Руководство пользователя

Table of contents:

Введение

Система tLab представляет собой корпоративный локальный сервис для удаленного и безопасного анализа подозрительных объектов. Данная система направлена на защиту от киберугроз нового типа, против которых типичный антивирус малоэффективен: от целевых атак, вредоносных программ нулевого дня и атак на пользователя.

tLab производит автономный анализ поведения программ и идентификацию вредоносных функциональностей на сервере (корпоративное облако). Система позволяет автоматизировать процедуру анализа поведения любых программ и выявлять в них признаки вредоносных функций.

Подозрительные объекты запускаются в виртуальных контейнерах, где производится непрерывный анализ поведения всех запущенных программ.

Используется уникальная технология глубокого анализа функциональности программ для надежного обнаружения вредоносных объектов, в том числе и нулевого дня.

Данная технология имеет инновационный аспект, который заключается в механизме распознавания заданных вредоносных функциональностей. Здесь отслеживается история поведения и связываются события различных процессов в реальном времени.

Руководство пользователя Авторизация

Для пользования системой необходимо авторизоваться с помощью логина и пароля, предоставленных администратором. Авторизация производится на странице входа в систему. Для входа в систему необходимо ввести имя пользователя и пароль в соответствующие поля. Создание пользователя описывается ниже, в пункте Администрация пользователей.

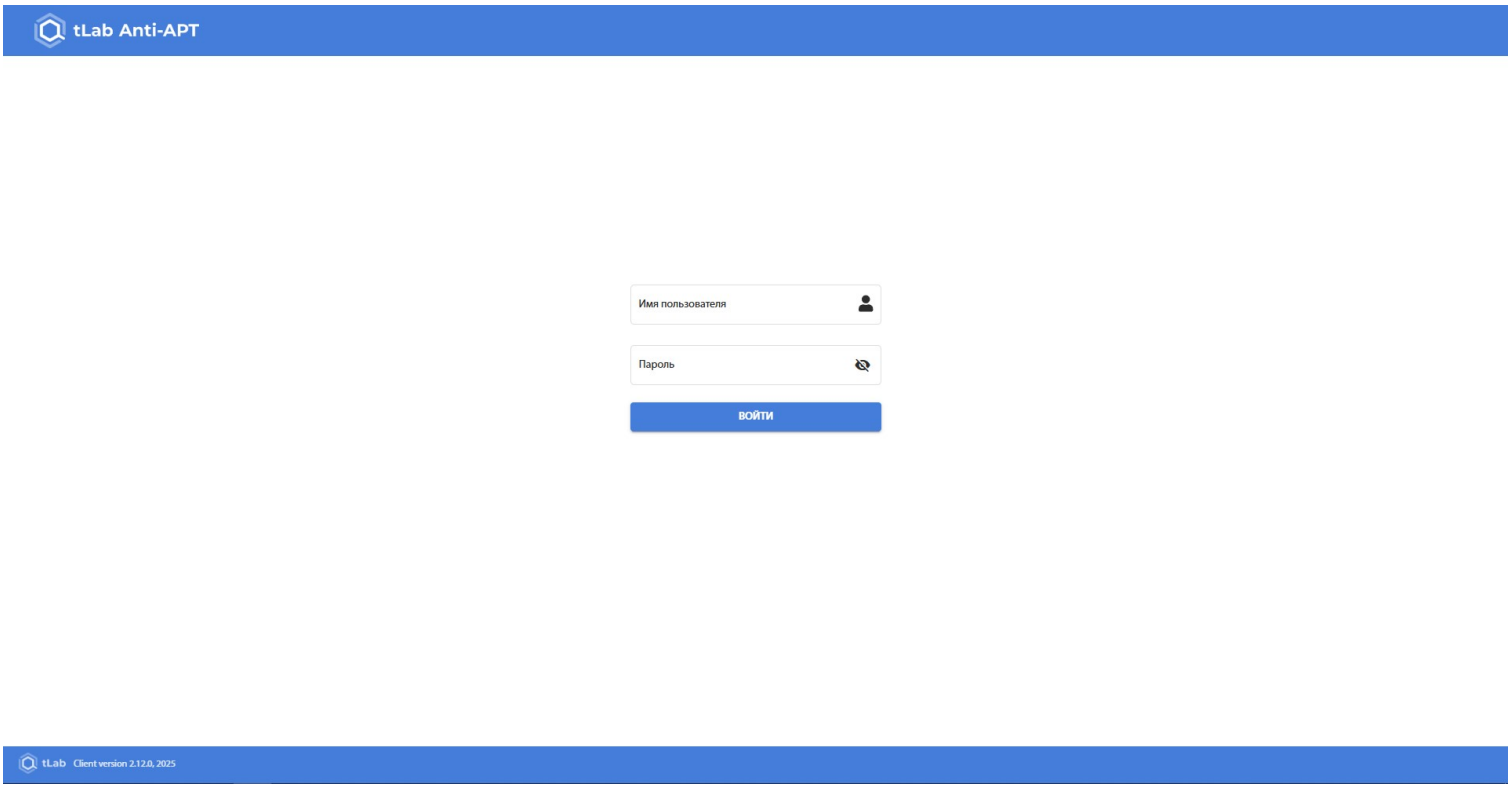
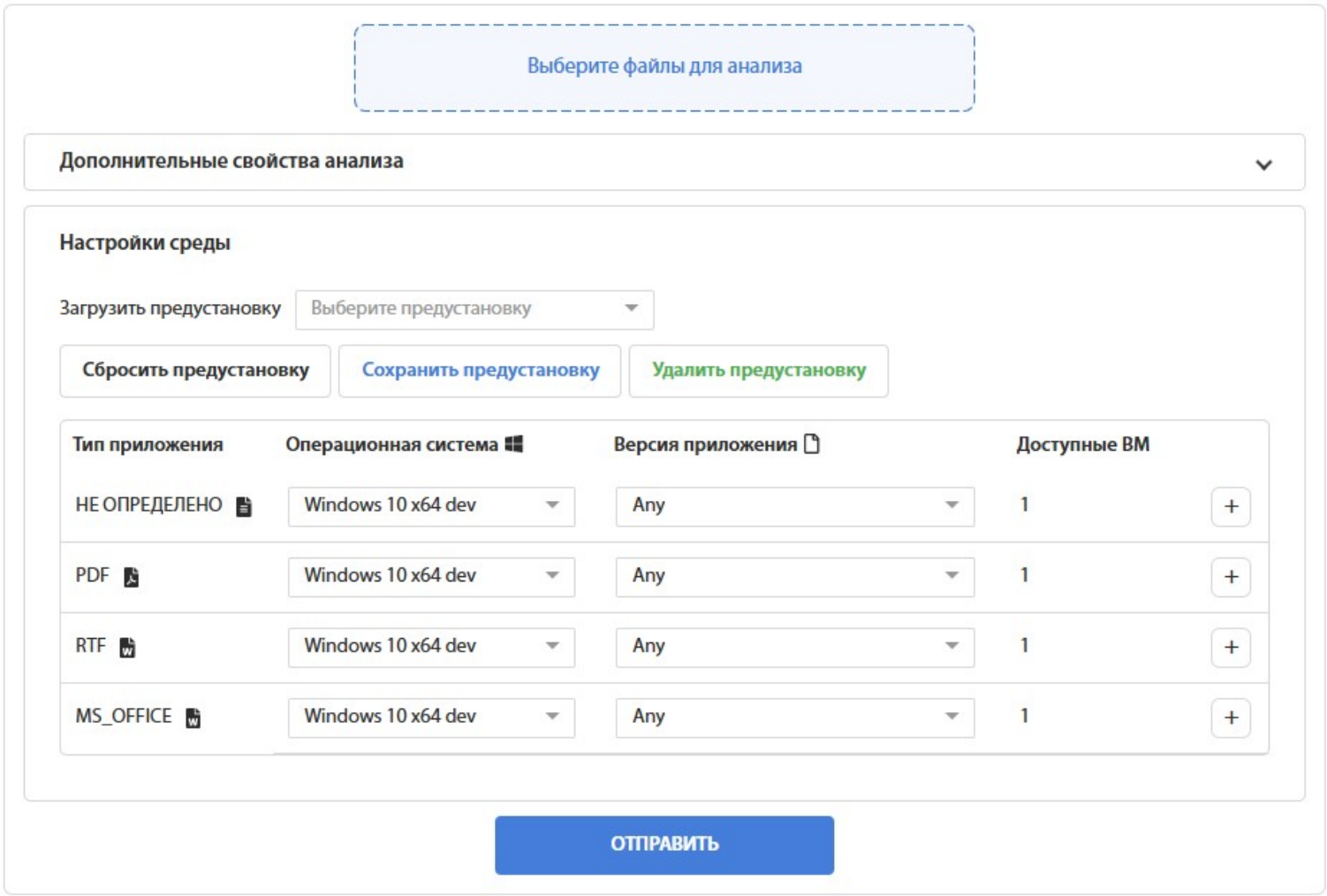


Рис. 1 – Страница авторизации

Загрузка файлов

Загрузка файлов на проверку осуществляется на вкладке Загрузка файлов страницы Загрузка, которая доступна через верхнее навигационное меню. При нажатии на кнопку Выбрать файлы для проверки появится диалоговое окно для выбора файлов любого типа. В диалоговом окне возможен выбор группы файлов через выделение мышью или с помощью комбинации *Ctrl* + *Левая кнопка мыши*. В данной версии tLab не поддерживается загрузка папок, только индивидуальных файлов.



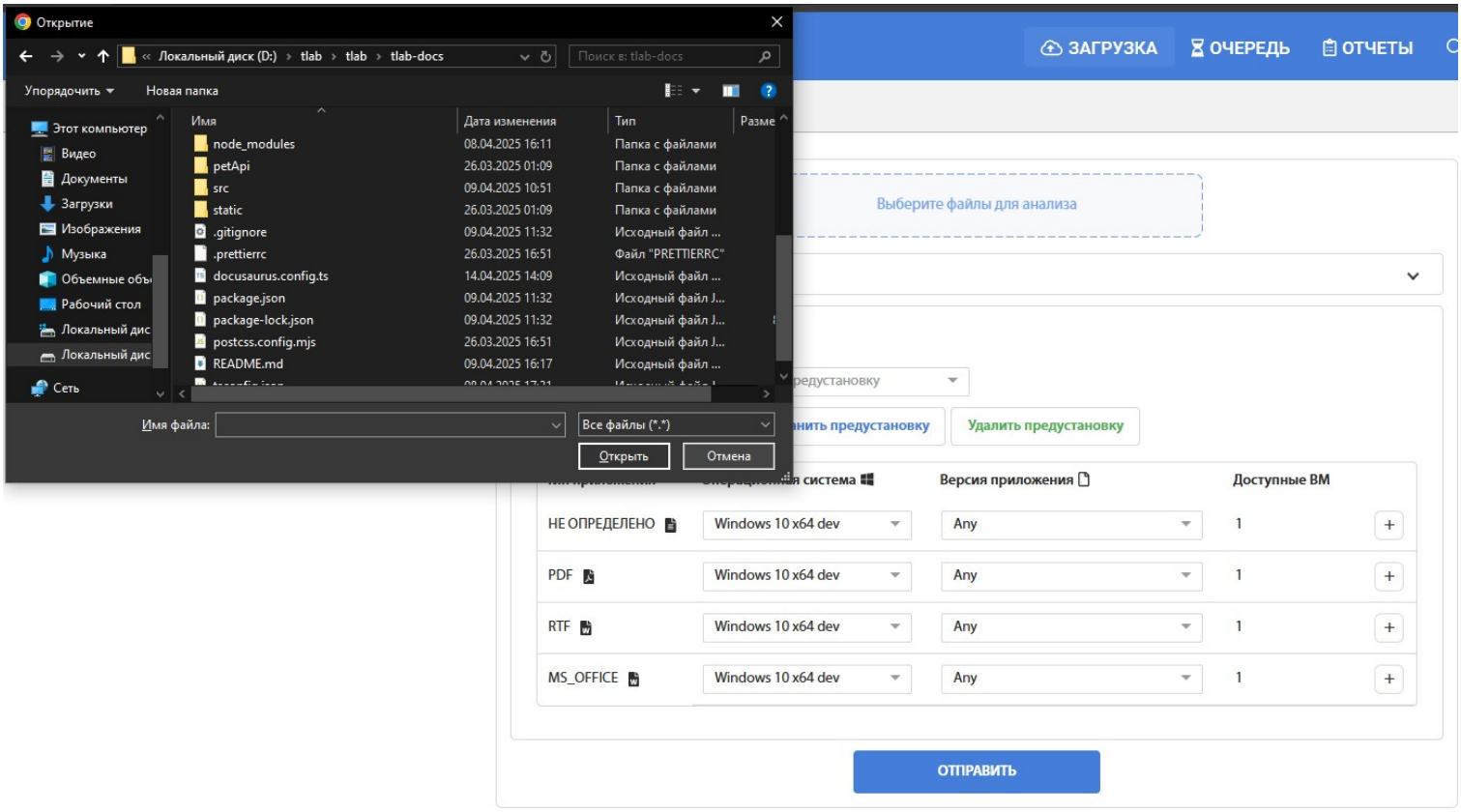


Рис. 2 — Диалог выбора файлов для загрузки

После выбора файлов кнопка Открыть закроет диалоговое окно выбора файлов. При повторных нажатиях Выбрать файлы для проверки можно выбрать файлы находящиеся в разных директориях. Общее количество и общий размер файлов по умолчанию составляют 10 файлов и 100 Мегабайт.

