ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА

Федеральное государственное бюджетное образовательное учреждение высшего образования
**«Петербургский государственный университет путей сообщения Императора Александра I»**
**(ФГБОУ ВО ПГУПС)**

**Петрозаводский филиал ПГУПС**

ОДОБРЕНО
на заседании цикловой комиссии
протокол № 10 от 20.06. 2017
Председатель цикловой комиссии:
_____(_____)

УТВЕРЖДАЮ
Начальник УМО
_____ А.В. Калько
«23» 06 2017г.

# МЕТОДИЧЕСКИЕ УКАЗАНИЯ
## по организации и проведению практических занятий/лабораторных работ

По дисциплине/МДК/ПМ: МДК.01.01 Организация, принципы построения и функционирования компьютерных сетей

Специальность: 09.02.02 Компьютерные сети

Выполнил (а): Фунев А.Г. – инженер по ремонту и обслуживанию средств ВТ.

2017г.

# ВВЕДЕНИЕ

Методические указания по выполнению практических и лабораторных работ по МДК.01.01. Организация, принципы построения и функционирования компьютерных сетей ПМ.01. Участие в проектировании сетевой инфраструктуры разработаны для студентов 3 курса специальности 09.02.02 Компьютерные сети в соответствии с требованиями Федерального государственного образовательного стандарта среднего профессионального образования к минимуму содержания и уровню подготовки выпускников данной специальности укрупнённой группы 09.02.02 Информатика и вычислительная техника.

Данное пособие содержит теоретические основы, описание хода работы, алгоритмы действий в процессе выполнения, решения задач, а также контрольные вопросы и задания по проверке освоения материала.

В пособие даны руководства по следующим темам:

- Обжим витой пары. Создание прямого и кроссового кабеля по стандартам EIA/TIA-568A и EIA/TIA-568B. Тестирование.
- Разводка сетевой розетки RJ-45 , коммутационной панели. Тестирование.- Идентификация повреждений кабельной системы
- Установка и настройка сетевой операционной системы семейства Windows.
- Расчёт адресного пространства
- Оформление проектной документации. - Создание рабочих чертежей: план здания, структурированной кабельной системы, телекоммуникационного шкафа
- Создание монтажной схемы разделки коммутационной панели
- Использование сетевых диагностических утилит: ping, nslookup, tracert
- Мониторинг состояния элементов сети
- Механизмы резервного копирования данных в операционной системе Windows 2003 Server.
- Установка антивирусного программного обеспечения.

Перечень лабораторных и практических работ соответствует профессиональным компетенциям, перечисленным в ФГОС по специальности среднего профессионального образования 09.02.02 Компьютерные сети (базовая подготовка), соответствует уровню требований к знаниям и умениям студентов, требованиям к эксплуатации компьютерных сетей, обеспечения мер охраны труда при эксплуатации сетей, при их техническом обслуживании и ремонте.

# ПЕРЕЧЕНЬ ПРАКТИЧЕСКИХ И ЛАБОРАТОРНЫХ РАБОТ

# ПО МДК01.01. ОРГАНИЗАЦИЯ, ПРИНЦИПЫ ПОСТРОЕНИЯ И ФУНКЦИОНИРОВАНИЯ КОМПЬЮТЕРНЫХ СЕТЕЙ

## Лабораторные работы

1. Обжим витой пары. Создание прямого и кроссового кабеля по стандартам EIA/TIA-568A и EIA/TIA-568B. Тестирование.
2. Разводка сетевой розетки RJ-45 , коммутационной панели. Тестирование.
3. Идентификация повреждений кабельной системы

## Практические работы

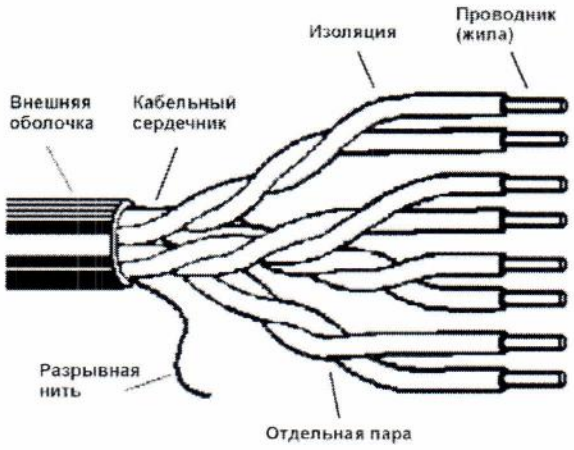
1. Установка и настройка сетевой операционной системы семейства Windows
2. Расчёт адресного пространства
3. Оформление проектной документации
4. Создание рабочих чертежей: план здания, структурированной кабельной системы, телекоммуникационного шкафа
5. Создание монтажной схемы разделки коммутационной панели
6. Использование сетевых диагностических утилит: ping, nslookup, tracert
7. Мониторинг состояния элементов сети
8. Механизмы резервного копирования данных в операционной системе Windows 2003 Server.
9. Установка антивирусного программного обеспечения.

## Лабораторная работа №1
## по теме «Обжим витой пары. Создание прямого и кроссового кабеля по стандартам EIA/TIA-568A и EIA/TIA-568B. Тестирование»

**Цель:** научиться обжимать неэкранированную витую пару категории 5е, создавать прямой и кроссовый кабель по различным стандартам.

### Конструкция кабеля связи

**Витая пара**" (twisted pair) - это кабель на медной основе, объединяющий в оболочке одну или более пар проводников. Каждая пара представляет собой два перевитых вокруг друг друга изолированных медных провода.



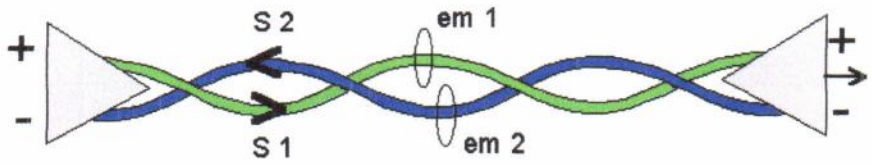

Кабели данного типа зачастую сильно отличаются по качеству и возможностям передачи информации. Соответствия характеристик кабелей определенному классу или категории определяют общепризнанные стандарты (ISO 11801 и TIA-568). Сами характеристики напрямую зависят от структуры кабеля и применяемых в нём материалов, которые и определяют физические процессы, проходящие в кабеле при передачи сигнала.

### Характеристики кабеля связи «витая пара», 5 категории

#### 1. Сбалансированность пары.

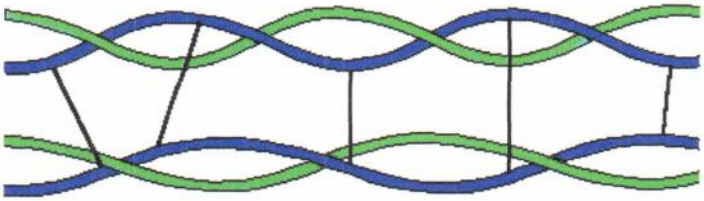
Сбалансированность пары является фактически определяющей характеристикой качества кабеля, поскольку влияет на большинство других его свойств. Дело в том, что электромагнитное (Electro Magnetic - EM) поле наводит электрический ток в проводниках и образуется вокруг проводника при протекании по нему электрического тока.

Взаимодействие между EM-полями и токонесущими проводниками может оказывать отрицательное воздействие на качество передачи сигнала. В обоих же проводниках сбалансированной пары электромагнитные помехи (em1 и em2) наводят одинаковые по амплитуде сигналы, (S1 и S2) находящихся в противофазе. За счет этого суммарное излучение "идеальной пары" стремится к нулю.




**S1 = S2 \ em1 = em2**

Если в кабеле присутствует более одной пары, то для исключения взаимных наводок пар, которые могли бы нарушить электромагнитный баланс, пары скручивают с различным шагом.



## 2. Характеристический импеданс.

Как всякий проводник, "Витая пара" имеет сопротивление переменному электрическому току. Однако это сопротивление может быть различным для различных частот. "Витая пара" имеет импеданс обычно 100 или 120 Ом (для кабеля категории 5 импеданс измеряется в диапазоне частот до 100 МГц и должен составлять 100 Ом ±15%).

Для идеальной пары импеданс должен быть одинаковым по всей длине кабеля, поскольку в местах неоднородности возникает эффект отражения сигнала, что в свою очередь может ухудшить качество передачи информации. Чаще всего однородность импеданса нарушается при изменении в рамках одной пары шага скрутки, перегиба кабеля при прокладке или иного механического дефекта.

Скорость/задержка распространения сигнала

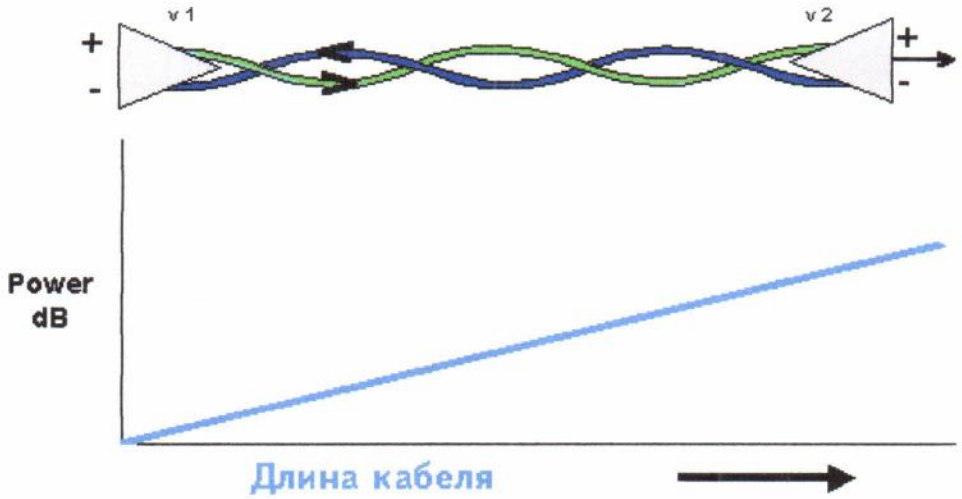
**NVP** (Nominal Velocity of Propagation) - скорость распространения сигнала. Выражается как отношение скорости распространения сигнала к скорости света. Однако часто применяется производная от NVP и длины кабеля характеристика "delay" (задержка), выражающаяся в наносекундах на 100 метров пары. Если в кабеле присутствует более одной пары, то вводят понятие "delay skew" или разность задержки. Дело в том, что пары не могут быть идеально одинаковы, что порождает разные задержки распространения сигнала в разных парах. Идеальные системы подразумевают, что подобные разницы будут минимальны.

## 3. Погонное затухание (Attenuation).

Помимо импеданса и скорости распространения сигнала выделяют и другие важные характеристики кабеля типа "Витая пара". Одной из таких является погонное затухание (attenuation), характеризующей величину потери мощности сигнала при передачи.

Характеристика вычисляется как отношение мощности полученного на конце линии сигнала к мощности сигнала, поданного в линию.

Поскольку величина затухания изменяется с ростом частоты, она должна измеряться для всего диапазона используемых частот. Сама величина выражается в децибелах на единицу длины.




На графике показаны потери мощности сигнала при передаче в зависимости как от длины кабеля, так и от используемой частоты.

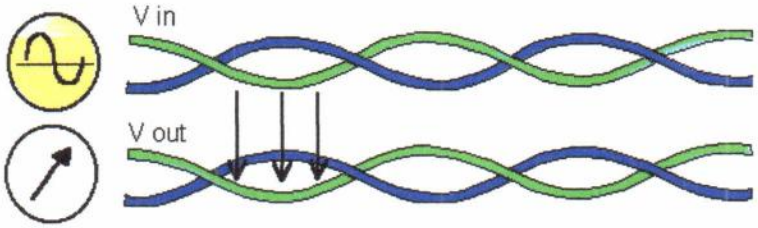
## 4. Переходное затухание между парами

### 5.1.Переходное затухание между парами (NEXT - Near End Crosstalk)

Другим важным параметром является NEXT (Near End Crosstalk), или переходное затухание между парами в многопарном кабеле, измеренное на ближнем конце — то есть со стороны передатчика сигнала, которое характеризует перекрестные наводки между парами.

NEXT численно равен отношению подаваемого сигнала на одну пару к полученному наведенному в другой паре и выражается в децибелах. NEXT имеет тем большее значение, чем лучше сбалансирована пара. Измерения необходимо проводить с обеих сторон, поскольку эта характеристика зависит от взаимного расположения измерительных приборов и мест возможных дефектов в кабеле.

Как и погонное затухание, NEXT необходимо измерять для полного ряда частот.

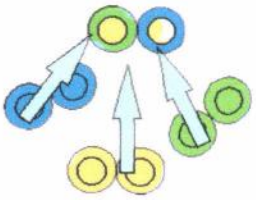



В многопарном кабеле измерения производятся для всех комбинаций пар. Однако в настоящее время все чаще применяют и более глубокие тесты, основанные на выявлении

групповых наводок на ближнем конце между всеми парами (Power Sum Crosstalk), присутствующими в кабеле.

**5.2.Переходное затухание между парами (Power Sum Crosstalk)**

Другое название данной характеристики - Power Sum NEXT или PS-NEXT. Как и NEXT, Power Sum CrossTalk выражает переходное затухание между парами в многопарном кабеле, измеренное на ближнем конце - то есть со стороны передатчика сигнала. Однако учитываются одновременные наводки со всех пар, присутствующих в кабеле. Подобно NEXT, PS-NEXT измеряется с обоих концов линии для всего диапазона применяемых частот.

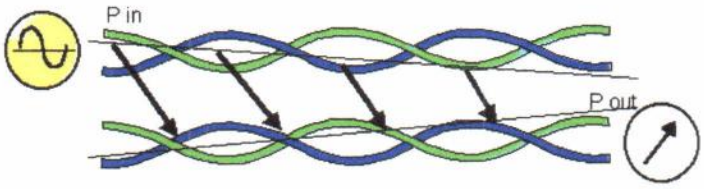


Кроме оценки взаимных наводок пар на ближнем конце кабеля, переходное затухание измеряют и со стороны приемника сигнала. Данный тест получил название FEXT (Far End Crosstalk).

**5.3. Переходное затухание между парам (FEXT - Far End Crosstalk)**

Far End Crosstalk или переходное затухание на дальнем конце характеризует влияние сигнала в одной паре на другую пару. В отличие от NEXT FEXT измеряется посредством подачи тестового сигнала на пару в кабеле с одной пары и замера наведенного сигнала в другой паре со стороны приемника.

Характеристика численно равна отношению тестового сигнала к наведенному посредством созданного электрического поля. FEXT как и все семейство характеристик переходного затухания, измеряется на всем диапазоне используемых частот и выражается в децибелах.

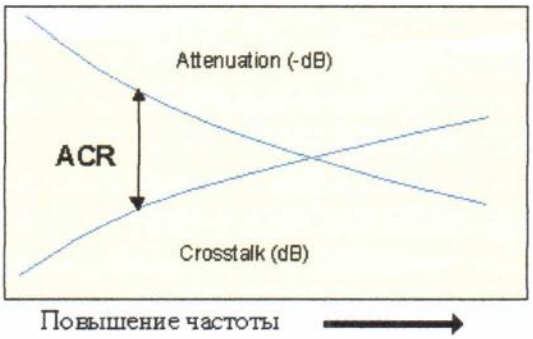



**6. Разность между погонным и переходным затуханиями (ACR - (Attenuation Crosstalk Ratio)**

Одной из самых важных характеристик, отражающих качество кабеля является разность между погонным и переходным затуханиями, выражающуюся в децибелах. Чем меньше погонное затухание, тем большую амплитуду имеет полезный сигнал на конце линии. С другой стороны, чем больше переходное затухание, тем меньше взаимные наводки пар.

Таким образом разность этих двух величин отображает реальную возможность выделения полезного сигнала принимающим устройством на фоне помех. Для уверенного приема сигнала необходимо чтобы Attenuation Crosstalk Ratio был не меньше заданного значения, определяемого стандартами для соответствующей категории кабеля.

При равенстве погонного и переходного затухания выделить полезный сигнал становится теоретически невозможно. Так как характеристика не измеряется, а является результатом вычислений на основе измерений затуханий, которые в свою очередь зависят от используемой частоты, ACR должен вычисляться для всего диапазона применяемых частот.




## 7. Приведенное переходное затухание (ELFEXT - Equal Far End Crosstalk)

ELFEXT - приведенное переходное затухание. Эта характеристика вычисляется на основании измерений переходного затухания на дальнем конце (FEXT) и погонного затухания (Attenuation) наводимой пары. Фактически ELFEXT - это ACR на дальнем конце кабельного линка, т.е. разница между параметрами FEXT первой пары и Attenuation второй. ELFEXT как и все семейство характеристик переходного затухания, вычисляется для всего диапазона используемых частот и выражается в децибелах.


