Государственное образовательное учреждение
дополнительного профессионального образования
Центр повышения квалификации специалистов Санкт-Петербурга
«Региональный центр оценки качества образования
и информационных технологий»

ЛОКАЛЬНАЯ СЕТЬ ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ В ГЕТЕРОГЕННОЙ СРЕДЕ: ПРОЕКТИРОВАНИЕ, ОРГАНИЗАЦИЯ, РАЗВИТИЕ

Санкт-Петербург
2010

УДК 004.9
Л 73

Локальная сеть образовательного учреждения в гетерогенной среде: проектирование, организация, развитие: Сб. метод. материалов / Авт.-составитель В.Е. Ильин. – СПб.: ГОУ ДПО ЦПКС СПБ «Региональный центр оценки качества образования и информационных технологий», – 71 с.

В настоящее время при построении и эксплуатации локальных сетей (ЛС) образовательных учреждений (ОУ) сложилась непростая ситуация. С одной стороны, в соответствии с требованиями Министерства образования и Правительства РФ образовательные учреждения все шире должны внедрять свободное программное обеспечение, не отказываясь при этом от привычных программ компании Microsoft. То есть реально функционирующие ЛС ОУ будут гетерогенными – компьютеры ЛС будут функционировать под управлением разных операционных систем (MS Windows и Linux). Слабое знание операционной системы Linux вызывает определенные сложности построения таких сетей.

С другой стороны, анализ существующих ЛС ОУ Санкт-Петербурга показывает, что они представляют собой достаточно пеструю картину: в большинстве своем ЛС – одноранговые, но есть и ЛС с выделенными серверами. Документация на ЛС практически отсутствует, что вызывает трудности при развитии ЛС для удовлетворения потребностей учебного процесса и процесса управления ОУ. Вопросы проектирования и развития ЛС мало знакомы ответственным за информатизацию ОУ.

Ограниченный объем пособия и многообразность задач при построении ЛС не позволяют ответить на все возможные вопросы и решить все проблемы построения ЛС, но дают основные положения и подходы к типовому построению и эксплуатации ЛС ОУ.

В приложении к пособию на компакт-диске представлены развернутые тексты статей авторов, дополнительный справочный и учебный материал, полезные программы для анализа и построения локальных сетей.

Сборник ориентирован на учителей информатики, инженеров, обслуживающих ЛС, и административных работников ОУ, ответственных за информатизацию. Авторами статей являются специалисты с многолетним опытом администрирования локальных сетей образовательных учреждений.

Составитель сборника: старший методист РЦОКОиИТ Ильин Валерий Евгеньевич.

ISBN 978-5-91454-037-8

СОДЕРЖАНИЕ

АНАЛИЗ СОСТОЯНИЯ И ХАРАКТЕРИСТИК СУЩЕСТВУЮЩЕЙ ЛОКАЛЬНОЙ СЕТИ

С. Е. Дюбин, учитель информатики школы № 412 Петродворцового района Санкт-Петербурга

Локальная сеть – это группа из нескольких компьютеров, соединенных посредством кабелей или радиоканалов, используемых для передачи информации между компьютерами. Для соединения компьютеров в локальную сеть необходимо сетевое оборудование и программное обеспечение.

Локальная сеть предоставляет возможность совместного использования оборудования. Оборудование, программы и данные информации объединяют одним термином: *ресурсы*. Можно считать, что основное назначение локальной сети – *доступ к ресурсам*. Часто дешевле создать локальную сеть и установить один принтер на все подразделение, чем приобретать по принтеру для каждого рабочего места. Файловый сервер сети позволяет обеспечить совместный доступ к программам. В локальной сети удобнее реализовывать администрирование ресурсов, контролировать ход работ над проектами в сети проще, чем иметь дело со множеством автономных компьютеров.

Прежде чем проводить работы по развитию локальной сети или проектированию новой сети, следует провести анализ состояния и характеристик существующей локальной сети (аудит сети).

Анализ состояния и характеристик (аудит) локальной сети

Анализ состояния и характеристик (аудит) локальной сети – это комплекс мероприятий, направленных на выяснение текущего состояния дел в локальной сети образовательного учреждения (количество и размещение компьютеров и сетевого оборудования, выявление характеристик компьютеров и установленного программного обеспечения, определение структуры кабельной системы), поиск и идентификацию «узких мест». По результатам аудита готовится отчет, описывающий текущее положение дел и содержащий рекомендации по дальнейшей модификации или эксплуатации локальной сети.

В каких случаях проводится аудит локальной сети?

Аудит локальной сети целесообразно проводить в следующих случаях:

1) перед модернизацией сети, чтобы можно было спроектировать новую сеть на основе объективных данных;

2) после модернизации сети, чтобы убедиться, что локальная сеть была реализована адекватно требованиям образовательного процесса;

3) для оценки качества сервиса. Например, чтобы убедиться, что провайдер сети Интернет выполняет взятые на себя обязательства по качеству предоставляемого сервиса (пропускная способность канала, время задержки, доступность канала и т.п.);

4) при передаче функций администрирования локальной сети другому лицу или организации.

Порядок проведения аудита локальной сети

Вне зависимости от объекта обследования проведение аудита включает три основных этапа:

- постановка задачи и уточнение границ работ;
- сбор данных. Инвентаризация сети;
- анализ данных и подготовка отчета.

Постановка задачи и уточнение границ работ

На данном этапе проводятся организационные мероприятия по подготовке проведения аудита:

1) уточняются цели и задачи аудита;

2) подготавливается и согласовывается техническое задание на проведение аудита.

Сбор данных. Инвентаризация сети

Инвентаризация сети на этом этапе обычно совмещается с интервьюированием персонала заказчика, предполагается осмотр активного и пассивного оборудования, сбор конфигурационной и операционной информации, измерение различных параметров сети.

Сбор данных может включать следующие типовые работы:

- интервьюирование пользователей ЛС ОУ (педагогических и административных работников ОУ, использующих в своей работе ЛС);
- документальное обследование (анализ представленных документов);
- визуальное обследование инфраструктуры, инвентаризацию сети;
- инструментальное обследование (приборные измерения):
  - нагрузочное (стрессовое) тестирование локальной сети;
  - нагрузочное тестирование каналов связи распределенной сети;
  - мониторинг «здоровья» сети и сетевых сервисов;
  - оценка качества канала связи с Интернет;
- оценку состояния информационной безопасности ЛС;
- сбор конфигурационной и операционной информации.

Детальный перечень выполняемых работ обычно определяется в техническом задании на аудит.

Автоматизация инвентаризации сети

Для сокращения затрат на сбор информации при проведении инвентаризации сети удобно использовать специальные программы*. Одной из таких доступных и бесплатных программ является программа Hardware Inspector Client/Server.

Программа **Hardware Inspector Client/Server** предназначена для автоматизированного учета компьютеров, а также заявок от пользователей. Уникальность программы заключается в возможности вести учет не просто текущего состояния параметров компьютера, а всей истории жизни каждого устройства. С помощью программы Hardware Inspector Client/Server можно решать широкий круг задач.

Основные возможности программы Hardware Inspector Client/Server:

Клиент-серверная технология. Позволяет работать с единой базой данных как в локальной сети, так и через Интернет. Отличается высокой устойчивостью к повреждениям данных, высокой скоростью работы и повышенной защищенностью информации.

Детальный учет устройств. На каждое устройство заводится паспорт, в котором отражается информация о его покупке, технических параметрах, истории его перемещений по рабочим местам и обслуживания.

Детальный учет лицензий на программное обеспечение. На каждую лицензию заводится паспорт, в котором отражается информация о ее покупке, параметрах, истории ее перемещений по рабочим местам.

Учет заявок от пользователей. Встроенный учет заявок от пользователей. История сообщений в заявке, прикрепляемые файлы и прочее. Возможность совместной работы с веб-интерфейсом.

Учет расходных материалов. Программа позволяет вести учет поступления на склад и выдачи расходных материалов, а также планирование их потребности на основе статистики расхода за прошлые периоды.

Наглядная иерархия подразделений и рабочих мест. «Дерево» рабочих мест организации может отображаться в двух разрезах: организационное представление (оргструктура) и территориальное (карта).

Визуализация компьютеров на поэтажных планах. Расположение рабочих мест на планах помещений предприятия помогает визуальному восприятию размещения компьютеров в сети. Наглядно показаны сетевые соединения, благодаря которым возможны переходы по этажам и кабинетам.

Проведение работ по обслуживанию устройств и рабочих мест. В программе ведется учет любых работ по обслуживанию устройств и рабочих мест: ремонт, профилактика и прочее. Фиксируются все обстоятельства работ, на основе чего могут строиться отчеты по выполненным работам IT-отделом и его сотрудниками.

* Программы, автоматизирующие инвентаризацию сети, приведены на компкт-диске.

Инвентаризация компьютеров. Механизм инвентаризации с использованием штрих-кодов показывает реальное наличие устройств на рабочих местах. Автоматизация и контроль процедуры проведения плановой инвентаризации оборудования.

Аудит рабочих мест. Этот инструмент проведения инвентаризации выявляет отклонения информации в базе данных от реального состояния конфигурации. Многоуровневая проверка уникальности каждого устройства позволяет сразу определить его статус, выполнить импорт или перемещение.

Большой набор отчетов: "Паспорт устройства", "Паспорт рабочего места", "Паспорт лицензии", "Список инвентарных номеров", "Список IP-адресов", "Полный перечень оборудования", "Выполненные работы за период времени" и прочее. Отчеты могут экспортироваться в PDF, MS Word, MS Excel, Open Office и другие форматы. При этом пользователь может самостоятельно настраивать шаблоны во встроенном визуальном дизайнере, а также создавать свои собственные отчеты.

Незарегистрированная копия программы Hardware Inspector Client/Server не ограничена по количеству рабочих мест и не имеет срока жизни БД. В качестве ограничения в некоторых формах и отчетах в случайном порядке вместо данных отображается текст [DEMO VERSION]. Кроме того, через 2 месяца использования к серверу одновременно сможет подключиться только один оператор.

Анализ данных и подготовка отчета

При анализе полученных при инвентаризации сети данных проводится проверка собранных данных на полноту и корректность, формирование выводов и рекомендаций, оформление результатов. В ходе анализа может быть принято решение о сборе дополнительных данных. Этап анализа данных и оформления результатов может включать следующие типовые работы:

1. Проверка и анализ собранных данных.
2. Анализ структуры сети.
3. Анализ конфигурационных файлов.
4. Подготовка эксплуатационной документации.
5. Подготовка отчета об аудите.

Для сбора данных о компьютерах, их характеристиках и установленном программном обеспечении целесообразно использовать специальные программы. В Интернете можно найти бесплатные и условно-бесплатные программы, позволяющие автоматизировать процесс сбора данных инвентаризации и составления отчетов. Некоторые полезные программы для инвентаризации сети приведены на компакт-диске.

Результатом аудита является создание пакета документов, содержащего детализированные данные о локальной сети образовательного учреждения, а также рекомендации по улучшению качества работы и повышению эффективности функционирования сети.

Основным отчетным документом является отчет об аудите. Он включает описание текущего состояния сети, выводы о соответствии локальной сети образовательного учреждения решаемым образовательным задачам, рекомендации по модернизации и развитию сети.

Эксплуатационная документация по локальной сети

Эксплуатационная документация по локальной сети образовательного учреждения может быть представлена совокупностью следующих документов.

1. Документы, описывающие структуру локальной сети (ЛС):

• Поэтажный план здания с указанием:
  – компьютерных классов;
  – кабинетов с компьютерной аппаратурой (административных, учебных, лаборантских и др.);
  – помещения серверной;
  – элементов компьютерных сетей (провода и др.);
  – сетей 220 В (щиты, проводка, розетки, линии заземления).

• Для каждого компьютерного класса, каждого кабинета с аппаратурой, серверной – отдельные схемы с указанием размещения в них:
  – аппаратуры (компьютеры, ноутбуки, тележки мобильного класса, сетевое оборудование);
  – линий локальных сетей (ЛС);
  – сетей 220 В (проводка, розетки, линии заземления).

• Описание среды передачи данных:
  – кабельной системы (схема прокладки кабеля по зданию);
  – схемы прокладки кабеля оптоволоконной сети и её оборудования (при наличии в ОУ);
  – системы радиосвязи – WiFi (схема зон охвата помещений здания) (при наличии в ОУ).

• Описания подключения компьютеров к сетевому оборудованию и связь сетевого оборудования между собой (подключение с точностью до порта сетевого оборудования).

• Описание адресного пространства ЛС: какие IP-адреса какими компьютерами используются при фиксированной адресации или какой диапазон IP-адресов выделен для DHCP для организации ЛС (адреса ПК в компьютерном классе, ПК учителей, администрации, бухгалтерии), для выхода в Интернет.

2. Документы учета технических средств информатизации ЛС:

– компьютеров (серверов, ПК, ноутбуков);

– сетевого оборудования (концентраторов, коммутаторов и маршрутизаторов);

– проекторов;

– интерактивных досок.

3. Документы учета программного обеспечения, установленного на компьютерах ЛС:

– операционных систем;

– антивирусных ПО;

– офисных программ;

– программ для работы с графической информацией;

– программно-педагогических средств, установленных на компьютерах пользователей ЛС и серверах;

– другого ПО.

4. Документы, подтверждающие лицензионную чистоту программного обеспечения:

• Лицензии;

• Документация по ПСПО;

• Голограммы.

5. Документы по организации доступа к сети Интернет:

• Приказ по ОУ на организацию доступа к Интернету с указанием ответственного лица.

• Схема подключения ЛС к Интернету с указанием портов сетевого оборудования, IP-адресов, шлюза (при его использовании).

• Документы по организации контентной фильтрации.

• Документы по организации учета интернет-трафика.

• Документы по организации доступа учителей и учеников к Интернету вне занятий.

6. Должностные инструкции для администратора и пользователей сети.

7. Документы по обеспечению безопасной работы в локальной сети:

• Документы по организации антивирусной защиты.

• План резервирования и восстановления информации.

• Документы по организации защиты персональных данных в автоматизированной информационной системе.

• Документация по технике безопасности.

Анализ состава и лицензионной чистоты программного обеспечения

В первую очередь следует оценить лицензионную «чистоту» ПО Microsoft.

Управление лицензиями Microsoft в образовательных организациях

Зачем нужно управлять лицензиями Microsoft в образовательной организации? Чтобы ответить на этот вопрос, нужно прежде всего понять, что же такое лицензии на программное обеспечение и зачем они нужны.

Для работы с любым программным обеспечением необходимо получить право на его использование. Такое право обычно предоставляет ли-

цензионное соглашение. Нужно ясно понимать, что именно соглашение дает право устанавливать программный продукт и работать с ним. Само по себе наличие оригинального «лицензионного» дистрибутива при отсутствии соглашения не дает права на использование данного продукта.

Существует несколько вариантов приобретения права на использование программного обеспечения Microsoft.

1. Коробочные (FPP) продукты (лицензии)

Данный тип лицензий рассчитан на индивидуального пользователя и представляет собой красочную упаковку, содержащую лицензионный сертификат, документацию и носитель с дистрибутивом. Этот продукт предназначен для розничной продажи и не подразумевает какие-либо дополнительные специальные условия при приобретении образовательной организацией. К тому же данный тип лицензии несет ряд ограничений по использованию продукта, устраивающих индивидуального пользователя, но не предоставляющих дополнительных возможностей, необходимых организации.

Вывод: Такой тип лицензии не лучшим образом может удовлетворить требования образовательной организации и к тому же оказывается дорогим при неоднократных закупках лицензий.

2. Лицензии на предустановленное программное обеспечение (OEM)

Программное обеспечение Microsoft может поставляться вместе с компьютером в предустановленном виде. В данном случае о наличии лицензии свидетельствует сертификат подлинности, наклеенный на корпус компьютера. Такие версии продуктов, предназначенные для поставки вместе с аппаратным обеспечением, называются OEM-версиями продуктов.

Основной отличительной особенностью OEM-версий является то, что они «привязаны» к компьютеру, на который были первоначально установлены, и не могут быть перенесены на компьютер, служащий заменой старого, или на другой ПК. Так же как и коробочные лицензии, данный вариант рассчитан на индивидуального пользователя, и права использования продукта в определенной степени ограничены, что не всегда подходит для организации.

Вывод: Данный тип лицензии является оптимальным вариантом приобретения базовой лицензии на операционную систему Windows в составе новых ПК. Весь необходимый функционал для операционной системы, а также любые другие продукты Microsoft (Microsoft Office, серверные продукты и т.д.) будет дешевле и удобнее получить в рамках *Академических программ лицензирования.*

3. Академические программы лицензирования

Купив одну коробку с программным продуктом, пользователь имеет право установить программу только на один компьютер. Однако в организациях, как правило, один и тот же продукт используется на нескольких

компьютерах. В этом случае наиболее выгодный способ приобретения лицензий – Академические программы лицензирования Microsoft.

Покупая продукты по программам академического лицензирования, плата осуществляется только за лицензионные права. Носители для установки продукта либо предоставляются бесплатно, либо могут быть заказаны отдельно. Один носитель может быть использован в качестве эталона для установки, что позволяет не только сократить расходы на приобретение, но и устранить сложности, связанные с развертыванием продукта на нескольких ПК в организации. Помимо всего прочего, лицензии, доступные в рамках таких программ, дают возможность использовать не только текущие, но и предыдущие версии программного обеспечения в количестве, соответствующем количеству приобретенных в рамках соглашения лицензий. Так называемое право «Downgrade». Это право дает, например, возможность перейти от операционной системы Windows Vista к операционной системе Windows XP или от пакета программ Office 2007 к пакету Office 2003. Право использования программных продуктов в данном случае подтверждается бумажным свидетельством (сертификатом) или подписанными документами соглашения, оформленного на Ваше образовательное учреждение.

Вывод: Академические программы являются оптимальным решением для образовательных организаций в случаях, когда планируется приобретение лицензий Windows Upgrade (расширение прав использования базовых лицензий на операционную систему, а также в случаях приобретения всех других продуктов Microsoft (Microsoft Office, серверные продукты и т.д.) при первоначальной закупке 5 и более лицензий. Кроме того, данные программы подразумевают специальный, существенно сниженный уровень цен для образовательных и академических организаций.

Как наладить процесс управления лицензиями?

Для этого нужно начать работы по организации управления, для начала текущими версиями ПО, имеющимися в образовательном учреждении. Такие работы можно организовать самостоятельно или прибегнуть к помощи партнерской организации, специализирующейся на данных видах работ.

В случае если в ОУ решили наладить процесс управления лицензиями самостоятельно, можно рекомендовать организовать его, распределив все мероприятия на несколько шагов:

Этап 1. Сбор необходимой начальной информации.
Этап 2. Проведение инвентаризации установленного программного обеспечения.
Этап 3. Сопоставление лицензий и программного обеспечения.
Этап 4. Разработка стратегического подхода и практических процедур для использования программного обеспечения.
Этап 5. Разработка плана управления лицензиями.

Этап 1: Сбор необходимой начальной информации

Этот этап носит подготовительный характер, в процессе его осуществления необходимо собрать информацию, требуемую для внедрения управления лицензиями в организации.

Информация включает в себя ответы на следующие вопросы:

- Какое количество персональных компьютеров используется в организации, объединены ли они в сеть?
- Какое количество серверов?
- Какое на них установлено программное обеспечение?
- Кто отвечает за закупку и эксплуатацию программного обеспечения?

Реализация всех этапов технологии управления лицензиями потребует определенного времени и усилий не только со стороны персонала отдела информационных технологий, руководящего состава, но и рядовых работников. Поэтому настоятельно рекомендуется составить и разослать внутри организации разъяснительную записку относительно целей проводимой работы. Понимание необходимости данной работы всеми сотрудниками организации способно значительно сократить сроки внедрения технологии управления лицензиями в организации.

Этап 2: Проведение инвентаризации установленного программного обеспечения

Проведение инвентаризации программного обеспечения является вторым этапом в процессе управления лицензиями. Существуют два способа инвентаризации программного обеспечения:

Ручная инвентаризация. Пользователь может провести инвентаризацию вручную, просмотрев жесткие диски всех компьютеров и зафиксировав всю информацию в виде отчета. Одним из простых способов является использование опции Add or Remove Programs.

