ОУД.09 Информатика

Преподаватели: Уханова Е.А., Жданова А.А.

Выполненные задания присылать на почту до 30.04.2020: uhelena@mail.ru; zdanova.anna86@mail.ru

Задание на дистанционное обучение.

ДО -161

Практическая работа № 14-15 (2 часа)

«Администрирование локальной компьютерной сети»

«Сервер. Сетевые операционные системы»

«Понятие о системном администрировании»

«Разграничение прав доступа в сети»

«Подключение компьютера к сети»

«Программное и аппаратное обеспечение компьютерных сетей»

Тема: Средства информационных и коммуникационных технологий
Цели занятия: изучить процесс регистрации (открытия почтового ящика), подготовки, отправки и приема писем на почтовом сайте.
Оборудование, программное обеспечение: ПК, ОС Windows, браузер InternetExplorer

Методические рекомендации

1. **Теоретические сведения законспектировать в тетрадь.**

Глобальная сеть – это объединения компьютеров, расположенных на удаленном расстоянии, для общего использования мировых информационных ресурсов. На сегодняшний день их насчитывается в мире более 200. Из них наиболее известной и самой популярной является сеть Интернет.

В отличие от локальных сетей в глобальных сетях нет какого-либо единого центра управления. Основу сети составляют десятки и сотни тысяч компьютеров, соединенных теми или иными каналами связи. Каждый компьютер имеет уникальный идентификатор, что позволяет "проложить к нему маршрут" для доставки информации. Обычно в глобальной сети объединяются компьютеры, работающие по разным правилам (имеющие различную архитектуру, системное программное обеспечение и т.д.). Поэтому для передачи информации из одного вида сетей в другой используются шлюзы.

Шлюзы (gateway)– это устройства (компьютеры), служащие для объединения сетей с совершенно различными протоколами обмена.

Протокол обмена – это набор правил (соглашение, стандарт), определяющий принципы обмена данными между различными компьютерами в сети.

Протоколы условно делятся на базовые (более низкого уровня), отвечающие за передачу информации любого типа, и прикладные (более высокого уровня), отвечающие за функционирование специализированных служб.

Главный компьютер сети, который предоставляет доступ к общей базе данных, обеспечивает совместное использование устройств ввода-вывода и взаимодействия пользователей называется **сервером.**

Компьютер сети, который только использует сетевые ресурсы, но сам свои ресурсы в сеть не отдает, называется **клиентом** (часто его еще называют рабочей станцией).

Для работы в глобальной сети пользователю необходимо иметь соответствующее аппаратное и программное обеспечение.

Программное обеспечение можно разделить на два класса:

- программы-серверы, которые размещаются на узле сети, обслуживающем компьютер пользователя;
- программы-клиенты, размещенные на компьютере пользователя и пользующиеся услугами сервера.

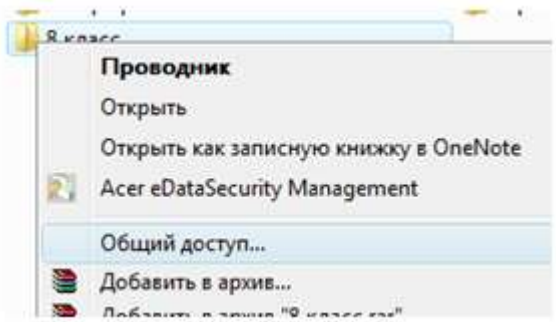
Глобальные сети предоставляют пользователям разнообразные услуги: электронная почта, удаленный доступ к любому компьютеру сети, поиск данных и программ и так далее.

Содержание работы:

Задание №1. Определите общий ресурс компьютера. Для этого:

- В операционной системе Windows найти на рабочем столе значок Сеть.
- Открыть папку, где будут видны все компьютеры, которые подключены в одну сеть. В данном окне появятся все компьютеры, которые подключены к сети.
- Открыть один из них. Посмотреть ресурсы компьютера, которыми можно воспользоваться. Такие ресурсы называются общими.

Задание № 2. Предоставьте доступ для пользователей локальной сети к папке на своем компьютере, подключенном к локальной сети. Для этого:



1. В операционной системе Windows открыть окно папки Компьютер и на одном из дисков C: или D: создать свою папку. Назвать ее номером своей группы.
2. Щелкнуть правой кнопкой мыши по значку папки и в контекстном меню папки выберите команду Общий доступ.
3. В появившемся диалоговом окне Дополнительный общий доступ установить флажок Открыть общий доступ к этой папке.
4. Если все правильно сделано, то на диске (у вашей папки) появится значок, который показывает, что папка является общей.

Задание №3. Проверьте возможности доступа к ресурсам компьютеров, подключенных к локальной сети. Для этого:

- Щелкнуть по значку Сеть, в окне появится список компьютеров, подключенных к локальной сети (смотри задание 1.)
- Открыть свой компьютер и внимательно посмотреть: какие из ресурсов доступны пользователям. Если название Вашей папки есть в перечне, то все сделано правильно.
-

Задание №4. Максимальная скорость передачи данных в локальной сети 100 Мбит/с. Сколько страниц текста можно передать за 1 сек, если 1 страница текста содержит 50 строк и на каждой строке - 70 символов?

Задание №5. Ответьте на вопросы:

– Указать основное назначение компьютерной сети.	
– Указать основную характеристику каналов связи.	
– Указать объект, который является абонентом сети.	

Сделайте вывод о проделанной работе

Практическая работа № 16-17-18 (2 часа + 4 часа)

«Защита информации, антивирусная защита»

Тема: Средства информационных и коммуникационных технологий.

Цельработы: выработать практические навыки работы с антивирусными программами, навыки правильной работы с компьютером.

Оснащение рабочего места: ПК,ОСWindows,рабочая тетрадь.

Техника безопасности: Правила ТБ при работе в компьютерном классе.

Методические рекомендации законспектировать в тетрадь:

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 ивнедрять 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 исполняемыемодули

По способу заражения:

- *Резидентные* –при заражении оставляет в оперативной памяти компьютерасвою 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 свободнойоперативной 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,легкообнаруживаются
- *Черви* –вычисляют адреса сетевых компьютеров и отправляют по ним своикопии
- *Стелсы* –перехватывают обращение ОС к пораженным файлам и секторам иподставляют вместо них чистые области
- *Мутанты* –содержат алгоритм шифровки-дешифровки,ни одна из копий непохожа 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 распостранение 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). Решить тест, сформулировать выводы и переслать на электронную почту

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) тключение жесткого диска
2) защита паролем
3) 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 состояни

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
преступлением