# Athena Sandbox

## СИСТЕМА ЗАЩИТЫ ОТ ЦЕЛЕНАПРАВЛЕННЫХ АТАК

### Функциональные характеристики

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



**Версия документа**

Сентябрь 16, 2021.

# СОДЕРЖАНИЕ

# 1 Перечень терминов и определений

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

**Таблица 1. Термины и определения**

| № п/п | Термин | Определение |
|---|---|---|
| 1. | Кибератака | Несанкционированное воздействие на вычислительную систему специальными программными средствами с целью нарушения её работы, получения доступа к чувствительной информации. |
| 2. | Песочница | Изолированная среда с контролируемым набором ресурсом, которая имитируем персональный компьютер или мобильное устройство, для исполнения программного обеспечения и анализа его поведения. |

## 2 Общие положения

Программный комплекс «ATHENA SANDBOX – система защиты от целенаправленных атак» (далее – ПК ATHENA) разработан компанией ООО «АВ Софт».

Компания ООО «АВ Софт» является единственным правообладателем ПК ATHENA.

Компания ООО «АВ Софт» находится в российской юрисдикции и не имеет участия иностранного капитала в своей организации.

## 3 Основные функциональные характеристики

Правообладатель и разработчик ПК ATHENA декларирует, что программный продукт совмещает в себе классы систем мультисканера и «песочницы» и предназначен для усиления безопасности ИТ-инфраструктуры организаций. Основная задача, решаемая ПК ATHENA – исследование программного обеспечения и веб-ссылок на предмет наличия в нем потенциально вредоносной угрозы серверам и рабочим станциям. В рамках основной задачи выносится вердикт и предоставляется информация, которая его обосновывает.

К функциональным возможностям ПК ATHENA относится:

- Обеспечение высокопроизводительной сигнатурной проверки поступающих в систему файлов;
- Выявление вредоносного программного обеспечения;
- Передача событий в SOC, SIEM, для последующего анализа;
- Возможность выгрузки семплов в карантин для последующего анализа;
- Формирование отчетности и статической информации по проверяемым файлам.

Результаты работы ПК ATHENA отображаются в веб-интерфейсе, возвращаются по API и могут быть отправлены в другую систему по протоколу syslog.

Общий алгоритм работы ПК ATHENA представлен на рисунке 1.

