Федеральное агентство по образованию Российской Федерации

Пензенский государственный университет

Кафедра «Информационная безопасность систем и технологий»

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

к курсовому проектированию по теме

“Проектирование локальной сети организации”

ПГУ 2.090105.001 ПЗ

Дисциплина СиСПИ

Группа

Разработал студент .

Проект принят с оценкой\_\_\_\_\_\_\_\_\_\_

Руководитель проекта .

Пенза 2006 г.

Реферат

Пояснительная записка: 28 с., 2 источника, 4 рис., 3 табл.

ЛОКАЛЬНАЯ СЕТЬ, ВИТАЯ ПАРА, 100BASE-TX, СЕРВЕР, ИНФОЛОГИЧЕСКАЯ МОДЕЛЬ, ПОЛЬЗОВАТЕЛЬ, МАРШРУТИЗАТОР

Объектом исследования является предприятие по разработке программного обеспечения.

Целью курсового проектирования является разработка проекта сети на предприятии по разработке программного обеспечения.

В процессе работы был разработан проект сети предприятия, были описаны все составляющие сети и была проведена стоимостная оценка сети.

В результате проделанного курсового проекта были получены навыки по проектированию сети организации.

Содержание

Введение

1. Определение объекта исследования

1.1 Цели использования сети

1.2 Характеристики сети

2. Определение размеров и структуры сети

3. Выбор сетевого оборудования

4. Выбор сетевого программного обеспечения

4.1 Выбор сетевой операционной системы

4.2 Формирование маршрутной таблицы

5 Обеспечение информационной безопасности в сети

6 Стоимостная оценка

Заключение

Список использованных источников

Введение

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

Назначение всех компьютерных сетей можно выразить двумя словами: совместный доступ (или совместное использование). Прежде всего имеется в виду совместный доступ к данным. Людям, работающим над одним проектом, приходится постоянно использовать данные, создаваемые коллегами. Благодаря локальной сети разные люди могут работать над одним проектом не по очереди, а одновременно.

Локальная сеть предоставляет возможность совместного использования оборудования. 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. Оборудование, программы и данные объединяют одним термином: ресурсы. Можно считать, что основное назначение локальной сети – доступ к ресурсам. У локальной сети есть также и административная функция. Контролировать ход работ над проектами в сети проще, чем иметь дело со множеством автономных компьютеров.

В ходе выполнения курсового проекта была разработана модель локальной сети организации, занимающейся разработкой программного обеспечения.

1. Определение объекта исследования

Объектом проектирования является локальная телекоммуникационная сеть организации. Данная сеть должна обеспечивать транспортировку информации в рамках организации и обеспечивать возможность взаимодействия с глобальной сетью Internet. Организация, для которой проектируется локальная сеть, является фирмой, основным видом деятельности которой является разработка программного обеспечения.

1.1 Цели использования сети

Для точной формулировки целей проектирования сети необходимо составить инфологическую модель организации, в которой выявляются потоки информации, циркулирующие внутри организации, каналы по которым данная информация перемещается, степень критичности и чувствительности информации.

Инфологическая модель определяет виды информации, которые находятся в определенных узлах сети, разделяет ее по степеням критичности и чувствительности. На приведенном рисунке используются следующие обозначения, для определения вида и качества информации:

информация о финансовой деятельности

информация о коньюктуре рынка

информация о продукции

информация о материально-техническом обеспечении

информация о требуемом виде продукции

эталоны программ.

Высокая чувствительность

Чувствительная информация

Внутренняя

Открытая

α.Существенная

β.Важная

γ. Нормальная

Инфологическая модель была построена исходя из бизнес-целей организации и бизнес-функция, их реализующих.

|  |  |
| --- | --- |
| Бизнес-цель | Бизнес-функции |
| Финансовая деятельность (получение прибыли) | Регистрация. Ведение финансовой отчетностиОтслеживание конъюнктуры рынка.Продажа товара |
| Разработка ПО | Материально-техническое обеспечение. Программно-технические средства.Лицензирование и сертификация. |

Таблица 1. Бизнес-цели и бизнес-функции организации.

