



**Защита  
информации,  
АНТИВИРУСНАЯ  
защита**

**Компьютерный вирус — это целенаправленно созданная программа, автоматически приписывающая себя к другим программным продуктам, изменяющая или уничтожающая их. Компьютерные вирусы могут заразить компьютерные программы, привести к потере данных и даже вывести компьютер из строя.**

Компьютерные вирусы могут распространяться и проникать в операционную и файловую систему ПК только через внешние магнитные носители (жесткий и гибкий диски, компакт-диски) и через средства межкомпьютерной коммуникации.

# Классы вредоносных программ

В зависимости от среды обитания вирусы можно разделить на сетевые, файловые, загрузочные и файлово-загрузочные.

**Сетевые** вирусы распространяются по различным компьютерным сетям.

**Файловые** вирусы внедряются главным образом в исполняемые модули, т.е. в файлы, имеющие расширения COM и EXE.

**Загрузочные** вирусы внедряются в загрузочный сектор диска или сектор, содержащий программу загрузки системного диска.

**Файлово - загрузочные** вирусы заражают файлы и загрузочные сектора дисков.

# Классы вредоносных программ

**По способу заражения** вирусы разделяются на резидентные и нерезидентные.

**Резидентный** вирус при заражении компьютера оставляет в оперативной памяти свою резидентную часть, которая потом перехватывает обращение операционной системы к объектам заражения (файлам, загрузочным секторам дисков и т.д.) и внедряется в них.

**Нерезидентные** вирусы не заражают память компьютера и являются активными ограниченное время.

# Классы вредоносных программ

*По степени воздействия* выделяют:

- **неопасные** вирусы, которые не мешают работе компьютера,
- **опасные**, которые могут привести к различным нарушениям в работе компьютера,
- **очень опасные**, воздействие которых может привести к потере программ, уничтожению данных, стиранию информации в системных областях диска.



Для обнаружения, удаления и защиты от компьютерных вирусов разработано несколько видов специальных программ, которые позволяют обнаруживать и уничтожать вирусы. Такие программы называются **антивирусными**.

# Виды антивирусных программ

**1. Программы-детекторы** осуществляют поиск характерной для конкретного вируса сигнатуры в оперативной памяти и 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.

**2. Программы-доктора** или **фаги** не только находят зараженные вирусами файлы, но и возвращают файлы в исходное состояние. В начале своей работы флаги ищут вирусы в оперативной памяти, уничтожая их, и только затем переходят к «лечению» файлов.

# Виды антивирусных программ

**3. Программы-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. Обнаружение изменения выводится на экран монитора.

**4. Программы - вакцины или иммунизаторы** — это резидентные программы, предотвращающие заражение файлов.



# Виды антивирусных программ

**5. Программы-фильтры** или **сторожа**, представляют собой небольшие резидентные программы, предназначенные для обнаружения подозрительных действий при работе компьютера, характерных для вирусов:

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

При попытке вирусной атаки сторож посылает сообщение и предлагает запретить или разрешить соответствующие действия.

# Признаки заражения вирусом

Существует ряд признаков, свидетельствующих о заражении компьютера:

- вывод на экран непредусмотренных сообщений или изображений;
- подача непредусмотренных звуковых сигналов;
- неожиданное открытие и закрытие лотка CD-ROM-устройства;
- произвольный, без вашего участия, запуск на компьютере каких-либо программ;
- вывод на экран предупреждения о попытке какой-либо из программ вашего компьютера выйти в Интернет, хотя вы никак не инициировали такое ее поведение (при наличии установленной на вашем компьютере соответствующей антивирусной программы).

# Признаки заражения вирусом

Существуют и косвенные признаки заражения вашего компьютера:

- частые зависания и сбои в работе компьютера;
- медленная работа компьютера при запуске программ;
- невозможность загрузки операционной системы;
- исчезновение файлов и каталогов или искажение их содержимого;
- частое обращение к жесткому диску, когда часто мигает лампочка на системном блоке;
- Microsoft Internet Explorer зависает или ведет себя неожиданным образом, например окно программы невозможно закрыть.