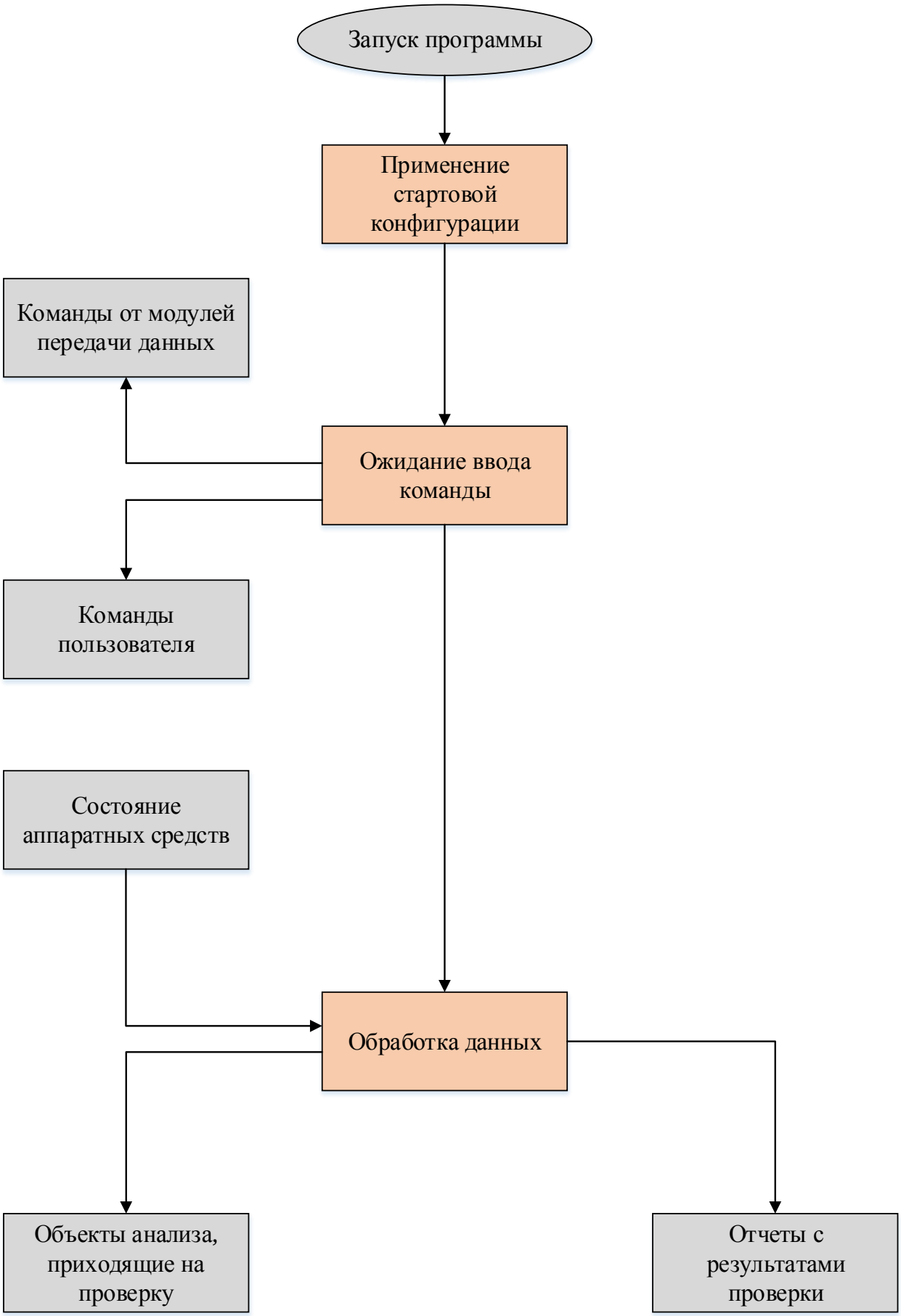
Запуск программы
Применение стартовой конфигурации
Команды от модулей передачи данных
Ожидание ввода команды
Команды пользователя
Состояние аппаратных средств
Обработка данных
Объекты анализа, приходящие на проверку
Отчеты с результатами проверки

**Рисунок 1. Общий алгоритм работы ПК ATHENA**

## 2.1 Используемые методы

Используемые методы основаны на возможностях аппаратных модулей технических средств, на котором развернут ПК ATHENA. Протоколы передачи данных второго и последующих уровней сетевой модели OSI реализованы по соответствующим стандартам.

## 2.2 Структура программы

ПК ATHENA является модульной системой, основная логика которой разделена по компонентам. Каждый компонент имеет интерфейс управления и внутреннюю логику работы.

ПК ATHENA имеет интерфейс управления. Команды пользователя проходят синтаксический анализ, затем вызываются интерфейсные методы компонентов, необходимые для выполнения команды.

Объекты анализа проходят проверки на корректность в соответствии со стандартами сетевых протоколов передачи данных, затем передаются компонентам с помощью интерфейсных методов компонентов. Внутренняя логика работы компонента может при необходимости использовать интерфейсные методы другого компонента.

Связь с аппаратными средствами устройства осуществляется через драйвер аппаратных средств.

Связи между основной процедурой и функциями программы выполняются в виде стандартных вызовов подпрограмм.

Связь с общесистемным программным обеспечением и общим программным обеспечением осуществляется посредством интерфейсов.

## 2.3 Вызов и загрузка

Вызов и загрузка данных в ПК ATHENA осуществляется через тонкий клиент (браузер) по сетевому адресу, выданному системе при её настройке.

# 4 Входные и выходные данные

Входными данными для ПК ATHENA являются:

- команды пользователя в веб-интерфейсе;
- объекты анализа, загружаемые на проверку и исследование;
- данные от внешних аналитических систем.

Выходными данными для ПК ATHENA являются:

- предоставление информации о проверенных объектах анализа;
- записи в базе данных.