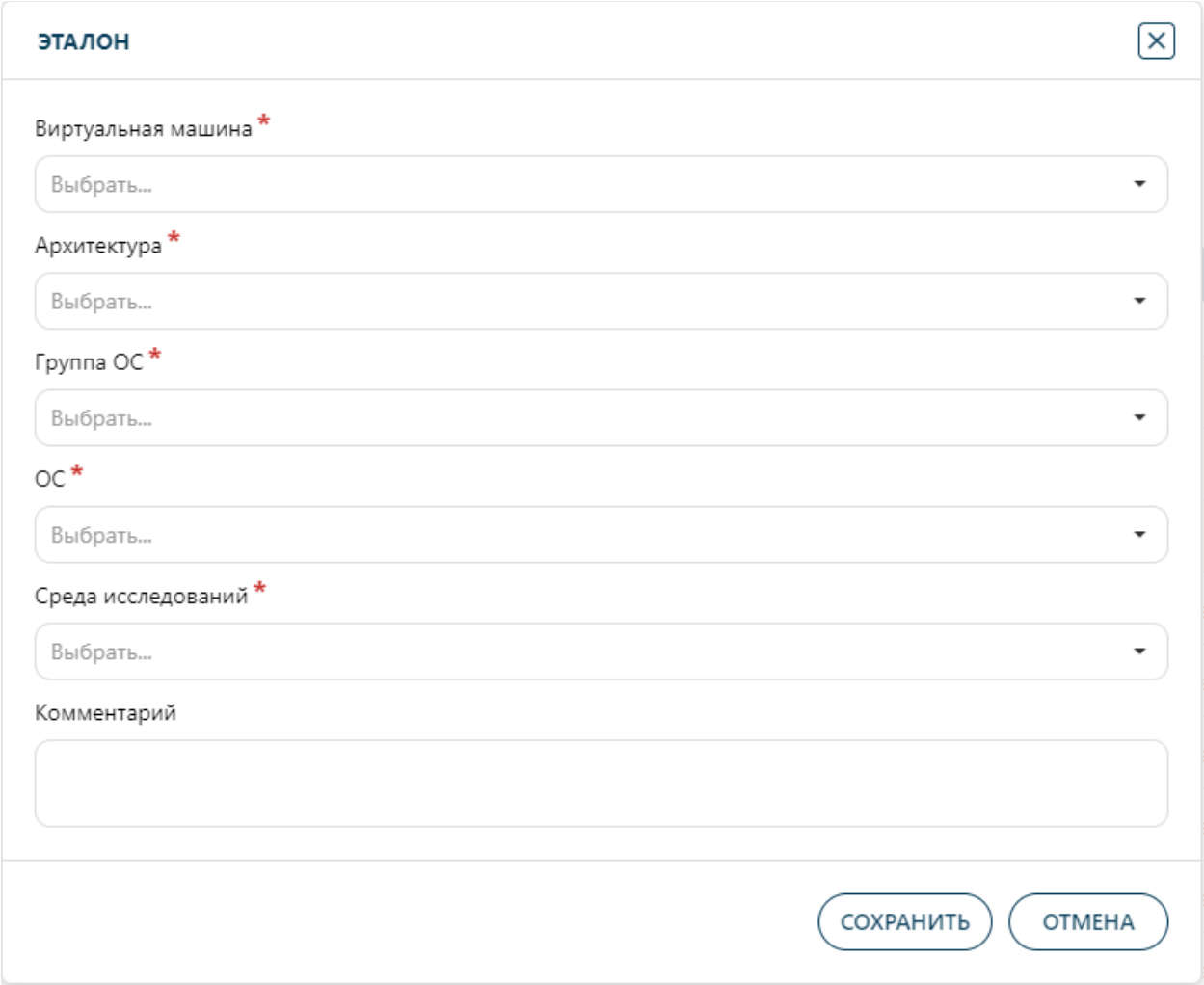


Рисунок 42. Форма добавления эталонной виртуальной среды

Для добавления нового эталона необходимо указать параметры, описанные в таблице 14.

Таблица 14. Описание параметров добавляемого эталона

№	Параметр	Описание
1.	Виртуальная машина	Выбор названия виртуальной машины для создаваемого эталона.
2.	Архитектура	Выбор архитектуры операционной системы для создаваемого эталона.
3.	Группа ОС	Выбор группы операционных систем к которой будет относится создаваемый эталон.

№	Параметр	Описание
4.	ОС	Выбор операционной системы создаваемого эталона. Зависит от выбранной группы ОС.
5.	Среда исследований	Выбор среды исследования создаваемого эталона. Зависит от выбора ОС. Все виртуальные машины должны обязательно иметь группу для возможности отправки файлов на проверку сразу на несколько физических сред.
6.	Комментарий	Комментарий к создаваемому эталону.