Автоматическая инвентаризация. Для автоматической инвентаризации ПО на компьютерах и серверах организации можно использовать специальные программы. Каталог продуктов для инвентаризации ПО и управления лицензиями содержит полный перечень всех типов программ. В дополнение для выявления всех основных установленных продуктов Microsoft можно использовать программу Microsoft Software Inventory Analyzer (MSIA)*. Эти автоматизированные средства существенно упрощают процесс инвентаризации. С помощью MSIA или программы из каталога продуктов для инвентаризации ПО и управления лицензиями можно проводить инвентаризацию ПО как для автономно работающих компьютеров, так и для подключенных к локальной сети. При анализе автономно работающих компьютеров нужно установить соответствующие программы на каждом из

* Программа приведена на компакт-диске.

них. Большая часть специальных программ для инвентаризации ПО автоматически генерирует инвентаризационные отчеты. После инвентаризации ПО всех компьютеров организации необходимо поместить всю собранную информацию в один отчет.

Этап 3: Сопоставление лицензий и программного обеспечения

После того как стало известно, какие программные продукты установлены на компьютерах организации, наступило время сопоставить установленное программное обеспечение с имеющимися лицензиями.

Перед тем как приступить к выполнению данного этапа, необходимо понять, какие документы являются подтверждением лицензии на каждый тип программного продукта, используемого организацией.

Поиск лицензионной документации. Сначала необходимо связаться с лицом, ответственным за приобретение или состояние программного обеспечения в ОУ. Если организация участвует в одной из программ корпоративного лицензирования Microsoft, то можно получить лицензионную документацию на специализированных сайтах. Если пользователь не может отыскать необходимую лицензионную документацию, он может обратиться за помощью к поставщикам оборудования или в Комитет по образованию Санкт-Петербурга.

Хранение лицензионной документации. Хранить всю лицензионную документацию необходимо в надежном месте, рекомендуется использовать сейф.

Сравнение данных. После того как вся лицензионная документация собрана, нужно зафиксировать информацию в виде отчета. Затем сравнить его с отчетом по инвентаризации программного обеспечения, подготовленным на этапе 2; подойдет даже суммарный отчет, использованный на этапе 2. При сравнении легко выяснить, какие программные продукты лицензированы, а какие нет.

Если образовательное учреждение располагает избыточным количеством лицензий, то это означает неэффективное использование ПО. Соответствующие программные продукты следует установить на дополнительных компьютерах так, чтобы количество лицензий было равно количеству установок. Если в ОУ наблюдается недостаток лицензий, то необходимо приобрести дополнительные лицензии (см. таблицу).

Программное обеспечение	Количество установок	Общее количество лицензий	Избыток или недостаток лицензий
Office 2003	24	22	-2
Office 2007	32	32	0
Windows XP	12	10	-2
Windows 2000	37	40	+3

Этап 4: Разработка стратегического подхода и практических процедур

Выбор и последующее использование надлежащих стратегий и процедур для использования программного обеспечения и его лицензирования являются важнейшей частью технологии управления лицензиями в целом.

Стандартизация используемого программного обеспечения. Одним из ключевых процессов, проводимых на этом этапе, является процесс стандартизации. Существенную выгоду могут получить ОУ, которые проведут у себя стандартизацию компьютеров и используемых программ. Например, это может выглядеть так: внутренний стандарт ОУ предусматривает "Рабочий компьютер для учителя – тип 1", который состоит из настольного компьютера, монитора и установленного программного обеспечения; "Рабочий компьютер для учителя-предметника – тип 2" – это ноутбук с определенными возможностями для расширения и конкретным набором программ, стандарт компьютера для администрации ОУ, бухгалтеров, учеников.

Необходимо, чтобы в ОУ имелось описание всех приведенных ниже стратегий и процедур. Если имеется вся документация, то следует провести ее оценку и при необходимости сделать соответствующую корректировку.

Стратегия приобретения программного обеспечения. Централизованное приобретение программного обеспечения позволит сэкономить денежные средства за счет использования скидок при лицензировании большого количества однотипных программ.

Система централизованного приобретения может помочь ОУ в:

- упрощении поиска лицензионных документов и экономии времени за счет хранения всех лицензий и соглашений в одном месте;
- уменьшении затрат при приобретении надлежащего типа лицензии;
- эффективном размещении программных ресурсов, согласовании финансовой сметы на программное обеспечение с реальными нуждами;
- максимально эффективном использовании программного обеспечения за счет потенциально многократного использования или перераспределения программного обеспечения между отделами.

Стратегия приобретения программного обеспечения может обеспечить достижение всех вышеуказанных целей при условии выполнения следующих процедур:

- централизация полномочий и документирование при приобретении нового программного обеспечения;
- приобретение программного обеспечения только у надежных торговых партнеров;
- хранение лицензионной документации (оригинальные CD, сертификат подлинности, лицензионное соглашение с конечным пользователем, оригинал руководства для пользователя и товарные чеки) в надежном месте;
- инвентаризация имеющихся программных средств на регулярной основе с целью обеспечения надлежащего лицензирования.

Контроль нового программного обеспечения. Для гарантированного включения данных о новом программном обеспечении следует разработать и включить в инвентаризационный отчет ОУ систему действий, которые должны быть выполнены при поступлении нового программного продукта. Система действий должна охватывать:

• хранение оригинальной документации, включая транспортную накладную;

• хранение оригинальной упаковки;

• корректировку базы или хранилища инвентаризационной информации.

Процессом контроля программных средств часто пренебрегают, однако только указанные выше действия могут гарантировать точное ведение базы данных с информацией о ПО в организации.

Стратегия использования программного обеспечения. Стратегия использования программного обеспечения должна включать те нормы и положения, которые приняты в организации при загрузке, инсталляции и дальнейшем использовании лицензионных программных средств.

Следует учесть, что:

• проверка сроков действия условий каждой лицензии для обеспечения надлежащего использования программного продукта;

• разработка процесса санкционированной инсталляции программного обеспечения (т. е. выделение одного сотрудника, ответственного за установку программных средств);

• контроль деятельности, связанной с инсталляцией программ или загрузкой программных средств через Интернет.

Важно, чтобы все сотрудники ОУ четко представляли все допустимые и недопустимые действия по отношению к программным и аппаратным средствам. Таким способом возможно исключить попадание вирусов в систему, уменьшить число обращений в службу технической поддержки, а следовательно, обеспечить эффективное использование программного обеспечения.

Чрезвычайный план для программных средств. Важно провести анализ самых неблагоприятных сценариев. Чрезвычайный план включает те процедуры, которые будет выполнять организация в случае чрезвычайной ситуации.

Чрезвычайный план должен содержать информацию по защите и восстановлению программных средств. Пункты плана должны охватывать:

• регулярное создание копий;

• хранение копий всех программных средств на CD в сейфах в специально охраняемых помещениях;

• хранение всей лицензионной документации в сейфах в специально охраняемых помещениях (в случае непрерывного использования информации следует изготовить копии документов, а оригиналы хранить в безопасном месте).

Этап 5: Разработка плана управления лицензиями

Конечным этапом процесса управления лицензиями является разработка плана действий, предусматривающих дальнейшее развитие.

Анализ потребностей в программных средствах. Чрезвычайно важно определить те программные продукты, в которых пользователи (ученики, учителя и административные работники) нуждается для выполнения всех задач по организации образовательного процесса и управления ОУ. Кроме того, целесообразно провести опрос учителей и административных работников: какие программные средства необходимы, а какие не используются в рабочем процессе? Выполнять данную процедуру можно один или два раза в год. На основании проведенного опроса можно создать таблицу, которая отражала бы соотношение между профессиональной компетентностью сотрудника и его потребностью в программном обеспечении. После выполнения этого анализа можно провести списание и деинсталляцию неиспользуемых в работе программных продуктов и предоставить пользователям программное обеспечение, которое действительно может потребоваться в рабочем процессе.

Обучение: как использовать программные продукты. Если ОУ имеет соответствующие ресурсы, можно организовать повышение квалификации в области обучения профессиональному использованию программных продуктов. Обучение может оказаться наиболее эффективно для новых программных продуктов, которые никогда ранее в ОУ не применялись. Повышение квалификации можно организовать и на базе соответствующих городских или районных учреждений.

Надлежащее обучение обеспечит максимальную отдачу от использования нового программного продукта и сократит число обращений в службу технической поддержки из-за неверного использования программного обеспечения.

Снижение затрат на поддержку. К основным направлениям сокращения затрат на поддержку программного обеспечения можно отнести следующие:

- сокращение числа приложений и устройств, требующих технической поддержки, с заменой их стандартизированными приложениями и системами (осуществляется соответствующим техническим персоналом);
- отказ от использования заказных "самодельных" решений – расходы на их поддержку могут существенно превосходить расходы на лицензирование. Кроме того, при возникновении проблем с использованием лицензионных программных продуктов специалисты технической службы могут связаться с поставщиком, тогда как в случае эксплуатации "самодельных" программных продуктов какие-либо консультации исключены.

График инвентаризации. Следует установить периодичность проведения инвентаризации программных средств с последующим обновлением

хранящейся информации. График проведения инвентаризации определяется масштабами ОУ и количеством компьютеров, периодами поставки нового программного обеспечения и темпами развития локальной сети.

С помощью технологии управления лицензиями можно в реальном времени проводить мониторинг вновь установленного ПО на компьютерах, подключенных к локальной сети, и создавать соответствующие отчеты по инвентаризации ПО.

Полностью изучив и внедрив поэтапный метод использования технологии управления лицензиями, руководитель ОУ и администраторы локальной сети обладают всей информацией о состоянии дел с имеющимся в организации программным обеспечением и точно знают, что необходимо приобрести и как максимально эффективно использовать программные ресурсы.

Литература

1. Сетевой сканер Nmap как средство аудиталокальной сети [Электронный ресурс]. – Режим доступа: www.compress.ru свободный. – Загл. с экрана. – Яз. рус.
2. Аудит сети Анализ защищенности сетевых ресурсов [Электронный ресурс]. – Режим доступа: www.securityhelp.ru свободный. – Загл. с экрана. – Яз. рус.
3. Microsoft. Основные протоколы семейства TCP/IP [Электронный ресурс]. – Режим доступа: http://technet.microsoft.com/ru-ru/library/cc780539(WS.10.).aspx, свободный. – Загл. с экрана. – Яз. рус.
4. Программное обеспечение для инвентаризации компьютерной техники [Электронный ресурс]. – Режим доступа: http://school9korolev.moy.su/2007/publichnyidoklad.pdf, свободный. – Загл. с экрана. – Яз. рус.
5. Инвентаризация компьютеров в сети 3,7 [Электронный ресурс]. – Режим доступа: http://centrosoft.ru, свободный. – Загл. с экрана. – Яз. рус.
6. SecurityLab.ru – информационный портал [Электронный ресурс]. – Режим доступа: www. securitylab.ru, свободный. – Загл. с экрана. – Яз. рус.
7. Управление лицензиями Microsoft в ОУ. Подробнее о лицензировании [Электронный ресурс]. – Режим доступа: http://www. microsoft.com/rus/education/licensing, свободный. – Загл. с экрана. – Яз. рус.
8. Управление активами программного обеспечения (Software Asset Management, SAM) [Электронный ресурс]. – Режим доступа: http://www.microsoft.com/rus/Licensemanagement/what, свободный. – Загл. с экрана. – Яз. рус.

ПРОЕКТИРОВАНИЕ ЛОКАЛЬНОЙ СЕТИ

В.С. Шаров, учитель информатики высшей категории,
МУК №1 Петроградского района Санкт-Петербурга

Термины и определения

Для исключения нечеткого понимания некоторых терминов, используемых в дальнейшем, приведем ряд терминов и определений в соответствии со стандартом ГОСТ Р 53246-2008.

Структурированная кабельная система: Законченная совокупность кабелей связи и коммутационного оборудования, отвечающая требованиям соответствующих нормативных документов.

Горизонтальная подсистема: Часть кабельной системы от телекоммуникационной розетки/разъема на рабочем месте до горизонтального кросса (этажного распределительного пункта) в телекоммуникационном помещении или кабельная система между розеткой системы автоматизации здания и горизонтальным кроссом, включая саму розетку, или между первой механической заделкой горизонтальной соединительной точки и горизонтальным кроссом (TIA).

Магистральная подсистема: Среды передачи и соединительное оборудование, обеспечивающие взаимосвязи между телекоммуникационными, аппаратными и городскими вводами внутри или между зданиями.

Кросс-соединение: Метод коммутации, в котором для подключения активного оборудования к магистральной кабельной подсистеме или пассивной коммутации между собой кабельных сегментов магистральной подсистемы используются две единицы коммутационного оборудования, соединяемые коммутационными шнурами.

Кросс: Установка, обеспечивающая подключение кабельных элементов, их кросс-соединение или межсоединение.

Проектирование локальной сети

Локальная сеть включает в себя структурированную кабельную систему, которая позволяет объединять активное оборудование. Вторая составляющая локальной сети – сетевое, серверное, компьютерное и периферийное оборудование, которое упрощенно называют компьютерной сетью. Поэтому объектами проектирования локальной сети выступают компьютерная сеть и структурированная кабельная система (СКС). Следует учитывать, что в пределах срока службы СКС может смениться три – четыре поколения компьютеров и сетевых устройств.

С целью создания долговечной системы на этапе проектирования СКС в горизонтальную подсистему целесообразно заложить определенный резерв. В горизонтальной подсистеме СКС предусмотрены универсальные кабели, достаточные для работы компьютерных сетей с гигабитными скоростями. Кроме того, проекты СКС реализуют избыточность рабочих мест. Цена такого подхода, безусловно, выше, однако избыточность системы обеспечивает снижение эксплуатационных издержек и быстрое увеличение количества компьютеров в ЛС.

Часто встречается другой подход. Задание дается, исходя из требований проектирования имеющейся локальной сети и расположения рабочих мест на ближайшую перспективу.

Следует также учитывать, что проектирование и конфигурирование компьютерной сети выполняет, как правило, образовательное учреждение (заказчик) силами администраторов ЛС и администрации ОУ. Проектирование СКС – задача, как правило, подрядных организаций, но ОУ должно видеть, что все требования к локальной сети в проекте учтены.

Проектирование СКС разделяют на две основные стадии: *архитектурную* и *телекоммуникационную*.

Основной задачей *архитектурной стадии* проектирования СКС является определение общей структуры, оптимальной по комплексу технико-экономических характеристик в процессе создания и последующей эксплуатации. Она проходит на этапе разработки проекта нового или реконструированного здания. На этой стадии в проект определяются вертикальные стояки, пути и способы прокладки кабелей как внутри, так и снаружи здания (кабельная канализация).

Основными исходными данными для этой стадии являются:

– форма, этажность, архитектурные, планировочные и другие особенности, геометрические характеристики здания или их комплекса, а также прилегающей территории;

– строительные и другие нормативные документы на проектирование служебных помещений систем телекоммуникаций и кабельных трасс;

– нормативная документация по СКС (стандарты);

– дополнительные требования заказчика.

На архитектурной стадии работы по проектированию СКС проводятся специализированными проектными организациями с учетом требований подрядчика, который потом будет реализовывать СКС.

Телекоммуникационная стадия проектирования СКС начинается по окончании архитектурной. На ней разрабатывается конкретная структура СКС, составляется перечень необходимого оборудования, планы его размещения и т. д. На данном этапе работы к проектированию могут привлекаться фирмы, специализирующиеся в области создания СКС и системной интеграции. Также они обычно выполняют большую часть монтажных и пусконала-

дочных работ, которые, как правило, по времени проводятся одновременно с отделкой внутренних помещений или сразу же после ее завершения.

Исходными данными для этой стадии являются:

• результаты обследования здания и прилегающей территории или их проект, выполненный на архитектурной стадии проектирования СКС;

• нормативная документация на СКС (стандарты). Новыми отечественными стандартами на проектирование СКС являются ГОСТ Р 53246-2008 и ГОСТ Р 53245-2008. Стандарт ГОСТ Р 53246-2008 устанавливает общие требования проектирования основных элементов структурированной кабельной системы на основе витой пары проводников и волоконно-оптических компонентов. Стандарт ГОСТ Р 53245-2008 распространяется на ввод и функционирование структурированной кабельной системы в помещении пользователя и устанавливает методы испытаний (тестирования), которые служат обеспечением гарантии соответствия СКС установленным требованиям*;

• дополнительные требования заказчика, например количество и размещение рабочих мест, число информационных розеток на них, требования к их производительности, надежности, безопасности.

Этапы создания структурированной кабельной системы

При проектировании СКС системные интеграторы часто используют ГОСТ 34.601–90. Согласно этому документу создание СКС разбивается на следующие этапы и фазы:

• Формирование требований:
  – обследование объекта;
  – формирование требований пользователя к системе.

• Техническое задание: разработка и утверждение технического задания на создание системы.

• Эскизный проект:
  – разработка предварительных проектных решений по системе и ее частям;
  – разработка пояснительной записки и локальной сметы эскизного проекта.

• Технический проект:
  – разработка проектных решений по системе и ее частям;
  – разработка документации на систему и ее части;
  – разработка и оформление документации на поставку изделий для комплектования системы.

• Техническая (рабочая) документация: разработка рабочей документации на систему и ее части.

---

* Тексты стандартов приведены на компакт-диске.

• Ввод в действие:
  – подготовка объекта автоматизации к вводу системы в действие;
  – подготовка и обучение персонала;
  – комплектация поставляемыми изделиями;
  – строительно-монтажные работы;
  – пусконаладочные работы;
  – проведение опытных испытаний;
  – проведение опытной эксплуатации;
  – проведение приемочных испытаний.
• Сопровождение системы:
  – выполнение работ в соответствии с гарантийными обязательствами;
  – послегарантийное обслуживание.

Техническое задание – первый этап проекта

Техническое задание включает требования заказчика по числу рабочих мест, их расположению, категории или классу системы. Этажные планы здания позволяют наглядно отобразить расположение различных элементов систем, оценить их параметры.

Как правило, удобно получить несколько конкурентных коммерческих предложений на проектирование и монтаж СКС. Для этого выбирают ряд компаний, которым рассылается техническое задание. Выбор большого числа претендентов позволяет собрать достаточно информации, однако требует усилий, в том числе организации аудита объекта. После аудита объекта претенденты предоставляют коммерческие предложения.

Хорошо подготовленное коммерческое предложение (КП) определяет большинство технических решений. Спецификация КП часто оказывается в основе договора проектирования и монтажа систем. В рамках коммерческого предложения разрабатываются следующие разделы:

- пояснительная записка;
- структурная схема;
- сроки проектирования и монтажа, гарантии;
- приложения.

В пояснительной записке обоснуется выбор систем с учетом их эксплуатационных параметров. Она содержит обоснование выбора среды передачи, телекоммуникационных шкафов, кабель каналов, комплектующих, оценочную стоимость, сроки проведения работ, порядок контроля, условия приемки, объем документации.

Структурная схема – это графический документ, который показывает взаимосвязь функциональных элементов структурированной кабельной системы. В ней обозначены распределительные пункты, магистральные каналы, точки ввода, внешние линии. Состав телекоммуникационных шкафов определяется детально.

При наличии этажных планов, подробного технического задания количественные и ценовые параметры подсистем СКС, кабель каналов, системы заземления рассчитываются точно. При неполных исходных требованиях стоимость дается оценочно на базе аналогичных реализованных проектов.

В приложениях раскрываются принципы построения, особенности сети, приводится информация о качественных параметрах, методах тестирования, гарантийных обязательствах.

Результатом является документ, дающий представление о модели, параметрах и особенностях кабельной системы, уровне стоимости и сроках реализации проекта. Коммерческое предложение проекта локальной сети дополняется разделом «активное оборудование».

Эту же документацию заказчик может разработать и самостоятельно при наличии квалифицированных сотрудников.

