

МИНИСТЕРСТВО ПО РАЗВИТИЮ ИНФОРМАЦИОННЫХ
ТЕХНОЛОГИЙ И КОММУНИКАЦИЙ РЕСПУБЛИКИ УЗБЕКИСТАН
ТАШКЕНТСКИЙ УНИВЕРСИТЕТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

защите

Допустить к

зав. кафедрой «КС»

Назаров А.И. _____

«_____» _____ 2015

г.

Выпускная работа бакалавра

на тему «Проектирования локальной сети для школы №3 на базе
оборудование Cisco»

Выпускник _____ **Свитина Е.И.**

(подпись)

(Фамилия)

Руководитель _____ А.А.

(подпись)

Хабибуллаев

(Фамилия)

Рецензент _____ А.А.

(подпись)

Каххаров

(Фамилия)

Консультант

по БЖД _____

Борисова Е.А

(подпись)

(Фамилия)

Ташкент - 2015

**МИНИСТЕРСТВО ПО РАЗВИТИЮ ИНФОРМАЦИОННЫХ
ТЕХНОЛОГИЙ И КОММУНИКАЦИЙ РЕСПУБЛИКИ УЗБЕКИСТАН
ТАШКЕНТСКИЙ УНИВЕРСИТЕТ ИНФОРМАЦИОННЫХ
ТЕХНОЛОГИЙ**

Факультет: Компьютерный инжиниринг

Кафедра: Компьютерные системы

**Направления (специальность): 5610600- Техника и технология
оказания услуг (по отраслям услуг)**

УТВЕРЖДАЮ

Зав. кафедрой Назаров А.И

« _____ » _____ 2015 г.

ЗАДАНИЕ

на выпускную работу

Свитина Екатерина Игоревна

(фамилия, имя, отчество)

- 1. Тема работы: *Проектирования локальной сети для школы №3 на базе оборудования Cisco.***
- 2. Утверждена приказом по университету от «17» января 2015г. № 59-15.**
- 3. Срок сдачи законченной работы: *31.05.15 г.***

4. Исходные данные к работе: **учебная литература, информационно-справочная литература, сведения о структуре школы.**

5. Содержание расчётно–пояснительной записи (перечень подлежащих разработке вопросов): **Введение. Теоретические основы построения локальных сетей. Проектирование локальной сети для школы № 3 на базе оборудования cisco. Организация локальной сети для школы № 3. Заключение. Литература.**

6. Перечень графического материала: **презентационный файл сделанный на базе программы Power Point - презентация.ppt**

7. Дата выдачи задания: **20.01.2015 г.**

Руководитель _____ Задание принял

(подпись)

(подпись)

8. Консультант по отдельным разделам выпускной работы

Раздел	Ф.И.О Руководителя	Подпись дата	
		Задание выдал	Задание получил
Основная часть	А.А. Хабибуллаев		
Безопасность жизнедеятельности	Борисова Е.А		

9. График выполнения работы

№	Наименование раздела работы	Срок выполнения	Отметка руководителя выполнении
1.	Теоретические основы построения локальных сетей	20.01.15- 24.01.15	
2.	Проектирования локальной сети для школы № 3 на базе оборудование cisco	26.01.15- 14.02.15	
3.	Организация локальной сети для школы № 3	09.03.15-	

4.	Безопасность жизнедеятельности	14.03.15	
5.	Заключение	18.03.15- 20.03.15	
		23.03.15- 28.03.15	

Выпускник _____ « ____ »
 _____ 2015 г.
 (подпись)

Руководитель _____ « ____ »
 _____ 2015 г.
 (подпись)

Битирув ишида куйдаги асосий натижалар олинган: локал хисоблаш тармок куришнинг асосий назарияси урганилди, №3 мактаб учун локал хисоблаш тармогининг функционал схемаси ишлаб чикилди, хисоблаш тармок таркиби режалаштирилди, Windows 2008 Server асосида тармокни ташкиллаштириш лойхалаштирилди, мактаб учун локал компьютер тармок структураси лойхалаштирилди, асосий бошқарув блоклари аникланди, тармоқда хавсизлик ва ишдан чиқиш масалалари ҳам куриб чикилди.

В выпускной работе проделаны следующие основные работы: изучены теоретические основы построения локальных сетей, разработана функциональная схема локальной вычислительной сети для школы №3, планирована структура вычислительной сети, разработана организация сети на основе Windows 2008 Server, разработана структура локальной компьютерной сети школы, определены основные административные блоки, рассмотрены вопросы защита и отказоустойчивость в сети.

In the final work done by the following key: To study the theoretical basis for the development of local networks, developed formulation of the problem, developed a functional diagram of a local area network for skull, planning the structure of the computer network, developed by the organization of the network based on Windows 2008 Server, designed the structure of the local network agencies property, the basic administrative units, the issues of information security in the network.

Содержание

Введение	6
I. ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПОСТРОЕНИЯ ЛОКАЛЬНЫХ СЕТЕЙ...	8
1.1. Оборудование, необходимое для построения различных компьютерных сетей	8
1.2. Принципы построения локальных сетей	9
1.3. Способы организации компьютерной сети	10
1.4. Топологии локальных сетей	13
1.5. Сетевые технологии	16
1.6. Кабели, применяемые в локальных сетях	18
1.7. Соединение сетей и маршрутизация	23
Выводы по главе I	25
II. ПРОЕКТИРОВАНИЯ ЛОКАЛЬНОЙ СЕТИ ДЛЯ ШКОЛЫ № 3 НА БАЗЕ ОБОРУДОВАНИЕ CISCO	26
2.1. Описание деятельности организации	26
2.2. Схема размещения рабочих мест сотрудников	27
2.3. Выбор сетевого оборудования	29
2.4. Структурная схема сети	36
Выводы по главе II	38
III. ОРГАНИЗАЦИЯ ЛОКАЛЬНОЙ СЕТИ ДЛЯ ШКОЛЫ № 3	39

3.1. Логическая организация сети.....	39
3.2. Программные средства для организации сети.....	39
3.3. Защита сети.....	42
3.4. Отказоустойчивость сети.....	43
Выводы по главе III.....	46
IV. БЕЗОПАСНОСТЬ ЖИЗНЕДЕЯТЕЛЬНОСТИ.....	47
4.1. Производительность труда и работоспособность человека...	47
4.2. Чрезвычайные ситуации.....	50
4.3. Техносфера.....	56
Выводы по главе IV.....	59
Заключение.	60
Литература.	61
Приложение	63

ВВЕДЕНИЕ

В век глобализации трудно представить какую-либо область деятельности без опоры на информационно-коммуникационные технологии. Поэтому данная сфера – одна из самых быстро развивающихся отраслей экономики Узбекистана. В нашей стране под руководством Президента Ислама Каримова создана мощная законодательная база, способствующая дальнейшему развитию рынка IT-технологий.

Сегодня свои дата-центры имеют операторы мобильной связи, крупные банки, операторы и провайдеры телекоммуникаций, всего более 30 хост-провайдеров, предоставляющие целый спектр комплексных услуг и сервисов. В Узбекистане мобильный интернет, следуя мировой тенденции, динамично набирает широкую популярность и уже в отдельных случаях претендует на роль альтернативы проводному доступу к всемирной паутине. Причины его роста в Узбекистане – появление новых технологий, доступность сотовых телефонов, поддерживающих стандарты и технологии, позволяющие подключаться к глобальной сети [1].

Локальная вычислительная сеть (ЛВС) – это такой способ совместного подключения нескольких компьютеров к общему каналу передачи данных, благодаря которому обеспечивается совместное использование ресурсов, таких, как базы данных, оборудование, программы. С помощью локальной сети удаленные рабочие станции объединяются в единую систему, имеющую следующие преимущества:

1. Разделение ресурсов – позволяет совместно использовать ресурсы, например, периферийные устройства (принтеры, сканеры), всеми станциями, входящими в сеть.

2. Разделение данных – позволяет совместно использовать информацию, находящуюся на жестких дисках рабочих станций и сервера.

3. Разделение программных средств – обеспечивает совместное использование программ, установленных на рабочих станциях и сервере.