После ввода указанных параметров необходимо нажать кнопку «Сохранить» и удостовериться в том, что созданный эталон отобразился в общем списке эталонов.

Во вкладке «Физические машины» присутствуют физические исследовательские среды, которые используются для динамического анализа аналогично виртуальным ресурсам (Рисунок 43).

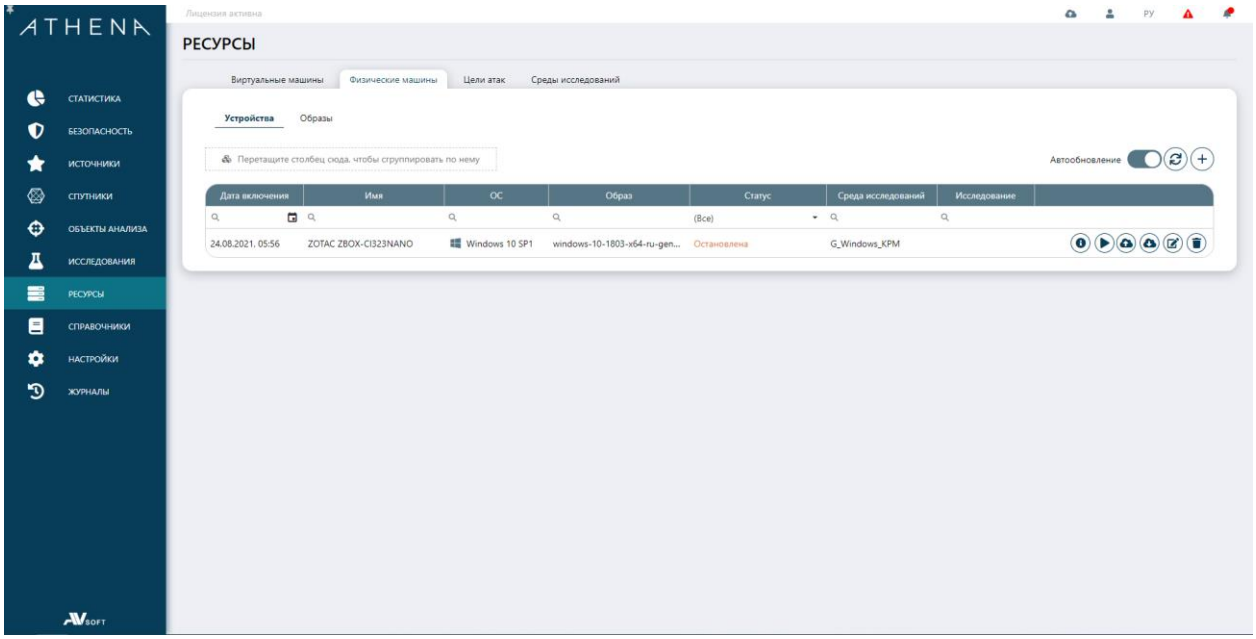


Рисунок 43. Вкладка «Физические машины» вложенная вкладка «Устройства»

Для добавления физической машины необходимо нажать кнопку «Добавить», которая откроет форму для заполнения (Рисунок 44).

