АНТИВИРУСЫ

МОРЕЙСКИЙ МИХАИЛ
ЖЕМОЙТЕЛЬ АЛЕКСАНДР

Каждый пользователь ПК сталкивается с компьютерными вирусами. Что же это такое? На самом деле под этим названием скрывается несколько видов вредоносных программ, каждая из которых уже давно имеет свою своеобразную методику проникновения в компьютер. На сегодня известно около 50 тысяч компьютерных вирусов. Эти маленькие вредоносные программы живут по трём правилам – размножаться, скрываться и портить.

Для обнаружения компьютерных вирусов, а также нежелательных (считающихся вредоносными) программ и восстановления заражённых (модифицированных) такими программами файлов и профилактики — предотвращения заражения (модификации) файлов или операционной системы вредоносным кодом разработано несколько видов специальных программ, которые

н

Виды антивирусных программ

- Программы-детекторы
- Программы-вакцины (иммунизаторы)
- Программы-доктора (фаги)
- Программы-фильтры
- Программы-ревизоры
- Сканер

Программы-детекторы осуществляют поиск характерной для конкретного вируса сигнатуры в оперативной памяти и в файлах и при обнаружении выдают соответствующее сообщение. Недостатком таких антивирусных программ является то, что они могут находить только те вирусы, которые известны разработчикам таких программ.

Программы-доктора или фаги, а также программы-вакцины не только находят зараженные вирусами файлы, но и «лечат» их, то есть удаляют из файла тело программы-вируса, возвращая файлы в исходное состояние. В начале своей работы фаги ищут вирусы в оперативной памяти, уничтожая их, и только затем переходят к «лечению» файлов. Среди фагов выделяют полифаги, то есть программы-доктора, предназначенные для поиска и уничтожения большого количества вирусов.

Программы-ревизоры (инспектора) относятся к самым надежным средствам защиты от вирусов. Ревизоры (инспектора) проверяют данные на диске на предмет вирусов-невидимок, изучают, не забрался ли вирус в файлы, нет ли посторонних в загрузочном секторе жесткого диска, нет ли несанкционированных изменений реестра Windows. Причем инспектор может не пользоваться средствами операционной системы для обращения к дискам (а значит, активный вирус не сможет это обращение перехватить).

Вакцины или иммунизаторы - это резидентные программы, предотвращающие заражение файлов. Вакцины применяют, если отсутствуют программы-доктора, «лечащие» этот вирус. Вакцинация возможна только от известных вирусов. Вакцина модифицирует программу или диск таким образом, чтобы это не отражалось на их работе, а вирус будет воспринимать их зараженными и поэтому не внедрится. В настоящее время программы-вакцины имеют ограниченное применение.

Программы-фильтры (мониторы) или «сторожа» представляют собой небольшие резидентные программы, предназначенные для обнаружения подозрительных действий при работе компьютера, характерных для вирусов. Такими действиями могут являться:

1. попытки коррекции файлов с расширениями COM, EXE
2. изменение атрибутов файла
3. прямая запись на диск по абсолютному адресу
4. запись в загрузочные сектора диска
5. загрузка резидентной программы.

Принцип работы **антивирусных сканеров** основан на проверке файлов, секторов и системной памяти, а также поиске в них известных и новых (неизвестных сканеру) вирусов. Для поиска известных вирусов используются так называемые «маски». Маской вируса является некоторая постоянная последовательность кода, специфичная для конкретного вируса. Если вирус не содержит постоянной маски или длина этой маски недостаточно велика, то используются другие методы.

Методы защиты от вирусов

Для защиты от вирусов используют три группы методов:

1. Методы, основанные на *анализе содержимого файлов* (как файлов данных, так и файлов с кодами команд). К этой группе относятся сканирование сигнатур вирусов, а также проверка целостности и сканирование подозрительных команд.
2. Методы, основанные на *отслеживании поведения программ* при их выполнении. Эти методы заключаются в протоколировании всех событий, угрожающих безопасности системы и происходящих либо при реальном выполнении проверяемого кода, ибо при его программной эмуляции.
3. Методы *регламентации порядка работы* с файлами и программами. Эти методы относятся к административным мерам обеспечения безопасности.

Требования предъявляемые к антивирусным программам:

- **Стабильность и надежность работы**
- **Размеры вирусной базы программы**
- **Скорость работы программы**
- **Многоплатформенность**

ПРИМЕРЫ АНТИВИРУСНЫХ

Антивирус Касперского	*Антивирус NOD32*	*Dr.Web*	*Avast*
антивирусное программное обеспечение, предоставляет пользователю защиту от вирусов, троянских программ, шпионских программ, руткитов, adware, а также неизвестных угроз с помощью проактивной защиты, включающей компонент HIPS.	Антивирус ESET NOD32 разработан на основе передовой технологии ThreatSense®. Ядро программы обеспечивает проактивное обнаружение всех типов угроз и лечение зараженных файлов (в том числе, в архивах) благодаря широкому применению интеллектуальных технологий, сочетанию эвристических методов и традиционного сигнатурного детектирования.	Предназначен для защиты от почтовых и сетевых червей, руткитов, файловых вирусов, троянских программ, стелс-вирусов, полиморфных вирусов, бестелесных вирусов, макровирусов, вирусов, поражающих документы MS Office, скрипт-вирусов, шпионского ПО (spyware), программ-похитителей паролей, клавиатурных шпионов, программ платного дозвона, рекламного ПО (adware), потенциально опасного ПО, хакерских утилит, программ-люков, программ-шуток, вредоносных скриптов и других вредоносных объектов.	Инновационное антивирусное и антишпионское ядро сканирования Эффективная защита от руткитов – вредоносных программ, невидимых для антивирусов Сканирование при загрузке – один из самых эффективных антивирусных инструментов Avast, позволяющий провести проверку ДО загрузки Windows Система avast! WebRep, позволяющая получить информацию о надёжности веб-сайтов на основе отзывов пользователей.

ЗАКЛЮЧЕНИЕ

Ни один тип антивирусных программ по отдельности не дает полной защиты от вирусов. Поэтому в современные антивирусные комплекты программ обычно входят компоненты, реализующие все эти функции.

Из всего вышесказанного можно смело сделать вывод, что для предотвращения заражения вирусом и соответственно всех его последствий необходимо правильно выбрать и установить в систему антивирусное программное обеспечение и соблюдать элементарные меры предосторожности.

Спасибо за внимание!