

# Лицензия Creative Commons Attribution-ShareAlike 4.0 International (CC BY-SA 4.0)

**Название работы:** Метод предотвращения вредоносного ПО

**Автор:** Анвар Кутлимуратов

**Год создания:** 2009

## Полное описание работы

### 1. Введение

Современное вредоносное ПО становится все более сложным, и традиционные антивирусные системы часто не могут обеспечить надежную защиту. В данном документе представлен **Метод предотвращения вредоносного ПО**, основанный на **изменении расширений файлов для предотвращения выполнения вредоносных программ в системе**. Этот метод был разработан как **альтернативный подход к традиционным антивирусным решениям** и тестировался на практике с 2009 года.

### 2. Принцип работы

Данный метод работает по следующим принципам:

1. **Изменение расширений файлов** – смена стандартного расширения `.exe` исполняемых файлов на другой формат, например `.123`.
2. **Блокировка выполнения на уровне системы** – поскольку вредоносное ПО обычно использует `.exe`, система, не распознающая такие файлы, не позволяет вирусу запуститься.
3. **Мониторинг активности системы** – если вредоносное ПО пытается восстановить расширение `.exe`, система не распознает его и предотвращает выполнение.
4. **Управляемый пользователем запуск** – только доверенные приложения могут выполняться с измененным расширением (`.123`).

### 3. Отличие от традиционных методов

Традиционные антивирусные программы обнаруживают вредоносное ПО следующими способами:

- **Обнаружение по сигнатурам** – выявление вирусов на основе известных сигнатур.
- **Анализ поведения** – выявление подозрительной активности во время выполнения программы.
- **Технология песочницы (Sandboxing)** – запуск файлов в изолированной среде для анализа их поведения.

Данный метод, однако, **не пытается обнаружить вредоносное ПО, а полностью предотвращает его выполнение**.

## 4. Обнаружение новых, неуловимых вирусов

Традиционные антивирусные системы испытывают трудности с выявлением **атак нулевого дня и полиморфных вирусов**. Метод предотвращения вредоносного ПО вынуждает такие вирусы раскрывать себя, поскольку они зависят от выполнения .exe. Если вирус пытается восстановить расширение .exe, система сразу же запрашивает у пользователя метод выполнения, что позволяет **моментально выявить и предотвратить подозрительную активность**.

Этот подход может стать **мощным инструментом для выявления и предотвращения новых и неизвестных вирусов**, создавая универсальный барьер безопасности против всех вредоносных программ.

## 5. Практическое применение

Данный метод может применяться в следующих областях:

- **Корпоративная ИТ-безопасность** – защита внутренних сетей от вредоносных угроз.
- **Персональные компьютеры** – усиление защиты индивидуальных пользователей.
- **Облачные сервисы и серверы** – защита облачных сред и серверных инфраструктур от вредоносных программ.

## 6. О лицензии

Данная работа распространяется по лицензии **Creative Commons Attribution-ShareAlike 4.0 International (CC BY-SA 4.0)**.

<https://creativecommons.org/licenses/by-sa/4.0/>