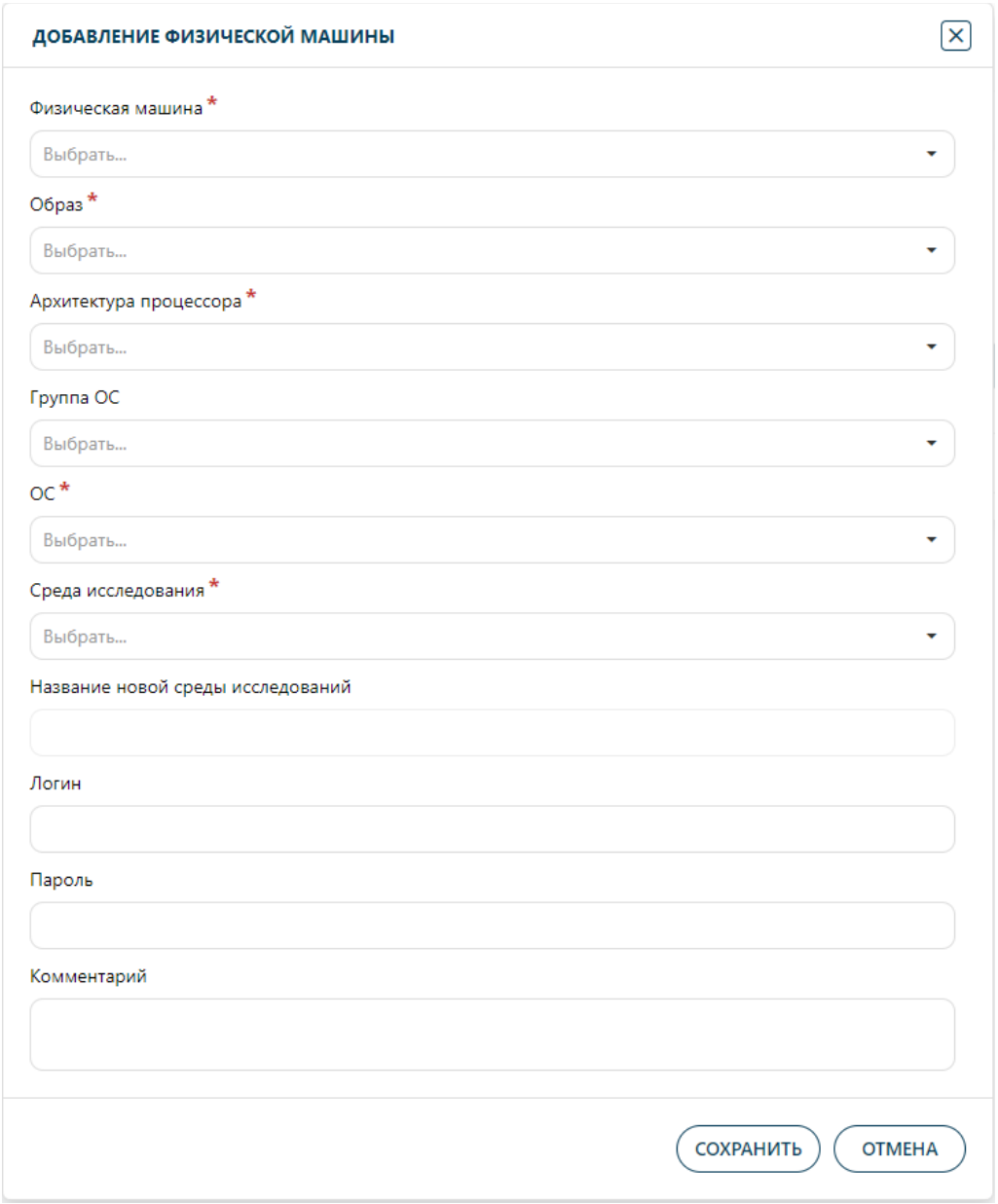


Рисунок 44. Форма «Добавление физической машины»

В форме добавления новой физической машины необходимо указать параметры, описанные в таблице 15.

Таблица 15. Описание параметров создания новой физической машины

№	Параметры	Описание
1.	Физическая машина	Выбрать из выпадающего списка новую физическую машину, не зарегистрированную ранее в общем списке таблицы.

№	Параметры	Описание
2.	Образ	Необходимо выбрать в выпадающем списке сохранённую копия жесткого диска с имитационной средой, которая именуется в системе образом.
3.	Архитектура процессора	Архитектура процессора физической машины, на которую разворачивается образ.
4.	Группа ОС	Группа операционных систем, к которой относится операционная система физической машины.
5.	ОС	Операционная система физической машины, на которую разворачивается образ.
6.	Среда исследования	Группа нескольких физических сред. Все виртуальные машины должны обязательно иметь группу для возможности отправки файлов на проверку сразу на несколько физических сред.
7.	Название новой среды исследования	Название группы физических машин для проведения динамических исследований.
8.	Логин	Логин от рабочей станции, на которую разворачивается образ диска.
9.	Пароль	Пароль от рабочей станции, на которую разворачивается образ диска.
10.	Комментарий	Комментарий для добавляемой физической машины.

По завершении ввода данных необходимо нажать кнопку «Сохранить» и удостовериться, что новая физическая машина отобразилась в общей таблице физических машин.

! Группа используется при создании шаблона исследования для использования его в сценарии.

Во вложенной вкладке «Образы» присутствуют образы жесткого диска, которые разворачиваются на физической машине для проведения динамических исследований (Рисунок 45).