Работы по проектированию выполняются на этапах *эскизный проект*, *технический проект* и *рабочая документация*. Кроме того, на момент ввода в действие должна быть разработана эксплуатационная документация, учитывающая изменения, внесенные в рабочую документацию в процессе строительно-монтажных и пусконаладочных работ, опытной эксплуатации и приемочных испытаний. Эксплуатационная документация также включает в себя руководства по использованию и поддержке системы в процессе ее использования.

В зависимости от конкретной ситуации та или иная стадия создания СКС может быть опущена, если это заведомо не приведет к снижению качества.

Техническая документация – завершающий этап проекта

Завершающим этапом проекта СКС является техническая документация. Это детально проработанный документ, раскрывающий все аспекты реализации системы. Качественно составленный технический проект может обеспечить монтаж даже независимыми сторонними исполнителями. **Проектирование СКС / локальной сети** ведется с учетом современных норм и отраслевых стандартов. Техническая документация включает:

- пояснительную записку;
- структурную схему СКС;
- структурную схему системы телекоммуникационного заземления;
- схемы кабельных проводок, расположения элементов телекоммуникационной инфраструктуры;
- схемы размещения шкафов/стоек, оборудования распределительных пунктов;
- схемы размещения панелей в телекоммуникационных шкафах / стойках;
- схемы подключений кабелей на панелях/кроссах;
- схемы организации рабочих мест;
- систему администрирования, в том числе систему маркировки, учетные записи в виде таблицы соединений;
- электрические однолинейные схемы;

• кабельный журнал, таблицы распределения групповых линий по фазам;
• спецификацию комплектующих, материалов и работ.

Пояснительная записка содержит текстовое изложение особенностей проектируемой сети, систем телекоммуникационного заземления, администрирования и электропитания.

Поэтажные планы дают точное пространственное расположение каждого элемента системы на архитектурных чертежах здания.

Функциональная схема отражает количественные параметры подсистем СКС: особенности, конфигурация, число рабочих мест, число кабелей в горизонтальной /магистральной подсистемах, число, тип шкафов и панелей. Таблицы соединений содержат перечень всех элементов инфраструктуры, их назначение, привязку к помещениям, портам, кабельным трассам. Спецификация включает точный перечень требуемых для реализации проекта конструктивных элементов.

Итог этапа технического проектирования – создание функционально полного комплекта документации, предоставляющего исчерпывающую информацию для проведения монтажных работ.

Для подготовки чертежей могут быть использованы системы автоматизированного проектирования или программы работы с графикой (например, MS Visio).

Требования к СКС

В Российской Федерации с 01.01.2010 г. введены в действие ГОСТ Р 53246-2008 и ГОСТ Р 53245-2008, которые определяют общие требования к основным узлам СКС и методику испытания, соответственно.

Если обобщить требования этих стандартов, то можно сделать несколько основных выводов, а именно: основными требованиями построения структурированной кабельной системы являются требования к длине кабеля, к техническим помещениям, к размещению оборудования, к прокладке кабельных трасс, принципы и правила размещения розеток RJ-45.

Требования к длине кабеля (расстояние)

Расстоянием в горизонтальной кабельной подсистеме является физическая длина кабеля (по внешней оболочке) от точки его терминирования в горизонтальном кроссе телекоммуникационной до точки терминирования в телекоммуникационной розетке на рабочем месте.

Длина кабеля горизонтальной кабельной подсистемы независимо от типа среды передачи не должна превышать 90 м.

Сумма длин коммутационного шнура и аппаратного кабеля, используемых в горизонтальном кроссе для создания кросс-соединений, межсоединений и подключения активного оборудования, не должна превышать 5 м.

Длина аппаратного кабеля, используемого для подключения активного оборудования на рабочем месте к телекоммуникационной розетке, не должна превышать 5 м.

Сумма длин кабеля горизонтальной подсистемы, аппаратного кабеля на рабочем месте, коммутационного шнура и аппаратного кабеля в горизонтальном кроссе не должна превышать 100 м.

Минимальная длина кабеля горизонтальной подсистемы на основе витой пары проводников должна составлять 15 м, что обеспечивает нормальные условия функционирования телекоммуникационных приложений в коротких кабельных линиях, когда близкое расположение единиц коммутационного оборудования относительно друг друга (эффект резонансных отражений электромагнитной волны от интерфейсов) отрицательно влияет на возвратные потери (RL) и NEXT.

В случаях когда длина кабеля в горизонтальной кабельной подсистеме составляет не более 15 м, его излишки следует укладывать в виде запаса в телекоммуникационной, на рабочем месте или в трассах горизонтальной подсистемы. Предпочтительно запас кабеля создавать в виде U-образных петель с соблюдением минимального радиуса изгиба или петель в виде «8» с большим радиусом. Не рекомендуется делать запас кабеля в виде бухты небольшого диаметра (до 30 см).

С целью обеспечения в будущем возможности выполнения изменений конфигурации горизонтальной кабельной подсистемы рекомендуется оставлять следующий запас кабеля:

- в телекоммуникационной: кабель на основе витой пары проводников – 3 м; волоконно-оптический кабель – 3 м;
- на рабочем месте: кабель на основе витой пары проводников – 0,3 м; волоконно-оптический кабель – 1 м.

Запас кабеля должен учитываться в общей длине сегментов горизонтальной кабельной подсистемы.

Требования к техническим помещениям (помещения можно разделить на серверные и кроссовые)

- Серверная должна располагается ближе к геометрическому центру системы (здания).
- В тех случаях, когда рабочая площадь этажа превышает 1000 м^2 или если горизонтальная проводка в длину превышает 90 м, ставится дополнительная кроссовая.
- В серверных, кроссовых не допускается наличие фальшпотолка и фальшпола.
- Дверь в серверную (кроссовую) комнату должна открываться наружу.
- Не допускается использование в распределительных комнатах ламп дневного освещения.
- Серверная может быть совмещена с кроссовой или максимально с кроссовой этажа для минимизации длины соединяющих их кабелей.
- Помещение серверной не должно быть проходным, так как это усложняет систему контроля доступа.

• Не рекомендуется размещать серверную в подвале (риск заливания ее помещения грунтовыми водами и аварий канализации), на верхних этажах здания (риск заливания при протечках крыши), близко к мощным источникам электрических или магнитных полей, а также к оборудованию, которое может вызвать повышенную вибрацию.

• Запрещается на основании правил пожарной безопасности ППБ 01-93, пункт 4.2 располагать серверную рядом с помещениями для хранения пожароопасных или агрессивных химических материалов.

• Над серверными на основании норм РД 45.120-2000, пункт 17.6 не допускается размещать помещения, связанные с потреблением воды (туалеты, душевые, столовые, буфеты и т.д.).

• Порог температуры воздуха в серверной, кроссовой – от 18 до 24°С. Максимальная скорость изменения температуры не должна превышать 3°С в час (при повышении этого порога возможен выход из строя сетевого оборудования).

• Порог влажности воздуха в серверной, кроссовой – от 30 до 55%. Скорость изменения влажности воздуха ограничена величиной не более 6% в час. Конденсация влаги должна быть исключена при любых условиях.

• Питание серверной, кроссовой должно содержать минимум две сдвоенные силовые розетки, рассчитанные на максимальный ток в 20 А. Питание этих розеток должно осуществляться от двух независимых фидеров. Запрещается применение розеток с выключателями.

• Питание розеток для сетевой аппаратуры и системы освещения серверной должно осуществляться от различных панелей силового щитка.

• Для минимизации длины кабелей и соответственно стоимости горизонтальной подсистемы следует располагать кроссовые как можно ближе к геометрическому центру обслуживаемой рабочей зоны.

Требования к размещению оборудования

Коммутационное оборудование СКС и активные сетевые устройства могут быть смонтированы тремя основными способами:

• на стене помещения с использованием штатных монтажных элементов (скоб, ножек, оснований кроссовых башен и т.д.) самих коммутационных панелей и прочих изделий или неглубоких монтажных конструктивов типа рам;

• в 19-дюймовом монтажном конструктиве стандартной глубины, функции которого на практике наиболее часто выполняет монтажный шкаф;

• по смешанному варианту монтажа.

Требования к прокладке кабельных трасс

• Кабельные трассы подсистемы внутренних магистралей предназначены для прокладки по ним кабелей, соединяющих кроссовые устройства этажей (кроссовые шкафы) и серверные.

• Обычно для магистральной системы используют экранированный провод.

• Для горизонтальной системы используют обычный кабель, если нет других требований исходя из помехоустойчивости.

• Основными требованиями ко всем перечисленным сооружениям являются: простота реализации, легкость прокладки кабелей, обеспечение противопожарной безопасности, необходимость заземления всех их металлических элементов: труб, лотков, коробов и т.д.

Принципы и правила размещение розеток RJ-45 (по стандарту BICSI)

• Высота установки розеток RJ-45 от пола до центра лицевой панели розетки – от 375 до 1220 мм.

• Высота установки розеток RJ-45 должна совпадать с высотой установки силовых розеток.

• Расстояние между силовыми розетками и розетками RJ-45 не должно превышать 1 метра.

Требования российского стандарта ВСН 60-89, регламентирующего расстояние от радиорозетки до силовой розетки, аналогичны требованиям стандарта BICSI.

Выбор между кабелем и радиосвязью

Wi-Fi (англ. *Wireless Fidelity* – «беспроводная точность») – беспроводная сеть, стандарт на оборудование Wireless LAN. В России использование Wi-Fi без разрешения на использование частот от Государственной комиссии по радиочастотам возможно для организации сети внутри зданий, закрытых складских помещений и производственных территорий.

Особенности WiFi по сравнению с кабельными системами:

• Не требует (а точнее – меньше требует) проведения технических работ по прокладке кабеля для создания технологических отверстий: все равно придется класть кабель до точек доступа.

• Прямая дальность сигнала – до 100 м; но это теоретически, на практике же каждая стенка здания приводит к затуханию сигнала (т.е. выше этажом сигнал практически не будет ощущаться и будет приниматься в основном только над точкой).

• Для установки периметра сигнала требуется достаточно дорогостоящее оборудование.

• По экономическим затратам (без установки периметра сигнала) идентична затратам на кабельную сеть.

• Сигнал может прерываться от действия рядом работающих электромагнитных приборов.

• Скорость передачи значительно ниже, чем у проводной сети.

• Простота взлома. Практически на данный момент существует множество программ, с помощью которых можно сканировать и проникать в радиосети.

Вывод: Установка Wireless LAN рекомендуется там, где развёртывание кабельной системы невозможно или экономически нецелесообразно. То есть WiFi можно использовать как дополнение к проводной сети, например, в актовом зале, в конференц-зале, т.е. там, куда будут приходить гости с ноутбуками, но построить сеть на основе WiFi во всем здании и защитить её – очень дорогостоящее занятие.

ОРГАНИЗАЦИЯ ФУНКЦИОНИРОВАНИЯ ЛОКАЛЬНОЙ СЕТИ В ГЕТЕРОГЕННОЙ СРЕДЕ И РАЗВИТИЕ СЕТИ

А.И. Хрыпов, главный инженер ГОУ ДПО ЦПКС СПб «Региональный центр оценки качества образования и информационных технологий»

1. Построение и функционирование одноранговой сети

В зависимости от того, как распределены основные функции между компьютерами сети, компьютерные сети делятся на два класса: одноранговые (рис. 1) и двухранговые (см. далее рис. 5). Последние чаще называют сетями с выделенными серверами.

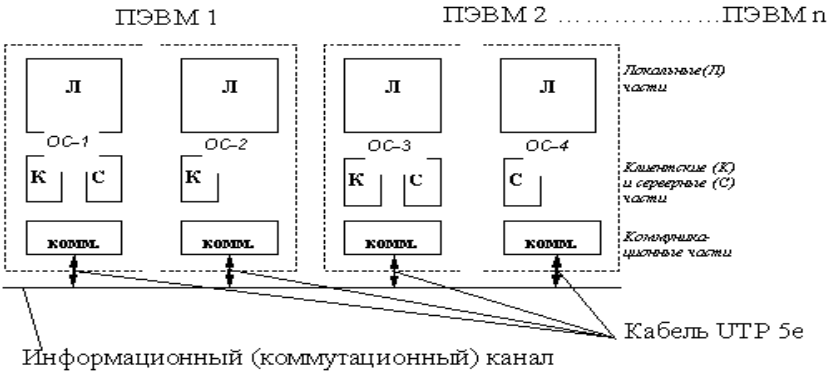

Рис. 1 Одноранговая сеть

Однора́нговые, **децентрализо́ванные** или **пи́ринговые** (от англ. *peer-to-peer, P2P* – равный к равному) сети – это компьютерные сети, основанные на равноправии участников. В таких сетях отсутствуют выделенные

серверы, а каждый узел (*peer*) является как клиентом, так и сервером. В отличие от архитектуры клиент-сервера, такая организация позволяет сохранять работоспособность сети при любом количестве и любом сочетании доступных узлов. Участниками сети являются пиры.

Каждая персональная ЭВМ (ПЭВМ), компьютер, имеет свою операционную систему (ОС), которая состоит из нескольких частей: локальной, клиентской, серверной и коммутационной.

Если компьютер предоставляет свои ресурсы другим пользователям сети, то он играет роль сервера. При этом компьютер, обращающийся к ресурсам другой машины, является клиентом. Компьютер, работающий в сети, может выполнять функции либо клиента, либо сервера, либо совмещать обе эти функции. Например, при установке на ПЭВМ – ОС MS Windows Server компьютер будет выполнять роль сервера, а при установке ОС MS Windows XP Proffessional – клиента. С другой стороны, на ПЭВМ с установленной ОС MS Windows XP Proffessional могут быть открыты папки для общего доступа, и тогда данный компьютер будет выполнять функции файлового сервера и другие функции.

В одноранговых сетях все компьютеры равны в правах доступа к ресурсам друг друга. Каждый пользователь может по своему желанию объявить какой-либо ресурс своего компьютера разделяемым (открытым), после чего другие пользователи могут его эксплуатировать. В таких сетях на всех компьютерах устанавливается одна и та же ОС, которая предоставляет всем компьютерам в сети потенциально равные возможности. Одноранговые сети могут быть построены, например, на базе ОС LANtastic, Personal Ware, Windows for Workgroup, Windows NT Workstation, Linux, Mac и т.д.

Каждая ПЭВМ подключается посредством коммутационной части, с помощью кабелей к информационному (коммутационному) каналу для взаимодействия и обмена информацией.

Итак попробуем построить самую простую одноранговую сеть из 3-5 ПЭВМ. Алгоритм действий следующий:

1) выбираем 3-5 аппаратно одинаковых по характеристикам ПЭВМ;

2) устанавливаем на них однотипную ОС, например MS Windows XP Proffessional;

3) устанавливаем на внутренние ПЭВМ по дополнительному сетевому адаптеру (сетевой карте);

4) соединяем ПЭВМ между собой проводами типа кросс-корд (учебное пособие на компакт-диске «Прокладка локальной сети с использованием витой пары», с. 18-19);

5) настраиваем сетевой протокол TCP/IP (рис. 2).

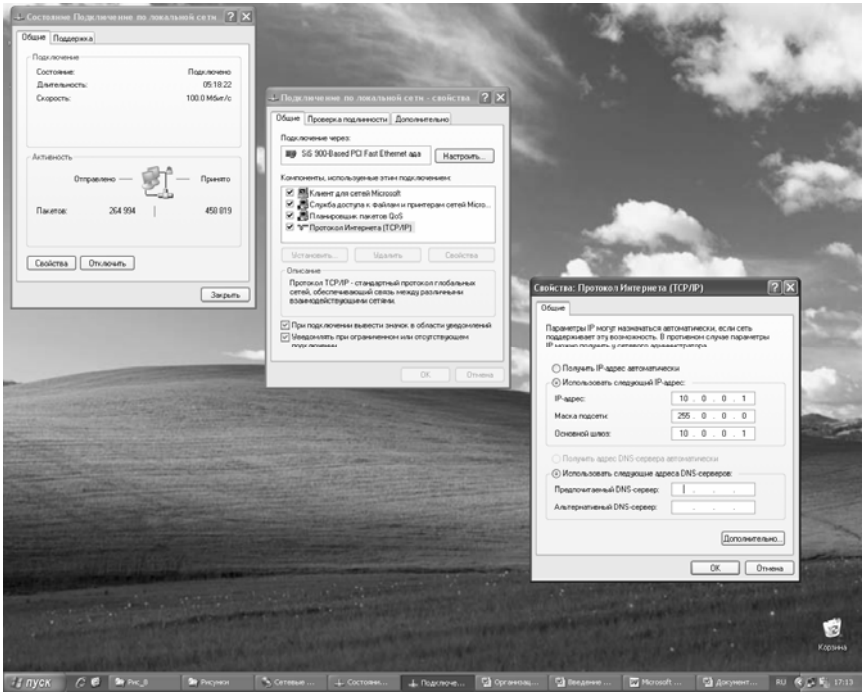

Рис. 2. Настройка сетевого протокола TCP-IP

Первой ПЭВМ следует присвоить вручную IP-адрес 10.0.0.1, второй – 10.0.0.2, третьей – 10.0.0.3 и т.д. Маска подсети стандартная 250.0.0. Если первая машина будет являться шлюзом и через неё будет организован выход, например, в Интернет, то в поле Основной шлюз необходимо будет прописать её IP-адрес 10.0.0.1;

6) на второй ПЭВМ две сетевые карты, и, следовательно, будет два сетевых подключения. Для того чтобы они работали правильно, необходимо организовать подключение «типа мост». Для этого в диалоговом окне (см. рис. 2) «Сетевые подключения» выделяем оба подключения по локальной сети и кликаем по ним правой кнопкой мыши. Открывается контекстное меню, в котором выбираем пункт «подключения типа мост»;

7) для того чтобы ПЭВМ видели друг друга в локальной сети, необходимо присвоить им имена Comp1, Comp2, Comp 3 и сделать их членами одной рабочей группы Work Group (рис. 3).

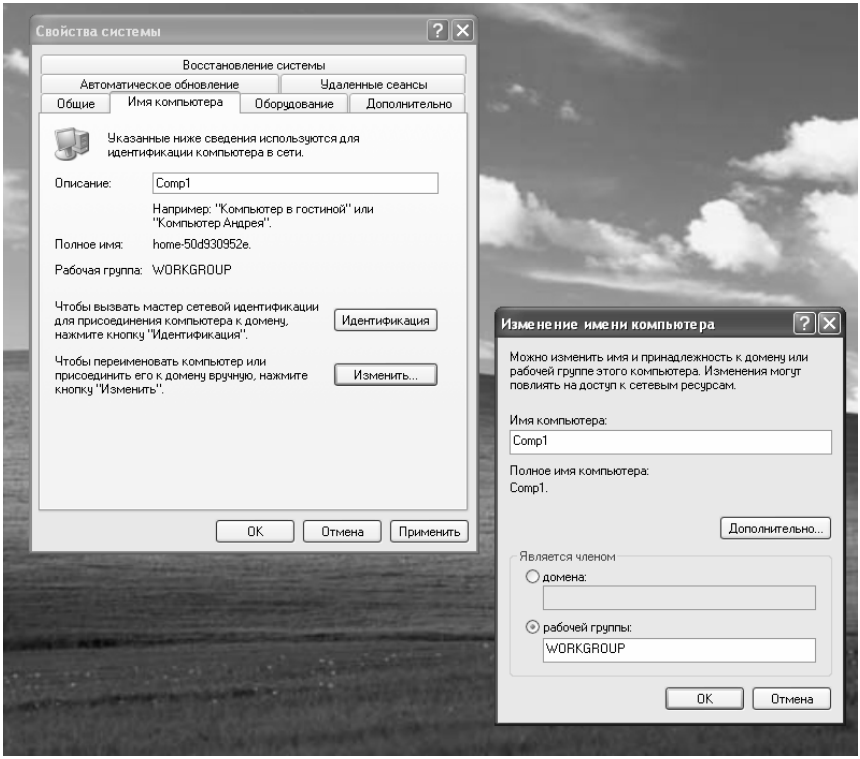

Рис. 3. Присоединение ПЭВМ к рабочей группе

Схема соединения простейшей рабочей группы из трех ПЭВМ показана на рис. 4.