## 8. Суммарное приведенное переходное затухание (PS-ELFEXT - Power Sum Equal Far End Crosstalk).

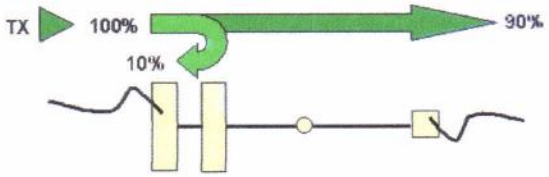
PS-ELFEXT - суммарное приведенное переходное затухание. Эта характеристика вычисляется для каждой отдельной пары простым суммированием значений её параметров elfext относительно всех остальных пар.

## 8. "Обратное затухание" или величина отражения сигнала (Return Loss - (RL).

При передачи сигнала, возникает так называемый эффект отражения сигнала в обратном направлении.

Величина отражения сигнала Return Loss или "обратное затухание" пропорциональна затуханию отраженного сигнала.

Характеристика особенно важна при построении сетей с поддержкой протокола Gigabit Ethernet, использующего передачу сигналов по витой паре в обе стороны (полнодуплексная передача). Достаточно большой по амплитуде отраженный сигнал может искажать передачу информации в обратном направлении. Return Loss выражается в виде отношения мощности прямого сигнала к мощности отраженного.




## СХЕМЫ ОБЖИМА «ВИТОЙ ПАРЫ»

Порядок разводки проводов витой пары для разъемов RJ-45 зависит от назначения соединительной линии, технологии и стандарта передачи данных.

Ниже приведены рисунки для локальных вычислительных сетей Ethernet для стандартов использующих медный кабель - витые пары (Twisted Pair). Аббревиатура таких стандартов как правило имеет вид ##### - **TX** (например, 10Base-TX, 100Base-TX).

Цифра в названии стандарта говорит о несущей частоте передачи данных. Для каждого стандарта используются специальные схемы обжима кабеля, используются различные кабели, применяются специфические ограничения по длине кабеля и количеству соединителей и коммутирующих устройств.

Для 10Base-TX и 100Base-TX задействованы лишь оранжевые и зеленые проводки (контакты 1+2 и 3+6). Синюю пару часто используют для телефонных линий (контакты 4+5).

Для технологий 1000Base-TX и ряда других менее популярных задействованы все 8 контактов, также для Gigabit технологий рекомендуется использовать экранированную витую пару.

На данный момент преобладают локальные сети со 100 Мегабитным оборудованием, где используется два стандарта - **568A и 568B.**

По стандарту **568A** последовательность обжима - **БЗ З БО С БС О БК К** . При этом коннектор RJ-45 должен быть повёрнут защелкой от Вас.

По стандарту **568B** последовательность обжима - **БО О БЗ С БС З БК К** , коннектор RJ-45 повернут защелкой от Вас. **БЗ, З, БО и О** - это номера по порядку 1, 2, 3, 6 - выделены жирным шрифтом - это несущие (используемые) жилы: одна пара на прием, другая на передачу.

Существуют две схемы обжима кабеля связи.

1. **Прямой порядок обжима витой пары, ведущей *от рабочей станции к концентратору* по стандарту А или В.**

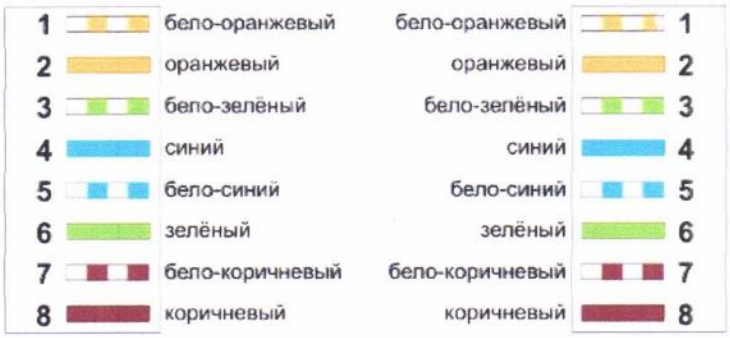
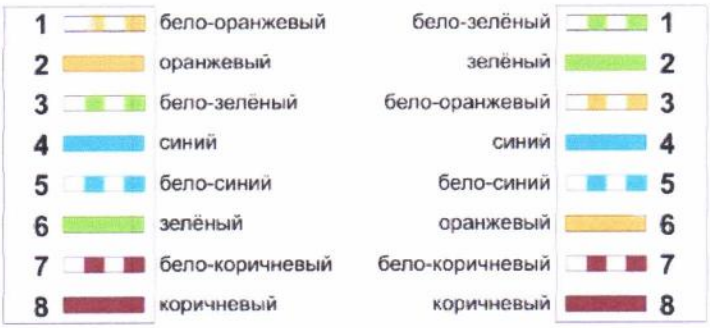



Схема обжима по стандарту 568В (на обоих концах провода)

**2. Кросс-линковый кроссоверный) порядок *для прямого соединения 2-х компьютеров.***

Также используется в том в случае, когда требуется соединить между собой 2 концентратора, не имеющих переключения uplink/normal).
Меняются местами 2 пары: 1-2 на 3-6. Где-то с 2004 года устройства научились автоматически переставлять пары местами и кроссовый обжим утратил смысл.




## ХОД РАБОТЫ:

**Вначале проводят зачистку наружной изоляции кабеля**. Наружную изоляцию круглого кабеля лучше только слегка надрезать на 2-3 см, осторожно поворачивая его в области зачистки, а затем снять кусочек изоляции по кольцевому надрезу вручную. На многих обжимных устройствах есть три рабочие области и соответственно выполняет три функции:

- Ближе всего к рукояткам устройства располагается область, в которой установлен нож для обрезания проводников витой пары.
- В центре находится гнездо для обжима разъема.
- В верхней части устройства - область для зачистки наружной изоляции витой пары.

2. **Далее разводят провода "витой пары" в одной плоскости** в определенном порядке, согласно стандарту.

3. **Выравнивают длину всех проводов** от конца изоляции на 1-1.5 см и ещё раз ровно подрезают.

4. **Затем производят заправку проводников в разъем корпуса RJ-45 до упора**, так, чтобы изоляция также вошла вовнутрь коннектора.

5. **Затем вставляют разъем в гнездо обжимного устройства,** кримпера, и надавливают до тех пор пока устройство полностью не закроется, до щелчка, и **опрессовывают.**

6. **Подключить LAN-тестер и проверить** на проходимость сигнала.

7. Предоставить результаты для проверки. Написать вывод.

## Лабораторная работа № 2
## по теме «Разводка сетевой розетки RJ-45 , коммутационной панели. Тестирование»

**Цель:**

1. Изучить конструкцию сетевой розетки и схему врезки кабеля по стандарту А и В, патч-панели, её классификация.
2. Произвести врезку кабеля связи cat5e в патч-панель и сетевую розетку.

**Оборудование:**

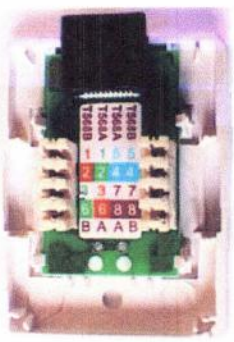
кабель связи витая пара;

инструменты для монтажа и заделки проводов: стриппер, вруб, кримпер, отвертка, сетевая коммуникационная розетка cat5e.

## ТЕОРЕТИЧЕСКИЕ ОСНОВЫ

### Сетевая коммутационная розетка

Представляет собой пластмассовый короб со съёмной крышкой, в верхней части которой смонтирован RJ-45. В этой части 8 подпружиненных контактов и приспособлено для подключения проводников сетевого кабеля. Для крепления на стену с тыльной стороны имеется клеящий слой, либо отверстие для винтов.



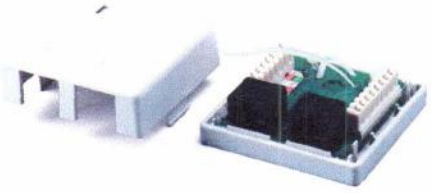



**Схема распределения проводников.**

Так же как и кабель, сетевые розетки различают по категориям (3 и 5е).CAT5. Проводники вставлены в контактные площадки под углом 90° из середины. При врезании проводников в контактные площадки удаляется защитный слой проводника.

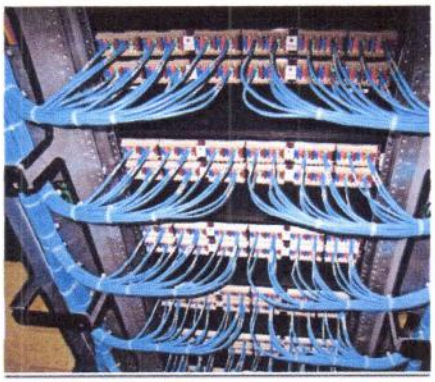
Для надёжности врезки проводников в контактные площадки используют вруб. Все контакты выделены цветом и пронумерованы.

**Инструменты для монтажа и заделки проводов.**

**Стриппер** – электромонтажный инструмент. Предназначен для удаления изоляции с концов проводов и разделки кабеля (UTP, STP). Имеет соответствующие пазы для проводов разного диаметра. Для зачистки и разделки кабелей диаметром до 9.5 мм.

**Вруб** – для зачистки и обработки витой пары. Инструмент с функцией «удара».

**Коммутационная панель**.




На лицевой панели находятся контакты, предназначенные для фиксированного соединения с кабелем.

**Классификация патч-панелей.**

1. **По составу разъёма.**
   1.1. Фиксированное: -медная (RJ-12, RJ-45).
   -волоконно-оптическая
   -мультимедийная1.2. Наборно-юнитовая – может содержать в корпусе различные разъёмы.
   1.3. Наборная. Для установки в промежуточные конструктивы.
2. **По количеству портов (12,24,48,96).**
3. **По экранированию (экранированная, неэкранированная).**
4. **По способу крепления.**
   4.1. В стену
   4.2. В стойку
   4.3. В промежуточные конструктивы.
5. **По способу представления портов**
   5.1. Одинарное
   5.2. Двойное

**Ход работы:**

1. Зачистить наружную изоляцию кабеля и развести провода «витой пары» по схеме А.
2. Произвести заправку проводников в разъем корпуса RJ-45 до упора, так, чтобы изоляция также вошла вовнутрь коннектора.
3. Вставить разъем в гнездо обжимного устройства - кримпера, и надавливаем до тех пор пока устройство полностью не закроется, до щелчка, и опрессовываем.
4. Те же операции проделать с другим концом кабеля.
5. Взять новый кабель и с помощью вруба врезать проводники в розетку. С другим концом данного кабеля проделать операции, указанные в первых трёх подпунктах.
6. Взять третий кабель и врезать с помощью вруба проводники в патч-панель. С другим концом данного кабеля проделать операции,
указанные в первых трёх подпунктах.
7. Собрать и протестировать схему. Написать вывод

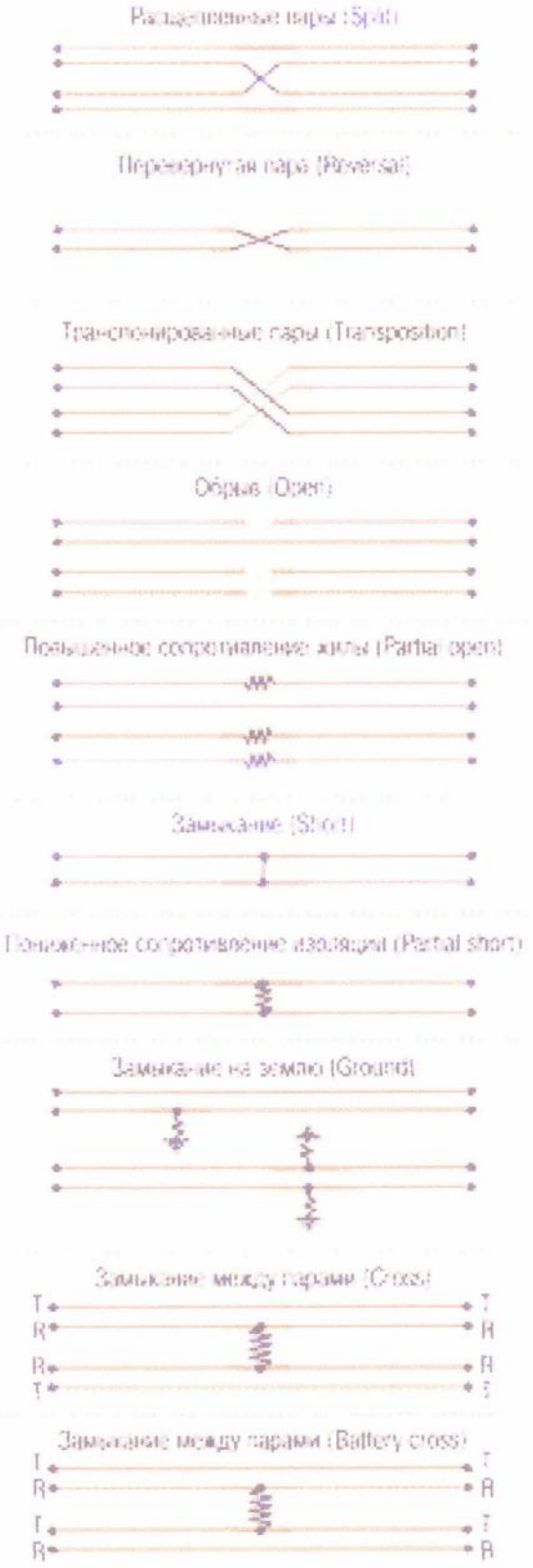
## Лабораторная работа № 3
## по теме «Идентификация повреждений кабельной системы»

**Цель:** научиться определять повреждения в кабеле, находить и диагностировать неисправности.

Нарушения нормального функционирования кабельных систем на базе витой пары могут быть вызваны грубыми ошибками при монтаже, скрытыми дефектами конструкции кабеля и повреждением во время его прокладки, процессами старения самих витых пар и арматуры кабельных линий связи, а также другими причинами.

## ОСНОВНЫЕ ПОВРЕЖДЕНИЯ ВИТОЙ ПАРЫ И ИХ ПРИЧИНЫ

К явным недостаткам монтажа относятся ошибки соединения жил витых пар в кроссах АТС, на стыках строительных длин, в распределительных шкафах и коробках, удаленных терминалах и т. д.




В соответствии с принятой терминологией, две пары, в которых нарушен правильный порядок подключения жил, называются расщепленными (split). Признаками расщепленных пар могут быть увеличенный резистивный и емкостной дисбаланс.

Неправильно смонтированная витая пара, где прямой и обратный провода переставлены местами, называется перевернутой, или скрещенной (reversal). В кабельных линиях СКС порядок подключения жил витой пары крайне важен.

Две витые пары с ошибочным подключением к зажимам терминала называются транспонированными парами (transposition). На телефонной сети такой дефект монтажа приведет к подключению неверного номера. В случае же СКС подключенное к линии оборудование может оказаться неработоспособным.

К основным скрытым дефектам кабельных линий связи относится некачественный монтаж муфт и сростков жил на стыках строительных длин. В первом случае нарушается герметичность оболочки кабеля и возникает опасность его намокания, а для второго характерно появление плохих контактов (partial open) и даже обрыв жил витой пары (open). К таким же результатам приводит коррозия контактов кроссовых устройств и некачественная кроссировка. Дефекты и пробои изоляции жил, влага в кабеле и загрязнение терминалов нередко ведут к замыканию жил пары между собой.

Замыкание может быть низкоомным (short) или высокоомным (partial short). Еще один аналогичный вид дефектов витой пары — замыкание на землю одной или нескольких ее жил (ground). Причем контакт жилы с землей совсем не обязательно будет находиться недалеко от места повреждения изоляции жилы — электри-

ческий путь от проводника жилы к земле пройдет через экран кабеля, металлические элементы конструкции терминалов и несущие элементы кабеля.

Замыкание случается и между жилами двух различных пар, причем замкнуты могут быть как одноименные, так и разноименные жилы (cross и battery cross, соответственно).

Такой вид дефектов приводит к наличию постороннего напряжения на линии, переходным явлениям, ослаблению сигнала.

Естественный процесс старения витой пары проявляется в виде увеличения вносимого ею затухания вследствие ухудшения диэлектрических свойств изоляции витой пары.

При идентификации неисправностей пары всегда нужно иметь в виду, что ее дефекты могут быть множественными (несколько однотипных дефектов) или комбинированными (несколько разнотипных дефектов), а показания приборов при измерениях с различных сторон могут существенно отличаться.


Источниками помех витой пары служат внутренние и внешние помехи кабеля.

*К основным источникам внутренних помех относят соседние витые пары того же кабеля, а к основным источникам внешних помех — помехи от сети переменного тока и атмосферные явления, включая разряды молнии и радиопомехи.*

Нарушение нормальной работы любого из них может стать причиной повышенных шумов витой пары.