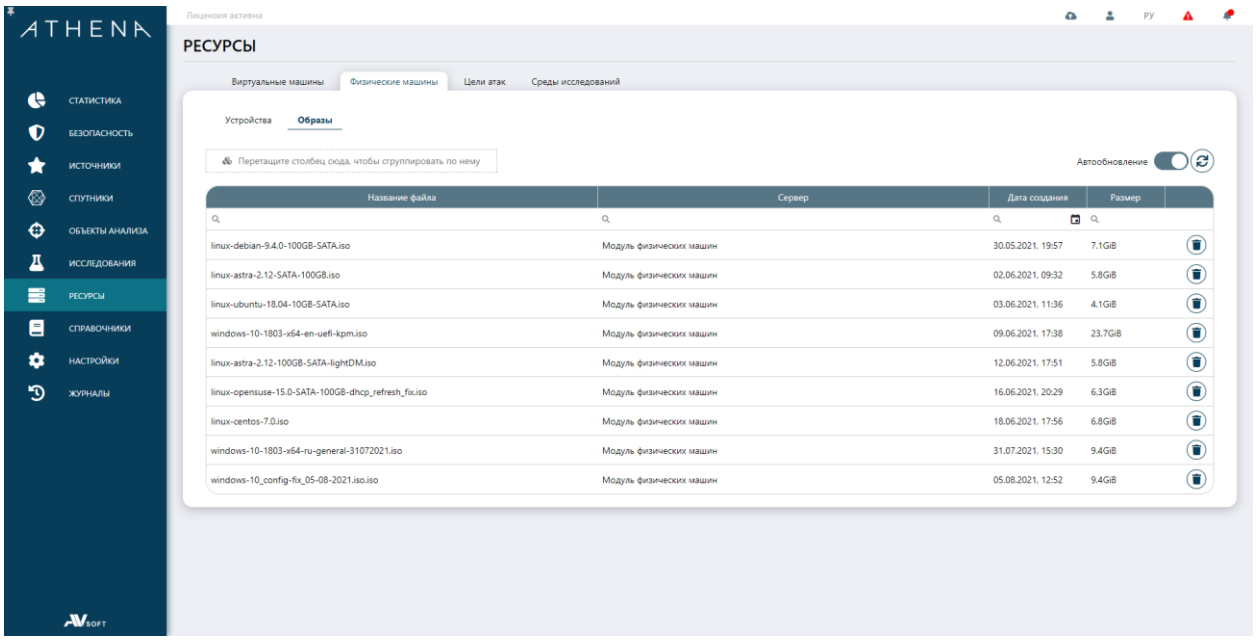


Рисунок 45. Образы для физических машин

! Для кастомизации и интеграции новой физической машины или образов необходимо обратиться к инженеру ПК ATHENA.

Система поддерживает интеграцию с системами класса «Deception», из которых возможен проброс атак и файлов в «песочницу» для детального исследования. При наличии такой интеграции во вкладке «Цели атак» содержится информация по «песочницам» (имитационным средам проверки динамического анализа), в которые могут быть проброшены кибератаки из систем класса «Deception» (Рисунок 46).

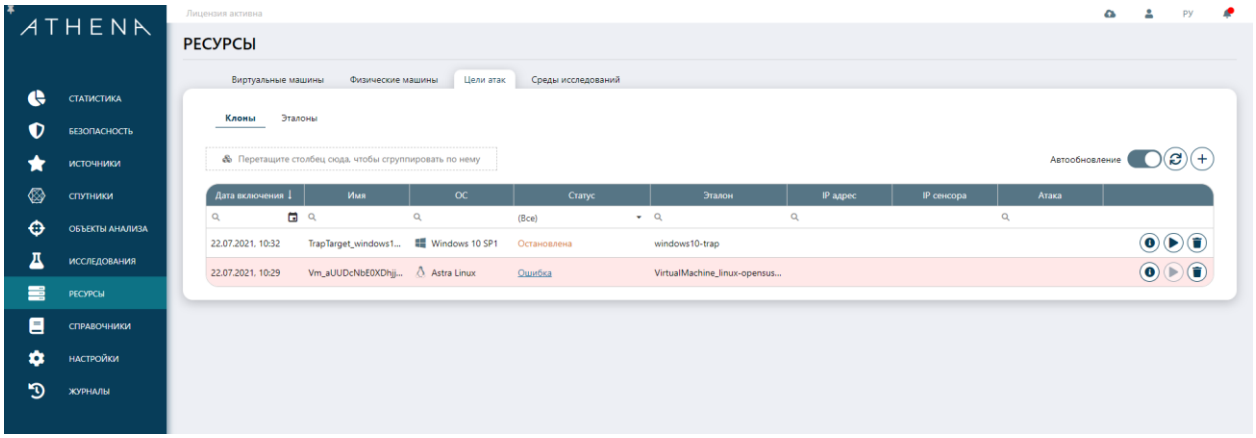


Рисунок 46. Цели атак

Во вкладке «Среды исследований» содержится информация по группам машин, используемым для одновременного анализа файлов в них (Рисунок 47).