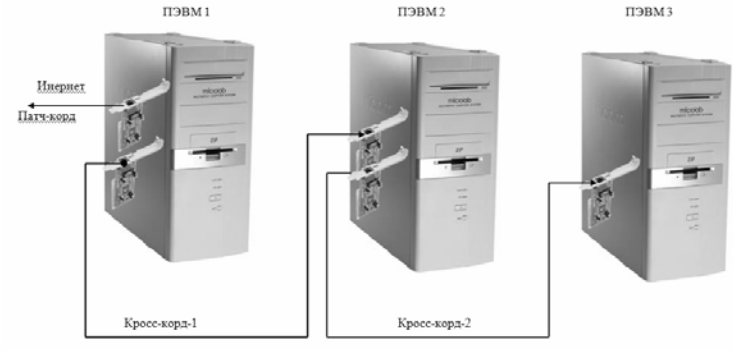

Рис. 4. Простейшая одноранговая сеть

В настоящее время такой архитектурой ЛВС пользуются достаточно редко – в случаях объединения 3-5 компьютеров. Если планируется в ЛВС включить большее количество ПЭВМ, то тогда имеет смысл каждый компьютер патч-кордом соединить с сетевой розеткой, а последнюю расшить UTP-кабелем категории 5е и соединить с патч-панелью в коммутационной стойке, в отдельном помещении (см. учебное пособие «Прокладка локальной сети с использованием витой пары»). Затем расшитые порты на патч-панели соединяются патч-кордами с портами в активном коммутаторе, тем самым происходит соединение компьютеров рабочей группы между собой. Затем производятся все настройки, описанные выше (TCP/IP).

В одноранговых сетях также может возникнуть функциональная несимметричность: одни пользователи не желают разделять свои ресурсы с другими, и в таком случае их компьютеры выполняют роль клиента; за другими компьютерами администратор закрепил только функции по организации совместного использования ресурсов, что означает, что они являются серверами; в третьем случае, когда локальный пользователь не возражает против использования его ресурсов и сам не исключает возможности обращения к другим компьютерам, ОС, устанавливаемая на его компьютере, должна включать и серверную, и клиентскую части. В отличие от сетей с выделенными серверами, в одноранговых сетях отсутствует специализация ОС в зависимости от преобладающей функциональной направленности – клиента или сервера. Все вариации реализуются средствами конфигурирования одной и той же ОС.

Одноранговые сети проще в организации и эксплуатации, однако они применяются в основном для объединения небольших групп пользователей, не предъявляющих больших требований к объемам хранимой информации, ее защищенности от несанкционированного доступа и к скорости доступа. При повышенных требованиях к этим характеристикам более подходящими являются двухранговые сети (сети с выделенными серверами), где сервер лучше решает задачу обслуживания пользователей своими ресурсами, так как его аппаратура и сетевая операционная система специально спроектированы для этой цели.

2. Сеть с выделенными серверами. Типы серверов

2.1. Сеть с выделенными серверами

Сеть с выделенными серверами представляет собой структуру, представленную на рис. 5.

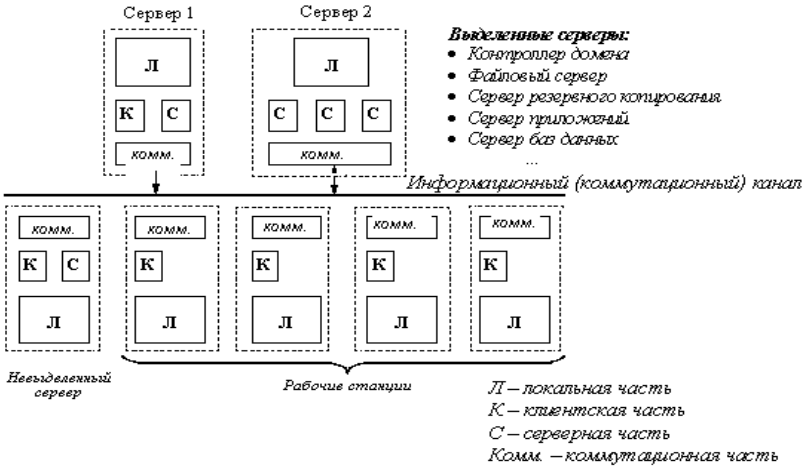

Рис. 5. Двухранговая сеть (клиент-сервер)

Если выполнение каких-либо серверных функций является основным назначением компьютера (например, предоставление файлов в общее пользование всем остальным пользователям сети, или предоставление всем пользователям сети возможности запуска на данном компьютере своих приложений, или выполнение функции сервера, который осуществляет резервное копирование важных в корпоративном отношении данных), то такой компьютер называется *выделенным сервером*. В зависимости от того, какой ресурс сервера является разделяемым, он называется файл-сервером, сервером приложений, сервером резервного копирования и т.д.

Очевидно, что на выделенных серверах желательно устанавливать ОС, специально предназначенные для выполнения тех или иных серверных функций. Поэтому в сетях с выделенными серверами чаще всего используются сетевые операционные системы, в состав которых входит нескольких вариантов ОС, отличающихся возможностями серверных частей. Например, сетевая ОС FreeNas семейства Unix имеет серверный вариант, оптимизированный для работы в качестве файл-сервера. Другим примером ОС, ориентированной на построение сети с выделенными серверами, является широко у нас используемая операционная система Microsoft Windows Server Standart 2008 (2003) R2 в качестве сервера и Microsoft Windows XP (7) Professional – в качестве клиента. Оба варианта сетевой ОС – Microsoft Windows Server Standart (для выделенного сервера) и Microsoft Windows XP (7) Professional (для рабочей станции) – могут поддерживать функции и клиента и сервера. Но серверный вариант Windows Server имеет больше возможностей для предоставления ресурсов своего компьютера другим пользователям сети, так как

может выполнять более широкий набор функций, поддерживает большее количество одновременных соединений с клиентами, реализует централизованное управление сетью, имеет более развитые средства защиты.

Выделенный сервер не принято использовать в качестве компьютера для выполнения текущих задач, не связанных с его основным назначением, так как это может уменьшить его производительность. Но, несмотря на это, в ОС Microsoft Windows Server Standart на серверной части имеется возможность выполнения обычных прикладных программ, то есть на сервере есть клиентская часть. В свою очередь на рабочих станциях под управлением Microsoft Windows XP (7) Professional присутствуют и серверные компоненты, позволяющие, например, осуществлять подключение к удаленному рабочему столу, открывать доступ к своим открытым («расшаренным») ресурсам, поддерживают работу в доменах и т.д. То есть рабочие станции могут выполнять функции невыделенного сервера.

Важно понять, что несмотря на то, что в сети с выделенным сервером все компьютеры в общем случае могут выполнять одновременно роли и сервера, и клиента, эта сеть функционально несимметрична: аппаратно и программно в ней реализованы два типа компьютеров: одни, в большей степени ориентированные на выполнение серверных функций и работающие под управлением специализированных серверных ОС, а другие – в основном выполняющие клиентские функции и работающие под управлением клиент-ориентированной ОС. Функциональная несимметричность, как правило, вызывает и несимметричность аппаратуры – для выделенных серверов используются более мощные компьютеры с большими объемами оперативной и долговременной памяти. Таким образом, функциональная несимметричность в сетях с выделенным сервером сопровождается несимметричностью и гетерогенностью операционных систем (специализация ОС) и аппаратной несимметричностью (специализация компьютеров).

2.2. Типы серверов

Принято различать аппаратную и программную части сервера.

С точки зрения аппаратной части, се́рвер – это мощный и высокопроизводительный компьютер, который специализируется на обработке больших потоков информации и может иметь несколько процессоров – от 2 до 8 и более, высокоскоростные SCSI HDD-диски, большой объем оперативной памяти 4-8-10 и более Гб, несколько LAN-интерфейсов, мощную систему охлаждения, источники питания с функцией горячей замены и т.д.

С точки зрения программной части, се́рвер (от англ. *to serve* – служить) – в информационных технологиях программный компонент вычислительной системы, выполняющий сервисные (обслуживающие) функции по запросу клиента (ПЭВМ), предоставляя ему доступ к определённым ресурсам или услугам.

Теоретически на одной единице аппаратного обеспечения (компьютере) может одновременно выполняться произвольное количество серверов (за исключением серверов, конфликтующих между собой по ресурсам или их назначению). Все они будут делить между собой аппаратные ресурсы одного высокопроизводительного компьютера.

Например, на одном сервере может быть поднят FTP-сервер, Web-сервер и Mail-сервер. Данный компьютер по установленному на нем программному обеспечению выполняет услуги корпоративной почты, на нем расположен сайт и находится файлообменник для обмена информацией для пользователей из внешней сети.

Как правило, каждый сервер обслуживает один или несколько схожих протоколов, и серверы можно классифицировать по типу услуг, которые они предоставляют, и по назначению. Рассмотрим предназначение основных типов серверов.

Универсальные серверы

Универсальные серверы – особый вид серверной программы, не предоставляющий никаких услуг самостоятельно. Такие серверы предоставляют серверам услуг упрощенный интерфейс к ресурсам межпроцессного взаимодействия и/или унифицированный доступ клиентов к различным услугам.

Универсальные серверы часто используются для создания всевозможных информационных серверов, которым не нужна какая-то специфическая работа с сетью, – серверов, не имеющих никаких задач, кроме обслуживания клиентов. Например, в роли серверов могут выступать обычные консольные программы и скрипты.

Серверы сетевых служб

Сетевые службы обеспечивают функционирование сети; например, серверы DHCP и BOOTP обеспечивают стартовую инициализацию серверов и рабочих станций, DNS – трансляцию имен в адреса и наоборот.

Серверы туннелирования (например, различные VPN-серверы) и прокси-серверы обеспечивают связь с сетью, закрытой маршрутизатором.

Серверы AAA и Radius обеспечивают в сети единую аутентификацию, авторизацию и ведение логов доступа.

Файл-серверы

Файл-серверы представляют собой серверы, обеспечивающие доступ к общим (закрытым) файлам и папкам на дисковом массиве сервера.

Прежде всего это серверы передачи файлов по заказу, по протоколам FTP, TFTP, SFTP и HTTP. Протокол HTTP ориентирован на передачу простых текстовых файлов. Файл-серверы могут передавать в качестве запрошенных файлов и другие данные, например динамически созданные вебстраницы, картинки, музыку, видео и т. д.

Есть серверы, позволяющие монтировать (подключать) дисковые разделы сервера в дисковое пространство клиента и полноценно работать с

файлами на них. Это позволяют делать серверы протоколов NFS и SMB. Серверы NFS и SMB работают через интерфейс RPC.

Серверные решения

Серверные решения – это готовые, аппаратно укомплектованные серверы, с предустановленной серверной ОС и/или пакеты программ, оптимизированные под выполнение компьютером функций сервера и/или содержащие в своем составе комплект программ для реализации типичного набора сервисов.

В качестве примера серверных решений могут служить Unix-системы, изначально предназначенные для реализации серверной инфраструктуры, или серверные платформы Microsoft Windows Server.

Серверные (готовые) решения служат для упрощения организации базовой ИТ-инфраструктуры, то есть для оперативного построения полноценной локальной сети в ОУ. Как правило, устанавливается серверная ОС, которая потом настраивается для решения конкретных задач. Причем выбор той или иной ОС определяется теми функциями, службами и сервисами, для которых она более всего подходит. Компоновка отдельных серверных приложений в решение подразумевает, что решение предназначено для выполнения большинства типовых задач; при этом значительно снижается сложность развертывания и общая стоимость владения ИТ-инфраструктурой, построенной на таких решениях.

По своему основному предназначению готовые серверные решения можно подразделить на:

1) серверы управления и обеспечения безопасности локальной сети (контроллер домена, антивирусный сервер, маршрутизатор);

2) серверы хранения данных (файловый сервер, сервер резервного копирования, сервер баз данных);

3) серверы внешнего взаимодействия (сервер динстанционного обучения, почтовый сервер, FTP-сервер, Web-сервер);

4) серверы специального назначения (серверы приложений, видеосерверы, сервер контроля и управления доступом, принт-серверы, факс-серверы);

5) серверы развлечений (серверы игровых приложений).

Рассмотрим, как организовано взаимодействие основных серверов на платформе Windows в защищенной локальной сети.

3. Организация функционирования локальной сети на основе Windows-серверов

В первую очередь следует отметить, что «…на основе Windows-серверов» означает то, что на платформе Windows построены основные серверные станции, управляющие локальной (LAN) сетью, отвечающие за её безопасность, индентификацию пользователей в ней, а не все серверы вообще. Грамотный инженеринг LAN проводится для оптимизации всех

основных задач, стоящих перед организацией. Серверные операционные системы должны подбираться исходя из их функциональности.

Рассмотрим организацию построения и функционирования LAN-сети на примере локальной сети Регионального центра оценки качества образования и информационных технологий, представленной на рис. 6.

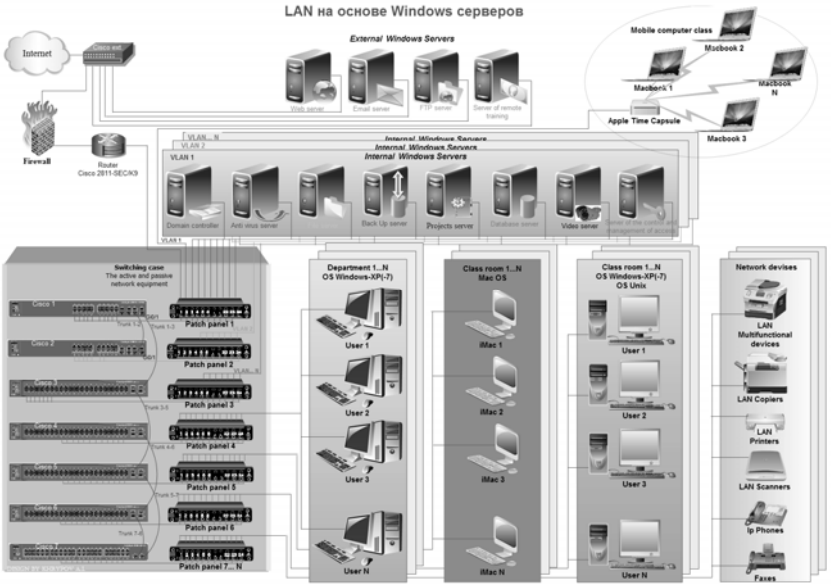

Рис. 6. Локальная сеть Регионального центра оценки качества образования и информационных технологий

Основными элементами такой сети являются:

1. Внешние серверные станции (*External Windows Servers)*. Выделенные серверы, находящиеся за пределами LAN-сети, имеющие постоянный диапазон внешних IP-адресов 82.137.164.1-6 для непосредственного выхода в Интернет.

2. Внутренние серверные станции (*Internal Windows Servers)*. Выделенные серверы, находящиеся за межсетевым экраном (*firewall*), защищающим LAN от несанкционированного доступа; имеющие постоянную (статическую) IP-адресацию во внутренней сети, находящуюся в диапазоне 192.168.0.1-254; управляющие и обслуживающие данную LAN-сеть.

3. Отдельные ПЭВМ (клиентские рабочие станции) сотрудников администрации, отделов, секторов (Department 1...N) под управлением Windows XP (7).

4. Компьютерные классы (Class room 1...N), оснащенные современными ПЭВМ для проведения ЕГЭ, процедур аттестации и лицензирования, курсов повышения квалификации и др. задач под управлением различных ОС: Windows XP (7), семейства Unix, Mac OS и т.д.

5. Мобильные компьютерные классы (Mobile computer class) на ноутбуках типа Macbook, работающие через беспроводную точку доступа Wi-Fi на Apple Time Capsule, выполняющей также функции резервного копирования информации с ноутбуков Macbook.

6. Периферийные сетевые устройства (Network devises) общего, раздельного использования. Устройства, имеющие сетевой интерфейс (имеющие статический IP-адрес в LAN-сети), работающие в многопользовательском режиме. К ним относятся:

- сетевые многофункциональные устройства;
- сетевые принтеры;
- сетевые сканеры.

7. Коммутационный шкаф (Switching case) с пассивным и активным сетевым оборудованием для коммутации и внутрисетевого взаимодействия всех компонентов LAN.

Организация функционирования предусматривает обмен информацией между выделенными серверными станциями, клиентами, периферийными сетевыми устройствами, высокоскоростной выход в Интернет.

Для обеспечения доступа на Web-сайты центра (Web server), пользования корпоративной электронной почтой (Mail server), доступа к файлообменнику (FTP server) для работы по программам динстанционного обучения необходим свободный доступ из Интернета всем заинтересованным пользователям. Поэтому такие серверные станции целесообразно разместить за пределами межсетевого экрана Firewall, присвоить им внешние IP-адреса, частично распарковать их DNSы на внешних серверах сторонних организаций, обеспечивая тем самым их безопасность.

Для контроля коммутации к нескольким каналам разных интернет–провайдеров и управления электронными портами, к которым подключены внешние серверные станции, целесообразно установить внешний электронный коммутатор со своим выделенным внешним IP-адресом.

В нашем случае роль такого «умного» коммутатора (Cisco Ext) выполняет Cisco Catalyst 2950. К нему подключены все без исключения External Windows Servers, имеющие внешние IP-адреса, включая и наш маршрутизатор (Router). Его назначение рассмотрим далее.

Следует отметить, что не все внешние серверные станции целесообразно строить на платформе Windows Server. Надо понимать, что эта самая распространенная платформа и дыры в ОС широко известны профессионалам в данной области. Поэтому FTP-сервер у нас построен на ОС Debian с ядром Linux.

Целесообразно Web-сервер и сервер электронной почты E-mail-сервер объединить в рамках одного устройства и построить их на ОС FreeBSD или на ОС Ubuntu Linux Server семейства Unix. Настройка и возможности этих серверов превосходят аналогичные на платформе Windows. На нашем Web-сервере размещается сайт ege.spb.ru и корпоративная почта.

В качестве ПО сервера динстанционного обучения (External Windows Servers) используется Moodle. Moodle написан на PHP с использованием SQL-базы данных (MySQL, PostgreSQL, Microsoft SQL Server и др. В качестве БД используется ADOdb XML). Moodle может работать с объектами SCO и отвечает стандарту SCORM. Сервер динстанционного обучения также использует стационарный внешний IP-адрес и имеет свой именной индентификатор.

Для управления LAN-сетью и обеспечения её безопасности важную роль играют *серверные станции управления*. Они защищают важную корпоративную информацию от НСД как внутри сети, так и от проникновения из Интернета и составляют основу выделенных внутренних серверных станций.

К таким серверам в первую очередь относится главный сервер организации – контроллер домена, в основе которого лежит интеллектуальная служба каталогов Active Directory.

Контроллер домена на базе Active Directory (AD) позволяет централизованно администрировать все ресурсы, включая пользователей, файлы, периферийные устройства, доступ к службам, сетевым ресурсам, веб-узлам, базам данных и так далее. AD поддерживает иерархическое пространство имён для учётной информации о пользователях, группах и компьютерах, а также о других каталогах, что в конечном счёте позволяет снизить административные издержки, связанные с поддержкой нескольких пространств имён. AD позволяет использовать единую точку администрирования для всех публикуемых ресурсов. В основе AD используется стандарт именования X.500, система доменных имён – Domain Name System (DNS) для определения местоположения, и в качестве основного протокола используется Lightweight Directory Access Protocol (LDAP). Кроме этого контролер домена осуществляет автоматическую раздачу IP-адресов через DHCP-сервер, ведет учет статических IP-адресов серверных станций, соответствие их именам через DNS-сервер и выполняет ряд других функций.

Настройка контроллера домена на базе ОС Windows Server 2003 Standart Edition (все до создания резервных копий – *back up*) подробно описана в приложениях к учебному пособию «Установка и настройка контроллера домена на WinServer 2003».

Настройка контроллера домена на базе ОС Windows Server 2008 R2 Enterprise Edition с настройкой основных функций брандмауэра Windows

подробно описана в приложениях к учебному пособию «Установка и настройка контроллера домена на WinServer 2008».