Таким образом, исходя из инфологической модели организации, можно выделить следующие цели проектирования сети:

обеспечение доступности информации.

централизованное хранение информации в базах данных

архивирование и резервное копирование информации

обеспечение информационной безопасности в рамках ТКС организации

взаимодействие локальной сети организации с глобальной сетью Internet.

1.2 Характеристики сети

Для достижения поставленных целей сеть должна иметь следующие характеристики:

Наличие доступа в Internet.

Высокая пропускная способность (100 – 1000 Мбит/с)

Высокая производительность сервера.

Средняя производительность АРМ отдела разработки и тестирования.

Высокая отказоустойчивость всех компонентов сети.

Возможность расширения.

2. Определение размеров и структуры сети

В соответствии с разработанной инфологической моделью организации, очевидно, что проектируемая сеть имеет малый размер, так как охватывает площадь, ограниченную одним этажом здания. При проектировании структуры сети необходимо учитывать возможность ее расширения. Анализ возможностей роста организации дает возможность предположить, что данная сеть может быть увеличена за счет добавления нового сегмента, располагающегося на другом этаже.

Сеть организована с использованием топологии «Звезда» (рис 2). При топологии "звезда" все компьютеры с помощью сегментов кабеля подключаются к центральному компоненту, именуемому концентратором (hub). Сигналы от передающего компьютера поступают через концентратор ко всем остальным. Рабочая станция, которой нужно послать данные, отсылает их на концентратор, а тот определяет адресата и отдаёт ему информацию. В определённый момент времени только одна машина в сети может пересылать данные, если на концентратор одновременно приходят два пакета, обе посылки оказываются не принятыми и отправителям нужно будет подождать случайный промежуток времени, чтобы возобновить передачу данных.

Достоинства

Выход из строя одной рабочей станции не отражается на работе всей сети в целом;

Хорошая масштабируемость сети;

Лёгкий поиск неисправностей и обрывов в сети;

Высокая производительность сети

Гибкие возможности администрирования

Недостатки

Выход из строя центрального концентратора обернётся неработоспособностью сети в целом;

Для прокладки сети зачастую требуется больше кабеля, чем для большинства других топологий;

Конечное число рабочих станций, т.е. число рабочих станций ограничено количеством портов в центральном концентраторе;

Рис 2. Топология «Звезда»

Структура сети определяется физической моделью, которая основывается на физической планировке помещений, охваченных сетью. Физическая модель локальной сети организации представлена на рисунке 3.

Рис. 3. Физическая модель локальной сети.

Вся сеть организации разделяется на три подсети. Каждая подсеть в свою очередь может состоять из нескольких сегментов. Первая подсеть сети – это группа разработчиков. Она состоит из 20 рабочих станций и сервера рабочей группы. Все хосты этой подсети объединены коммутатором, который соединен с маршрутизатором сети. Вторая подсеть – это группа тестирования. Структура этой подсети аналогична предыдущей. Третья подсеть включает в себя АРМ руководства, администраторов, сервер.

Такая структура сети легко может быть расширена. Для этого достаточно подключить новую подсеть к маршрутизатору и настроить сетевые адреса для нее.

После разработки структуры сети необходимо выбрать тип кабельной системы, используемой в сети.

Сеть строится на основе стандарта 100BASE-TX. Стандарт 100BASE-TX определяет сегмент Ethernet на основе неэкранированных витых пар (UTP) категории 3 и выше с топологией пассивная звезда (Twisted-Pair Ethernet). Данный тип сегмента Ethernet имеет все преимущества и недостатки пассивной звезды. Суммарное количество кабеля, необходимого для объединения такого же количества компьютеров, оказывается гораздо больше, чем в случае шины. С другой стороны, обрыв кабеля не приводит к отказу всей сети, монтаж, а также диагностика неисправности сети проще. В сегменте 100BASE-TX передача сигналов осуществляется по двум витым парам проводов, каждая из которых передает только в одну сторону (одна пара – передающая, другая – принимающая). Кабелем, содержащим такие двойные витые пары, каждый из абонентов сети присоединяется к концентратору (хабу). Концентратор производит смешение сигналов от абонентов для реализации метода доступа CSMA/CD, то есть в данном случае реализуется топология пассивная звезда.