**Задание:** обследовать образцы витой пары и указать причину неисправностей. Оформить результаты в виде таблице.

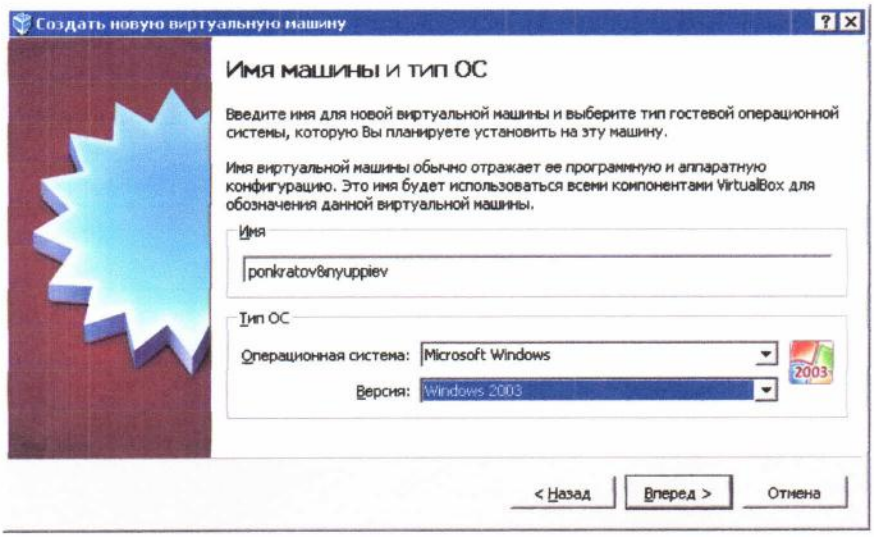
## Практическая работа № 1
## по теме «Установка и настройка сетевой операционной системы семейства Windows»

**Цель:** научиться устанавливать и настраивать сетевую ОС Windows.

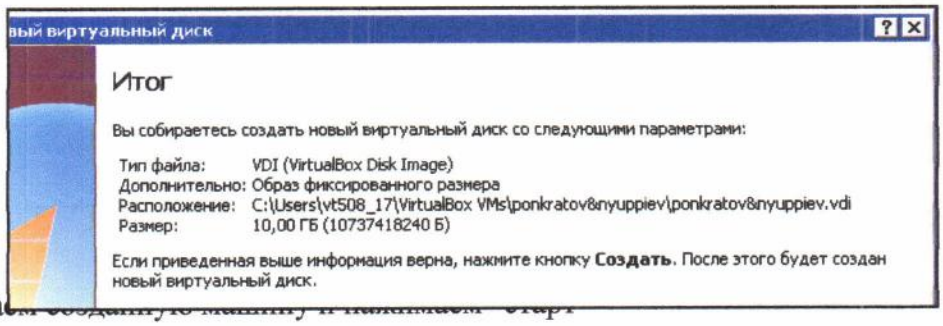
### Ход работы:

1)Главное меню-все программы-стандартые-подключение к удаленному рабочему столу
2)Подключаемся к серверу Virtual b
3)Входим на сервер Virtual под своим пользователем
4)Открываем окно программы Oracle Vm Virtual Box менеджер
5)Нажимаем "создать" , открывается окно "Мастер создания Новой виртуальной машины"

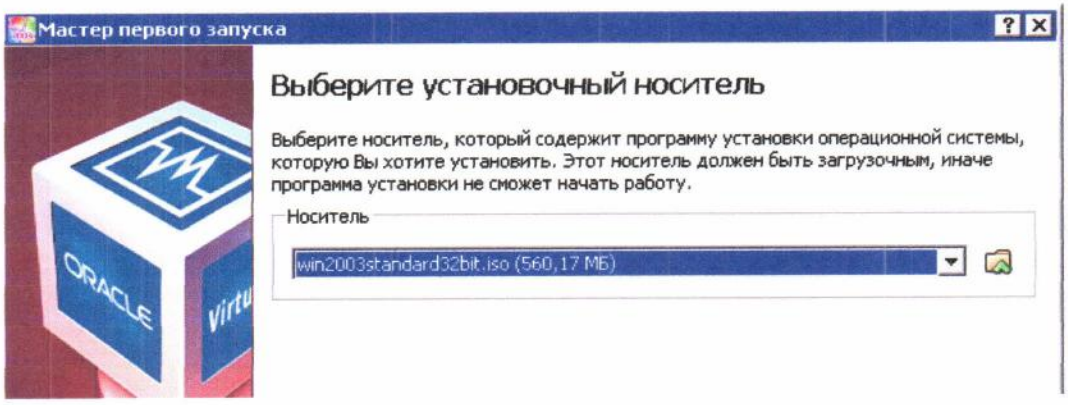
6) Вводим имя виртуальной машины(фамилия) и устанавливаем тип ОС(Windows 2003) - далее




7)Устанавливаем кол-во оперативной памяти 512 мб - далее
8) Устанавливаем загрузочный ЖД "Создать новый ЖД" - далее
9)Выбираем VBDI(Virtual box disk image) - далее
10)Выбираем фиксированный ЖД - далее
11)Устанавливаем 10 Гб размер ЖД, выбираем его путь (F\Образы) - далее
12)нажимаем кнопку "Создать "
13)Виртуальная машина создана

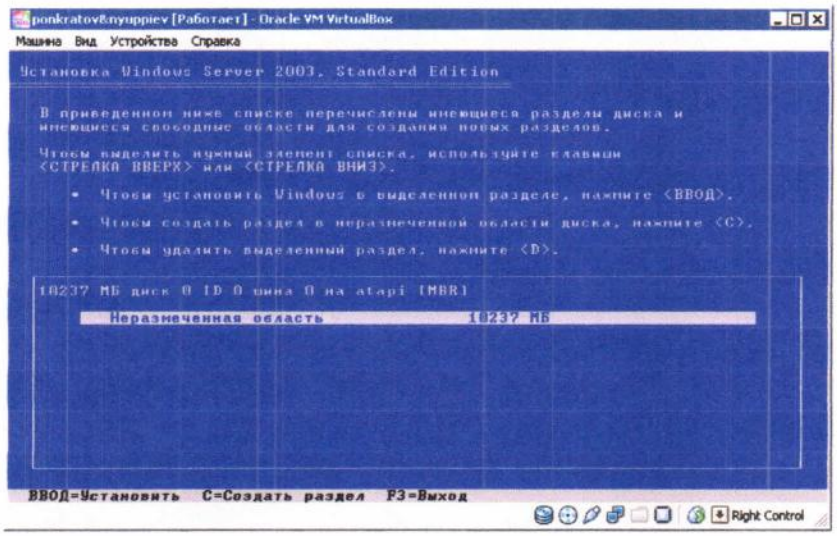



14)Выбираем созданную машину и нажимаем "старт"
15)Откроется "Мастер первого запуска" - далее
16)Выбираем образ Windows на рабочем столе – вперед



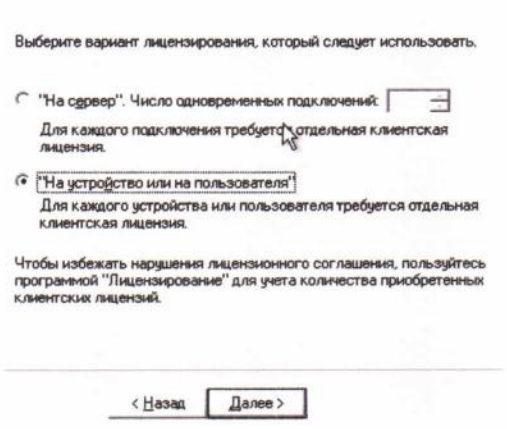

17)Началась установка WIndows

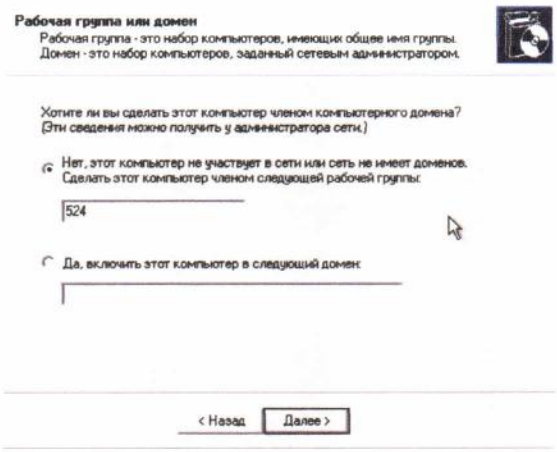
18)Создаем раздел на ЖД, форматируем его в NTFS(быстрое)



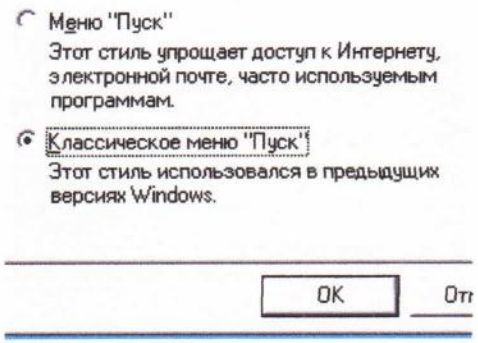

19)Выбираем созданный раздел диска для установки ОС
20)Идет процесс установки
21)Устанавливаем региональные настройки - далее
22)Вводим лицензионный ключ - Далее
23)Выбираем лицензию "На пользователя или устройство" - далее

24)Вводим имя пользователя-администратора
и устанавливаем пароль (123) - далее
25)Вводим рабочую группу(524) – далее

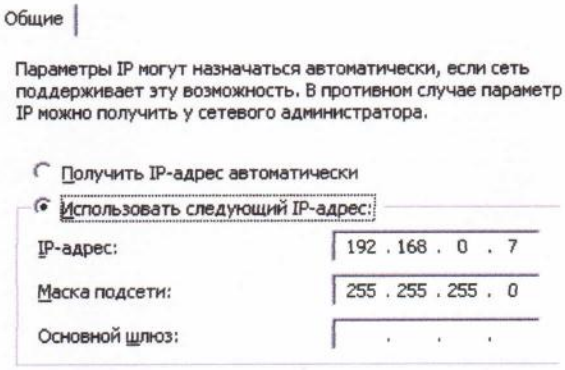


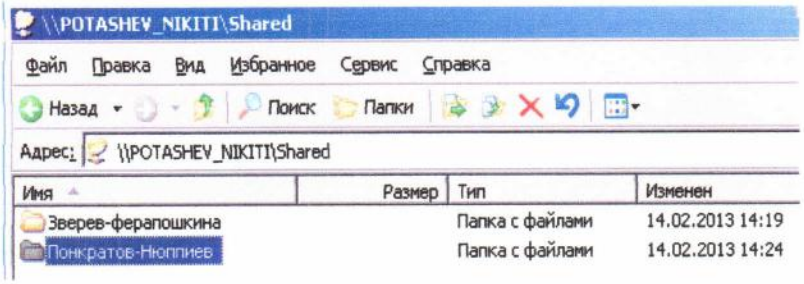

26)Продолжается процесс установки Windows.
27)Ос установлена
28)В панели меню виртуальной машины выбираем пункт "Устройства-установить дополнения для гостевой ОС"
29)Далее устанавливаем классический вид меню Пуск




30)Отключаем сетевые службы: Автоматическое обновление, Брандмауэр, беспроводная настройка, Вэб-клиент
31)Включаем службы: Сервер
32)Устанавливаем сетевые настройки




33)Создать папку "Shared"




Путь C:\Shared и открываем для нее
общий доступ: ПКМ - общий доступ и безопасность - Открыть общий доступ

34)Меню окна виртуальной машины: Машина - Свойства - Сеть - Тип подключения "Сетевой мост"
35) Зайти на общую папку другого
компьютера сети и создать там папку,
проверить доступ к общим папкам к
компьютерам сети в диапазоне IP
от 192.168.0.2 - 192.168.0.13
36) Провести пинг компьютера сети в диапазоне IP
от 192.168.0.2 - 192.168.0.13:

Иванова А.Н.

**УТВЕРЖДАЮ:**
**Начальник УМО**

_____
**О.А. Дедова**

# График мероприятий месяца ЦК

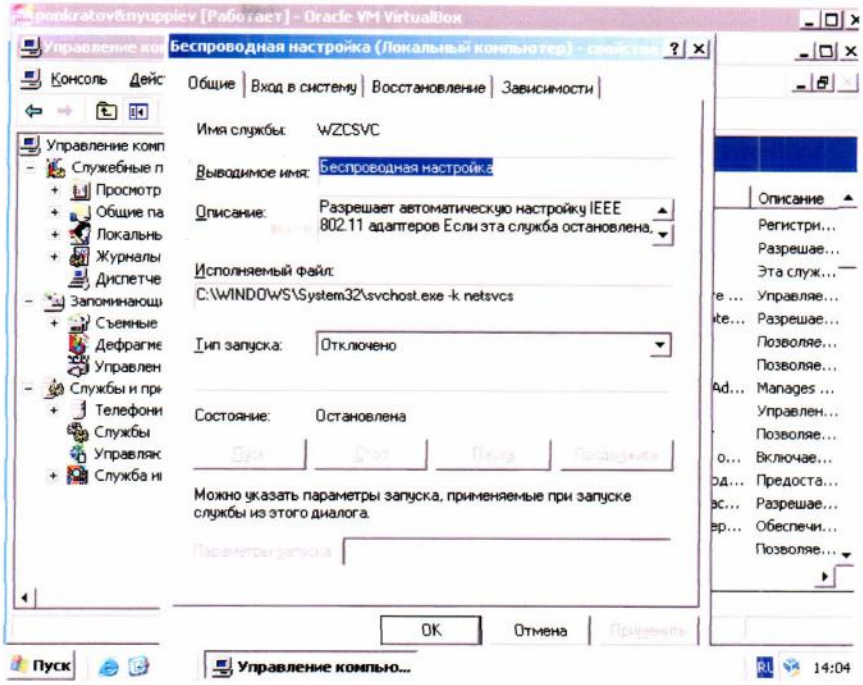
Специальности 09.02.02 с «6».04. 2015 по «6».05. 2015

| № п/п | Мероприятие | Ответственные | Дата, время, место проведения | Взаимопосещения |
|---|---|---|---|---|
| 1. | Олимпиада по информатике и ИКТ между студентами I курса Секция «Гранит науки» | Марченко Г.А Капланова М.М. Штунь Е.Н. Иванова А.Н. | 6.04.2015 каб 418, 420 | Преподаватели цикловой |
| 2. | Региональная Олимпиада по информатике и ИКТ | Марченко Г.А Капланова М.М. | 8.04.2015 КИРО | |
| 3. | Классный час в группе ВТ-512 «Моя профессия - системный инженер» | Голодюк А.О. | 16.04.2014 | Капланова М.М. Марченко Г.А. |
| 4. | Олимпиада по информатике среди студентов 2 курса | Марченко Г.А Капланова М.М. Штунь Е.Н. | 21-24 .04.2015 | Преподаватели цикловой |
| 5. | Субботник бережливого производства | Иванова А.Н. Усков А.А. | 25. 04.2015 | Преподаватели цикловой |
| 6. | Создание видео ролика колледжа. Посвященного 85-летию колледжа | Иванова А.Н. Усков А.А. Голодюк А.О. Фунев А.Г. Копороаский | 17.04.2015 | |
| 7. | Открытое занятие по теме «Графический редактор GIMP» в гр. ВТ-513 | Штунь Е.Н. | 23.04.2015 | Капланова М.М., Зайцев В.А. Марченко Г.А. |
| 8. | Открытое занятие Деловая игра «Один день из жизни IT-специалиста» | Иванова А.Н. Капоровский В.Е. Голодюк А.О. | 4.05.2015 | Преподаватели цикловой |
| 9. | Экскурсия в Сервис-центр Apple Sampo.ru | Зайцев В.А. | 29.04.2015 | - |
| 10. | Выпуск стенгазеты по итогам недели Цикловой комиссии 230111 | Иванова А.Н. Усков А.А. Капланова М.М. | 25.04.2015 | - |
| 11. | Заседание ЦК «Подведение итогов недели ЦК» | Капланова М.М. члены ЦК | 7.05.2015 | - |

Председатель ЦК _____/_____/

Пуск - выполнить - cmd - ping 192.168.0.8

Оформляем вывод




## Практическая работа № 2 по теме «Расчёт адресного пространства»

**Цель:** научиться рассчитывать адресное пространство.

### АДРЕСАЦИЯ В IPV4. IP-АДРЕСА

*В стеке протоколов TCP/IP используются три типа адресов:*

- **Локальные (аппаратные**) – адреса, используемые “локальными” технологиями для доставки пакетов в пределах подсети. Например, MAC-адреса в сетях Ethernet, FDDI, WiMAX и т.д.
- **IP-адреса** – адреса межсетевого уровня, используемые для идентификации сетевых интерфейсов интерсети. На основе IP-адресов организуется универсальная, не зависящая от “локальных” технологий идентификация сетевых интерфейсов интерсети.
- **Символьные доменные адреса (имена)** – используются для присвоения сетевым интерфейсам легко запоминаемых символьных имен.

В заголовке IP- пакета для IP-адресов получателя и отправителя отводится по 32 бита (4 байта). Наиболее часто IP-адрес записывают в виде четырех однобайтовых чисел, разделенных точкой.