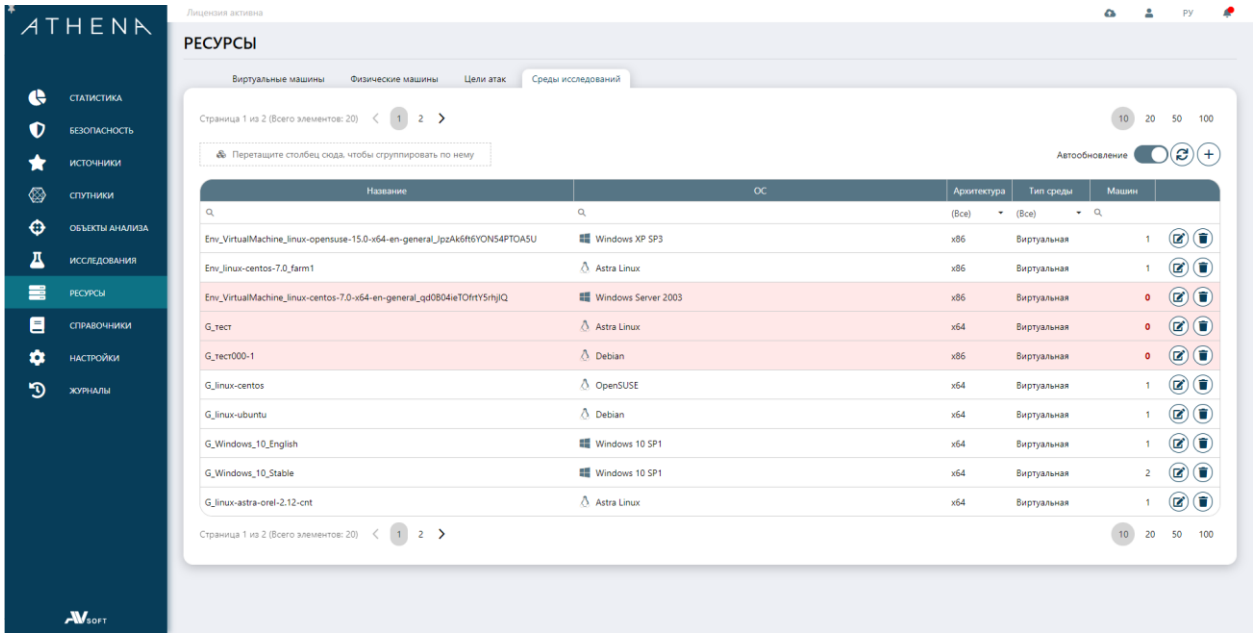


Рисунок 47. Среды исследований

Для добавления новой группы необходимо нажать кнопку «Добавить», которая откроет форму для заполнения «Среда исследований» (Рисунок 48).