Так как характеристики сети удовлетворяют требованиям для использования витой пары в качестве сетевой среды, то выбрана был кабель UTP категории 5Е 24AWG. Кабели имеют стандартные разъемы RJ-45.

3. Выбор сетевого оборудования

Одной из наиболее ответственных задач при проектировании сети является выбор сетевого оборудования, так как при этом необходимо обеспечить необходимые характеристики сети и избежать лишних материальных затрат. Перечень используемого оборудования приведен в приложении А.

Самым дорогим компонентом сети является сервер. Сервер должен выполнять несколько функций.

Обеспечивать резервное копирование данных.

Поддерживать СУБД для хранения эталонов программ

Обработка действий с файлами, находящимися на его носителях.

Выполнять функцию маршрутизации данных в сети.

Так же в сети используется proxy-сервер, для выхода в internet. Данный сервер имеет реальный ip-адрес, который используется хостами сети для выхода в глобальную сеть. Функции, выполняемые данным сервером, сводятся к обработке электронной почты, подмене локальных адресов хостов реальным ip-адресом. Вследствие этого, он не отличается высокой производительностью и по своей архитектуре близок к стандартному АРМ. Данный сервер введен в сеть исходя из целей безопасности. Если ограничиться лишь одним сервером, и возложить на него помимо вышеописанных функций еще и функции по взаимодействию с глобальной сетью, то он станет уязвим к внешним атакам, так как содержит всю важнейшую информацию организации и является одной из основных целей атак злоумышленников.

Исходя из вышеописанных функций сервера, была подобрана следующая конфигурация:

Hyperion RS110



|  |  |
| --- | --- |
| Платформа:  | ETegro Hyperion RS110 |
| Процессор:  | AMD Opteron 165 1.8G dual core |
| Оперативная память:  | 2 x DDR 1Gb PC3200 ECC + Registered |
| Жесткие диски:  | 1 x HDD 500 GB SATA 7200 rpm, 16MB |
| Операционная система:  | Microsoft Windows Server 2003 R2 Standard Edition RUS 5 CL |
| Расширенная гарантия:  | ETcare 3 years Classic |

Вторым по стоимости компонентом проектируемой сети являются рабочие станции сотрудников организации. Так как, фирма разрабатывает программное обеспечение, то производительность АРМ должна быть достаточно высокой. Как отмечалось выше, сервер, через который происходит взаимодействие локальной сети с сетью Internet, по архитектуре аналогичен с рабочими станциями сотрудников. Исходя из данных соображений, были выбраны следующие компоненты, для АРМ:

AMD Athlon™ 64 3200+ Socket-939

Socket-939: nVidia nForce-4 Ultra

2 x DIMM 512MB DDR SDRAM PC3200

FDD 3.5"

Card Reader all-in-1

SATA 80.0GB 7200rpm 8MB

DVD+-R/RW&CD-RW IDE

256Mb PCI-E GeForce 7300GT

Корпус AOpen QF50C

После выбора составляющих хостов сети необходимо выбрать непосредственно сетевое оборудование.

В проектируемой сети используется кабель типа UTP категории 5e, он имеет следующие характеристики.

