Практическая работа

Тема: Использование технических программных средств защиты информации при работе с компьютерными системами в соответствии с приёмами антивирусной защиты.

Цель работы: изучение вредоносных программ и антивирусного программного обеспечения.

Краткие сведения

Информационная безопасность.

Информационная безопасность государства – состояние сохранности информационных ресурсов государства и защищённости законных прав личности и общества в информационной сфере.

Информационная безопасность - это процесс обеспечения конфиденциальности, целостности и доступности информации.

- Конфиденциальность: Обеспечение доступа к информации только– авторизованным пользователям.
- Целостность: Обеспечение достоверности и полноты информации и– методов ее обработки.
- Доступность: Обеспечение доступа к информации и связанным с ней– активам авторизованных пользователей по мере необходимости.

Информационная безопасность – все аспекты, связанные с определением, достижением и поддержанием конфиденциальности, целостности, доступности, неотказуемости, подотчётности, аутентичности и достоверности информации или средств её обработки.

Безопасность информации (данных) – состояние защищённости информации (данных), при котором обеспечиваются её (их) конфиденциальность, доступность и целостность.

Безопасность информации (данных) определяется отсутствием недопустимого риска, связанного с утечкой информации по техническим каналам, несанкционированными и непреднамеренными воздействиями на данные и (или) на другие ресурсы автоматизированной информационной системы, используемые в автоматизированной системе.

Вирусы. Антивирусное программное обеспечение

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:

- *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
- *Файлово-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 Web, Norton Antivirus, AVP
- постоянно обновляйте антивирусные базы
- делайте архивные копии ценной для Вас информации (гибкие диски, CD)

Классификация антивирусного программного обеспечения

- *Сканеры (детекторы).* Принцип работы антивирусных сканеров основан на проверке файлов, секторов и системной памяти и поиске в них известных и новых (неизвестных сканеру) 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 распространение вируса на самой ранней стадии.
- *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. 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.

Содержание работы:

Задание №1. Заполнить таблицу, описать 3 антивирусных программы.

Наименование антивирусной программы	Характеристики	Условия использования (платно/бесплатно)

Задание №2. Выполнить тест по теме «Защита информации, антивирусная защита».

1. Информационная безопасность – это …

1) отсутствие зараженных файлов на компьютере
2) процесс работы антивирусных программ
3) процесс обеспечения конфиденциальности, целостности и доступности информации
4) состояние защищённости информации, при котором обеспечиваются её (их) конфиденциальность, доступность и целостность.

2. Основные угрозы доступности информации:

1) непреднамеренные ошибки пользователей
2) злонамеренное изменение данных
3) перехват данных
4) хакерская атака.

3. Один из методов защиты информации на компьютере:

1) полное отключение системного блока
2) отключение жесткого диска
3) защита паролем
4) копирование информации.

4. К биометрической системе защиты относятся:

1) антивирусная защита
2) защита паролем
3) идентификация по отпечаткам пальцев
4) физическая защита данных.

5. Что такое "компьютерный вирус"?

1) самостоятельная компьютерная программа или компонент программного комплекса, предназначенная для создания и изменения текстовых файлов.
2) это совокупность программ, находящиеся на устройствах долговременной памяти;
3) это программы, которые могут "размножаться" и скрытно внедрять свои копии в файлы, загрузочные секторы дисков и документы;
4) это сведения об объектах и явлениях окружающей среды, их параметрах, свойствах и состоянии.

6. Свойство вируса, позволяющее называться ему загрузочным – способность …

1)заражать загрузочные сектора жестких дисков
2)заражать загрузочные дискеты и компакт-диски
3) вызывать перезагрузку компьютера-жертвы
4) подсвечивать кнопку Пуск на системном блоке.

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

1) работы с файлами
2) форматирования дискеты
3) выключения компьютера
4) печати на принтере

8. Неопасные компьютерные вирусы могут привести:

1) к сбоям и зависаниям при работе компьютера;
2) к потере программ и данных;
3) к форматированию винчестера;
4) к уменьшению свободной памяти компьютера.

9. Опасные компьютерные вирусы могут привести…

1) к сбоям и зависаниям при работе компьютера;
2) к потере программ и данных;

3) к форматированию винчестера;
4) к уменьшению свободной памяти компьютера.

10. Какой вид компьютерных вирусов внедряются и поражают исполнительный файлы с расширением *.exe, *.com и активируются при их запуске?

1) файловые вирусы;
2) загрузочные вирусы;
3) макро-вирусы;
4) сетевые вирусы.

11. Какой вид компьютерных вирусов внедряются и поражают файлы с расширением *.txt, *.doc?

1) файловые вирусы;
2) загрузочные вирусы;
3) макро-вирусы;
4) сетевые вирусы.

12. Сетевые черви это:

1) Вирусы, которые внедряются в документ под видом макросов
2) Вирусы, которые проникну на компьютер, блокируют работу сети
3) Вредоносные программы, которые проникают на компьютер, используя сервисы компьютерных сетей
4) Вредоносные программы, устанавливающие скрытно от пользователя другие программы.

13. Антивирусные программы - это программы для:

1) Обнаружения вирусов
2) Удаления вирусов
3) Размножения вирусов

14. 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.

15. Какие программы относятся к антивирусным?

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

16. Можно ли обновить антивирусные базы на компьютере, не подключенном к Интернет?

1) да, позвонив в службу технической поддержки компании-производителя антивирусной программы. Специалисты этой службы продиктуют последние базы, которые нужно сохранить на компьютере воспользовавшись любым текстовым редактором
2) да, это можно сделать с помощью мобильных носителей скопировав антивирусные базы с другого компьютера, на котором настроен выход в Интернет и установлена эта же антивирусная программа или на нем нужно вручную скопировать базы с сайта компании-производителя антивирусной программы
3) нет.

17. Основные меры по защите информации от повреждения вирусами:

1) проверка дисков на вирус
2) создавать архивные копии ценной информации
3) не пользоваться "пиратскими" сборниками программного обеспечения
4) передавать файлы только по сети.

18. Создание компьютерных вирусов является

1) последствием сбоев операционной системы
2) необходимым компонентом подготовки программистов
3) побочным эффектом при разработке программного обеспечения
4) преступлением.

Контрольные вопросы

1. Дайте понятие компьютерного вируса.
2. Какие угрозы информации способны нанести вредоносные программы?
3. Для чего предназначены антивирусные программы?
4. В чем разница между антивирусными сканерами и мониторами?
5. Какие существуют признаки заражения компьютерным вирусом?
6. Что необходимо сделать в первую очередь в случае заражения компьютерным вирусом?
7. Какие существуют типы компьютерных вирусов?
8. Как сетевые черви проникают на компьютер?
9. Какие вредоносные действия выполняют троянские программы?
10. Приведите классификацию антивирусных программ.