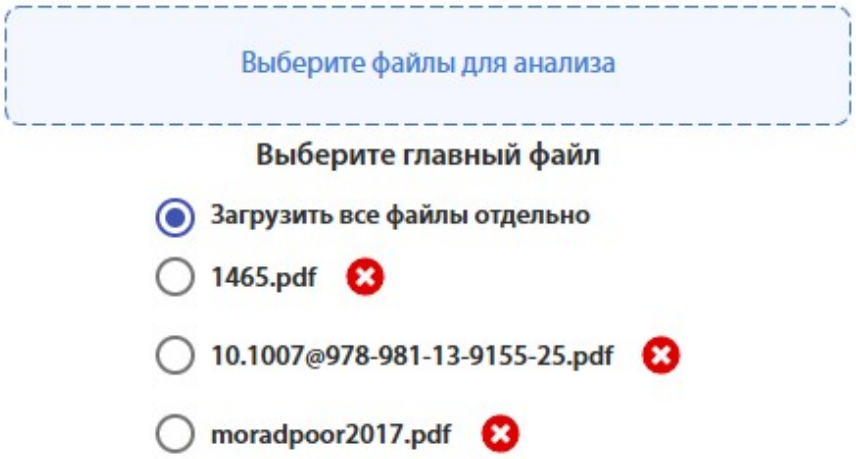


Рис. 3 – Форма загрузки после выбора группы файлов

Отменить выбор файлов (или группы файлов) можно через нажатие красного X рядом с файлом (группой).

При загрузке группы файлов возможно проведение динамического анализа всей группы. Данное свойство необходимо для проверки файлов с зависимостями. Для этого необходимо выбрать главный

файл, который будет запущен во время анализа. Тогда остальные файлы будут использоваться в качестве зависимостей и располагаться в одной директории.

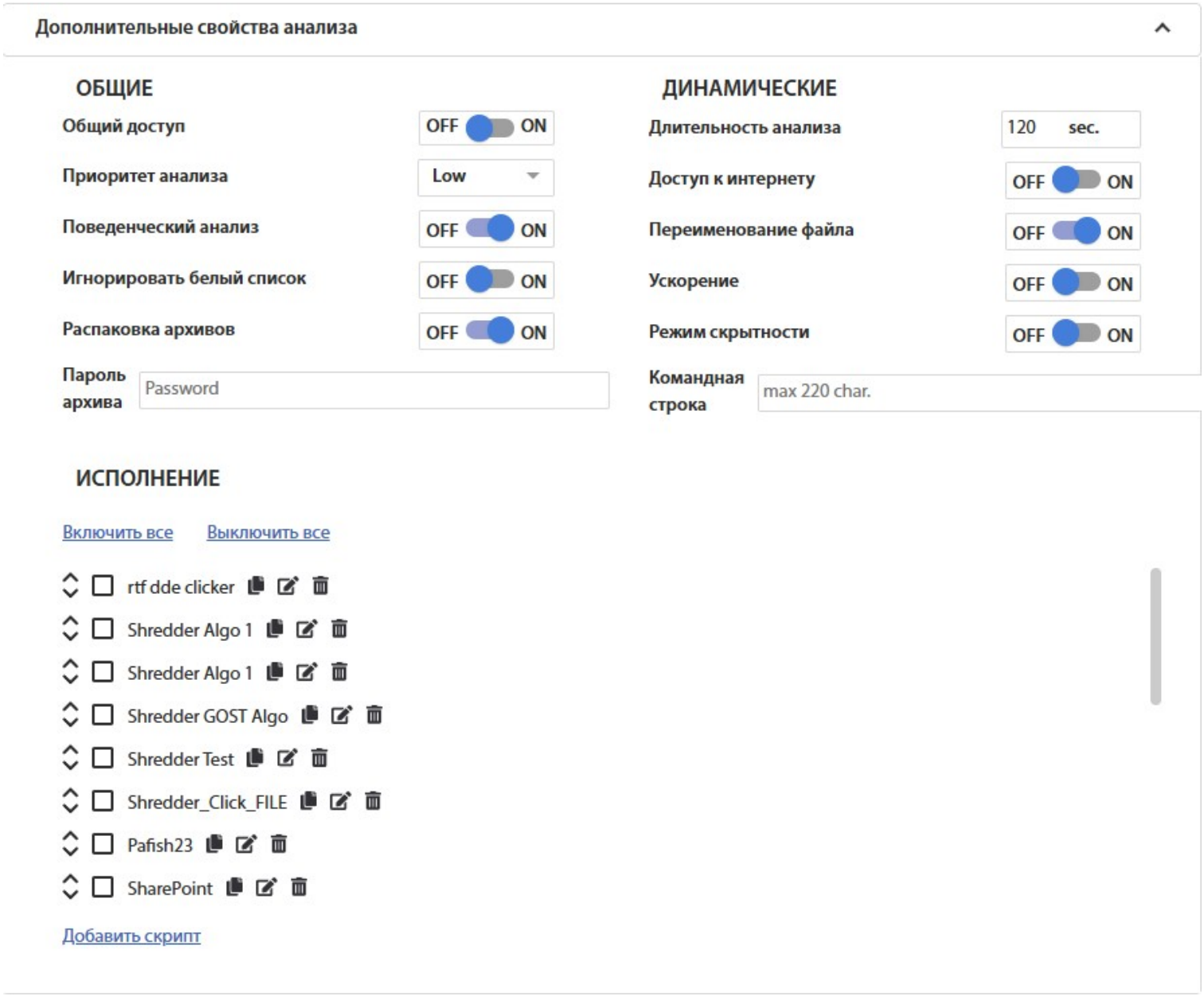


Рис. 4 – Форма загрузки файлов с дополнительными настройками

Дополнительные свойства анализа позволяет изменить дополнительные настройки анализа. Список возможных свойств:

Доступ – При включении данной опции отчеты выбранных файлов станут доступными для просмотра всем пользователям системы. В ином случае доступ к сформированным отчетам имеет пользователь, загружающий объекты, и администратор.

Приоритет анализа – Позволяет провести более срочные анализы вне очереди.

Тип анализа – Включает или отключает проведение статического и динамического анализов. По умолчанию производятся все виды анализа.

Игнорировать белый список – По умолчанию доверенные файлы не анализируются и появляется сообщение об их доверенном статусе. При включении данной опции производится анализ всех файлов, даже находящихся в белом списке доверенных.

Распаковка архивов – При активации данной опции производится распаковка загружаемых архивов и производится отдельный анализ для каждого объекта, находящегося в архиве. Активации данной опции никак не влияет на обработку других типов файлов при загрузке.

Пароль архива – Данное поле используется для ввода пароля от архива, в случае его наличия

Длительность анализа – Используется для установки длительности динамического анализа. 2 минуты по умолчанию, максимум 60 минут.

Доступ к интернету – Открывает доступ в сеть интернет из контейнера при динамическом анализе. Требуется осторожность при загрузке вирусов распространяющихся через сеть, таких как WannaCry и Petya. По умолчанию доступ к сети отключен.

Переименование файла – При активации данной опции оригинальное имя загружаемого объекта будет изменено во время динамического анализа. Это имя затем используется в цепочке событий.

Ускорение – При включении данной опции производится нивелирование основных видов задержек, включая трудноустранимые циклы микрозадержек.

Командная строка – Позволяет указать параметры командной строки для запуска анализируемого файла при динамическом анализе.

Версии – Данная опция дает возможность выбора окружения для динамического анализа для документов Microsoft Office и Adobe Reader. При выборе более одной версии будет создано несколько анализов и формируется несколько отчетов. Для одного анализа следует выбирать окружение из одной группы (например, только из группы Microsoft Office или Adobe Reader).

Сценарии симуляции пользовательской активности – На данной панели происходит выбор сценариев, используемых при динамическом анализе объекта с графическим интерфейсом. У каждого сценария есть имя, условия активации (совпадение по названию окна и/или имени процесса), выполняемые команды, минимальное и максимальное количество повторов команды, задержка перед выполнением действий и задержка между действиями. Сценарии выполняются в порядке сверху вниз, таким

образом можно создать и выполнить несколько сценариев по порядку для определенных программ, например, сценарий №1 нажимает кнопку TAB 3 раза, а сценарий №2 нажимает кнопку ENTER