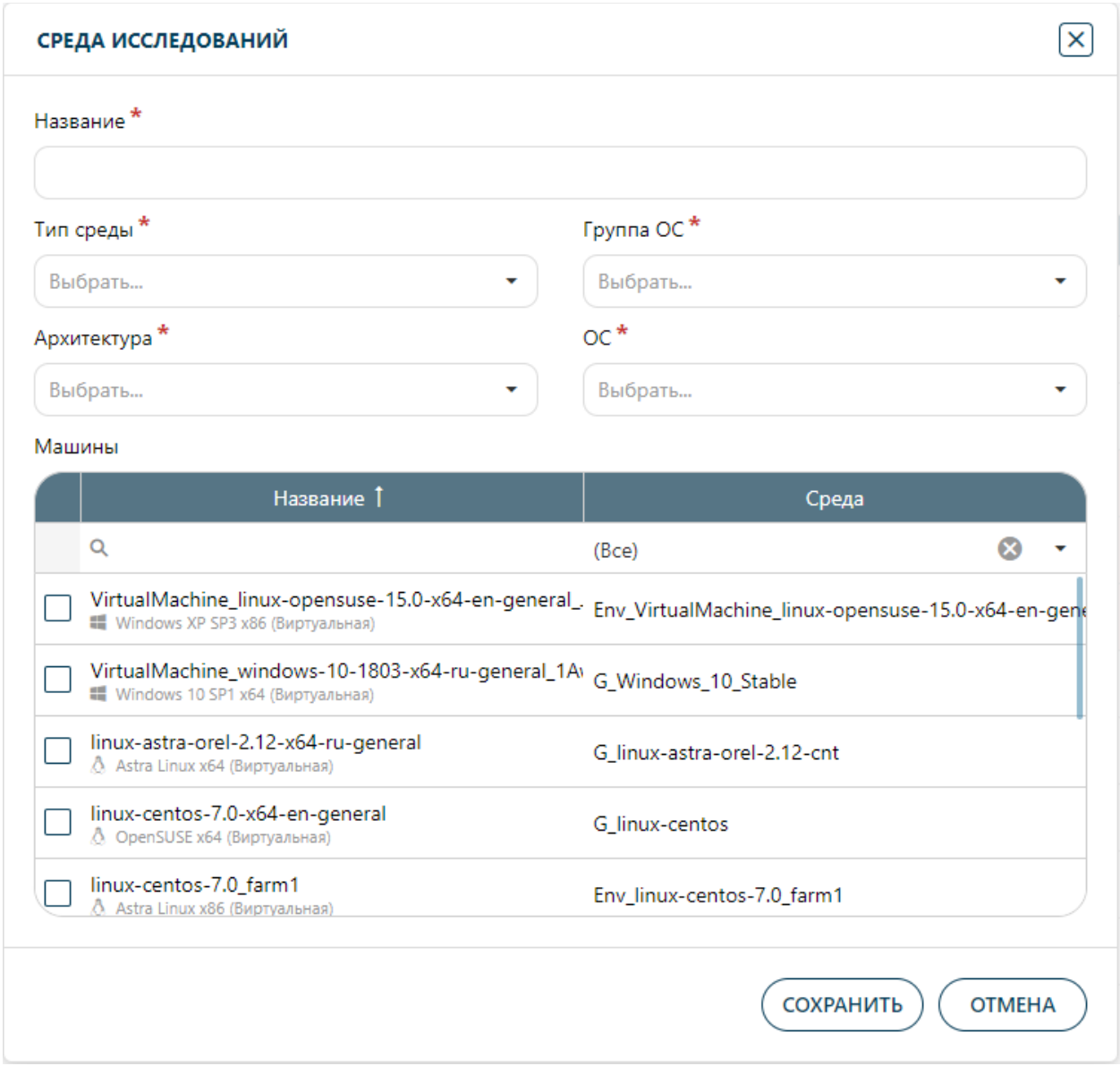


Рисунок 48. Добавление новой группы исследовательских машин

В форме необходимо указать параметры, описанные в таблице 16.

Таблица 16. Параметры создания новой среды исследования

№	Параметры	Описание
1.	Название	Название новой среды исследования.
2.	Тип среды	Тип создаваемой среды исследования. Физическая или виртуальная.
3.	Архитектура	Архитектура операционной системы группы исследовательских машин.

№	Параметры	Описание
4.	Группа ОС	Общая группа операционных систем, к которой относится операционная система новой группы.
5.	ОС	Операционная система группы исследовательских машин.
6.	Машины	Выбор машин из имеющихся в системе и подходящих под указанные параметры создаваемой среды исследования.

После завершения ввода данных необходимо нажать кнопку «Сохранить» и удостовериться, что новая среда исследования отобразилась в общей таблице «Среды исследования».

12 Уведомления

В системе реализовано несколько видов уведомлений, описание которых представлено в таблице 17.

Таблица 17. Описание видов уведомлений

№	Вид	Описание
1.		Уведомления об успешных операциях.
2.		Информационные уведомления.
3.		Предупреждения.
4.		Уведомления об ошибках.

При авторизации пользователя в системе может возникнуть ситуация некорректного указания логина или пароля, в данной ситуации пользователю отобразится оповещение, которое представлено на рисунке 51.

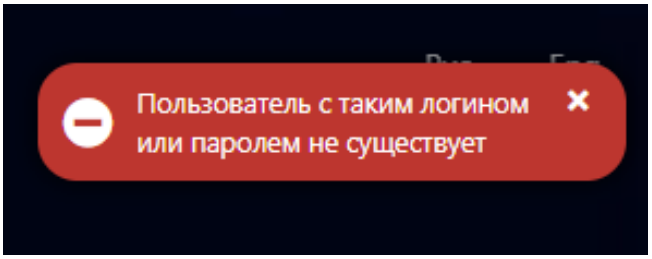


Рисунок 49. Уведомление о некорректных данных авторизации

В данной ситуации пользователю необходимо попробовать скорректировать пароль, восстановить пароль или инициировать регистрацию в системе повторно.

При успешной загрузке файлов в систему для исследования пользователю отобразится оповещение об этом, которое представлено на рисунке 52.