Для ПЭВМ или другого любого LAN-устройства контроллер домена по DHCP в автоматическом режиме выдает ему динамический IP-адрес в том случае, если в свойствах подключения по локальной сети ПЭВМ, в свойствах протокола Интернета TCP/IP установлен переключатель «Получить IP-адрес автоматически». Это означает, что любой компьютер пользователя не потребует дополнительных сетевых настроек для работы в данной сети.

Для входа в сеть с доменами с ПЭВМ проводится проверка имени пользователя и пароля. Если такое имя пользователя и пароль существуют в AD, то пользователь входит в домен, а если нет, то вход закрывается и ОС не пускает пользователя в сеть. Если пользователь входит не в домен, а на свою ПЭВМ, то такой компьютер попадает автоматически в рабочую группу Workgroup. Он может работать на своем компьютере локально, выходить в Интернет, так как получил свободный IP-адрес по DHCP от контроллера домена, но без авторизации в AD он не сможет работать с общими ресурсами LAN-сети на правах пользователей домена. Например, заходить в общие («расшаренные») папки на File Server и т.д.

Вторым важным сервером управления является маршрутизатор, или роутер (Router). Главной функцией маршрутизатора является защита внутренней LAN-сети и её ресурсов от проникновения извне. Он выполняет функцию Firewall, но при этом рядовые пользователи (users) свободно выходят в Интернет для решения служебных задач, отправки почтовых сообщений, сбора информации и т.п.

Основными задачами маршрутизатора при передаче пакета внутрь LAN-сети являются:

- принять пакет;
- найти клиента (компьютер), на которого следует этот пакет или следующий маршрутизатор по маршруту к нему (в таблице маршрутов);
- передать пакет или вернуть ICMP-сообщение о невозможности его доставки по следующим причинам:
  - назначение недостижимо (Destination unreachable) – у пакета кончилось «*время жизни*», прежде чем он достиг места назначения;
  - хост недостижим (Host unreachable) – компьютер или следующий маршрутизатор выключен или не существует;
  - сеть недостижима (Network unreachable) – маршрутизатор не имеет маршрута в сеть назначения;
- если пакет не может быть доставлен по причине перегрузки маршрутизатора (или LAN-сети) — отбросить пакет без уведомлений.

Маршрутизация может быть настроена на платформе ОС Windows Server 2003 (2008). Для этого необходимо выделить отдельную ПЭВМ под сервер и произвести соответствующие настройки. На практике удобнее ис-

пользовать аппаратно готовые маршрутизаторы с интуитивным графическим Web-интерфейсом под управлением своей ОС. Это экономит лицензии Windows и собственно целый компьютер, который целесообразно использовать для других важных задач. Поэтому в рамках этой главы мы не будем рассматривать алгоритм настройки маршрутизатора на платформе Windows Server. Следует только отметить, что маршрутизатор должен иметь минимум две сетевые карты и два настроенных протокола TCP/IP как для внешней интернет-сети, так и для внутренней LAN-сети, которые должны быть описаны при настройках в контроллере домена. Более того, маршрутизатор через свой IP-адрес внутренней LAN-сети является шлюзом для всех компьютеров локальной сети, через который они выходят в Интернет.

В нашем случае роль маршрутизатора выполняет аппаратный маршрутизатор Cisco 2811-SEC/K9 под управлением своей ОС IOS. Достоинствами данного роутера является его возможность соединять LAN-сети, находящиеся на удаленных площадках центра, в других районах, по VPN (Virtual Private Network)-туннелю и поддерживать шифрование передаваемых данных по протоколам IP Sec. Тем самым обеспечивается объединение территориально разбросанных, удаленных LAN-сетей в единую локальную сеть центра. Аппаратные функции и уникальность встроенной ОС особенно важны, так как именно маршрутизатор в первую очередь подвергается сетевым и вирусным атакам, попыткам «доброжелателей» прорваться внутрь LAN-сети.

Третьим сервером управления и контроля LAN-сети является антивирусный сервер. При большом количестве выделенных серверных станций, периферийных устройств и ПЭВМ-пользователей в LAN-сети он имеет большое значение, так как блокирует распространение вирусов и других угроз по сети от хоста к хосту. Кроме того, он поддерживает архитектуру клиент-сервер, облегчая тем самым развертывание антивирусных клиентов на ПЭВМ-пользователей и их обновление. Практически все известные производители антивирусного ПО как у нас, так и за рубежом имеют готовые серверные решения. В LAN-сети РЦОКОиИТ антивирусный сервер развернут на отдельном сервере, на платформе Windows Server 2008 R2 и построен на ПО Symantec Endpoint Protection ver. 11.0 I/O basic.

Важной группой серверных станций, обеспечивающих хранение, восстановление и работу с важной структурированной корпоративной информацией, являются *серверы хранения данных*. К ним относятся файловый сервер (File server), сервер резервного копирования (Back Up server) и сервер баз данных (Database server). Все они имеют статическую внутреннюю IP-адресацию в LAN-сети и именные идентификаторы в AD.

Файловый сервер построен на ОС Windows Server 2003 SP3. Через дополнительный контроллер к нему подключена внешняя корзина HP Storage Works Bay 14 ULTRA320 SCSI емкостью 2 Тб. Специальной настройки серверная ОС не требует; она необходима для одновременной работы на

сервере большого количества пользователей и настройки политик безопасности с целью ограничения доступа к отдельным сетевым папкам и каталогам. Данный сервер подключен к сети через сетевую карту, поддерживающую скорость обмена информацией 1 Гбит/с.

Сервер резервного копирования построен на программе FreeNas, в основе которой лежит ОС FreeBSD. FreeNAS-сервер включён в домен Microsoft AD и имеет хороший графический Web-интерфейс для администрирования. Основным предназначением данного сервера является хранение резервных копий основных активных разделов серверных и рабочих станций и их восстановление при сбоях и по заданию. Архивация данных может осуществляться в автоматическом режиме, по сети с использованием специального программного обеспечения (Acronis True Image Enterprise Server, Cobian Back Up и пр.). Резервному копированию в автоматическом режиме подлежат наиболее важные рабочие сетевые паки и каталоги. Данный сервер имеет встроенную корзину для хранения информации объемом 4 Тб. Используется в интересах обеспечения сохранности важной корпоративной информации всего центра.

Сервер баз данных обслуживает базы данных и обеспечивает целостность и сохранность данных при их хранении, а также операциях ввода-вывода при доступе клиента к информации. Сервер базы данных – один из ключевых компонентов в архитектуре вычислительной сети типа "клиент-сервер", в которой пользовательский интерфейс располагается на менее мощной машине-клиенте, а функции системы управления базами данных (СУБД) размещены на мощном сервере. Сервер баз данных работает под управлением СУБД Microsoft SQL Server и получает клиентские запросы на языке SQL. Используется отделом оценки качества образования для осуществления процедур оценки качества образования и процедур лицензирования и аккредитации учреждений СПО и ДПО в Санкт-Петербурге.

Последней группой внутренних серверных станций (Internal Windows Servers), используемой в РЦОКОиИТ, являются серверы специального назначения. К ним относятся выделенные серверы приложений (Projects servers), видеосерверы (Video servers), серверы контроля и управления доступом (Servers of the control and management of access), принт-серверы (Print servers), факс-серверы (Fax servers) и т.д.

Серверы приложений – это серверные станции, на которых в качестве платформы используется серверная ОС Windows Server или другая, а в качестве основного ПО используются различные приложения, позволяющие в многопользовательском режиме клиент-сервер решать узконаправленные, специальные задачи. Например, АИС «Экзамен» служит для обработки результатов тестирования выпускников 9-х классов, АИС «РОД» (регламентация образовательной деятельности) – для автоматизации процедур формирования и обработки данных лицензионной и аккредитационной

экспертизы в образовательных учреждениях, АИСУ «Параграф-Движение» – для контроля обучения детей школьного возраста, предупреждения их отсева, анализа потоков движения между ОУ, составлению статистической отчетности и т.д. Серверы приложений имеют распределенную структуру (могут находиться не на одном компьютере), получают данные для своих АИС не только от внешних источников ввода информации и клиентских ПЭВМ, но и от СУБД, т.е. тесно взаимодействуют с серверами баз данных.

Видеосерверы и серверы контроля и управления доступом составляют основу комплексной системы безопасности центра. Первые служат для сбора, хранения видеоинформации, поступающей от внешних и внутренних видеокамер, и её отображения на несколько постов видеоконтроля в режиме реального времени; в качестве платформы используется ОС Windows Server 2003 Std. Edition, а в качестве СПО – VideoNet ver. 8. Видеосерверы имеют статическую IP-адресацию и включены в отдельную рабочую группу. Серверы контроля и управления используются для автоматизированного управления доступом через точки прохода и накопления статистической информации о пользователях системы через их электронные ключи. Сервер контроля и управления доступом построен на такой же платформе, с использованием СПО Скайрос Quest-1000D. На него установлен доступ из LAN-сети для управления и администрирования.

Рассмотрим, как выполнена коммутация и осуществляется сетевое взаимодействие всех элементов внутренней LAN-сети.

Все серверные станции (смонтированы в специальные шкафы для серверов, которые находятся в отдельном помещении – серверной. Здесь поддерживается необходимая температура и микроклимат через систему кондиционирования воздуха. Мощные источники бесперебойного питания (APC SU5000R5/BX120, APC Symmetra 6000VA, APC SMART-UPS RT 10000VA) от 5 до 10 кВА, установленные внизу шкафов, обеспечивают серверы стабильным напряжением питания и защищают их от помех, в том числе и при отключении питания, при авариях городской электросети.

Каждая из серверных станций отдельным кабелем категории 5е или 6е коммутируется (расшивается) на выделенной патч-панели (Patch panel 1-2) для серверных станций в коммутационном шкафу (см. рис. 6). В этот же коммутационный шкаф из кабинетов отделов, учебных классов, от ПЭВМ сотрудников и слушателей, от периферийного оборудования через информационные розетки, каждое в отдельности устройство по кабель-трассам информационными кабелями категории 5е приходит и расшивается на портах с внутренней стороны патч-панелей.

Патч-панели составляют основу пассивного сетевого оборудования коммутационного шкафа. С внешней стороны задействованные порты каждой патч-панели патч-кордами соединяются с портами на активных электронных коммутаторах Cisco, которые составляют основу активного сетевого оборудования коммутационного шкафа.

Все электронные коммутаторы Cisco с 1-го по 7-й соединены между собой через выделенные порты Trunk-кабелями со скоростью 1 Гбит/с в единый электронный коммутатор. Причем Cisco (Catalyst 2960) № 1, 2 являются коммутаторами верхнего уровня. У них все порты поддерживают скорость обмена информации до 1 Гбит/с. Поэтому серверные станции и выделенные ПЭВМ, которым нужна высокая скорость подключения к LAN-сети, коммутируются к ним. Cisco (Catalyst 3560, 2960) № 3-7 имеют по 48 рабочих портов со скоростью обмена информацией до 100 Мбит/с. К ним подключается всё остальное сетевое оборудование. Таким образом, происходит коммутация на физическом уровне всех устройств в единую LAN-сеть.

На программном уровне взаимодействие между ПЭВМ, периферийными устройствами (ПУ), клиент-серверами и серверами осуществляется независимо от того, какая ОС используется на том или ином устройстве (Windows, Unix, Mac и т.д.) по стеку протоколов TCP/IP (англ. *Transmission Control Protocol/Internet Protocol*). Остается лишь настроить параметры подключения по локальной сети для выделенных серверных станций со статической IP-адресацией или установить автоматическое получение настроек сети (по DHCP) для клиентов. Кроме того, все хосты LAN-сети должны быть членами того или иного домена.

Важно отметить, что все электронные коммутаторы Cisco поддерживают VLANы (*Virtual Local Area Network*). Поэтому в нашей LAN-сети пока организованы 2 виртуальные подсети со своим набором внешних и внутренних серверных станций и их клиентами. Причем клиенты и ПУ могут мигрировать между VLANами, подключаясь к первой или второй виртуальной сети в зависимости от решаемых задач и требуемого состава оборудования. Это достигается переводом необходимых портов на электронных коммутаторах в тот или другой VLAN через специальные команды в IOS Cisco. Обе виртуальные подсети разделены между собой, имеют свою IP-адресацию и закрыты для пользователей другой подсети. Это достигается расширенной сетевой безопасностью, применяемой Cisco с использованием широкого диапазона методов идентификации, технологий кодирования данных, сетевым управлением по пользователю, порту и MAC-адресу.

4. Организация функционирования локальной сети на основе Linux-серверов

Как уже было отмечено выше в основе LAN-сети стоят серверные станции управления. Первоочередным сервером управления является контроллер домена, в основе которого лежит интеллектуальная служба каталогов Active Directory. Рассмотрим варианты построения DC на *nux-системах для выбора оптимального решения. Вашему вниманию предлагается несколько вариантов DC, описанных в приложении (статья «Обзор контроллеров домена на Linux-платформах»), на: Mandriva Directory Server

(MDS), BSL OS, ClarkConnect Server (CCS), Fedora Directory Server (FDS, он же 389 Directory Server).

Выводы:

1. Используя одно из вышеописанных решений, Вы получаете домен уровня NT4 (Samba3+LDAP). Этот стандарт ниже, чем домен на базе Windows 2003/2008.

2. Данные решения подойдут организациям, в которых парк ПЭВМ не превышает 80-100 единиц.

3. Их плюсы состоят в том, что все они входят в сегмент свободно распространяемого программного обеспечения.

4. Существует возможность их интеграции «без особых проблем» в *nux-машины на уровне LDAP.

5. ПЭВМ на ОС Windows в домене на ОС Linux работают отлично, профили пользователей сохраняются, подключаются сетевые диски, имеется частичная возможность по реализации групповых политик безопасности (http://hidx.wordpress.com/2009/01/28/gpo-samba-domen/), но только на уровне домена NT4. Глобальные групповые политики, которые есть в Windows 2003/2008, реализовать не получится. Это основная причина, которая затрудняет использование данных доменов в организациях с парком более чем в 100 единиц ПЭВМ.

5. Развитие локальной сети

Развитие LAN-сети должно проходить по направлениям: масштабируемость и виртуализация. Это означает, что построенная LAN-сеть на физическом уровне должна обеспечить развитие Вашей организации как минимум на 10 лет вперед, пока не будут разработаны новые стандарты скорости передачи данных и не будут спроектированы их физические прототипы.

В каждом помещении, где возможно расположение «сотрудников на вырост», должно быть установлено необходимое количество сетевых розеток для подключения ПЭВМ и различных сетевых устройств с 15-20%-ным запасом, чтобы потом не пришлось протягивать дополнительные кабели витой пары. Розетки рекомендуется ставить двухпортовые, использовать только полноценную витую пару кабеля категорий 5е или 6е до каждого отдельного порта! Только в этом случае будет возможность «поднять» по LAN-сети скорость передачи данных в единицы-десятки Гбит/с, что позволит в последующем работать с потоковым видео в режиме Real Time, проводить видеоконференции и круглые столы, и многое, многое другое.

Коммутаторы LAN-сети должны иметь возможность электронного управления портами, с функцией виртуализации (поддержкой Virtual LAN).

Клиентов в современных локальных сетях следует подключать по коммутируемым каналам *Fast Ethernet*. Главную магистраль предачи данных современных сетей следует строить на основе коммутаторов *Gigabit Ethernet*, причем коммутаторы «ядра сети» нужно соединять по мультигигабитным каналам, а коммутаторы «края сети» должны быть соединены с ядром по каналам с пропускной способностью не менее 1 Гбит/с.

Центральные серверы (серверы, доступные большинству клиентов сети) следует подключать по гигабитным каналам связи к ядру сети.

При построении кабельной системы следует стремиться к созданию СКС (структурированной кабельной системы). Вертикальная проводка должна быть выполнена оптическим кабелем. Абонентскую часть LAN-сети (горизонтальную проводку) рекомендуется строить унифицированной, т.е. необходимо использовать однотипные кабели и розетки для компьютерной и телефонной сети. Это позволит без дополнительных усилий подключать телефонные станции в обычные информационные розетки и осуществлять необходимую коммутацию прямо в коммутационном шкафу на портах патч-панелей.

Для соединения удаленных площадок одной организации в единую LAN-сеть с обеспечением высокого уровня безопасности передаваемой информации по открытым каналам связи необходимо использование маршрутизаторов с поддержкой VPN-туннелей (Virtual Private Network) и шифрованием данных по протоколам IP Sec.

ПОДКЛЮЧЕНИЕ МОБИЛЬНЫХ КЛАССОВ APPLE К ЛОКАЛЬНОЙ СЕТИ

В.Е. Ильин, старший методист ГОУ ДПО ЦПКС СПб «Региональный центр оценки качества образования и информационных технологий»

Для обеспечения совместной работы компьютеров мобильного класса Apple и подключения их к локальной сети (Ethernet) используется точка доступа AirPort. В настоящее время в мобильных классах Apple, поступивших в образовательные учреждения Санкт-Петербурга, используются различные версии этого устройства: AirPort, AirPort Express и AirPort Extreme (Time Capsule). Несмотря на различные модификации точки доступа, действия по подключению мобильного класса к локальной сети выполняются аналогично с использованием **AirPort-Утилиты**.

Подключение мобильного класса с помощью точки доступа к локальной сети и Интернету можно отобразить с помощью рис.1.

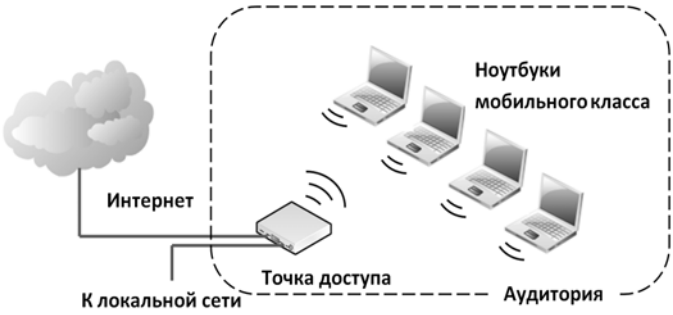

Рис. 1. Подключение мобильного класса к локальной сети и Интернету

Как это работает

Точка доступа (в нашем примере Time Capsule) использует сеть Ethernet для связи с Интернетом через порт Ethernet локальной сети. Компьютеры мобильного класса обращаются к Интернету и локальной сети через беспроводное устройство Apple – AirPort.

Что необходимо для подключения компьютеров мобильного класса к Ethernet

1. Беспроводное устройство Apple (базовая станция AirPort Extreme, AirPort Express или Time Capsule), настроенное в режиме моста.

2. Маршрутизатор Ethernet, коммутатор или другое сетевое устройство. Маршрутизатор, коммутатор или другое сетевое устройство настраиваются так, чтобы предоставлять IP-адреса компьютерам и устройствам в сети Ethernet. Минимально для подключения точки доступа вполне достаточно сетевой розетки RJ-45, подключенной к локальной сети.

Как правило, при корректном соединении точки доступа с локальной сетью и включении компьютеров мобильного класса сразу получаем работоспособную систему. В том случае, если связь компьютеров с локальной сетью и Интернетом отсутствует, может потребоваться настроить точку доступа и компьютеры вручную. Для настройки точки доступа используется специальная программа – AirPort-Утилита.

При использовании AirPort-Утилиты для настройки беспроводного устройства вручную выполните следующие действия:

1. С помощью программы Finder откройте AirPort-Утилиту, расположенную в папке «Служебные программы» папки «Программы» на компьютере Mac (или «Пуск» > «Все программы» > «AirPort» на компьютере с ОС Windows).

2. Выберите устройство и выберите «Настройка вручную» в меню «Базовая станция» или дважды нажмите значок устройства для открытия настройки в отдельном окне.

3. Нажмите «Интернет» и выберите «Ethernet» во всплывающем меню «Подключиться, используя» (рис. 2).

4. Выберите «Вручную» или «Использовать DHCP» во всплывающем меню «Конфигурация IPv4» в зависимости от предоставления IP-адресов в сети Ethernet.

5. Если адреса предоставляются вручную, выберите «Вручную» во всплывающем меню «Конфигурация IPv4». Введите информацию об IP-адресе в поля, расположенные ниже всплывающего меню «Конфигурация IPv4».