Широкие возможности компьютеров по обработке информации делают их в принципе пригодными для разнообразного использования в области образования. Компьютеры пригодны для использования в таких областях, как языковедение и математика, история и естественные науки, профессиональная подготовка, музыка и изобразительное искусство, а также чтение и письмо. Компьютеры открывают новые пути в развитии навыков мышления и умения решать проблемы, предоставляют новые возможности для активного обучения. С помощью компьютеров можно сделать проведение уроков, упражнений, контрольных работ, а также учет успеваемости более эффективными. Это разгружает учителей и позволяет им уделять больше времени индивидуальным занятиям. Компьютеры могут сделать многие уроки более интересными и убедительными, а огромный поток информации – легкодоступным.

Целью выпускной работы является проектирование локальной компьютерной сети для школы №3 на базе оборудования Cisco.

Для решения поставленной цели в работе решаются следующие задачи:

- выбор сетевой архитектуры для компьютерной сети метод доступа, топология, тип кабельной системы;
- выбор способа управления сетью;
- конфигурация сетевого оборудования – количество серверов, коммутаторов, сетевых принтеров;
- управление сетевыми ресурсами и пользователями сети;
- рассмотрение вопросов безопасности сети и отказоустойчивость;

Необходимо разработать рациональную, гибкую структурную схему сети школы, предусмотреть режимы быстрого обновления оперативной информации на сервере, а так же проработать вопросы обеспечения необходимого уровня защиты данных и отказоустойчивость.

1. ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПОСТРОЕНИЯ ЛОКАЛЬНЫХ СЕТЕЙ

1.1. Оборудование, необходимое для построения различных компьютерных сетей

Компьютерной сетью можно считать соединение двух и более компьютеров с помощью кабеля или телефонной линии и модема, при котором становится возможен обмен данными между ними. Компьютеры, расположенные в одном помещении или здании и связанные между собой, называют локальной компьютерной сетью (LAN – Local Area Network). Количество компьютеров, подключенных к такой сети, ограничивается возможностями применяемой кабельной системы и сетевого оборудования. Несколько локальных компьютерных сетей при объединении образуют кампусную сеть (CAN – Campus Area Network), например, локальные сети расположенных по соседству зданий или корпусов одного предприятия или учебного заведения. MAN (Metropolitan Area Network) – сеть уже городского масштаба, к которой могут быть подключены несколько кампусных или локальных сетей предприятий и организаций. WAN (Wide Area Network) – широкомасштабная сеть, охватывающая, например, несколько городов, область или край.

CAN (Global Area Network) – глобальная компьютерная сеть – это объединение нескольких широкомасштабных компьютерных сетей, например, в масштабе страны. И, наконец, сетью всех сетей является Интернет, в состав которого входят Всемирная Компьютерная Паутина (World Wide Web), система электронной почты и другие системы хранения и передачи информации [2].

Для реализации сетевых возможностей необходимо соединить два или более компьютеров в локальную сеть. Какой бы способ соединения вы не выбрали, вам не обойтись без дополнительного оборудования. В случае если

вы будете использовать для связи прямое кабельное соединение, потребуются многожильный кабель и разъемы для подключения его к COM- или LPT-портам компьютеров. Обычно используются разъемы типа DB-9 или DB-25.

Если у вас имеется телефонная линия, то, чтобы подсоединиться к другому компьютеру или к Интернету, вам нужен модем, который необходимо подключить к свободному COM- или USB-порту или установить в слот на материнской плате, после чего настроить модем на соединение с Интернетом или другим компьютером. Если вы хотите создать локальную компьютерную сеть в своем подъезде, доме или офисе, то вам потребуются сетевые карты, кабель необходимой длины, а также могут потребоваться хабы, свитчеры и репитеры, в зависимости от протяженности и разветвленности вашей сети. Локальная сеть представляет собой коммуникационную систему, обеспечивающую высокоскоростной обмен данными между несколькими компьютерами в пределах ограниченной территории. В отличие от нее, глобальная сеть (Wide Area Network, сокращенно – WAN) может простираться на сотни и тысячи километров. Обе разновидности компьютерных сетей имеют много общего в программном обеспечении, но отличаются используемыми телекоммуникационными каналами и оборудованием связи.

1.2. Принципы построения локальных сетей

При построении локальных компьютерных сетей необходимо учитывать множество различных факторов, например, количество объединяемых в сеть компьютеров, удаленность их друг от друга, обеспечение конфиденциальности передаваемых по сети данных и т.д. Поэтому для выбора наиболее подходящей в каждом конкретном случае

структуры сети необходимо знать, какие бывают сети, и познакомиться с основными понятиями, используемыми при описании компьютерных сетей.

К таким понятиям относятся:

- сетевые компоненты;
- способы организации сети, определяющие возможность доступа компьютера к данным, передаваемым по сети и хранящимся на других сетевых компьютерах;
- роли компьютеров в сети;
- топология компьютерной сети;
- технология компьютерной сети;
- тип кабельной системы, используемой для соединения компьютеров;
- соединение сетей и маршрутизация.

Сетевые компоненты

Основными компонентами локальной сети являются узлы (Node), связанные между собой соединительным кабелем, который иначе называется сегментом (Segment) [2].

В сетевых узлах чаще всего находятся компьютеры, однако может располагаться и другое оборудование, например:

- сетевой принтер;
- концентратор;
- повторитель;
- мост;
- маршрутизатор [3].

1.3. Способы организации компьютерной сети

Компьютерные сети, в зависимости от роли каждого конкретного подключенного к сети компьютера, делятся на два вида:

- одноранговые;

– иерархические.

В одноранговой сети все компьютеры имеют равные права, и каждый пользователь делает доступными или недоступными для общего использования ресурсы своего компьютера: файлы, принтеры и т.п. В такой сети компьютеры находят друг друга по имени или по уникальному адресу и этого оказывается достаточно для нормальной работы сети [2].

В иерархической сети права доступа отдельного компьютера к сетевым ресурсам и адресация, т.е. присвоение каждому конкретному компьютеру, входящему в сеть, уникального адреса, регулируется выделенным сервером. Сервер, с помощью специальных программных средств, следит за тем, чтобы адреса в сети не повторялись, и чтобы информация, посланная с одного компьютера, попала адресату и была недоступна другим пользователям сети. Управление правами доступа и распределение сетевых адресов называется администрированием и выполняется специалистами – сетевыми администраторами.

Компьютер, подключенный к локальной сети, может называться по-разному, в зависимости от основных выполняемых им функций:

- рабочая станция (Workstation);
- сервер (Server).

Рабочая станция использует только доступные для нее ресурсы локальной сети.

Сервер выполняет определенные действия по запросам рабочих станций, предоставляя им свои ресурсы, например, дисковое пространство, вычислительную мощность процессора, принтер, модем и другое оборудование.

На самом деле, если рассмотреть вопрос еще глубже, все взаимодействия в сети происходят на уровне программ. Это выглядит примерно так: программа-сервер получает по сети запрос от программы-клиента с рабочей станции, обрабатывает его и посылает ответ.

Разновидности серверов

Чаще всего название сервера включает и наименование его основной функции:

- файловый сервер;
- сервер печати;
- почтовый сервер;
- сервер новостей;
- Web-сервер;
- сервер баз данных;
- факс-сервер и т. д.

Серверы также могут классифицироваться по признаку, указывающему на характер его использования:

- выделенный сервер;
- невыделенный сервер [5].

Выделенный сервер в локальной сети предназначен исключительно для предоставления своих ресурсов в общее пользование, а не для непосредственной работы на нем, поэтому может полноценно функционировать без монитора и клавиатуры. Обычно он обладает повышенной мощностью и надежностью аппаратуры, а также используемого программного обеспечения. В качестве операционной системы выделенного сервера чаще всего используются:

- Microsoft Windows 2000 Server;
- Microsoft Windows 2008 Server;
- Linux, FreeBSD, Sun Solaris и другие разновидности Unix;
- Novell NetWare.

Невыделенный сервер совмещает функции сервера и рабочей станции. Иными словами, это рабочая станция, некоторые ресурсы которой выделены для совместного доступа к ним по сети. На рабочей станции (невыделенном сервере) операционной системой может быть, например:

- Microsoft Windows 98/ME;
- Microsoft Windows XP Professional;
- Microsoft Windows 2000 Workstation;
- Linux.

В одноранговых локальных сетях компьютеры объединены рабочие группы (Workgroups), где они функционируют в качестве рабочих станций или невыделенных серверов, предоставляя часть своих ресурсов для использования своей рабочей группе. Одноранговые сети проще в администрировании, но не обеспечивают высокой степени защиты информации [5].

