**Корпоративные информационные сети**

**1. Подготовка к проектированию сети**

**1.1 Общие сведения о предприятии**

Основными задачами ФСИН России являются:

1) исполнение в соответствии с законодательством Российской Федерации уголовных наказаний, содержание под стражей лиц, подозреваемых либо обвиняемых в совершении преступлений, и подсудимых (далее – лица, содержащиеся под стражей);

2) контроль за поведением условно осужденных и осужденных, которым судом предоставлена отсрочка отбывания наказания;

3) обеспечение охраны прав, свобод и законных интересов осужденных и лиц, содержащихся под стражей и т.д.

**1.2 Размещение производственных и административных зданий**

В данном проекте в качестве корпоративной сети будут использоваться вторые этажи двух зданий.

**1.3 Необходимость создания сети**

Необходимость сети обусловлена использованием информации разными отделами, быстрым обменом информацией между ними, хранением информации в одном месте. Реализация предложенного проекта позволит сократить бумажный документооборот внутри ФСИН, повысить производительность труда, сократить время на обработку информации с использованием специализированных приложений, хранящихся на сетевом сервере, и работать с общими устройствами: принтерами, факсами и другой периферией.

**1.4 Назначение использования сети**

Назначение сети состоит в облегчении и более эффективной работы сотрудников и передачи данных, управления учреждением и администрирования рабочих станций, подготовки основы единого информационного пространства.

**1.5 Характер выполняемых работ**

1С-бухгалтерия;

АКУС – для картотеки осужденных;

СЭДД – система электронного документооборота;

GOAL – видеонаблюдение;

К+ (КонсультанПлюс) – ведения бухгалтерского и / или оперативного учета.

**1.6 Требования и ограничения**

Основное требование, которое должно удовлетворяться при проектировании сети – это обеспечение доступа пользователей ко всем разделяемым ресурсам в пределах их прав. В целях информационной безопасности следует разграничить доступ пользователей на уровне отделов, так же в связи с родом деятельности а именно оказание услуг пользования компьютерами и доступа в Интернет, следует усилить меры безопасность по контролю несанкционированного доступа. Производительность, которая проявляется как: время реакции систем на введенный запрос, не должен превышать 1.5 сек.

**2. Анализ исходных данных**

**2.1 Масштаб проектируемой сети**

Данная проектируемая сеть является корпоративной кабельной системой.

**2.2 Варианты трафика**

Пульсирующий неравномерый трафик, который в основном используется для традиционной вычислительной сети, предназначенный для обеспечения совместного пользования сети.

**2.3 Оценка параметров и ограничений**

Требования к техническому обеспечению серверов

При документообороте от 300 до 1000 документов в день

Intel Core 2 Duo (1866/800/2048)/2x512 mb PC5300/FDD/200Gb SATA-II/SVGA 256mb GeForce7600/DVD

СУБД: MSSQL 2000 Enterprise Edition SP3 СКЗИ: Crypto Pro 2.0.2049a

Требования к техническому обеспечению рабочих станций

Pentium IV – 1,8 GHz, ОЗУ – 256Mb, HDD IDE – 40Gb

Операционная система Windows XP Pro, Windows 2000 Pro.

MS Office 2000 или выше

Рассмотрим время реакции на примере работы программы 1С Предприятия. Так как это программа использует трафик сети для работы с общими базами данных находящийся на сервере.

На предприятии имеется 35 компьютеров. В среднем каждый пользователь отправляет по 20 запросов.

Количество всех запросов: 35\*20=700

l1запр=315 байт+35 байт= 350 байт= 2800 бит

lзапр=2800\*700= 1960000

tзапр= 1960000\*10-8= 0,02с tобр≈0

l1 отв=1500 байт+ 35 = 1535 байт= 12280 бит

lотв = 12280\*700= 8596000 бит

tотв= 8596000\*10-8= 0,09с

tреак= tзапр+tобр+tотв

tреак=0,02+ 0,09= 0,11с

**3. Сетезависимая часть**

**3.1 Выбор основных сетевых технологий**

Для данного проекта выбрана технология Fast Ethernet, так как она позволяет обеспечить более быструю передачу данных (100 Мб/с). Для передачи данных использовано два типа кабелей: неэкранированная витая пара категории 5 – для передачи данных по сети внутри здания и оптоволоконный – для прокладывания сети между зданиями. Между зданиями необходимо использовать оптоволоконный кабель так как он более устойчив к внешним условиям, а так же он более помехоустойчив.