**Пример 1.**
Записи IP-адреса в различных форматах:
десятичная: 219.17.25.157
двоичная: 11011011.00010001.00011001.10011101
шестнадцатеричная: DB11199D

Если узел IP-сети имеет несколько сетевых интерфейсов, каждому из них присваивается отдельный IP-адрес. Например, если узел имеет два сетевых интерфейса, с помощью которых он подключен к двум "локальным" сетям, его сетевым интерфейсам будут сопоставлены два IP-адреса.

**Способы назначения адресов:**

1. ***администратором (вручную),*** с помощью утилит конфигурирования операционной системы (ОС);
2. ***автоматически,*** с помощью протокола динамической конфигурации узла DHCP (Dynamic Host Configuration Protocol, RFC 2131).

**IP-адреса состоят из двух частей** – номера сети и номера узла. Номер сети идентифицирует в интерсети подсеть, к которой принадлежит узел, номер узла однозначно определяет узел внутри подсети. Для разделения IP-адреса на части используют две схемы:

- на основе классов адресов,
- на основе масок.

## РАЗДЕЛЕНИЕ IP-АДРЕСА НА НОМЕР СЕТИ И НОМЕР УЗЛА НА ОСНОВЕ КЛАССОВ

Традиционная схема разделения IP-адреса на номер сети и номер узла основана на понятии класса, определяемого значениями нескольких первых бит адреса.

**Класс A.** Первый бит равен 0: адрес класса A, первый байт адреса используется для номера сети, остальные три – для номера узла (количество адресов в сети 224). Адреса: 1.0.0.0 – 127.255.255.255

**Класс B.** Первые биты равны 10: адрес класса B, первые два байта используются для номер сети, остальные – для номер узла (количество адресов в сети 216). Адреса: 128.0.0.0 – 191.255.255.255

**Класс C.** Первые биты равны 110: адрес класса C, первые три байта используются для номера сети, последний байт – для номера узла (количество адресов в сети 28). Адреса: 192.0.0.0 – 223.255.255.255

**Класс D.** Первые биты равны 1110 – адреса мультикаст (multicast), предназначены для адресации группы узлов. Адреса: 224.0.0.0 – 247.255.255.255

В некоторых случаях необходимо отдельно записывать номер сети и номер узла, из которых состоит IP-адрес. В записи номера сети соответствующие номеру узла разряды адреса заменяют нулями, в записи номера узла нулями заменяют разряды, соответствующие номеру сети.

**Пример 2**.

IP-адрес 192.9.7.5 (11000000.00001001.00000111.00000101)

Поскольку первые биты равны 110, следовательно, это адрес класса C.
Номер сети – 192.9.7.0 (11000000.00001001.00000111.00000000),
Номер узла – 0.0.0.5 (00000000.00000000.00000000.00000101).

**Пример 3.**
IP-адрес 62.76.9.17 (00111110.01001100.00001001.00010001)
Поскольку первый бит равен 0, следовательно, это адрес класса А.
Номер сети – 62.0.0.0 (00111110.00000000.00000000.00000000)
Номер узла – 0.76.9.17 (00000000.01001100.00001001.00010001)

## СООТВЕТСТВИЕ БЛОКОВ АДРЕСОВ НОМЕРАМ СЕТЕЙ НА ОСНОВЕ КЛАССОВ

Номер сети определяет блок адресов с одинаковым префиксом (одинаковой старшей частью), зависящим от класса адреса.

**Пример 4.**
Рассмотрим номер сети 192.168.169.0.
Первые разряды адреса имеют значение 110, следовательно, это адрес класса С. Этому номеру сети соответствует блок адресов 192.168.169.0 – 192.168.169.255, все адреса этого блока имеют одинаковые первые три октета, равные 192.168.169.

**Пример 5.**
Рассмотрим номер сети 62.0.0.0.
Первый разряд адреса имеет значение 0, следовательно, этот адрес класса А. Этому номеру сети соответствует блок адресов 62.0.0.0 – 62.255.255.255, все адреса этого блока имеют одинаковый первый октет, равный 62.

## НЕЭФФЕКТИВНОСТЬ АДРЕСАЦИИ НА ОСНОВЕ КЛАССОВ

Как показывает практика, выделение сетям блоков адресов на основе классов (адресация на основе классов) не обеспечивает оптимальное использование адресного пространства IPv4. Например, для большинства организаций средней величины блок адресов класса С (256 адресов) слишком мал, а блок класса В (65534 адресов) слишком велик. Как правило, в таких организациях для адресации узлов используют менее половины адресов. В настоящее время адресация на основе классов считается устаревшей и на практике почти не используется. Возможные пути решения проблемы:

1. Увеличить количество бит, выделяемых для номера сети в классах А, В. Например, можно в классе В выделить под номер сети 19–20 бит;
2. Использовать схему адресации, в которой для номера сети можно использовать произвольное количество бит адреса.

## РАЗДЕЛЕНИЕ IP-АДРЕСА НА НОМЕР СЕТИ И НОМЕР УЗЛА НА ОСНОВЕ МАСОК

Маска – это используемое совместно с IP-адресом четырехбайтовое число, двоичная запись которого содержит единицы в разрядах, соответствующих в адресе номеру сети, и нули в раз-

рядах, соответствующих номеру узла. Единицы в маске начинаются в первом разряде адреса и не могут чередоваться с нулями.
С помощью маски можно выделять произвольное количество разрядов для номера сети, что позволяет отказаться от понятий классов адресов и сделать более гибкой систему адресации.

**Примеры 6.**
Запись маски и IP-адреса
Десятичная форма:
192.168.74.64/255.255.255.192
Двоичная форма:
11000011. 10101000. 01001010 .01000000/11111111.11111111.11111111.11000000

Для указания количества разрядов, выделенных для номера сети, также используется указание префикса адреса. Запись адреса с префиксом имеет вид: IP-адрес/Префикс, где Префикс – число разрядов, выделенных для номера сети.

**Например,** запись 192.168.75.64/26 означает, что в адресе 192.168.75.64 под номер сети отведено 26 двоичных разрядов, соответствующая маска 255.255.255.192.
Значения масок стандартных классов адресов:
класс A – 11111111.00000000.00000000.00000000 (255.0.0.0);
класс B – 11111111.11111111.00000000.00000000 (255.255.0.0);
класс C – 11111111.11111111.11111111.00000000 (255.255.255.0).

## ВЫЧИСЛЕНИЕ НОМЕРА СЕТИ И НОМЕРА УЗЛА ПО ЗАДАННОМУ IP-АДРЕСУ И МАСКЕ

Для вычисления номера сети по заданному IP-адресу и маске необходимо применить побитовую операцию “И” к адресу и маске. Такая операция называется наложением маски на адрес.
На рисунке 1 представлено табличное побитовой операции “И”.

| 1-ый операнд | 2-ой операнд | Значение “И” |
|---|---|---|
| 0 | 0 | 0 |
| 1 | 0 | 0 |
| 0 | 1 | 0 |
| 1 | 1 | 1 |

Рис. 1. Определение побитовой операции “И”

Для вычисления номера узла по заданному IP-адресу и маске необходимо применить побитовую операцию “И” к адресу и результату применения побитовой операции “НЕ” к маске.

На рисунке 2 представлено табличное определение унарной операции побитового отрицания “НЕ” (побитового дополнения).

| Операнд | Значение "НЕ" |
|---|---|
| 0 | 1 |
| 1 | 0 |

Рис. 2. Определение побитовой операции "НЕ"

**Пример 7**.

Применим побитовую операцию "И" к однобайтовым числам 185 и 221.

Представим числа в двоичной форме: 185 = 10111001, 221 = 11011101.

$$\begin{array}{ll} & 10111001 \\ \textbf{И} & \underline{11011101} \\ & 10011001 \end{array}$$

Применим побитовую операцию "НЕ" к числу 185.

$$\begin{array}{ll} \textbf{Н} & \underline{10111001} \\ & 01000110 \end{array}$$

**Пример 8.**

Вычислим номер сети и номер узла для адреса 215.17.125.177 и маски 255.255.255.240.

IP-адрес: 215.17.125.177 (11010111.00010001.01111101.10110001)

Маска: 255.255.255.240 (11111111.11111111.11111111.11110000)

В этом случае номер сети (Н.с.) и номер узла (Н.у.) будут следующими:

Н.с.: 215.17.125.176 (11010111.00010001.01111101.10110000)

Н.у.: 0.0.0.1 (00000000.00000000.00000000.00000001)

**Пример 9**.

Вычислим номер сети и номер узла для адреса 67.38.173.245 и маски 255.255.240.0.

IP-адрес: 67.38.173.245 (01000011.00100110.10101101.11110101)

Маска: 255.255.240.0 (11111111.11111111.11110000.00000000)

Н.с.: 67.38.160.0 (01000011.00100110.10100000.00000000)

Н.у.: 0.0.13.245 (00000000.00000000.00001101.11110101)

## СООТВЕТСТВИЕ БЛОКОВ АДРЕСОВ НОМЕРАМ СЕТЕЙ НА ОСНОВЕ МАСОК

При использовании маски, так же, как и в случае адресации на основе классов, номер сети определяет блок адресов с одинаковым префиксом.

**Пример 10.**

В маске 255.255.255.192 (11111111.11111111.11111111.11000000) выделено 26 разрядов под номер сети и 6 разрядов под номер узла.

Номеру сети 192.168.74.64 с данной маской соответствует блок адресов:

Маска: 11111111.11111111.11111111.11000000 (255.255.255.192)

Н.с: 11000011.10101000.01001010.01000000 (192.168.74.64)

Адрес 1: 11000011.10101000.01001010.01000000 (192.168.74.64)

Адрес 2: 11000011.10101000.01001010.01000001 (192.168.74.65)
Адрес 3: 11000011.10101000.01001010.01000010 (192.168.74.66)
……
Адрес 63: 11000011.10101000.01001010.01111110 (192.168.74.126)
Адрес 64: 11000011.10101000.01001010.01111111 (192.168.74.127)
Всего в этом блоке $2^6 = 64$ адресов (192.168.74.64 – 192.168.74.127).
Все адреса имеют одинаковый префикс (первые 26 разрядов):
11000011.10101000.01001010.01

**Пример 11.**

В маске 255.255.254.0 (1111111.11111111.11111110.00000000) выделено 23 разряда под номер сети и 9 разрядов под номер узла.
Номеру сети 192.168.74.0 с данной маской соответствует блок адресов:
Маска: 11111111.11111111.11111110.00000000 (255.255.254.0)
Н.с: 11000011.10101000.01001010.00000000 (192.168.74.0)
Адрес 1: 11000011.10101000.01001010.00000000 (192.168.74.0)
Адрес 2: 11000011.10101000.01001010.00000001 (192.168.74.1)
Адрес 3: 11000011.10101000.01001010.00000010 (192.168.74.2)
……
Адрес 511: 11000011.10101000.01001011.11111110 (192.168.75.254)
Адрес 512: 11000011.10101000.01001011.11111111 (192.168.75.255)

Всего в этом блоке $2^9 = 512$ адресов (192.168.74.0 – 192.168.75.255). Все адреса имеют одинаковый префикс (первые 23 разряда):
11000011.10101000.0100101

***Замечание:*** размер блока адресов, соответствующий некоторой маске, всегда равен степени двойки.

## ЗАДАНИЯ ДЛЯ РАСЧЁТА АДРЕСНОГО ПРОСТРАНСТВА:

1. Подсчитайте, каков диапазон хостов для IP-адреса 192.168.168.188 255.255.255.192
2. Подсчитайте, каков адрес широковещательной рассылки для адреса подсети 192.168.99.20 255.255.255.252
3. Подсчитайте, какому диапазону хостов принадлежит хост с идентификатором 192.168.10.33 255.255.255.224
4. Определите все характеристики подсетей для IP-адреса 192.168.10.0 255.255.255.240
5. Определите все характеристики подсетей для IP-адреса 192.168.10.0 255.255.255.248
6. Определите подсеть, широковещательный адрес и диапазон допустимых хостов для 172.16.10.5 255.255.255.128
7. Определите подсеть, широковещательный адрес и диапазон допустимых хостов для 172.16.10.17 255.255.255.252
8. Подсчитайте, каков допустимый диапазон хостов для IP-адреса 172.16.10.22 255.255.255.240
9. Определите, каков широковещательный адрес для подсети 10.254.255.19 из 255.255.255.248

Расчетные задания оформить на листе, результаты представить для проверки преподавателю.

## Практическая работа № 3
## по теме «Оформление проектной документации»

**Цель:** ознакомиться с правилами оформления проектной технической документации инаучиться оформлять специальную часть курсового проекта.

Оформление проектной технической документации начинается с ознакомления с ведомостью ссылочных документов. В этой ведомости содержатся названия стандартов и их сокращенное наименование.

При оформлении пояснительной записки и графической части проекта необходимо обратить внимание на:

– комплектность пояснительной записки в соответствии с заданием на проектирование;

– правильность заполнения титульного листа, наличие необходимых подписей;

– наличие и правильность рамок, основных надписей на всех страницах, выделение заголовков, разделов и подразделов, наличие красных строк;

– правильность оформления содержания, соответствие названий разделов и подразделов в содержании соответствующим названиям в тексте записки;

– правильность нумерации страниц, разделов, подразделов, иллюстраций, таблиц, приложений, формул (ГОСТ 2.105-79, ГОСТ 7.32-81);

– правильность оформления иллюстраций-чертежей, схем, графиков (ГОСТ 2.319-81);

– правильность оформления таблиц (ГОСТ 2.105-95);

В процессе оформления чертежей необходимо обратить внимание на:

– соответствие с требованиями стандартов;

– соблюдение форматов, правильность их оформления (ГОСТ 2.301-68);

– правильность выполнения схем;

– соблюдение масштабов, правильность их обозначений (ГОСТ 2.302-68);

– правильность начертания и применение линий, написание текста (согласно выбранного типа шрифта) (ГОСТ 2.303-68);

В специальной части проекта даётся описание проектируемой ЛВС на основе частного технического задания в соответствии с требованиями стандартов. Проектная документация должна содержать полное описание используемого оборудования, их технические характеристики и совместимость, обоснование выбранной конфигурации сети с подробным описанием всех сетевых подключений и соединений. При описании активного сетевого оборудования должны быть указаны все технические характеристики. При описании программного обеспечения необходимо представить все компоненты используемого ПО: операционная система, пакет драйверов, программное и прикладное обеспечение, антивирус, используемые межсетевые экраны или брандмауэры, пакет программ для оптимизации сетевой ОС.

Для создания безотказной работы, уменьшения проблем функционирования и выхода оборудования из строя должна быть установлена система источников бесперебойного питания (ИБП) с указанием технических характеристик, выбранного оборудования.

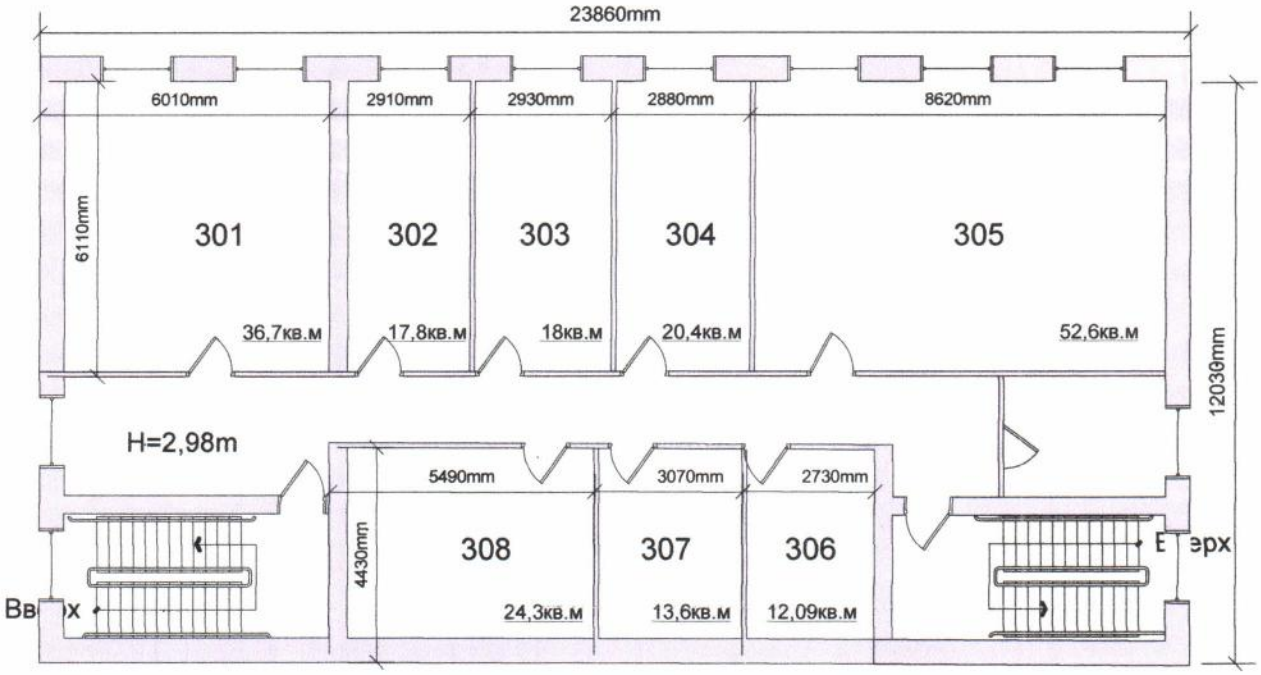
Любая проектная документация заканчивается выводами по проделанной работе и содержит краткий итог.