Локальные сети с выделенным сервером, напротив, имеют повышенную надежность и защищенность информации, которая хранится на сервере.

1.4. Топологии локальных сетей

Компьютеры и другие компоненты локальной сети могут соединяться между собой различными способами. Используемая схема физического расположения сетевых компонентов называется топологией (Topology). Топология сети определяется геометрической фигурой, образованной линиями связи между компьютерами, или физическим расположением по отношению друг к другу компьютеров, связанных между собой. Топология сети может служить одной из характеристик для сравнения и классификации различных компьютерных сетей.

Существуют три основные топологии построения локальной сети:

- звезда (Star);
- кольцо (Ring);
- шина (Bus) [2].

Звезда

В сети с топологией «звезда» все компьютеры соединены с центральным компьютером, или (hub – центр). Все данные поступают на центральный узел, который передает их получателю непосредственно. В этой топологии отсутствуют прямые связи между компьютерами сети. Передача всей информации происходит только через хаб (центральный компьютер). В качестве хаба может использоваться специальное устройство – концентратор, представляющий собой многопортовый репитер (repeater – повторитель). Основная функция репитера – получив данные на одном из портов, немедленно перенаправить их на другие порты.

Организация сети с топологией «звезда» проста и эффективна. При обрыве одного из кабелей, соединяющего отдельный компьютер сети с хабом, связь между остальными компьютерами, включенными по данной схеме, останется работоспособной. Если же из строя будет выведен сам центральный компьютер, то передача данных между компьютерами такой сети будет невозможна.

Достоинства звездообразной топологии:

- нарушение соединения в одном месте, кроме центрального узла, не прерывает работы локальной сети;
- при подключении большого количества компьютеров не происходит снижения производительности;
- безопасность информации обеспечивается на высоком уровне, так как компьютеры не получают чужих данных.

Недостатки звездообразной топологии:

- большой расход соединительного кабеля;
 - поломка центрального узла приводит к неработоспособности всей сети;
 - наращивание сети сопряжено с большими финансовыми затратами
- [2].

Кольцо

В топологии типа «кольцо» отсутствуют концевые точки соединения, т.е. сеть получается замкнутой в неразрывное кольцо.

В сети, построенной по кольцевой топологии, данные передаются в одном направлении от одного компьютера «кольца» к другому. Компьютер не передает информацию, пока не получит специальный маркер.

Достоинства кольцевой топологии:

– при подключении большого количества компьютеров происходит лишь незначительное снижение производительности.

Недостатки кольцевой топологии:

– нарушение соединения в одном месте приводит к прекращению работы всей локальной сети;

– безопасность информации обеспечивается не на очень высоком уровне: данные, посланные одним компьютером сети другому, могут быть легко перехвачены любым из компьютеров сети, которому они не предназначены, что может нарушить конфиденциальность передаваемой информации.

Шина

Топология «шина» использует для передачи данных один общий канал связи (чаще всего выполненный на основе коаксиального кабеля), к которому подключаются все компьютеры локальной сети.

Работа в сети с топологией «шина» осуществляется следующим образом. Когда один из компьютеров локальной сети с шинной топологией отправляет данные, они передаются по кабелю в обоих направлениях и принимаются всеми без исключения компьютерами, но использует их только тот из них, кому они были предназначены. Данные в сети с топологией «шина» могут следовать в любом направлении одновременно. На

противоположных концах шины устанавливаются специальные заглушки – терминаторы [2].

Достоинства шинной топологии:

- легкость наращивания сети;

– не очень высокая стоимость оборудования. Недостатки шинной топологии:

- нарушение соединения в одном месте приводит к неработоспособности всей локальной сети;

- при подключении большого количества компьютеров к одной шине происходит резкое снижение производительности;

- безопасность информации обеспечивается не на высоком уровне.

1.5. Сетевые технологии

Понятия технологии и топологии локальных сетей нередко путают между собой. Если топология компьютерной сети описывает геометрическую конфигурацию кабельных соединений между компьютерами, то под сетевой технологией следует понимать совокупность стандартов, описывающих процесс передачи информации, или особенности в аппаратной реализации сетевых адаптеров и заложенных в них принципов передачи информации. Сетевые адаптеры представляют собой электронные устройства, предназначенные для передачи данных от одного компьютера к другому по компьютерной сети. Они выполнены в виде печатной платы, которая устанавливается в свободный слот шины ISA или PCI материнской платы компьютера и имеет один или несколько разъемов, которые выводятся на заднюю панель компьютера для подключения к ним сетевого кабеля. Многие современные материнские платы имеют сетевые карты [4].

Наиболее известными и часто реализуемыми сетевыми технологиями являются:

- Ethernet;
- ARCNET;
- IBM Token Ring.

Технология Ethernet была разработана фирмой Xerox в 1973 г. и предназначена для построения сетей с топологией «звезда» или «шина». Когда в качестве канала связи используется коаксиальный кабель, то сеть Ethernet конфигурируется как «шина». Если же применяется витая пара, то строится сеть с топологией «звезда». На сегодняшний день эта технология является наиболее распространенной благодаря низкой стоимости, расширяемости и поддержке практически всеми производителями сетевого оборудования. Поэтому в следующих главах мы будем рассматривать построение сетей преимущественно на базе именно технологии Ethernet.

Технология ARCNET (Attached Resource Computer NET work) разработана компанией Datapoint Corporation в году и, так же, как Ethernet, может использоваться при построении сетей с топологией «звезда» или «шина». На основе ARCNET было построено множество сетей Novell NetWare 2.x; многие из них используются и сегодня. Тем не менее, данная технология считается устаревшей и в настоящее время уже не применяется.

Технология Token Ring, разработанная фирмой IBM в 1986 году, предназначена для построения сетей со смешанной топологией («звезда» и Компьютеры, объединенные в сеть по технологии Token Ring, подключаются к специальному устройству, которое называется станцией много пользовательского доступа Access Union, MAU), по топологии «звезда» используется в качестве центрального хаба, но для соединения с каждым компьютером сети используется два кабеля: по одному данные посылаются, по другому принимаются. Таким образом, получается, что сеть, построенная по технологии Token Ring, представляет собой кольцо, оформленное в виде звезды.

Сети Token Ring значительно дороже сетей Ethernet. Например, стоимость сетевой карты Token Ring в 3–5 раз превышает стоимость карты для Ethernet. Такое же соотношение характерно и для другого сетевого оборудования. По этой, а также по некоторым другим причинам технология Token Ring не нашла широкого признания. Так, сетевые карты и другие компоненты сети Token Ring производят всего несколько фирм, в то время как для Ethernet можно выбирать продукцию множества производителей.

1.6. Кабели, применяемые в локальных сетях

Для соединения двух и более компьютеров в единую компьютерную сеть чаще всего применяются кабельные системы на основе медных экранированных электрических проводов (Copper cable). Существуют также и оптоволоконные кабельные системы (Fiber-optic cable), которые по сравнению с электрическими кабелями обладают большей пропускной способностью и малыми потерями, однако более дороги. Поэтому оптоволоконные кабельные соединения применяются там, где нужно с большой скоростью передавать большой поток информации на большое расстояние, например, между районами города или при создании междугородной или международной сети. Альтернативой простому кабельному соединению может служить радиосвязь и связь, основанная на инфракрасном излучении. Однако эти виды связи не получили широкого распространения.

Электрические кабельные системы используют два типа кабелей. Первый тип представляет собой экранированный коаксиальный кабель с волновым сопротивлением 50 Ом, другой – витую пару [2].

Витая пара представляет собой два изолированных медных провода, скрученных между собой, но такой вид соединения в чистом виде не

подходит для связи между двумя компьютерами и используется только для соединений в специальных коммутационных шкафах.

Для связи между компьютерами используются кабели, содержащие несколько витых пар (3, 4 1000 и более) в общей изоляционной оболочке. В зависимости от эффективного диапазона рабочих частот витые пары делятся на несколько категорий, в соответствии с таблицей 1.1.

