Компьютерные вирусы и антивирусные программы

Компьютерный вирус

- это программа, которая может копировать себя в другие программы, чтобы продолжать размножение, выполняясь вместе с ними и, возможно, совершать некоторые побочные действия от безобидных шуток до действий, ведущих к потере информации и полной остановке работы компьютера.

- **Компьютерный вирус** – это целенаправленно созданная программа автоматически приписывающая себя к другим программным продуктам. изменяющая или уничтожающая их.
- **Компьютерным вирусом** называется программа, способная выполнить на компьютере несанкционированные действия
- **Компьютерный вирус** – это программный код, встроенный в программу или документ или в определенные области носителя данных и предназначенный для несанкционированных действий на компьютере.
- **Компьютерный вирус** – это программа способная создавать свои копии, внедрять их в различные обьекты или ресурсы компьютерных систем и сетей и производить определенные действия без ведома пользователя.

Т.о., вирус

1. Специально созданная программа
2. Самопроизвольно присоединяется к др.программам
3. Создает свои копии
4. Приводит к порче и потере информации

Свойства программ-вирусов

1) способность к саморазмножению;
2) скрытность;
3) способность нести деструктивные действия.

Компьютерные вирусы могут распространяться через

- Исполняемые файлы
- Документы Word, Excel
- Web-страницы
- Файлы Интернета
- Письма e-mail
- Внешние носители (flash-носители и др.)

Механизм воздействия вируса

- **При запуске инфицированной программы** или **при обращении к носителю**, имеющему **вредоносный вирусный код** в системной области. Происходит заражение.
- При каждой загрузке инфицированной программы в ОП происходит размножение.
- Последняя фаза развития вируса – активизация или вирусная атака.

Признаки появления вирусов

- неправильная работа нормально работавших программ;
- медленная работа компьютера;
- невозможность загрузки ОС;
- 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.

Авторами вирусов могут быть профессиональные программисты, студенты и даже дети школьного возраста.

Написать работающий вирус не составляет большого труда.

Сама угроза вирусов порождает многомиллиардный рынок соответствующих продуктов.

Сейчас ситуация с вирусами и антивирусами напоминает гонку вооружений недавних времен.

Почти каждый день появляются новые вирусы, а антивирусные компании выпускают дополнения к своим антивирусным базам данных.

Этому не видно конца, но пока никто не придумал ничего лучше, чем регулярное обновление антивирусного ПО.

Классификация вирусов

Вирус может внедрится в файлы трех типов:

1) командные файлы (файлы с расширением BAT);
2) загружаемые драйверы (файлы с расширением SYS или BIN);
3) выполняемые двоичные файлы (файлы с расширениями EXE, COM).

Классификаций компьютерных вирусов:

1. **По среде обитания** различают вирусы сетевые, файловые, загрузочные, файлово-загрузочные, драйверные.
2. **По способу заражения** выделяют резидентные и нерезидентные вирусы.
3. **По степени воздействия** вирусы бывают неопасные, опасные и очень опасные;
4. **По особенностям алгоритмов** вирусы делят на паразитические, репликаторы, невидимки, мутанты (призраки, полиморфные), троянские, макро-вирусы.

Классификация по среде обитания

группа вирусов	*характеристика вирусов*
Файловые	Внедряются в исполняемые файлы (программы) и активизируются при их запуске. Находятся в ОЗУ до выключения компьютера.
Загрузочные	Записывают себя в загрузочный сектор диска (в программу – загрузчик ОС). При загрузке ОС с зараженного диска внедряются в ОЗУ и ведут себя как файловые вирусы.
Драйверные	Заражают драйверы устройств компьютера или запускают себя путем включения в файл конфигурации дополнительной строки.
Сетевые	Заражают компьютер после открытия вложенного файла (вируса) в почтовое сообщение. Похищают пароли пользователей. Рассылают себя по электронным адресам.

Классификация по способу заражения

группа вирусов	*характеристика вирусов*
резидентные	записывают в оперативную память свою часть, которая потом перехватывает обращения ОС к любым объектам, активны до выключения или перезагрузки компьютера
нерезидентные	не заражают память компьютера, активны ограниченное время, активизируются в определенные моменты

Классификация по степени вредных воздействий

группа вирусов	*характеристика вирусов*
Безвредные	Уменьшают свободную память на диске за счет своего «размножения»
Неопасные	Уменьшают свободную память на диске. Вызывают появление графических, звуковых и др. внешних эффектов
Опасные	Могут привести к сбоям и зависаниям при работе компьютера
Очень опасные	Потеря программ и данных (изменение, удаление файлов и каталогов), форматирование винчестера и т.п.