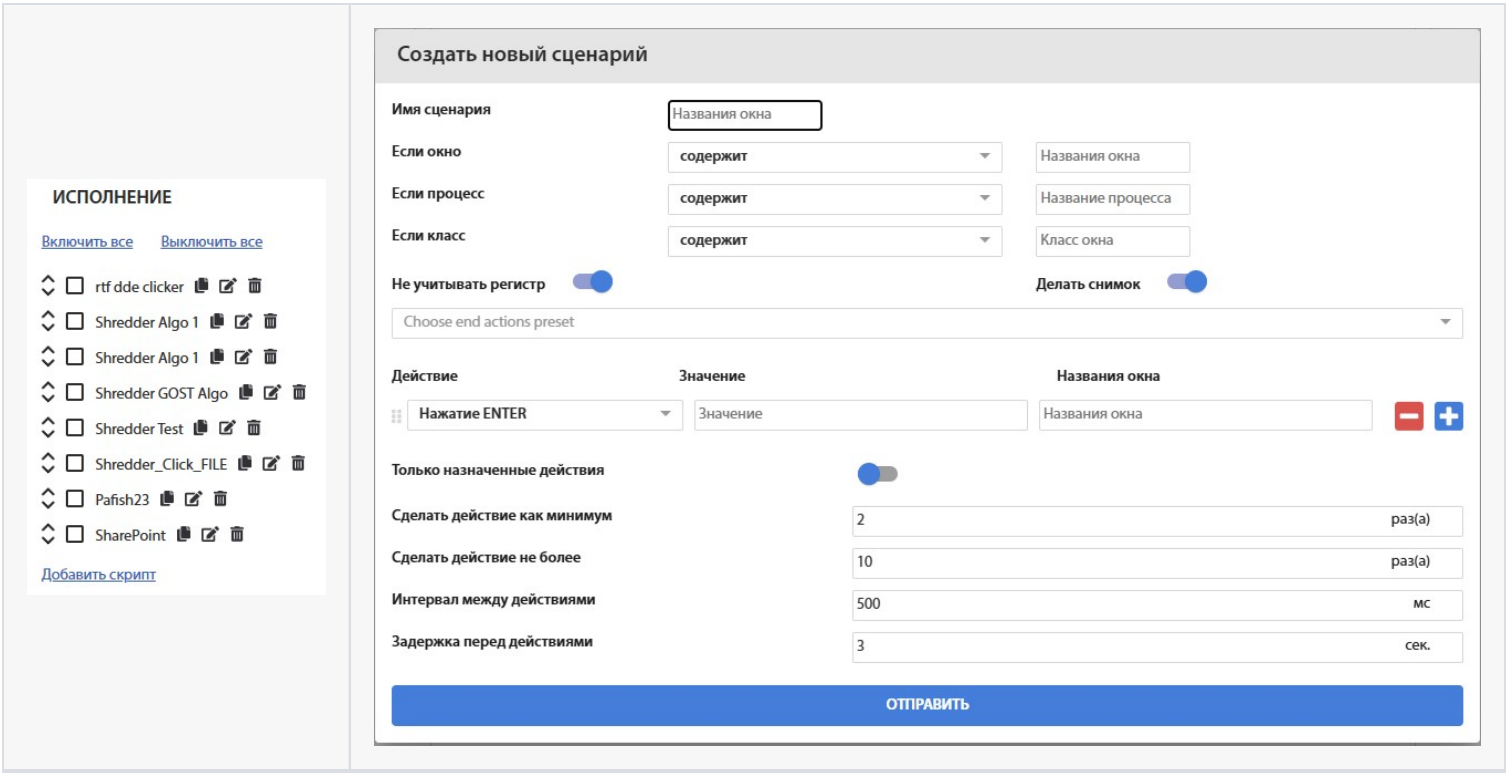


Рис. 5 – Сценарии симуляции пользовательской активности

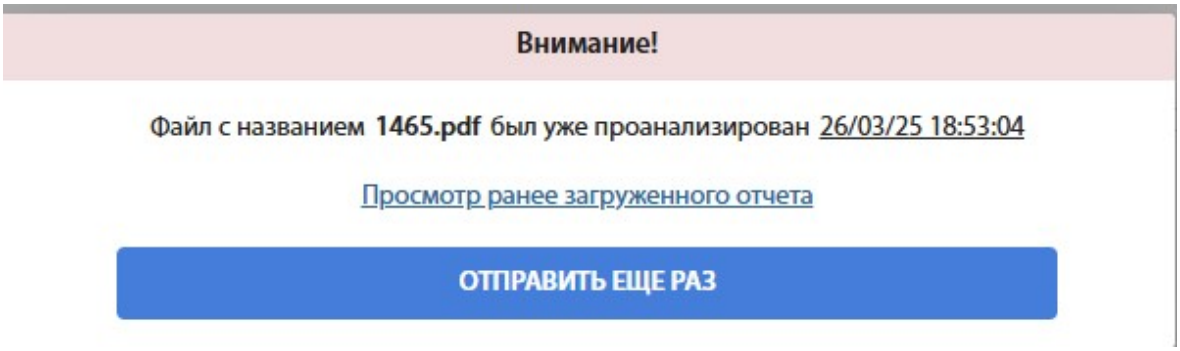


Рис. 6 – Сообщение о повторной загрузке

При повторной загрузке существующего в системе tLab файла появится сообщение с административным заключением, ссылкой-датой на последний отчет и кнопкой Отправить заново, для повторного анализа файла

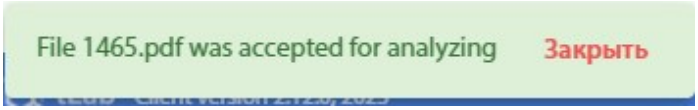


Рис. 7 — Сообщение об успешной загрузке файла

Очередь анализов

Загружаемые файлы на анализ помещаются в очередь проверки. При нажатии на кнопку **Очередь** в верхней навигационной панели веб-клиента открывается страница со списком объектов в очереди. Если в очереди присутствуют файлы, на кнопке Очередь справа отображается число с количеством элементов в очереди. Анализы с более высоким приоритетом имеют расположены в очереди выше анализов с меньшим приоритетом, и соответственно отчеты формируются раньше. Страница очереди обновляется автоматически. Завершившиеся анализы удаляются из очереди.

На вкладке **Неудачные анализы** отображается список анализов завершившихся ошибкой. Для каждого файла представлен тип ошибки и список всех неудавшихся попыток с данным файлом. После первого успешного анализа ранее неудачного файла его запись будет удалена из **Неудачных анализов**.

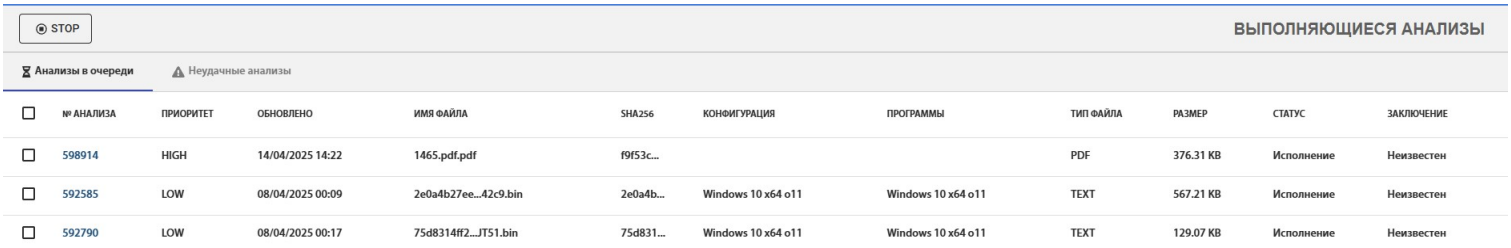


Рис. 8 – Очередь анализов

Отчеты

Таблица с готовыми отчетами можно отображается при нажатии на кнопку **Отчеты** в верхнем навигационном меню. Число справа на кнопке **Отчеты** информирует о количестве непрочитанных отчетов.

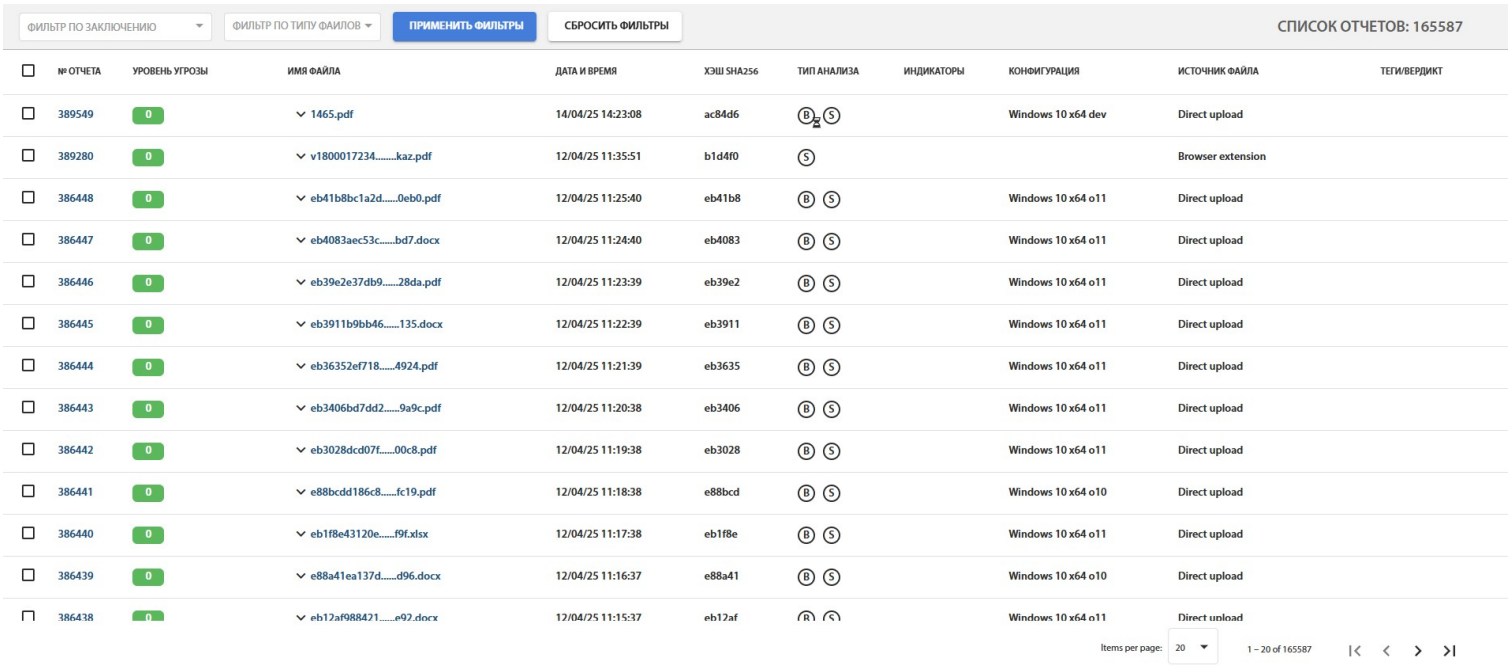


Рис. 9 – Список сформированных отчетов

Таблица содержит следующие столбцы:

- Флажок для выделения нескольких отчетов для проведения операции над группой объектов;
- Статус о прочтении отчета;
- Тип анализа (ряд иконок) – динамический, статический;
    - Ⓓ - Динамический анализ выполняется
    - Ⓓ - Динамический анализ готов
    - Ⓢ - Статический анализ готов
- Дата и время генерации отчета;
- Имя файла – ссылка на сам отчет и имя, под которым был загружен файл;

- Значение хэш-функции SHA256 для файла, который можно использовать для быстрого поиска идентичных файлов;
- Индикаторы активности файла (ряд иконок), такие как интернет активность, внедрение в процессы, создание сервисов, запуск на автозагрузку (Список возможных индикаторов приведен в Приложении 1).;
- Количество снимков экрана, снятых при динамическом анализе;
- Уровень угрозы, подсчитанный системой tLab в зависимости от объема и вредоносности активностей найденных при динамической анализе. Чем выше значение, тем опаснее файл;
- Индикатор опасности указывает опасность файла на цветовой шкале: зеленый – безопасный, оранжевый – требует внимания, красный – высокая вероятность вредоносности;
- Заключение эксперта или администратора. Заключение выставляется внутри отчета.

При нажатии на кнопку Фильтры отображается дополнительное меню, в котором можно отсортировать список отчетов по различным свойствам или выбрать количество результатов размещаемых на одной странице. Кнопка Выделить все выделяет все отчеты на странице, над которыми затем можно произвести действия: Пометить как прочитанные/непрочитанные или Удалить. Удаленные файлы перемещаются в корзину, доступ к которой имеет только администратор. Случайно удаленные файлы можно восстановить из корзины.