Таблица 1.1 – Категории витых пар

Полоса частот, МГц	Категория	Класс
до 0.1	1	A
до 1	2	B
до 16	3	C
до 20	4	
до 100	5	D
до 200	6	E
до 600	7	F

Витая пара может быть экранированной (STP – Shielded Twisted Pair) (Рис. 1.9) и неэкранированной (UTP – Unshielded Twisted Pair) (Рис. 1.8). Экранированная витая пара имеет множество разновидностей в зависимости от типа применяемого экрана. Экранированные витые пары, по сравнению с неэкранированными, имеют большую помехозащищенность, но и более дороги. Чаще всего для кабельной системы Ethernet применяется неэкранированный кабель пятой категории с 4 витыми парами.

Другие способы соединения компьютеров в сеть

Для связи двух компьютеров можно использовать и более простые способы соединения, такие как прямое кабельное соединение и соединение с помощью модема через телефонную линию. Кроме того, существуют и активно развиваются технологии, использующие существующую телефонную и электрическую проводку, а также беспроводную связь.

Прямое кабельное соединение

Прямое кабельное соединение использует для передачи данных встроенные в материнскую плату компьютера коммуникационные порты COM (Communication Port) или LPT (Line Printer). В современных компьютерах появилась также возможность связи двух и более компьютеров с помощью шины USB (Universal Serial Bus – универсальная последовательная шина). Порты COM обеспечивают асинхронный обмен данными по протоколу RS-232C со скоростью до 115 Кбит/сек. Современные компьютеры являются скоростными двунаправленными устройствами ввода-вывода и обеспечивают работу с DMA (Direct Memory Access – прямой доступ к памяти). Скорость передачи данных через может достигать до Мбит/с. Скорость передачи данных между компьютерами, соединенными с помощью шины USB 1.1, может достигать 12 Мбит/сек и до 480 Мбит/сек для USB 2.0. К достоинствам таких соединений можно отнести их простоту и малые затраты на построение, к недостаткам – небольшую дальность связи, ограниченную обычно несколькими десятками метров и, в случае соединения через низкую скорость передачи данных [5].

Соединение с помощью модема

Если в вашей квартире или офисе установлен телефон, то для передачи данных с одного компьютера на другой можно использовать модем (сокращение от модулятор-демоулятор). Модемы бывают внутренние (Internal), которые устанавливаются непосредственно в разъем материнской платы компьютера, и внешние (External), которые связаны с компьютером через COM-порт или шину USB. Большинство современных модемов обеспечивают скорость передачи данных до 33,6 Кбит/сек, а приема – до 56 Кбит/сек. К достоинствам такого вида связи можно отнести практически неограниченную дальность (любое место, куда можно дозвониться по

телефону), к недостаткам – низкую скорость передачи, которая к тому же сильно зависит от качества телефонной связи.

Сети на телефонных линиях

Для создания локальных сетей можно использовать имеющуюся в квартире или в офисе телефонную проводку. Для реализации таких сетей используется стандарт Home PNA (Home Phonenumber Networking Alliance – Альянс домашних телефонных сетей), разработанный в 1998 году. В 2000 году появилась его новая версия – Home PNA 2.0. Данный стандарт определяет сети с пропускной способностью до 32 Мбит/сек при длине сегмента до 300 м. В ближайшее время ожидается появление сетей Home PNA с пропускной способностью до Мбит/сек.

Сети данного типа используют существующие телефонные линии, но работают в особом частотном диапазоне, чтобы не создавать помех для обычных телефонных разговоров. После установки внутреннего или внешнего адаптера компьютер подключается к телефонной розетке с помощью обычного телефонного кабеля. Каждая телефонная розетка в доме становится портом сети, что позволяет обойтись без сетевого концентратора. Home PNA – это удобное решение для домашней сети, избавляющее от необходимости протягивать сетевые кабели по всему дому. Однако, учитывая высокую стоимость оборудования, а также низкое качество отечественных телефонных линий, сети Home PNA в странах СНГ пока не имеют широкого распространения [2].

Сети на основе электропроводки

Некоторый интерес представляет технология построения локальной сети на основе существующей электропроводки, которая называется (Home Power Line Cable – Кабель домашней электросети). В этой технологии используются сетевые карты, подключаемые через специальные разъемы к розеткам электропитания. При передаче информации компьютер посылает по электросети низкочастотный радиосигнал, не влияющий на электрический

ток в линиях электропитания. Этот радиосигнал принимает другой компьютер, также подключенный к сетевой розетке через адаптер Home PLC.

Основным недостатком сети Home PLC является незащищенность передаваемой информации от перехвата посторонним компьютером, подключенным к той же линии электропитания. Эту проблему можно решить созданием системы защиты, блокирующей доступ к локальной сети с помощью брандмауэра. Другой недостаток заключается в наличии в электросети электрических помех, вызванных бытовым электрооборудованием.

Беспроводные сети

Технологии беспроводных сетей включают в себя широкий диапазон решений, начиная от глобальных сетей передачи голоса и данных, позволяющих пользователю устанавливать беспроводные соединения на значительных расстояниях, и заканчивая технологиями инфракрасной и радиосвязи, используемыми на небольших расстояниях. Технологии беспроводных сетей применяются в портативных и настольных компьютерах, карманных компьютерах, персональных цифровых помощниках (PDA), сотовых телефонах, компьютерах с перьевым вводом и пейджерах. Беспроводные технологии могут использоваться для самых различных целей. Например, мобильные пользователи могут использовать свои сотовые телефоны для доступа к электронной почте. Путешественники с портативными компьютерами могут подключаться к Интернету через базовые станции, установленные в аэропортах, на вокзалах и в других общественных местах. У себя дома можно подключать устройства к настольному компьютеру для синхронизации данных и передачи файлов.

Беспроводные технологии позволяют использовать многообразные устройства для доступа к данным по всему миру, а также снижают или полностью устраняют затраты на прокладку дорогостоящих оптоволоконных

или кабельных каналов передачи данных, предоставляя при этом все возможности проводных сетей [2].

Адаптеры беспроводной сети, которые бывают внутренними и внешними, позволяют подключать компьютеры к сети без помощи кабелей или каких-либо иных физических соединений. Передаваемые данные разбиваются на небольшие пакеты и транслируются между компьютером и приемопередатчиками в виде радиосигналов в специально отведенном диапазоне частот.

1.7. Соединение сетей и маршрутизация

Чтобы разобраться, как именно происходит обмен данными между сетями, рассмотрим пример двух локальных сетей А и В, связанных между собой в одной точке соединения, называемой **узлом (Node)** (Рис. 1.10). В сетевом узле может находиться специальное устройство или компьютер с двумя сетевыми картами, выполняющий одну из следующих функций:

- повторитель (Repeater);
- мост (Bridge);
- маршрутизатор (Router), иногда также называемый межсетевым шлюзом (Gateway) [3].

Выбор того или иного устройства, расположенного в узловой точке, зависит от степени сетевой интеграции.

Повторитель используется при необходимости соединения двух относительно далеко расположенных участков (сегментов) одной и той же сети. Повторитель просто усиливает сигнал в линии связи в обе стороны, делая это совершенно незаметно для компьютеров, подключенных к разным сетевым сегментам.

Мост является более интеллектуальным устройством, чем повторитель. Мост соединяет локальные сети, базирующиеся на единой технологии. Он

отличается от повторителя тем, что отфильтровывает информацию, пропуская через себя только ту часть, которая адресована компьютерам, расположенным в другом сегменте. Естественно, попутно с этим электрический сигнал подвергается усилению до нужного уровня. Использование мостов снимает ограничения на максимальное количество соединенных ими кабельных сегментов. Мосты находят довольно широкое применение в сетевой операционной системе Novell NetWare, а в Windows используются редко, поэтому нас больше интересуют маршрутизаторы.

Маршрутизатор (межсетевой шлюз) выполняет сходные с мостом функции, но, в отличие от него, имеет в каждой подсети собственный сетевой адрес и может связывать сети, использующие различные технологии, например, Ethernet и Token Ring. Маршрутизатор связывает между собой не кабельные сегменты одной локальной сети, а уже разные сети, которые могут даже отличаться по используемым технологиям, например, на базе коаксиального кабеля и витой пары. Количество локальных сетей, соединенных между собой маршрутизаторами, может быть очень велико. Интернет представляет собой именно такое объединение.

В роли маршрутизатора обычно используется компьютер с двумя сетевыми картами, каждая из которых подключена к своему кабельному сегменту. Этот компьютер должен быть включен постоянно или хотя бы на время работы локальных сетей, иначе связь между ними прервется.