**3.2 Коммуникационные функции**

В качестве коммуникационного оборудования используется коммутатор с большим количеством портов и поддерживающий технологию Fast Ethernet.

**3.3 Архитектура сети**

Основными элементами сети являются рабочие станции, серверы и коммутаторы.

Основную часть сети составляют рабочие станции, которые подключены к коммутаторам. Коммутаторы пересылают пакеты данных из одного порта в другой по нужному адресу. Также в сети имеются серверы, обеспечивающие работу рабочих станций в составе сети.

Топология сети – иерархическая древовидная структура. Основным преимуществом такого типа топологии является относительная простота модификации.

**3.4 Размещение оборудования**

Размещение оборудования показано в приложении 1.

**3.5 Качество обслуживания**

Качество обслуживания в сети не задается, так как используется технология Fast Ethernet, не являющаяся технологией реального времени.

**4. Кабельная система сети**

В данном проекте используется 2 типа кабелей. Первый тип – неэкранированная витая пара категории 5 для проложения сети внутри здания и второй тип – оптоволоконный кабель для проведения между зданиями.

Неэкранированная витая пара. Наиболее дешевым и, пожалуй, самым распространенным на сегодняшний день кабельным соединением является неэкранированная витая пара (UTP, Unshielded Twisted Pair).Такой кабель состоит из двух или четырех пар одножильных изолированных проводов, заключенных в оболочку из гибкого пластика. Провода каждой пары свиты между собой для повышения помехоустойчивости. Для соединения применяется разъем RJ-45. Надежный контакт достигается за счет того, что позолоченные контактные пластины врезаются в медные жилы проводов. Так как тип разъема во всех сетях, использующих кабель с витой парой, одинаков, то при замене оборудования проводить трудоемкую замену кабельной системы не понадобиться. Преимуществами являются низкая цена и безпроблемная установка.

Оптоволоконный кабель. Это наиболее качественный тип кабеля – он обеспечивает передачу данных с очень большой скоростью и к тому же лучше других типов передающей среды обеспечивает защиту данных от внешних помех [В.Г. Олифер, Н.А. Олифер, Компьютерные сети, 3-е издание].

Наиболее оптимальным архитектурным решением для проектируемой сети является сосредоточенная сетевая магистраль (рис. 1)

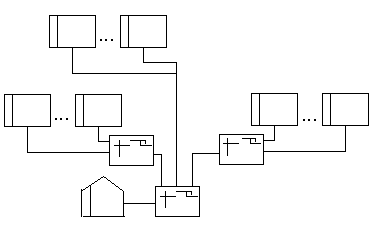


Рис. 1

**5. Система энергообеспечения и температурный режим в помещениях**

Компьютерное и коммуникационное оборудование выделяет большое количество тепла, что способствует повышению температуры в помещении на несколько градусов. Для сохранения нормального температурного режима в помещении следует оценить эффективность работы блоков питания.

Энергетический бюджет (совокупная мощность потребляемой энергии) может оказаться очень существенным. Потребляемую оборудованием величину тока I можно определить из следующего выражения:

W = I? U,

где W – потребляемая мощность, U – величина напряжения.

Расчет энергетического бюджета для данной проектируемой сети:

Общая потребляемая мощность различными устройствами W приблизительно равна 350 Вт.

Наибольшее количество компьютеров в одном кабинете составляет 8 шт.

I = =10.9 (А)



В здании имеется стандартная проводка, которая может обеспечить 20А, следовательно необходимости в модернизации существующей проводки нет.