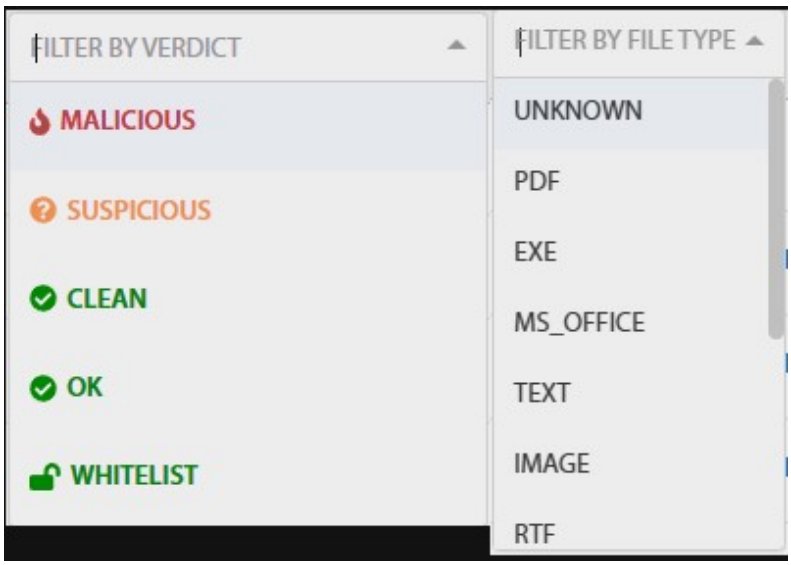


Рис. 10 – Меню фильтров

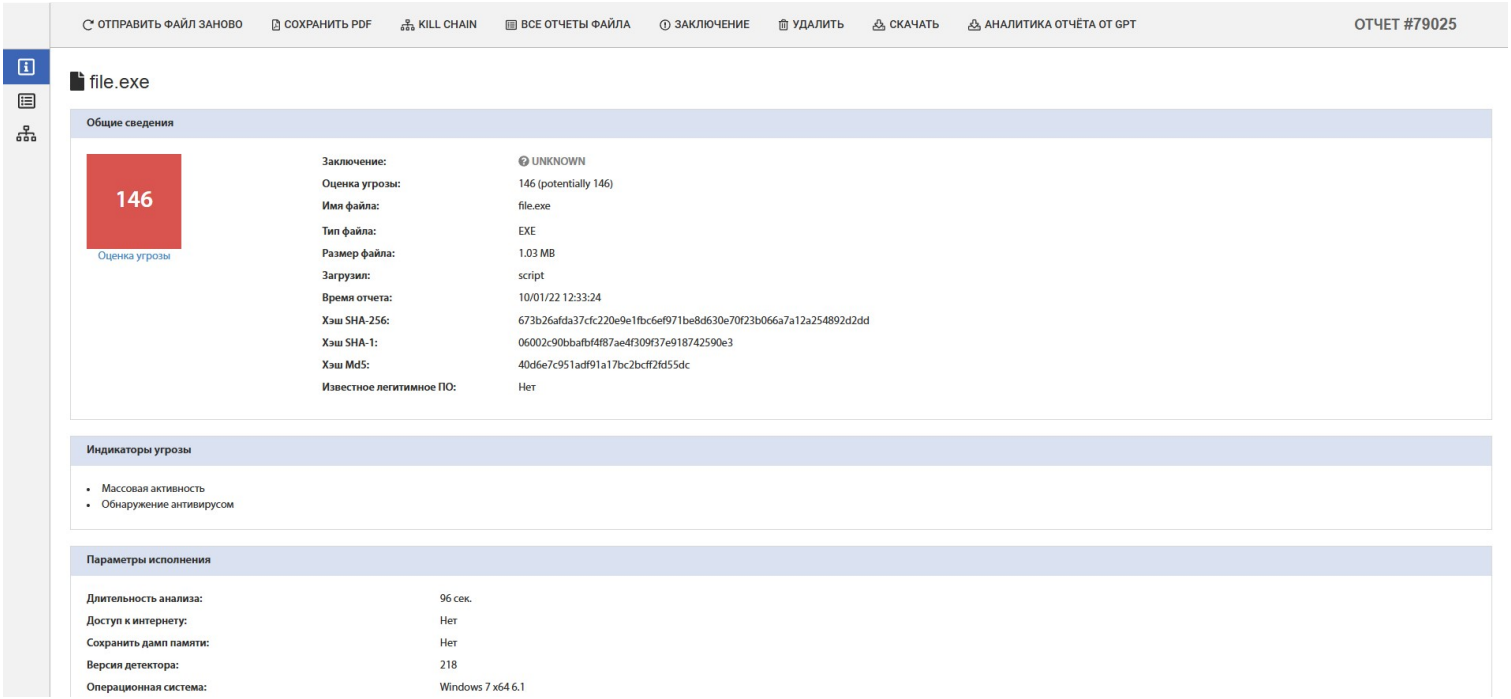


Рис. 11 – Общий отчет

Страница отчета состоит из трех вертикальных вкладок. Вкладка Общий отчет содержит общую информацию о файле, заключение эксперта и параметры анализа. Вкладка Статический отчет содержит данные собранные статическим анализатором. Вкладка Динамический отчет содержит результаты динамического анализа. При нажатии на кнопку Операции с файлом отображается соответствующее меню, которое содержит следующие пункты:

- Отправить заново (открывает форму повторной отправки файла на анализ);
- История (список всех отчетов с этим файлом, даты-ссылки на отчеты);

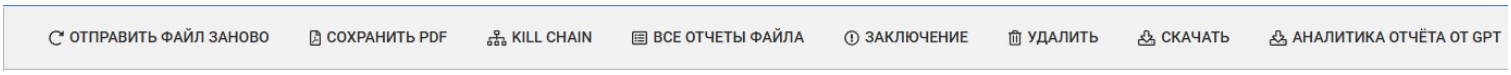


Рис. 12 – Меню операций с файлом

При нажатии на кнопку **Поиск** в навигационном меню открывается страница поиска отчетов в системе. Поиск ведется по многочисленным полям, которые можно увидеть в общем отчете и начало которого показано в соответствующих колонках списков отчетов и очереди. При вводе 4-6 символов в поле поиска SHA256 в поле ввода отображается всплывающий список с присутствующими отчетами, в которых совпадают введенные символы. Для перехода к найденному отчету необходимо ввести полное значение хэшфункции (или выбрать в списке) и нажать кнопку **Поиск**.

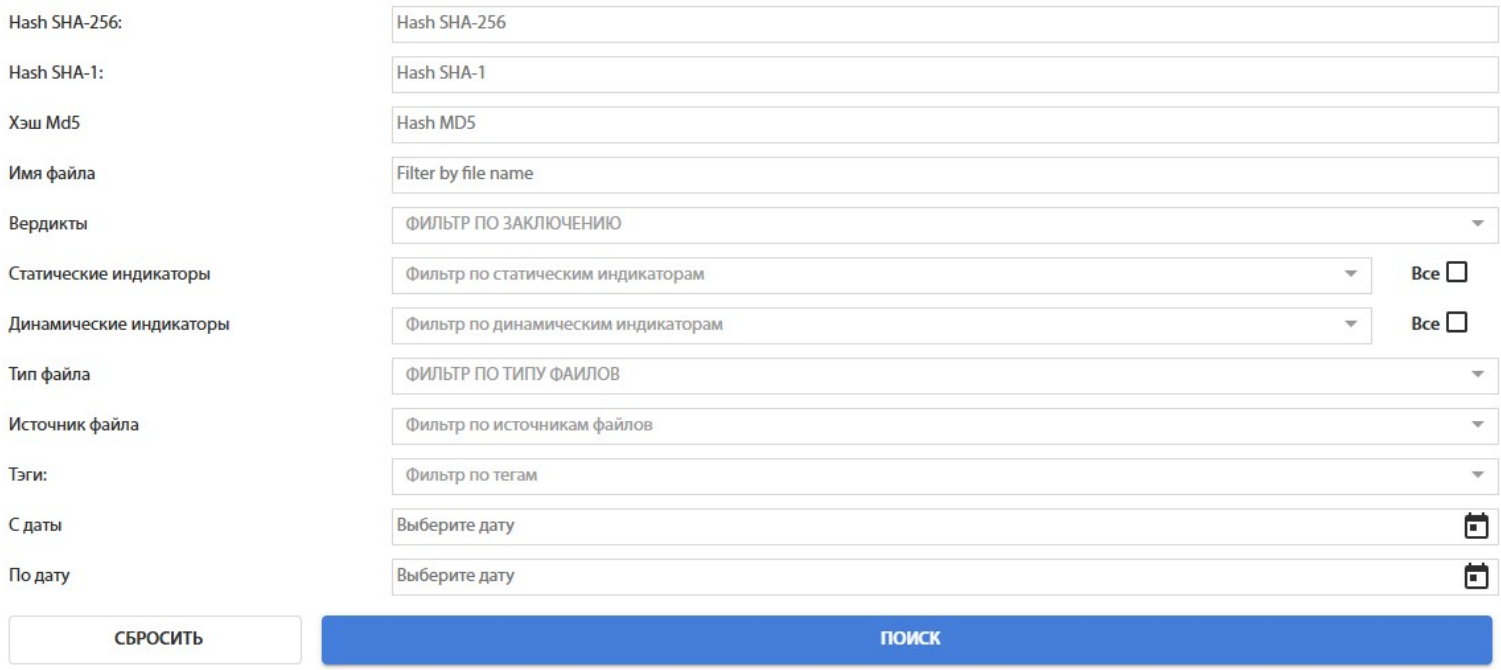


Рис. 13 – Страница поиска отчетов

Отчет статического анализа

На странице статического анализа отображаются результаты анализа статической информации файла, т.е. анализ содержимого файла без его запуска.

В системе tLab уровень угрозы статического анализа вычисляется на основе статических индикаторов угроз, таких как импортирование подозрительных API- функций, наличие скриптов и макросов в документах, аномальная структура секций, шифрованные данные, возможность оперирования на низком уровне, наличие встроенных файлов и т.д.

Отчет статического анализа для разных типов файлов содержит специфическую информацию.

Для исполняемых файлов PE:

- Раскрывающийся список импортируемых модулей и функций;
- Список экспортируемых функций;
- Список извлеченных строк и поиск по частичному совпадению;
- Значок программы;
- Информация о секциях исполняемого файла.
  Для файлов MS Office и PDF: метаданные документа, такие как автор, количество страниц, название, год и т.п.
  Для анализа скриптов:
  - Возможная активность;
  - Обнаруженная активность;

  Для анализа Android приложений:
  - Информация о приложении;
  - Анализ андроида;

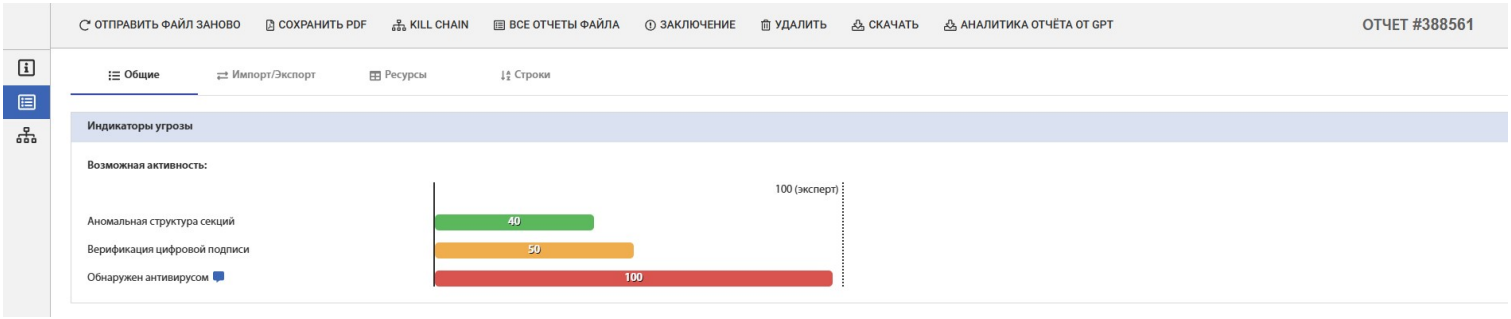


Рис. 14 – Отчет по статическому анализу

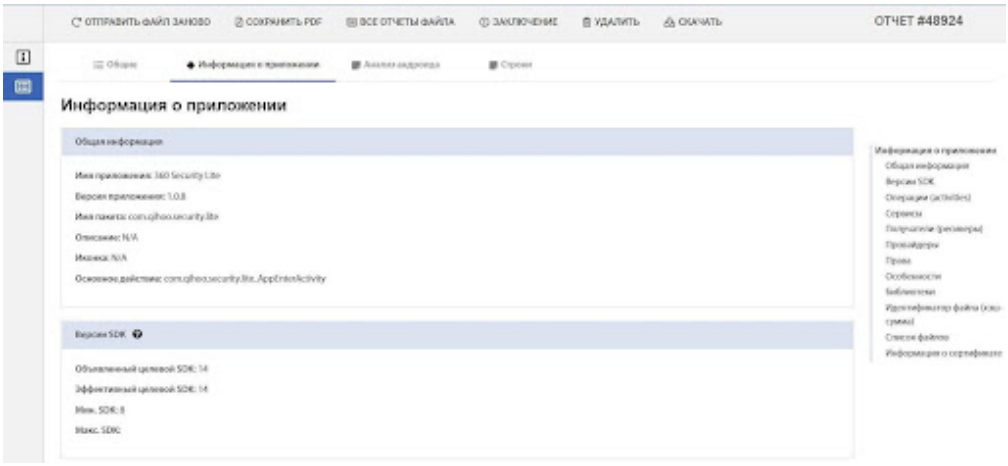


Рис. 14.1 – Отчет по анализу андроид приложения

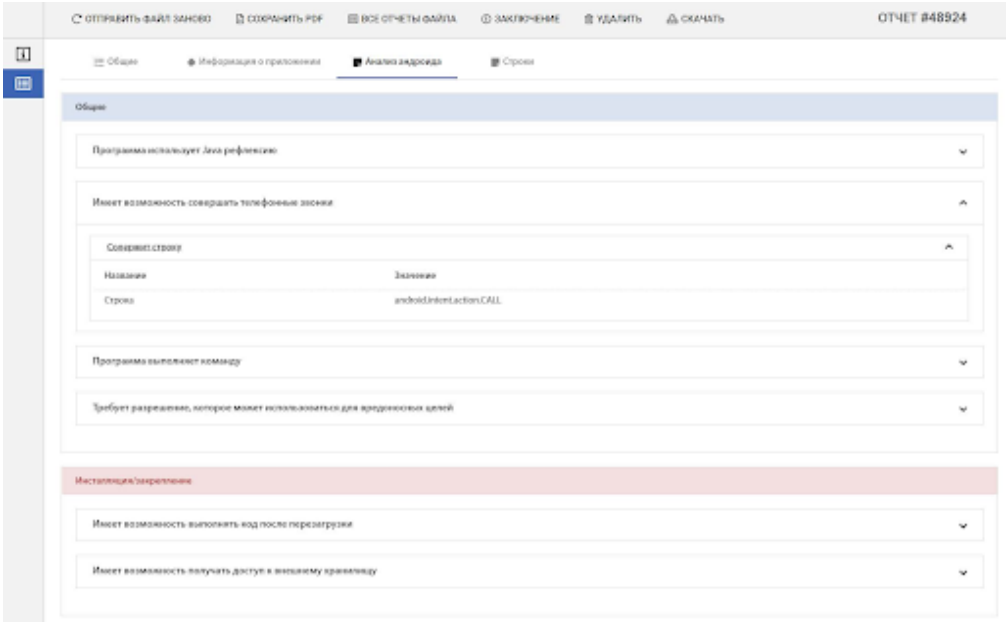


Рис 14.2 – Отчет по анализу андроид приложения

DeepSlicer

DeepSlicer - статический анализатор. Читает текст скрипта, определяет язык, на котором он написан и выдает информацию о его подозрительном функционале без непосредственного запуска. Например, запись в реестр или скачивание файлов.