Предположим, что компьютер №1 посылает пакет данных, адресованный компьютеру №2. Так как оба эти компьютера находятся в сети А, компьютер №2 распознает свой адрес и принимает пакет. Аналогичным образом происходит непосредственная доставка пакетов данных в сети В между компьютерами №3, №4 и №5. В данном случае маршрутизатор не задействуется.

Непосредственная доставка пакетов данных в пределах одной сети происходит независимо от ее топологии: общая шина, звезда или кольцо. Не играет роли и используемая сетевая технология.

А что произойдет, если компьютер 1 из сети А, захочет отправить пакет данных, адресованный компьютеру №5, находящемуся в сети В? Компьютер №1 в процессе отправки определит, что адрес получателя пакета не входит в адресный диапазон сети А, и перешлет его на пункт промежуточной доставки – шлюз А, являющийся функциональным компонентом маршрутизатора.

Маршрутизатор, получивший пакет данных, просмотрит свою таблицу маршрутизации (Routing Table) и определит, что пакет нужно отправить через шлюз В. Когда пакет данных через шлюз В попадет в соответствующую сеть, он благополучно будет принят компьютером.

Имейте в виду, что здесь рассмотрена наиболее простая схема. Во-первых, к маршрутизатору может быть подключено не две, а несколько сетей. Во-вторых, получатель не обязательно должен быть непосредственно связан с сетью, куда передается пакет.

Выводы по главе I

В данной главе анализировано оборудование, необходимое для построения различных компьютерных сетей.

А также:

- Принципы построения локальных сетей;
- Способы организации компьютерной сети;
- Топологии локальных сетей;
- Сетевые технологии;
- Кабели, применяемые в локальных сетях;
- Соединение сетей и маршрутизация.

2. ПРОЕКТИРОВАНИЯ ЛОКАЛЬНОЙ СЕТИ ДЛЯ ШКОЛЫ № 3 НА БАЗЕ ОБОРУДОВАНИЕ CISCO

2.1. Описание деятельности организации

В рамках данной выпускной работы необходимо спроектировать локальную сеть для школы № 3 на базе оборудование Cisco.

ЛВС в данной школы должна состоять из 27 компьютеров. Сеть позволит ускорить перемещение данных между компьютерами. Для каждой рабочей станции необходимо обеспечить доступ к глобальной сети Интернет, для некоторых доступ к сетевому принтеру.

Здание школы состоит из трех этажей. ЛВС необходимо развернуть на третьем этаже. Так же необходимо поставить сервер для хранения данных школы.

На предприятии уже присутствует следующее оборудование: 27 компьютеров, 3 принтера и проектор.

Таблица 1. Требования сотрудников к сетевым ресурсам

Категория пользователя	Доступ в интернет	Доступ к файловому серверу	Доступ к сетевым принтерам
директор	должен присутствовать	полноценный	должен присутствовать
секретарь	должен присутствовать	полноценный	должен присутствовать
бухгалтер	должен присутствовать	ограниченный (доступ только к ресурсу «Бухгалтерия»)	должен присутствовать
Учитель физики	должен присутствовать	ограниченный (доступ только к ресурсу «Школьная программа»)	без доступа

Учитель информатики	должен присутствовать	ограниченный (доступ только к ресурсу «Школьная программа»)	без доступа
Зам. директора по воспитательной работе	должен присутствовать	отсутствует	без доступа
Ученик	ограниченный	ограниченный (доступ только к ресурсу «Школьникам»)	без доступа

Общее количество компьютеров составляет 27: по одному компьютеру у директора, секретаря, заместителя директора по воспитательной работе, учителя физики и учителя информатики; два компьютера у бухгалтеров и по 10 компьютеров на классы физики и информатики для учеников старших классов. У каждого сотрудника или ученика свое рабочее место.

2.2. Схема размещения рабочих мест сотрудников

Каждый из сотрудников имеет свое рабочее место, которое определяется кабинетом сотрудника.

На этаже находятся следующие кабинеты:

1. Кабинет директора;
2. Кабинет секретаря;
3. Кабинет бухгалтерии;
4. Кабинет физики;
5. Кабинет информатики;
6. Актный зал;
7. Служебное помещение.

Расположение оборудования каждого рабочего места изображено на схеме (рис. 1).

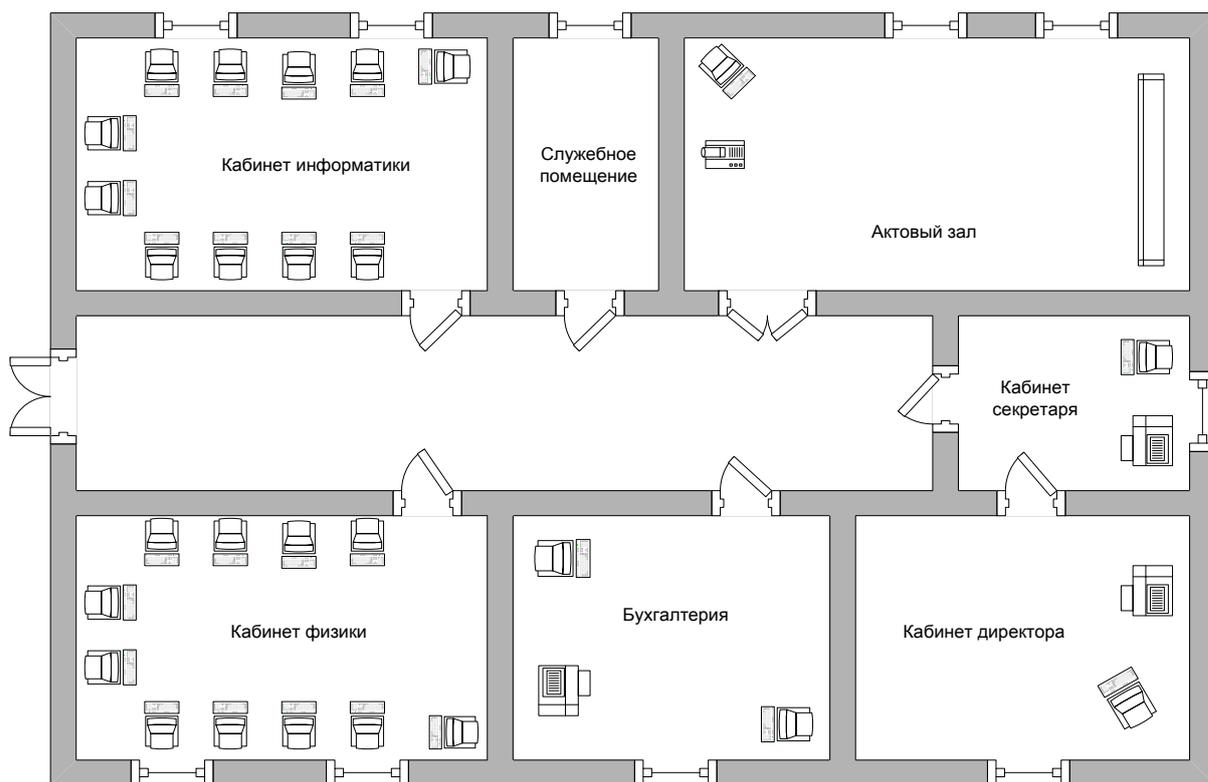


Рис. 1. План помещений 3-го этажа школы

Будем считать, что в школе уже присутствует следующее оборудование: 27 компьютеров, 3 принтера и проектор.

У каждой рабочей станции имеется розетка с разъемом RJ45 и в каждой станции есть сетевой адаптер, который встроен в системную плату. Поэтому, для подключения рабочей станции к сети необходимо иметь в наличии сетевой кабель с разъемами RJ45 на концах.

Рабочая станция как место работы специалиста представляет собой полноценный компьютер или компьютерный терминал (устройства ввода-вывода, отделённые и часто удалённые от управляющего компьютера), набор необходимого ПО, по необходимости дополняемые вспомогательным оборудованием: печатающее устройство, внешнее устройство хранения данных на оптических носителях, сканер и др. [5].

