МОСКОВСКИЙ АВТОМОБИЛЬНО-ДОРОЖНЫЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ (МАДИ)

«Автоматизированные системы управления»

ОСТРОУХ А.В.

МОНТАЖ И ТЕСТИРОВАНИЕ КОМПЬЮТЕРНЫХ СЕТЕЙ

Методические указания

Научно-инновационный центр

Красноярск, 2017

УДК 004.382.7

ББК 32.973.26

О79

Остроух А.В.

Монтаж и тестирование компьютерных сетей: методические указания [Электронный ресурс] / А.В. Остроух. – Электрон. текстовые дан. – Красноярск: Научно-инновационный центр, 2017. – 78 с.

ISBN 978-5-906314-61-1

DOI: 10.12731/asu.madi.ru/MTKS.2017.78

Методические указания содержат учебный материал по основам построения информационно-вычислительных сетей для укрупненной группы направлений подготовки 090000 – «Информатика и вычислительная техника».

В методических указаниях описаны основные модели, технологии доступа к среде передачи данных, а также их характеристики и область их применения. Даны практические рекомендации по планированию и монтажу структуры компьютерной сети, а также размещению сетевого оборудования.

Методические указния могут использоваться при подготовке бакалавров, специалистов, магистров и кадров высшей квалификации в области информационно-коммуникационных технологий, а также для повышения квалификации педагогических работников в системе профессионального образования.

УДК 372.8: 004.9

ББК 71.263.2: 32.97

ISBN 978-5-906314-61-1

Введение

Методические указания разработаны в соответствии с федеральными государственными образовательными стандартами (ФГОС) по направлениям подготовки, входящим в состав укрупненной группы 090000 – «Информатика и вычислительная техника».

Учебные материалы, изложенные в методических указаниях, помогут сформировать общепрофессиональную компетенцию:

- способность сопрягать аппаратные и программные средства в составе информационных и автоматизированных систем.

Перечень планируемых результатов обучения:

знать:

- основные модели, технологии и протоколы доступа к среде передачи данных, структуру протоколов доступа к среде;
- основные типы сред передачи данных, их характеристики, область их применения;
- принципы организации адресного пространства IPv4 и IPv6;

уметь:

- ориентироваться в стандартах IEEE 802;
- определять элементы структурированной кабельной системы организации, ограничения их применения;

владеть:

- способностью планировать структуру сети передачи данных.

1. Построение сетевой инфраструктуры

К поиску идеального решения для построения сетевой инфраструктуры, полностью отвечающей требованиям организации, необходимо подходить индивидуально, глубоко вникнув в исходные данные и возможности.

1.1. Помещение для серверного оборудования

Серверное помещение по праву можно назвать «сердцем» офиса. В этом помещении сконцентрировано оборудование, без которого уже сложно представить современный офис. Здесь располагаются коммутационные стойки, серверное оборудование, источники бесперебойного питания оборудования и т.д. В общем можно констатировать что серверная – это помещение специального назначения, в котором располагается телекоммуникационное оборудование и к которому предъявляется ряд определённых требований.

Сразу стоит оговориться, что организация серверного помещения – процесс не дешевый и к нему нужно подходить с чётким понимаем того, зачем Вы оборудуете серверную. Исходя из этого можно понять какой тип помещения и его размеры требуются. Достаточно ли одной комнаты, для централизованной установки оборудования, или лучше его разнести по небольшим настенным шкафам по всему офису. Всё зависит от поставленной задачи, от размеров, от конфигурации самого офиса.

Основные критерии, которые важно учесть при организации серверного помещения:

- эффективное, централизованное размещение оборудования;
- защита от несанкционированного доступа;
- удобная защита и эффективная защита от сбоев питания;
- соблюдение микроклимата.

В стандарте TIA-569 полностью описаны все требования к серверному помещению. Но далеко не всегда есть возможность следовать этому стандарту. Конечно, хорошо, когда ваша компания – собственник здания и вы можете выбрать подходящее для своих задач помещение и оборудовать его соответствующим образом, однако реальность такова, что большинство компаний малого и среднего

бизнеса арендуют помещение под свой офис и у них нет возможности следовать этому стандарту. Поэтому ниже будут предоставлены лишь общие рекомендации по выбору серверного помещения.

Начать следует с расположения помещения в офисе – идеальным вариантом расположения можно назвать помещение, которое будет равноудалено от противоположных концов вашего офиса, что впоследствии упростит организацию вычислительной сети. Высота потолка в помещении должна быть не менее 2,5 м, так как самым распространенным размером телекоммуникационной стойки является высота в 2100 мм. Кроме того, требуется около 500 мм свободного пространства над ней для эффективного отвода тепла от стойки.

В серверной не должно быть окон, так как они являются источники тепла в летнее время. Но и не стоит выбирать помещение в самой глубине здания, ведь нам нужно будет организовать кондиционирование помещения, а это значит, что потребуется сделать отвод жидкости от кондиционера.

Вообще, выбирая помещения для серверной, ни в коем случае нельзя забывать о **БЕЗОПАСНОСТИ**.

С одной стороны – помещение должно быть легко доступно для администраторов и/или авторизованных специалистов, с другой стороны – гарантировать защиту от несанкционированного доступа.

Источником опасности для оборудования служат трубопроводы и дренажные системы – необходимо заранее удостовериться что под фальш-потолком не проходит никаких коммуникаций, иначе вероятность затопления серверного помещения – крайне высока.

Следует обратить внимание на дверной проём, его размеры должны быть не менее 90x200 мм, иначе у вас появятся трудности с перемещением оборудования/стоек/шкафов.

1.2. Электропитание, освещение, охлаждение, пожаротушение

Как и во всём, что касается обеспечения доступности оборудования, стоит следовать правилу «всего по два» или N + 1, то же самое касается и **электропитания**. Будет очень хорошо, если вы сможете подвести питание к серверной от двух разных питающих кабелей, это поможет вам сохранить питание даже в случае выхода из строя одного из силовых кабелей, что впоследствии предотвратит отключение оборудования. И крайне важно помнить о необходимости

заземления оборудования, особенно если ваш офис располагается в достаточно старом здании.

Как правило, мало кто задумывается об **освещении** в серверной комнате, ведь свет там есть и так, только многие забывают о том, что в случае неполадок с электропитаним освещения в серверной так же не будет, что может усложнить аварийные работы (допустим демонтаж и вынос оборудования в случае затопления). Поэтому нужно задуматься и о том, каким образом вы можете организовать резервное освещение, незавязанное на основной электросети. Можно банально обойтись 2-3 (в зависимости от размеров серверной) фонарями дневного света на аккумуляторах, рассчитав объём аккумулятора исходя из приблизительно времени проведения аварийных работ, а так же небольшого запаса сверху.

Продумывая **систему охлаждения** серверной, стоит так же руководствоваться правилом «всего по два» или N + 1. Для охлаждения серверного помещения с потреблением меньше 5 кВт, вопрос охладления можно решить бытовыми кондиционерами, главное – установить их на 1 больше, чем требуется. В этом случае, уменьшается износ кондиционеров. Кондиционеры настраиваются на поочерёдную работу. Таким образом обеспечивается время на остановку работы кондиционера и время на ремонт сломавшегося кондиционера, без ухудшения качества охлаждения серверной. А также возможность стабильного охлаждения в случае резкого увеличения парка оборудования или при резком повышении температуры, в период жаркого лета. Как правило, для нормальной работы оборудования требуется соблюдать температурный режим в границах 18-25 °С, а относительную влажность воздуха – от 45 до 60%. В этом случае оборудование оказывается защищенным от остановки по причине переохлаждения, от выхода из строя в случае выпадения конденсата при высокой влажности, от статического электричества в случае с низкой влажностью или же из-за перегрева.

Помещение должно быть оборудовано **охранно-пожарной сигнализацией** и **системой газового пожаротушения**. Согласно пункту 6.5 нормативного документа РФ СН 512-78 "Технические требования к зданиям и помещениям для установки средств вычислительной техники» – огнегасящим веществом должен быть газ, который имеет российский сертификат.

Использование фреона и порошковых огнегасителей в этих помещениях категорически запрещено!

Системы газового пожаротушения применяются в тех случаях, когда применение воды может вызвать короткое замыкание или иное повреждение оборудования.

Автоматические установки газового пожаротушения должны обеспечивать:

- своевременное обнаружение пожара;
- возможность задержки подачи газового огнетушащего вещества в течение времени, необходимого для эвакуации людей из защищаемого помещения;
- создание огнетушащей концентрации газового огнетушащего вещества в защищаемом объёме или над поверхностью горящего материала за время, необходимое для тушения пожара.

1.3. Ограничения доступа в серверную комнату

Система контроля и управления доступом (СКУД) – *совокупность программно-аппаратных технических средств безопасности, в задачи которой входит ограничение и регистрация входа-выхода авторизованных сотрудников.*

Основная задача – управление доступом на заданную территорию (кого пускать, в какое время и на какую территорию), включая так же:

- ограничение доступа на заданную территорию;
- идентификация лица, имеющего доступ на заданную территорию;
- интеграция с системой безопасности:
    - системой видеонаблюдения для совмещения архивов событий систем, передачи системе видеонаблюдения извещений о необходимости стартовать запись, повернуть камеру для записи последствий зафиксированного подозрительного события;
    - системой охранной сигнализации (СОС), например, для ограничения доступа в помещения, стоящие на охране, или для автоматического снятия и постановки помещений на охрану;

- системой пожарной сигнализации (СПС) для получения информации о состоянии пожарных извещателей, автоматического разблокирования эвакуационных выходов и закрывания противопожарных дверей в случае пожарной тревоги.

Надежность (устойчивость к взлому) системы контроля доступа в значительной степени определяется типом используемого идентификатора: например, наиболее распространенные бесконтактные карты proximity могут подделываться в мастерских по изготовлению ключей на оборудовании, имеющемся в свободной продаже. Поэтому для объектов, требующих более высокого уровня защиты, подобные идентификаторы не подходят. Принципиально более высокий уровень защищенности обеспечивают RFID-метки, в которых код карты хранится в защищённой области и шифруется. Но так же не стоит использовать и слишком дорогие системы авторизации, такие как сканер сетчатки глаза или распознования лиц - это не слишком эффективные инструменты, которые к тому же не отличаются высокой точностью работы и «узнают» сотрудника далеко не с первого раза.

1.4. Выбор шкафа-стойки для размещения серверного оборудования, коммутации

К выбору шкафа для серверов или серверных стоек стоит отнестись как можно внимательнее, ведь это то, с чем будет сталкиваться ваш персонал постоянно при обслуживании оборудования, и, чем удобнее будет шкаф-стойка, тем быстрее и проще станет возможным проведение каких-либо работ с оборудованием. В первую очередь разделим шкафы на два типа: настенные серверные шкафы (рис. 1) и напольные шкафы (рис. 2).

Рис. 1. Настенный шкаф Hyperline TDC

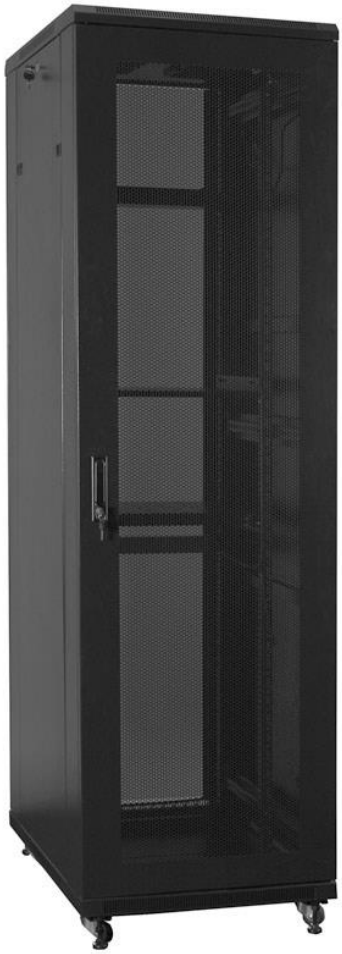

Рис. 2. Напольный шкаф Hyperline TDC

Если оборудуется серверное помещение, которое будет содержать всё ваше оборудование, то скорее всего вам больше всего подойдёт именно напольный вариант – ввиду его большей вместимости, но, если вам предстоит размещать оборудование где-то на территории офиса (к примеру, сетевое оборудование), то для этих целей стоит обратить внимание на меньшие по вместимости и размерам - настенные шкафы-стойки. Настенные шкафы-стойки обычно бывают размерами от 6 до 18U (Один юнит (1U) равен – 44,45 мм.), в то время как наполные начинаются обычно с 18U и доходят до 47U. Для размещения оборудования вам нужны шкафы-стойки стандартной шириной в 19", в то время как их глубина может доходить до 1200 мм. Так же шкафы-стойки бывают открытыми и закрытыми.

Рис. 3. Двурамная стойка Hyperline ORV2

Открытые серверные стойки, соответственно, лучше охлаждаются, в то время как закрытые - обеспечивают более высокую степень защиты от физических атак на оборудование. Какой тип шкафа выбирать - уже зависит от желаний заказчика. От качества исполнения стойки, зависит надёжность установки оборудования. Встречаются стойки низкого качества, которые имеют свойство раскачиваться от малейших прикосновений, что, естественно, недопустимо.

Достаточно часто стойки для серверов комплектуются дополнительными аксессуарами: кабельными органайзерами, полками и вентиляторными модулями, для организации дополнительных

воздушных потоков. Очень часто в шкафу-стойке (обычно отдельной) размещаются так же и патч-панели, облегчающие коммутацию сетевых и/или телефонных офисных розеток с сетевым оборудованием. Патч-панель представляет собой горизонтальную систему разъемов для организации точки коммутации между портами рабочих мест и портами сетевого оборудования. Кабель от розетки рабочего места подходит к лицевой стороне патч-панели и подключается к одному из разъемов, с тыльной стороны располагается кроссовое поле. Патч-панели так же бывают различных размеров, от 12 до 48 портов каждая.

Размещение кабелей в кабель-канал, как в самой серверной, так и по всему офису, это не просто «наведение красоты», но также и их защита от намеренной или случайной порчи. Конечно большая часть кабелей в серверной будет находится у вас снаружи и применение кабель-каналов не является возможным, но для качественной укладки и упорядовачивания кабелей служат такие аксессуары как кабельные органайзеры, стяжки и маркировочное оборудование для кабелей (рис. 4).

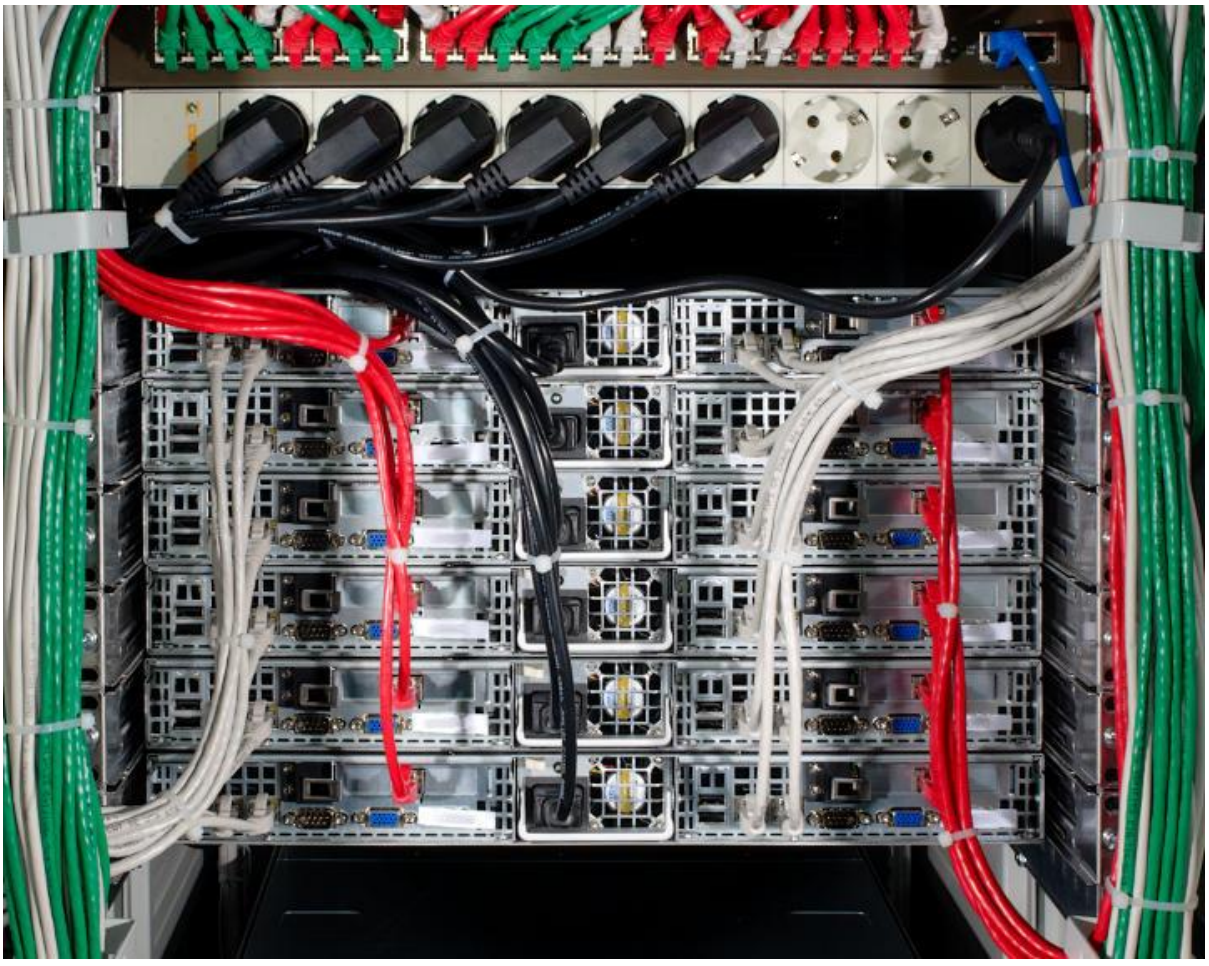

Рис. 4. Качественная укладка сетевых кабелей

Качественная укладка кабеля, позволит впоследствии в минимальные сроки отыскать нужный кабель, «выплести» его из основной косички и произвести его перекоммутацию или замену. Конечно, залог качественной укладки кабеля не только в наличии необходимого оборудования, но и большом опыте работы монтажников. Обращаясь за данной услугой к специалистам, вы можете быть уверены в качестве исполнения поставленной задачи.

2. Монтаж проводной сети

2.1. Преимущества и недостатки проводных сетей

Структури́рованная ка́бельная систе́ма *(СКС) – законченная совокупность кабелей связи и коммутационного оборудования, отвечающая требованиям соответствующих нормативных документов [34].*

СКС включает набор кабелей и коммутационных элементов, и методику их совместного использования, позволяющую создавать регулярные расширяемые структуры связей в локальных сетях различного назначения. СКС – физическая основа инфраструктуры здания, позволяющая свести в единую систему множество сетевых информационных сервисов разного назначения: локальные вычислительные сети и телефонные сети, системы безопасности, видеонаблюдения и т. д.

СКС представляет собой иерархическую кабельную систему, смонтированную в здании или в группе зданий, состоящую из структурных подсистем. В состав СКС входят такие элементы, как главный кросс (МС), кабель магистральной подсистемы первого и второго уровня, промежуточные кроссы (IC), горизонтальные кроссы (HC) и кабели горизонтальной подсистемы, а также консолидационные точки (CP), многопользовательские телекоммуникационные розетки (MuTOA или MuTO) и телекоммуникационные розетки (TO) и другие. Система может быть построена на основе медных или оптических кабелей, все элементы СКС интегрируются в единый комплекс (систему) и эксплуатируются согласно определённым правилам.

Преимущества:

- при относительно высокой начальной стоимости оправдывает капиталовложения за счет длительной и безотказной эксплуатации;
- доступная оптическая и медная UTP-технология;
- обеспечивает модульность и возможность наращивания и легкого внесения изменений;
- способность к передаче на высокой скорости и полосе пропускания;

- открытая архитектура допускает одновременное использование различных протоколов и продуктов различных пользователей;
- не зависит от изменений информационной технологии;
- допускает использование уже существующего активного оборудования;
- использует стандартные компоненты и материалы;
- допускает обслуживание минимальным количеством персонала пользователя;
- соответствует всем существующим стандартам по кабельной проводке здания в настоящее время и в будущем.

Недостатки:

- высокая стоимость проектирования и инсталляции.

Простые (неструктурированные) кабельные сети представляют из себя обычные кабельные системы на основе витой пары проложенные в кабельных каналах. Для передачи данных и офисной телефонии используются разные кабельные системы. Часто представляют из себя очень печальное зрелище: провода запутаны, просто валяются на полу, под столами.

Преимущества:

- низкая стоимость монтажа по сравнению с СКС;
- сравнительно высокая скорость монтажа;
- высокая надежность.

Недостатки:

- небольшая гарантия на систему;
- сложность расширения системы, дополнительные затраты на расширение.

2.2. Монтаж локальной сети

При монтаже проводных локальных сетей нет ничего запредельно сложного или требующего каких-то специальных навыков или знаний. Достаточно запомнить несколько простых правил и следовать им.

Основным носителем в подавляющем большинстве проводных сетей Ethernet сейчас является **витая пара**. Этот кабель делится по категориям. Наиболее распростарнен кабель с маркировкой UTP-8 Cat 5 или 5e, состоящий из 4-х пар (8 проводников) (рис. 5).

