- **Компьютерный вирус** – специально написанная компьютерная программа, способная самопроизвольно присоединяться к другим программам, создавать свои копии, внедрять их в файлы с целью порчи и уничтожения файлов и каталогов, создания помех в работе.
- **Антивирусными** называются программы, предназначенные для обнаружения и удаления компьютерных вирусов и защиты данных от порчи и удаления.

- **Основные способы борьбы с вирусами:**
- исправление зараженного файла;
- изоляция файла (карантин);
- удаление зараженного файла с диска и последующая замена его (по возможности) незараженной копией.

Признаки проявления вирусов:

- неправильная работа нормально работавших программ;
- медленная работа компьютера;
- невозможность загрузки операционной системы;
- исчезновение файлов и каталогов;
- изменение размеров файлов;

- неожиданное увеличение количества файлов на диске;
- уменьшение размеров свободной оперативной памяти;
- вывод на экран неожиданных сообщений и изображений;
- подача непредусмотренных звуковых сигналов;
- частые зависания и сбои в работе компьютера.

Классификация

- **По степени опасности**:

- ***неопасные*** (не мешают работе, не уменьшают объём оперативной памяти и дисковой памяти, могут проявляться подачей звуковых сигналов, текстовых или графических сообщений);
- ***опасные*** (могут привести к сбоям в работе, зависанию компьютера);
- ***очень опасные*** (приводят к потере программ, уничтожению данных).

- **По среде обитания**:

- файловые (внедряются в исполняемые файлы и активизируются при их запуске);
- макровирусы (обычно заражают текстовые документы);
- загрузочные (записывают себя в загрузочный сектор диска);
- сетевые (распространяются по сетям, к ним относятся «вирусы-черви», «трояны», «Backdoor»).

- **По способу активации:**
  - нерезидентные вирусы (являются активными ограниченное время и активизируются, например, при запуске зараженных выполняемых программ или при обработке документов текстовым редактором);

- ***резидентный вирус*** (при заражении оставляет в оперативной памяти резидентную часть, которая затем перехватывает обращения операционной системы к объектам заражения: файлам, загрузочным секторам и т.д., и внедряется в них *(к ним относятся стелс-вирусы, название которых происходит от названия самолетов-невидимок STEALTH). Резидентные вирусы сохраняют свою активность вплоть до выключения или перезагрузки компьютера*).

«Троянские кони» (Trojan) – компьютерные программы, способные уничтожать информацию на дисках (разрушать загрузочный сектор и файловую систему дисков), собирать и передавать своим владельцам конфиденциальную информацию о пользователе и приводить к «зависанию» системы.

Backdoor» – компьютерные программы, цель которых – скрытное управление компьютером. Как правило, позволяют копировать файлы с пораженного компьютера и, наоборот, передавать на пораженный компьютер файлы и программы.

обычно Backdoor позволяет получить удаленный доступ к реестру, производить системные операции (например, перезагрузку компьютера). Особенность многих Backdoor-программ – то, что они позволяют использовать компьютер пользователя для сканирования сети, сетевых атак и взлома сетей. При этом попытки взлома ведутся с компьютера пользователя, ничего не подозревающего об этом.

- **Worm» (черви)** – компьютерные программы, которые размножаются, но не являются частью других файлов. Сетевые черви подразделяются на Интернет-червей (распространяются по Интернету), LAN-червей (распространяются по локальной сети). При размножении они копируют свой код в какие-либо каталоги дисков в надежде, что эти новые копии будут когда-либо запущены пользователем.
- Черви не только уменьшают количество свободной памяти на диске, но и уничтожают файлы.

Macro» (макровирусы) – компьютерные программы на макроязыках, встроенных в некоторые программы (текстовые редакторы, электронные таблицы, базы данных и т.д.). Большинство макровирусов – резидентные, они активны, пока запущен соответствующий редактор. Способны заражать файлы, делая, например, текстовые файлы нечитаемыми.

Классификация антивирусных программ

- **Доктора и вакцины** могут обнаруживать и «лечить» заражённые файлы, удаляя из файла тело вируса.
- **Сторожа** – небольшие резидентные программы, подающие сигнал тревоги, но лечить не способны.

- **Детекторы** производят поиск характерной для конкретного вируса последовательности байтов (сигнатуры вируса), поэтому могут находить только известные им вирусы. Многие детекторы имеют режимы лечения или уничтожения зараженных файлов.
- **Ревизоры** запоминают исходное состояние системных областей диска, каталогов и файлов и сразу после загрузки операционной системы производят сравнение (проверяется контрольная сумма файла

Характеристики антивирусных программ

- стабильность и надежность работы;
- размеры вирусной базы программы (количество вирусов, которые правильно определяются программой);
- возможность программы определять разнообразные типы вирусов, и умение работать с файлами различных типов (архивы, документы);
- наличие резидентного монитора, проверяющего все новые файлы;
- скорость работы программы;
- многоплатформенность (наличие версий программы под различные операционные системы).

- **Доктора (фаги) и вакцины** – Aidstest, Doctor Web, Norton AntiVirus.
- **Сторожа** небольшие резидентные программы, подающие сигнал тревоги, но обычно лечить не способны –
- (Symantec Norton AntiVirus Monitor,
- AntiViral Toolkit Pro Monitor)
- **Ревизоры** – ADinf.