Компьютерное и коммуникационное оборудование, размещенное в помещении, выделяет большое количество тепла, что способствует повышению температуры на несколько градусов. Так как в кабинетах помещения уже установлены кондиционеры, то необходимости в установке кондиционеров нет.

**6. Сетенезависимая часть сети и транспортный уровень**

**6.1 Структура служб сети**

В проектируемой сети выделяются следующие службы сети:

Active Directory – служба каталога обеспечивающее хранение и представление пользователям и программам информации о различных объектах, их свойствах и взаимосвязях.

DNS (Domain Name System) – представляет собой распределенное пространство имен, используемое в глобальной сети для разрешение имен компьютеров и служб в адреса TCP/IP.

IIS (Internet Information Server) – это собственнический набор серверов для нескольких служб Интернета от компании Майкрософт.

**6.2 План IP-адресации**

В сети используется внутренняя IP-адресация, которая приводится в следующей таблице

|  |  |  |
| --- | --- | --- |
| Номер здания | специализация | IP-адреса |
| 1 | бухгалтерия | 192.168.0.1 – 192.168.0.13 |
| 1 | спец. отдел | 192.168.0.14–192.168.0.19 |
| 1 |  | 192.168.0.20 – сервер |
| 1 | соц. отдел | 192.168.0.21 – 192.168.0.23 |
| 1 | отдел кадров | 192.168.0.24 – 192.168.0.28 |
| 1 |  | 192.168.0.24 – 192.168.0.28 |
| 2 | бухгалтерия | 192.168.0.29–192.168.0.34 |
| 2 | экон. отдел | 192.168.0.35 – 192.168.0.38 |

**6.3 Сетевые службы**

Используется служба каталога Active Directory 2003. Active Directory(AD) имеет иерархическую структуру, состоящую из объектов. Объекты разделяются на три основные категории: ресурсы (например принтеры), службы (например, электронная почта) и люди (учетные записи пользователей и групп пользователей). Active Directory предоставляет информацию об объектах, позволяет организовывать объекты, управлять доступом к ним, а так же устанавливает правила безопасности.

Каталог содержит объекты, являющиеся стандартными. Стандартными контейнерными объектами, которые входят в каталог, являются такие, как:

– Namespace – пространство имен,

– Country – страна,

– Locality – район,

– Organization – организация,

– Organization Unit – организационная единица,

– Domain – домен,

– Computer – компьютер.

Стандартными листьями, входящими в каталог, являются следующие объекты:

– User – пользователь,

– Group – группа,

– Alias – псевдоним,

– Service – служба,

– Print Queue – запрос печати,

– Print Device – устройство печати,

– Print Job – задача печати,

– File Service – файловая служба,

– File Share – совместный доступ к файлу,

– Session – Сеанс,

– Resource – ресурс.

При необходимости включения в схему объектов других типов, схему можно изменить с помощью программы Active Directory Schema Manager.

В проекте используется один лес и один домен. Развертывание единственного леса означает, что будет возможно простое совместное использование ресурсов и доступ к информации.

При управлении только одним доменом необходим только один набор администраторов доменного уровня и один набор политик домена. Управлять необходимо только одним набором контроллеров домена. При единственном домене проще осуществлять планирование аутентификации и доступа к ресурсам.

Проектируемая сеть содержит две организационные единицы высшего уровня (здание 1 и здание 2).

Нижние уровни организационных единиц следующие:

– OU учетных записей – содержит учетные записи пользователей и групп отдела.

– OU компьютеров – содержит все компьютеры.

– OU ресурсов – содержит ресурсы, связанные с данной OU. Включает совместно используемые данные, папки.

Задачи управления администратора состоят в следующем:

– создание политик безопасности уровня домена,

– проектирование конфигурации «Групповая политика» уровня домена,

– создание в домене структуры организационной единицы,

– делегирование административных прав в пределах домена,

– управление административными группами уровня домена.

**6.4 Серверы сети**

В сети используется один сервер.