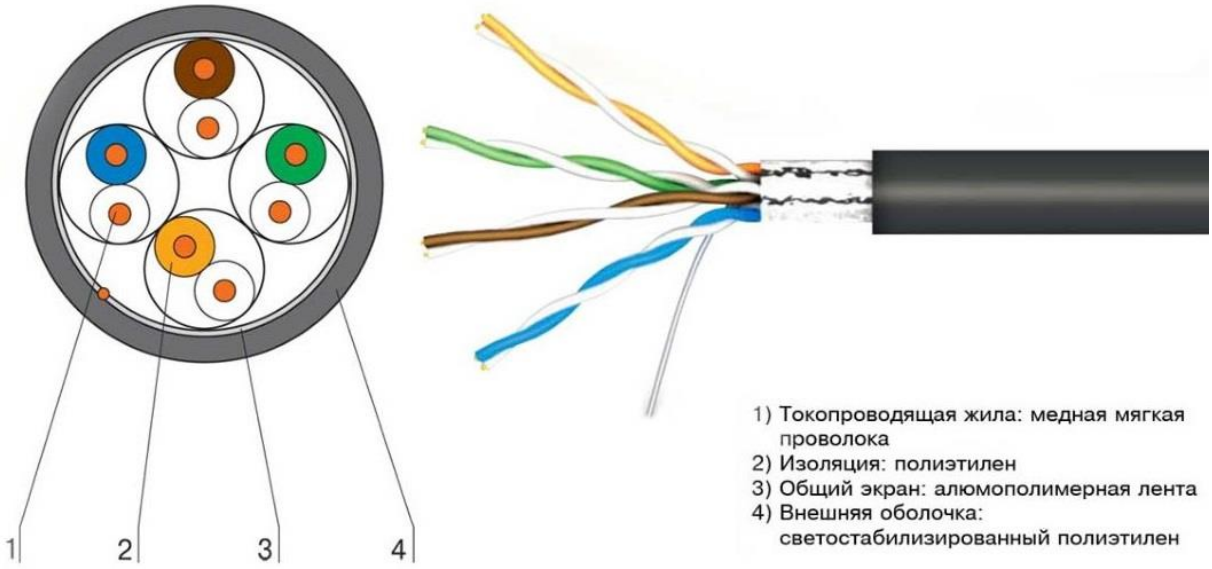

Рис. 5. Витая пара

Каждая пара скручена со своим определённым шагом, что служит защитой от помех. Проводники в парах имеют цветную маркировку: оранжевый+бело-оранжевый, зелёный+бело-зелёный, синий+бело-синий, коричневый+бело-коричневый. Маркировка двухцветных проводов может быть выполнена одним из двух способов: «колечками» – когда дополнительный цвет нанесён на белый проводник через определённое расстояние небольшими колечками, либо «полосками» – когда проводник поделён вдоль пополам, одна половина белого цвета, вторая – дополнительного. Предпочесть следует кабель второго типа по одной простой причине: после зачистки кабеля от изоляции на одном из двухцветных проводов ближайшее колечко может остаться под изоляцией, и мы будем иметь проводник неопределённого белого цвета.

Максимальная длина отрезка кабеля, используемого между двумя устройствами, по стандарту не может быть больше 100 метров. Розетки, переходники и прочие пассивные элементы устройствами в

данном контексте не считаются. Устройство принимает сигнал и отправляет дальше, предварительно усилив его. В небольших сетях это концентраторы (hub), коммутаторы (switch hub), мосты (bridge) и маршрутизаторы (router). Ну и, конечно же, сами компьютеры с сетевыми картами. Давайте остановимся на сетевых устройствах чуть более подробно, ведь, в конечном счёте, именно от них в большей степени зависит качество работы и удобство использования нашей будущей сети.

Концентратор – это многопортовый повторитель. То есть он принимает сигнал на один из своих портов (порт – это, проще говоря, гнездо, в которое вставляется сетевой кабель), и, усилив его, передаёт его на все остальные свои порты. Это один из самых дешёвых способов объединить компьютеры в локальную сеть, но у него есть один существенный недостаток. Допустим, в сеть соединены четыре компьютера. Так вот, если с первого компьютера пользователь передаёт файл на второй и, в это же время, с третьего компьютера пользователь передаёт файл на четвёртый, то скорость передачи падает более чем вдвое по сравнению с максимальной. Это происходит из-за того, что сигналы каждого из компьютеров передаются на все порты. Возникают так называемые «коллизии». Для решения этой проблемы были созданы коммутаторы. Внешне они ничем, как правило, не отличаются от концентраторов (да и по стоимости не очень заметно), но работают они принципиально по-другому. При включении компьютера в сеть коммутатор запоминает его физический адрес (MAC-адрес). Таким образом, если с первого компьютера файл передаётся на второй, а с третьего на четвёртый, то коммутатор сигнал, пришедший на первый порт, усиливает и передаёт только на второй порт, а сигнал, пришедший на третий – только на четвёртый. Таким образом, за счёт этого две передачи файлов происходят одновременно, причём на максимально возможной скорости и безо всяких коллизий.

Мосты используются для связи в одно целое двух отдельных сегментов сети. То есть, допустим, у нас в одном кабинете 4 компьютера, объединённые в локальную сеть, и в дугом кабинете 3 компьютера, также объединённые в локальную сеть. Расстояние между кабинетами равно 150 метрам. Нам необходимо объединить эти две сети в одну. Просто протянуть витую пару у нас не получится (как мы помним, её максимальная длина – 100 метров). Значит, надо либо где-то на посторонней территории устанавливать ретранслятор (усилитель сигнала), а это не всегда возможно, либо использовать, например,

коаксиальный кабель (его длину стандарт ограничивает уже 200 метрами). Либо, даже при гораздо меньшем расстоянии, но при невозможности проложить вообще какой-либо кабель, использовать беспроводную связь (Wi-Fi). Так вот, мост как раз и даёт возможность соединять сети, построенные на одном носителе (в нашем случае, витой паре), с помощью другого носителя (коаксиального кабеля или радиоволн) в одну сеть. Либо просто объединять в одну сеть два сегмента, построенные на разных носителях (допустим, все стационарные компьютеры подключены к сети с помощью кабеля, а ноутбуки и планшеты – по Wi-Fi).

Маршрутизаторы или роутеры. Сейчас для небольших домашних и офисных сетей это наиболее распространённые устройства. Недостаток коммутатора состоит, прежде всего, в том, что для того, чтобы обеспечить всем выход в Интернет по одной линии (одному подключению), необходимо для этого настроить один из компьютеров, который для этого будет подключён и к локальной сети и к Интернету. Более того, для обеспечения выхода остальных пользователей в Интернет этот компьютер должен быть постоянно включён даже тогда, когда его пользователь на нём не работает. То же самое относится и к другим общим устройствам, например, принтерам или сканерам (если они используются по сети совместно).

Роутер объединяет в себе функции коммутатора, моста и такого компьютера. То есть он подключается к Интернету, а все остальные подключены к нему как к коммутатору (по кабелю или по Wi-Fi). Наиболее продвинутые модели также позволяют подключать к себе принтеры, сканеры и внешние жёсткие диски при помощи USB. Так же они содержат программное обеспечение, которое может постоянно работать без включения компьютера (например, торрент-клиент). При выборе роутера необходимо учесть все потребности и откинуть всё лишнее (так, для дома, вероятнее всего, вряд ли понадобится 12-и портовый роутер со встроенным принт-сервером. А вот в небольшом офисе это будет практически идеальный вариант. Также выбор модели зависит от способа вашего подключения к провайдеру (наиболее распространены сейчас, по понятным причинам, Ethernet-роутеры и ADSL-роутеры).

Ниже рассмотрим, как создать небольшую локальную сеть, центральным узлом которой будет являться роутер. Для начала надо определиться с его месторасположением. Оно должно отвечать следующим требованиям:

1. Роутер должен быть легко доступен, и к нему без затруднений должен подключаться кабель провайдера Интернет.
2. В непосредственной близости от места размещения роутера (не дальше 1 метра) должна быть электророзетка.
3. Общая длина кабеля, идущего на подключение компьютеров к роутеру, должна быть минимальной.

Кабели обычно проложены либо методом скрытой проводки (в стене), либо в кабель-каналах и под фальшпотолком. На их конце монтируются розетки под разъёмы RJ-45 (рис. 6), а компьютеры в эти розетки подключаются с помощью так называемых патч-кордов. **Патч-корд** – это отрезок гибкой витой пары, длиной от 75 см до 1 м, на обоих концах которого находятся разъёмы RJ-45. Их можно приобрести в любом магазине, торгующем компьютерным оборудованием либо изготовить самостоятельно.

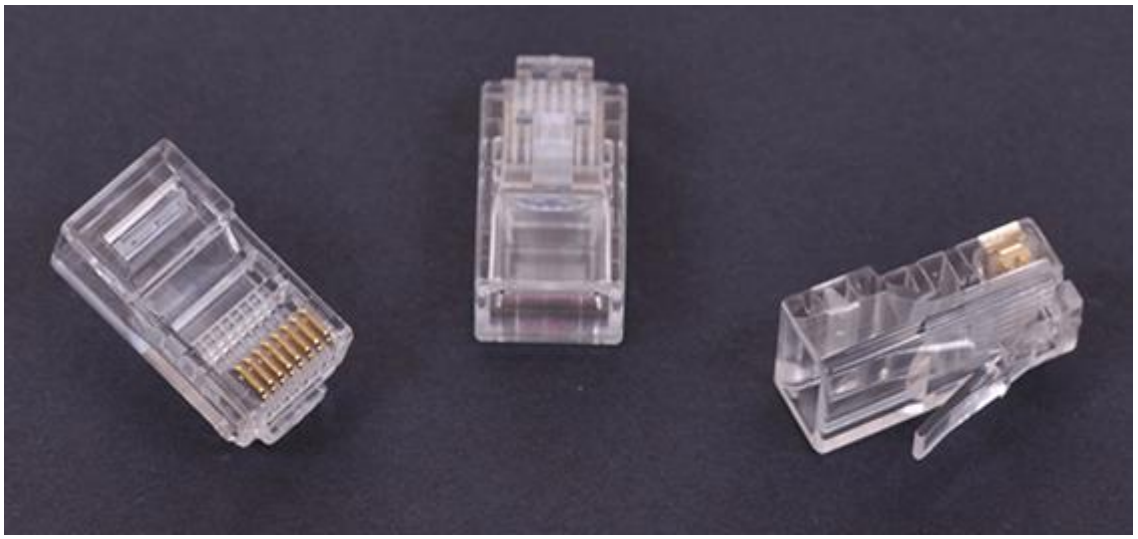

Рис. 6. Разъёмы RJ-45

Для присоединения кабеля «витая пара» к розеткам и для присоединения к кабелю разъёмов RJ-45 нам понадобятся два инструмента:

- **обжимной инструмент R-45** (обжимные клещи или кримпер, рис. 7) – служит для закрепления на концах кабеля разъёмов
- **устройство для зачистки RJ-45** (куттер, рис. 7) – служит для закрепления кабеля в розетке.

Рис. 7. Обжимной инструмент R-45

Рис. 8. Устройство для зачистки RJ-45

У разъёма RJ-45 восемь контактов. Нумеруются они следующим образом: если взять разъём и повернуть его фиксирующим язычком

вниз, чтобы металлические контакты были направлены от себя, то контакты слева направо нумеруются с 1 по 8.

Для фиксации разъёма на кабеле («обжима»), необходимо сделать следующие операции (рис. 9):

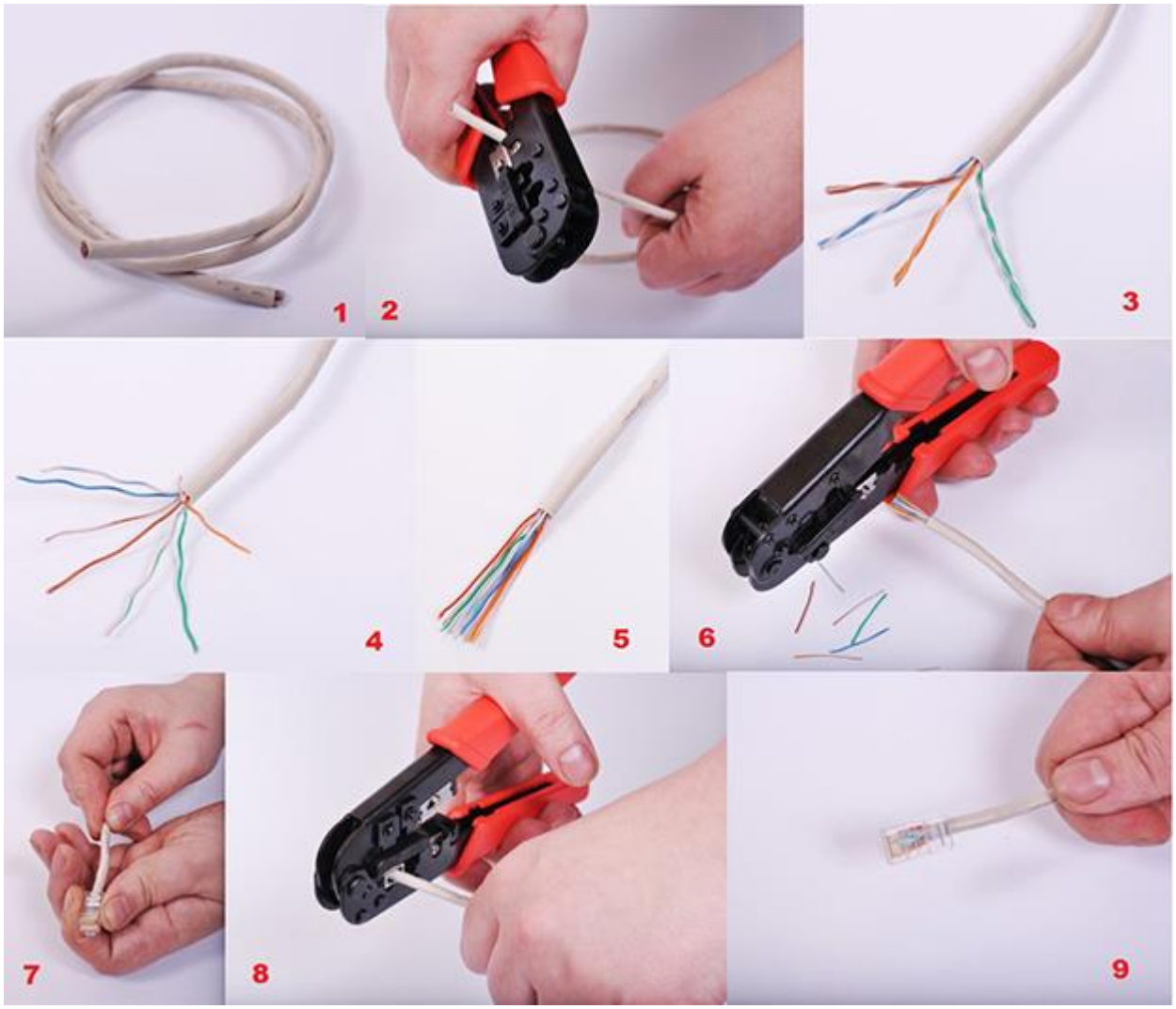

Рис. 9. Операции «обжима» витой пары

- зачистить конец кабеля от изоляции (рис. 9 (1,2));
- раскрутить витые пары и разложить провода в линейку согласно цветовой схемы (рис. 9 (3,4,5));
- срезать лишние провода до необходимой длины (чтобы провода помещались в разъём, а изоляция кабеля входила в него на несколько миллиметров) (рис. 9 (6));
- вставить провода в разъём, внимательно следя за тем, чтобы последовательность проводов не была нарушена (рис. 9 (7));

- вставить разъём в кримпер и сдавливанием рукояток зафиксировать разъём на кабеле (рис. 9 (8));
- извлечь разъём из клещей (рис. 9 (9)).

В настоящее время применяются две схемы обжима: TIA/EIA-568A и TIA/EIA-568B, который используется гораздо чаще. Расположение проводников в них следующее:

№ контакта	TIA/EIA-568A	TIA/EIA-568B	Crossover 1000 Mbit/s
1	Бело-зелёный	Бело-оранжевый	Бело-зелёный
2	Зелёный	Оранжевый	Зелёный
3	Бело-оранжевый	Бело-зелёный	Бело-оранжевый
4	Синий	Синий	Бело-коричневый
5	Бело-синий	Бело-синий	Коричневый
6	Оранжевый	Зелёный	Оранжевый
7	Бело-коричневый	Бело-коричневый	Синий
8	Коричневый	Коричневый	Бело-синий

При соединении компьютера с роутером оба конца кабеля обжимаются одинаково. Для соединения же однотипного оборудования (компьютер соединяется напрямую с компьютером либо, например, два концентратора соединяются между собой), используется так называемая «перекрёстная» схема обжима (crossover). Она также существует в двух вариантах. Первый вариант (который применяется на скоростях до 100 мбит/с и поэтому является наиболее распространённым), один конец кабеля обжимается по схеме «A», а второй – по схеме «B». Для скорости же до 1000 мбит/с применяются следующие схемы обжима: один конец кабеля обжимается по схеме «B», а второй – по схеме «Crossover 1000 Mbit/s».

Обжим розеток производить ещё проще. На розетках уже нанесены цветовые маркировки. Так что, в зависимости от выбраной схемы обжима «A» или «B» вам надо произвести следующие действия:

- с помощью куттера зачистить конец кабеля от изоляции;
- раскрутить пары проводов;

- наложить каждый провод на своё гнездо и с помощью носика куттера сдвинуть их вниз по лезвиям гнезда до упора;
- закрепить розетку в подрозетнике.

После этого необходимо с помощью патч-кордов соединить компьютеры с розетками локальной сети.

2.3. Настройка локальной сети

После того, как все компоненты локальной сети физически соединены в одно целое, необходимо их настроить. Первым делом настраиваем центральное устройство нашей сети, то есть роутер. Узнать в подробностях, как это делается, Вы можете здесь. С компьютерами же ещё проще. Обычно все компьютеры под управлением любой версии Windows по-умолчанию настроены как клиенты DHCP.

DHCP – это сервер, который занимается тем, что каждому подключающемуся к сети компьютеру либо другому устройству он выдаёт по заданным правилам все необходимые сетевые настройки, получив которые, компьютер подключается к сети и может в ней работать. После удачного входа в сеть этот ключ компьютер запоминает, и при последующих подключениях необходимость в его вводе отсутствует.

Но иногда (правда, довольно редко), возникает необходимость в настройке сетевых свойств вручную. Для этого нам необходимо будет зайти в «Центр управления сетями и общим доступом». Проще всего это сделать, кликнув по значку подключения к сети в трее и выбрав там «Центр управления сетями и общим доступом» (рис. 10).

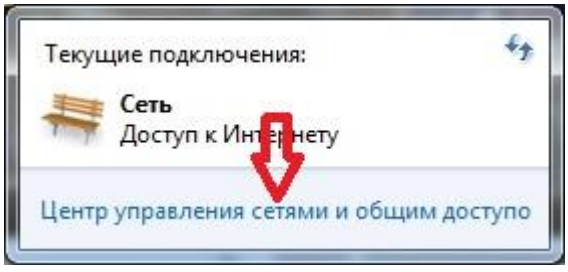

Рис. 10. Центр управления сетями и общим доступом

Либо зайти в меню «Пуск», далее в «Панель управления», в ней войти в раздел «Сеть и Интернет» и там выбрать «Центр управления сетями и общим доступом».

Там, в зависимости от того, какое подключение Вы настраиваете, Вам необходимо будет выбрать либо «Подключение по локальной сети» (1), либо «Беспроводное сетевое соединение» (2) (рис. 11).

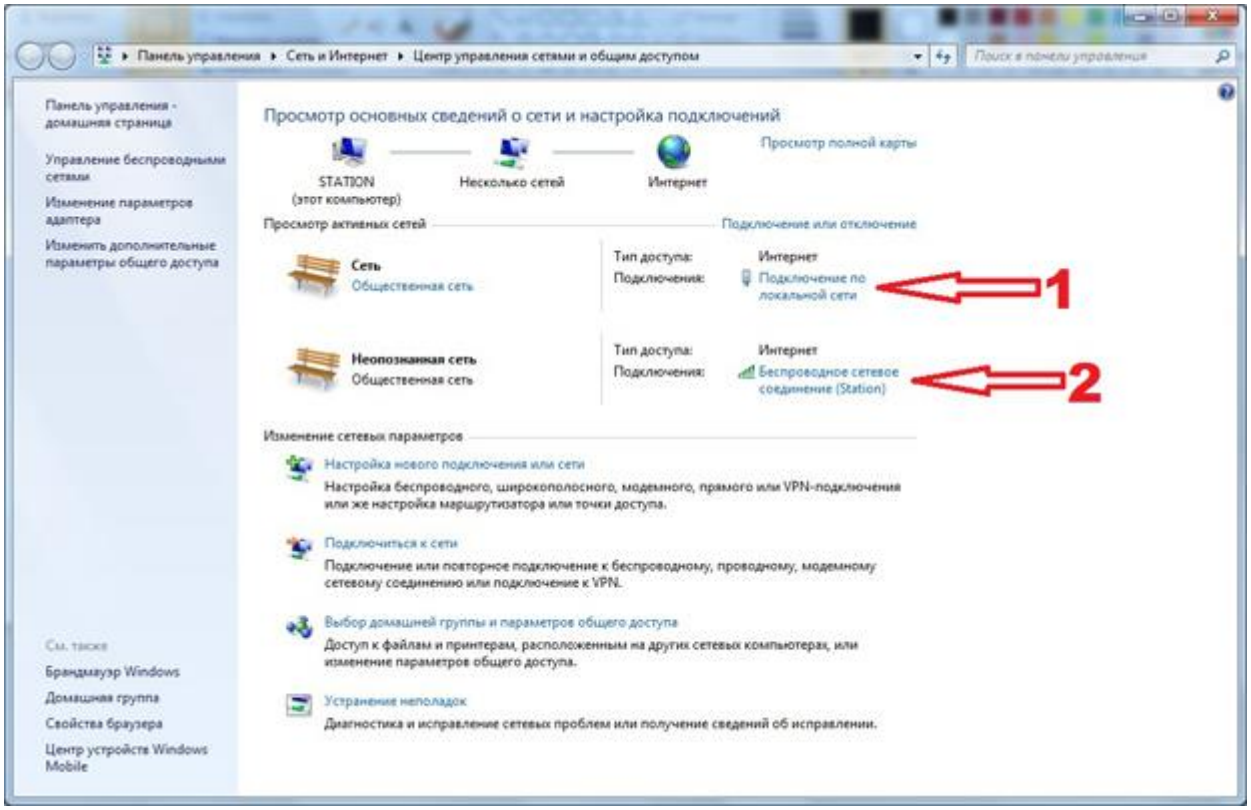

Рис. 11. Настройка сетевых подключений

Ручная настройка сети, вне зависимости от типа подключения, производится следующим образом.