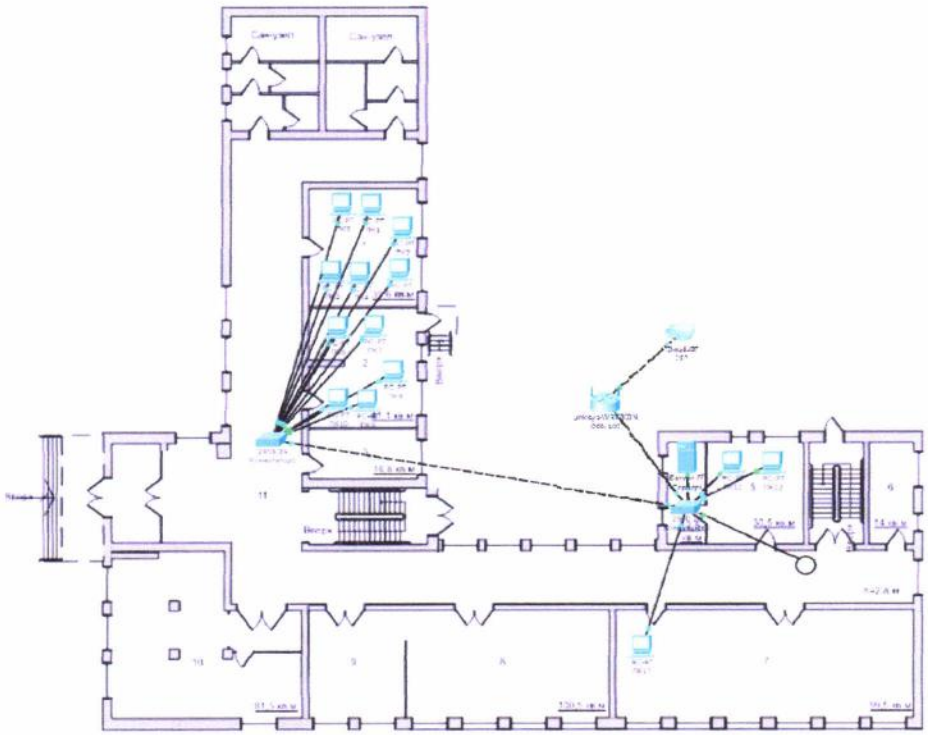
В качестве дополнительных листов к проектной документации могут выступать таблицы, чертежи рисунки, схемы и планы.

**Практическая работа № 4**

**по теме «Создание рабочих чертежей: план здания, структурированной кабельной системы, телекоммуникационного шкафа»**

**Цель:** научиться создавать рабочие чертежи: строительные планы зданий, планы расположения оборудования и горизонтальную кабельную систему.



## Практическая работа № 5
## по теме «Создание монтажной схемы разделки коммутационной панели»

**Цель:** научиться создавать в среде MS Visio монтажную схему разделки коммутационной панели.

Монтажная схема разделки коммутационного шкафа содержит в себе графическое отображение всех соединений и подключений. Это позволяет наглядно увидеть схему соединений и сориентироваться при возникновении проблем в сети.

Для создания монтажной схемы необходимо задать параметры листа и создать элемент сетевой розетки для последующей комплектации коммутационного шкафа. Магистральное пассивное и активное оборудование монтируется в коммутационном шкафу в аппаратной, коммутационной или серверной. Выбор высоты коммутационного шкафа определяется по формуле, затем определяется местоположение технических средств в шкафу и описывается таблицей.

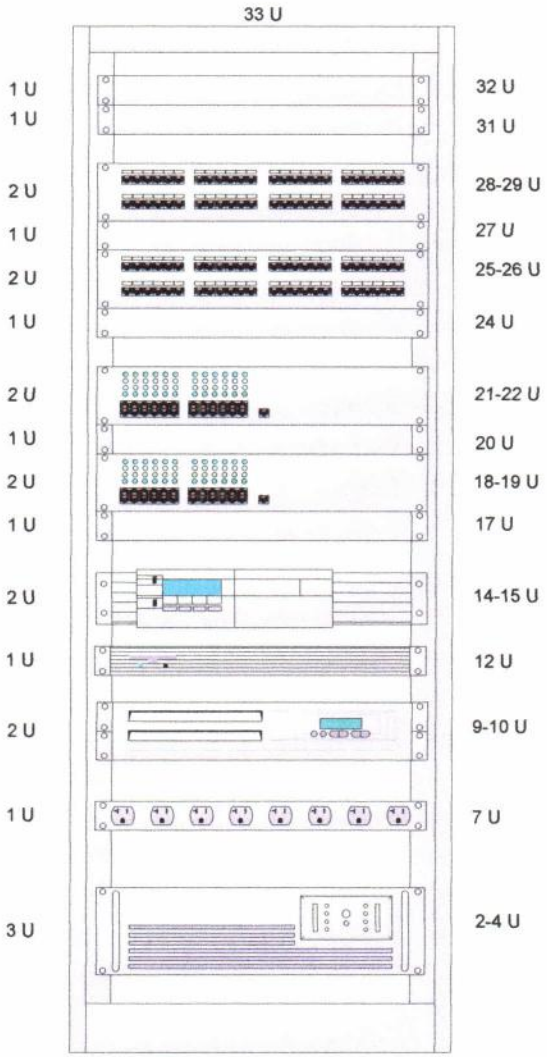



Рисунок 1. Коммутационный шкаф и таблица расположения оборудования в коммутационном шкафу.

| № об. | Размещение | Наименование оборудования | Фирма-производитель |
|---|---|---|---|

| | | | |
|---|---|---|---|
| 1 | 32 U | Модуль вентиля-торный | Nix |
| 2 | 31 U | Блок Освещения | Nix |
| 3 | 28-29 U | Коммутационная панель | Krone |
| 4 | 27 U | Органайзер | Siemon |
| 5 | 25-26 U | Коммутационная панель | Krone |
| 6 | 24 U | Органайзер | Siemon |
| 7 | 21-22 U | Коммутатор | D-link |
| 8 | 20 U | Органайзер | Siemon |
| 9 | 18-19U | Коммутатор | D-link |
| 10 | 17 U | Органайзер | Siemon |
| 11 | 14-15 U | Маршрутизатор | TP-Link |
| 12 | 12 U | Модем | TP-Link |
| 13 | 9-10 U | Сервер | Intel |
| 14 | 7 U | Сетевой фильтр | Ever |
| 15 | 2-4 U | ИБП | GE |

Прежде чем создать данную схему нужно создать элемент сетевой розетки. Далее необходимо сгруппировать их по количеству портов в коммутационной панели или активном сетевой оборудовании, таких как коммутатор или маршрутизатор.

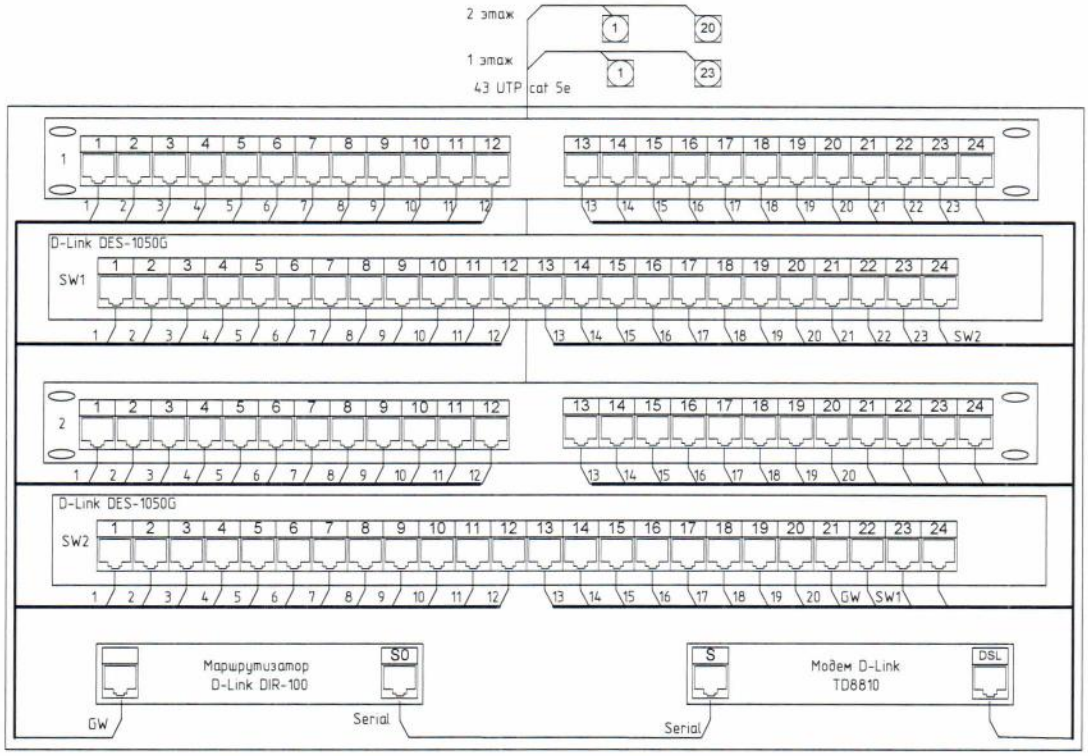



Рисунок 2.Монтажная схема разделки коммутационного оборудования

Отчёт представить преподавателю в виде рисунка в соответствующей рамке для оформления практических занятий и лабораторных работ.

## Практическая работа № 6

## по теме «Использование сетевых диагностических утилит: ping, nslookup, tracert»

**Цель:** научиться использовать диагностические утилиты TCP/IP в ОС Windows

### ДИАГНОСТИЧЕСКИЕ УТИЛИТЫ TCP/IP

В состав TCP/IP входят диагностические утилиты, предназначенные для проверки конфигурации стека и тестирования сетевого соединения.

| Утилита | Применение |
|---|---|
| hostname | Выводит имя локального хоста. Используется без параметров. |
| ipconfig | Выводит значения для текущей конфигурации стека TCP/IP: IP-адрес, маску подсети, адрес шлюза по умолчанию, адреса WINS (Windows Internet Naming Service) и DNS (Domain Name System) |
| ping | Осуществляет проверку правильности конфигурирования TCP/IP и проверку связи с удаленным хостом. |
| tracert | Осуществляет проверку маршрута к удаленному компьютеру путем отправки эхо-пакетов протокола ICMP (Internet Control Message Protocol). Выводит маршрут прохождения пакетов на удаленный компьютер. |
| arp | Выводит для просмотра и изменения таблицу трансляции адресов, используемую протоколом разрешения адресов ARP (Address Resolution Protocol - определяет локальный адрес по IP-адресу) |
| route | Модифицирует таблицы маршрутизации IP. Отображает содержимое таблицы, добавляет и удаляет маршруты IP. |
| netstat | Выводит статистику и текущую информацию по соединению TCP/IP. |
| nslookup | Осуществляет проверку записей и доменных псевдонимов хостов, доменных сервисов хостов, а также информации операционной системы, путем запросов к серверам DNS. |

### 1. ТЕСТИРОВАНИЕ СВЯЗИ С ИСПОЛЬЗОВАНИЕМ УТИЛИТЫ *PING*.

Утилита ***ping*** (Packet Internet Grouper) используется для проверки конфигурирования TCP/IP и диагностики ошибок соединения. Она определяет доступность и функционирование конкретного хоста. Использование ping лучший способ проверки того, что между локальным компьютером и сетевым хостом существует маршрут. Хостом называется любое сетевое устройство (компьютер, маршрутизатор), обменивающееся информацией с другими сетевыми устройствами по TCP/IP.

Команда ping проверяет соединение с удаленным хостом путем отправки к этому хосту эхо-пакетов ICMP и прослушивания эхо-ответов. Ping ожидает каждый посланный пакет и печатает количество переданных и принятых пакетов.

Каждый принятый пакет проверяется в соответствии с переданным сообщением. Если связь между хостами плохая, из сообщений ping станет ясно, сколько пакетов потеряно.

По умолчанию передается 4 эхо-пакета длиной 32 байта (возможны и другие варианты значения по умолчанию) - периодическая последовательность символов алфавита в верхнем регистре. Ping позволяет изменить размер и количество пакетов, указать, следует ли записы-

вать маршрут, который она использует, какую величину времени жизни (ttl) устанавливать, можно ли фрагментировать пакет и т.д.. При получении ответа в поле time указывается, за какое время (в миллисекундах) отправленный пакет доходит до удаленного хоста и возвращается назад.

Так как значение по умолчанию для ожидания отклика равно 1 секунде, то все значения данного поля будут меньше 1000 миллисекунд.

Если вы получаете сообщение «Request time out» (Превышен интервал ожидания), то, возможно, если увеличить время ожидания отклика, пакет дойдет до удаленного хоста. Это можно сделать с помощью ключа –w.

Ping можно использовать для тестирования как имени хоста (DNS или NetBIOS), так и его IP-адреса. Если ping с IP-адресом выполнилась успешно, а с именем – неудачно, это значит, что проблема заключается в распознавании соответствия адреса и имени, а не в сетевом соединении.

**Утилита ping используется следующими способами**:

1) Для проверки того, что TCP/IP установлен и правильно сконфигурирован на локальном компьютере, в команде ping задается адрес петли обратной связи (loopback address):

**ping 127.0.0.1**

Если тест успешно пройден, то вы получите следующий ответ:

Ответ от 127.0.0.1: число байт=32 время<1мс TTL=128
Ответ от 127.0.0.1: число байт=32 время<1мс TTL=128
Ответ от 127.0.0.1: число байт=32 время<1мс TTL=128
Ответ от 127.0.0.1: число байт=32 время<1мс TTL=128

2) Чтобы убедиться в том, что компьютер правильно добавлен в сеть и IP-адрес не дублируется, используется IP-адрес локального компьютера:

**ping IP-адрес_локального_хоста**

3) Чтобы проверить, что шлюз по умолчанию функционирует и что можно установить соединение с любым локальным хостом в локальной сети, задается IP-адрес шлюза по умолчанию:

**ping IP-адрес_шлюза**

4) Для проверки возможности установления соединения через маршрутизатор в команде ping задается IP-адрес удаленного хоста: **ping IP-адрес_удаленного хоста**

**СИНТАКСИС:**

ping [-t] [-a] [-n count] [-l length] [-f] [-i ttl] [-v tos] [-r count] [-s count] [ [-j host-list] | [-k host-list] ] [-w timeout] destination-list

**Параметры:**

**-t** выполняет команду ping до прерывания. Control-Break - посмотреть статистику и продолжить. Control-C - прервать выполнение команды;

**-a** позволяет определить доменное имя удаленного компьютера по его IP-адресу;

**-n count** посылает количество пакетов ECHO, указанное параметром count;

**-l length** посылает пакеты длиной length байт (максимальная длина 8192 байта);

**-f** посылает пакет с установленным флагом «не фрагментировать». Этот пакет не будет фрагментироваться на маршрутизаторах по пути своего следования;

**-i ttl** устанавливает время жизни пакета в величину ttl (каждый маршрутизатор уменьшает ttl на единицу);

**-v tos** устанавливает тип поля «сервис» в величину tos;
**-r count** записывает путь выходящего пакета и возвращающегося пакета в поле записи пути. Count - от 1 до 9 хостов;
**-s count** позволяет ограничить количество переходов из одной подсети в другую (хопов). Count задает максимально возможное количество хопов;
**-j host-list** направляет пакеты с помощью списка хостов, определенного параметром host-list. Последовательные хосты могут быть отделены промежуточными маршрутизаторами (гибкая статическая маршрутизация). Максимальное количество хостов в списке, позволенное IP, равно 9;
**-k host-list** направляет пакеты через список хостов, определенный в host-list. Последовательные хосты не могут быть разделены промежуточными маршрутизаторами (жесткая статическая маршрутизация). Максимальное количество хостов – 9;
**-w timeout** указывает время ожидания (timeout) ответа от удаленного хоста в миллисекундах (по умолчанию – 1сек);
**destination-list** указывает удаленный хост, к которому надо направить пакеты ping.