2.3. Выбор сетевого оборудования

Теперь, когда уже установлены требования для сети, можно определиться с тем, с помощью чего можно это реализовать. Во-первых, для совместной работы с файлами, нам необходим отдельный компьютер, который будет выполнять обязанности файлового сервера. На нем будут храниться документы, доступ к которым будет обеспечен большинству компьютеров сети. Кроме этого нам понадобятся несколько коммутаторов, чтобы соединить несколько компьютеров в один сегмент. Это позволит не прокладывать кабель по всему зданию, из чего следует, что снизятся затраты и увеличится надежность. Далее стоит отметить, что одним из требований к нашей ЛВС было наличие Wi-Fi. Чтобы его обеспечить, необходимо использовать Wi-Fi роутер. Кроме того для прокладки сети будет необходим сам кабель и коробка, чтобы защитить провода от повреждений.

Итак, можно сделать вывод, что для создания локальной сети потребуется следующее оборудование:

- файловый сервер;
- коммутаторы;
- Wi-Fi роутер;
- сетевой кабель (витая пара);
- коробка.

Файловый сервер

Файловый сервер – это выделенный сервер, оптимизированный для выполнения файловых операций ввода-вывода и предназначенный для хранения файлов любого типа. Как правило, обладает большим объемом дискового пространства. Его наличие в сети позволяет повысить скорость обмена данными, повысить надежность хранения информации [5].

Для повышения отказоустойчивости файлового сервера так же необходимо приобрести источник бесперебойного питания.

При выборе сервера следует обратить внимание на такие характеристики как:

- производительность процессора;
- объем оперативной памяти;
- скорость жесткого диска;
- отказоустойчивость [6].

Учитывая все вышеприведенные характеристики в качестве файл-сервера можно выбрать следующее:



Рис. 2. Системный блок Matrix Office Comfort RC13

Системный блок Matrix Office Comfort RC13 (2.93 ГГц, 2 ядра, Intel Core i3/4096 Мб DDR3/диск 1000 Гб/встроенная видеокарта, 384 Мб/DVD/CD-RW)

Описание / Процессор: Intel, Core i3, 2930 МГц, 2 ядра, Core i3–530 4Мб+2x256 Clarkdale LGA1156 / Вентилятор процессора: Cooler Master Hyper TX3 PWM [RR-910-HTX3-GP] (1156/1155 /775/AM2/AM3/754/939/940) / Оперативная память: DDR3, 4096 Мб, 1333 МГц, 1 Шт., DDR3 2048 Мб pc-10660 1333MHz *2 шт. / Материнская плата: iH55 S1156 2*DDR3 PCI-E16x SATA II HDMI GB Lan mATX / Разъемы материнской карты (сзади корпуса):

PS/2 VGA DVI LAN Audio USB 2.0 / Винчестер: 1000 Гб, HDD, 7200rpm
 32Mb S-ATA / Видеокарта: встроенная, 384 Мб, разъемы: D-SUB DVI /
 Оптический привод: DVD/CD-RW, DVD+-R/RW&CD-RW SATA /
 Аудиосистема: 5.1 / Сетевая карта: есть (10/100/1000Mbps Gigabit Ethernet
 UTP NIC 32-bit) / Корпус: mATX, INWIN EMR013 Black MicroATX 400W
 (24+4 пин) / Блок питания: 400 Вт (24+4 pin + SATA) [12].

Источник бесперебойного питания

ИБП Ironn Back Power Pro 400 ВА является приемлемым по критерию цена / качество / количество ВА. Сервер имеет не слишком высокую потребляемую мощность, поэтому использование ИБП на 400 ВА вполне оправдано. ИБП представлен на рис. 3.



Рис. 3. ИБП Ironn Back Power Pro

Таблица 2. Файловый сервер

Наименование	Модель
Системный блок	Системный блок Matrix Office Comfort RC13
Источник бесперебойного питания	Ironn Back Power Pro 400 ВА

Коммутаторы

Так как локальная сеть будет состоять из сегментов, то для объединения компьютеров в сегменте и сегментов между собой используются коммутаторы.

Одной из главной характеристики для коммутатора является количество портов, оно определяет количество соединяемых компьютеров.

В качестве коммутационного оборудования были выбраны коммутаторы (2 коммутатора с 16 портами и 2 коммутатора с 8 портами), а не концентраторы, так как по цене они практически не различаются, но коммутаторы имеют ряд преимуществ:

1) повышение пропускной способности сети (коммутатор имеет способность «запоминать» адрес каждого компьютера, подключённого к его портам и действовать как регулировщик – только передавать данные на компьютер адресата и ни на какие другие, так же устраняются ненужные передачи и тем самым освобождается сетевая пропускная способность);

2) коммутаторы предоставляют каждому узлу сети выделенную пропускную способность протокол.

В качестве коммутаторов будут использоваться:

- Коммутатор Cisco SG200-18 16 портов 10/100/1000 +2 combo порта RJ45/SFP, коммутатор такого типа изображен на рис. 4.





Рис. 4. Коммутатор Cisco SG200-18

Особенности и преимущества коммутатора Cisco SG200-18:

- Многофункциональные возможности: появляется возможность получить сеть бизнес-класса с такими функциями, как качество обслуживания (QoS), безопасность, Power Over Ethernet, а так же поддержка протокола IPv6.
- Экологически чистые решения: оптимизация энергопотребления для повышения эффективности без ущерба для производительности.
- Простая настройка и управление: интуитивно понятные инструменты на основе веб-браузера упрощают настройку и конфигурацию.
- Коммутатор Cisco SB SF100D-08-EU, коммутатор такого типа изображен на рис. 5.



Рис. 5. Коммутатор Cisco SB SF100D-08-EU

Таблица 3. Коммутаторы

Наименование	Модель	Кол-во
Коммутатор	Коммутатор Cisco SG200-18	2
Коммутатор	Коммутатор Cisco SB SF100D-08-EU	2

Wi-Fi роутер

Благодаря технологии Wi-Fi можно осуществлять выход с ноутбуков, КПК, сотовых телефонов и других устройств, оборудованных приемниками Wi-Fi в интернет без подключения сетевого кабеля.

Wi-Fi позволяет развивать сеть без весомых материальных затрат путем добавления точек доступа и приемников.

На рис. 6 показана точка доступа: Cisco SB WAP121-E-K9-G5.



Рис. 6. Cisco SB WAP121-E-K9-G5

Преимущества Wi-Fi:

- Позволяет развернуть сеть без прокладки кабеля, может уменьшить стоимость развёртывания и расширения сети. Места, где нельзя проложить кабель, например, вне помещений и в зданиях, имеющих историческую ценность, могут обслуживаться беспроводными сетями.
- Wi-Fi-устройства широко распространены на рынке. А устройства разных производителей могут взаимодействовать на базовом уровне сервисов.
- Wi-Fi сети поддерживают роуминг, поэтому клиентская станция может перемещаться в пространстве, переходя от одной точки доступа к другой.

- Wi-Fi – это набор глобальных стандартов. В отличие от сотовых телефонов, Wi-Fi оборудование может работать в разных странах по всему миру.

Недостатки Wi-Fi:

- Частотный диапазон и эксплуатационные ограничения в различных странах неодинаковы. Обычно Wi-Fi-роутер работает в диапазоне 2.4 GHz, также в этом диапазоне работает множество других устройств, таких как устройства, поддерживающие Bluetooth, это ухудшает электромагнитную совместимость.

- Довольно высокое по сравнению с другими стандартами потребление энергии, что уменьшает время жизни батарей и повышает температуру устройства.

- Наложение сигналов закрытой или использующей шифрование точки доступа и открытой точки доступа, работающих на одном или соседних каналах может помешать доступу к открытой точке доступа. Эта проблема может возникнуть при большой плотности точек доступа.

Сетевой кабель и коробка

Для выхода в интернет используется выделенная линия. Выбор именно этого средства обуславливается тем, что по сравнению с другими способами он обеспечивает более высокую скорость соединения.

Другой положительной чертой является то, что гарантирует не только высокую скорость входящего, но и исходящего соединений. Сейчас данная технология развивается очень стремительно, что делает ее более доступной.

Выход в интернет будет организован с помощью выделенного канала, который уже предоставлен местным провайдером.

В сети же компьютеры будут подключены с помощью витой пары.

Витая пара

Для прокладки сети используется сетевой кабель FTP (экранированная витая пара) категории 5, она изображена на рис. 7.



Рис. 7. Витая пара 5 категории.

Кабель-канал

Для прокладки кабеля используются короб шириной до 5 см для общего потока, и до 2 см для одного кабеля. Рис. 8 иллюстрирует стандартный короб.