В окне подключения кликнуть по кнопке «Свойства» (рис. 12).

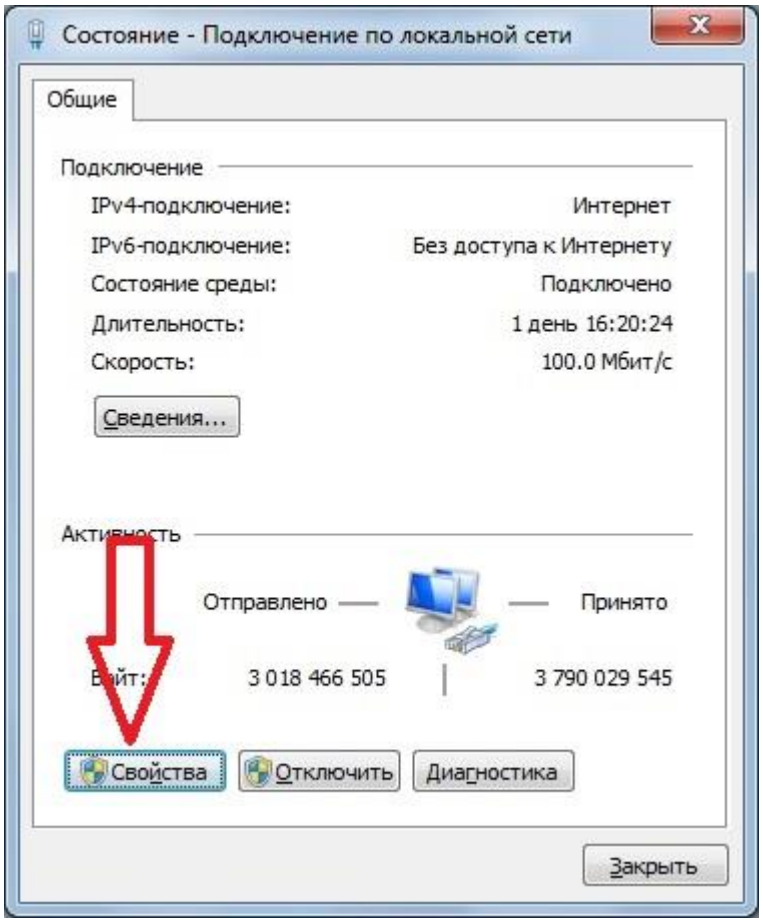

Рис. 12. Окно состояния подключения по локальной сети

Далее необходимо выбрать «Протокол Интернета 4 (TCP/IPv4)» и нажать «Свойства» (рис. 13).

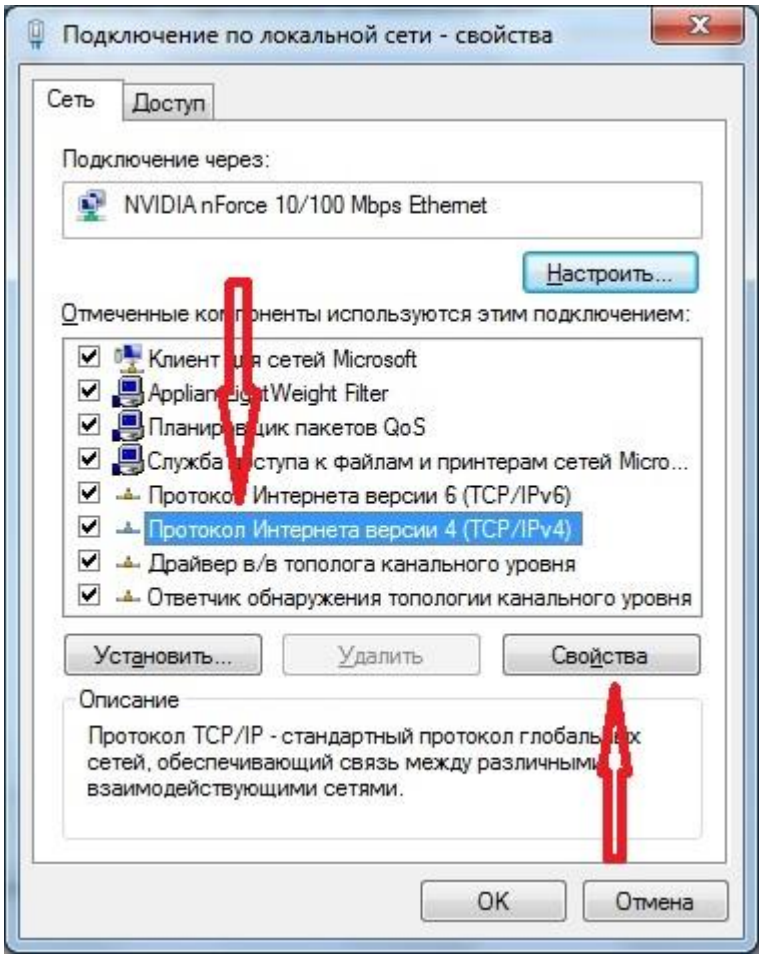

Рис. 13. Настройка парметров подключения по локальной сети

В свойствах необходимо будет ввести IP-адрес Вашего компьютера, маску подсети, шлюз по умолчанию и один либо два адреса (основной и резервный) сервера доменных имён DNS (рис. 14).

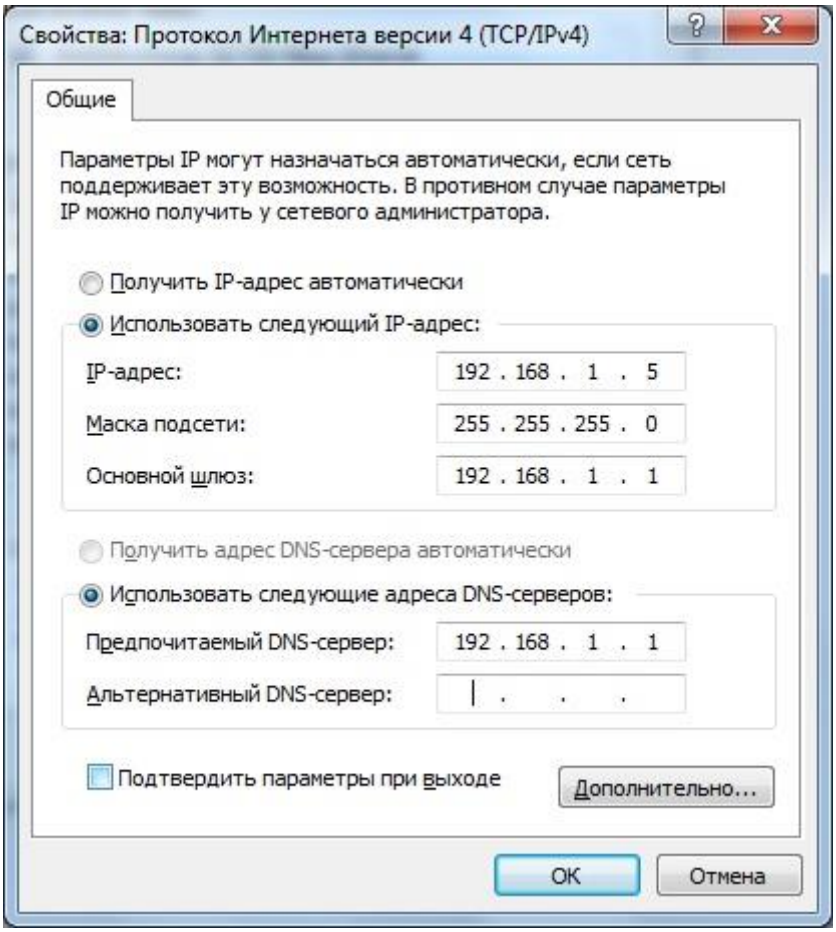

Рис. 14. Настройка параметров протокола TCP/IP

Сервер DNS занимается тем, что по символьному адресу URL, который Вы вводите в браузере, например, www.fixitbook.ru, выдаёт сопоставленный ему IP-адрес, с помощью которого Ваш компьютер может подключиться к нужному и показать Вам тот сайт, который Вам необходим. Сделана эта служба была потому, что названия из слов подавляющее большинство людей запоминает гораздо лучше и проще, нежели последовательность случайных цифр, которую представляет из себя IP-адрес.

2.4. Установка сетевого принтера

После этого Вам только останется, при необходимости, открыть для доступа такие устройства, как принтеры. Для этого вам нужно будет на том компьютере, к которому подключён принтер, зайти в его свойства («Пуск» – «Устройства и Принтеры», правый клик по принтеру, выбрать «Свойства принтера»). В открывшемся окне перейти на вкладку «Доступ» и нажать кнопку «Настройка общего доступа» (рис. 15).

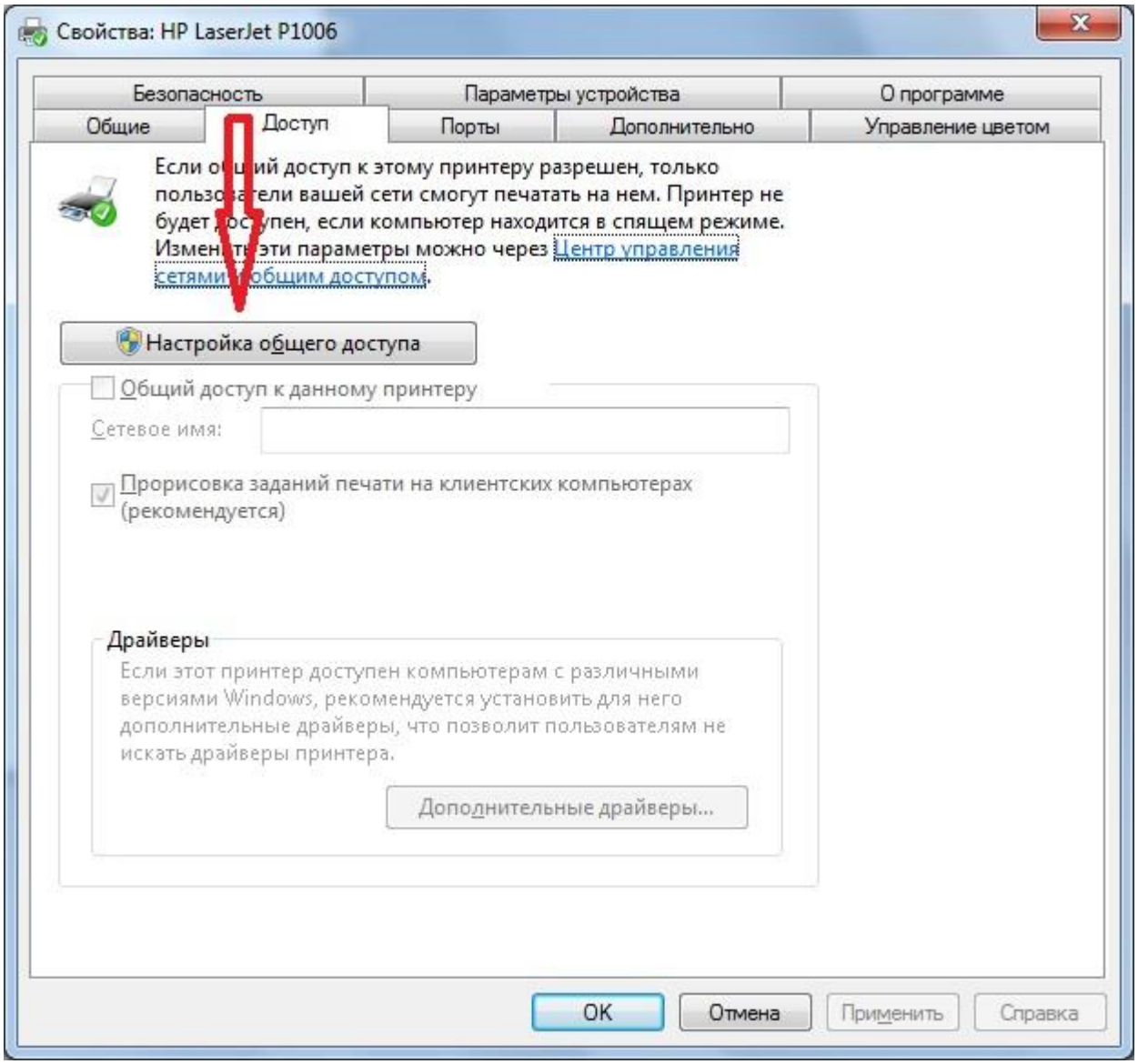

Рис. 15. Настройка сетевого принтера

После этого необходимо будет установить флажок «Общий доступ к данному принтеру», при необходимости ввести или отредактировать предложенное по умолчанию сетевое имя принтера. Также рекомендуется установить флажок «Прорисовка заданий печати на клиентских компьютерах», так как, если его не установить, то при одновременной печати нескольких документов с разных компьютеров нагрузка на компьютер, к которому подключён принтер, возрастёт настолько, что пользоваться им до окончания печати будет практически невозможно. Затем нажимаем «Применить» и «ОК» (рис. 16).

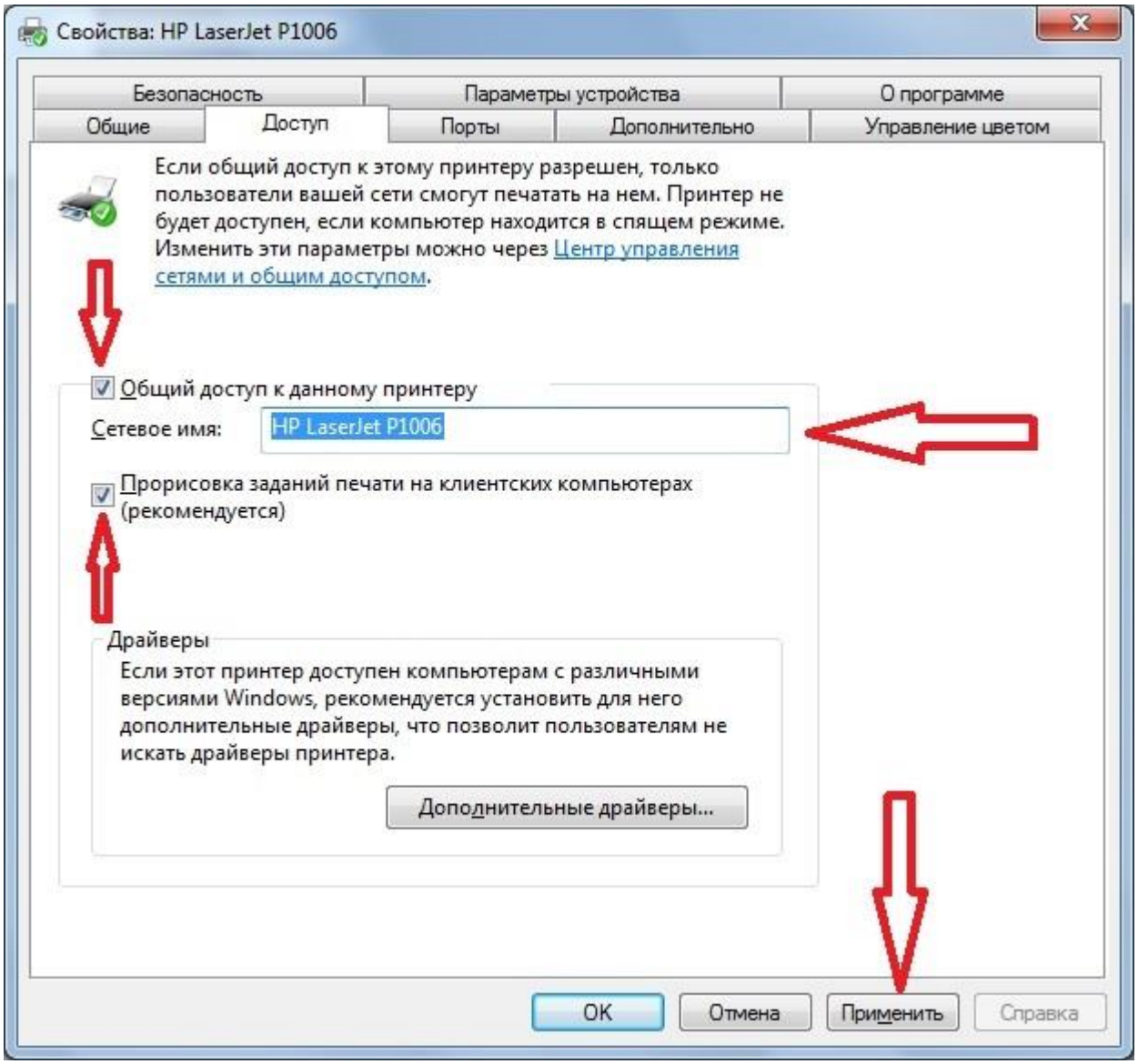

Рис. 16. Настройка параметров доступа к сетевому принтеру

На остальных компьютерах сети этот принтер необходимо будет установить как сетевой. Для этого надо зайти в меню «Пуск» и выбрать раздел «Устройства и Принтеры». Далее выбрать «Установка принтера» (рис. 17).

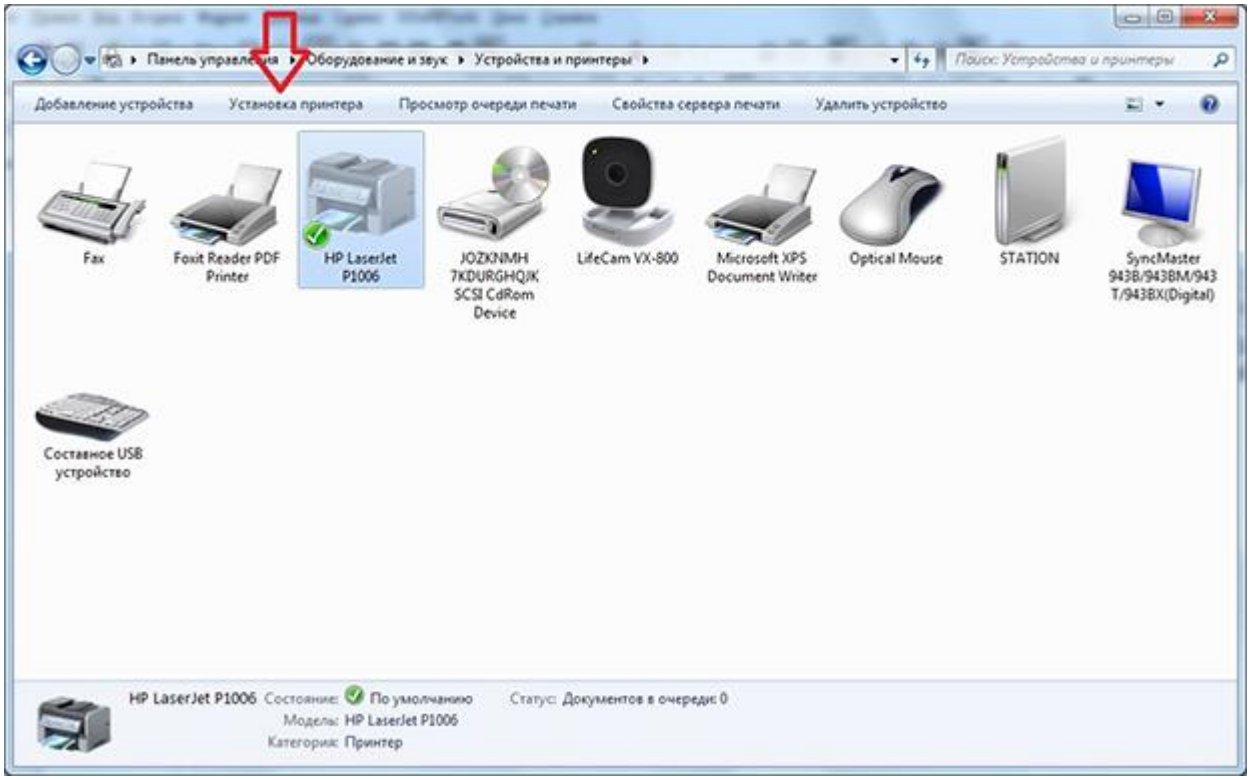

Рис. 17. Окно установки сетевого принтера с сетевых компьютеров

В появившемся окне выбрать «Добавить сетевой, беспроводной или Bluetooth-принтер». Через некоторое время, когда компьютер просканирует сеть, из предложенного списка выбрать Ваш сетевой принтер (возможно, и даже наиболее вероятно, что он будет там единственным), и нажать далее. При необходимости в следующем окне установить флажок «Сделать принтером по умолчанию» и нажать «Готово».

3. Монтаж беспроводной сети

3.1. Преимущества и недостатки беспроводных сетей

Беспроводные локальные сети Wi-Fi позволят повысить мобильность сотрудников в офисных или производственных помещениях, избавиться от кучи проводов в офисе или дома, вдобавок исключив затраты на монтаж и обслуживание проводной сети.

