О К Т О П У С

СИСТЕМА КОМПЛЕКСНОЙ АНТИВИРУСНОЙ ПРОВЕРКИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

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

Авторское право

Версия документа

Декабрь 20, 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.	Автоматический режим	Режим работы системы, в котором файлы и приложения, поступающие на интерфейс, автоматически загружаются в систему и анализируются на предмет нелегитимного содержимого.
2.	Сигнатурная проверка	Анализ файла на предмет наличия вредоносных сочетаний кода внутри синтаксической структуры.
3.	Синтаксическая структура файла	Набор правил, описывающий комбинации символов алфавита, считающиеся правильно структурированной программой (документом) или её фрагментом.

2 Общие положения

Система комплексной антивирусной проверки программного обеспечения Октопус (далее – система Октопус) разработана компанией ООО «АВ Софт».

Компания ООО «АВ Софт» является единственным правообладателем системы Октопус.

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

Правообладатель и разработчик системы Октопус декларирует, что система Октопус относится к классу систем антивирусных мультисканеров и предназначена для усиления информационной безопасности в ИТ-инфраструктуре организации. Система осуществляет статическую проверку файлов на предмет вредоносных или подозрительных элементов в составе их синтаксической структуры и позволяет снизить риски использования стандартных антивирусных средств защиты, минимизировать количество ложных срабатываний. Система Октопус также может применяться для целей детального изучения синтаксической структуры файлов, поступающих на проверку.

3 Основные функциональные возможности

К основным функциональным возможностям системы Октопус относится:

- Обеспечение высокопроизводительной статической проверки поступающих в систему файлов;
- Выявление вредоносного программного обеспечения (далее – ВПО);
- Передача событий в SOC, SIEM для последующего их анализа;
- Возможность выгрузки семплов в карантин для последующего разбора и анализа;
- Формирование отчётности и статистической информации по проверяемым файлам.

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

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

Система Октопус поддерживает проверку следующих типов объектов:

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

Система Октопус принимает на анализ любые типы файлов, примеры:

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

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

Общий алгоритм работы системы представлен на рисунке 1.

Общий алгоритм работы

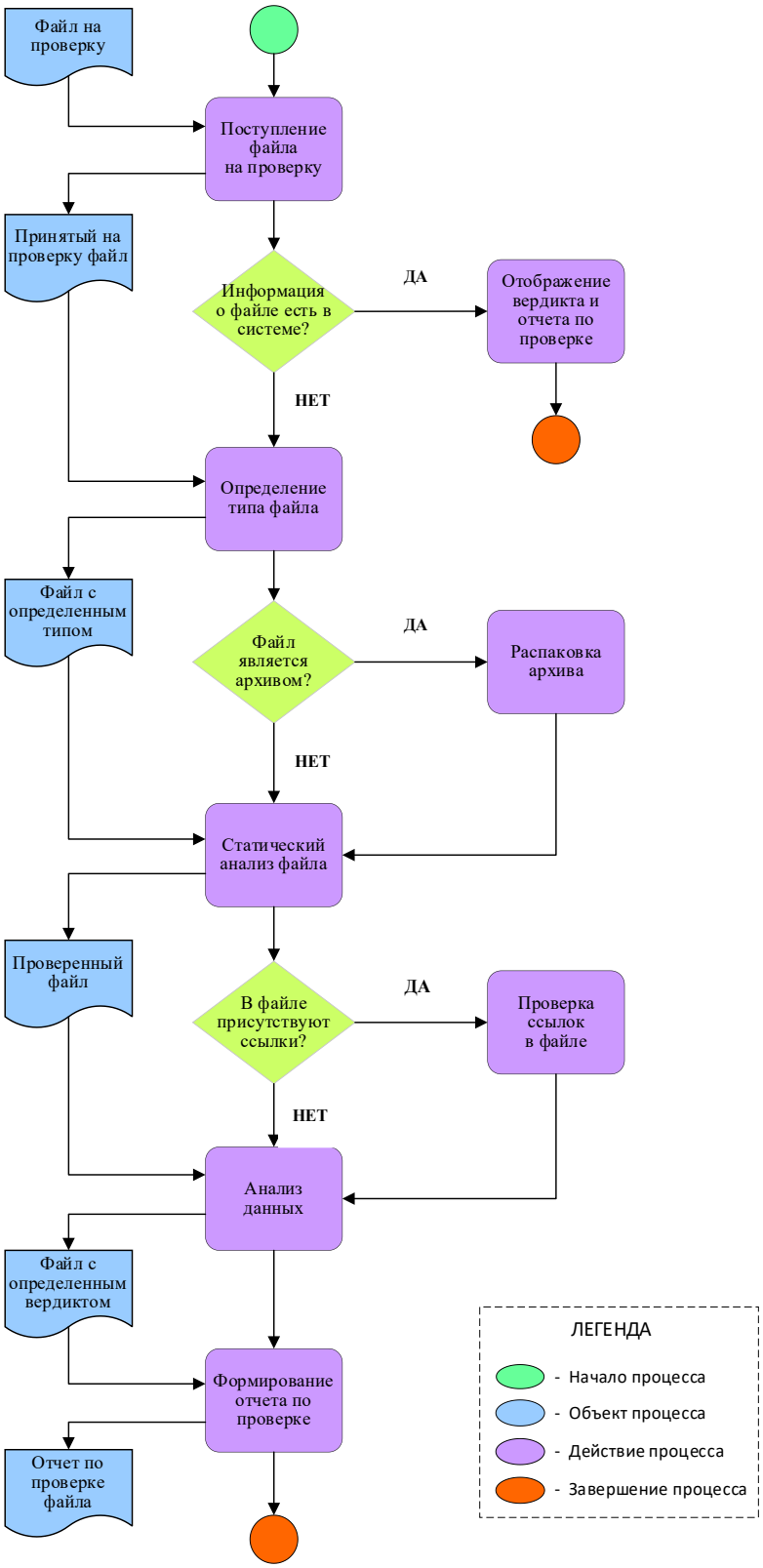

Рисунок 1. Общий алгоритм работы системы

4 Режимы работы

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

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