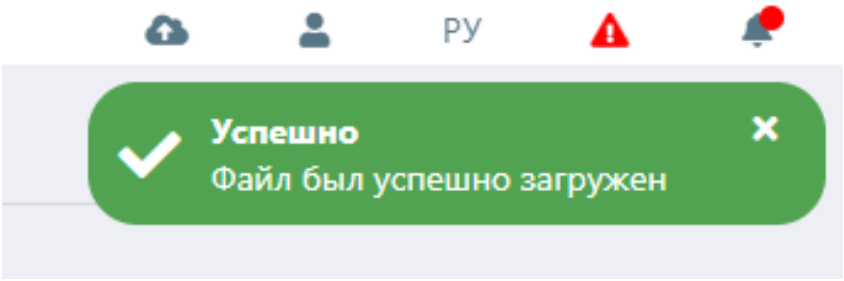


Рисунок 50. Оповещение об успешной загрузке файла в систему

Если загрузка файла в систему выполнена неуспешно, то пользователю отобразится оповещение об этом, которое представлено на рисунке 53.

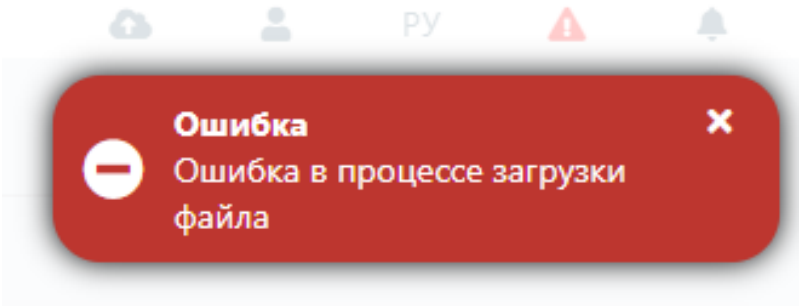


Рисунок 51. Оповещение о неуспешной загрузке файла в систему

! При отображении данного сообщения необходимо обратиться к администратору ПК ATHENA.

Когда файл или ссылку, которые уже есть в системе, повторно загружают на анализ, то пользователю отображается оповещение, представленное на рисунке 54.

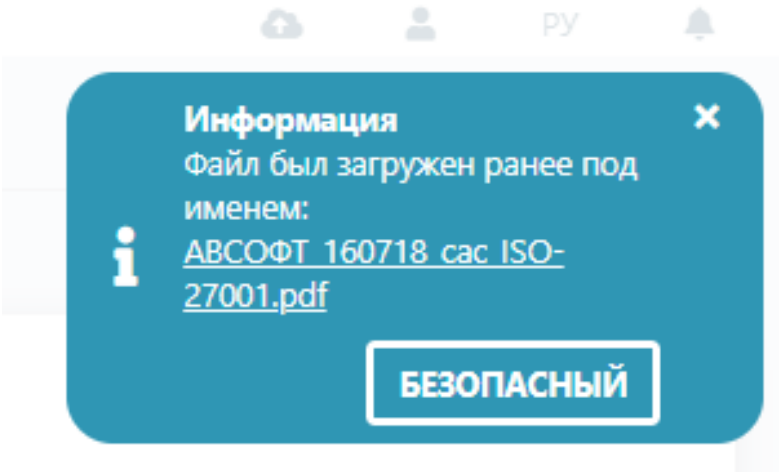


Рисунок 52. Оповещение об информации по объекту анализа в системе

В данном оповещении есть информация, что объект уже был загружен в систему ранее, ссылка на его отчет и вердикт.

Для того, чтобы обезопасить пользователя от случайного удаления объектов в системе ему отображается уточняющее оповещение уверенности в инициации его намерений (Рисунок 55).

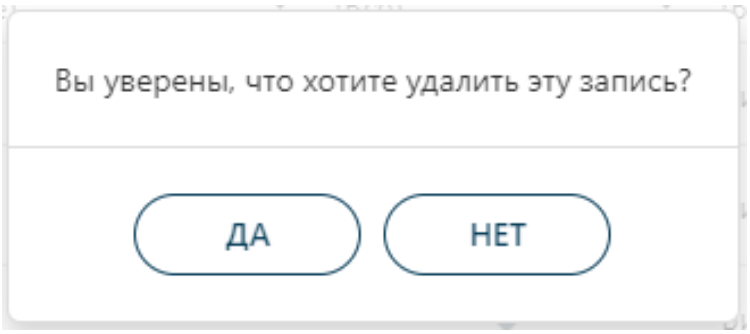


Рисунок 53. Подтверждение намерения удаления объекта

Если модули системы неисправны и не могут осуществлять свои функции, то пользователю отображается оповещение об этом, которое представлено на рисунке 56.