Wi-Fi имеет смысл использовать в компаниях с небольшим количеством рабочих мест или при наличии большого количества беспроводных устройств (ноутбуков, нетбуков, коммуникаторов и т. д.). Чаще всего используются оба типа сетей одновременно: проводные сети и беспроводные сети Wi-Fi.

Премущества:

- простота и скорость развертывания сети;
- низкая стоимость развертывания;
- отсутствие проводов на рабочем месте (хотя бы части проводов).

Недостатки:

- скорость передачи делится между всеми устройствами Wi-Fi в пределах обслуживания их одной и той же точкой доступа. Это значит, что если точка доступа предоставляет скорость передачи данных 300 мбит/с и к ней будет одновременно подключено, например, 5 ноутбуков, то скорость передачи данных для каждого ноутбука составит 300 / 5 = 60 мбит/с. А в реальности и того меньше, поскольку объем передаваемой служебной информации может достигать 30-40%. В итоге скорость передачи составляет около 36 мбит/с на устройство;
- влияние окружающей среды (деревья, стены зданий);
- сравнительно низкая надежность;
- низкая устойчивость к взлому при неправильной настройке.

Недостатки частично можно закрыть более качественным оборудованием и добавлением в состав беспроводной сети большего количества точек доступа Wi-Fi.

3.2. Режимы функционирования беспроводных сетей

Беспроводные сети Wi-Fi поддерживают несколько различных режимов работы, реализуемых для конкретных целей.

3.2.1. Режим Ad Hoc

В режиме Ad Hoc (рис. 18) клиенты устанавливают связь непосредственно друг с другом.

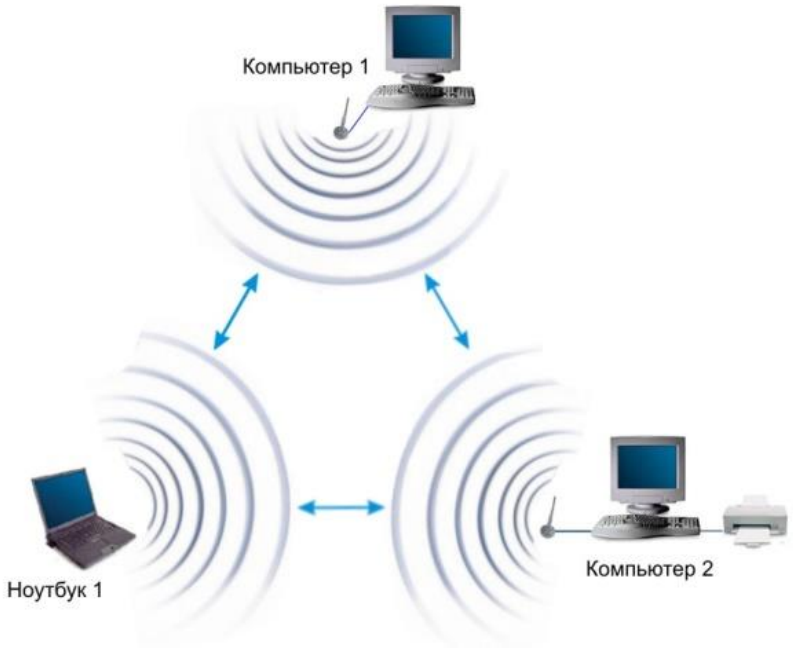

Рис. 18. Режим Ad Hoc

Устанавливается одноранговое взаимодействие по типу "точка-точка", и компьютеры взаимодействуют напрямую без применения точек доступа. При этом создается только одна зона обслуживания, не имеющая интерфейса для подключения к проводной локальной сети.

Основное достоинство данного режима – простота организации: он не требует дополнительного оборудования (точки доступа). Режим может применяться для создания временных сетей для передачи данных.

Однако необходимо иметь в виду, что режим Ad Hoc позволяет устанавливать соединение на скорости не более 11 Мбит/с, независимо от используемого оборудования. Реальная скорость

обмена данными будет ниже и составит не более 11/N Мбит/с, где N - число устройств в сети. Дальность связи составляет не более ста метров, а скорость передачи данных быстро падает с увеличением расстояния.

Для организации долговременных беспроводных сетей следует использовать инфраструктурный режим.

3.2.2. Инфраструктурный режим

В этом режиме точки доступа обеспечивают связь клиентских компьютеров (рис. 19).

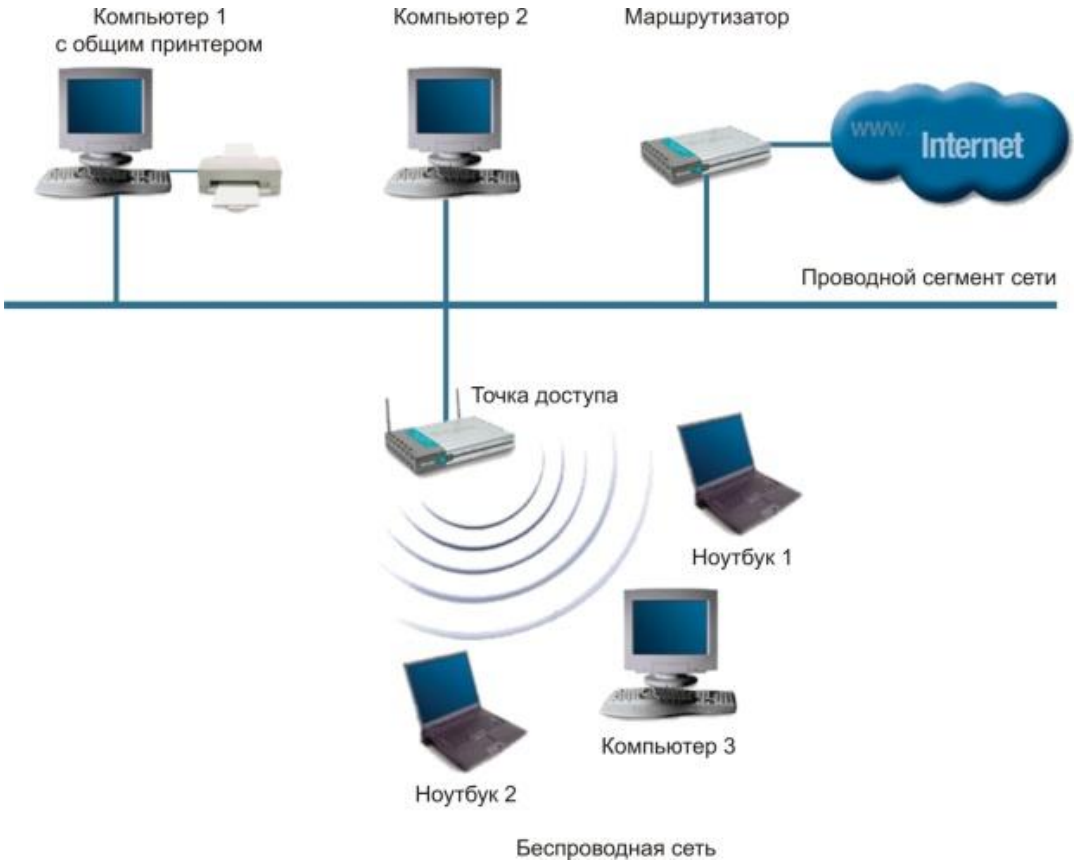

Рис. 19. Инфраструктурный режим

Точку доступа можно рассматривать как беспроводной коммутатор. Клиентские станции не связываются непосредственно одна с другой, а связываются с точкой доступа, и она уже направляет пакеты адресатам.

Точка доступа имеет порт Ethernet, через который базовая зона обслуживания подключается к проводной или смешанной сети – к сетевой инфраструктуре.

3.2.3. Режим WDS

Термин WDS (Wireless Distribution System) расшифровывается как "распределенная беспроводная система". В этом режиме точки доступа соединяются только между собой, образуя мостовое соединение. При этом каждая точка может соединяться с несколькими другими точками. Все точки в этом режиме должны использовать один и тот же канал, поэтому количество точек, участвующих в образовании моста, не должно быть чрезмерно большим. Подключение клиентов осуществляется только по проводной сети через uplink-порты точек (рис. 20).

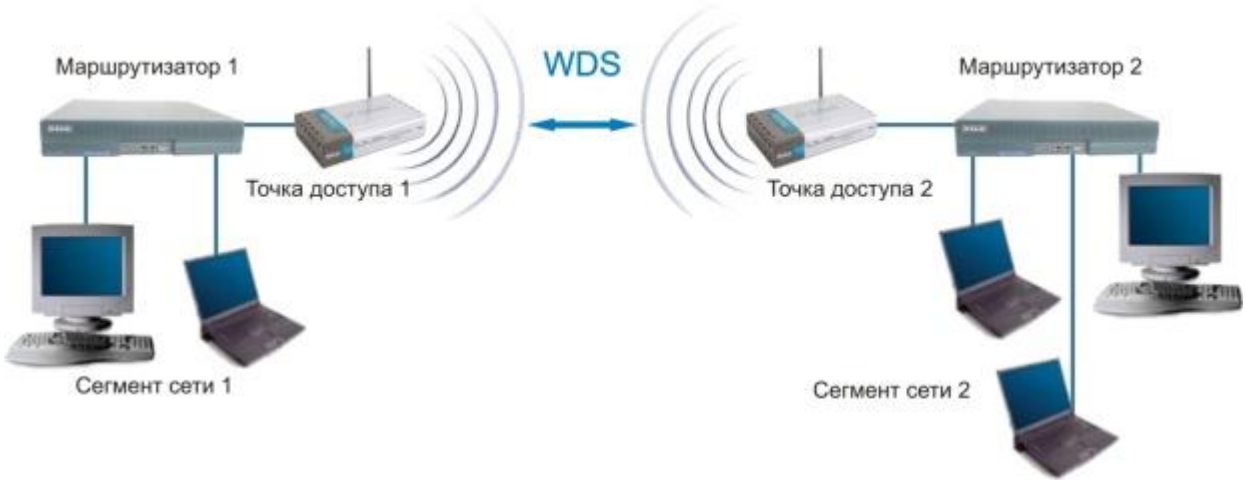

Рис. 20. Мостовой режим

Режим беспроводного моста, аналогично проводным мостам, служит для объединения подсетей в общую сеть. С помощью беспроводных мостов можно объединять проводные LAN, находящиеся как в соседних зданиях, так и на расстоянии до нескольких километров. Это позволяет объединить в сеть филиалы и центральный офис, а также подключать клиентов к сети провайдера Internet (рис. 21).

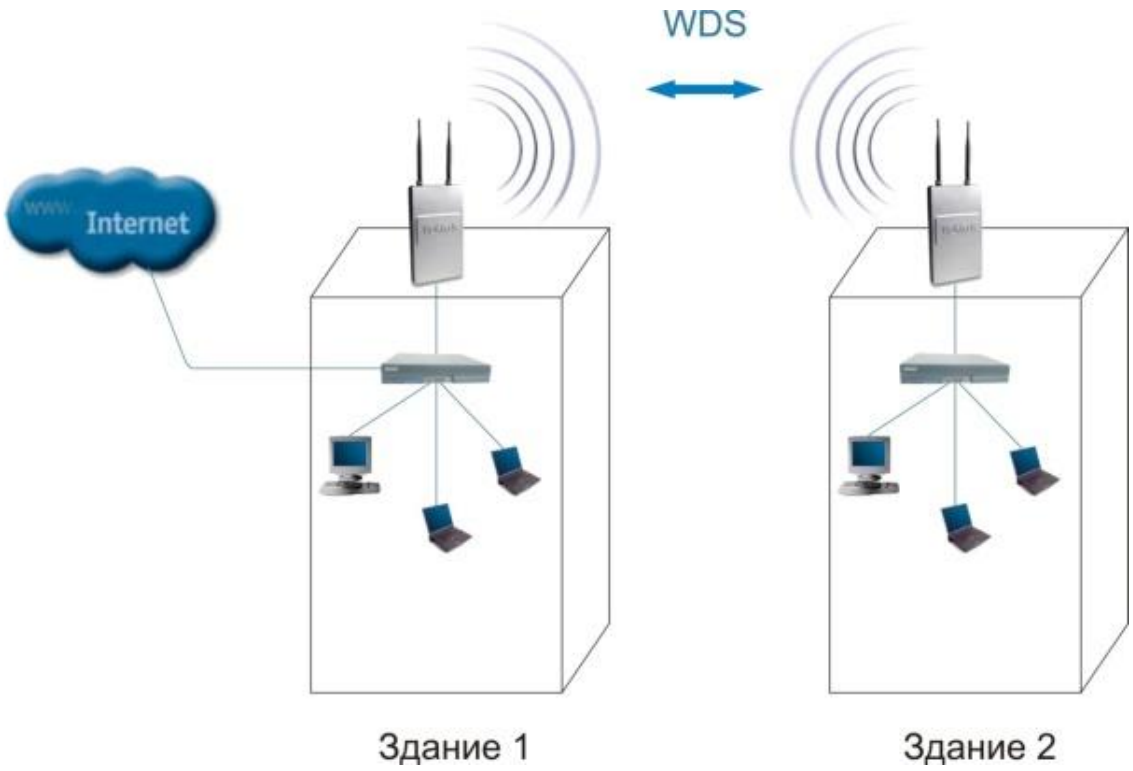

Рис. 21. Мостовой режим между зданиями

Беспроводной мост может использоваться там, где прокладка кабеля между зданиями нежелательна или невозможна. Данное решение позволяет достичь значительной экономии средств и обеспечивает простоту настройки и гибкость конфигурации при перемещении офисов.

К точке доступа, работающей в режиме моста, подключение беспроводных клиентов невозможно. Беспроводная связь осуществляется только между парой точек, реализующих мост.

3.2.4. Режим WDS WITH AP

Термин WDS with AP (WDS with Access Point) означает "распределенная беспроводная система, включающая точку доступа", т.е. с помощью этого режима можно не только организовать мостовую связь между точками доступа, но и одновременно подключить клиентские компьютеры (рис. 22). Это позволяет достичь существенной экономии оборудования и упростить топологию сети. Данная технология поддерживается большинством современных точек доступа.

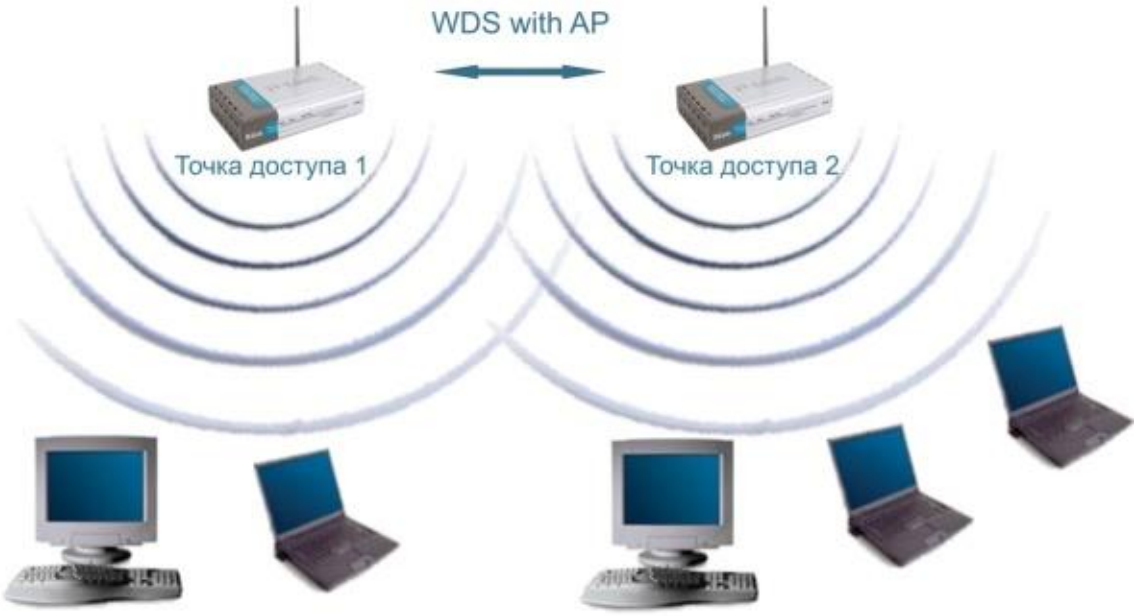

Рис. 22. Режим WDS with AP

Тем не менее необходимо помнить, что все устройства в составе одной WDS with AP работают на одной частоте и создают взаимные помехи, что ограничивает количество клиентов до 15-20 узлов. Для увеличения количества подключаемых клиентов можно использовать несколько WDS-сетей, настроенных на разные неперекрывающиеся каналы и соединенные проводами через uplink-порты.

Топология организации беспроводных сетей в режиме WDS аналогична обычным проводным топологиям.

3.3. Стандарты беспроводной связи

Существует несколько типов беспроводных стандартов: 802.11a, 802.11b и 802.11g. В соответствии с этими стандартами используются различные типы оборудования. Кроме того, всё чаще встречаются точки доступа с поддержкой одновременно нескольких стандартов, например, 802.11g и 802.11a. Стандарты беспроводных сетей семейства 802.11 отличаются друг от друга и максимально возможной скоростью передачи, и радиусом действия беспроводной сети. Так, стандарт 802.11b подразумевает максимальную скорость передачи до 11 Мбит/с, а стандарты 802.11a и 802.11g - максимальную скорость передачи до 54 Мбит/с. Кроме того, в стандартах 802.11b и 802.11g предусмотрено использование одного и тот же частотного диапазона - от 2,4 до 2,4835 ГГц, а стандарт 802.11a подразумевает использование

частотного диапазона от 5,15 до 5,35 ГГц. Соответственно, если точка доступа поддерживает одновременно стандарт 802.11a и 802.11g, то она является двухдиапазонной.

Оборудование стандарта 802.11a, в силу используемого им частотного диапазона, не сертифицировано в России. Это, конечно, не мешает использовать его в домашних условиях. Однако купить такое оборудование проблематично. Именно поэтому в дальнейшем мы сосредоточимся на рассмотрении стандартов 802.11b и 802.11g.

Следует учесть, что стандарт 802.11g полностью совместим со стандартом 802.11b, то есть стандарт 802.11b является подмножеством стандарта 802.11g, поэтому в беспроводных сетях, основанных на оборудовании стандарта 802.11g, могут также работать клиенты, оснащённые беспроводным адаптером стандарта 802.11b. Верно и обратное - в беспроводных сетях, основанных на оборудовании стандарта 802.11b, могут работать клиенты, оснащённые беспроводным адаптером стандарта 802.11g. Впрочем, в таких смешанных сетях заложен один подводный камень: если мы имеем дело со смешанной сетью, то есть с сетью, в которой имеются как клиенты с беспроводными адаптерами 802.11b, так и клиенты с беспроводными адаптерами 802.11g, то все клиенты сети будут работать по протоколу 802.11b. Более того, если все клиенты сети используют один и тот же протокол, например, 802.11b, то данная сеть является гомогенной, и скорость передачи данных в такой сети выше, чем в смешанной сети, где имеются как клиенты 802.11g, так и 802.11b. Дело в том, что клиенты 802.11b 'не слышат' клиентов 802.11g. Поэтому для того, чтобы обеспечить совместный доступ к среде передачи данных клиентов, использующих различные протоколы, в подобных смешанных сетях точки доступа должны отрабатывать определенный механизм защиты. Не вдаваясь в подробности реализации данных механизмов, отметим лишь, что в результате использования механизмов защиты в смешанных сетях реальная скорость передачи становится ещё меньше.

Поэтому при выборе оборудования для беспроводной домашней сети стоит остановиться на оборудовании одного стандарта. Протокол 802.11b на сегодня является уже устаревшим, да и реальная скорость передачи данных при использовании данного стандарта может оказаться неприемлемо низкой. Так что оптимальный выбор - оборудование стандарта 802.11g.

Некоторые производители предлагают оборудование стандарта 802.11g+ (SuperG), а на коробках своих изделий (точках доступа и беспроводных адаптерах) помимо надписи '802.11g+' указывают ещё и скорость в 100, 108 или даже 125 Мбит/с.

Фактически никакого протокола 802.11g+ не существует, и всё, что скрывается за этим загадочным протоколом - это расширение базового стандарта 802.11g.

На самом деле, все производители чипсетов для беспроводных решений (Intersil, Texas Instruments, Atheros, Broadcom и Agere) в том или ином виде реализовали расширенный режим 802.11g+. Однако проблема заключается в том, что все производители по-разному реализуют данный режим, и нет никакой гарантии, что решения различных производителей смогут взаимодействовать друг с другом. Поэтому при покупке точки доступа стандарта 802.11g+ следует убедиться, что беспроводные адаптеры также поддерживают данный стандарт.

3.4. Проблемы выбора точка доступа или маршрутизатор

Кроме того, что точки доступа могут выполнять в виде отдельных законченных решений, существуют так называемые беспроводные маршрутизаторы, в которых беспроводная точка доступа является составной частью устройства. Соответственно, при развертывании беспроводной сети встает вопрос выбора между точкой доступа и беспроводным маршрутизатором. Выбор в пользу того или иного устройства зависит от того, как именно будет использоваться беспроводная сеть. Рассмотрим несколько типичных ситуаций.

В простейшем случае несколько компьютеров объединяются в беспроводную сеть исключительно для обмена данными между ПК. В этом случае оптимальным выбором будет точка доступа, которая подключается к одному из ПК сети (причём ПК, к которому подключается точка доступа, не должен быть оборудован беспроводным адаптером).