Если AirPort-Утилита уже использовалась для настройки беспроводного устройства, следующие поля снизу от всплывающего меню «Конфигурация IPv4» могут уже содержать соответствующую информацию. В том случае, если утилита используется впервые, поля будут пусты (см. рис. 2).

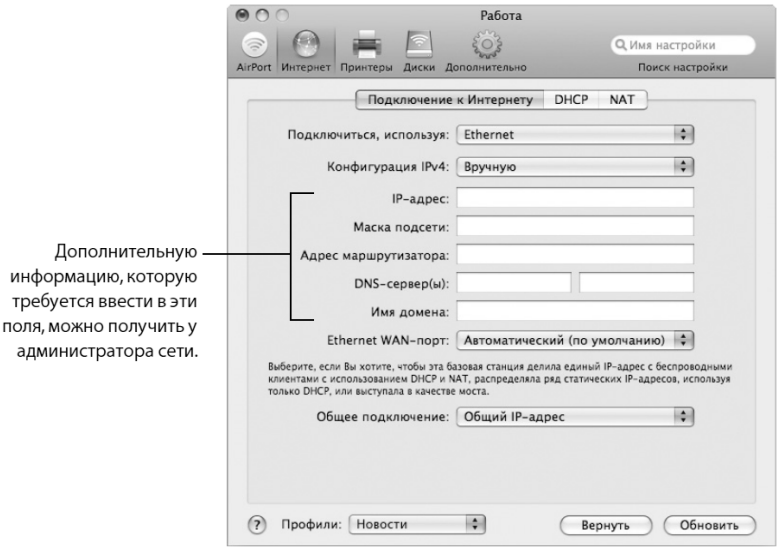

Рис. 2. Окно настройки AirPort-Утилиты

Если IP-адрес предоставляется с помощью DHCP, выберите «Использовать DHCP» (рис 3) во всплывающем меню «Конфигурация IPv4».

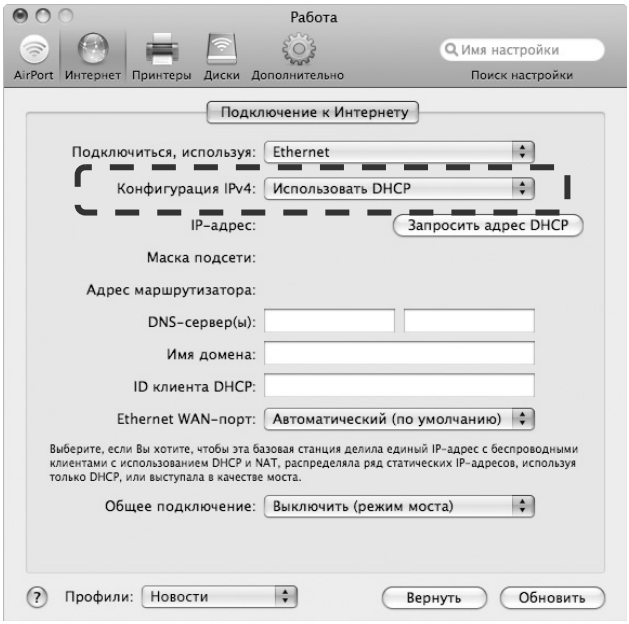

Рис. 3. Окно настройки DHCP

6. Выберите «Выключить (режим моста)» во всплывающем меню «Общее подключение».

Для создания сети AirPort следует выполнить следующие шаги:

1. Открыть «**Настройки сети**» и выбрать **AirPort** из всплывающего меню «**Показать**». Нажать **AirPort** и убедиться в том, что маркером отмечена опция «**Разрешить этому компьютеру создавать сети**».

2. Открыть программу «**Подключение к Интернету**» и нажать значок **AirPort** на панели кнопок.

3. Выбрать «**Создать сеть**» во всплывающем меню «**Сеть**». Задать имя сети и нажать **«Показать параметры**», чтобы создать пароль для сети.

4. Также можно использовать значок статуса AirPort в строке меню для создания сети «компьютер-компьютер».

Другие компьютеры также могут подключаться к созданной беспроводной сети, выбирая ее из меню статуса **AirPort** или всплывающего меню «**Сеть**» в окне программы «**Подключение к Интернету**».

Работа в локальной сети

Изменение приоритета сетевых соединений

Если компьютер устанавливает соединение с Интернетом или сетью разными способами (например, используя AirPort или встроенный Ethernet, т.е. напрямую соединен с ЛС-кабелем), можно изменить приоритет конфигураций сетевых портов, используемых компьютером для подключения.

Настройка клиентских компьютеров

Для настройки протокола TCP/IP на ноутбуках MacBook следует выполнить следующие действия.

1. Откройте программу «Системные настройки» на ноутбуке MacBook и нажмите «Сеть».

2. Используя диалоговое окно «Сеть», выполните одно из следующих действий.

A. Если на ноутбуке MacBook используется AirPort, в списке услуг подключения к сети выберите AirPort и нажмите «Дополнительно» (рис. 4).

Рис. 4. Окно настройки сети AirPort

Затем выберите «DHCP» во всплывающем меню «Конфигурация IPv4», если используется автоматическое распределение IP-адресов (рис. 5).

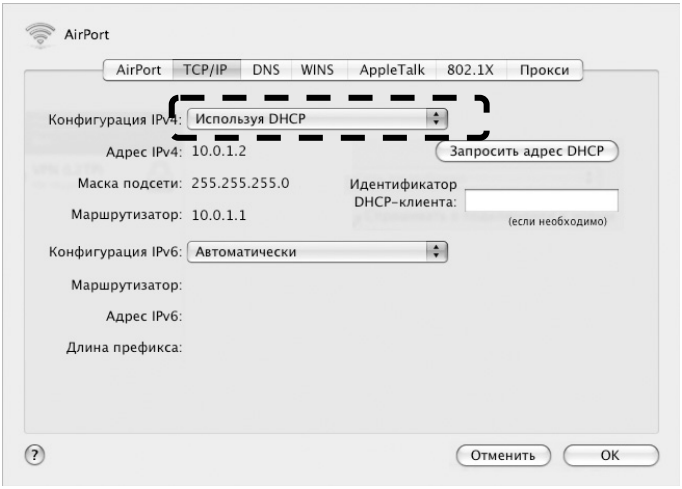

Рис. 5. Окно настройки сети. Настройка IP-адреса компьютера

Б. Если при настройке сети беспроводного устройства разрешен сервер DHCP (автоматическое распределение IP-адресов) и ноутбук подключается непосредственно к локальной сети (использует Ethernet), в списке услуг подключения к сети выберите Ethernet и выберите «Используя DHCP» во всплывающем меню «Настройка» (рис. 6).

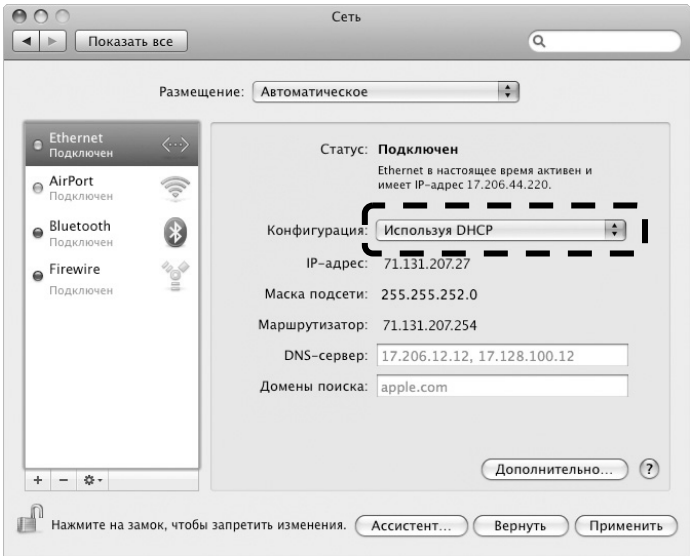

Рис. 6. Окно настройки сети при непосредственном подключении ноутбука к локальной сети

B. Если при настройке сети беспроводного устройства выбран параметр «Распределить диапазон IP-адресов», можно предоставить клиентским компьютерам с Ethernet доступ к Интернету, настроив IP-адреса клиента вручную.

В списке услуг подключения к сети выберите Ethernet и выберите «Вручную» во всплывающем меню «Настройка» (рис. 7).

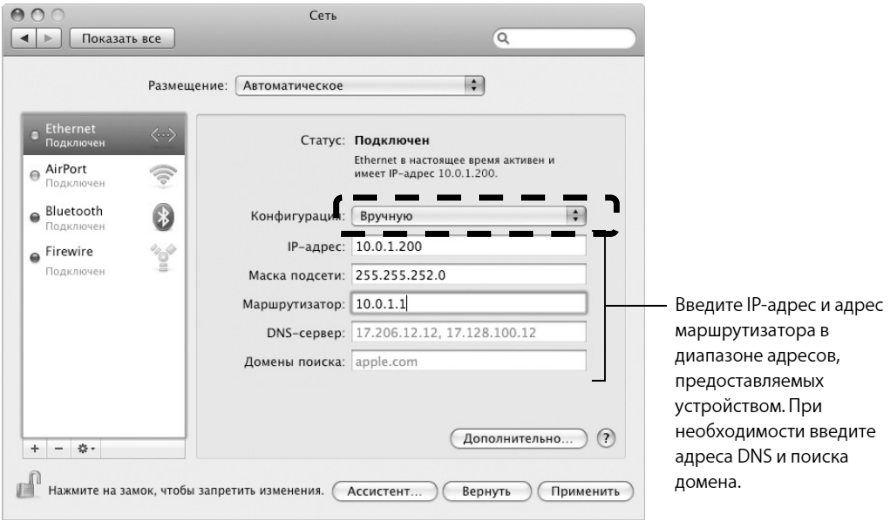

Рис. 7. Окно настройки сети при назначении IP-адреса компьютера вручную

ФАЙЛОВЫЙ СЕРВЕР FREENAS

И.А. Туманов, программист, Центр технического сопровождения образовательных программ (ЦТСОП) по факультету прикладной математики – процессов управления (ПМ-ПУ) СПбГУ

Общая информация

FreeNAS – свободно распространяемый дистрибутив на основе операционной системы (ОС) FreeBSD, предназначенный для организации сетевого файлового хранилища. FreeNAS не требует специальных знаний в области

UNIX-систем, управляется полностью через веб-интерфейс, русифицирован и достаточно демократичен в использовании системных ресурсов.

Официальный сайт проекта – www.freenas.org.

Подготовка системы

FreeNAS представляет собой LIVE-CD-дистрибутив, который может загружаться без установки системы на постоянный носитель, и позволяет сохранять настройки системы в виде XML-файла на обычный флоппи-диск или на USB-диск, отформатированные в FAT.

FreeNAS может быть установлен на ПК, причём не только на жёсткий диск, но также и на flash-накопитель.

Для функционирования ОС достаточно наличия 64 Мб свободного места на носителе информации, что позволяет использовать в качестве носителя как старые жёсткие диски, так и малоёмкие flash-накопители.

FreeNAS позволяет конфигурировать разделы дисков для хранения данных, в том числе и с использованием программных RAID-массивов, что позволяет организовать эффективную систему хранения даже на обычных ПК.

FreeNAS позволяет организовать доступ к сетевым ресурсам при помощи как встроенной системы авторизации (пользователи и группы), так и внешних систем, таких, например, как LDAP, и реализует поддержку технологий Active Directory, что позволяет применять его в доменах на основе Microsoft Windows Server.

Для минимальной установки FreeNAS версии 0.7.1 требуется 256 Мб оперативной памяти (более ранние версии, которые можно также скачать на сайте проекта, требовали 128 и даже 96 Мб), floppy-диск или USB-устройство для хранения конфигурационных файлов, а также жесткий диск и\или flash-накопитель для хранения данных.

Для оптимальной конфигурации желательно выделить отдельный накопитель (не менее 64 Мб) для установки ОС (жесткий диск или flash-накопитель, но тогда ПК должен поддерживать загрузку с USB-устройством), а также несколько жестких дисков (не меньше двух) для хранения данных для организации RAID-массива.

Установка системы

После загрузки системы с CD-диска можно увидеть следующее меню (рис. 1):

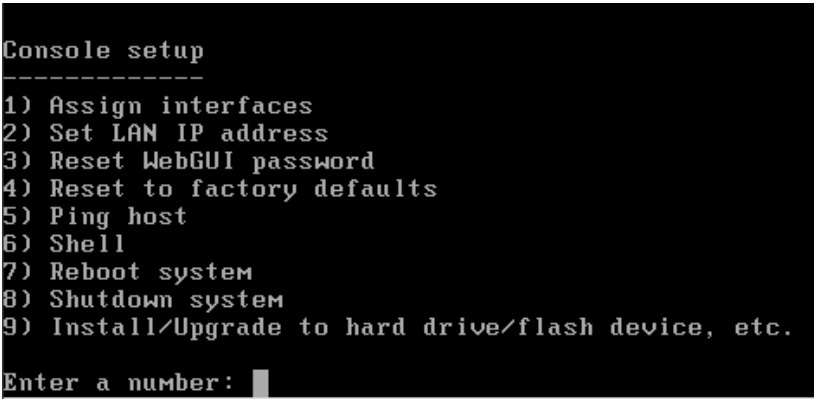

Рис. 1. Окно меню установки системы

Система уже работоспособна, но мы рассмотрим способ её установить на жёсткий диск или flash-накопитель, используя для этого пункт 9 (см. рис. 1).

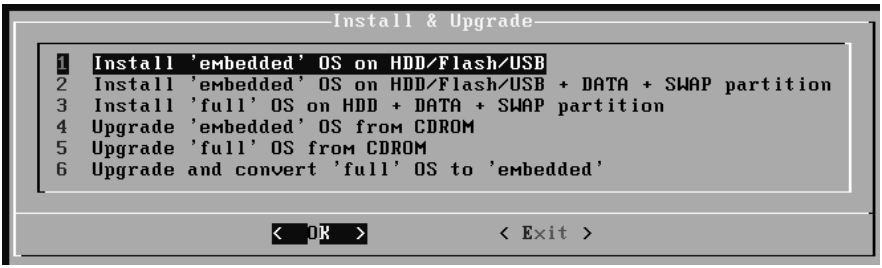

Рис. 2. Окно выбора способа установки

В следующем окне (рис. 2) рассмотрим чуть подробнее пункты:

• Установка «встроенной» ОС – это режим для ПК, где есть выделенный носитель только для ОС (HDD,FLash,USB). Для такого носителя достаточно 64 Мб оперативной памяти и нет никаких требований к производительности – можно использовать старый медленный жёсткий диск, USB-накопитель, а также IDE-Flash-диски небольшого размера, которые чаще всего устанавливаются в терминальных ПК. При установке все данные с диска будут уничтожены и его НЕЛЬЗЯ БУДЕТ ИСПОЛЬЗОВАТЬ для других нужд (например, для хранения данных).

• Установка «встроенной» ОС + DATA + SWAP – это режим для ПК только с одним носителем (в будущем можно будет добавить другие носители). В этом режиме установщик уничтожит все данные с диска и разобьёт его самостоятельно на раздел для системы, раздел для данных и SWAP-раздел (для файла подкачки).

• Установка «полной» ОС. Отличие «полной» ОС от «встроенной» заключается в том, что в полном режиме остается возможность доустанавливать дополнительное ПО, совместимое с ОС FreeBSD. Данный режим рассматривать не будем, так как он требует специальных знаний по работе в UNIX-системах.

• 5 и 6 пункты (см. рис. 2) – это режимы для обновления уже установленной системы.

В рамках данной статьи выберем п. 2 (см. рис. 2) для установки системы на ПК с одним жёстким диском. Откроется окно предупреждения об особенностях данного режима установки (рис. 3). Для продолжения следует нажать «ОК».

Рис. 3. Окно предупреждения об особенностях режима установки

В окне создания виртуального CDROM нажимаем ОК (рис. 4).

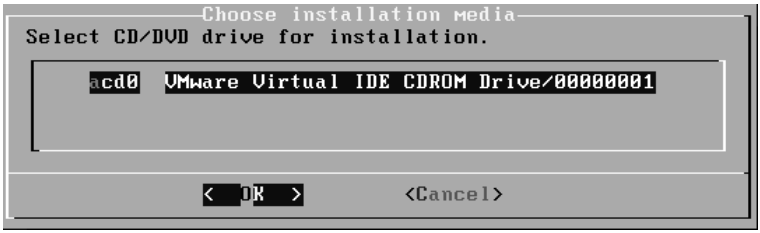

Рис. 4. Окно создания виртуального CDROM

Открывается окно создания SWAP-раздела (рис. 5).

Рис. 5. Окно создания SWAP-раздела

От создания SWAP-раздела можно отказаться (нажимаем «No»).

Установка завершена. Нажимаем ENTER для продолжения и вернемся в меню установки. Выбираем EXIT, а потом пункт 7 (см. рис. 1) для перезагрузки системы уже без СД-диска.

Настройка системы

После запуска системы на экране предлагается меню из нескольких пунктов для основных элементов настройки системы (все остальные возможности реализованы в режиме веб-интерфейса). Рассмотрим основные пункты подробнее (рис. 6):

Рис. 6. Окно настройки системы

- Выбор сетевой карты для доступа к локальной сети (для ПК с несколькими сетевыми картами).
- Установка IP-адреса для доступа к FreeNAS (по умолчанию 192.168.1.250).
- Сброс пароля администратора web-интерфейса (пользователь «admin», пароль по умолчанию «freenas»).
- Сброс всех настроек до первоначальных.

Для начала скорее всего придется изменить IP-адрес на подходящий для конкретной ЛВС, выберем пункт 2 (см. рис. 6).

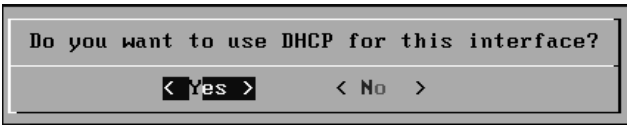

Рис. 7. Окно настройки использования DHCP

В данном окне (рис. 7) рекомендуется выбрать режим ручной адресации устройства, чтобы не использовать автоматически назначаемый IP-адрес. Нажимаем «No». Откроется окно для ввода IP-адреса (рис. 8).

Рис. 8. Окно для ввода IP-адреса

Изменим адрес, например, на 192.168.0.220 (рис 9).

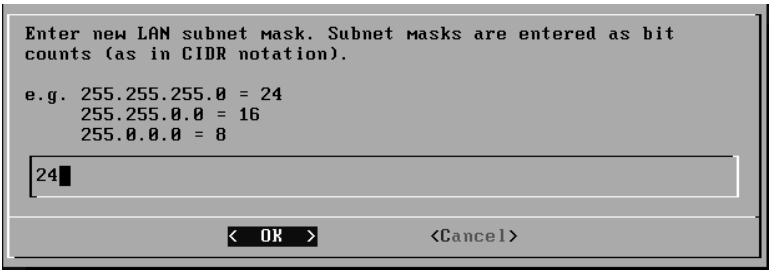

Рис. 9. Окно ввода маски сети

Выбираем маску сети (обычно достаточно оставить 24 по умолчанию).

Следующие два окна попросят ввести адрес шлюза и DNS-сервера, их можно оставить пустыми.

Настройку протокола IPv6 мы в нашем примере делать не будем (рис. 10). Нажимаем «No» и продолжаем настройку FreeNAS.

Рис. 10. Окно конфигурирования протокола IPv6

Все настройки сделаны и можно переходить в режим веб-управления (рис. 11).