Классификация по особенности алгоритма

группа вирусов	*характеристика вирусов*
компаньоны (спутники)	не изменяют файлы, а создают для исполняемых программ (.exe) одноименные командные программы (.com), которые при выполнении исходной программы запускаются первыми, а затем передают управление исходной программе
репликаторы (черви)	распространяются по компьютерным сетям, вычисляют адреса сетевых компьютеров и записывают по этим адресам свои копии, не изменяют файлы или сектора на дисках
паразиты	изменяют содержимое файлов и секторов диска, легко обнаруживаются и уничтожаются
троянские (квазивирусы)	маскируясь под полезную программу, разрушают загрузочный сектор и файловую систему дисков, передают конфиденциальную информацию, модифицируют программы систем защиты
невидимки (стелс)	перехватывают обращения операционной системы к пораженным файлам и подставляют вместо своего тела незараженные участки
мутанты (призраки)	не содержат одинаковых фрагментов .хранят свое тело в закодированном виде, постоянно меняя параметры этой кодировки
Макровирусы	Являются макрокомандами, которые заражают файлы документов Word, Excel. Находятся в ОЗУ до закрытия приложения.

Классификация по целостности

группа вирусов	*характеристика вирусов*
монолитные	внедряются в программы нераздельно
распределенные	части вредоносного кода внедряются в различные места кода программ

Вирусом могут быть заражены следующие объекты:

1. **Исполняемые файлы**, т.е. файлы с расширениями имен .com и .exe, Вирусы, заражающие файлы, называются **файловыми.** Вирус в зараженных исполняемых файлах начинает свою работу при запуске той программы, в которой он находится. Наиболее опасны те вирусы, которые после своего запуска остаются в памяти резидентно - они могут заражать файлы и выполнять вредоносные действия до следующей перезагрузки компьютера. А если они заразят любую программу из автозапуска компьютера, то и при перезагрузке с жесткого диска вирус снова начнет свою работу.

2. Загрузчик ОС и главная загрузочная запись ЖД. Вирусы, поражающие эти области, называются **загрузочными**. Такой вирус начинает свою работу при начальной загрузке компьютера и становится резидентным, т.е. постоянно находится в памяти компьютера. Механизм распространения загрузочных вирусов - заражение загрузочных записей вставляемых в компьютер внешних носителей информации.

3. **Файлы документов, информационные файлы баз данных, таблицы табличных процессоров** и другие аналогичные файлы могут быть заражены **макро-вирусами**. Макро-вирусы используют возможность вставки в формат многих документов макрокоманд.

Средства защиты от вирусов

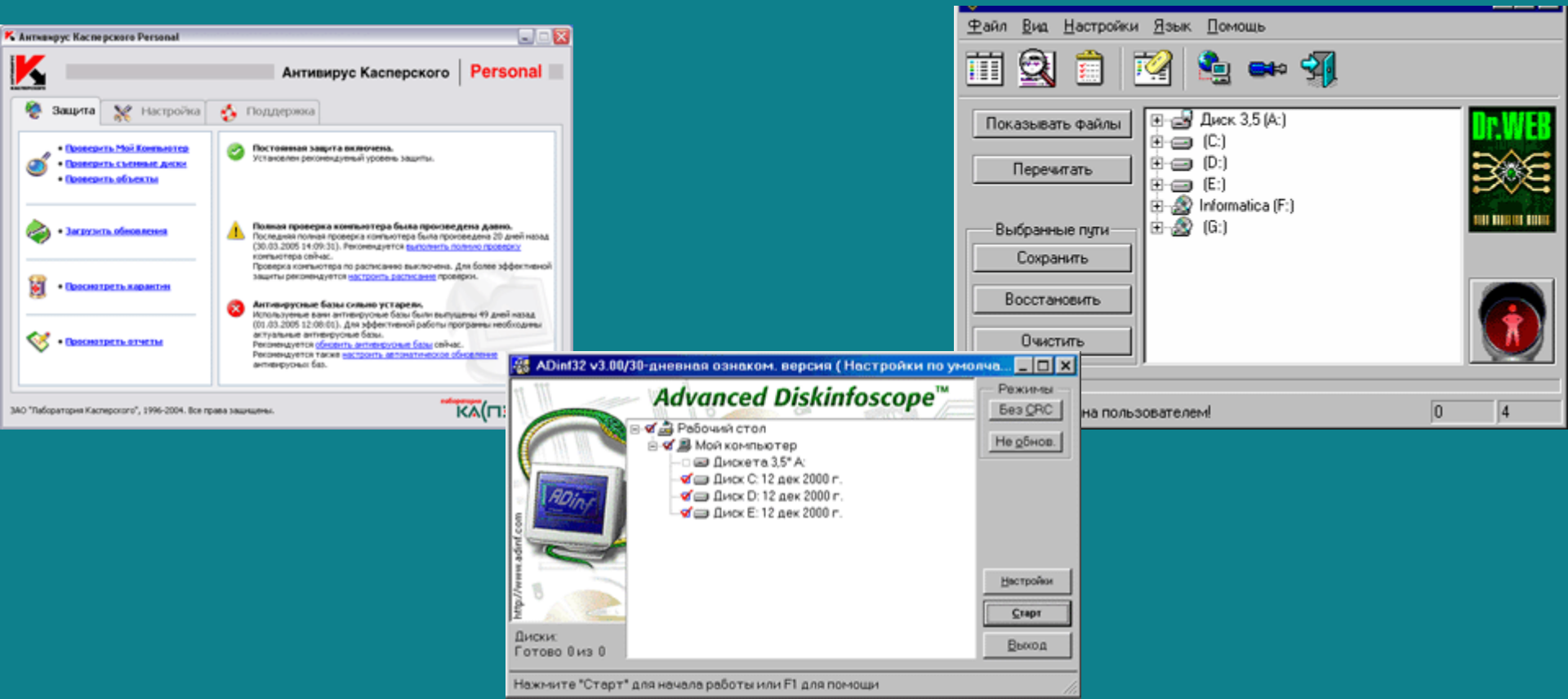
- **Для защиты** от вирусов можно использовать:
  - Общие средства защиты информации,;
  - профилактические меры, позволяющие уменьшить вероятность заражения вирусом;
  - специализированные программы для защиты от вирусов.