Во втором варианте предполагается, что помимо обмена данными между компьютерами, объединенными в беспроводную сеть, необходимо реализовать для всех компьютеров разделяемый доступ в Интернет с использованием аналогового модема (модема, который подключается к телефонной линии). В этом случае модем подключается к одному из компьютеров беспроводной сети, а

Интернет-соединение настраивается в режиме разделяемого доступа. К этому же компьютеру подключается точка доступа, а на всех компьютерах беспроводной сети настраивается выход в Интернет в режиме доступа через локальную сеть. Понятно, что оптимальным решением в рассмотренном случае так же является именно использование точки доступа.

И, наконец, последний вариант топологии беспроводной сети - использование высокоскоростного доступа в Интернет с использованием DSL, кабельного модема или Ethernet-подключения. В этом случае оптимальным вариантом является использование точки беспроводного доступа, встроенной в маршрутизатор.

Маршрутизаторы являются пограничными сетевыми устройствами, то есть устройствами, устанавливаемыми на границе между двумя сетями или между локальной сетью и Интернетом, и в этом смысле они выполняют роль сетевого шлюза. С конструктивной точи зрения они должны иметь как минимум два порта: к одному из них подключается локальная сеть (этот порт называется внутренним LAN-портом), а ко второму - внешняя сеть (Интернет) и этот порт называется внешним WAN-портом. Как правило, маршрутизаторы, используемые для дома или небольшого офиса (SOHO-маршрутизаторы), имеют один WAN-порт и несколько (от одного до четырёх) внутренних LAN-портов, которые объединяются в коммутатор. В большинстве случаев WAN-порт коммутатора имеет интерфейс 10/100Base-TX и к нему может подключаться xDSL-модем с соответствующим интерфейсом либо сетевой Ethernet-кабель.

Интегрированная в маршрутизатор точка беспроводного доступа позволяет организовать беспроводной сегмент сети, которая, с точки зрения маршрутизатора, относится к внутренней сети, и в этом смысле компьютеры, подключаемые к маршрутизатору беспроводным способом, ничем не отличаются от тех, что подключены к LAN-порту.

Использование беспроводного маршрутизатора вместо точки доступа выгодно не только потому, что это позволяет сэкономить на покупке дополнительного сетевого Ethernet-контроллера или мини-коммутатора, но и потому, что маршрутизаторы предоставляют дополнительные средства защиты внутренней сети от несанкционированного доступа. Так, практически все современные маршрутизаторы класса SOHO имеют встроенные аппаратные брандмауэры, которые также называются сетевыми экранами или firewall.

3.5. Настройка точки доступа

Для развертывания беспроводной сети прежде всего необходимо настроить точку доступа (беспроводной маршрутизатор). Предполагается, что на всех компьютерах, входящих в беспроводную сеть, используется операционная система Windows XP Professional SP2 (английская версия).

Шаг 1. Установка (изменение) IP-адреса компьютера

Для того, чтобы развернуть локальную сеть, необходимо, чтобы все компьютеры сети имели один IP-адрес одной подсети. Поскольку точка доступа также входит в локальную сеть, нужно, чтобы и её IP-адрес входил бы в ту же подсеть, что и все остальные клиенты сети.

Как правило, последовательность действий в данном случае следующая: прежде всего, необходимо выяснить IP-адрес точки доступа и пароль, заданный по умолчанию. Любая точка доступа или маршрутизатор, будучи сетевым устройством, имеет свой собственный сетевой адрес (IP-адрес). Для того чтобы выяснить IP-адрес и пароль, придётся пролистать инструкцию пользователя. Предположим, что IP-адрес точки доступа по умолчанию 192.168.1.254.

Далее необходимо подключить точку доступа к компьютеру с использованием традиционного сетевого интерфейса Ethernet (для этого на компьютере должен быть установлен сетевой Ethernet-контроллер). В случае использования беспроводного маршрутизатора подключение компьютера производится через LAN-порт маршрутизатора.

Для настройки точки доступа необходимо, чтобы компьютер, к которому подключается точка доступа, имели бы IP-адрес из той же подсети, что и точка доступа. Поскольку в нашем случае точка доступа имеет IP-адрес 192.168.1.254, то компьютеру необходимо присвоить статический IP-адрес 192.168.1.x (например, 192.168.1.100) с маской подсети 255.255.255.0.

Для присвоения компьютеру статического IP-адреса щелкните на значке My Network Places (Сетевое окружение) правой кнопкой мыши и в открывшемся списке выберите пункт Properties (Свойства). В открывшемся окне Network Connection (Сетевые соединения) выберите значок Local Area Connection (Локальная Сеть) и, щёлкнув на нём правой кнопкой мыши, снова перейдите к пункту Properties. После этого должно открыться диалоговое окно Local Area Connection

Properties (Свойства сетевого соединения), позволяющее настраивать сетевой адаптер (рис. 23).

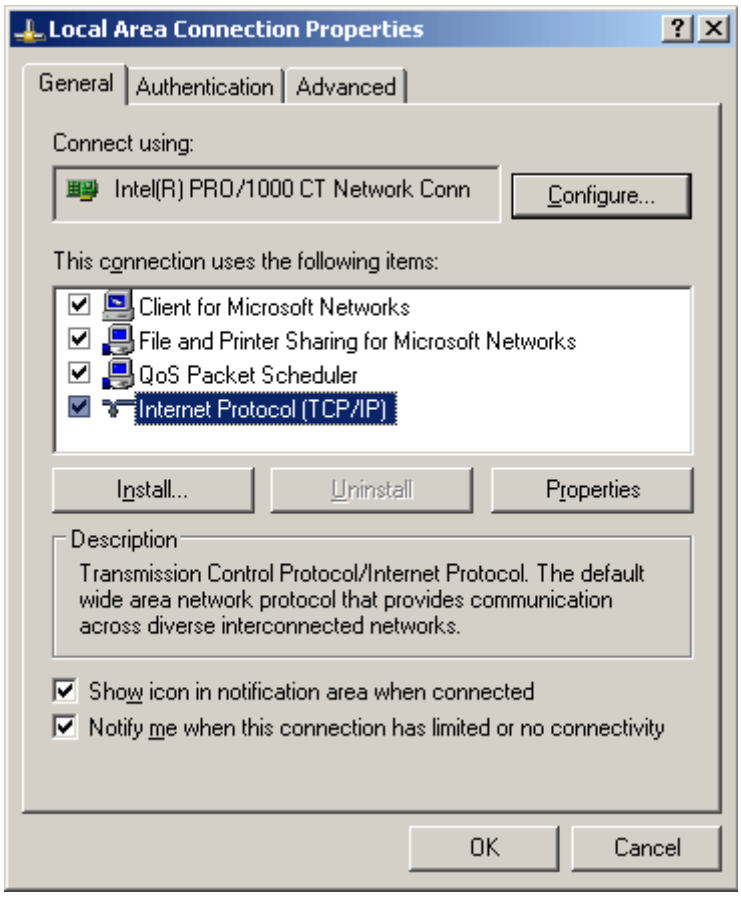

Рис. 23. Диалоговое окно Local Area Connection Properties

На вкладке General выделите протокол Internet Protocol (TCP/IP) и нажмите на кнопку Properties. Перед вами откроется диалоговое окно, позволяющее задавать IP-адрес компьютера и маску подсети. Отметьте в данном диалоговом окне пункт Use the following IP address: и введите в соответствующие текстовые поля IP-адрес и маску подсети (рис. 24).

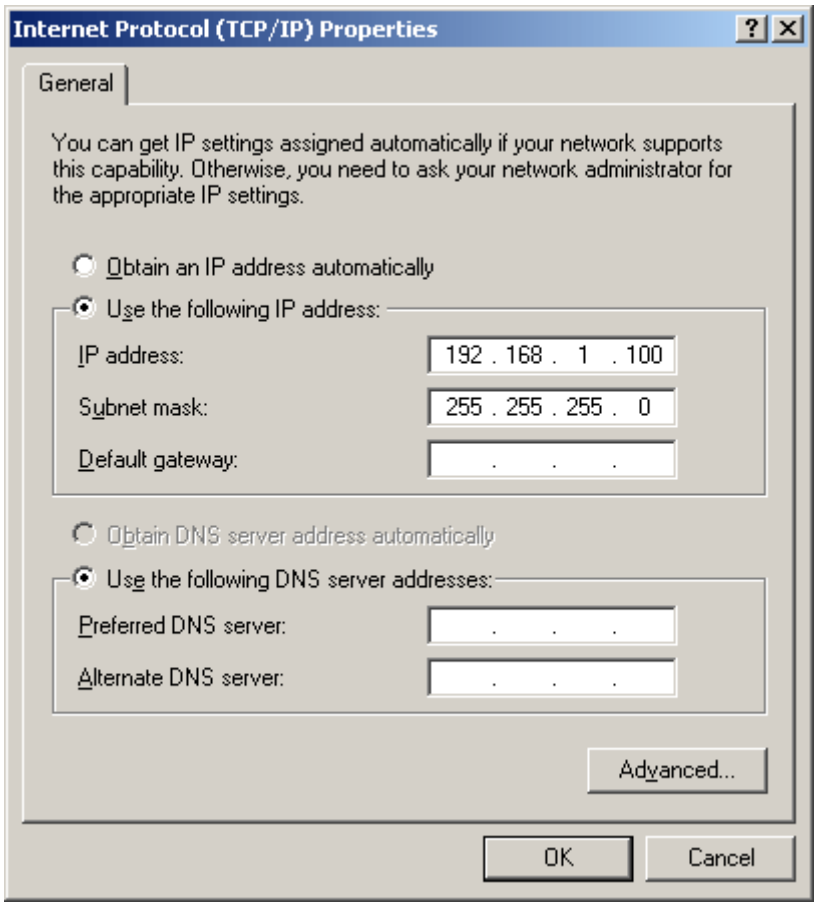

Рис. 24. Задание статического IP-адреса и маски подсети

Шаг 2. Настройка беспроводного соединения

После того как задан статический IP-адрес компьютера, можно получить непосредственный доступ к настройкам самой точки доступа. Для этого в поле адреса Web-браузера введите IP-адрес точки доступа (192.168.1.254). Если всё сделано правильно, то перед вами откроется диалоговое окно настроек точки доступа (маршрутизатора). Возможно, предварительно потребуется ввести логин и пароль (они имеются в документации).

Используя диалоговое окно настроек точки доступа, можно задать новый IP-адрес точки доступа (если в этом имеется необходимость), однако следует помнить, что после окончания сеанса связи с точкой доступа необходимо также изменить и IP-адрес компьютера (в противном случае новое соединение с точкой доступа станет невозможным).

Если точка доступа используется только для организации локальной беспроводной сети без выхода в Интернет, то нет необходимости менять IP-адрес точки доступа. Возможно, проще

поменять (или задать) IP-адреса всех беспроводных клиентов. Однако в ряде случаев изменение IP-адреса точки доступа необходимо. Например, для реализации разделяемого доступа в Интернет с использованием аналогового модема, компьютеру, к которому подключён модем, присваивается статический IP-адрес 192.168.0.1 с маской подсети 255.255.255.0. В этом случае приходится задавать IP-адрес точки доступа из той же подсети (192.168.0.x). Пример с организацией разделяемого беспроводного доступа в Интернет с использованием аналогового модема будет рассмотрен далее.

Кроме изменения IP-адреса точки доступа, используя диалоговое окно настроек точки доступа, для настройки беспроводной сети требуется задать следующие параметры:

Тип беспроводной сети. Если точка доступа поддерживает несколько беспроводных стандартов, необходимо в явном виде указать стандарт беспроводной сети (например, 802.11g+). Однако следует учесть, что жёсткое задание стандарта отсекает клиентов, не поддерживающих данный стандарт. Поэтому в некоторых случаях целесообразно указывать смешанный тип протоколов, например, 802.11b/g.

Номер канала. Для беспроводного соединения точки доступа с клиентами сети могут использоваться различные частотные каналы. К примеру, в случае протокола 802.11g можно использовать каналы с первого по тринадцатый. Можно в явном виде указать, какой именно канал будет использоваться для установления соединения, а можно задать автоматический выбор канала (Enable auto channel select), причём автоматический выбор каналов предпочтительнее.

SSID. Каждая беспроводная сеть имеет свой уникальный идентификатор SSID, который представляет собой условное название беспроводной сети. Для функционирования беспроводной сети необходимо, чтобы SSID точки доступа и SSID профиля беспроводного соединения на клиентах сети был бы одинаковым.

Rate. Точка доступа позволяет в явном виде указать скорость (Rate) устанавливаемого соединения. Впрочем, делать это не рекомендуется, и лучше всего задать автоматическое определение скорости соединения (auto/best).

Итак, после того как все основные настройки точки доступа сделаны, можно приступать к созданию профиля беспроводного соединения на клиентах сети.

Шаг 3. Создание профиля беспроводного соединения

Настройка конкретного беспроводного адаптера, естественно, зависит от версии используемого драйвера и утилиты управления. Однако сами принципы настройки остаются неизменными для всех типов адаптеров. Кроме того, существует и общий, независимый от типа утилиты управления конкретного адаптера способ, - использовать для настройки беспроводного адаптера клиента Microsoft (встроенную в операционную систему Windows XP утилиту настройки беспроводного адаптера). Рассмотрим подробно оба способа настройки. Кроме того, учитывая популярность ноутбуков на базе мобильной технологии Intel Centrino, неотъемлемой частью которой является наличие модуля беспроводной связи, настройку беспроводного соединения мы опишем на примере драйвера Intel PROSet/Wireless (версия 9.0.1.9), используемого в ноутбуках на базе технологии Intel Centrino.

3.6. Настройка беспроводного адаптера

3.6.1. Настройка с использованием утилиты управления

Итак, прежде всего необходимо установить драйвер беспроводного адаптера. В случае ноутбука на базе мобильной технологии Intel Centrino откроем диалоговое окно Intel PROSet/Wireless (значок этого окна находится в системном трее), с помощью которого будет создаваться профиль нового беспроводного соединения (рис. 25).

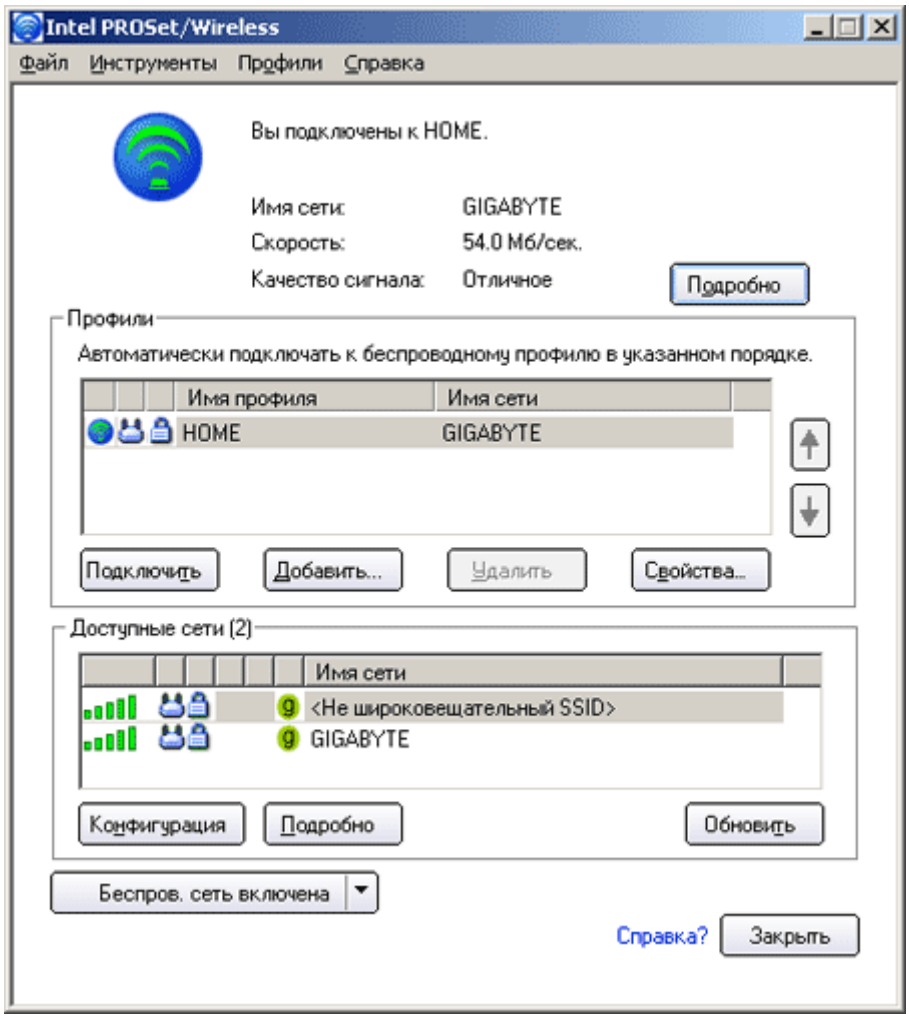

Рис. 25. Диалоговое окно настройки беспроводного соединения

Нажмите на кнопку 'Добавить', чтобы создать профиль нового беспроводного соединения. В открывшемся диалоговом окне 'Создать профиль беспроводной сети' (рис. 26) введите имя профиля (например, HOME) и имя беспроводной сети (SSID), которое было задано при настройке точки доступа.

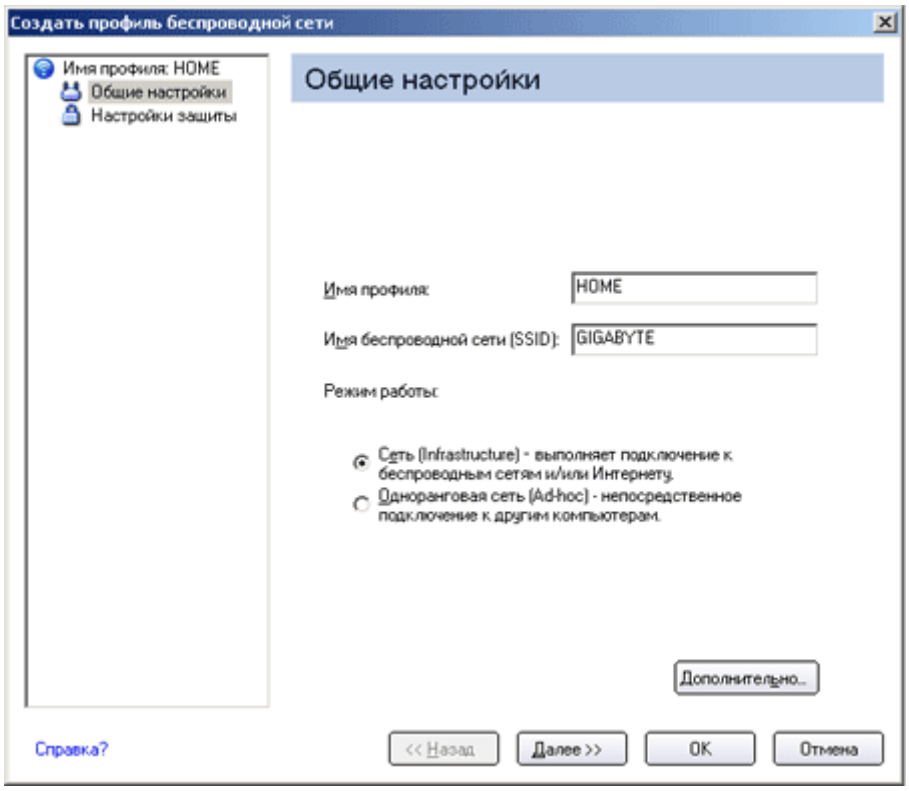

Рис. 26. Диалоговое окно настройки нового профиля беспроводной сети

Далее предлагается настроить защиту беспроводной сети, но на первом этапе (этап отладки) делать этого не нужно, поэтому следующие диалоговые окна оставляем без изменений.

3.6.2. Настройка с использованием клиента Microsoft

При использовании для настройки беспроводного адаптера клиента Microsoft (универсальный метод, который подходит для всех беспроводных адаптеров) прежде всего следует убедиться в том, что не используется иная утилита управления адаптером.

Щелкните на значке My Network Places (Сетевое окружение) правой кнопкой мыши и в открывшемся списке выберите пункт Properties (Свойства). В открывшемся окне Network Connection (Сетевые соединения) выберите значок Wireless Network Connection (Беспроводные соединения) и, щёлкнув на нём правой кнопкой мыши, снова перейдите к пункту Properties. После этого должно открыться диалоговое окно Wireless Network Connection Properties (Свойства беспроводного сетевого соединения), позволяющее настраивать беспроводной сетевой адаптер (рис. 27).

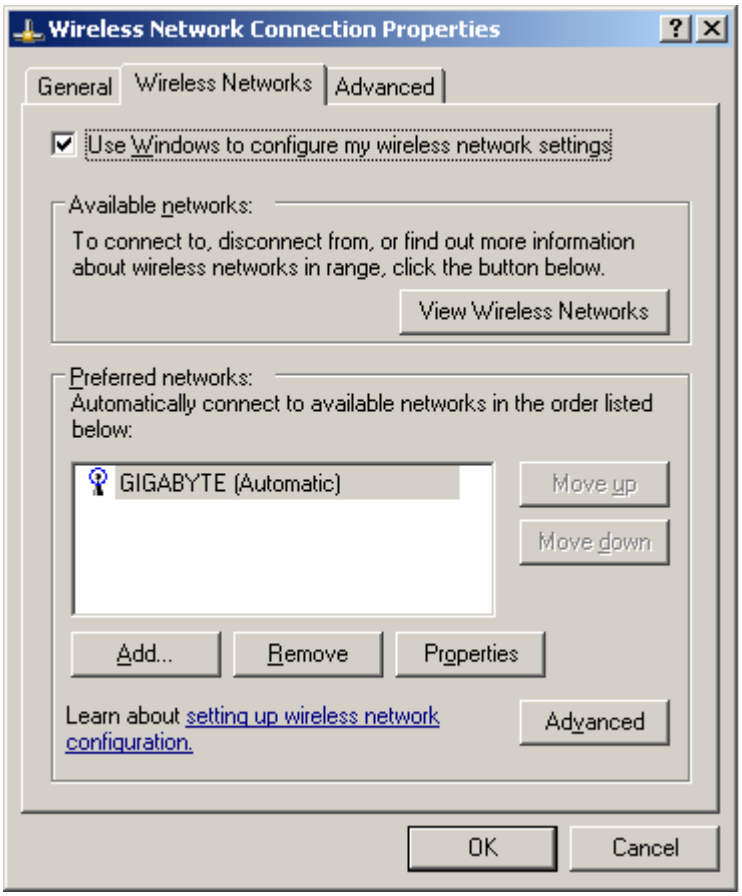

Рис. 27. Диалоговое окно настройки беспроводного сетевого адаптера

Перейдя на вкладку 'Wireless Networks' (беспроводные сети), нажмите на кнопку 'Add:' (добавить) и в открывшемся диалоговом окне 'Wireless network properties' (свойства беспроводного соединения) введите имя беспроводной сети (SSID) (рис. 28). Остальные поля (настройка защиты) пока оставьте без изменения.