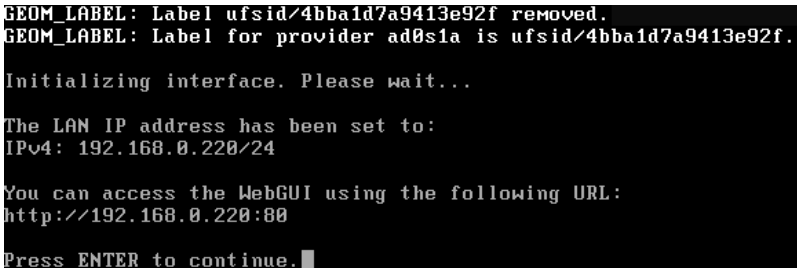

Рис. 11. Окно состояния настройки IP-адреса

Настройка FreeNAS с помощью Web-интерфейса

Если настройки IP-адреса были сделаны корректно, то можно с любого другого ПК, подключенного к данной сети, зайти на FreeNAS при помощи Web-интерфейса, т. е. набрать в строке браузера http://192.168.0.220 (рис. 12):

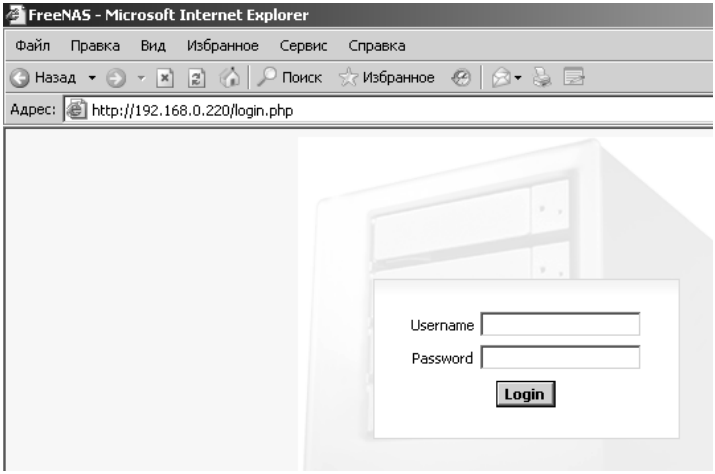

Рис. 12. Окно Web-интерфейса настройки FreeNAS

Имя входа по умолчанию «admin», пароль «freenas». Вводим данные, нажимаем кнопку «Login» и попадаем в первоначальное окно настройки системы (рис. 13).

Рис. 13. Начальное окно настройки FreeNAS по Web-интерфейсу

Для начала целесообразно изменить язык настройки системы на русский. Меню System->General (рис. 14).

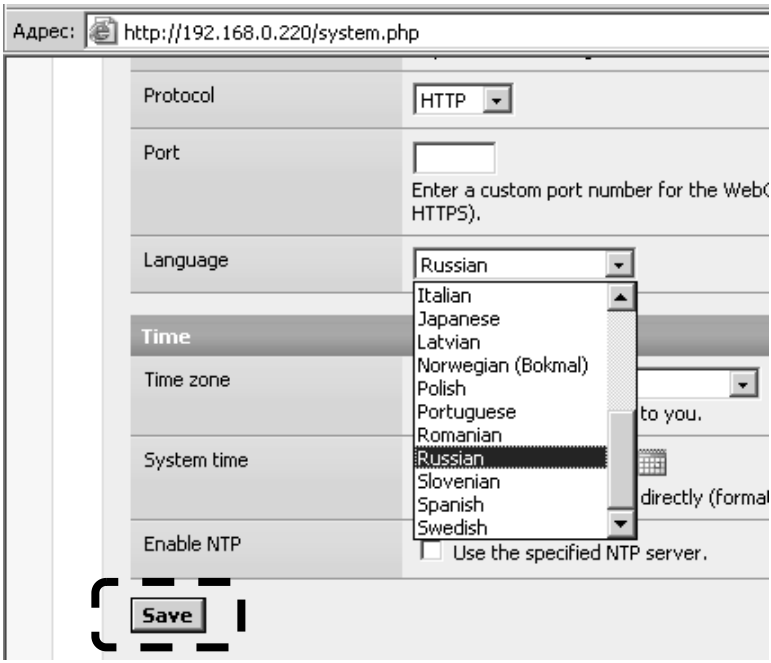

Рис. 14. Окно выбора языка настройки

После выбора языка настройки следует нажать «Save» внизу экрана. После первого входа в систему настоятельно рекомендуется изменить пароль администратора в меню Система→Общие→Пароль.

Подготовка диска для хранения данных

Теперь нужно подготовить диск для хранения данных (мы его уже создали и отформатировали при установке системы, сейчас его надо подключить). Выбираем меню Диски→Управление и нажимаем «✚» в правом углу для добавления диска (рис. 15).

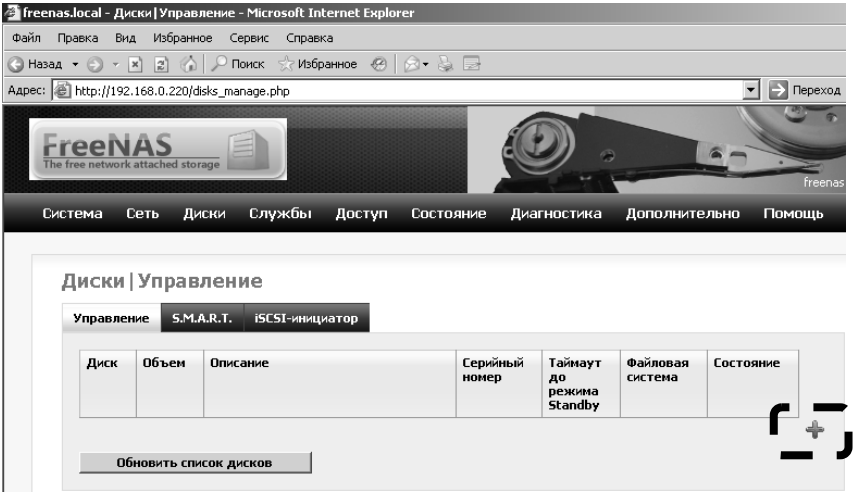

Рис. 15. Начальное окно настройки дисков

Выбираем диск (созданный нами диск имеет размер 8 Гб), устанавливаем для него имеющуюся файловую систему UFS), остальные параметры оставляем по умолчанию и нажимаем «ДОБАВИТЬ» внизу экрана (рис. 16 и 16, *а*).

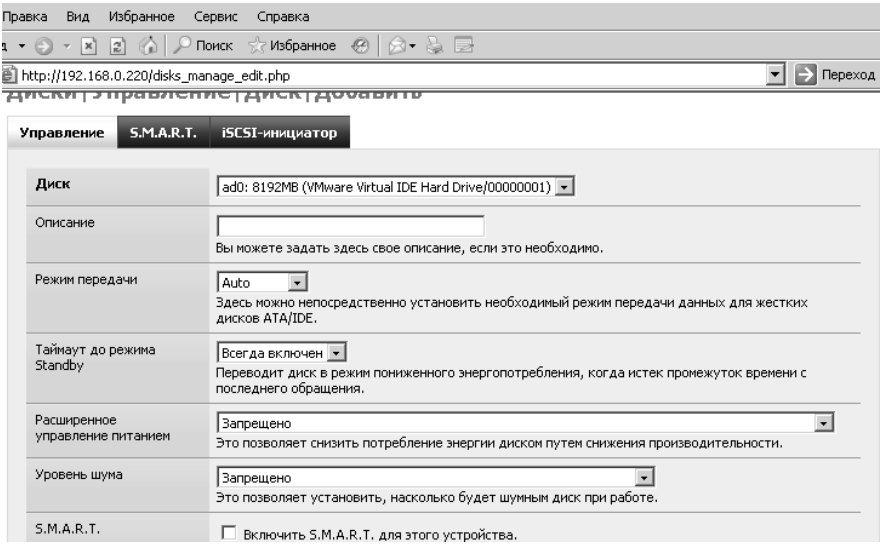

Рис. 16. Окно настройки параметров диска

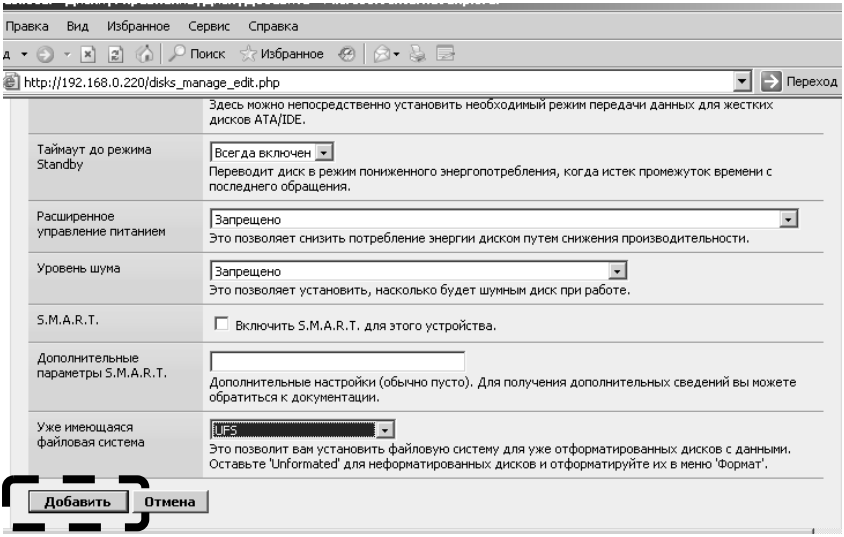

Рис. 16, а. Окно настройки параметров диска

В следующем окне нажимаем «Применить изменения» (рис. 17).

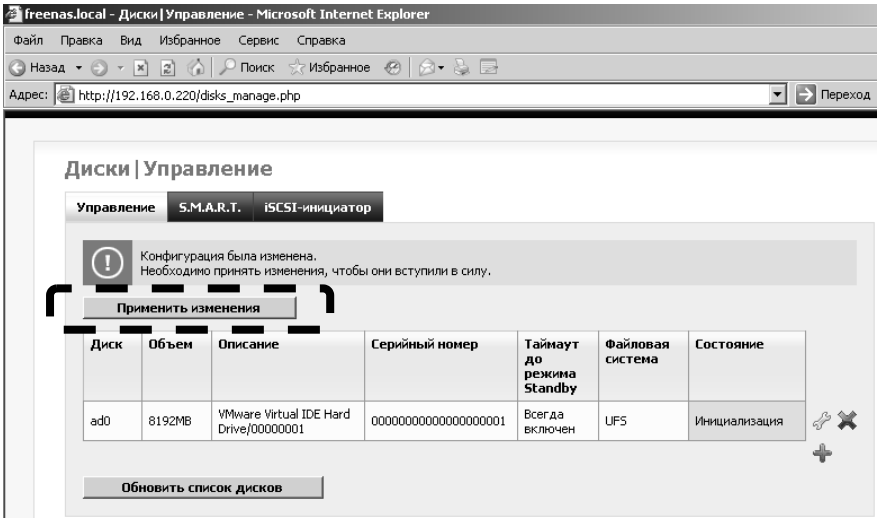

Рис. 17. Окно завершения настройки диска

Диск добавлен и доступен в режиме on-line (рис. 18).

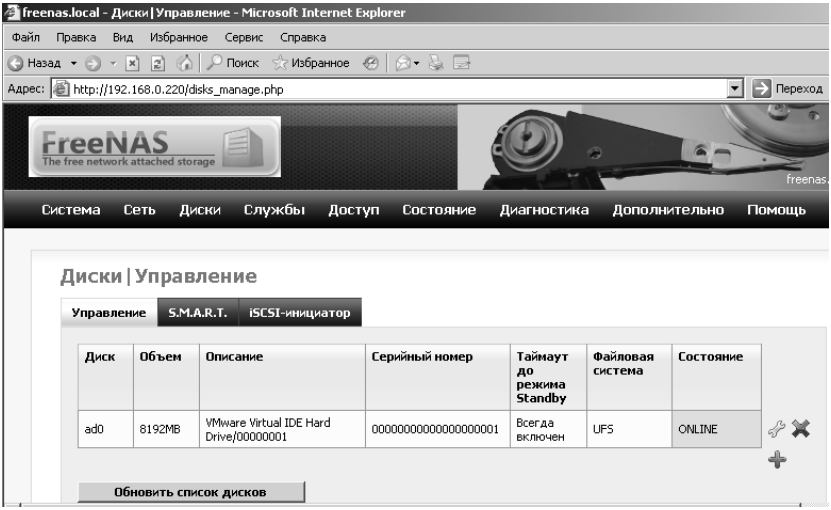

Рис. 18. Окно состояния настроек диска

Далее этот диск нужно подмонтировать к файловой системе (аналог назначения буквы диска в Windows). Выбираем меню Диски→Точка монтирования→Добавить(«✚»).

В появившемся окне выбираем наш диск, указываем тип раздела MBR, номер раздела 2 и придумываем имя точки монтирования, пусть это будет DATADISK; затем нажимаем ДОБАВИТЬ, а в следующем окне – «Применить изменения». Конечный вариант приведен на рис. 19.

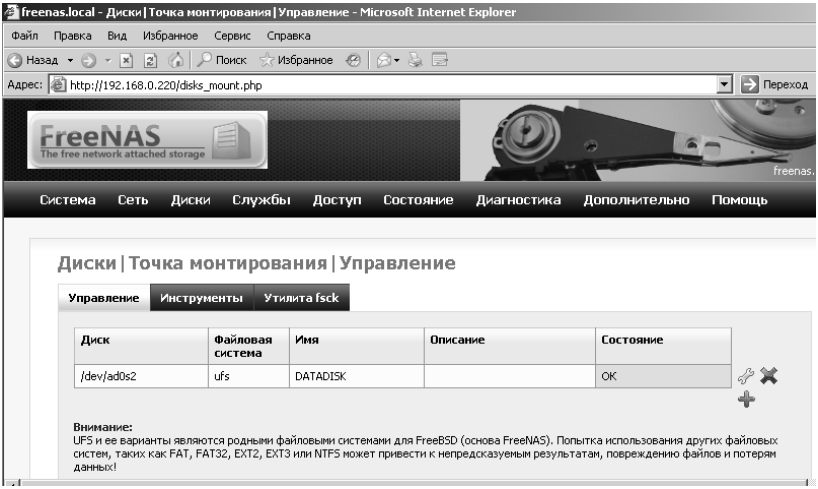

Рис. 19. Окно настроек смонтированного диска

Теперь диск подготовлен к использованию. После настройки диска следует перейти к настройкам доступа к нему.

Доступ к общим каталогам без авторизации

Для предоставления общего доступа к каталогу надо сначала создать этот каталог, а потом предоставить к нему сетевой доступ.

Для примера создадим общий ресурс FILES.

Запустим файловый менеджер (рис. 20).

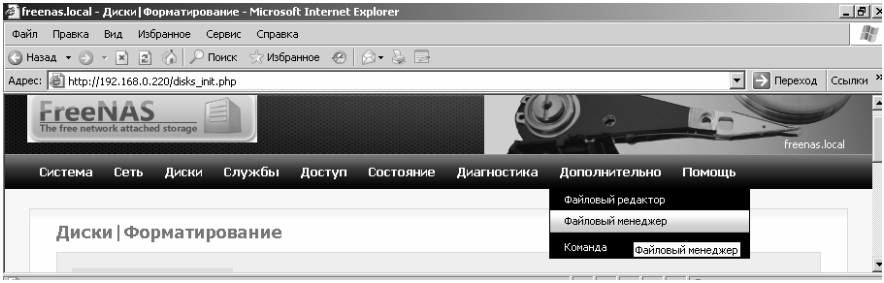

Рис. 20. Окно файлового менеджера

Зайдем в каталог mnt, а потом в созданный и смонтированный ранее диск DATADISK (рис. 21).

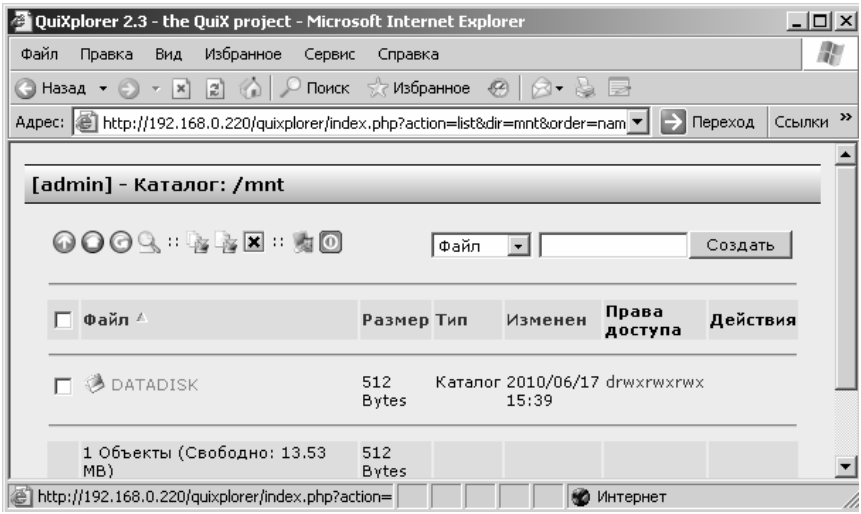

Рис. 21. Окно диска DATADISK

Сверху в выпадающем списке выберем «Каталог», введем название FILES и нажмем «Создать» (рис. 22).

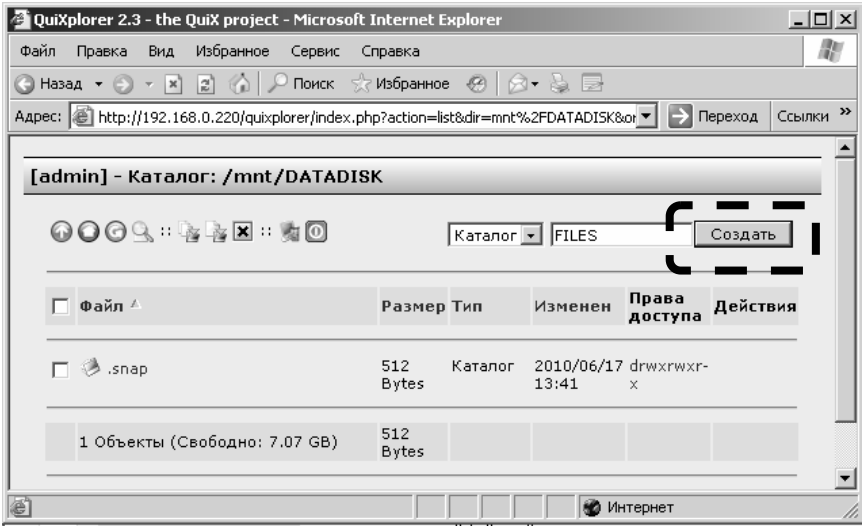

Рис. 22. Окно создания каталога FILES

Теперь каталог создан, но доступен всем только для чтения. Нажмем на набор символов напротив FILES в столбце «Права доступа» (рис. 23).

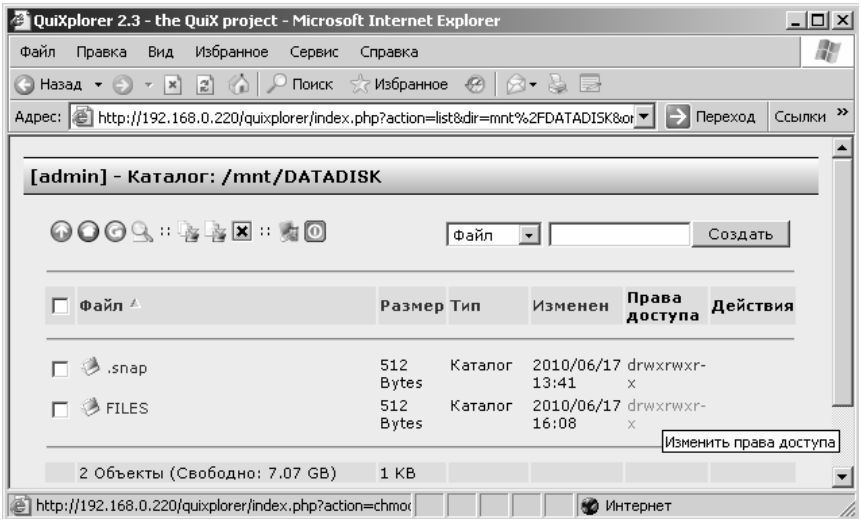

Рис. 23. Окно настройки прав доступа к каталогу FILES

Если необходимо разрешить запись всем пользователям в этот каталог, то надо установить галочку для параметра w (право на запись) и нажать «Изменить» (рис. 24).

