

## ИСТОРИЯ ПОЯВЛЕНИЯ ВИРУСОВ И АНТИВИРУСНЫХ ПРОГРАММ

Габун Айман, Марокко

Научный руководитель – доц., канд. психол. наук В.А. Демченко  
Харьковский национальный университет радиоэлектроники  
e-mail: [viktoriia.demchenko@nure.ua](mailto:viktoriia.demchenko@nure.ua)

Более 25 лет компьютерные вирусы досаждают пользователям по всему миру, и более 25 лет антивирусные эксперты борются с ними.

Антивирусная программа (антивирус) – программа, позволяющая выявлять вирусы, лечить зараженные файлы и диски, обнаруживать и предотвращать подозрительные действия.

Однако практически все основные антивирусные технологии были придуманы еще к середине 90-х годов, а в настоящее время наблюдается экстенсивное их развитие, включающее в себя различные технологические совершенствования. Антивирусы были далеко не первым направлением в области защиты информации. Гораздо раньше были созданы, например, системы контроля за доступом, защиты от взлома. Антивирусные программы в виде законченных коммерческих проектов впервые появились около 20 лет назад.

Первый вирус для компьютеров Apple появился в 1977, а уже в 1981 появились вирусные программы, представляющие реальную угрозу данным. Энди Хопкинс создал первые антивирусные программы в 1984 году, они носили названия и – ВОСНК4ВОМВ и СНК4ВОМВ. СНК4ВОМВ сканировал текст загрузочного модуля для выявления текстовых сообщений и подозрительных участков в коде. Вторая программа ВОСНК4ВОМВ перехватывала запись и форматирование, которые выполнялись через BIOS. Выполнение запрещенных операций можно было запретить или разрешить.

Первая антивирусная программа, которую мы знаем, и сейчас, защищает от вирусных атак и появилась в 1985 году. Джи Вонг создал программу под названием DRPROTECT. Антивирус блокировал все операции, такие как запись и форматирование, которые выполнялись через BIOS. При выявлении какой либо операции антивирус требовал перезагрузки системы.

До начала 90-х годов антивирусы представляли собой набор образцов вирусного кода, которые сохранялись в программе. В антивирусе существовал поиск сохраненных образцов в файлах. Образцы вирусного кода не были зашифрованы создателями, поэтому случалось такое, что антивирусные программы, сканируя друг друга, находили те самые не зашифрованные образцы вирусного кода и считали это вирусом.

Со временем антивирусными программами стали интересоваться крупные компании, в штате которых было много программистов. Большую роль в развитии антивирусов сыграли русские программисты. В 1992 году появляется новый антивирус с названием MtE, который был доступен не только опытному, но и начинающему программисту. MtE – это генератор постоянно меняющегося (полиморфного) кода. Полиморфные вирусы стали появляться ежедневно, из-за этого дополнительные способы противостояния вирусам перестали действовать. На помощь пришел эмулятор кода. Антивирусная программа обходила зашифрованную часть и добиралась до самого вируса. Первой программой с эмулятором кода стал AVP, который был создан программистом Евгением Касперским. Наряду с эмулятором кода, который помог антивирусным программам бороться с быстро растущим количеством вирусов, появились системы защиты, такие как криптоанализ, эвристический анализатор, статистический анализ и поведенческий блокатор. Принцип работы этих систем защиты от вирусов используется до сих пор.

С появлением сложных программ требования к антивирусным программам возросли. Одной из задач была проверка файлов во время обращения к ним, а также отличная работа с программой Microsoft Office. К этому времени количество программистов-разработчиков уменьшилось в связи со строгими требованиями.

В связи с быстрым распространением Интернета и появлением вирусов, которые маскируются под обычные программы, разработчики антивирусного программного обеспечения внедрили файрволы. Борьба с вирусными программами продолжается и сегодня. На данный момент существует приблизительно 60 компаний, которые разрабатывают новые антивирусы.

Вместе с платными антивирусами существуют и бесплатные, один из которых является Microsoft Security Essentials, который по своей функциональности ничуть не хуже чем платные антивирусные программы.