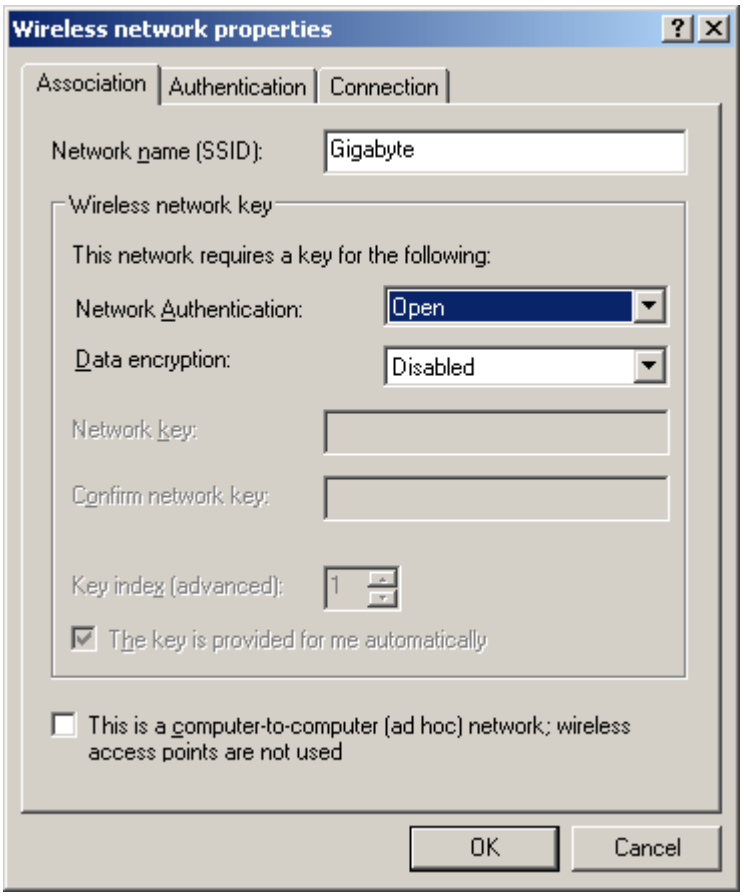

Рис. 28. Настройка профиля беспроводного соединения

Независимо от того, какой из перечисленных способов используется для создания профиля беспроводного соединения, после его создания беспроводной адаптер должен автоматически установить соединение с точкой доступа.

3.7. Обмен данными в беспроводной сети

Если после настройки точки доступа и беспроводных адаптеров сетевых компьютеров вы попытаетесь получить доступ с одного ПК к данным, хранящимся на другом ПК, то, скорее всего, у вас ничего не получится. Дело в том, что данные, к которым необходимо организовать сетевой доступ, должны располагаться в разделяемой (shared) папке или даже на логическом диске. Поэтому на тех компьютерах, между которыми предполагается реализовать обмен данными, необходимо создать разделяемые сетевые ресурсы.

Для этого щёлкните левой кнопкой мыши на значке ' My Computer ' (Мой компьютер) и в открывшемся окне выберите логический диск (или папку), которую требуется сделать доступной для пользователей сети. Щёлкнув на ней правой кнопкой мыши, выберите в открывшемся

списке пункт 'Sharing and Security:'. В открывшемся диалоговом окне (рис. 29) перейдите на вкладку Sharing.

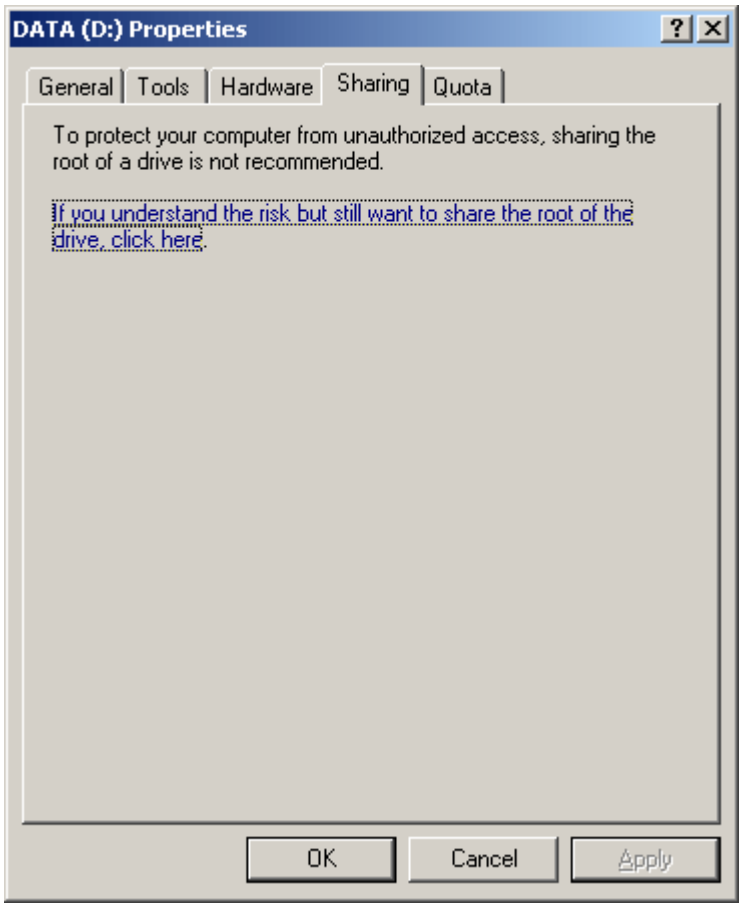

Рис. 29. Диалоговое окно создания разделяемого логического диска

В этом диалоговом окне имеется только одна опция: 'if you understand the risk but still want to share the root of the drive, click here'. Это не что иное, как предупреждение о риске разделения логического диска. Если вы, несмотря ни на что, желаете сделать этот диск доступным для пользователей сети, то просто щёлкните на этой надписи. Диалоговое окно изменит свое вид, и в новом окне (рис. 30) нужно будет выбрать пункт 'Share this folder on the network' (сделать данную папку (диск) доступной для пользователей сети'). Кроме того, если вы хотите, чтобы данные разделяемого диска могли изменять (а не только скачивать) пользователи сети, то необходимо дополнительно выбрать опцию 'Allow network users to change my files' (разрешить пользователям сети изменять файлы).

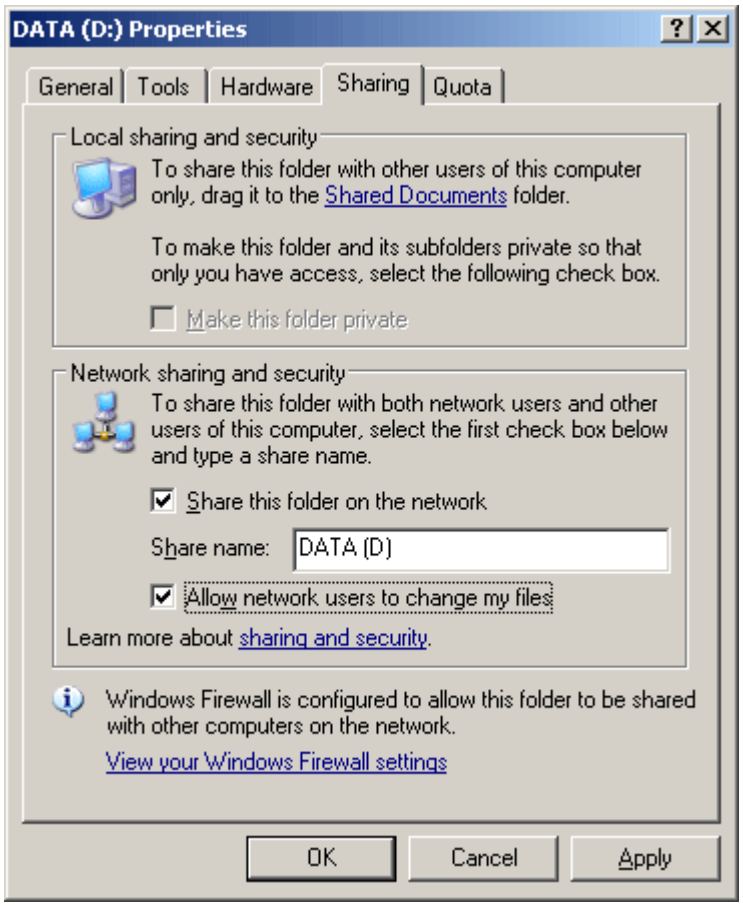

Рис. 30. Задание опций разделяемого логического диска

Реализация разделяемого доступа в Интернет с использованием аналогового модема

Следующий важный аспект, который необходимо рассмотреть – это реализации разделяемого доступа в Интернет с использованием аналогового модема. Для этого прежде всего необходимо присвоить статический IP-адрес компьютеру, к которому подключён модем.

IP-адрес компьютера должен быть 192.168.0.1, а маска подсети - 255.255.255.0. Использование другого IP-адреса при создании разделяемого доступа в Интернет не допускается. В крайнем случае, если вы зададите другой IP-адрес, то при активизации разделяемого доступа вам будет послано уведомление об автоматическом изменении IP-адреса сервера.

Соответственно, IP-адрес самой точки доступа должен находиться в той же подсети, то есть быть равным 192.168.0.x с маской подсети 255.255.255.0. Если IP-адрес точки доступа по умолчанию отличается от указанного, то его следует сначала поменять.

После того как компьютеру будет присвоен статический IP-адрес, щелкните на значке My Network Places (Сетевое окружение) правой кнопкой мыши и в открывшемся списке выберите пункт Properties (Свойства). В открывшемся окне Network Connection (Сетевые соединения) выберите значок с названием соединения с Интернетом (название этого соединения задаётся произвольно при настройке соединения с Интернетом). Щёлкнув на нём правой кнопкой мыши, перейдите к пункту Properties и в открывшемся диалоговом окне Internet Properties (Свойства соединения с Интернетом) перейдите к вкладке Advanced.

В группе Internet Connection Sharing (Разделяемый доступ в Интернет) отметьте пункт Allow other network users to connect through this computer's Internet connection (Разрешить пользователям локальной сети пользоваться соединением с Интернетом через данный компьютер). Тем самым вы активизируете разделяемый доступ в Интернет для всех компьютеров вашей локальной сети. Автоматически в этом диалоговом окне окажутся отмеченными и два последующих пункта. Первый из них (Establish a dial-up connection whenever a computer on my network attempts to access the Internet) разрешает устанавливать соединение с Интернетом по требованию с любого компьютера вашей сети. Даже при отсутствии в данный момент на сервере (компьютере, к которому подключен модем) непосредственного соединения с Интернетом в случае соответствующего запроса с любого компьютера сети модем начнёт набор номера провайдера и установит соединение с Интернетом.

Второй пункт (Allow other networks users to control or disable the shared Internet connection) разрешает всем пользователям сети управлять разделяемым доступом в Интернет.

После того как разделяемый доступ в Интернет будет активизирован на компьютере, необходимо проверить сетевые настройки на всех остальных компьютерах сети. В отличие от сервера, все остальные компьютеры сети не должны иметь статического IP-адреса. Для того чтобы убедиться, что это действительно так, повторите процедуру назначения IP-адреса на всех компьютерах сети, но в диалоговом окне Internet Protocol (TCP/IP) Properties отметьте пункт Obtain an IP address automatically. При этом все компьютеры локальной сети (кроме сервера) будут автоматически получать динамические IP-адреса.

Не вникая во все тонкости динамического конфигурирования сети, отметим лишь, что на сервере будет запущен специальный сервис DHCP, который и будет заниматься автоматическим распределением IP-адресов в диапазоне той же самой подсети, что и сервер, то есть в диапазоне 192.168.0.x.

По окончании настройки сервера и всех компьютеров сети можно будет пользоваться разделяемым доступом в Интернет.

3.8. Настройка защиты беспроводной сети

Если первоначальное тестирование созданной беспроводной сети прошло успешно, можно переходить ко второму этапу - настройке безопасности сети для предотвращения несанкционированного доступа в свою сеть.

Прежде всего отметим, что созданная нами беспроводная сеть является одноранговой, то есть все компьютеры этой сети равноправны, и выделенный сервер, регламентирующий работу сети, отсутствует. Поэтому полагаться на политику системной безопасности в такой сети бессмысленно, поскольку подобной политики там просто нет. К сожалению, посредством операционной системы Windows XP Professional в такой сети не удастся настроить список авторизованных для доступа в сеть пользователей. Но выход всё же есть. Для этого необходимо воспользоваться возможностями точки доступа или беспроводного маршрутизатора, то есть реализовать защиту сети на аппаратном уровне.

3.8.1. Фильтрация по MAC-адресам

На первой 'линии обороны' желательно настроить фильтрацию по MAC-адресам. MAC-адрес - это уникальный (в том смысле, что не может быть двух одинаковых) идентификатор конкретного сетевого оборудования, например, беспроводного адаптера или точки доступа. MAC-адрес записывается в шестнадцатеричном формате. Например, MAC-адрес может быть записан в виде 00-0 F-EA-91-77-9 B. Для того чтобы выяснить MAC-адрес установленного беспроводного адаптера, нажмите кнопку 'Start' (Пуск) и в появившемся списке выберите пункт 'Run:' (Выполнить). В открывшемся окне наберите команду 'cmd' (рис. 31), что приведёт к запуску окна командной строки.

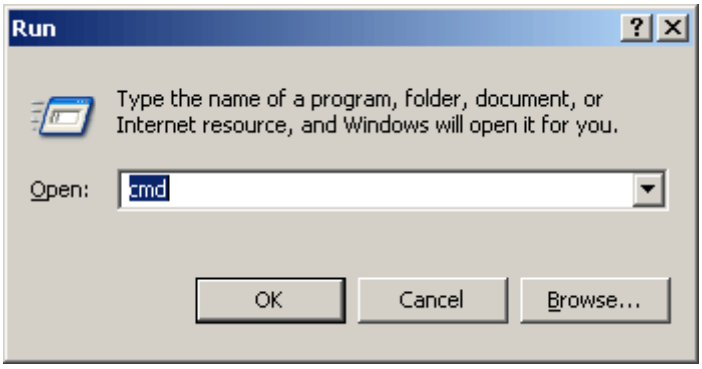

Рис. 31. Запуск окна командной строки

В командной строке наберите команду 'ipconfig/all' (рис. 32).

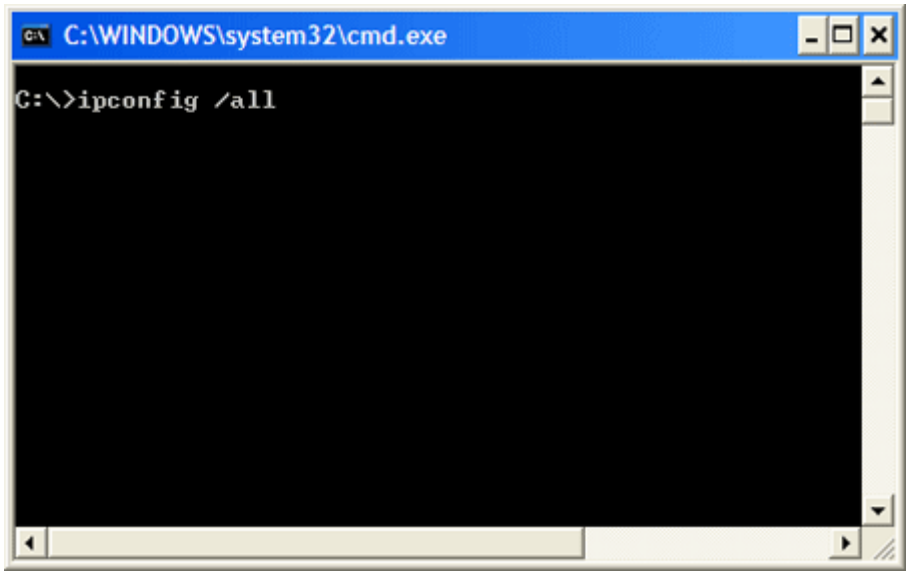

Рис. 32. Выполнение команды 'ipconfig/all'

Это позволит выяснить IP-адрес беспроводного адаптера и его MAC-адрес.

После того как будут выяснены MAC-адреса всех компьютеров в сети, необходимо настроить таблицу фильтрации по MAC-адресам на точке доступа. Практически любая точка доступа и маршрутизатор предоставляют подобную возможность. Настройка этой таблицы сводится, во-первых, к необходимости разрешить фильтрацию по MAC-адресам, а во-вторых, к внесению в таблицу разрешённых MAC-адресов беспроводных адаптеров. После настройки таблицы фильтрации по MAC-адресам любая попытка входа в сеть с использованием беспроводного адаптера, MAC-адрес которого не внесён в таблицу, будет отвергнута точкой доступа.

3.8.2 Настройка режимов шифрования и аутентификации пользователей

Любая точка доступа, и тем более беспроводной маршрутизатор, предоставляют в распоряжение пользователей возможность настраивать шифрование сетевого трафика при его передаче по открытой среде. Существует несколько стандартов шифрования, которые поддерживаются точками доступа.

Первым стандартом, использующимся для шифрования данных в беспроводных сетях, был стандарт WEP (Wired Equivalent Privacy). В соответствии со стандартом WEP шифрование осуществляется с помощью 40-или 104-битного ключа (некоторые модели беспроводного оборудования поддерживают и более длинные ключи), а сам ключ представляет собой набор ASCII-символов длиной 5 (для 40-битного) или 13 (для 104-битного ключа) символов. Набор этих символов переводится в последовательность шестнадцатеричных цифр, которые и являются ключом. Допустимо также вместо набора ASCII-символов напрямую использовать шестнадцатеричные значения (той же длины).

Как правило, в утилитах настройки беспроводного оборудования указываются не 40-или 104-битные ключи, а 64-или 128-битные. Дело в том, что 40 или 104 бита - это статическая часть ключа, к которой добавляется 24-битный вектор инициализации, необходимый для рандомизации статической части ключа. Вектор инициализации выбирается случайным образом и динамически меняется во время работы. В результате с учётом вектора инициализации общая длина ключа получается равной 64 (40+24) или 128 (104+24) битам.

Протокол WEP-шифрования, даже со 128-битным ключом, считается не очень стойким, поэтому в устройствах стандарта 802.11g поддерживается улучшенный алгоритм шифрования WPA (Wi-Fi Protected Access), который включает протоколы 802.1x, EAP, TKIP и MIC.

Протокол 802.1x - это протокол аутентификации пользователей. Для своей работы данный протокол требует наличия выделенного RADIUS-сервера, которого в домашней сети, естественно, нет. Поэтому воспользоваться данным протоколом в домашних условиях не удастся.

Протокол TKIP (Temporal Key Integrity Protocol) – это реализация динамических ключей шифрования. Ключи шифрования имеют длину 128 бит и генерируются по сложному алгоритму, а общее количество

возможных вариантов ключей достигает сотни миллиардов, и меняются они очень часто.

Протокол MIC (Message Integrity Check) – это протокол проверки целостности пакетов. Протокол позволяет отбрасывать пакеты, которые были 'вставлены' в канал третьим лицом.

Помимо упомянутых протоколов, многие производители беспроводного оборудования встраивают в свои решения поддержку стандарта AES (Advanced Encryption Standard), который приходит на замену TKIP.

Итак, после небольшого экскурса в основные понятия технологии шифрования и сетевой аутентификации пользователей приступим к настройке нашего беспроводного оборудования. При этом будем по возможности придерживаться следующих рекомендаций: если все устройства в сети поддерживают шифрование на основе WPA, мы будем использовать именно этот способ шифрования (в противном случае следует выбрать WEP-шифрование со 128-битным ключом). Ну а если все устройства в сети поддерживают AES-шифрование, то воспользуемся именно им.

Начнём с настройки беспроводной точки доступа. Прежде всего, выберем тип аутентификации (Authentication). В списке типа аутентификации возможны следующие варианты:

- Open System (открытая);
- Shared Key (общая);
- 802.1x;
- WPA и WPA2;
- WPA Pre-Shared Key и WPA2 Pre-Shared Key;

Open System (режим по умолчанию) – фактически это режим, не имеющий сетевой аутентификации. При выборе данного режима для входа в беспроводную сеть достаточно знать лишь идентификатор сети (SSID).

В режиме Pre-Shared Key возможно использование WEP-шифрования трафика. Причём для входа в сеть требуется установить общий для всей сети WEP-ключ шифрования.