К общим средствам защиты информации относятся следующие методов защиты:

- - резервное копирование информации, т. е. создание копий файлов и системных областей дисков на дополнительном носителе;
- - разграничение доступа, предотвращающее несанкционированное использование информации, в частности, защиту от изменений программ и данных вирусами, неправильно работающими программами и ошибочными действиями пользователей.

Антивирусные программы

Антивирусные программы включают антивирусные базы, содержащие средства против самых опасных вирусов.



Специализированные программы

1.Программы-**детекторы** (**AVP, Aidstest и Doctor Web)** позволяют обнаруживать файлы, зараженные одним из нескольких известных вирусов.

2.Программы-**доктора**, или **фаги**, восстанавливают зараженные программы убирая из них тело вируса, т.е. программа возвращается в то состояние, в котором она находилась до заражения вирусом.

3.Программы-**ревизоры** (***MicrosoftAnti-Virus, Adinf)*** сначала запоминают сведения о состоянии программ и системных областей дисков, а затем сравнивают их состояние с исходным. При выявлении несоответствий об этом сообщается пользователю.

4. **Доктора-ревизоры** - это гибриды ревизоров и докторов, т.е. программы, которые не только обнаруживают изменения в файлах и системных областях дисков, но и могут автоматически вернуть их в исходное состояние.
5. **Программы-фильтры (Vsafe, Avast)** располагаются резидентно в оперативной памяти компьютера, перехватывают те обращения к операционной системе, которые используются вирусами для размножения и нанесения вреда, и сообщают о них пользователю. Пользователь может разрешить или запретить выполнение соответствующей операции.

- **Средствами разведки** в защите от вирусов являются ***программы-детекторы***, позволяющие проверять вновь полученное программное обеспечение на наличие вирусов.

- **На первом уровне защиты** находятся резидентные программы для защиты от вируса. Эти программы могут первыми сообщить о вирусной атаке и предотвратить заражение программ и диска.

- **Второй уровень защиты** составляют программы-ревизоры, программы-доктора и доктора-ревизоры.
- Ревизоры обнаруживают нападение тогда, когда вирус сумел пройти сквозь первый уровень.
- Программы-доктора применяются для восстановления зараженных программ, если ее копий нет в архиве, но они не всегда лечат правильно.
- Доктора-ревизоры обнаруживают нападение вируса и лечат зараженные файлы, причем контролируют правильность лечения.

- **Третий уровень защиты** - это средства разграничения доступа. Они не позволяют вирусам и неверно работающим программам, даже если они проникли в компьютер, испортить важные данные.

В **резерве** находятся архивные копии информации и эталонные диски с программными продуктами. Они позволяют восстановить информацию при ее повреждении на жестком диске.

Вопросы для самоконтроля

1. Что такое компьютерные вирусы, в чем состоят их вредные действия?
2. Какие существуют средства борьбы с компьютерными вирусами?