Intel Core 2 Duo (1866/800/2048)/2x512 mb PC5300/FDD/200Gb SATA-II/SVGA 256mb GeForce7600/DVD

**6.5 Используемые протоколы**

В проектируемой сети использован протокол TCP/IP.

TCP (IP идентификатор) – «гарантированный» транспортный механизм с предварительным установлением соединения, предоставляющий приложению надёжный поток данных, дающий уверенность в безошибочности получаемых данных, перезапрашивающий данные в случае потери и устраняющий дублирование данных. TCP позволяет регулировать нагрузку на сеть, а также уменьшать время ожидания данных при передаче на большие расстояния. Более того, TCP гарантирует, что полученные данные были отправлены точно в такой же последовательности.

**6.6 Система управления коммуникационным оборудованием**

В качестве коммуникационного оборудования в проекте использовался неуправляемый тип коммутаторов.

**7. Решения по защите информации, бесперебойному питанию, резервному копированию и антивирусной защите**

Следует предусмотреть непрерывную инвентаризацию оборудования администраторами сетевого оборудования. Данные по инвентаризации должны храниться должны храниться в электронном виде в заданном формате в файле на рабочем месте администраторов. Следует предусмотреть процедуру подключения пользователей. Администраторы сетевого оборудования осуществляют регистрацию подключаемого пользователя в журнале коммутации, который хранится в электронном виде у администратора сетевого оборудования. Данная информация включает в себя номер порта коммутатора и аппаратный адрес сетевой платы станции. Сетевое оборудование должно размещаться в специальных шкафах, закрываемых на ключ. Ключи должны храниться у администраторов сетевого оборудования. Помещения, в которых будет установлено сетевое оборудование, возможно, необходимо будет оборудовать системами кондиционирования, резервного электропитания, пожарной сигнализации и пожаротушения.

Технические меры по защите информации, могут включать:

– управление доступом к консолям управления сетевыми устройствами;

– регистрацию действий администраторов и событий, возникающих при работе сетевого оборудования;

– обеспечение целостности служебной информации сетевого оборудования

Источники бесперебойного питания.

Описание технических средств. Технические средства ИПБ могут использоваться для электропитания серверов, ленточных библиотек и активного сетевого оборудования. Питание может обеспечиваться этажными централизованными или раздельно расположенными ИПБ. Нагрузка на ИПБ не должна превышать возможную мощность.

Описание программных средств. Управление может производиться с рабочих станций специалистов отдела, ответственного за эксплуатацию ИПБ, через WEB-интерфейс. При возникновении критического события по электронной почте специалистам отдела отправляется уведомление о произошедшем событии.

Антивирусная защита. Для защиты от вирусов предлагается использовать программу Антивирус Касперского. Эта антивирусная программа имеет оптимальное сочетание качества защиты системы и требований к ресурсам системы. Антивирус Касперского является достаточно надежным средством защиты компьютеров от воздействия вирусов и сетевых атак. Антивирусное программное обеспечение централизованно управляется с рабочего места администраторами службы технического обеспечения.

Резервное копирование. В качестве оборудования резервного копирования предлагается использовать оборудование фирмы Hewlett Packard семейства HP StorageWorks.

Ленточные накопители HP известны своими прекрасными рабочими качествами, отказоустойчивостью, распространенностью и постоянной поддержкой со стороны производителя. [Ф.И. Эминов, Проектирование корпоративных информационных сетей]

**8. Ведомость оборудования и материалов**

Требования к техническому обеспечению серверов

При документообороте от 300 до 1000 документов в день

Процессор Intel Core 2 Duo (1866/800/2048)/2x512 Мб

Операционная система MS Windows Server2003 Enterprise Edition

СУБД: MSSQL 2000 Enterprise Edition SP3 СКЗИ: Crypto Pro 2.0.2049a

Требования к техническому обеспечению рабочих станций

Pentium IV – 1,8 GHz, ОЗУ – 256Mb, HDD IDE – 40Gb

Операционная система Windows XP Pro, Windows 2000 Pro.