3.8.3. Настройка WEP-шифрования

Если по каким-либо соображениям принято решение использовать WEP-шифрование, то необходимо установить тип аутентификации Shared Key. Далее следует установить размер ключа (рекомендуемое значение 128 бит) и ввести сам ключ. К примеру, ключ можно записать в шестнадцатеричном формате: 00-11-22-33-44-55-66-77-88-aa-bb-cc-dd. Всего возможно задать до четырёх значений ключа, и, если задано несколько ключей, необходимо указать, какой именно из них используется.

Далее требуется реализовать аналогичные настройки на всех беспроводных адаптерах сетевых компьютеров. Делается это либо с помощью утилиты управления (в нашем случае Intel PROSet / Wireless), либо посредством клиента Microsoft. Если используется утилита Intel PROSet / Wireless, откройте главное окно утилиты, выберите профиль соединения и нажмите на кнопку 'Свойства:'. В открывшемся диалоговом окне (рис. 33) перейдите к закладке 'Настройка защиты' и выберите тип сетевой аутентификации 'Общая' (это соответствует типу Shared Key).

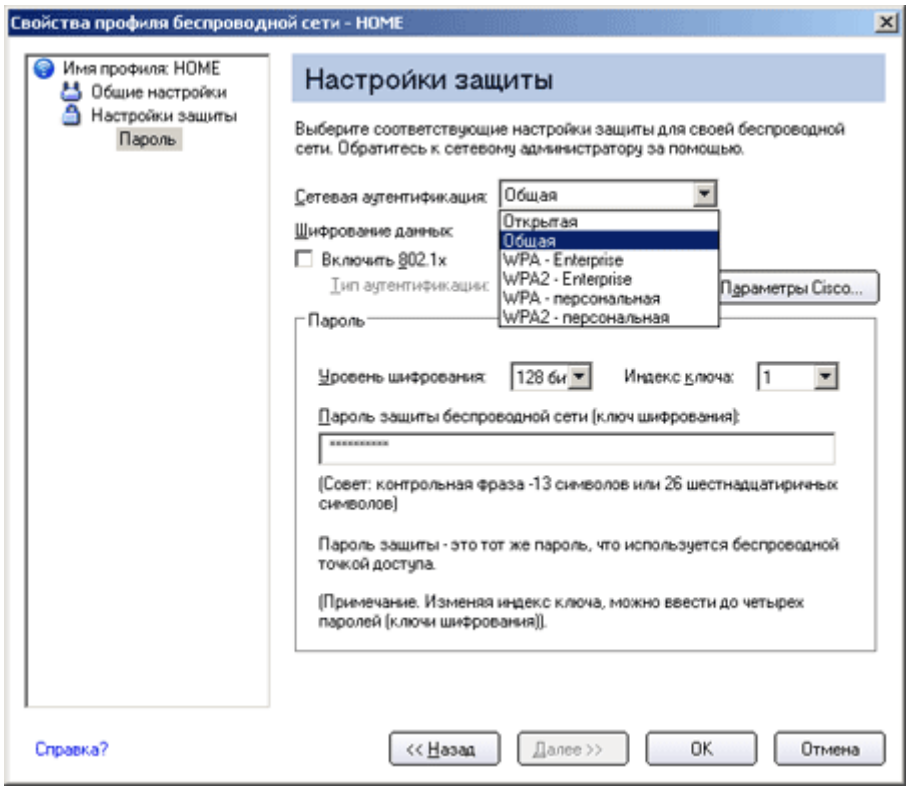

Рис. 33. Задание параметров WEP-шифрования на беспроводном адаптере с помощью утилиты Intel PROSet/Wireless

Далее выберите тип шифрования WEP, задайте длину ключа 128 бит и введите ключ шифрования (00-11-22-33-44-55-66-77-88-aa-bb-cc-dd).

При использовании для настройки адаптера клиента Microsoft откройте диалоговое окно Wireless Network Connection Properties (Свойства беспроводного сетевого соединения) и на вкладке 'Wireless Networks' (беспроводные сети) выберите нужный профиль беспроводного соединения. Нажмите на кнопку 'Properties' (Свойства) и в открывшемся диалоговом окне (рис. 34) установите тип сетевой аутентификации (Network Authentication) Shared, тип шифрования (Data encryption) WEP и введите точно такой же ключ шифрования, который был задан при настройке точки доступа.

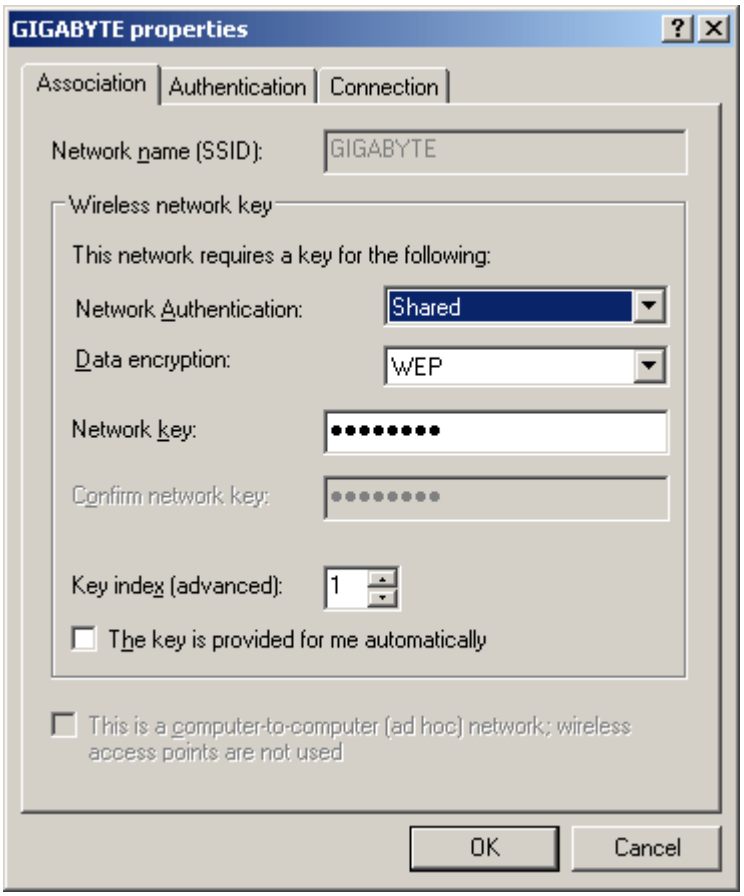

Рис. 34. Задание параметров WEP-шифрования на беспроводном адаптере с помощью клиента Microsoft

3.8.4. Настройка WPA-шифрования

Если есть возможность использовать WPA-шифрование (то есть если все устройства сети его поддерживают), то рекомендуется выбрать именно этот тип шифрования.

Существует два типа WPA-шифрования: стандартный режим WPA (иногда встречается название WPA - Enterprise) и WPA Pre-shared key или WPA - персональный.

Режим WPA – Enterprise используется в корпоративных сетях, поскольку требует наличия RADIUS-сервера. Естественно, что в домашних условиях воспользоваться данным режимом не удастся.

А вот режим WPA Pre-shared key предназначен для персонального использования. Этот режим предусматривает использование заранее заданных ключей шифрования (пароль доступа), одинаковых для всех сетевых устройств, а первичная аутентификация пользователей осуществляется с использованием данного ключа.

Существует также алгоритм WPA2 (следующая версия протокола WPA). Если все устройства беспроводной сети поддерживают данный режим, то вполне можно им воспользоваться. Настройки в данном случае осуществляются точно такие же, как и в случае WPA-режима.

В качестве алгоритмов шифрования при использовании стандарта WPA можно выбрать TKIP или AES.

Для настройки WPA-шифрования в главном окне настройки точки доступа выберите тип аутентификации WPA Pre-shared key и установите тип шифрования (WPA Encryption) TKIP или AES. Затем требуется задать ключ шифрования (WPA PSK Passphrase). В качестве ключа может быть любое слово (например, FERRA).

Далее необходимо реализовать аналогичные настройки на всех беспроводных адаптерах сетевых компьютеров. Делается это точно так же, как и в случае уже рассмотренного нами WEP-шифрования. Пример настройки беспроводного адаптера при помощи утилиты управления Intel PROSet / Wireless показан на рис. 35.

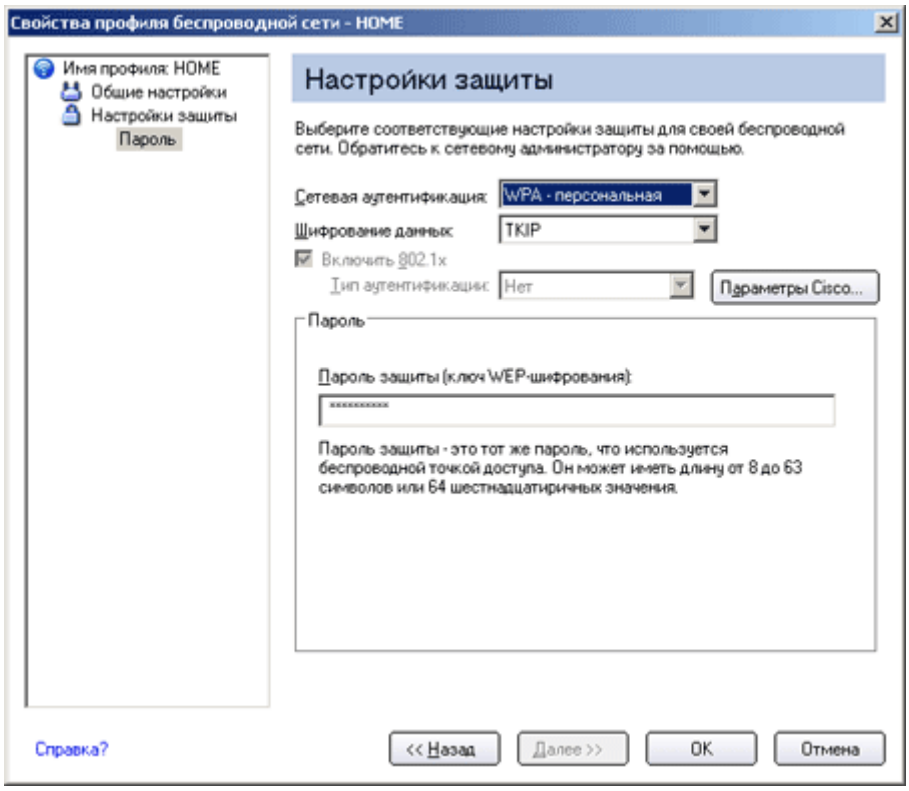

Рис. 35. Пример настройки WPA-шифрования на беспроводном адаптере с помощью утилиты Intel PROSet/Wireless

4. Тестирование сети с помощью специального оборудования

4.1. Общие сведения о тестировании сетей с помощью специального оборудования

Любая компьютерная сеть состоит из рабочих станций, которые связаны как между собой, так и с серверами.

Первым этапом построения любой сети является прокладка кабеля. Кабель используется как для объединения компьютеров между собой, так и со специальным сетевым оборудованием.

Перед прокладкой кабеля, кабель необходимо протестировать.

Тестированию подлежат следующие параметры:

1. Длина кабеля;
2. Сопротивление кабеля;
3. Уровень шумов в кабеле;
4. Затухание сигналов в кабеле;
5. Отражения сигналов на ближнем конце.

Для проверки кабеля применяются два типа приборов:

1. **Кабельные пробники** – устройства, которые позволяют проверить наличие либо отсутствие электрического сигнала между двумя точками.
2. **Кабельные тестеры** –устройства, которые позволяют определять определенные электрические характеристики такие как: отражение сигнала на ближнем конце кабеля, уровень наводимых шумов, т.е. этот приборы, позволяющие судить о правильности работы проверяемого кабеля.

4.2. Ручные кабельные пробники

Как правило, ручные кабельные пробники (рис. 36) это небольшие устройства, которые имеют питания от батареек и применяются они для проверки, экранированной и не экранированной витой пары.

Рис. 36. Ручной кабельный пробник

Принцип работы состоит в подаче напряжения на один конец кабеля и проверки наличия напряжения или его отсутствия на удаленном конце кабеля. Таким образом, кабель можно проверить на обрыв, либо использовать такой прибор при поиске нужной пары проводов в пучке проводов.

Вне зависимости от модели большинства этих приборов они состоят из двух компонентов, которые подключаются к противоположным концам кабеля.

4.3. Кабельные тестеры

Кабельные тестеры (рис. 37) – это устройства по своим возможностям на порядок выше, чем у кабельных пробников, с помощью тестеров можно замерять уровни сигналов на ближнем конце кабеля, уровень затухания, уровень шума, импеданс кабеля.

Кабельные тестеры могут производить расчеты по определению длины кабеля и расстояния по кабелю до поврежденного участка. Кроме этого такие тестеры используются для проверки соответствия проводов, т.е. правильности подключения пар кабеля к контактам терминатора. В своей работе эти тестеры не используют ПК.

Часть моделей тестеров выводят на ЖК панель формализованный текст, который содержит описание того или иного типа ошибки при проходе того или иного теста. Эти устройства питаются от аккумуляторных батарей, а часть моделей работают от сети 220 В.

Кроме этого часть дорогих моделей тестеров отображают ряд дополнительных функций таких как: нагрузка в сети, осуществляют сбор сведений о количестве возникающих коллизий.

Рис. 37. Кабельный тестер

Часть тестеров позволяют сохранять протоколы работы в буферной памяти для последующего их анализа. Они так же имеют возможность подключиться к ПК и к принтеру для считывания протоколов.

4.4. Аудит сетевой кабельной системы

Аудит (проверка) сетевой кабельной системы (СКС) предусматривает следующие виды работ:

- осмотр оборудования;
- анализ схемы сети;
- проверка целостности сети;
- тестирование всех элементов и узлов;
- сертификация СКС по одной из категорий – cat. 5, cat. 6, cat. 7 и других;
- оформление технической документации;

- при обнаружении нарушений в системе – составление плана проведения ремонтных работ;
- при организации новой ЛВС: отладка серверов, внедрение службы каталогов Active Directory и др.;
- при необходимости – дополнение ЛВС новыми элементами, например, системой видеонаблюдения (мы также осуществляем продажу систем видеонаблюдения, их установку и интеграцию в сеть.

Если СКС смонтирована правильно, она должна служить не менее 10 лет. Когда приходит время замены, именно стабильность работы сети играет важнейшую роль в стабильности дальнейшей работы информационной системы фирмы.

В связи с этим СКС регламентируется несколькими международными и региональными стандартами, основными из которых являются:

- американский стандарт EIA/TIA-568B;
- европейский стандарт CENELEC EN 50173;
- международный стандарт ISO/IEC IS 11801;
- российские стандарты ГОСТ Р 53246-2008 (общие требования к системам СКС) и ГОСТ Р 53245-2008 (методика испытаний), которые вступили в силу с 1 января 2010 г.

5. Тестирование сети с помощью специального программного обеспечения

Программы для тестирования сети позволяют не только определить скорость обмена информацией между компьютером и сетевым ресурсом (и показать их в цифровом или графическом виде), но и существенно обезопасить ваш ПК. Такие программы способны к сбору данных, определенной привязке, оценке собранных данных. На основании полученной информации, программы для тестирования могут выявить уязвимости и оценить их опасность.

Специальное программное обеспечение **AIDA64 Network Audit** позволяет провести подробную инвентаризацию программного и аппаратного обеспечения на клиентских компьютерах с ОС Windows, подключенных к одной корпоративной сети (рис. 38).

Рис. 38. Настройка инвентаризации в AIDA64 Network Audit

Основные возможности программы AIDA64 Network Audit:

- точная низкоуровневая информация о материнской плате и центральном процессоре;

- подробная информация о видеоадаптере, драйверах и мониторе;
- информация обо всех устройствах хранения;
- исчерпывающая информация о сетевых адаптерах, мультимедиа и устройствах ввода;
- информация о других устройствах (PCI, PnP, PCMCIA, USB);
- подробная информация о Windows, включая дату установки, лицензионный ключ и многое другое;
- информация об общих сетевых ресурсах, список пользователей, групп и многое другое;
- большой объем информации о сетевом статусе, учетных записях почты, сетевых ресурсах и настройках интернет;
- подробная информация об установленных программах, запланированных задачах и программах в автозапуске;
- информация о безопасности операционной системы;
- список межсетевых экранов, антишпионов и антитроянов;
- тест стабильности системы;
- панель CPUID;
- мониторинг аппаратного обеспечения;
- тесты производительности CPU и FPU;
- тесты производительности памяти;
- модуль тестирования производительности дисков;
- обнаружение возможных проблем настройки и совместимости программного и аппаратного обеспечения;
- мастер отчетов;
- отправка по почте и распечатка отчетов;
- русская/английская зарегистрированная и портативная версии в одном установщике.

Поддержка параметров командной строки позволяет сделать инвентаризацию полностью автоматической, а отчеты, созданные по компьютерам, – сохранить в открытых форматах, пригодных для дальнейшей обработки или в формате базы данных SQL. Встроенная функция управления изменениями позволяет отследить изменения между различными снимками сетевого аудита, сделанными в разное время. AIDA64 Network Audit совместима со всеми 32- и 64-битными версиями ОС Windows, в том числе Windows 8.1 и Windows Server 2012 R2.

Для бизнес-версий AIDA64 можно загрузить инструмент, позволяющий системным администраторам также собирать аудиторские отчеты с клиентов на базе ОС Linux.

Объем информации, собираемый программой, можно полностью подстроить под требования пользователя, а администраторы получают возможность выбора между несколькими шаблонами (профилями отчета).

Гибкость конфигурации

Программа не требует установки, следовательно, ее можно запустить с общей центральной папки на любом клиенте в доменной среде (рис. 39).

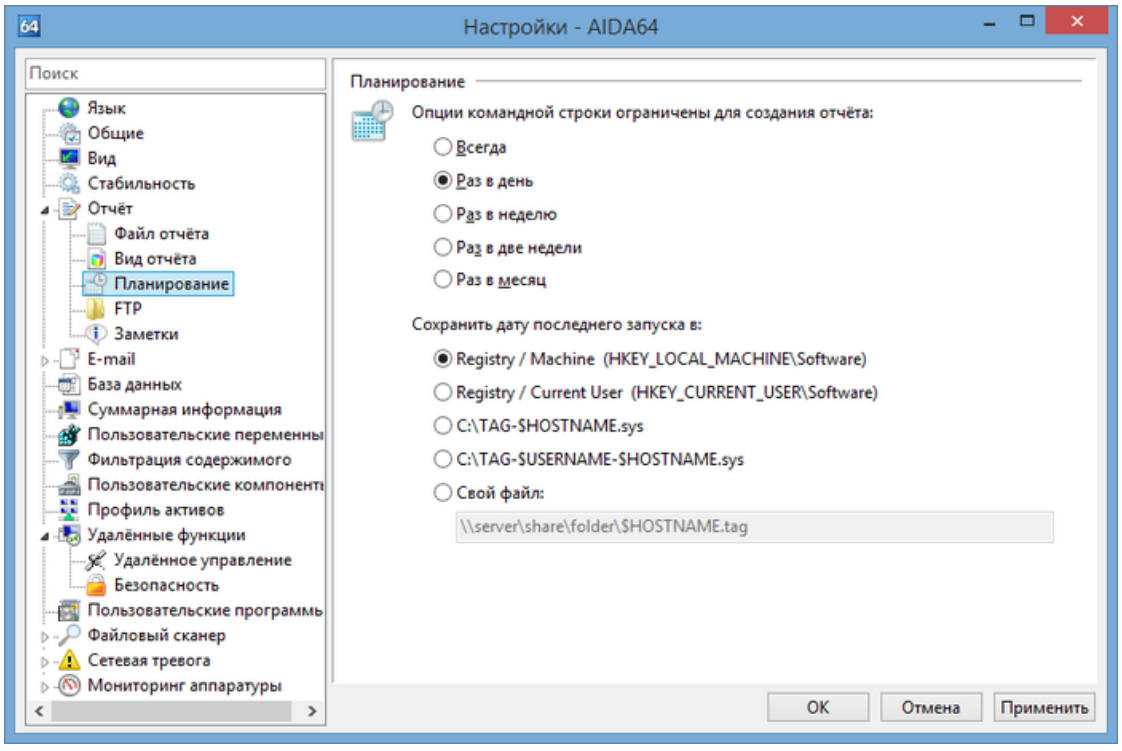

Рис. 39. Настройка работы AIDA64 Network Audit

Конечно же, AIDA64 позволяет установить частоту создания отчетов (инвентаризации) компьютеров: отчеты можно собирать раз в месяц, раз в неделю, раз в сутки или после каждого входа пользователя в систему. Поскольку AIDA64 поддерживает параметры командной строки, процесс может быть полностью автоматизированным.

Отчеты можно сохранять в открытых форматах, готовых для дальнейшей обработки, а также в базе данных SQL. Версии AIDA64 Network Audit и AIDA64 Business поддерживают следующие форматы отчетов:

- обычный текстовый формат (TXT);
- HTML;
- MHTML;
- XML;
- CSV;
- MIF;
- INI;
- ADO (для вставки в базу данных).

Интегрированный администратор аудита

Администратор аудита (рис. 40) позволяет просматривать и анализировать инвентаризацию программного и аппаратного обеспечения компьютерного парка.

