**Защита информации, антивирусная защита**

**Объяснение нового материала**

### Несколько десятилетий назад компьютерные вирусы были, скорее, городской легендой, нежели реальной угрозой, однако спустя годы ситуация кардинально изменилась. В настоящее время вредоносные программы (в народе именуемые вирусами) представляют большую угрозу для всех и вся — от правительств и крупных международных корпораций до малого бизнеса и Интернет-пользователей.

Созданные разными людьми, от опытных хакеров до любителей и даже детей, компьютерные вирусы являются вредоносными программами, которые — при выполнении — создают копии самих себя, внедряясь в код других компьютерных программ, в файлы данных или в загрузочный сектор жёсткого диска.

Вирусы часто выполняют некоторые виды вредоносной деятельности на заражённых хостах: «съедают» место на жёстком диске, потребляют другие ресурсы системы, получают доступ к конфиденциальной информации, повреждают структуры размещения данных, отображают политические или юмористические сообщения на экране пользователя, спамят, устанавливают свои кейлоггеры (программы, регистрирующие нажатия клавиш на клавиатуре) и многое другое.

Количество людей, пользующихся компьютером и сотовым телефоном, имеющим выход в Интернет, постоянно растет. Зна­чит, возрастает возможность обмена данными между ними по элект­ронной почте и через Всемирную сеть. Это приводит к росту угро­зы заражения компьютера вирусами, а также порчи или хищения информации чужими вредоносными программами, ведь основ­ными источниками распространения вредоносных программ яв­ляются электронная почта и Интернет. Правда, заражение может также произойти через дискету или CD-диск.

**Компьютерный вирус -** программа способная самопроизвольно  внедряться и внедрять свои копии в другие программы, файлы, системные области компьютера и в вычислительные сети, с целью создания всевозможных помех работе на компьютере  
**Признаки заражения**

* прекращение работы или неправильная работа ранее функционировавших программ
* медленная работа компьютера
* невозможность загрузки ОС
* исчезновение файлов и каталогов или искажение их содержимого
* изменение размеров файлов и их времени модификации
* уменьшение размера оперативной памяти
* непредусмотренные сообщения, изображения и звуковые сигналы
* частые сбои и зависания компьютера и др.

**Классификация** **компьютерных вирусов**

* по среде обитания
* по способу заражения
* по воздействию
* по особенностям алгоритма

**По среде обитания**

* **Сетевые** – распространяются по различным компьютерным сетям
* **Файловые** – внедряются в исполняемые модули (COM, EXE)
* **Загрузочные** – внедряются в загрузочные сектора диска или сектора, содержащие программу загрузки диска
* **Фалово-загрузочные** – внедряются и в загрузочные сектора и в исполняемые модули

**По способу заражения**

* **Резидентные** – при заражении оставляет в оперативной памяти компьютера свою резидентную часть, которая потом перехватывает обращения ОС к объектам заражения
* **Нерезидентные** – не заражают оперативную память и активны ограниченное время

**По воздействию**

* **Неопасные** – не мешают работе компьютера, но уменьшают объем свободной оперативной памяти и памяти на дисках
* **Опасные** – приводят к различным нарушениям в работе компьютера
* **Очень опасные** – могут приводить к потере программ, данных, стиранию информации в системных областях дисков

**По особенностям алгоритма**

* **Паразиты** – изменяют содержимое файлов и секторов, легко обнаруживаются
* **Черви** – вычисляют адреса сетевых компьютеров и отправляют по ним свои копии
* **Стелсы** – перехватывают обращение ОС к пораженным файлам и секторам и подставляют вместо них чистые области
* **Мутанты** – содержат алгоритм шифровки-дешифровки, ни одна из копий не похожа на другую
* **Трояны** – не способны к самораспространению, но маскируясь под полезную, разрушают загрузочный сектор и файловую систему

**Основные меры по защите от вирусов**

* оснастите свой компьютер одной из современных антивирусных программ: Doctor Weber, Norton Antivirus, AVG/
* постоянно обновляйте антивирусные базы
* делайте архивные копии ценной для Вас информации (флэш накопители, CD)

**Классификация антивирусного программного обеспечения**

* Сканеры (детекторы)
* Мониторы
* Ревизоры

**Сканеры**

*Принцип работы антивирусных сканеров основан на проверке файлов, секторов и системной памяти и поиске в них известных и новых (неизвестных сканеру) вирусов.*