***Пример использования утилиты ping:***

```
C:\WINDOWS>ping –n 10 www.netscape.com
Обмен пакетами с www.netscape.com [205.188.247.65] по 32 байт:
Ответ от 205.188.247.65: число байт=32 время=194мс TTL=48
Ответ от 205.188.247.65: число байт=32 время=240мс TTL=48
Ответ от 205.188.247.65: число байт=32 время=173мс TTL=48
Ответ от 205.188.247.65: число байт=32 время=250мс TTL=48
Ответ от 205.188.247.65: число байт=32 время=187мс TTL=48
Ответ от 205.188.247.65: число байт=32 время=239мс TTL=48
Ответ от 205.188.247.65: число байт=32 время=263мс TTL=48
Ответ от 205.188.247.65: число байт=32 время=230мс TTL=48
Ответ от 205.188.247.65: число байт=32 время=185мс TTL=48
Ответ от 205.188.247.65: число байт=32 время=406мс TTL=48
Статистика Ping для 205.188.247.65:
Пакетов: послано = 10, получено = 10, потеряно = 0 (0% потерь)
Приблизительное время передачи и приема:
Наименьшее = 173мс, наибольшее = 406мс, среднее =236мс
```

В случае невозможности проверить доступность хоста утилита выводит информацию об ошибке. Ниже приведен пример ответа утилиты ping при попытке послать запрос на несуществующий хост.

```
Обмен пакетами с 172.16.6.21 по 32 байт:
Превышен интервал ожидания для запроса.
Статистика Ping для 172.16.6.21:
Пакетов: отправлено = 4, получено = 0, потеряно = 4 (100% потерь),
Приблизительное время передачи и приема:
наименьшее = 0мс, наибольшее = 0мс, среднее = 0мс
```

Утилита сообщает не об отсутствии хоста, а о том, что за отведенное время не был получен

ответ на посланный запрос. Причиной этого не обязательно является отсутствие хоста в сети. Проблема может крыться в сбоях связи, перегрузке или неправильной настройке маршрутизаторов и т. п. Ошибка «сеть недоступна» (network unreachable) прямо указывает на проблемы маршрутизации.

## 2. ИЗУЧЕНИЕ МАРШРУТА МЕЖДУ СЕТЕВЫМИ СОЕДИНЕНИЯМИ С ПОМОЩЬЮ УТИЛИТЫ *TRACERT.*

**Tracert** - это утилита трассировки маршрута. Она использует поле TTL (time-to-live, время жизни) пакета IP и сообщения об ошибках ICMP для определения маршрута от одного хоста до другого.

Утилита tracert может быть более содержательной и удобной, чем ping, особенно в тех случаях, когда удаленный хост недостижим.

С помощью нее можно определить район проблем со связью (у Internet-провайдера, в опорной сети, в сети удаленного хоста) по тому, насколько далеко будет отслежен маршрут. Если возникли проблемы, то утилита выводит на экран звездочки (*), либо сообщения типа «Destination net unreachable», «Destination host unreachable», «Request time out», «Time Exeeded».

**Утилита tracert работает следующим образом:**

посылается по 3 пробных эхо-пакета на каждый хост, через который проходит маршрут до удаленного хоста. На экран при этом выводится время ожидания ответа на каждый пакет (Его можно изменить с помощью параметра -w). Пакеты посылаются с различными величинами времени жизни. Каждый маршрутизатор, встречающийся по пути, перед перенаправлением пакета уменьшает величину TTL на единицу. Таким образом, время жизни является счетчиком точек промежуточной доставки (хопов). Когда время жизни пакета достигнет нуля, предполагается, что маршрутизатор пошлет в компьютер-источник сообщение ICMP “Time Exeeded” (Время истекло). Маршрут определяется путем посылки первого эхо-пакета с TTL=1. Затем TTL увеличивается на 1 в каждом последующем пакете до тех пор, пока пакет не достигнет удаленного хоста, либо будет достигнута максимально возможная величина TTL (по умолчанию 30, задается с помощью параметра -h).

Маршрут определяется путем изучения сообщений ICMP, которые присылаются обратно промежуточными маршрутизаторами.

Примечание: некоторые маршрутизаторы просто уничтожают пакеты с истекшим TTL и не будут видны утилите tracert.

**Синтаксис:**

tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout] имя_целевого_хоста

**Параметры:**

**-d** указывает, что не нужно распознавать адреса для имен хостов;

**-h maximum_hops** указывает максимальное число хопов для того, чтобы искать цель;

**-j host-list** указывает нежесткую статическую маршрутизацию в соответствии с host-list;

**-w timeout** указывает, что нужно ожидать ответ на каждый эхо-пакет заданное число мсек.

## 3. УТИЛИТА *NSLOOKUP.*

Утилита **nslookup** предназначена для диагностики службы DNS, в простейшем случае - для выполнения запросов к DNS-серверам на разрешение имен в IP-адреса.

**В общем случае утилита позволяет просмотреть любые записи DNS-сервера:**

*A* – каноническое имя узла, устанавливает соответствие доменного имени ip-адресу.

*SOA* – начало полномочий, начальная запись, единственная для зоны;

*MX* – почтовые серверы (хосты, принимающие почту для заданного домена);

*NS* – серверы имен (содержит авторитетные DNS-серверы для зоны);

*PTR* – указатель (служит для обратного преобразования ip-адреса в символьное имя хоста)

и т. д.

Утилита nslookup достаточно сложна и содержит свой собственный командный интерпретатор.

В простейшем случае (без входа в командный режим) утилита **nslookup** имеет следующий

**Синтаксис:**

nslookup хост [сервер]

**Параметры:**

*Хост* DNS-имя хоста, которое должно быть преобразовано в IP-адрес.

*Сервер* Адрес DNS-сервера, который будет использоваться для разрешения имени. Если этот параметр опущен, то будут последовательно использованы адреса DNS-серверов из параметров настройки протокола TCP/IP.

***Примеры использования утилиты nslookup:***

1. Получение списка серверов имен для домена yandex.ru без входа в командный режим (с использованием ключей).

```
C:\> nslookup -type=ns yandex.ru
Server:  dns01.catv.ext.ru
Address:  217.10.44.35
Non-authoritative answer:
yandex.ru       nameserver = ns4.yandex.ru
yandex.ru       nameserver = ns5.yandex.ru
yandex.ru       nameserver = ns2.yandex.ru
yandex.ru       nameserver = ns1.yandex.ru

ns2.yandex.ru   internet address = 213.180.199.34
ns5.yandex.ru   internet address = 213.180.204.1
```

2. Получение адреса почтового сервера для домена yandex.ru.

```
C:\ >nslookup
Default Server:  dns01.catv.ext.ru
Address:  217.10.44.35
> set q=mx
> yandex.ru
Server:  dns01.catv.ext.ru
Address:  217.10.44.35
Non-authoritative answer:
yandex.ru       MX preference = 10, mail exchanger = mx2.yandex.ru
yandex.ru       MX preference = 10, mail exchanger = mx3.yandex.ru
```

```
yandex.ru       MX preference = 10, mail exchanger = mx1.yandex.ru
yandex.ru       nameserver = ns2.yandex.ru
yandex.ru       nameserver = ns1.yandex.ru
yandex.ru       nameserver = ns4.yandex.ru
yandex.ru       nameserver = ns5.yandex.ru
mx1.yandex.ru   internet address = 77.88.21.89
mx2.yandex.ru   internet address = 93.158.134.89
mx3.yandex.ru   internet address = 213.180.204.89
ns2.yandex.ru   internet address = 213.180.199.34
ns4.yandex.ru   internet address = 77.88.19.60
ns5.yandex.ru   internet address = 213.180.204.1
>
```

Указав ключ type=any, можно получить все записи о узле или домене. Ключи querytype, t, q эквивалентны type.

**Задание 1. Тестирование связи с помощью утилиты ping.**

1. Проверьте правильность установки и конфигурирования TCP/IP на локальном компьютере.
2. Проверьте функционирование основного шлюза, послав 5 эхо-пакетов длиной 64 байта.
3. Проверьте возможность установления соединения с удаленным хостом.
4. С помощью команды ping проверьте адреса, данные преподавателем и для каждого из них отметьте время отклика. Попробуйте изменить параметры команды ping таким образом, чтобы увеличилось время отклика. Определите IP-адреса узлов.

**Задание 2. Получение DNS-информации с помощью nslookup.**

1. Узнайте ip-адреса узлов, данные преподавателем.
2. Узнайте авторитетные (компетентные) сервера для этих узлов.

**Задание 3. Определение пути IP-пакета.**

С помощью команды tracert проверьте для перечисленных ниже адресов, через какие промежуточные узлы идет сигнал. Изучите ключи команды.

a) pkjt.karelia.ru

b) moodle.lm.interso.ru

## Практическая работа №7
## по теме «Мониторинг состояния элементов сети»

**Цель:** научиться выполнять мониторинг сетевых подключений.

1. Запустите оснастку **Производительность** (***Пуск/Администрирование/Проивзводительность***).

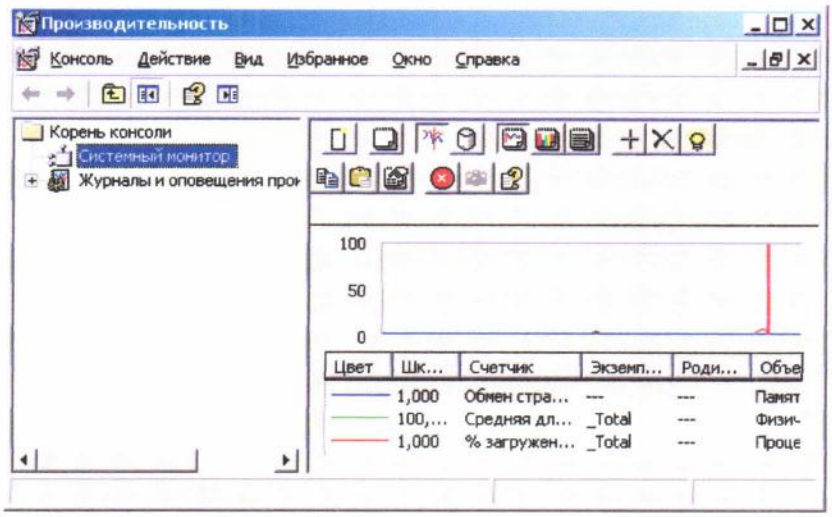



*Рисунок 1. - Оснастка Производительность*

**2. Удалите все счетчики из системного монитора:**

- активируйте **Системный монитор** в левой части окна **Производительность**;
- откройте диалоговое окно свойств **Системного монитора** кнопкой ***Свойства***  ;
- перейдите на вкладку **Данные**;
- выделите один из счетчиков и удалите его кнопкой ***Удалить***;
- аналогично удалите все остальные счетчики.

**3. Добавьте счетчик активных подключений TCP:**

- активируйте добавление счетчика кнопкой Добавить;
- выберите в раскрывающемся списке Объект – TCPv4;
- выберите в списке Выбрать счетчик из списка – Активных подключений;
- просмотрите информацию о добавляемом счетчике, щелкнув по кнопке Объяснение;
- добавьте счетчик кнопкой Добавить.

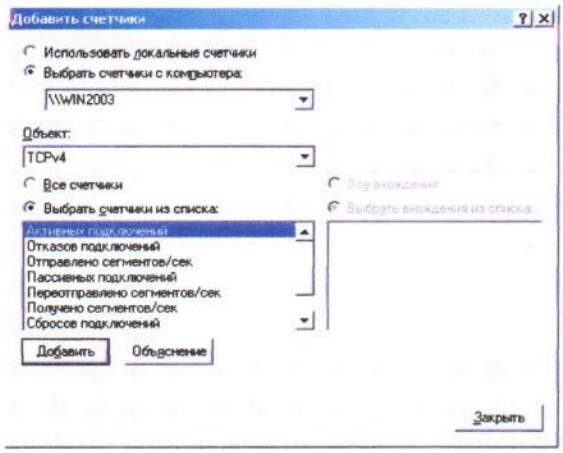



*Рисунок 2 - Добавление счетчика.*

- самостоятельно добавьте счетчик ***Всего байт/сек*** для объекта ***Сервер***;
- закройте окно добавления счетчиков кнопкой ***Закрыть***.

4. Закройте диалоговое окно свойств **Системного монитора** кнопкой ***ОК***.
   *В правой области начнет отображаться информация добавленных счетчиков в графическом виде.*

5. Переключите вид отображения информации счетчиков в текстовый вид кнопкой ***Просмотр отчета***  на панели инструментов.

6. Настройте автоматический сбор информации о загруженности сервера в период **с** 8.00 **до** 17.00:
- активируйте раздел **Журналы счетчиков** в левой части окна **Производительность**;
- активируйте создание новых параметров журнала (***Действие/Новые параметры журнала***);
- введите название журнала в поле **Имя** - *Дневная нагрузка* и подтвердите кнопкой ***ОК***;
- добавьте объект **Сервер**:
  - откройте окно добавления объектов кнопкой ***Добавить объект***;
  - выделите в списке **Объект** – *Сервер*;
  - добавьте объект кнопкой ***Добавить***;
  - закройте окно добавления объектов кнопкой ***Закрыть***;
- аналогично добавьте объект **Сетевой интерфейс**;
- установите время сбора данных:
  - перейдите на вкладку **Расписание**;
  - установите в поле **Время** – *8.00*;
  - установите время остановки – *17.00*;
- закройте диалоговое окно параметров нового журнала кнопкой ***ОК***. *В правой части окна* ***Производительность*** *появится новый журнал. Просмотреть результат работы журнала можно в папке* ***C:\perflogs***.

7. Настройте оповещение, если количество доступной памяти станет менее ***100 Мб***.
- активируйте раздел **Оповещения** в левой части оснастки **Производительность**;
- откройте диалоговое окно **Новые параметры оповещения** (***Действия/Новые параметры оповещения***);
- введите **имя новых параметров** - *Мало памяти* и подтвердите ввод кнопкой ***ОК***;

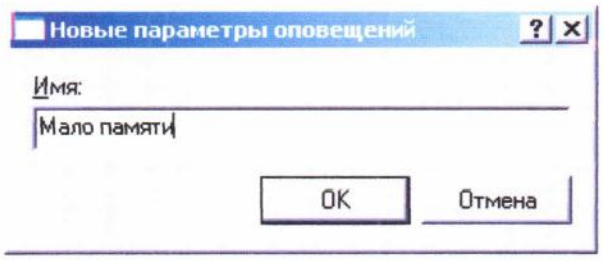



*Рисунок 3 - Ввод имени новых параметров оповещения.*

- введите в поле **Комментарий** – *Оповещение о малом количестве оперативной памяти*;
- добавьте счетчик ***Доступно МБ*** для объекта **Память**;

- введите в поле **Порог** значение, при котором должно срабатывать оповещение – *100*;

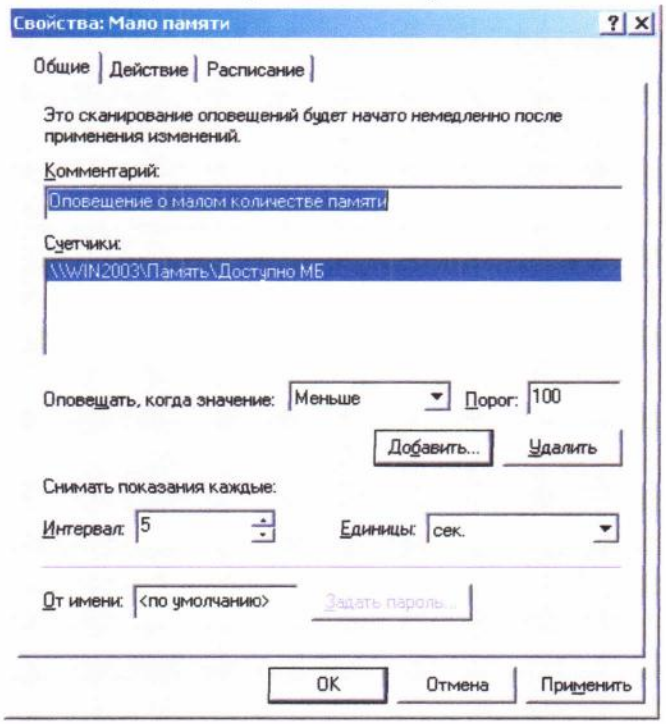



*Рисунок 4 - Установка параметров оповещения.*

- задайте действие, которое должно срабатывать при установленном условии:
  - перейдите на вкладку **Действие**;
  - установите флажок *Послать сетевое сообщение* и введите в поле текст сообщения - *Слишком мало памяти*;
- завершите настройку оповещения кнопкой ***ОК***.