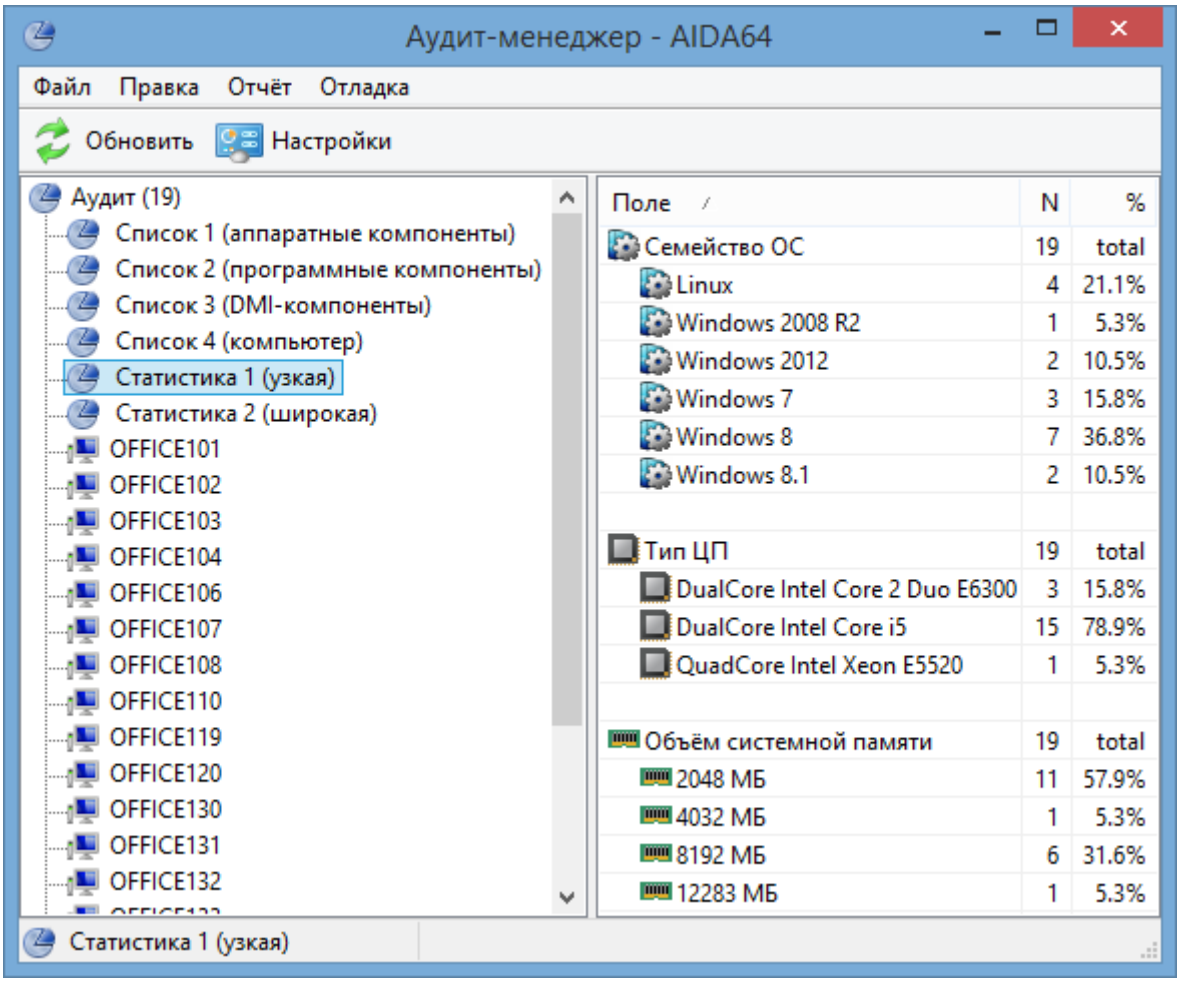

Рис. 40. Администратор аудита

Здесь можно также отфильтровать данные и создать графики. Например, системные администраторы могут с легкостью определить клиентов, которые не отвечают минимальным системным требованиям новой применяемой программы, или для которых не установлены последние пакеты обновлений операционных систем и систем безопасности. В статистическом отчете (который можно отфильтровать по нескольким критериям), предоставляемом программой, можно сразу же увидеть процентное соотношение корпоративных компьютеров с определенным типом процессора, размером памяти или установленной версией Windows.

Также можно отследить изменения между снимками сетевого аудита, сделанными в разное время, и обнаружить изменения в оборудовании или программной среде компьютеров.

Интегрированное управление изменениями

AIDA64 Network Audit и AIDA64 Business позволяют отследить изменения между снимками сетевого аудита, сделанными в разное время (рис. 41).

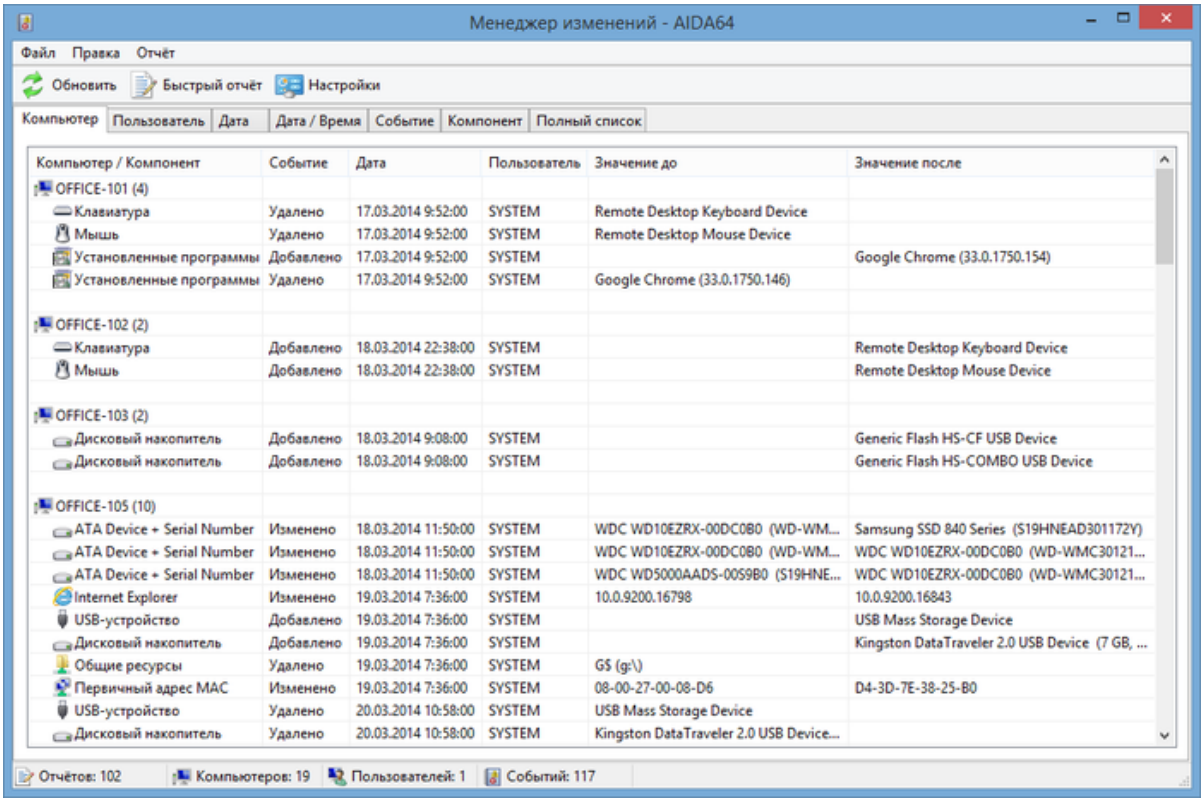

Рис. 41. Интегрированное управление изменениями

Всего при помощи нескольких нажатий системные администраторы могут определить те компьютеры в корпоративной сети, конфигурация оборудования которых была изменена, или на которых установлено новое программное обеспечение, возможно, без разрешения. Можно также отследить, установлено ли на компьютере последнее обновление программ или операционной системы.

При помощи доступных файлов отчетов в формате CSV или SQL, функция AIDA64 Change Manager позволяет отсортировать изменения по пользователям, по компьютеру, по дате, компоненту или событию, а также удалить некоторые выбранные компьютеры или пользователей из списка.

Мониторинг изменений в режиме реального времени

AIDA64 может отправлять оповещения в случае обнаружения изменений программного (или аппаратного) обеспечения или при возникновении каких-либо проблем. Например, системные администраторы могут затребовать оповещения по электронной почте

в случае, если пользователь подключает USB-накопитель к своему компьютеру, хотя не имеет на это права. При необходимости в подобных случаях специалист может даже вмешаться при помощи функции удаленного контроля.

AIDA64 поддерживает следующие виды инициации оповещений, показанные на рис. 42.

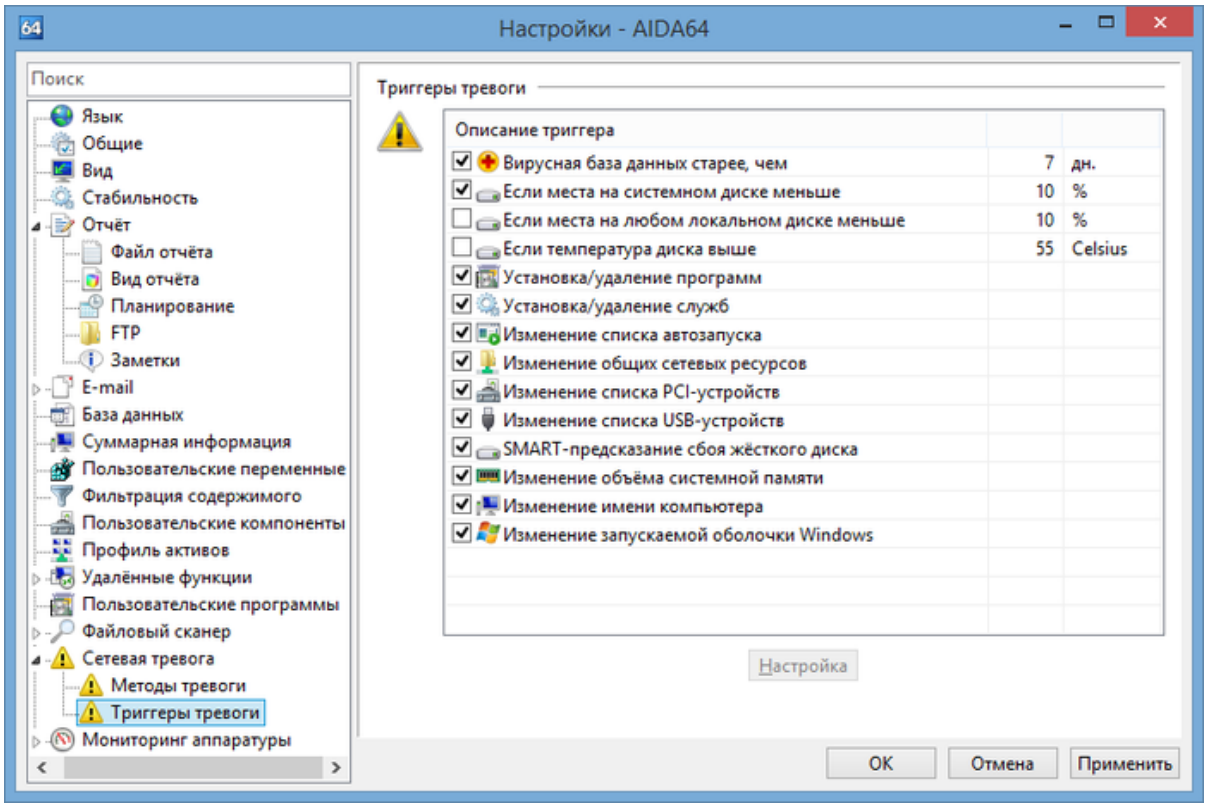

Рис. 42. Инициация оповещений

При обнаружении события для оповещения, AIDA64 может отправить оповещение как пользователю, так и администратору несколькими способами, например, отобразив окно оповещения, отправив оповещение по электронной почте или сообщение Windows, или же записав событие в журнал.

Заключение

Таким образом, в методических указаниях изложены возможности сопряжения аппаратных и программных средств в составе информационных и автоматизированных систем, функционирующих в компьютерных сетях.

Описаны основные модели, технологии и протоколы доступа к среде передачи данных, структуру протоколов доступа к среде, а также основные типы сред передачи данных, их характеристики и область их применения.

Определены элементы структурированной кабельной системы и ограничения их применения.

Даны практические рекомендации по планированию и монтажу структуры компьютерной сети, а также размещению сетвого оборудования.

Уровень изложения материала предполагает знание основ вычислительной техники, принципов построения и функционирования компьютеров, принципов организации программных и информационных средств.

Литература

1. Хорев П.Б. Методы и средства защиты информации в компьютерных системах. – М.: Академия, 2007.

2. Компьютерные сети: Пер. с англ. / Э. Таненбаум; пер.: В. Шрага. – 4-е изд. – СПб.: Питер, 2007. – 991[1] с.: ил. – (Классика Computer Science). – Библиогр.: с. 941-970.

3. Современные беспроводные сети: состояние и перспективы развития / И. А. Гепко [и др.]; ред. В. Ф. Олейник. – Киев: ЕКМО, 2009. – 671 с.

4. Беспроводные сети Wi-Fi: учебное пособие / А. В. Пролетарский [и др.]. – М.: Интернет-Университет Информационных Технологий, 2007; М.: БИНОМ. Лаборатория знаний, 2007. – 215 с.

5. Сети. Беспроводные технологии: пер. с англ. / П. Беделл; пер. Р. М. Евтеев. – М.: НТ Пресс, 2008. – 441 с.

6. Киселев С.В. Аппаратные средства персоанльного компьютера: учеб. пособие / [С.В. Киселев, С.В. Алексахин, А.В. Остроух и др.]. – 3-е изд., стер. - М.: Издательский центр «Академия». 2012. – 64 с. – ISBN 978-5-7695-8890-7.

7. Краснянский М.Н., Остроух А.В., Карпушкин С.В., Обухов А.Д. Разработка комплексной системы управления научно - инновационной деятельностью: взаимодействие базы данных изделий и архива документации // Приборы и системы. Управление, контроль, диагностика. – 2014. – №12. – С. 19-23.

8. Краснянский М.Н., Карпушкин С.В., Обухов А.Д., Молоткова Н.В., Галыгина И.В., Остроух А.В. Структура системы электронного документооборота для управления научно-образовательной деятельностью высшего учебного заведения // Промышленные АСУ и контроллеры. – 2014. – №8. – С. 23-31.

9. Николаев А.Б. Информационные технологии в менеджменте и транспортной логистике: учебное пособие / А.Б. Николаев, А.В. Остроух. – Saint-Louis, MO, USA: Publishing House Science and Innovation Center, 2013. – 254 с. – ISBN 978-0-615-67110-9.

10. Остроух А.В. Ввод и обработка цифровой информации: учебник для нач. проф. образования / А.В. Остроух. – М.: Издательский центр «Академия», 2012. – 288 с. – ISBN 978-5-7695-9457-1.

11. Остроух А.В. Основы информационных технологий: учебник для сред. проф. образования / А.В. Остроух. – М.: Издательский центр «Академия», 2014. – 208 с. – ISBN 978-5-4468-0588-4.

12. Остроух А.В. Основы построения систем искусственного интеллекта для промышленных и строительных предприятий: монография / А.В. Остроух. – М.: ООО «Техполиграфцентр», 2008. – 280 с. – ISBN 978-5-94385-033-2.

13. Остроух А.В. Рефакторинг баз данных. Автоматизация технологических процессов рефакторинга баз данных промышленных предприятий / А.В. Остроух, Д.А. Пшеничный, О.Б. Рогова. – Saarbrucken, Germany: LAP LAMBERT Academic Publishing, 2013. – 133 p. – ISBN 978-3-659-38753-1.

14. Остроух А.В. Интеллектуальные системы в науке и производстве / А.В. Остроух, А.Б. Николаев. – Saarbrucken, Germany: Palmarium Academic Publishing, 2012. – 312 p. – ISBN 978-3-659-98006-0.

15. Остроух А.В. Мультимедиа-технологии / А.В. Остроух, А.М. Васьковский, А.Б. Николаев. – Saarbrucken, Germany: Palmarium Academic Publishing, 2012. – 228 p. – ISBN 978-3-659-98030-5.

16. Остроух А.В. Системы искусственного интеллекта в промышленности, робототехнике и транспортном комплексе: монография / А.В. Остроух – Красноярск: Научно-инновационный центр, 2013. – 326 с. – ISBN 978-5-906314-10-9.

17. Остроух А.В. Проектирование системы распределенных баз данных / А.В. Остроух, А.В. Помазанов. – Saarbrucken, Germany: Palmarium Academic Publishing, 2015. – 117 p. – ISBN 978-3-659-60041-8.

18. Остроух А.В., Николаев А.Б. Проект разработки виртуальных лабораторных работ в среде iLABS // Международный журнал прикладных и фундаментальных исследований. – 2013. – № 11. – С. 36-38.

19. Помазанов А.В. Методика оптимизации баз данных / А.В. Помазанов, А.И. Белоусова, А.О. Васильева, А.В. Остроух // В мире научных открытий. Серия «Проблемы науки и образования». – 2012. – №12. – С.49-54.

20. Помазанов А.В., Остроух А.В. Создание и тестирование распределённой системы работы с удалёнными узлами //

Автоматизация и современные технологии. – 2014. – №7. – С. 17-23.

21. Помазанов А.В., Остроух А.В. Новый подход к разработке прототипа распределенной системы баз данных промышленного предприятия // Промышленные АСУ и контроллеры. – 2014. – №9. – С. 11-20.

22. Сальный А.Г., Николаев А.Б., Остроух А.В., Оуер М.Е. Концепция интеграции программного и методического обеспечения кафедры АСУ МАДИ в среду iLAB // Автоматизация и управление в технических системах. – 2013. – № 2. – С. 3-8.

23. Сальный А.Г., Збавитель П.Ю., Николаев А.Б., Остроух А.В. Описание унифицированных программных модулей для лаборатории коллективного пользования // Автоматизация и управление в технических системах. – 2013. – № 2. – С. 12-17.

24. Суркова Н.Е. Методология структурного проектирования информационных систем: монография / Н.Е. Суркова, А.В. Остроух. – Красноярск: Научно-инновационный центр, 2014. – 190 с. – ISBN 978-5-906314-16-1.

25. M.N. Krasnyanskiy, A.V. Ostroukh, S.V. Karpushkin, A.D. Obukhov. Information Technology for the Development of Automated Control System for University Projects // Математические методы в технике и технологиях – ММТТ-27: сб. трудов XXVII Междунар. науч. конф.: в 12 т. Т.4. Секции 10, 11 / под общ. ред. А.А. Большакова. – Тамбов: Тамбовск. гос. техн. ун-т, 2014. – С. 42-45. – ISBN 978-5-7433-2386-9.

26. Ostroukh A.V., Nikolaev A.B. Development of virtual laboratory experiments in iLabs. International Journal of Online Engineering (IJOE). 2013. Vol. 9, No 6. pp. 41-44. DOI: 10.3991/ijoe.v9i6.3176.

27. A.V. Ostroukh, M.N. Krasnyanskiy, S.V. Karpushkin, A.D. Obukhov. Development of Automated Control System for University Research Projects // Middle East Journal of Scientific Research. 2014. Vol. 20 (12). pp. 1780-1784. DOI: 10.5829/idosi.mejsr.2014.20.12.21091.

28. A. Ostroukh, A. Pomazanov. Realtime Development and Testing of Distributed Data Processing System for Industrial Company // Middle East Journal of Scientific Research. 2014. Vol. 20 (12). pp. 2184-2193. DOI: 10.5829/idosi.mejsr.2014.20.12.21106.

29. Ostroukh A.V., Belousova A.I., Pavlov D.A., Yurchik P.F. Problems of organization and search the knowledge base in the CRM-systems // IOSR Journal of Engineering (IOSRJEN). 2014. Vol. 04. Issue 02. V3. pp. 18-23. DOI: 10.9790/3021-04231823. ANED: 0.4/3021-04231823.

30. Ostroukh A.V., Gusenitsa D.O., Golubkova V.B., Yurchik P.F. Integration of PDM and ERP systems within a unified information space of an enterprise // IOSR Journal of Computer Engineering (IOSR-JCE). 2014. Vol. 16. Issue 02. V6. pp. 31-33. DOI: 10.9790/0661-16263133. ANED: 11.0661/iosr-jce-E016263133.

31. Krasnyanskiy M.N., Karpushkin S.V., Obukhov A.D., Ostroukh A.V. Automated control system for university research projects // International Journal of Advanced Studies (iJAS). 2014. Vol. 4, Issue 1, pp. 22-26. DOI: 10.12731/2227-930X-2014-1-4.

32. Mikhail Nikolaevich Krasnyanskiy, Andrey Vladimirovich Ostroukh, Sergey Viktorovich Karpushkin, Artyom Dmitrievich Obukhov, Nataliya Vyacheslavovna Molotkova and Irnina Vladimirovna Galygina. Electronic Document Management Systems Structure for University Research and Education // Journal of Engineering and Applied Sciences. 2014. Vol 9. Issue 5. pp. 182-189. DOI: 10.3923/jeasci.2014.182.189.

33. A.V. OSTROUKH, A.B. NIKOLAEV, N.E. SURKOVA, M.N. KRASNYANSKIY. DEVELOPMENT OF LABORATORY WORK FOR REMOTE ACCESS LABORATORY // 14th SGEM GeoConference on Informatics, Geoinformatics and Remote Sensing, www.sgem.org, SGEM2014 Conference Proceedings, ISBN 978-619-7105-10-0 / ISSN 1314-2704, June 19-25, 2014, Vol. 1, 119-126 pp. DOI:10.5593/SGEM2014/B21/S7.016.

34. http://ru.wikipedia.org.

Содержание

Учебное издание

Остроух Андрей Владимирович

МОНТАЖ И ТЕСТИРОВАНИЕ КОМПЬЮТЕРНЫХ СЕТЕЙ

Методические указания

Издательство «Научно-инновационный центр»

660127, г. Красноярск, ул. 9 Мая, 5, 192

Тел. +7 (923) 358-10-20