Рис. 8. Кабель-канал

В результате анализа сетевого оборудования и выбора оптимальной комплектации получена следующая таблица:

Таблица 5. Список сетевого оборудования

Наименование	Количество
Системный блок Matrix Office Comfort RC13	1 шт.
Iron Back Power Pro 400 BA	1 шт.
Коммутатор Cisco SG200-18	2 шт.
Коммутатор Cisco SB SF100D-08-EU	2 шт.
Wi-Fi-роутер Cisco SB WAP121-E-K9-G5	1 шт.
Витая пара	500 м

2.4. Структурная схема сети

Наиболее распространенной на сегодняшний день является топология «звезда» на технологии Ethernet, которая отвечает всем современным требованиям к локальной сети и довольно удобна в эксплуатации. Из схемы структурированной кабельной системы рис. 10 можно однозначно судить о том, что данная топология лучше всего подходит для данной школы.



Рис. 9. Топология «звезда»

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 (при условии правильного проектирования) и гибкие возможности администрирования.

Недостатки:

- выход из строя центрального концентратора обернётся неработоспособностью сети (или сегмента сети) в целом;
- для прокладки сети зачастую требуется больше кабеля, чем для большинства других топологий;
- конечное число рабочих станций в сети (или сегменте сети) ограничено количеством портов в центральном концентраторе.

В центре каждой «звезды» – концентратор или коммутатор, который непосредственно соединен с каждым отдельным узлом сети через тонкий гибкий кабель UTP, так же называемый «витой парой». Кабель соединяет сетевой адаптер с ПК, с одной стороны, с концентратором или коммутатором – с другой. Устанавливать сеть с топологией «звезда» просто и недорого. Число узлов, которые можно подключить к концентратору, определяется возможным количеством портов самого концентратора. Однако имеется ограничение по числу узлов: сеть может иметь максимум 1024 узла. Рабочая группа, созданная по схеме «звезда», может функционировать независимо или может быть связана с другими рабочими группами [2].

В качестве технологии доступа был выбран Fast Ethernet, обеспечивающий скорость обмена данными в 100 Мбит/с. В качестве подвида данной технологии был выбран 100BASE-TX, IEEE 802.3u – развитие стандарта 10BASE-T для использования в сетях топологии «звезда». Задействована витая пара категории 5: CAT5e – скорость передач данных до 100 Мбит/с при использовании 2 пар. Кабель категории 5e является самым распространённым и используется для построения компьютерных сетей. Преимущества данного кабеля в более низкой себестоимости и меньшей толщине [5].

Формирование адресной структуры сети: Для формирования адресного пространства данной сети выбраны IP-адреса класса C. (адреса из диапазона от 192.0.0.0 до 223.255.255.0). Маска подсети имеет вид 255.255.255.0.

Первые 3 байта формируют номер сети, последний байт формирует номер узла.

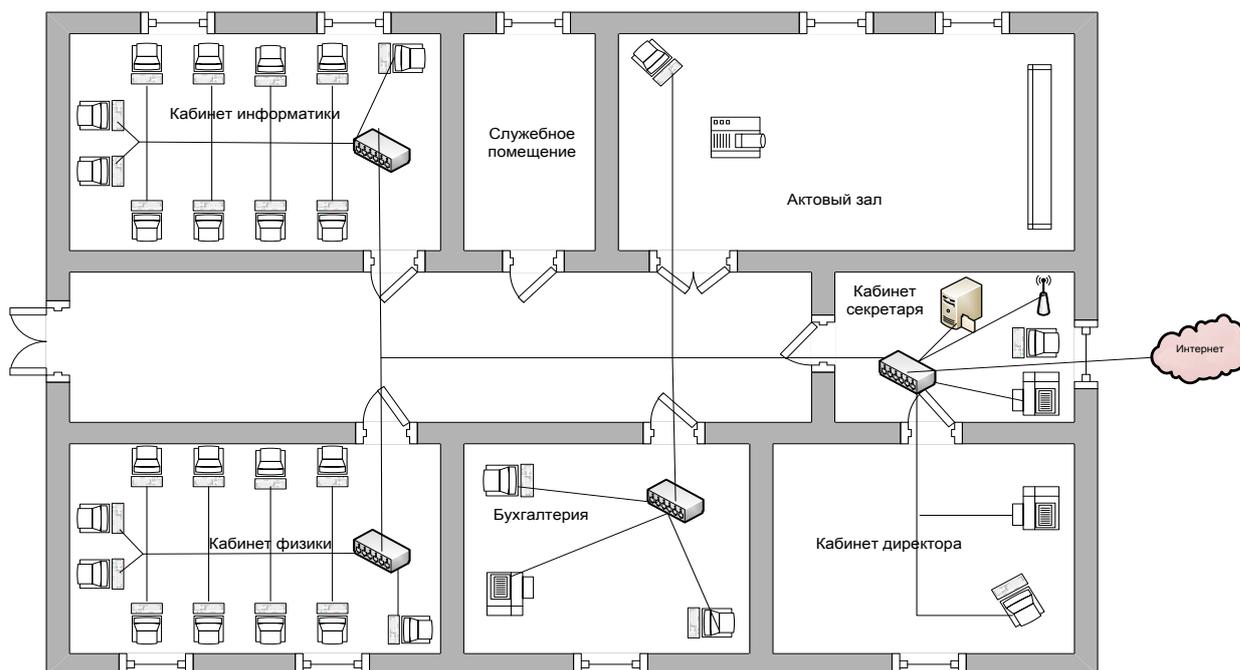


Рис. 10. Схема структурированной кабельной системы

Выводы по главе II

Во второй главе были проанализированы и выбраны технические средства, топология и технология сети для проектирования. А также спроектирована структурная схема сети.

3. ОРГАНИЗАЦИЯ ЛОКАЛЬНОЙ СЕТИ ДЛЯ ШКОЛЫ № 3

3.1. Логическая организация сети

Имеется ряд IP-адресов, которые зарезервированы для использования только в локальных сетях. Пакеты с такими адресами не передаются маршрутизаторами Интернета. В классе С к таким IP-адресам относятся адреса от 192.168.0.0 до 192.168.255.0.

Поэтому для локальной сети школы назначаем следующие IP-адреса:

- сервер – 192.168.1.1;
- компьютер в актовом зале – 192.168.1.2;
- компьютер секретаря – 192.168.1.3
- сетевой принтер в кабинете секретаря – 192.168.1.4;
- точка доступа Wi-Fi – 192.168.1.5;
- компьютер директора – 192.168.1.6;
- сетевой принтер в кабинете директора – 192.168.1.7;
- компьютер главного бухгалтера – 192.168.1.8;
- компьютер бухгалтера – 192.168.1.9;
- сетевой принтер в кабинете бухгалтеров – 192.168.1.10;
- компьютеры в кабинете физики имеют IP-адреса от 192.168.1.11 до 192.168.1.21;
- компьютеры в кабинете информатики имеют IP-адреса от 192.168.1.22 до 192.168.1.32.

3.2. Программные средства для организации сети

В качестве операционной системы сервера будет использоваться Windows Server 2008, которая является наиболее надежной и безопасной операционной системой в семействе серверных ОС Windows, что является необходимым условием для сервера.

Windows Server 2008 версия серверной операционной системы от Microsoft. Выпущена 27 февраля 2008 года. Эта версия заменяет Windows Server 2003 как представитель операционных систем поколения Vista (NT 6.x).

В Windows Server 2008 имеются средства для анализа состояния и диагностики операционной системы, так же данная серверная операционная система предлагает целый ряд новых технических возможностей в области безопасности, управления и администрирования, разработанных для повышения надежности и гибкости работы сервера [5].



Рис. 11. Windows 2008 Server

В качестве ОС на рабочих станциях оставляется установленная ранее Windows XP Professional.

Операционная система Windows XP Professional:

- обеспечивает высокий уровень масштабируемости и надежности;
- обеспечивает более высокий уровень безопасности, включая возможность шифрования файлов и папок с целью защиты корпоративной информации;

- обеспечивает поддержку мобильных устройств для обеспечения возможности работать автономно или подключаться к компьютеру в удаленном режиме;
- обеспечивает встроенную поддержку высокопроизводительных многопроцессорных систем;
- обеспечивает возможность работы с сервером Microsoft Windows Server;
- обеспечивает эффективное взаимодействие с другими пользователями по всему миру благодаря возможностям многоязычной поддержки.