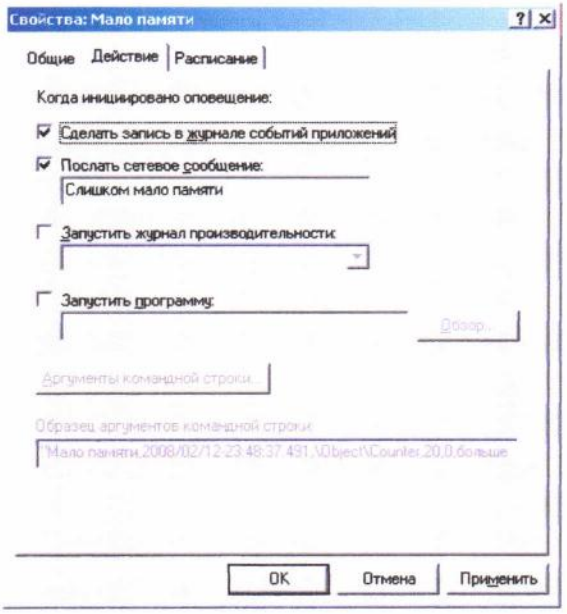



*Рисунок 5 - Диалоговое окно свойств параметров оповещения.*

Запишите выводы по выполнению данной работы в соответствии с поставленной целью.

**Практическая работа № 8**
**по теме «Механизмы резервного копирования данных**
**в операционной системе Windows 2003 Server»**

**Цель работы:** получить навыки резервного копирования системы, используя стандартные утилиты Windows Server 2003.

## БАЗОВЫЕ ПОНЯТИЯ СЛУЖБЫ РЕЗЕРВНОГО КОПИРОВАНИЯ

### Типы резервного копирования

Утилитой *ntbackup* можно создавать резервные копии различных типов. Рассмотрим их отличительные особенности и различные варианты их применения.

***Обычный (Normal)***

При выполнении данного типа архивирования утилита *ntbackup* архивирует все файлы, отмеченные для архивации, при этом у всех заархивированных файлов очищается атрибут «Файл готов для архивирования». Данный вид архивирования необходим для создания еженедельных полных резервных копий каких-либо больших файловых ресурсов.

Если в компании или организации имеются достаточные ресурсы, то можно ежедневно осуществлять полное архивирование данных.

***Разностный (Differential)***

При выполнении Разностного архивирования утилита *ntbackup* из файлов, отмеченных для архивирования, архивирует только те, у которых установлен атрибут «Файл готов для архивирования», при этом данный атрибут не очищается. Использование Обычного и Разностного архивирования позволяет сэкономить пространство на носителях с резервными копиями и ускорить процесс создания ежедневных копий.

Например, если раз в неделю (как правило, в выходные дни) создавать Обычные копии, а в течение недели ежедневно (как правило, в ночное время) — Разностные, то получается выигрыш в объеме носителей для резервного копирования. При такой комбинации архивирования «Обычный + Разностный» процесс восстановления данных в случае утери информации потребует выполнения двух операций восстановления — сначала из последней Полной копии, а затем из последней Разностной резервной копии.

***Добавочный (Incremental)***

При выполнении Добавочного архивирования утилита *ntbackup* из файлов, отмеченных для архивирования, архивирует только те, у которых установлен атрибут «Файл готов для архивирования», при этом данный атрибут очищается. Использование Обычного (раз в неделю по выходным) и Добавочного (ежедневно в рабочие дни) архивирования также позволяет сэкономить пространство на носителях с резервными копиями и ускорить процесс создания ежедневных копий. Но процесс восстановления данных при использовании комбинации «Обычный + Добавочный» уже будет выполняться иначе: в случае утери информации для восстановления данных потребуется сначала восстановить данные из последней Полной копии, а затем последовательно из всех Добавочных копий, созданных после Полной копии.

***Копирующий (Copy)***

При таком типе архивирования утилита *ntbackup* заархивирует все отмеченные файлы, при этом атрибут «Файл готов для архивирования» остается без изменений.

***Ежедневный (Daily)***

Ежедневный тип архивирования создает резервные копии только тех файлов, которые были модифицированы в день создания резервной копии.

Два последних типа не используются для создания регулярных резервных копий. Их удобно применять в тех случаях, когда с какой-либо целью нужно сделать копию файловых ресурсов, но при этом нельзя нарушать настроенные регулярные процедуры архивирования.

**Разработка и реализация стратегии резервного копирования. Понятие плана архивации**

Для построения правильной и эффективной системы резервного копирования необходимо детально изучить и задокументировать все файловые ресурсы, используемые в компании, а затем тщательно спланировать стратегию резервного копирования и реализовать ее в системе. Для планирования стратегии необходимо ответить на следующие вопросы:

- какие именно ресурсы будут архивироваться;
- минимальный промежуток времени для восстановления данного ресурса при возникновении аварии;
- какой объем данных будет архивироваться;
- какова емкость носителей для хранения резервных копий и скорость записи на эти носители;
- сколько времени будет занимать архивирование каждого ресурса;
- как часто будет производиться архивация каждого ресурса;
- если резервные копии записываются на ленты, то как часто будет производиться перезапись лент;
- по какому графику будет производиться тестовое восстановление данных.

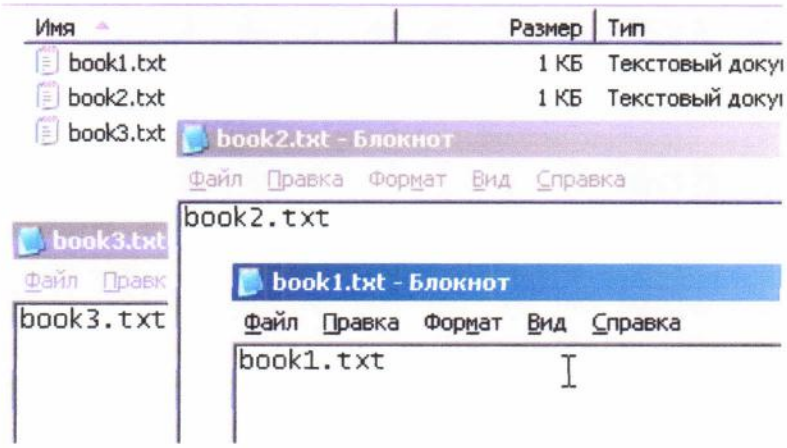
При ответе на эти вопросы будет спланирована потребность в количестве и емкости накопителей и устройств для выполнения резервных копий, требования к пропускной способности сети для создания резервных копий, график выполнения резервного копирования, план восстановления на случай аварии.

**Ход работы:**

**Создания задания на выполнения архивации данных**

1. Создать на диске «С» Вашего сервера каталог *backup* и *restore*;

2. В папке library, созданной в одной из предыдущих работ создать 3 текстовых файла с наименованиями *book1.txt*, *book2.txt* и *book3.txt*. Файлы должны содержать свое наименование.

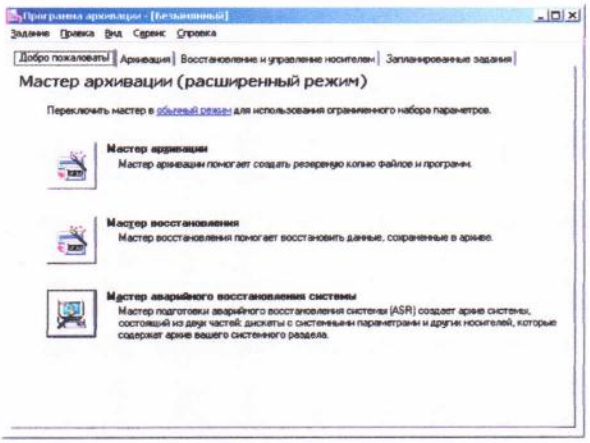



3. Запустить утилиту резервного копирования *ntbackup*.

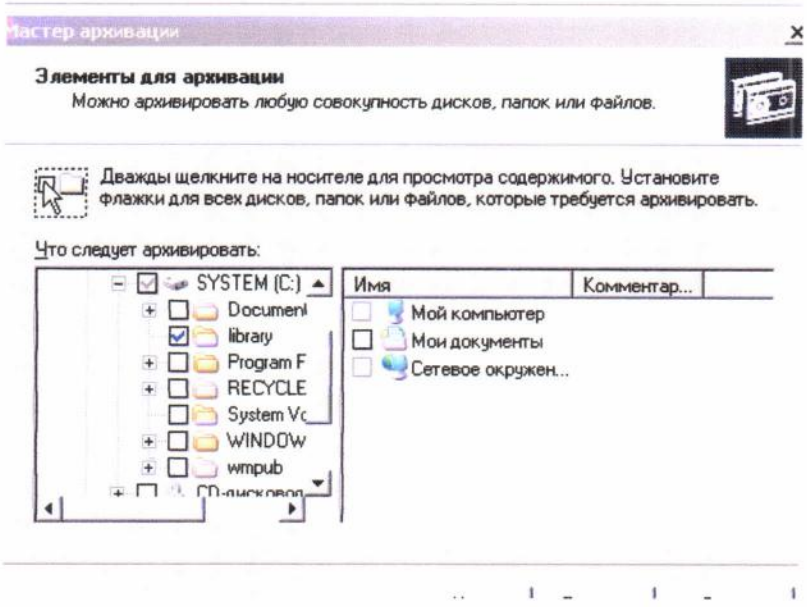
*Эту утилиту можно запустить из Главного меню системы (кнопка «Пуск» — «Все программы» — «Стандартные» — «Служебные» — «Архивация данных»), а можно запустить более быстро из командной строки (кнопка «Пуск» — «Выполнить» — «ntbackup» — кнопка «ОК»). При первом запуске утилиты рекомендуем убрать галочку у поля «Всегда запускать в режиме мастера».*

4. Запустить «Мастер архивации» (на закладке «Добро пожаловать» нажать кнопку «Мастер архивации».

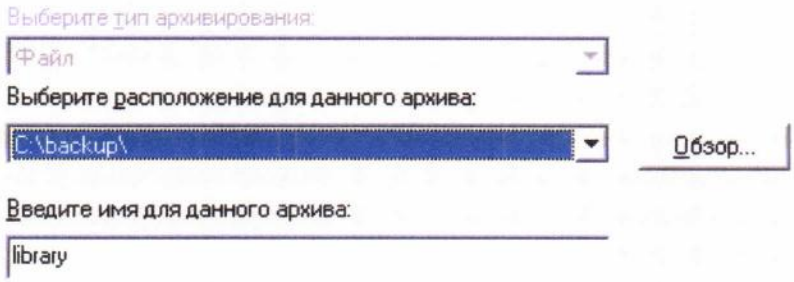
5. После запуска мастера нажмем кнопку «Далее» и выберем, что нам нужно архивировать, в данном примере — «Архивировать выбранные файлы, диски или сетевые данные»



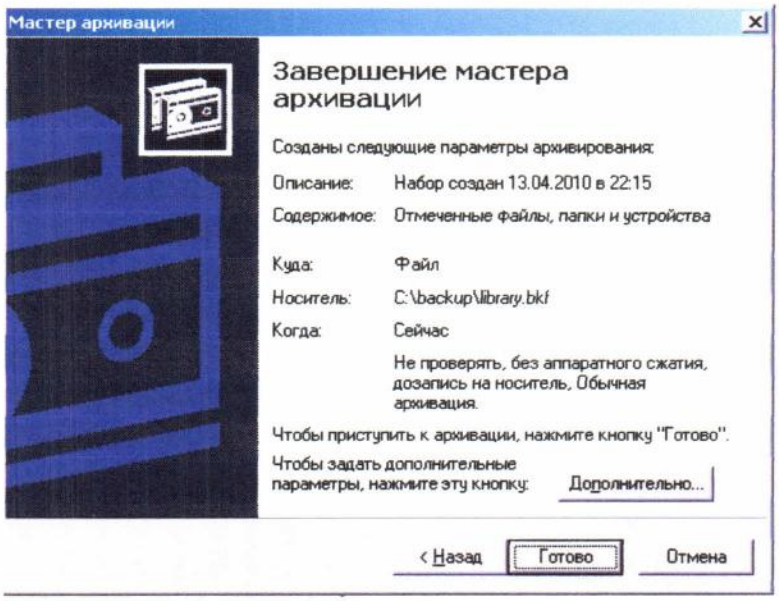
6. Выберем для архивирования папку library.



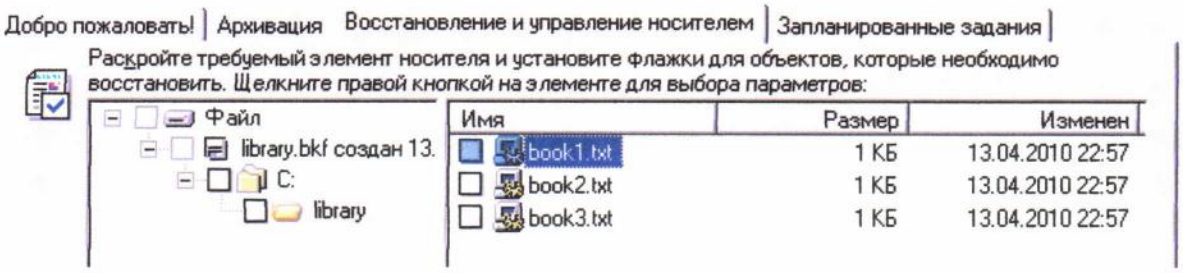

7. Выберем место для создания резервной копии, создадим файл с именем *library*, этому файлу автоматически будет назначено расширение «*.bkf*»




8. На данном этапе нажмем кнопку «Готово».

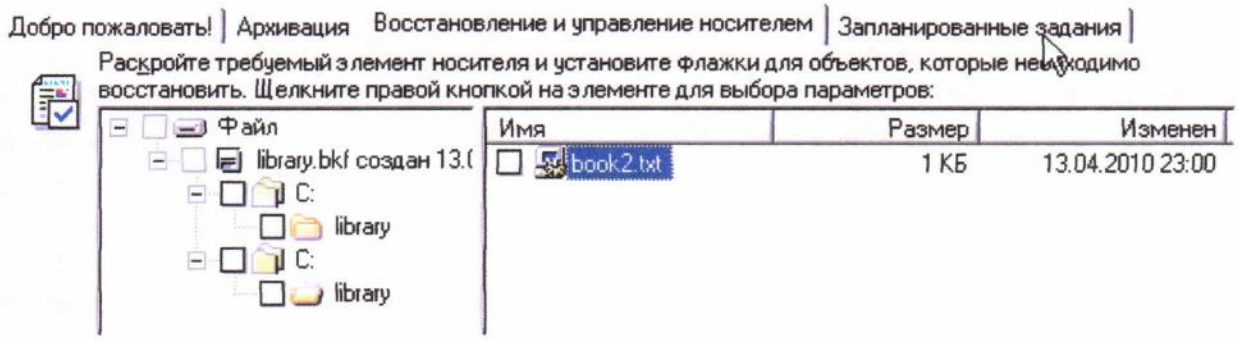


9. Проверяем полученный результат.




10. Вносим изменение в файл *book1.txt* и *book2.txt*, у файла *book1.txt* убираем атрибут «Файл готов для архивирования», а *book3.txt* - удаляем.

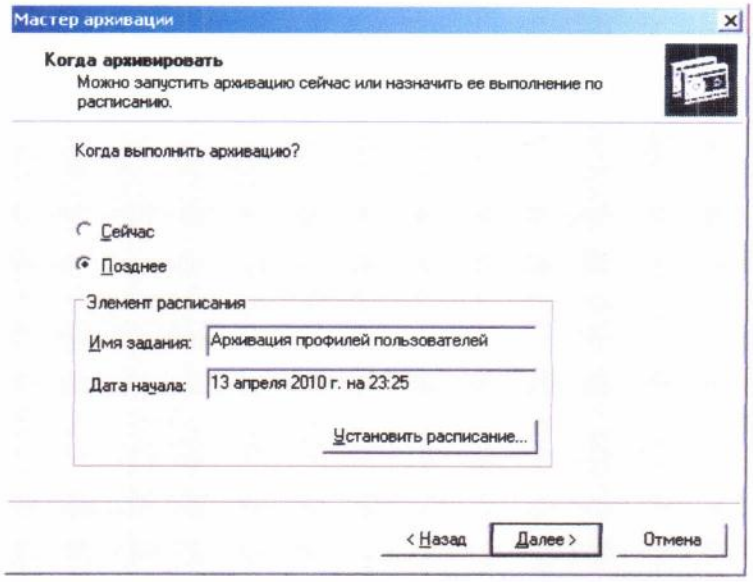
11. Запускаем снова процесс архивации, но на 8 этапе нажмем кнопку «Дополнительно», чтобы задать дополнительные параметры и выбираем тип архивации «Добавочный». Далее все пункты по умолчанию, но при этом не забывайте запоминать, что Вы делаете. Проверяем полученный результат. Почему он такой?




