

## Практическое занятие 16.

### **Профилактические и антивирусные мероприятия для компьютерного рабочего места в соответствии с его комплектацией для профессиональной деятельности.**

по учебной дисциплине «Информатика и ИКТ»

**Тема:** *Защита информации, антивирусная защита*

**Цель:**

- выработать практические навыки работы с антивирусными программами, навыки правильной работы с компьютером. *изучить*

**Норма времени:** 2 часа

**Оснащение рабочего места:** ПК, ОС Windows, рабочая тетрадь.

**Техника безопасности:** Правила ТБ при работе в компьютерном классе.

**Методические рекомендации:**

### **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.

## **Задание 1. Тест (30 баллов).**

### **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. Брандмауэр (firewall) – это программа, ...**

- 1) которая следит за сетевыми соединениями и принимает решение о разрешении или запрещении новых соединений на основании заданного набора правил
- 2) которая следит за сетевыми соединениями, регистрирует и записывает в отдельный файл подробную статистику сетевой активности
- 3) на основе которой строится система кэширования загружаемых веб-страниц
- 4) реализующая простейший антивирус для скриптов и прочих использующихся в Интернет активных элементов.

**6. Положительные моменты в использовании для выхода в Интернет браузера, отличного от Microsoft Internet Explorer, но аналогичного по функциональности**

- 1) уменьшение вероятности заражения, поскольку использование иного браузера может косвенно свидетельствовать об отсутствии у пользователя достаточных средств для покупки Microsoft Internet Explorer
- 2) уменьшение вероятности заражения, поскольку большинство вредоносных программ пишутся в расчете на самый популярный браузер, коим является Microsoft Internet Explorer
- 3) возможность установить отличную от `www.msn.com` стартовую страницу  
возможность одновременно работать в нескольких окнах.

**7. 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.

**8. Назовите основные типы компьютерных вирусов:**

- 1) почтовые, файловые, программные
- 2) аппаратные, программные, загрузочные
- 3) программные, макровирусы, загрузочные.

**9. 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.

**10. Программа, осуществляющая несанкционированные действия по сбору, и передаче информации злоумышленнику, а также ее разрушение или злонамеренную модификацию это:**

- 1) Макровирус
- 2) Сетевой червь
- 3) Троян

4) Загрузочный вирус

**11. Заражение компьютерными вирусами может произойти в процессе ...**

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

**12. Какие файлы заражают макро-вирусы?**

- 1) исполнительные;
- 2) файлы документов Word и элект. таблиц Excel;
- 3) графические и звуковые;
- 4) html документы.

**13. К каким вирусам относится "троянский конь"?**

- 1) макро-вирусы
- 2) скрипт-вирусы
- 3) интернет-черви
- 4) загрузочные вирусы.

**14. 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.

**15. 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.

**16. 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.

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

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

**18. Как происходит заражение почтовыми вирусами?**

- 1) При подключении к web-серверу, зараженному "почтовым" вирусом
- 2) При открытии зараженного файла, присланного с письмом по e-mail
- 3) При подключении к почтовому серверу
- 4) При получении с письма, присланном по e-mail, зараженного файла.

**19. 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.

**20. Руткит – это:**

- 1) Программа для скрытого взятия под контроль взломанной системы
- 2) Вредоносная программа, маскирующаяся под макрокоманду
- 3) Разновидность межсетевого экрана
- 4) Программа, выполняющая несанкционированные действия по передаче управления компьютером удаленному пользователю.

**21. Какие существуют вспомогательные средства защиты?**

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

**22. Антивирусные программы - это программы для:**

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

**23. 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.

**24. Какие программы относятся к антивирусным?**

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

**25. Какие программы не относятся к антивирусным?**

- 1) программы-фаги
- 2) программы сканирования
- 3) программы-ревизоры
- 4) программы-детекторы

**26. 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.

**27. 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.

**28. Наиболее эффективное средство для защиты от сетевых атак**

- 1) использование антивирусных программ
- 2) использование сетевых экранов или «firewall»
- 3) посещение только «надёжных» Интернет-узлов



4) использование только сертифицированных программ-браузеров при доступе к сети Интернет.

### 29. Основная функция межсетевого экрана

- 1) управление удаленным пользователем
- 2) фильтрация входящего и исходящего трафика
- 3) проверка дисков на вирусы
- 4) программа для просмотра файлов.

### 30. Создание компьютерных вирусов является

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

*Задание 2. Заполнить таблицу (10 баллов).*

**Описать 5 антивирусных программ.**

<b>Наименование антивирусной программы</b>	<b>Характеристики</b>	<b>Условия использования (платно/бесплатно)</b>
...	...	...

*Задание 3. Сделайте вывод по проделанной работе (2 балла).*

### **Критерии оценивания практического задания**

<b>Количество набранных баллов</b>	<b>Оценка</b>
<b>38 - 42</b>	<b>5 (отлично)</b>
<b>35 – 37</b>	<b>4 (хорошо)</b>
<b>29 - 34</b>	<b>3 (удовлетворительно)</b>
<b>менее 28</b>	<b>2 (неудовлетворительно)</b>