На рисунке 14.3.1 изображена возможная активность - функции, которые присутствуют в коде, но возможно не запускаются.

На рисунке 14.3.2 изображена обнаруженная активность - функции, которые вызываются в коде.

ВНИМАНИЕ

Стоить обратить внимание на потенциально вредоносную активность

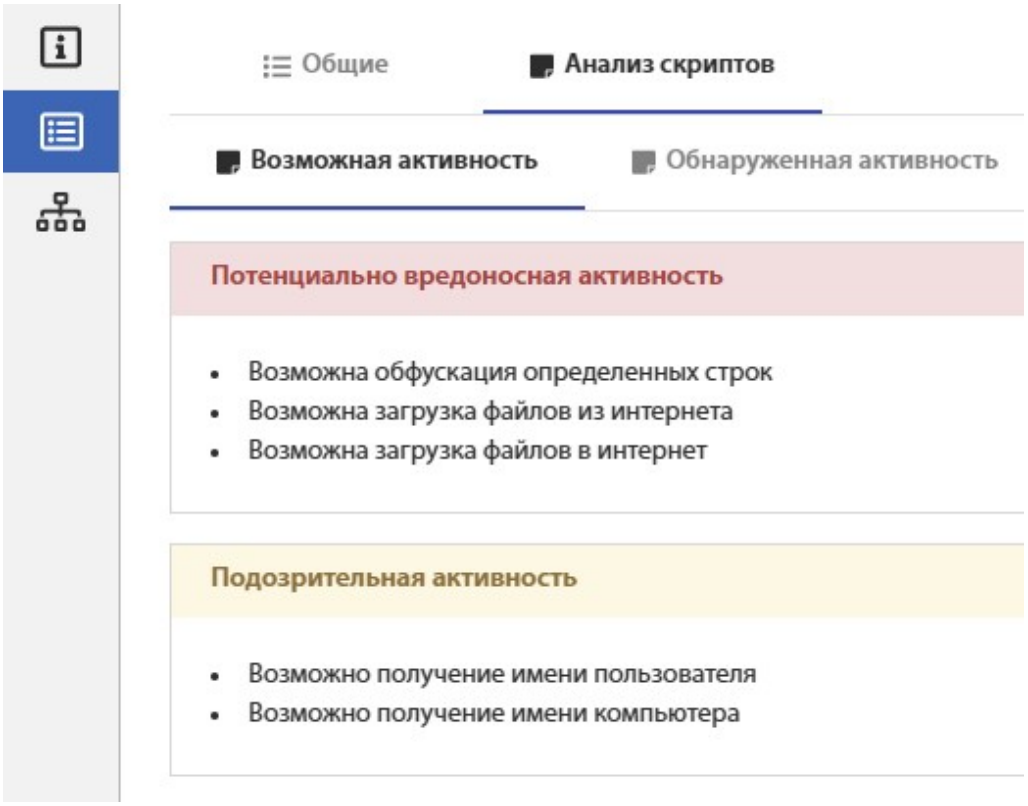


Рис. 14.3.1 - страница Deepslicer: возможная активность

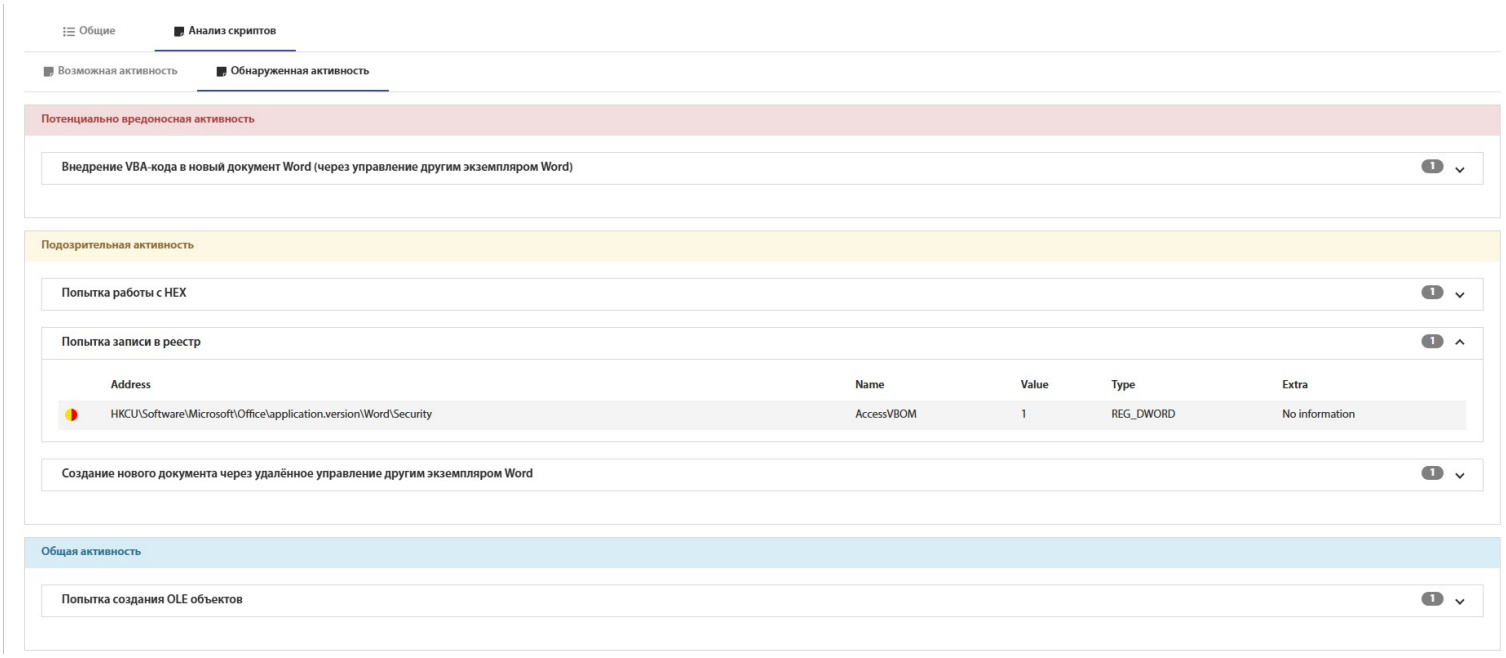


Рис. 14.3.2 - страница DeepSlicer: обнаруженная активность

Рис. 14.3.3 - страница DeepSlicer: легитимная активность

Структурная валидация Binary Eye

Позволяет описывать структуры файлов в удобном и быстром формате. С помощью программ, написанных на этом языке, можно компилировать инструкции для валидации файлов и объектов. Такой подход позволяет в короткие сроки вводить статический анализ для различных форматов файлов и уязвимостей.

Модуль анализирует файлы на соответствие определенной спецификации, автоматически разбирая и анализируя структуру документа с выделением отдельных подобъектов и полей.

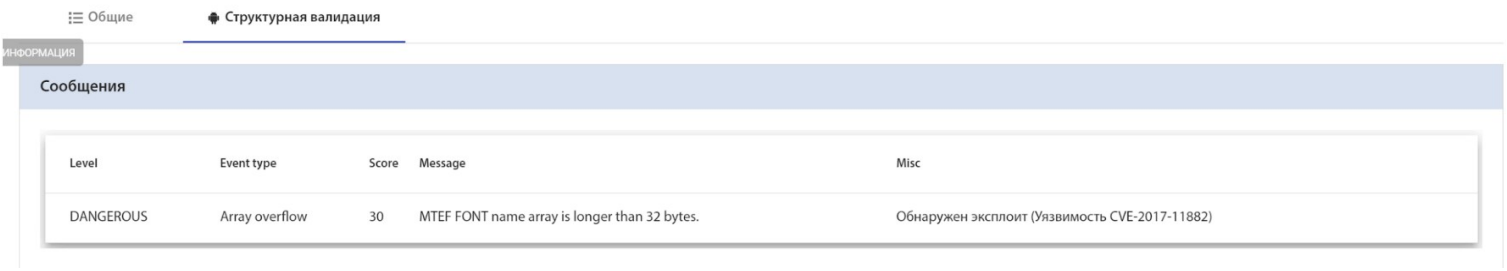


Рис 14.3.4 - страница структурной валидации

Отчет динамического анализа

На странице динамического анализа отображаются результаты динамического анализа, проведенного на виртуальной машине среды исполнения.

Краткий отчет - показывает индикаторы потенциальных угроз и раскрывающийся список найденных активностей.

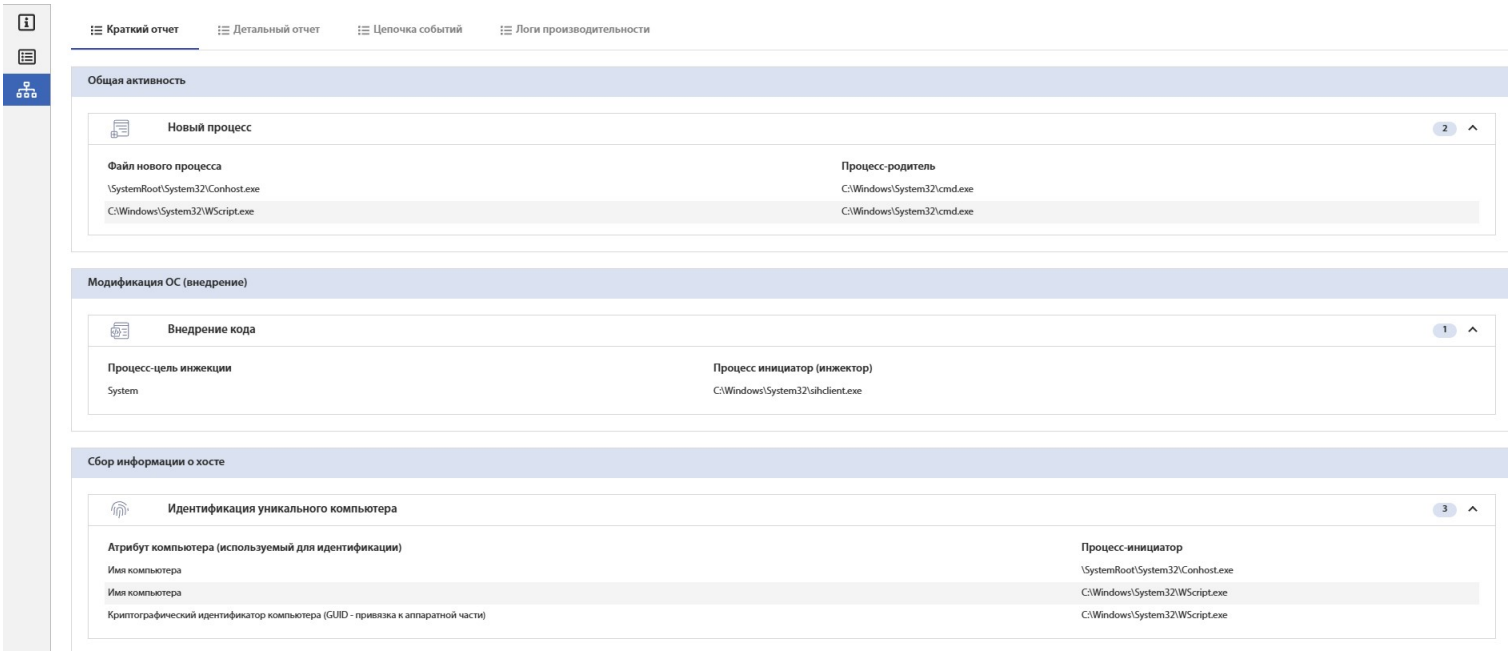


Рис. 15 – Отчет по динамическому анализу

Детальный отчет

Детальный отчет – интерактивный список активностей с возможностью фильтрации по типу событий. Список всех активностей с параметрами приведен в Приложении 2. При нажатии *Правой кнопки мыши* на параметр активности отображается контекстное меню с дополнительными для данного параметра фильтрами. Каждая активность имеет уровень опасности. Список возможных уровней опасности представлен в Приложении 3.