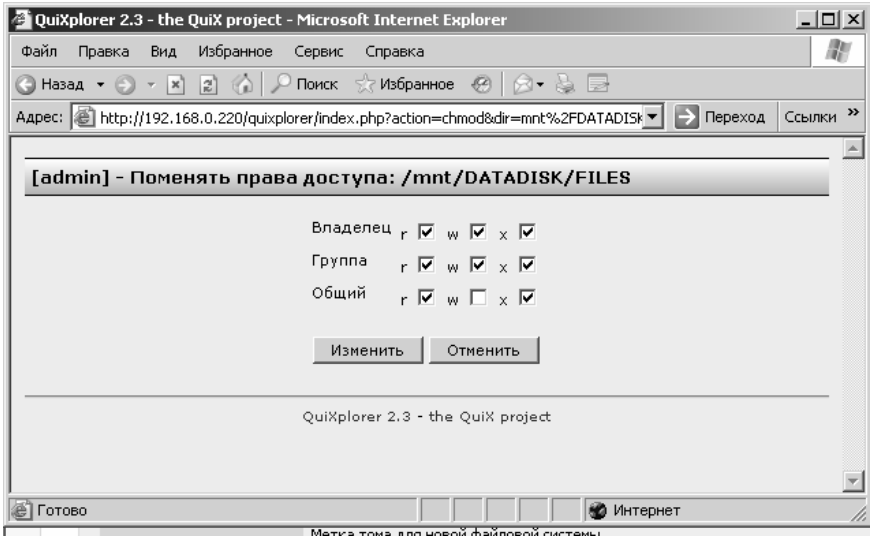

Рис. 24. Окно свойств каталога

Теперь каталог создан в файловой системе. Осталось предоставить доступ к этому каталогу из сети. Для этого зайдем в меню Службы-CIFS/SMB (рис. 25).

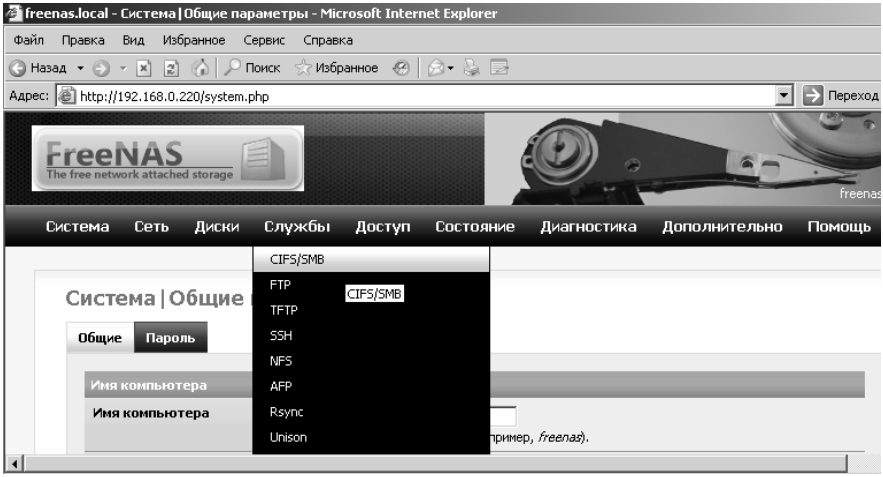

Рис. 25. Окно службы-CIFS/SMB

Выбираем вкладку «Общие ресурсы» и нажимаем «Добавить» («✚»), Вводим желаемое сетевое имя (оставим также FILES), комментарий и указываем путь к каталогу (рис. 26).

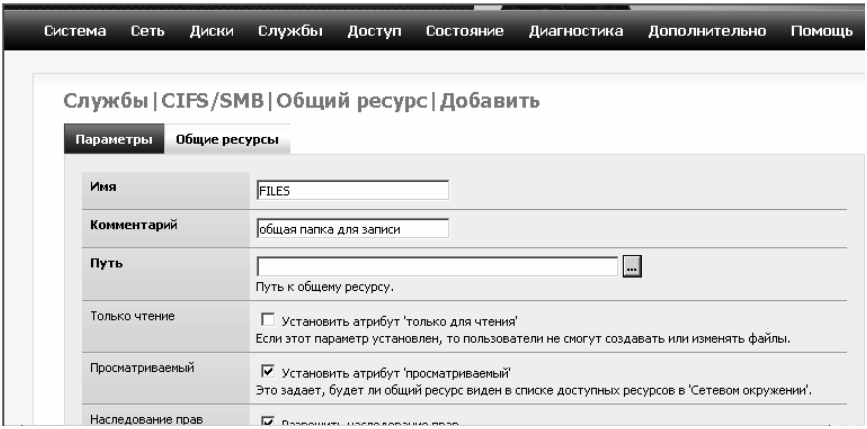

Рис. 26. Окно настройки общих ресурсов

Остальные параметры можно оставить без изменения. Нажимаем внизу кнопку «Добавить», а потом «Применить изменения». Все, каталог доступен из сети.

Также желательно внести изменение в параметр кодовой страницы для службы CIFS/SMB (рис. 27).

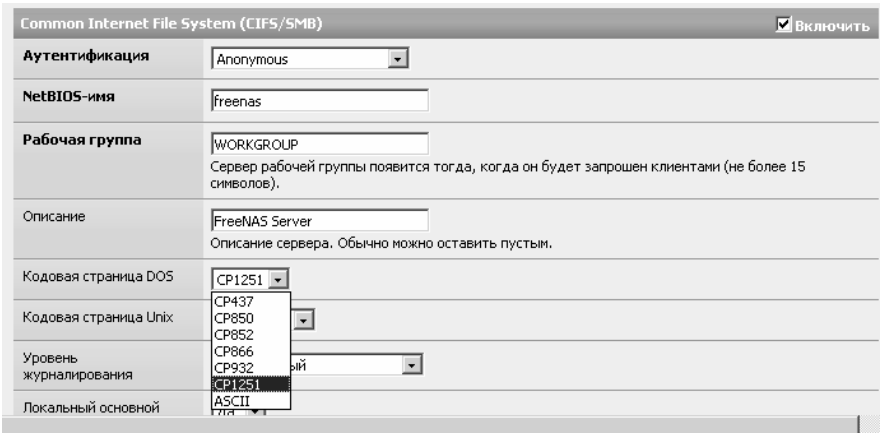

Рис. 27. Окно настройки кодовой страницы для службы CIFS/SMB

Затем внизу страницы нажать «Сохранить и перезапустить». Теперь не должно быть проблем с кодировками файлов в разных ОС.

Для доступа обычного пользователя к созданному каталогу необходимо в среде Windows выбрать соответствующий каталог (рис. 28).

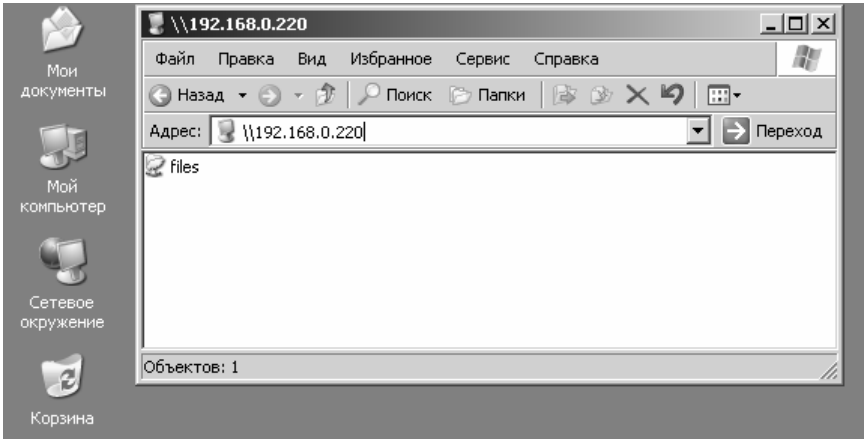

Рис. 28. Окно отображения созданного каталога FILES

Каталог доступен, и файловый сервер готов к работе.

В данной статье был описан механизм создания одной общей папки средствами дистрибутива FreeNAS, но на этом возможности использования данного продукта не исчерпываются. Так, например, можно решить проблему ограничения количества одновременных сетевых подключений в ОС семейства Windows. Файловый сервер FreeNAS позволяет создать любое количество пользователей с возможностью предоставления им персональных каталогов. Также предусмотрена возможность использования внешней авторизации, в том числе и механизмов LDAP и Microsoft Active Directory.

Минусом данного дистрибутива можно назвать невозможность средствами web-интерфейса устанавливать разрешения на доступ к файлам и каталогам средствами ACL (*Access Control List* – список контроля доступа). Можно решить данную проблему следующим образом: открыть один каталог на полный общий доступ, создать в нём подкаталоги и настроить на них права безопасности средствами, например, Windows. После этого в web-консоли FreeNAS доступ к первоначальному каталогу закрыть, а к созданным средствами Windows – предоставить. Таким образом можно получить каталоги со сложными правами безопасности (например, выставить группе учителей полный доступ, а ученикам – только чтение).

ПЕРСПЕКТИВЫ РАЗВИТИЯ ЛОКАЛЬНОЙ СЕТИ НА ОСНОВЕ «ТОНКИХ КЛИЕНТОВ»

В.Е. Ильин, старший методист ГОУ ДПО ЦПКС СПб «Региональный центр оценки качества образования и информационных технологий»

На сегодняшний день в образовательных учреждениях Санкт-Петер-бурга достаточно широко внедрены компьютеры в процессы управления и обучения. И всё чаще и острее встает вопрос о целесообразности затрат на закупку нового оборудования, сервисное сопровождение и ремонт имеющегося парка компьютеров, покупки лицензионного программного обеспечения.

Альтернативой существующего «покомпьютерного» подхода представляется использование терминальных систем – «тонких клиентов». Решения с использованием средств удалённого доступа к другому компьютеру, называемого также терминальным доступом, направлены на оптимизацию стоимости владения прикладным программным обеспечением, снижение стоимости эксплуатации как программных, так и аппаратных средств и на обеспечение безопасности данных.

Что такое «тонкий клиент»

Тонкий (терминальный) клиент в компьютерных технологиях – бездисковый компьютер-клиент в сетях с клиент-серверной или терминальной архитектурой, который переносит все или большую часть задач по обработке информации на терминальный сервер (рис. 1).

Рис. 1. «Тонкие клиенты»

Терминальный сервер, или сервер терминалов, – сервер, предоставляющий клиентам вычислительные ресурсы (процессорное время, память, дисковое пространство) для решения задач. Технически терминальный сервер представляет собой очень мощный компьютер (либо несколько компьютеров), соединенный по сети с терминальными клиентами, которые, как правило, представляют собой маломощные или устаревшие рабочие станции или специализированные решения для доступа к терминальному серверу. Терминальный сервер служит для удалённого обслуживания пользователей с предоставлением каждому собственного рабочего стола.

Сетевые технологии постоянно развиваются, и теперь можно не покупать для каждого пользователя персональный компьютер. Вам потребуется всего ОДИН компьютер - сервер и необходимое количество терминальных (тонких) клиентов (по количеству пользователей). Рабочее место пользователя представляется следующим составом оборудования: монитор. манипулятор мышь и «тонкий клиент».

Для соединения сервера и рабочих мест с применением «тонких клиентов» в локальную сеть используется обычный коммутатор (рис. 2).

Рис. 2. Структура компьютерного класса с использованием «тонких клиентов»

Какие **ПРЕИМУЩЕСТВА** могут получить школы от внедрения терминальных технологий и «тонких клиентов»?

Сокращение совокупной стоимости владения

По оценкам специалистов, стоимость рабочего места уменьшается за счет стоимости аппаратной части на 20%, за счет стоимости лицензий на пользовательское программное обеспечение – до 40% и за счет стоимости инсталляции – до 80%.

Уменьшается стоимость эксплуатации рабочего места (до 80%) за счет централизованного администрирования и радикального сокращения затрат рабочего времени на обслуживание рабочих мест пользователей, уменьшения затрат на обучение сотрудников – для сопровождения рабочих мест не потребуются высококвалифицированные специалисты.

Сокращение затрат на модернизацию

Отсутствует необходимость в модернизации компьютерной техники рабочих мест. При эксплуатации терминальных решений надо проводить регулярную модернизацию не всего компьютерного парка компании, а лишь только одного терминального сервера. А благодаря отсутствию движущихся частей и малой потребляемой мощности срок службы «тонкого клиента» (ТК) в разы превышает срок службы системного блока.

Рассмотрим пример стоимости вложений за 6 лет с периодом обновления вычислительной техники 3 года по двум вариантам:

- на приобретение 30 терминалов и двух терминальных серверов;
- на приобретение 30 персональных компьютеров (см. таблицу).

Наименование	Кол-во, шт.	Цена, руб.	Сумма, руб.	Итого, руб.
Начальные вложения				
Персональный компьютер АРМ на базе ПК (ПК + 17" ЖК-монитор)	 30	 15 000	 450 000	450 000
ТК «Тонкий клиент» Сервер АРМ на базе ТК (ТК + 17" ЖК-монитор)	 2 30	 50 000 8 000	 100 000 240 000	340 000
Вложения через 3 года				
Персональный компьютер	30	15 000	450 000	450 000
Сервер	2	50 000	100 000	100 000
Сумма вложений за 6 лет				
Персональный компьютер				900 000
«Тонкий клиент»				440 000

Статистика приведена без учета затрат на обслуживание ПК, простоя из-за его поломки и т.п., что еще больше увеличивает совокупную стоимость владения парком ПК по сравнению с ТК.

Экономия электроэнергии. Сокращение затрат на источники бесперебойного питания

Типовой тонкий клиент потребляет в среднем в 10 - 50 раз меньше электроэнергии, чем усредненный системный блок компьютера. Значит, можно использовать один источник бесперебойного питания (ИБП) на 10 и более терминальных рабочих мест.

Надежность

Большее время наработки на отказ. Отсутствие механических компонентов, а также сама по себе упрощенная архитектура повышают надежность системы в целом, что немаловажно, учитывая гораздо больший срок эксплуатации терминалов по сравнению с рабочими станциями.

Повышение безопасности обработки данных

«Тонкие клиенты» не имеют каких-либо устройств для хранения и записи информации пользователем. Благодаря тому, что абсолютно вся информация хранится на сервере и не передается по сети, снижается риск хищения данных и атаки вирусов. Для обеспечения повышенной безопасности можно воспользоваться дополнительными средствами, например устройством чтения смарт-карт, usb-ключом или биометрическим считывателем отпечатков пальцев, которые подключаются к терминалу и предоставляют более высокий и сложный уровень аутентификации пользователей.

Высокий уровень безопасности системы. Отсутствие дисков и дисководов существенно снижает риски утечки информации.

Данные по сети не передаются, так как на клиентские места передается только изображение экрана.

Централизованное хранение данных и настроек упрощает процедуры резервного копирования. Отпадает необходимость заботы о сохранности ценных данных и программ на рабочих станциях.

Быстрое развертывание

Просто включите терминал в розетку, и настройки будут автоматически загружены с сервера. Можно развертывать и администрировать все рабочие места пользователей и приложения с рабочего места администратора с помощью программного обеспечения для развертывания и управления, например компании Altiris.

Централизация администрирования

Упрощается администрирование и снижаются расходы на поддержание пользователей. Пользователи не могут повлиять на стабильность работы ПО на своем рабочем месте.

Администрирование терминальной системы полностью централизовано. Легче контролировать и управлять используемым программным обеспечением. В терминальной системе проще контролировать пользователей и ограничить использование нежелательных ресурсов.

Отсутствие в «тонких клиентах» обслуживаемого администратором программного или аппаратного обеспечения исключает необходимость его периодического обслуживания, диагностики и обновления. Нет необходимости в антивирусных программах на рабочих местах. Все прикладное программное обеспечение для пользователей размещено на сервере и контролируется системным администратором.

Сокращение требований к быстродействию локальной сети

При работе «тонких клиентов» с терминальным сервером приложения и данные не передаются по сети, а происходит передача данных (протокол RDP) о нажатии клавиш, движениях мыши и обновлениях дисплея, которая эффективно работает даже в устаревших сетях предыдущего поколения. Благодаря этому администраторы информационных систем могут обеспечить пользователям высокий уровень производительности как в проводных, так и в беспроводных сетях.

Снижается загрузка локальной сети, так как на терминал передаются только состояния экрана, в то время как на персональный компьютер могут передаваться значительные объемы данных, загружающие как сеть, так и компьютер. В случае нехватки вычислительных ресурсов достаточно провести модернизацию терминального сервера, а не всего парка персональных компьютеров.

Сокращается время выполнения многих программ, предъявляющих повышенные требования к полосе пропускания сети. Такими программами являются приложения, активно работающие с базами данных. При размещении программ на одной машине устраняется узкое место – пересылка данных по сети во время запроса клиентов к базе, и программы начинают выполняться намного быстрее.

Простота наращивания вычислительной мощности

Нет необходимости в обновлении терминала, так как он является лишь устройством ввода и отображения информации, ничего не обрабатывая сам. При нехватке вычислительных ресурсов достаточно провести обновление сервера (обычно это выгоднее, чем модернизировать несколько полноценных рабочих станций), причем новые ресурсы будут доступны сразу всем терминалам.

Масштабируемость

Чтобы добавить еще одно рабочее место, нет необходимости в установке и настройке целого компьютера, достаточно просто подключить еще один терминал.

Эргономичность

Бесшумная работа «тонких клиентов». Как правило, тонкие клиенты либо не имеют совсем, либо оснащены одним вентилятором. Их размеры обычно не превышают размеров большой книги, и они не занимают много места на столе.

Недостатки использования терминальных систем

• Терминалы не предназначены для выполнения задач, связанных со сложными вычислениями (например, программы обработки видео- и графической информации, системы моделирования) или генерирующих большой трафик для передачи в сторону клиента (например, просмотр видеофильмов). В первом случае это связано с большой загрузкой вычислительной мощности сервера (он сможет обслужить очень мало клиентов), во втором – с пропускной способностью сети. В этом случае целесообразнее использовать рабочие станции.

• Более низкая стоимость терминала компенсируется высокой ценой сервера. Ведь эта машина должна быть достаточно мощной, чтобы выполнять задачи многих «тонких клиентов», подключенных к ней. Справедливости ради отмечу, что зависимость мощности сервера от количества работающих «клиентов» нелинейна. Большинство типичных задач (например, несколько копий MS Office в памяти) используют библиотеки уже запущенной первой копии для своей работы, поэтому потребности в оперативной памяти будут относительно невысоки.

• В общем случае все работает на одном компьютере-сервере. Поэтому должны быть обеспечены все возможные меры для его безотказной работы и сохранности данных.

• Потребность в постоянном канале связи. В некоторых случаях для рабочей станции не обязательно наличие постоянного, а тем более быстрого канала связи. Терминалу же необходима постоянная связь с сервером. В среднем нужен канал с пропускной способностью не менее 20 Кбит/с.

Резюмируя, можно сказать, что преимущества «тонких клиентов» достаточно привлекательны для использования их во многих образовательных учреждениях, и в первую очередь для организации компьютерных классов. Надо лишь четко определить для себя плюсы и минусы терминального подхода и вариант его реализации.

ЛОКАЛЬНАЯ СЕТЬ ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ В ГЕТЕРОГЕННОЙ СРЕДЕ: ПРОЕКТИРОВАНИЕ, ОРГАНИЗАЦИЯ, РАЗВИТИЕ

Редактор – Уткина Л.В.
Компьютерная верстка – Маркова С.А.

Подписано в печать 18.10.2010. Формат 60x90 1/16
Гарнитура Times. Усл. печ. л. 4,4. Тираж 1000 экз. Зак. 32

Издано в ГОУ ДПО ЦПКС СПБ «Региональный центр оценки качества образования и информационных технологий»

190068, Санкт-Петербург, Вознесенский пр. д. 34, лит. А
Тел.+7 (812) 576-34-50, +7 (812) 576-34-81

Отпечатано в типографии Тиражи.RU
127055, Москва, Приютский пер., д. 3. Тел.: (495) 585-08-95