MS Office 2000 или выше

Коммутатор D-link DES-1016D (switch), 16 портов Ethernet 10/100/1000 Мбит/сек, монтируется в стойку

**9. Программы и процедуры, а также параметры настроек**

Используется служба каталогов Active Directory, которая включает в себя программы и интерфейсы прикладного программирования:

– Active Directory Service Interfaces (ADSI);

– антивирусная программа Kaspersky Internet Security 2009

– 1C Бухгалтерия;

– АКУС;

– СЭДД;

**10. Оценка работоспособности сети**

Работоспособность сети проверяется на практике в процессе тестирования сети. Уровень производительности станций полностью справляется с поставленными задача. Время реакции сети вполне удовлетворяет потребностям пользователей, так как была поставлена задача чтобы это время не превышало 1.5 секунды. После расчетов времени реакции, получилось время равное 0.11 секунд. Эта величина входит в поставленные ограничения.

Помехоустойчивость сети при передачи данных на высоком уровне. Этому результату способствовала правильная проводка кабелей и соблюдение правил стандартизаций.

Защищенность сети поддерживается программными средствами защиты. Также защищенность сети повышает выполняемые организационные и технические меры.

Сеть имеет возможность расширения. Имеющим коммутаторам можно присоединит новые вычислительные машины.

**11. Документы по комплектации сети и расчет затрат**

Расчет затрат на оборудование и кабельную систему

|  |  |  |  |
| --- | --- | --- | --- |
| Наименование | Кол-во | Стоимость | Сумма |
| Кабель неэкранированная витая пара | 4.5 | 450 | 2025 |
| Kramer C-FOHM/FOHM-164 оптоволоконный кабель HDMI 50 м  26 286 р. | 300 м | 525.72 | 157716 |
| Процессор Intel Pentium 4 | 35 | 2900 | 101500 |
| Процессор Intel Core 2 Duo (1866/800/2048)/2x512 mb PC5300/FDD/200Gb SATA-II/SVGA 256mb GeForce7600/DVD/ Lan | 1 | 19200 | 19200 |
| Монитор Acer X223W | 1 | 6010 | 6010 |
| Монитор Samsung SyncMaster 923NW | 35 | 3997 | 139895 |
| коммутатор D-link DES-1016D | 3 | 1 218 | 3654 |
| ИБП  APC Smart-UPS RM 2U | 1 | 12000 | 12000 |
| **Итого:** | | | 442000 |

**12. Документы для реализации сети**

План перехода к работе в составе сети:

1. Проверка проектной документации и выявление ошибок.

2. Корректировка проектной документации

3. Разработка инструкций для эксплуатационного персонала

4. Определение групп и лиц, которые будут выполнять запланированные работы

5. Назначение работ

6. прокладка кабельной системы

7. Монтаж оборудования

8. Проверка вычислительной сети на работоспособность

9. Тестирование вычислительной сети на отказоустойчивость

10. Сдача вычислительной сети в эксплуатацию

**Заключение**

Данная сеть спроектирована для ФСИН и должна обладать наиболее высоким уровнем защиты информации. Для обеспечения этого аспекта сеть поделена на несколько лесов для того чтобы конфиденциальная информация не могла быть доступна всем отделам. Помимо требования о высоком уровне защиты информации необходимо чтобы сеть была экономически выгодна, поэтому был выбран не самый дорогой тип кабеля – неэкранированная витая пара категории 5, оптоволоконный проложен лишь для связи зданий. Проект данной сети может быть модернизирован в дальнейшем без излишних затрат.

**Список литературы**

1. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. – СПб: Питер, 2006.
2. Эминов Ф.И. Сетевые технологии. Часть 1.: Учебное пособие. – Казань: Издательство «ДАС», 2002.
3. Эминов Ф.И. Сетевые технологии. Часть 2.: Учебное пособие. – Казань: ЗАО «Новое знание», 2006.
4. Эминов Б.Ф., Эминов Ф.И. Безопасное управление ресурсами и пользователями в корпоративных информационных сетях: Учебное пособие. – Казань: ЗАО «Новое знание», 2006.