Кабель UTP cat.5e 4 пары (305 м) NEOMAX Taiwan [NM10001]. Неэкранированная витая пара (спецификация 10Base-T, 100Base-TX) широко используется в ЛВС. Максимальная длинна сегмента составляет 100м. (328ф.) Неэкранированная витая пара состоит из двух изолированных медных проводов. Существует несколько спецификаций, которые регулируют количество витков на единицу длины - в зависимости от назначения кабеля. Тип оболочки: стандартная (ПВХ) Наружный диаметр оболочки: 5 мм Назначение: Кабель предназначен для использования в компьютерных сетях, в горизонтальной подсистеме структурированных кабельный систем. Совместимость: RJ-45 Ключевые особенности: категория 5е, частота работы: до 125 МГц, сопротивление: 89 Ом Диапазон температур монтажа: 5...+40 Диапазон рабочих температур: -15...+70 Вес кабеля: 40 кг/км

Сетевой адаптер.

ZyXEL OMNI FN312 RTL. Полное описание: Сетевая карта от ZyXEL. Карта с поддержкой стандартов IEEE802.3/IEEE802.3u . Карта может работать с полным дуплексом, поддержка витой пары категории 3, 4, 5. Поддерживается функция Wake-On-Lan Модель: ZyXEL FN312 Интерфейс подключения к компьютеру: PCI. Среда передачи: Медная пара. Разъемы: 1 RJ-45. Поддерживаемые скорости: 10\100 Мб\с. Поддержка полнодуплексного режима: Есть Поддерживаемые ОС: Microsoft Windows 98/2000/ME/XP Microsoft Windows NT 4.0 Microsoft Windows Workgroup 3.11 Novell NetWare 5.x/4.x Novell NetWare client 32 Linux Redhat 6.x, 7.x

Коммутатор

Коммутатор (управляемый) D-Link DES-3226S 24-ports 10/100 Mbps DES-3226S - это высокопроизводительный управляемый коммутатор уровня 2, представляющий собой идеальное решение для небольших рабочих групп. Коммутатор имеет 24 порта 10/100Мбит/с Fast Ethernet и дополнительно может быть укомплектован модулями 100BaseFX или Gigabit Ethernet, необходимыми для подключения высокоскоростного оборудования и обеспечивающими дополнительную гибкость коммутатору. DES-3226S имеет 24 порта 10/100 Мбит/с, поддерживающие автоопределение скорости и режима передачи данных. Дополнительные модули с 2-мя оптическими портами Fast Ethernet, а также оптическими или медными портами Gigabit Ethernet устанавливается в свободный слот, находящийся на передней панели коммутатора. Высокопроизводительные модули применяются для подключения коммутатора к серверам или магистрали предприятия. Архитектура DES-3226S обеспечивает неблокирующую коммутацию потока данных с режимом коммутации store-and-forward. Размеры и питание Питание - 100-240VAC, 50/60Hz Потребляемая мощность - 30-42 Watts (max.) Габаритные размеры - 441 x 388 x 66 mm 19" - для установки в шкаф, 1.5U высота, вес 6 kg

Принтер

Принтер HP LaserJet 1018, лазерный, черно-белый, A4, 600 x 600 dpi, 12 стр/мин, 2 МБ, USB 2.0

Производитель HP. Модель LaserJet 1018. Тип устройства черно-белый лазерный принтер. Тип печати лазерная печать. Формат (макс.) A4. Скорость печати (макс.) 12 стр/мин. Ёмкость 150 листов. Выход первой страницы 10 сек. Ежемесячная нагрузка до 3000 страниц. Дополнительные характеристики. Процессор RISC • 234 МГц. Оперативная память 2 МБ. Разрешение 600 x 600 dpi Скорость 12 стр/мин. Поддерживаемые материалы бумага: A4, A5, A6 почтовые открытки конверты. Системные требования (мин.) MS Windows 98SE/ME/2000/XP • Intel Pentium 90 МГц • HDD 120 МБ Тип подключения USB Интерфейсы USB 2.0. (4530 р.)

Источник бесперебойного питания Ippon BACK COMFO PRO 800 black.

