

**Защита от
компьютерных
вирусов.
Антивирусные
программы.**

Способы защиты от компьютерных вирусов

- 1) Не запускайте программы, полученные из Интернета или в виде вложения в сообщение электронной почты без проверки на наличие в них вируса.
- 2) Необходимо проверять все внешние диски на наличие вирусов, прежде чем копировать или открывать содержащиеся на них файлы или выполнять загрузку компьютера с таких дисков.

Способы защиты от компьютерных вирусов

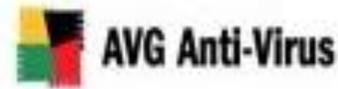
- 3) Необходимо установить антивирусную программу и регулярно пользоваться ею для проверки компьютеров. Оперативно пополняйте базу данных антивирусной программы набором файлов сигнатур вирусов, как только появляются новые сигнатуры.
- 4) Основным средством защиты информации – это резервное копирование ценных данных, которые хранятся на жестких дисках

Способы защиты от компьютерных вирусов

- 5) Необходимо регулярно сканировать жесткие диски в поисках вирусов. Сканирование обычно выполняется автоматически при каждом включении ПК и при размещении внешнего диска в считывающем устройстве. При сканировании антивирусная программа ищет вирус путем сравнения кода программ с кодами известных ей вирусов, хранящихся в базе данных.
- 6) создавать надежные пароли, чтобы вирусы не могли легко подобрать пароль и получить разрешения администратора. Регулярное архивирование файлов позволит минимизировать ущерб от вирусной атаки

Антивирусная программа

- **Антивирусная программа (антивирус)** — специализированная программа для обнаружения компьютерных вирусов, а также нежелательных (считающихся вредоносными) программ вообще и восстановления заражённых (модифицированных) такими программами файлов, а также для профилактики — предотвращения заражения (модификации) файлов или операционной системы вредоносным кодом.



Модули антивирусной программы

- Эвристический модуль – для выявления неизвестных вирусов.
- Монитор – программа, которая постоянно находится в оперативной памяти ПК
- Устройство управления, которое осуществляет запуск антивирусных программ и обновление вирусной базы данных и компонентов
- Почтовая программа (проверяет электронную почту)
- Программа сканер – проверяет, обнаруживает и удаляет фиксированный набор известных вирусов в памяти, файлах и системных областях дисков
- Сетевой экран – защита от хакерских атак

Программы-детекторы

-обеспечивают поиск и обнаружение вирусов в оперативной памяти и на внешних носителях, и при обнаружении выдают соответствующее сообщение. Различают детекторы универсальные и специализированные.

- **Универсальные детекторы** в своей работе используют проверку неизменности файлов путем подсчета и сравнения с эталоном контрольной суммы. Недостаток универсальных детекторов связан с невозможностью определения причин искажения файлов.
- **Специализированные детекторы** выполняют поиск известных вирусов по их сигнатуре (повторяющемуся участку кода). Недостаток таких детекторов состоит в том, что они неспособны обнаруживать все известные вирусы. Детектор, позволяющий обнаруживать несколько вирусов, называют **полидетектором**. Недостатком таких антивирусных программ является то, что они могут находить только те вирусы, которые известны разработчикам таких программ.

Программы-доктора

-не только находят зараженные вирусами файлы, но и «лечат» их, т.е. 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**, т.е. программы-доктора, предназначенные для поиска и уничтожения большого количества вирусов.

- Учитывая, что постоянно появляются новые вирусы, программы-детекторы и программы-доктора быстро устаревают, и требуется регулярное обновление их версий.

Программы-ревизоры

-относятся к самым надежным средствам защиты от вирусов. Ревизоры запоминают исходное состояние программ, каталогов и системных областей диска тогда, когда компьютер не заражен вирусом, а затем периодически или по желанию пользователя сравнивают текущее состояние с исходным. Обнаруженные изменения выводятся на экран видеомонитора. Как правило, сравнение состояний производят сразу после загрузки операционной системы. При сравнении проверяются длина файла, код циклического контроля (контрольная сумма файла), дата и время модификации, другие параметры.

- Программы-ревизоры имеют достаточно развитые алгоритмы, обнаруживают стелс-вирусы и могут даже отличить изменения версии проверяемой программы от изменений, внесенных вирусом.

Программы-фильтры

-представляют собой небольшие резидентные программы, предназначенные для обнаружения подозрительных действий при работе компьютера, характерных для вирусов. Такими действиями могут являться:

- попытки коррекции файлов с расширениями COM и EXE;
- изменение атрибутов файлов;
- прямая запись на диск по абсолютному адресу;
- запись в загрузочные сектора диска;
- загрузка резидентной программы.

Программы-*Вакцины*

-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.

- Существенным недостатком таких программ является их ограниченные возможности по предотвращению заражения от большого числа разнообразных вирусов.