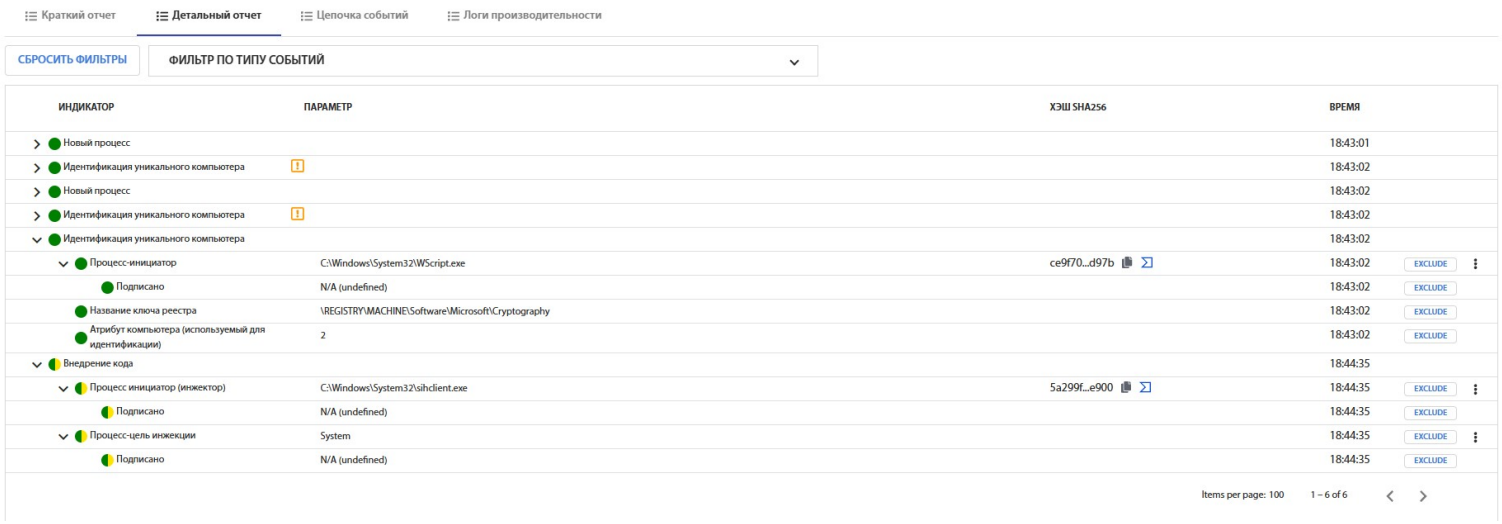


Рис. 16 – Список зафиксированных активностей

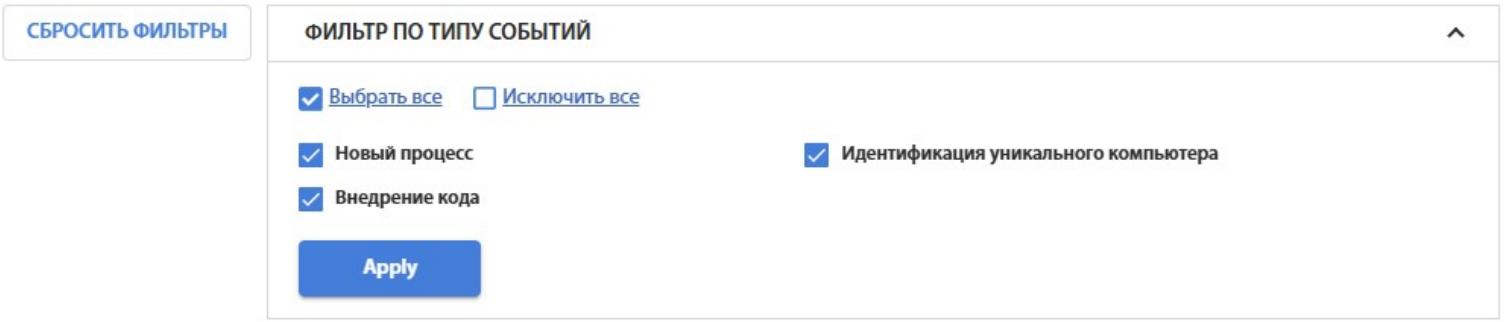


Рис. 17 – Фильтры списка зафиксированных активностей

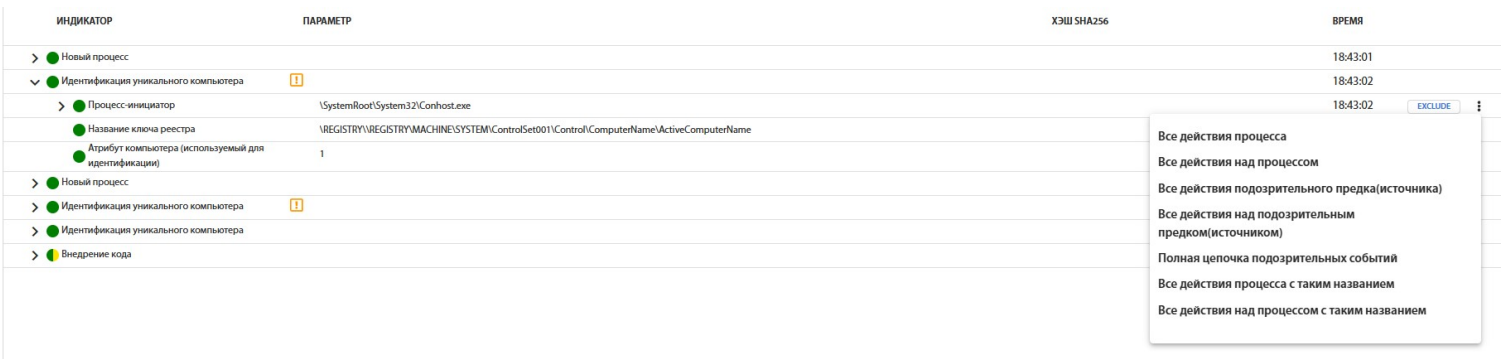


Рис. 18 – Фильтры списка зафиксированных активностей, доступные через контекстное меню

Система предоставляет возможность добавления файл или путь в исключение для анализа. Выделив путь или его часть и нажав правой кнопкой, откроется меню, в котором можно открыть окно добавления исключения.

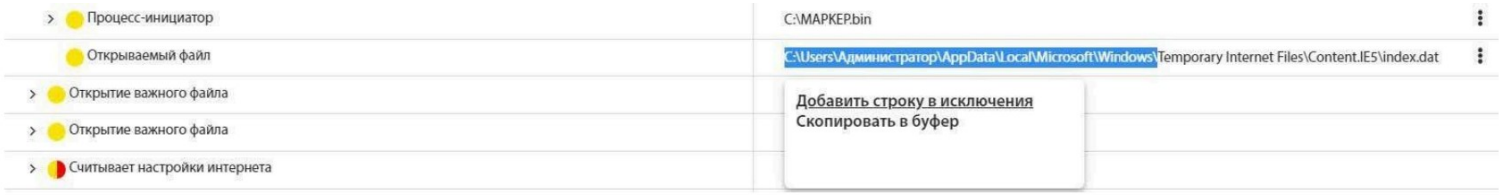


Рис 18.1 – Определение пути файла/директории исключения

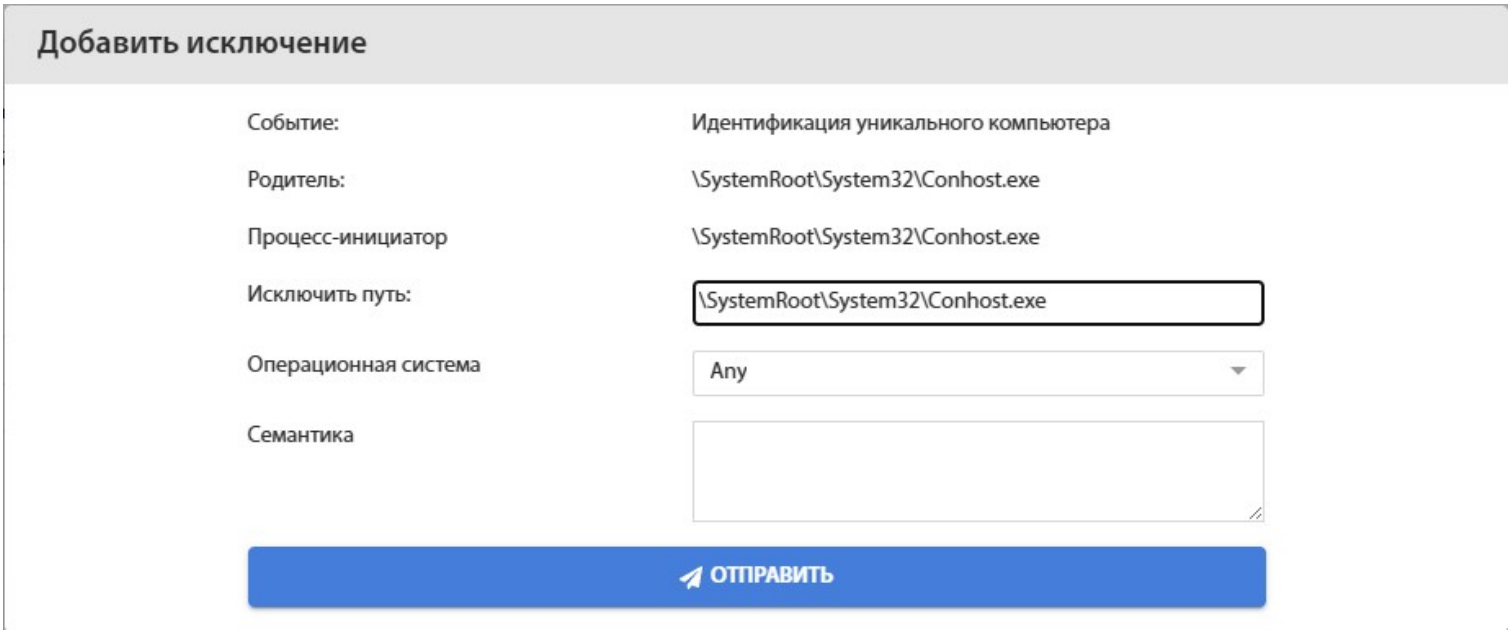


Рис 18.2 – Окно добавления исключения

Цепочка событий

Цепочка событий – интерактивное дерево событий. Максимальный размер дерева перед отображением ограничивается количеством отображаемых элементов.

Режим полного экрана открывает всплывающее окно для более удобного просмотра деревьев большого размера. Колесиком мышки можно масштабировать дерево. Нажатием и перетаскиванием левой кнопки мыши осуществляется изменение области просмотра. Щелчок левой мыши по событию выделяет все события в дереве с похожими путями красным цветом. Опция Выделить разными цветами отображает ранее невидимые элементы дерева и выделяет события с похожими путями одинаковым цветом. Список событий дерева активности приведен в Приложении 4.