Back Comfo Pro - новый, очень удобный источник бесперебойного питания для домашних и корпоративных пользователей. Есть модели мощностью 400, 600 и 800 VA. Для удобства пользователей Back Comfo Pro имеет 2 дополнительные евроразетки. Кроме того, для подключения к компьютеру имеется как стандартный, так и USB-порт. Вместе с UPS поставляется русифицированое програмное обеспечение WinPower2003, которое позволяет эффективно контролировать все параметры работы источников бесперебойного питания. Поддерживаемая мощность: 800 VA (480 Вт). Описание модели: Back Comfo Pro 800. Выходной сигнал: аппроксимированная синусоида. Время перехода на батарею: 2-6 мс. Общее количество выходных розеток: 4 компьютерные розетки, 2 бытовые евророзетки. Пороги перехода на батареи: 220 Вт +20% и -30%. Частота: 50 Гц (автоматическое определение). Коммуникационный интерфейс: RS-232/USB Защита линий передачи: Да. Время подзарядки батарей: до 90% за 8 часов после полной разрядки. Спецификация заменяемых батарей: Герметичная свинцовая батарея из 6 элементов. Время работы в резервном режиме: от 5 до 30 мин. Программное обеспечение: Полностью русифицированное программное обеспечение WinPower2003. Поддерживает Windows 95/98/NT/2000/XP, Novell и Linux. Размеры и вес: 300 x 124 x 210 мм. Вес: 7 кг.

4. Выбор сетевого программного обеспечения

4.1 Выбор сетевой операционной системы

Большое разнообразие типов компьютеров, используемых в вычислительных сетях, влечет за собой разнообразие операционных систем: для рабочих станций, для серверов сетей уровня отдела и серверов уровня предприятия в целом. К ним могут предъявляться различные требования по производительности и функциональным возможностям, желательно, чтобы они обладали свойством совместимости, которое позволило бы обеспечить совместную работу различных ОС.

Сетевые ОС могут быть разделены на две группы: масштаба отдела и масштаба предприятия. ОС для отделов или рабочих групп обеспечивают набор сетевых сервисов, включая разделение файлов, приложений и принтеров. Они также должны обеспечивать свойства отказоустойчивости, например, работать с RAID-массивами, поддерживать кластерные архитектуры.

Сетевая операционная система масштаба предприятия прежде всего должна обладать основными свойствами любых корпоративных продуктов, в том числе:

масштабируемостью, то есть способностью одинаково хорошо работать в широком диапазоне различных количественных характеристик сети,

совместимостью с другими продуктами, то есть способностью работать в сложной гетерогенной среде интерсети в режиме plug-and-play.

Корпоративная сетевая ОС должна поддерживать более сложные сервисы. Подобно сетевой ОС рабочих групп, сетевая ОС масштаба предприятия должна позволять пользователям разделять файлы, приложения и принтеры, причем делать это для большего количества пользователей и объема данных и с более высокой производительностью. Кроме того, сетевая ОС масштаба предприятия обеспечивает возможность соединения разнородных систем - как рабочих станций, так и серверов. Например, даже если ОС работает на платформе Intel, она должна поддерживать рабочие станции UNIX, работающие на RISC-платформах. Аналогично, серверная ОС, работающая на RISC-компьютере, должна поддерживать DOS, Windows и OS/2. Сетевая ОС масштаба предприятия должна поддерживать несколько стеков протоколов (таких как TCP/IP, IPX/SPX, NetBIOS, DECnet и OSI), обеспечивая простой доступ к удаленным ресурсам, удобные процедуры управления сервисами, включая агентов для систем управления сетью.

Важным элементом сетевой ОС масштаба предприятия является централизованная справочная служба, в которой хранятся данные о пользователях и разделяемых ресурсах сети. Такая служба, называемая также службой каталогов, обеспечивает единый логический вход пользователя в сеть и предоставляет ему удобные средства просмотра всех доступных ему ресурсов. Администратор, при наличии в сети централизованной справочной службы, избавлен от необходимости заводить на каждом сервере повторяющийся список пользователей, а значит избавлен от большого количества рутинной работы и от потенциальных ошибок при определении состава пользователей и их прав на каждом сервере.