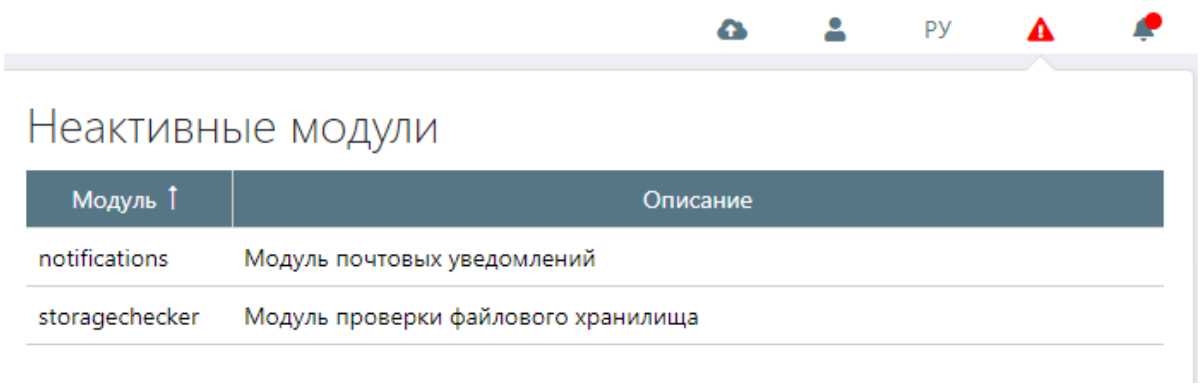
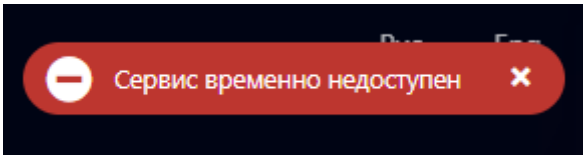


Рисунок 54. Оповещение о неактивности модулей

При отображении данного сообщения необходимо обратиться к администратору ПК ATHENA.



При успешном сохранении настроек пользователем система отобразит оповещение, которое представлено на рисунке 57.

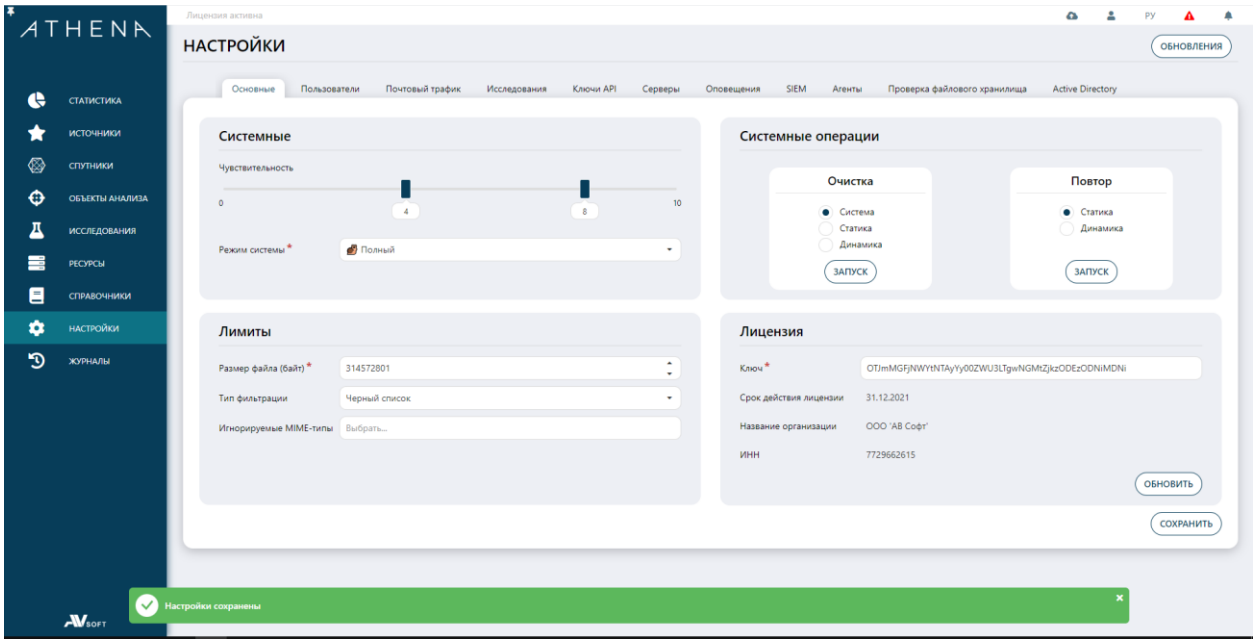


Рисунок 55. Оповещение об успешном сохранении настроек