**Примеры программ-сканеров**

* ***Aidstest Дмитрия Лозинского*** умеет обнаруживать около 2000 вирусов
* ***Сканер антивирусного пакета Евгения Касперского AntiviralToolkitPro*** распознает по сигнатурам более 10.000 вирусов
* ***База сигнатур антивирусного сканера NortonAntiViru s***распознаетболее 8.000 вирусов

**Мониторы**

*Это целый класс антивирусов, которые постоянно находятся в оперативной памяти компьютера и отслеживают все подозрительные действия, выполняемые другими программами.*  
*С помощью монитора можно остановить распостранение вируса на самой ранней стадии.*

**Примеры программ-мониторов**

* Вместе с антивирусным пакетом ***AntiviralToolkidPro (AVP),*** созданным фирмой Е. Касперского поставляется резидентрый монитор ***Antiviral*** ***Monitor***. Он позволяет обнаружить и сообщить обо всех проявлениях, которые могут быть вызваны компьютерными вирусами.
* В комплект ***McAfee*** ***Virus*** ***Scan*** входит резидентный монитор, позволяющий постоянно контролировать работу компьютера.
* В состав комплекта ***Norton*** ***AntiVirus*** входит приложение ***Norton*** ***AntiVirus*** ***Auto***-***Protect***. Кроме проверки запускаемых файлов ***Norton*** ***AntiVirus*** ***Auto***-***Protect*** выполняет все функции обычного резидентного монитора, позволяя при этом пользователям сделать установки случаев, в которых необходимо сообщать о подозрительном действии.
* В комплекте антивируса ***DrWeb*** входит монитор ***SpIDer*** ***Guard***, который перехватывает обращения к файлам и системным областям дисков, осуществляя проверку на наличие в них компьютерных вирусов «на лету».

**Ревизоры**

*Программы-ревизоры первоначально запоминают в специальных файлах образы главной загрузочной записи, загрузочных секторов логических дисков, информацию о структуре каталогов, иногда - объем установленной оперативной памяти.*  
*Для определения наличия вируса в системе программы-ревизоры проверяют созданные ими образы и производят сравнение с текущим состоянием.*

**Примеры программ-ревизоров**

* Простейшая программа-ревизор ***MicrosoftAnti-Virus*** входит в состав операционной системы MS-DOS.
* Более известна программа-ревизор ***Adinf***, созданная Дмитрием Юрьевичем Мостовым.

Нет необходимости говорить, что вредоносное ПО — это сильный раздражитель, который, к тому же, может привести к весьма печальным последствиям.

**Задания:**

1. **Сделать краткий конспект в тетради по плану:**

* Компьютерный вирус
* Признаки заражения
* Классификация компьютерных вирусов
* Основные меры по защите от вирусов
* Классификация антивирусного программного обеспечения

1. **Ответить на вопросы теста «Вирусы и антивирусные программы»,**

**форма ответа: номер вопроса – цифра**

1. Что такое компьютерный вирус?

1. Прикладная программа
2. Системная программа
3. Программа, выполняющая на компьютере несанкционированные действия
4. База данных.

2. Компьютерным вирусом является

1. Программа проверки и лечения дисков
2. Любая программа, созданная на языках низкого уровня
3. Программа, скопированная с плохо отформатированной дискеты
4. Специальная программа небольшого размера, которая может приписывать себя к другим программам, она обладает способностью " размножаться "

3. Заражение компьютерными вирусами может произойти в процессе ...

1. Работы с файлами
2. Форматирования дискеты
3. Выключения компьютера
4. Печати на принтере

4. Основные типы компьютерных вирусов:

1. Аппаратные, программные, загрузочные
2. Программные, загрузочные, макровирусы
3. Файловые, программные, макровирусы

5. Что называется вирусной атакой?

1. Неоднократное копирование кода вируса в код программы
2. Отключение компьютера в результате попадания вируса
3. Нарушение работы программы, уничтожение данных, форматирование жесткого диска

6. Какие существуют методы реализации антивирусной защиты?

1. Аппаратные и программные
2. Программные, аппаратные и организационные
3. Только программные

7. Какие существуют основные средства защиты?

1. Резервное копирование наиболее ценных данных
2. Аппаратные средства
3. Программные средства

8. Какие существуют вспомогательные средства защиты?

1. Аппаратные средства
2. Программные средства
3. Аппаратные средства и антивирусные программы

9. На чем основано действие антивирусной программы?

1. На ожидании начала вирусной атаки
2. На сравнении программных кодов с известными вирусами
3. На удалении зараженных файлов

10. Какие программы относятся к антивирусным

1. AVG, DrWeb, Norton AntiVirus
2. MS-DOS, MS Word, AVP
3. MS Word, MS Excel, Norton Commander