Важным свойством справочной службы является ее масштабируемость, обеспечиваемая распределенностью базы данных о пользователях и ресурсах.

Такие сетевые ОС, как Banyan Vines, Novell NetWare 4.x, IBM LAN Server, Sun NFS, Microsoft LAN Manager и Windows NT Server, могут служить в качестве операционной системы предприятия, в то время как ОС NetWare 3.x, Personal Ware, Artisoft LANtastic больше подходят для небольших рабочих групп.

Критериями для выбора ОС масштаба предприятия являются следующие характеристики:

Органичная поддержка многосерверной сети;

Высокая эффективность файловых операций;

Возможность эффективной интеграции с другими ОС;

Наличие централизованной масштабируемой справочной службы;

Хорошие перспективы развития;

Эффективная работа удаленных пользователей;

Разнообразные сервисы: файл-сервис, принт-сервис, безопасность данных и отказоустойчивость, архивирование данных, служба обмена сообщениями, разнообразные базы данных и другие;

Разнообразные программно-аппаратные хост-платформы: IBM SNA, DEC NSA, UNIX;

Разнообразные транспортные протоколы: TCP/IP, IPX/SPX, NetBIOS, AppleTalk;

Поддержка многообразных операционных систем конечных пользователей: DOS, UNIX, OS/2, Mac;

Поддержка сетевого оборудования стандартов Ethernet, Token Ring, FDDI, ARCnet;

Наличие популярных прикладных интерфейсов и механизмов вызова удаленных процедур RPC;

Возможность взаимодействия с системой контроля и управления сетью, поддержка стандартов управления сетью SNMP.

Учитывая выше описанные критерии и доводы, для использования в сети была выбрана ОС Microsoft Windows NT Server 4.0.

Данная операционная система имеет следующие характеристики:

Серверные платформы: компьютеры на базе процессоров Intel, PowerPC, DEC Alpha, MIPS. Клиентские платформы: DOS, OS/2, Windows, Windows for Workgroups, Macintosh Организация одноранговой сети возможна с помощью Windows NT Workstation и Windows for Workgroups Windows NT Server представляет собой отличный сервер приложений: он поддерживает вытесняющую многозадачность, виртуальную память и симметричное мультипроцессирование, а также прикладные среды DOS, Windows, OS/2, POSIX Справочные службы: доменная для управления учетной информацией пользователей (Windows NT Domain Directory service), справочные службы имен WINS и DNS Хорошая поддержка совместной работы с сетями NetWare: поставляется клиентская часть (редиректор) для сервера NetWare (версий 3.х и 4.х в режиме эмуляции 3.х, справочная служба NDS поддерживается, начиная с версии 4.0), выполненная в виде шлюза в Windows NT Server или как отдельная компонента для Windows NT Workstation; Служба обработки сообщений - Microsoft Message Exchange, интегрированная с остальными службами Windows NT Server. Поддерживаемые сетевые протоколы: TCP/IP, IPX/SPX, NetBEUI, Appletalk. Поддержка удаленных пользователей: ISDN, коммутируемые телефонные линии, frame relay, X.25 - с помощью встроенной подсистемы Remote Access Server (RAS). Служба безопасности: мощная, использует избирательные права доступа и доверительные отношения между доменами; узлы сети, основанные на Windows NT Server, сертифицированы по уровню C2. Простота установки и обслуживания. Отличная масштабируемость.

4.2 Формирование маршрутной таблицы

Спроектированная сеть состоит из трех подсетей, которые объединяют некоторое количество хостов. Для связи подсетей используется маршрутизатор, который перенаправляет пакеты из одной подсети в другую. Для осуществления маршрутизации в сети необходимо для всех компонентов сети определить уникальные ip адреса, и составить таблицу маршрутизации. Структура адресов сети представлена на рисунке 4.

Рис. 4. Структура адресов сети.