12. Восстановите файл *book3.txt*. Для этого выполните следующие действия:

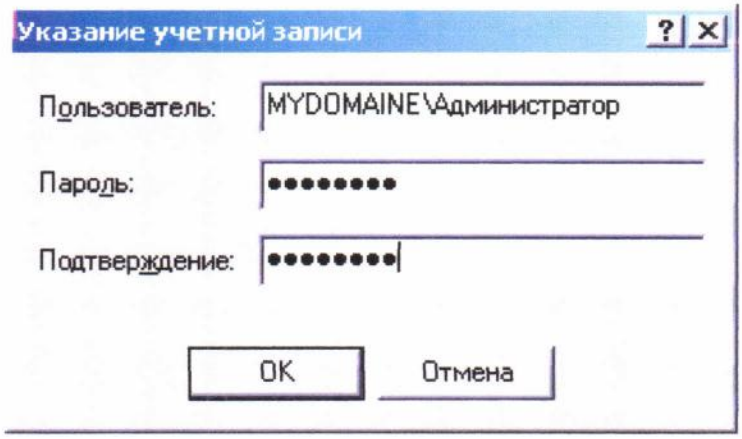
- Запустим утилиту резервного копирования *ntbackup*.
- Перейдем на закладку "Восстановление и управление носителем".
- После появления в списке архивных файлов нужного архива раскроем этот архив и выберем файлы для восстановления из резервной копии. При этом мы можем восстановить файлы в то место, где они были ранее ("Исходное размещение") или выбрать иной путь для их сохранения ("Альтернативное размещение"). Выберите папку *restore*.
- После определения всех параметров восстановления нажмем кнопку "Восстановить", утерянные данные будут восстановлены.

13. Создайте задания на выполнения архивации данных для папки *profiles*, используя выбор дополнительных возможностей:




- Выбираем тип архивирования (выберем «Обычный»).
- Ничего не меняем на странице «Способы архивации».На странице «Параметры архивации» можно выбрать замену существующих архивов или добавление архива (если файл с архивной копией уже существует).

14. На странице «Когда архивировать» задайте расписание для автоматического создания резервной копии — выберите вариант «Позднее» и задайте расписание архивирования, чтобы архивирование происходило по всем рабочим дням недели. Время начала установите, исходя из текущего времени системы + пять минут.
15. Нажмите далее. Система запросит имя и пароль пользователя, с чьими полномочиями будет выполняться задание архивирования. Рекомендуем для выполнения заданий резервного копирования создать специальные учетные записи, обладающие достаточными правами (как минимум члены группы «Операторы архива»).



16. Нажмем кнопку «Готово», задание будет создано, и оно появится в списке «Назначенных заданий». Теперь оно будет выполняться регулярно в соответствии с расписанием.
17. Завершите сеанс администратора, ожидайте до завершения задания. После проверьте результат.

По окончании выполнения работы с помощью скриншотов оформить работу в соответствующей рамке и предоставить отчёт преподавателю.

## Практическая работа № 9

## по теме «Установка антивирусного программного обеспечения»

**Цель**: ознакомиться с процессом инсталляции, принципами работы и управлением Антивирусом Касперского для Microsoft Windows 2000 Professional.

**Программное обеспечение:** операционная система: Microsoft Windows XP Professional

Антивирус Касперского - это программный продукт, предназначенный для комплексной защиты рабочей станции от угроз связанных с работой в локальных вычислительных сетях и в интернет.

Продукт предназначен для защиты рабочих станций в корпоративной сети под управлением Kaspersky Administration Kit. При необходимости, Антивирус Касперского может работать автономно, в отсутствие сервера управления, без ограничения функций защиты.

Продукт объединяет функциональность антивируса, брандмауэра, антиспама и антибаннера и обеспечивает защиту компьютера пользователя от следующих угроз:

- Вирусов
- Вредоносных и потенциально опасных программ
- Сетевых атак
- Интернет мошенничества
- Нежелательной интернет рекламы
- Спама

**Для выполнения поставленных задач, в продукте реализованы следующие функции:**

- Защита файловой системы в режиме реального времени - перехватываются все операции с файлами на жестких, сменных и сетевых дисках. Объекты, с которыми выполняются операции, проверяются на наличие вредоносного кода
- Защита электронной почты в режиме реального времени - проверяются все входящие и исходящие электронные письма по протоколам POP3, SMTP, IMAP, NNTP; обеспечивается защита от нежелательных почтовых сообщений (спама)
- Защита при работе в интернет - проверка HHTP трафика, блокировка выполнения опасных скриптов (при помощи поведенческого блокиратора), блокировка рекламных баннеров и всплывающих окон, защита от фишинг-атак
- Контроль активности приложений - поведенческий блокиратор позволяющий противодействовать заражению и распространению еще не внесенных в базы вирусов и других вре-

доносных программ. Дополнительно обеспечивается защита системного реестра, контроль целостности приложений и блокировка опасных VBA скриптов

• Контроль сетевых соединений - Антивирус Касперского для Windows Workstations выполняет функции персонального брандмауэра, позволяет контролировать все сетевые соединения и фильтровать сетевые пакеты согласно установленным пользователем правилам

• Защита от сетевых атак - ведется постоянный мониторинг и анализ сетевой активности компьютера пользователя. В случае выявления сетевой активности классифицируемой как атака, атакующий компьютер блокируется на определенный период времени

• Поиск вирусов - приложение позволяет по требованию пользователя или по расписанию осуществлять поиск вирусов среди стандартных, или указанных пользователем объектов на жестких, сменных и сетевых дисках, а также в оперативной памяти компьютера

• Обновление сигнатур угроз - для обеспечения эффективной защиты от новых типов вирусов производится регулярное обновлений антивирусных баз, адресов потенциально опасных интернет ресурсов и сигнатур сетевых атак.

Новая технология позволяет существенно уменьшить размер обновлений и тем самым уменьшить время их загрузки

• Аварийная проверка системы - Антивирус Касперского для Windows Workstations предоставляет возможность создавать диски аварийной проверки, которые, в случае потери работоспособности системы в результате вирусной атаки, позволяют выполнить проверку и лечение компьютера

## УСТАНОВКА

Перед началом установки необходимо убедиться, что параметры операционной системы соответствуют системным требованиям Антивируса Касперского для Windows Workstations и установка производится под учетной записью обладающей правами администратора. В случае невыполнения этих условий мастер установки выдает сообщение об ошибке, и установка прерывается.

Одновременная работа Антивируса Касперского для Windows Workstations с другими антивирусами и брандмауэрами может привести к возникновению ошибок, снижению производительности или полной потере работоспособности операционной системы.

Дистрибутив продукта доступен в виде инсталляционного файла в формате Microsoft installer - например, kav6ws.ru.msi. Где "kav" - аббревиатура названия продукта Kaspersky Anti-Virus, "6" - версия, "ws" - тип систем, для которых предназначен продукт (Workstations), "ru" - язык интерфейса.

При исполнении файла kav6ws.ru.msi, запускается мастер установки приложения, и появляется окно приветствия. Для продолжения установки нужно нажать кнопку Далее. При нажатии кнопки Отмена установка будет прервана.

В случае если установка выполняется на компьютер под управлением Microsoft Windows XP Service Pack 2 с включенным брандмауэром Windows, необходимо выбрать режим взаимодействия Антивируса Касперского для Windows Workstations с брандмауэром:

• Отключить сетевой экран Microsoft Windows - при выборе этого пункта брандмауэр Windows будет автоматически отключен, и контроль всех сетевых соединений будет выпол-

няться средствами Антивируса Касперского для Windows Workstations

• Использовать сетевой экран Microsoft Windows - в этом режиме контроль сетевых соединений выполняется брандмауэром Windows. При этом по умолчанию компонент Анти-Хакер будет отключен

После окончания копирования файлов открывается окно с сообщением об успешном завершении установки. Далее необходимо произвести предварительную настройку установленного продукта. Для перехода к этапу предварительной настройки следует нажать кнопку Далее.

## РЕЗУЛЬТАТ УСТАНОВКИ

После успешно завершенной установки на компьютере пользователя появляется папка Program Files\Kaspersky Lab\Kaspersky Ati-Virus for Windows Workstations\, - которая содержит файлы и программные модули антивируса, а также используемые файлы графической оболочки (каталог Skin) и каталог с сопутствующей документацией (Doc).

**Также в процессе установки создается папка:**

• Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP6\ для Microsoft Windows 2000/XP

• Windows\All Users\Application Data\Kaspersky Lab\AVP6\ для Microsoft Windows 98/ME

• WINNT\All Users\Application Data\Kaspersky Lab\AVP6\ для Microsoft Windows NT

с подкаталогами, в которых хранятся:

• файлы, помещенные в Резервное хранилище (каталог Backup)

• антивирусные базы (Bases)

• пользовательские настройки (каталог Data)

• служебные файлы компонента Проактивная защита (PdmHist)

• файлы Карантина (Quarantine)

• отчеты (Reports)

• служебные файлы компонентов продукта (Dskm)

В реестр Windows в процессе установки Антивируса Касперского для Windows Workstations вносится ветвь HKLM\SOFTWARE\KasperskyLab\.

В каталог операционной системы Windows\System32\drivers\ (или Winnt\System32\drivers\) устанавливаются драйвера:

• kl1.sys - отвечает за перехват сетевого трафика

• klick.sys - вспомогательный драйвер kl1.sys, обеспечивает перехват пакетов сетевого уровня

• klin.sys - вспомогательный драйвер kl1.sys, обеспечивает перехват пакетов транспортного уровня

• klop.sys - вспомогательный драйвер kl1.sys, отслеживает использование лицензионных ключей в локальной сети

• klif.sys - осуществляет перехват файловых операций

Для Microsoft Windows NT-подобных операционных систем дополнительно в реестр вносятся ветви, отвечающие за параметры запуска службы Kaspersky Anti-Virus 6.0 и драйверов kl1.sys и klif.sys. Одноименные ветви создаются в HKLM\SYSTEM\CurrentControlSet\Services.

Также в реестре в список программ автозапуска добавляется ключ AVP со значением C:\Program Files\Kaspersky Lab\Kaspersky Anti-Virus 6.0 for Workstation\avp.exe.

В список локальных служб добавляется служба Kaspersky Anti-Virus 6.0 запускаемая автоматически под системной учетной записью. Исполняемый файл службы avp.exe с ключом -r

При запуске продукта запускается два процесса avp.exe. Один из них запущен от имени системы и отвечает службе Kaspersky Anti-Virus 6.0, второй от имени пользователя - это процесс интерфейса.

В контекстном меню файлов и папок появляется пункт Проверить на вирусы, с помощью которого можно запустить задачу проверки по требованию выбранного объекта.

В главное меню Windows в раздел Программы добавляется папка Антивирус Касперского для Windows Workstations, в которой находятся:

• Ярлык для запуска продукта

• Ярлык для запуска мастера установки Антивируса Касперского для Windows Workstations

•Ярлык для доступа к справочной системе Антивируса Касперского для Windows Workstations

• Ссылка на лицензионное соглашение

• Ссылка на официальный сайт Лаборатории Касперского

На системной панели Windows появляется значок антивируса, с помощью которого пользователь может открыть графически интерфейс продукта. Значок также является индикатором состояния Антивируса Касперского для Windows Workstations.

**Задание:**

1. Установите локально Антивирус Касперского на рабочую станцию. Место расположения дистрибутива и ключевого файла уточните у преподавателя.

2. Убедитесь, что установка Антивируса Касперского прошла успешно, а компоненты защиты автоматически запустились при старте операционной системы. Запишите какие службы добавились, и какие процессы и задачи запускаются при старте Антивируса Касперского.

3. Откройте интерфейс **Антивируса** и ознакомьтесь с интерфейсом.

4. В корне диска C: создайте папку test_virus и скопируйте в нее содержимое аналогичной папки с компьютера преподавателя. Убедитесь, что зараженные объекты (вирус EICAR) блокируются.

5. Удалите содержимое папки test_virus на вашем компьютере, включите проверку архивов Файловым антивирусом и повторите копирование. Убедитесь в том, что зараженные архивы также не могут быть скопированы.

6. Протестируйте работу **Доверенной зоны**. Для этого отключите проверку Сетевых дисков в

Файловом антивирусе, затем внесите папку c:\test_virus в Доверенную зону и повторите копирование зараженных файлов с сетевого ресурса. Убедитесь, что копирование прошло успешно.

7. Изучите работу **Проактивной защиты**. Для этого откройте соответствующее окно настроек Антивируса Касперского, нажмите Настройка в разделе **Анализ активности приложений** и включите отслеживание запуска браузера с параметром.

8. Нажмите Пуск, Выполнить, в строке Открыть введите "%SystemDrive%\Program Files\Internet Explorer\IEXPLORE.EXE"

www.kaspersky.ru и нажмите кнопку ОК, для имитации запуска браузера с параметром сторонним приложением. Запишите результаты в протокол лабораторной работы

9. Включите **Мониторинг системного реестра**, и проверьте работу правил, отвечающих за автоматический запуск программ при загрузке операционной системы. Такой контроль позволяет заблокировать автозапуск вредоносных программ при старте системы, путем внесения соответствующего ключа в реестр.

10. Откройте редактор реестра regedit, и найдите ветвь HKLM\Software\Microsoft\Windows\CurrentVersion\Run\AVP6. Попробуйте удалить ветвь и убедитесь, что это невозможно. Внесите в протокол работы полученные сообщения

11. Откройте и самостоятельно изучите интерфейс компонента Анти-Хакер.

12. Протестируйте работу **Системы обнаружения вторжений** с помощью утилиты kltps.exe. Для продолжения работы разбейтесь по парам. Сначала первые номера будут имитировать сетевую атаку компьютеров вторых номеров, затем атаку на компьютеры первых номеров выполнят вторые номера.

13. **Первые номера**. Создайте в корне диска C:\ папку test и скопируйте в нее утилиту kltps.exe (местоположение утилиты уточните у преподавателя). В главном окне интерфейса Антивируса Касперского обратите внимание на секцию статус на панели результатов Анти-Хакера. Убедитесь, что Система обнаружения вторжений работает

14. В окне настройки **Анти-Хакера** в секции **Система обнаружения вторжений** уберите отметку с пункта **Включить систему обнаружения вторжений** и нажмите **Применить.** Нажмите Пуск, Выполнить. Наберите строку C:\test\kltps.exe 192.168.0.1 80 (здесь следует указать, IP адрес компьютера второго номера Вашей пары ) в поле Открыть окна Запуск программы и нажмите ОК.

15. **Вторые номера**. Убедитесь, что попытка атаки, выполненная с компьютера первого номера Вашей пары, зарегистрирована системой обнаружения вторжений на Вашем компьютере, открылось всплывающее окно с сообщением о блокировании атаки

16. Вернитесь к окну интерфейса Антивируса Касперского. Убедитесь, что счетчик заблокированных атак в блоке Статистика равен 1

17. Поменяйтесь местами и повторите действия, начиная с п.13.

18. Настройте задачу **Обновление для обновления из источника**, указанного преподавателем и запустите ее. Опишите в протоколе работы, какие изменения произошли в папке Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP6\Bases после успешного завершения задачи обновления.

19. Выполните задачу **Откат обновления антивирусных баз.** Опишите какие изменения

произошли в папке Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP6\Bases после успешного завершения задачи Откат обновления антивирусных баз.

20. Создайте задачу проверки по требованию папки Program Files с включенными технологиями iChecker(tm) и iSwift(tm). Выполните созданную задачу 3 раза подряд, каждый раз фиксируя время выполнения.

21. Создайте пользовательскую задачу проверки по требованию папки Program Files с выключенными технологиями iChecker(tm) и iSwift(tm). Выполните созданную задачу 3 раза подряд, каждый раз фиксируя время выполнения.

22. Проанализируйте полученные результаты. Есть ли разница? В чем она заключается? Как можно ее объяснить?

23. Создайте на своем компьютере папку test_virus1. Скопируйте в нее по одному файлу содержимое папки test_virus (ее местоположение уточните у преподавателя), не отключая системную Файловый Антивирус. Перечислите в протоколе лабораторной работы, какие файлы удалось скопировать и объясните почему.

24. Создайте на диске С: своего компьютера папку с названием test_virus4. Скопируйте в нее содержимое папки test_virus2, не отключая постоянную защиту. Месторасположение папки test_virus2 уточните у преподавателя. Опишите в протоколе лабораторной работы, какие изменения необходимо произвести в настройках Файлового Антивируса, для того чтобы скопировать все файлы, которые содержатся в папке test_virus2, без изменений в папку test_virus4.

25. Создайте пользовательскую задачу проверки по требованию папки test_virus2 и запустите ее. В окне Пожалуйста, введите пароль в поле Пароль введите "1" и нажмите ОК. По окончании проверки произведите обработку обнаруженных зараженных объектов. Ознакомьтесь с отчетом выполненной задачи, содержимым карантина и резервного хранилища. Опишите, по каким признакам найденные инфицированные и подозрительные файлы помещаются в карантин и в резервное хранилище, перечислите в протоколе лабораторной работы, какие действия возможны над объектами, помещенными в карантин, и над объектами, помещенными в резервное хранилище.

26. Экспортируйте отчет задачи проверки по требованию папки test_virus2 в файл, ознакомьтесь с получившимся файлом. Перечислите в протоколе лабораторной работы, в файлах каких форматов может быть сохранен файл отчета.

27. Не останавливая службу Антивируса Касперского измените системную дату на своем компьютере на 2 года вперед. Опишите в протоколе лабораторной работы, какие изменения произойдут с Антивирусом Касперского после изменения системной даты и истечения срока действия лицензионного ключа.

Результаты работы, оформленные в соответствии со стандартом, представить преподавателю для проверки.