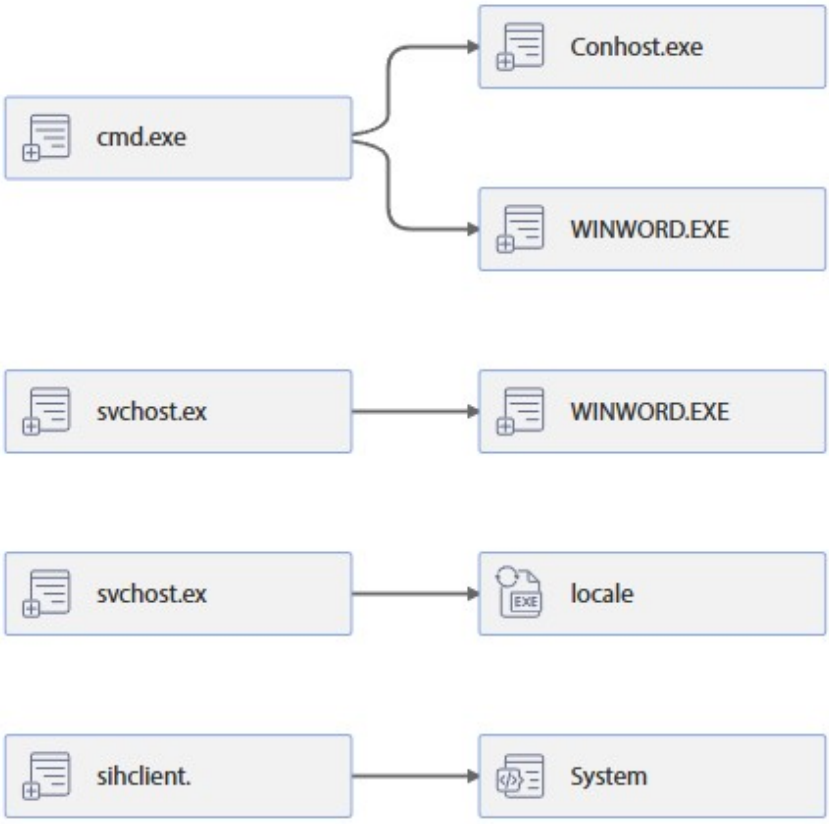


Рис. 19 – Представление активности в виде цепочки событий

Снимки экрана

Снимки экрана – галерея снимков экрана сделанных при обнаружении графического пользовательского интерфейса в анализируемых файлах. Зеленым цветом выделены области в которых обнаружены изменения между двумя последовательными снимками экрана. Отключение опции Выделять изменения скрывает такие снимки экрана. Снимки экрана с курсором мыши указывают на нажатие левой кнопки мыши при симуляции пользовательской активности на определенный элемент интерфейса, который вызвал изменение на экране. В нижнем правом углу снимков показана метка времени в формате `<минуты>:<секунды>.<сотая доля секунды>` со старта анализа.

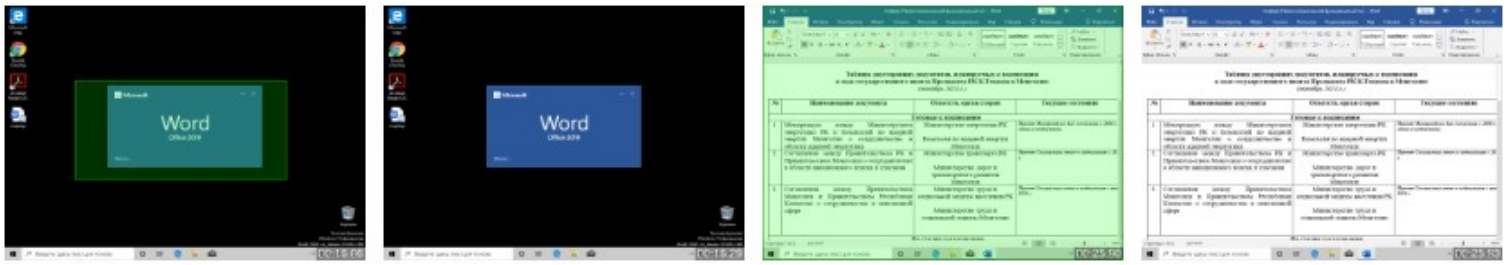


Рис. 20 – Галерея снимков экрана

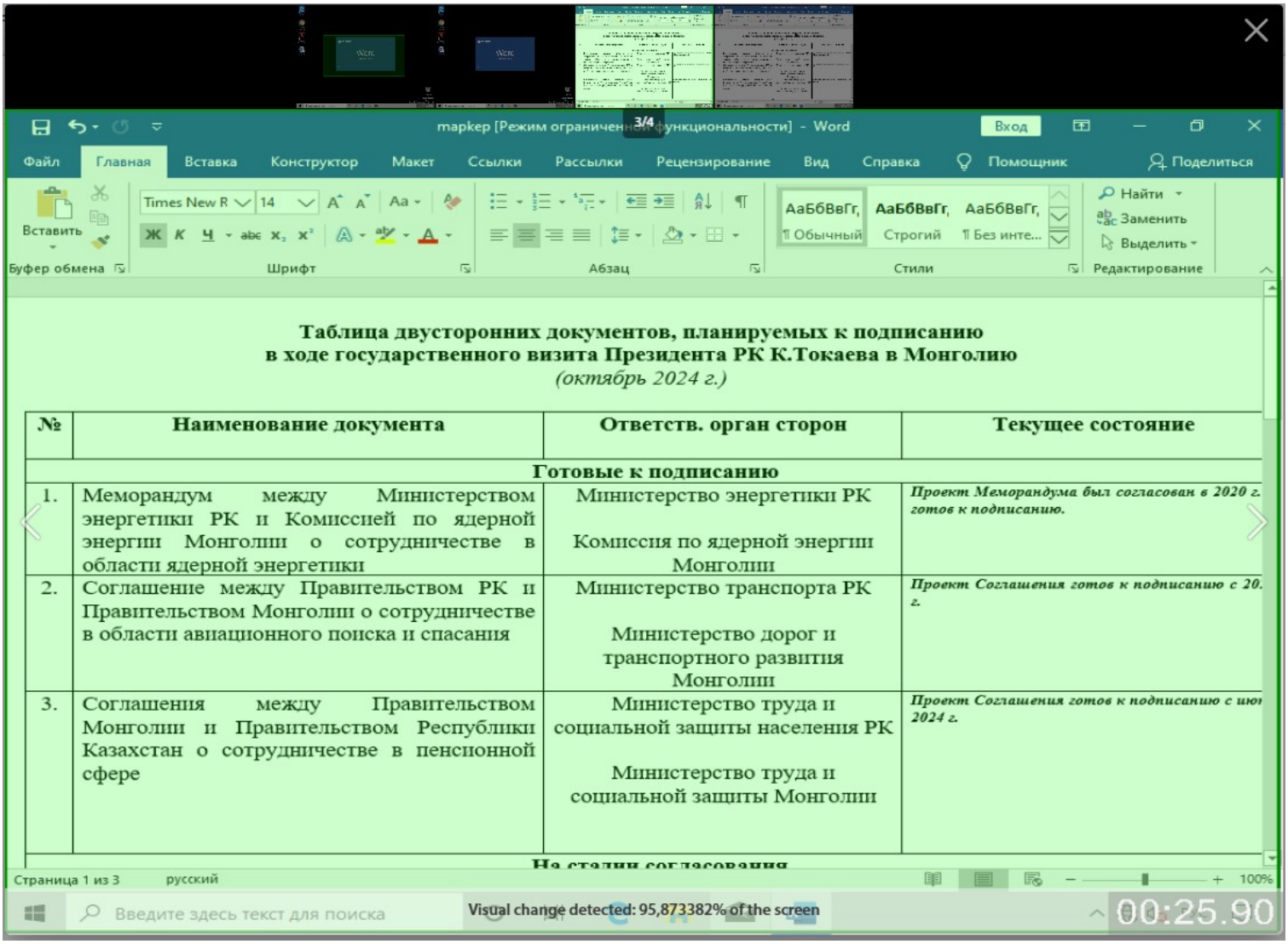


Рис. 21 – Снимок экрана

Сетевой анализ

На данной странице отображается информация по сетевому анализу PCAP файла.

> **ВНИМАНИЕ**
>
> Данный анализ производится только при включенном интернете во время анализа файла.

В рамках сетевого анализа представлена информация по запросам DNS, HTTP трафика и взаимодействия с хостами.

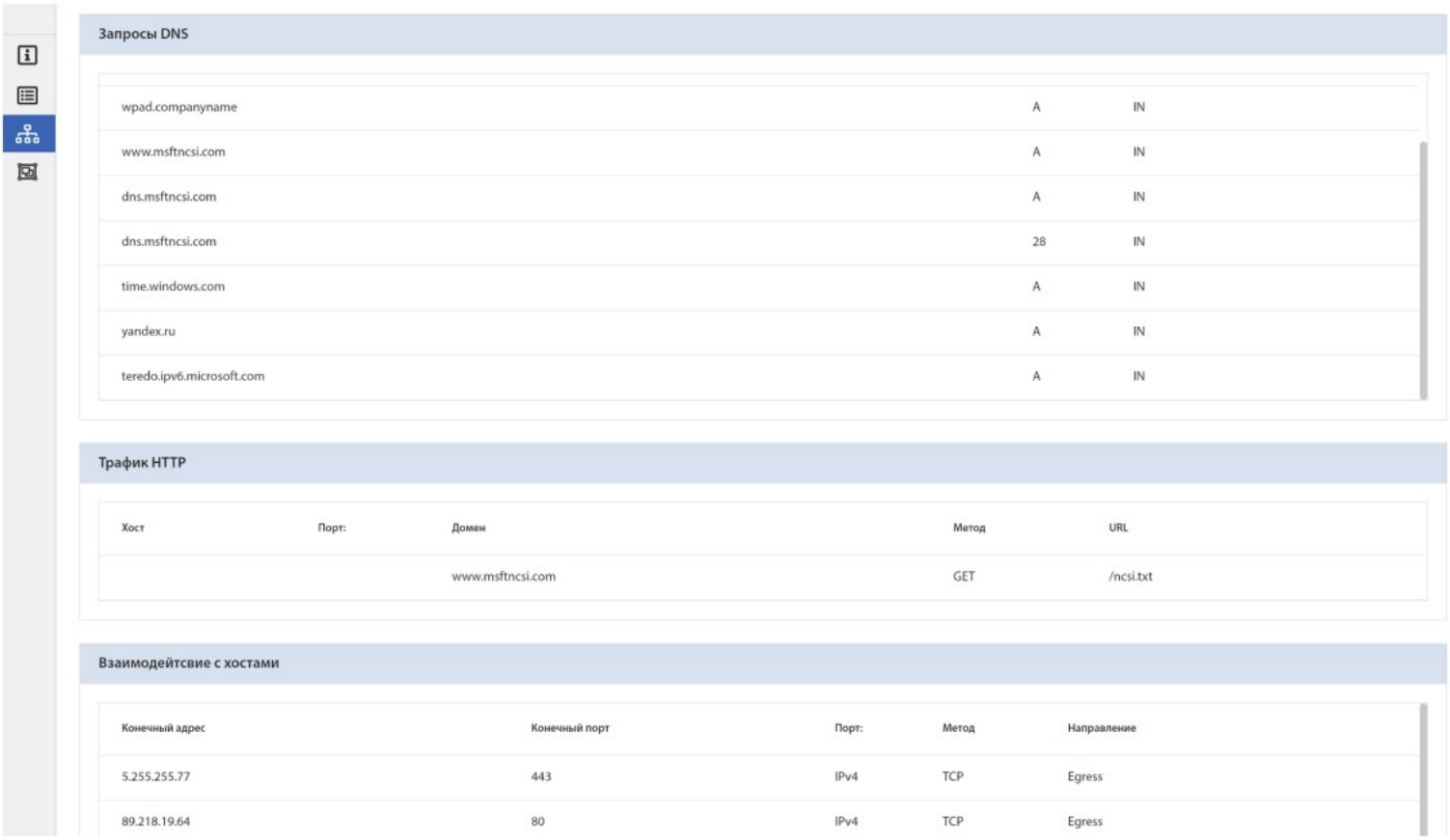


Рис. 21.1 - страница сетевого анализа

Извлеченные файлы

На данной странице отображается информация по извлеченным файлам во время динамического анализа. Это означает, что если во время динамического анализа, происходят процессы, извлекающие дополнительные файлы, то они посылаются на анализ отдельно. Информация о них отображается на данной странице. Извлеченные файлы показываются в таблице отчётов, найти их можно по хэшу.