Сеть организации имеет адрес 10.10.0.0, соответственно, маска сети 255.255.0.0. Первая подсеть имеет адрес 10.10.1.0 и маску 255.255.255.0. Вторая подсеть имеет адрес 10.10.2.0 и маску 255.255.255.0. Адрес третьей подсети 10.10.3.0, маска подсети 255.255.255.0. Маршрутизатором является сервер, который входит в подсеть 10.10.3.0. Маршрутизатор имеет адрес 10.10.3.1. В подсети 10.10.3.0 есть proxy-сервер. Реальный IP-адрес этого сервера, используемый для выхода в Интернет локальными хостами 85.234.44.234.

Таблица маршрутизации приведена в таблице 2.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Адрес назначения | Маска подсети | Адрес следующего маршрутизатора | Интрефейс |
| 1 | 127.0.0.0 | 255.0.0.0 | 10.10.3.1 | 3 |
| 2 | 10.10.0.0 | 255.255.0.0 | 10.10.3.1 |  |
| 3 | 10.10.1.0 | 255.255.255.0 | 10.10.3.1 |  |
| 4 | 10.10.1.1 – 10.10.1.21 | 255.255.255.0 | 10.10.3.1 |  |
| 5 | 10.10.2.0 | 255.255.255.0 | 10.10.3.1 |  |
| 6 | 10.10.2.1 – 10.10.2.10 | 255.255.255.0 | 10.10.3.1 |  |
| 7 | 10.10.3.0 | 255.255.255.0 | 10.10.3.1 |  |
| 8 | 10.10.3.1 – 10.10.3.6 | 255.255.255.0 | 10.10.3.1 |  |

Табл. 2. Таблица маршрутизации сети

5. Обеспечение информационной безопасности в сети

Защита информации – это комплекс мероприятий, проводимых с целью предотвращения утечки, хищения, утраты, несанкционированного уничтожения, искажения, модификации (подделки), несанкционированного копирования, блокирования информации и т.п. Поскольку утрата информации может происходить по сугубо техническим, объективным и неумышленным причинам, под это определение подпадают также и мероприятия, связанные с повышением надежности сервера из-за отказов или сбоев в работе винчестеров, недостатков в используемом программном обеспечении и т.д.

Переход от работы на персональных компьютерах к работе в сети усложняет защиту информации по следующим причинам:

большое число пользователей в сети и их переменный состав. Защита на уровне имени и пароля пользователя недостаточна для предотвращения входа в сеть посторонних лиц;

значительная протяженность сети и наличие многих потенциальных каналов проникновения в сеть;

уже отмеченные недостатки в аппаратном и программном обеспечении, которые зачастую обнаруживаются не на предпродажном этапе, называемом бета- тестированием, а в процессе эксплуатации. В том числе неидеальны встроенные средства защиты информации даже в таких известных и "мощных" сетевых ОС, как Windows NT или NetWare.

Возможна утечка информации по каналам, находящимся вне сети:

хранилище носителей информации,

элементы строительных конструкций и окна помещений, которые образуют каналы утечки конфиденциальной информации за счет так называемого микрофонного эффекта,

телефонные, радио-, а также иные проводные и беспроводные каналы (в том числе каналы мобильной связи).

Любые дополнительные соединения с другими сегментами или подключение к Интернет порождают новые проблемы. Атаки на локальную сеть через подключение к Интернету для того, чтобы получить доступ к конфиденциальной информации, в последнее время получили широкое распространение, что связано с недостатками встроенной системы защиты информации в протоколах TCP/IP. Сетевые атаки через Интернет могут быть классифицированы следующим образом:

Сниффер пакетов (sniffer – в данном случае в смысле фильтрация) – прикладная программа, которая использует сетевую карту, работающую в режиме promiscuous (не делающий различия) mode (в этом режиме все пакеты, полученные по физическим каналам, сетевой адаптер отправляет приложению для обработки).

IP-спуфинг (spoof – обман, мистификация) – происходит, когда хакер, находящийся внутри корпорации или вне ее, выдает себя за санкционированного пользователя.

Отказ в обслуживании (Denial of Service – DoS). Атака DoS делает сеть недоступной для обычного использования за счет превышения допустимых пределов функционирования сети, операционной системы или приложения.

Парольные атаки – попытка подбора пароля легального пользователя для входа в сеть.

Атаки типа Man-in-the-Middle – непосредственный доступ к пакетам, передаваемым по сети.

Атаки на уровне приложений.

Сетевая разведка – сбор информации о сети с помощью общедоступных данных и приложений.

Злоупотребление доверием внутри сети.

Несанкционированный доступ (НСД), который не может считаться отдельным типом атаки, так как большинство сетевых атак проводятся ради получения несанкционированного доступа.

Вирусы и приложения типа "троянский конь".

В сети используется дискреционная модель разграничения доступа. В рамках этой модели для каждого субъекта определено, какой вид доступа он может осуществлять к каждому объекту сети. На основе этих определений была построена матрица доступа, которая приведена в таблице 3.

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | ПС | СУБД | СРК | АРМ АБД | АРМ Рук. | Сет. обор. | АРМ прогр. | БД этал. | АРМ АИБ | СОР |
| АИБ | 2 | 2 | 1 | 2 | 2 | 2 | 2 | 2 | 2 | 2 |
| АБД | 1 | 2 | 2 | 0 | 2 | 2 | 1 | 0 | 0 | 0 |
| Рук-во | 2 | 2 | 2 | 2 | 1 | 1 | 2 | 2 | 0 | 2 |
| Разраб. | 1 | 1 | 0 | 0 | 2 | 2 | 1 | 1 | 0 | 2 |
| Прочие. | 1 | 0 | 0 | 0 | 1 | 1 | 1 | 0 | 0 | 0 |

Таблица 3. Матрица доступа организации.

Применяемые сокращения:

АИБ – администратор информационной безопасности

АБД – администратор базы данных

Рук-во. – руководство организации

Разраб. – разработчики

ПС – почтовый сервер

СУБД – система управления базой данных

СРК – сервер резервного копирования

АРМ - автоматизированное рабочее место.

СОР – сервер отдела разработки.

0 – нет доступа

1 – чтение

2 – чтение/запись.

Для защиты локальной сети от атак из сети Интернет используется firewall OutPost Firewall 4.0. Данный продукт осуществляет комплексную защиту компонентов сети от вторжений и злонамеренных воздействий извне.

6.Стоимостная оценка

Заключительным этапом проектирования локальной сети является проведение стоимостной оценки компонентов сети.

|  |  |  |  |
| --- | --- | --- | --- |
| Название компонента | кол-во. | цена | стоимость |
|

|  |
| --- |
| Сервер |

 | 1 | 41500 | 41500 |
|

|  |
| --- |
| АРМ |

 | 34 | 24690 | 839460 |
|

|  |
| --- |
| Кабель |

 | 200 | 8 | 1600 |
|

|  |
| --- |
| Сетевой адаптер |

 | 34 | 228 | 7752 |
| Коммутатор | 3 | 10902 | 32706 |
| Принтер | 3 | 4530 | 13590 |
| ИБП | 1 | 2507 | 2507 |
| Итого: |  |  | 939115 |

В результате проведенной стоимостной оценки установлено, что размер затрат на проектирование сети является приемлемым, и следовательно, позволяет реализовать данный проект.

Заключение

В результате выполнения данного курсового проекта были сформулированы и описаны цели использования сети организации, осуществлен выбор размера и структуры сети, кабельной системы, разработана инфологическая и физическая модель сети, а также сетевого оборудования, сетевых программных средств и способов администрирования сети, также произведена стоимостная оценка локальной сети.

Таким образом, задание на курсовое проектирование выполнено в полном объеме.

Список использованных источников

1. Мали В.А. Проектирование локальной ТКС. Методические указания к выполнению курсового проекта.

2. www.intuit.ru