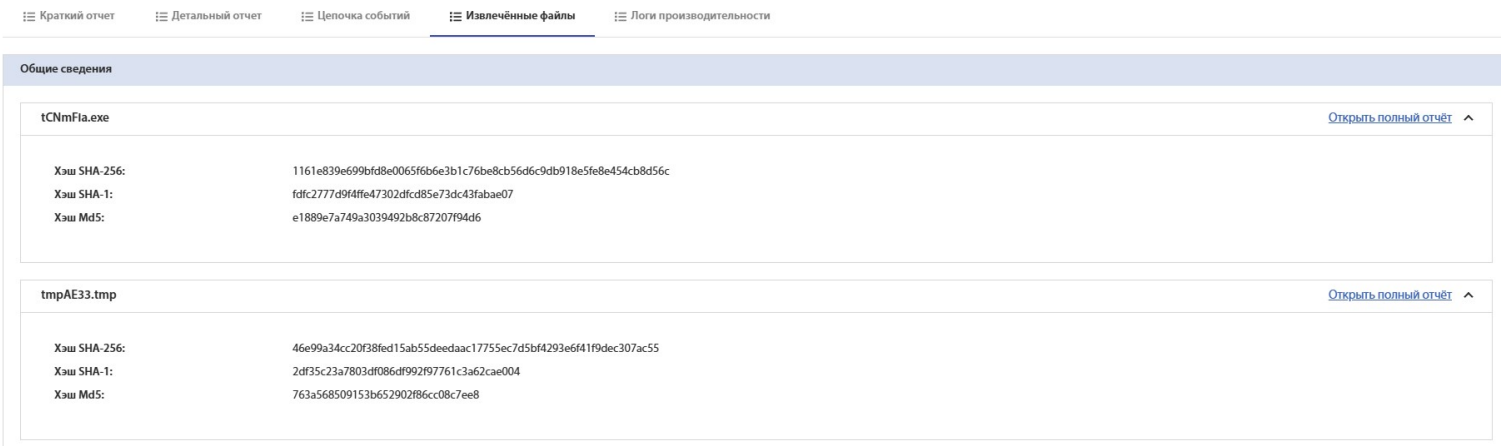


Рис 21.2 - страница извлеченных файлов

Логи производительности

На данной странице отображаются графики загрузки ЦПУ и памяти различными процессами, выявленными во время динамического анализа файла.

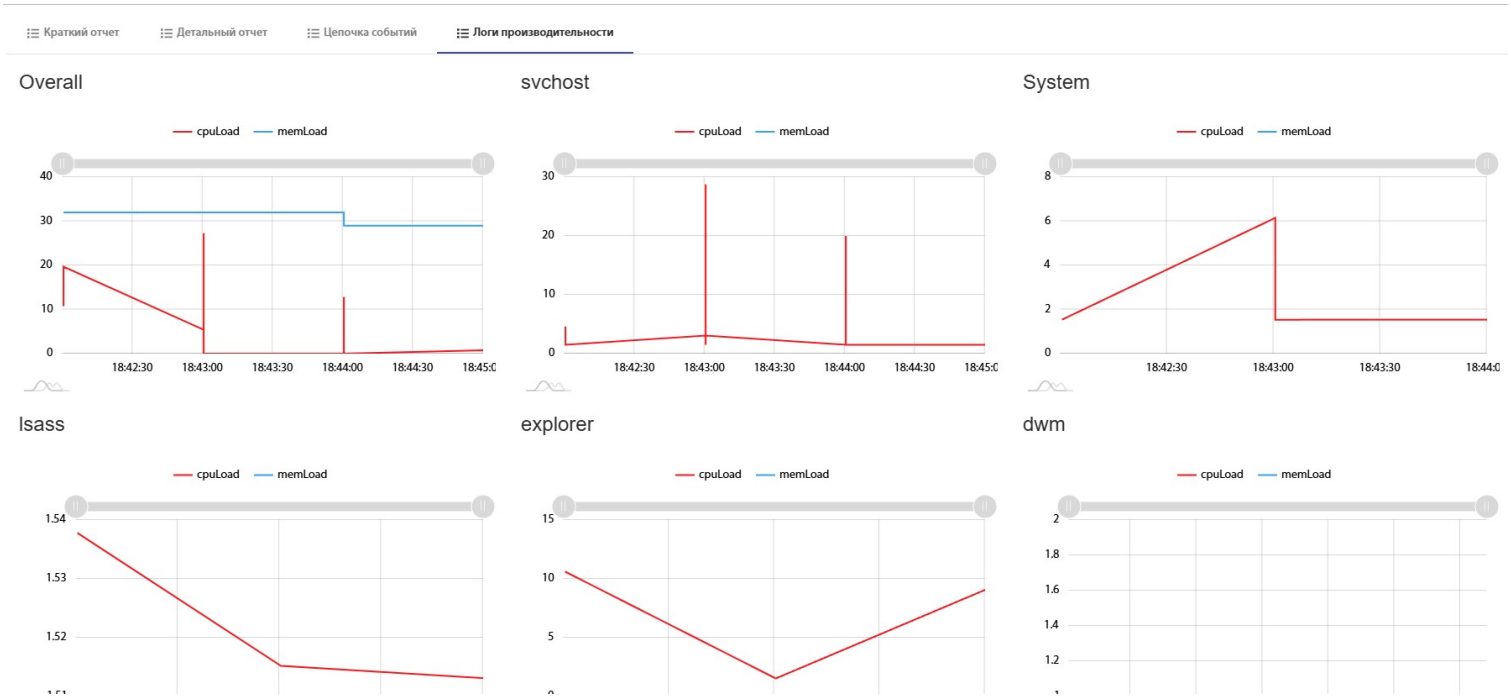


Рис. 21.3 - страница логов производительности

Приложение 1 – Индикаторы активности

 - Закрепление в ОС

 - Эксплоит

 - Прокси активность (вторжение)

 - Модификация ОС

 - Сетевая активность

 - Недоверенный процесс задерживает исполнение (возможно для обхода детекта)

Приложение 2 – Список активностей (событий)

Название события	Название параметров активности
Автозагрузка	Раздел реестра
	Имя ключа
	Путь до запускаемой программы
	Процесс-инициатор автозапуска
Новый процесс	Файл нового процесса
	Командная строка
	Процесс-родитель
Новый сервис	Имя сервиса
	Путь до программы сервиса
	Процесс инициатор
Внедрение кода	Процесс-цель инжекции
	Процесс инициатор (инжектор)
Кейлоггер	Процесс-шпион
	Программа-жертва
	Лог-файл клавиш (файл-учетки)

Название события	Название параметров активности
Доступ к внедрению кода	Открываемый процесс
	Процесс-источник
Доступ к реестру автозагрузки	Процесс инициатор
	Название ключа реестра
Извлечение исполняемого файла	Процесс-создатель файла (дроппер)
	Созданный файл
Установлено интернет - соединение	Процесс инициатор соединения
	Удаленный адрес
	Удаленный порт
	Локальный порт
	Тип протокола
Ожидание входящего подключения	Процесс-инициатор ожидающий подключения
	Локальный порт
	Тип протокола
Попытка установки интернет- соединения (неудачно)	Процесс инициатор соединения
	Удаленный адрес
	Удаленный порт
	Локальный порт

Название события	Название параметров активности
	Тип протокола
Перемещение важного файла	Процесс инициатор важного файла
	Новое имя файла
	Старое имя файла
Открытие чужого исполняемого файла	Процесс инициатор
	Открываемый файл
Открытие множества других исполняемых файлов	Процесс-инициатор
	Количество файлов
	Директории
Запись в чужой исполняемый файл (модификация)	Процесс-инициатор
	Модифицированный файл
Запись в многие исполняемые файлы (массовая модификация)	Процесс-инициатор
	Количество файлов
	Типы файлов
	Директории
Инфицирование чужого исполняемого файла (инжект кода в файл)	Процесс-инициатор
	Инфицированный файл
Инфицирование многих чужих исполняемых файлов (массовый инжект кода в файлы)	Процесс-инициатор

Название события	Название параметров активности
	Количество файлов
	Типы файлов
	Директории
Создание нового системного задания для планировщика задач	Процесс-инициатор
	Имя задания в планировщике
Установка исполняемого файла на самозапуск (через планировщик задач)	Процесс-инициатор
	Объект установленный на самозапуск
	Имя задания в планировщике
	Время и дата запуска объекта
	Имя пользователя для задания
Подозрительный процесс вторгся в легитимный процесс (внедрение DLL)	Процесс-цель инжекции
	Процесс инициатор (инжектор)
	Внедренный файл DLL
Недоверенный процесс задерживает исполнение (возможно для обхода детекта)	Процесс инициатор
	Время задержки исполнения
	Метод задержки
	Имя системного объекта используемого для задержки
Доступ к диску на низком уровне	Процесс инициатор

Название события	Название параметров активности
	Тип доступа
	Имя диска
Доступ на низком уровне ко многим дискам	Процесс инициатор
	Тип доступа
	Типы дисков
	Количество дисков
Управление диском на низком уровне	Процесс инициатор
	Имя диска
	Тип операции с диском
	Код управления для драйвера
Отслеживание ключа реестра	Процесс инициатор
	Название ключа реестра
	Значение фильтра события
	Тип операций с ключом
Идентификация уникальной инсталляции Windows	Процесс инициатор
	Название ключа реестра
	Атрибут Windows (используемый для идентификации)
Идентификация уникального компьютера	Процесс инициатор

Название события	Название параметров активности
	Название ключа реестра
	Атрибут компьютера (используемый для идентификации)
Считывает настройки интернета	Процесс инициатор
	Название ключа реестра
	Настройка
Попытка установки множества интернет-соединений (перебор IP- адресов)	Процесс инициатор соединения
	Количество сетевых соединений
	Подсеть удаленных адресов
	Список удаленных портов
	Список локальных портов
	Типы протоколов
Запись на диск на низком уровне	Процесс инициатор
	Имя диска
	Позиция начала записи (смещение)
	Количество записанных байт
	Записанный текст (символы)
	Записанный сырой буфер (байты)

Приложение 3 – Градация уровня опасности активности

- Нормальная активность
- Необычная активность
- Подозрительная активность
- Крайне подозрительная активность
- Вредоносная активность
- Критически вредоносная активность
- Опасная–разрушительная активность

Приложение 4 – Обозначения активностей в цепочке событий

 - Новый процесс

 - Автозагрузка

 - Новый сервис

 - Внедрение кода

 - Доступ к клавиатуре

 - Доступ к внедрению кода

 - Доступ к реестру автозагрузки

 - Извлечение исполняемого файла

 - Установлено интернет – соединение

 - Ожидание входящего подключения

 - Подключение к локальной сети

 - Попытка установки интернет – соединения (неудачно)

 - Перемещение важного файла

 - Открытие чужого исполняемого файла

 - Запись в чужой исполняемый файл (модификация)

 - Инфицирование чужого исполняемого файла (инжект кода в файл)

 - Открытие множества чужих исполняемых файлов

 - Запись в многие исполняемые файлы (массовая модификация)

 - Инфицирование многих чужих исполняемых файлов (массовый инжект кода в файлы)

 - Создание нового системного задания для планировщика задач

 - Установка исполняемого файла на самозапуск (через планировщик задач)

 - Подозрительный процесс вторгся в ЛЕГИТИМНЫЙ процесс (внедрение DLL)

 - Недоверенный процесс задерживает исполнение (возможно для обхода детекта)

 - Доступ к диску на низком уровне

 - Доступ на низком уровне ко многим дискам

 - Управление диском на низком уровне

 - Отслеживание ключа реестра

 - Идентификация уникальной инсталляции Windows

 - Идентификация уникального компьютера

 - Считывает настройки интернета

 - Попытка установки множества интернет-соединений

 - Запись на диск на низком уровне

 - Удаление чужого исполняемого файла

 - Удаление многих исполняемых файлов (массовое удаление)

 - Открытие важного файла

 - Открытие множества важных файлов

 - Модификация важного файла

 - Модификация множества важных файлов

 - Удаление важного файла

 - Удаление множества важных файлов