Кроме этого, на все компьютеры необходимо поставить антивирусную программу ESET NOD32 Business Edition.

Эта антивирусная программа была выбрана по следующим причинам:

1) Проактивная защита и точное обнаружение угроз. Антивирус ESET NOD32 разработан на основе передовой технологии ThreatSense®. Ядро программы обеспечивает проактивное обнаружение всех типов угроз и лечение зараженных файлов (в том числе, в архивах) благодаря широкому применению интеллектуальных технологий, сочетанию эвристических методов и традиционного сигнатурного детектирования.

2) Host Intrusion Prevention System (HIPS). Усовершенствованная система защиты от попыток внешнего воздействия, способных негативно повлиять на безопасность компьютера. Для мониторинга процессов, файлов и ключей реестра HIPS используется сочетание технологий поведенческого анализа с возможностями сетевого фильтра, что позволяет эффективно детектировать, блокировать и предотвращать подобные попытки вторжения.

3) Высокая скорость работы. Работа Антивируса ESET NOD32 не отражается на производительности компьютера – сканирование и процессы обновления происходят практически незаметно для пользователя, не нагружая систему.

4) Удобство. Антивирус ESET NOD32 разработан по принципу минимальной нагрузки на систему и занимает не более 44 Мб памяти.

5) Простота использования.

В результате анализа программного обеспечения получена следующая таблица:

Таблица 6. Стоимость программного обеспечения

Программа	Модель	Количество
Операционная система на сервер	Windows Server 2008	1
Антивирусная программа	ESET NOD32 Business Edition newsale for 28 User	1

3.3. Защита сети

Для нормального и бесперебойного функционирования сети необходимо обеспечить ее безопасность. Специализированные программные средства защиты информации от несанкционированного доступа обладают в целом лучшими возможностями и характеристиками, чем встроенные средства сетевых ОС. Кроме программ шифрования, существует много других доступных внешних средств защиты информации. Из наиболее часто упоминаемых, следует отметить следующие системы, позволяющие ограничить информационные потоки.

1. Firewalls – брандмауэры (дословно firewall – огненная стена). Между локальной и глобальной сетями создаются специальные промежуточные сервера, которые инспектируют и фильтруют весь проходящий через них трафик сетевого/ транспортного уровней. Это позволяет резко снизить угрозу несанкционированного доступа извне в корпоративные сети, но не устраняет эту опасность совсем. Более защищенная разновидность метода – это способ маскировки (masquerading),

когда весь исходящий из локальной сети трафик посылается от имени firewall-сервера, делая локальную сеть практически невидимой.

2. Proxy-servers (proxy – доверенность, доверенное лицо). Весь трафик сетевого / транспортного уровней между локальной и глобальной сетями запрещается полностью – попросту отсутствует маршрутизация, а обращения из локальной сети в глобальную происходят через специальные серверы-посредники. Очевидно, что при этом методе обращения из глобальной сети в локальную становятся невозможными. Очевидно также, что этот метод не дает достаточной защиты против атак на более высоких уровнях – например, на уровне приложения (вирусы и JavaScript).

3. Антивирусная программа (антивирус) – изначально программа для обнаружения и лечения программ, заражённых компьютерным вирусом, а также для предотвращения заражения файла вирусом. Многие современные антивирусы позволяют обнаруживать и удалять также троянские программы и прочие вредоносные программы. И напротив – программы, создававшиеся как файрволы, также обретают функции, роднящие их с антивирусами (например, Outpost Firewall), что со временем может привести к ещё более очевидному распространению смысла термина на средства защиты вообще [5].

В нашей сети будет использоваться антивирусная программа ESET NOD32 Business Edition.

3.4. Отказоустойчивость сети

Отказоустойчивость – это один из основных факторов, который нужно учитывать при построении локальных сетей.

В случае выхода сети школы из строя возможны нарушение работы сотрудников, потеря данных. В таблице 7 приведены различные неисправности и их последствия.

Для того, что бы свести к минимуму вероятность отказа сети прибегают к нескольким средствам:

- дублирование блоков питания;
- возможность «горячей» замены компонентов;
- дублирование управляющего модуля;
- дублирование коммутационной матрицы / шины;
- использование нескольких дублирующих соединений;
- использование технологии Multi-Link Trunk (MLT) и Split-MLT;
- возможное внедрение протоколов балансировки нагрузки и дублирования на уровне маршрутизации;
- разнесение окончания каналов;
- разнесение каналов;
- использование высоконадежного оборудования [6].

Таблица 7. Возможные неисправности и их последствия

Неисправность	Возможная причина	Последствия для сети	Решение проблемы	Меры предотвращения
Выход из строя главного коммутатора	Механическая неисправность; неправильная эксплуатация.	Выход из строя всей сети.	Замена коммутатора.	Правильная эксплуатация; наличие запасного коммутатора.
Выход из строя коммутатора в одном из отделов.	Механическая неисправность; неправильная эксплуатация.	Выход из строя сегмента сети.	Замена коммутатора.	Правильная эксплуатация; наличие запасного коммутатора.

Выход из строя сервера.	Механическая неисправность; неправильная эксплуатация; отказ комплектующих сервера.	Вероятность потери всех данных; пропадает возможность централизованного хранения данных.	Ремонт сервера (возможна замена комплектующих, или в крайнем случае полная замена сервера).	Подбор сервера, полностью справляющегося с потребностями фирмы; подбор комплектующих с повышенной надежностью.
Выход из строя компьютеров пользователей.	Механическая неисправность, деятельность вирусов, неправильная эксплуатация; конфликты ПО.	Пропадает возможность обмена данными с неисправным компьютером.	Ремонт клиентского компьютера.	Правильная эксплуатация: технические осмотры; наличие антивируса; ограничение прав пользователей.
Выход из строя модема, точки доступа, сетевого принтера.	Механическая неисправность; неправильная эксплуатация.	Ограничение функций неисправного оборудования (отсутствие Wi-Fi, выхода в Интернет...)	Замена оборудования.	Правильная эксплуатация: технические осмотры; наличие антивируса; наличие запасного оборудования.
Выход из строя сетевого кабеля	Механическое повреждение.	Выход из строя сети или ее части.	Замена сетевого кабеля.	Кабель должен находиться в коробах; наличие запасного кабеля.

Сеть обладает несколькими преимуществами в плане отказоустойчивости:

- топологией сети является «звезда», что позволяет легко находить и устранять неисправности;
- в случае выхода из строя одного из коммутаторов он в экстренном темпе заменяется на рабочий, и сеть снова полностью функционирует;
- в случае выхода из строя одной из рабочих станций, остальные пользователи продолжают функционировать в обычном режиме;
- применение антивирусного программного обеспечения позволяет обезопасить сеть от сбоев в случае атак вирусов.

Выводы по главе III

В третьей главе была выбрано программное средства для организации сети, распределены адресные пространства, решены задачи по вопросу защита и отказоустойчивость сети. И в итоге спроектирована локальная сеть для школы № 3.

4. БЕЗОПАСНОСТЬ ЖИЗНЕДЕЯТЕЛЬНОСТИ

4.1. Производительность труда и работоспособность человека.

Уровень развития производительных сил проявляется в производительности труда. Производительность труда - это плодотворность, продуктивность производственной деятельности людей, измеряемая количеством времени, затрачиваемым на единицу продукции, или количеством продукции, производимой в единицу рабочего времени (час, день, месяц, год).

Повышение производительности труда - объективный экономический закон развития человеческого общества. В процессе труда живой труд использует результаты прошлого, овеществленного труда (предметы и средства труда) для производства новых продуктов. Рост производительных сил означает экономию не только живого, но и овеществленного труда [8].

Факторы, влияющие на производительную силу труда, разнообразны. Многие из них действуют на протяжении всего развития человеческого общества, однако значение отдельных факторов, определяющих производительную силу труда, меняется на разных этапах. Первоначально ведущую роль играли природные условия. От них в значительной мере зависели продуктивное использование других факторов и общая производительность труда в целом. Позднее все большую роль приобретает средняя степень искусства работника, умение эффективно использовать свои профессиональные навыки и производственный опыт. Промышленная революция оттесняет природные условия и квалификацию на задний план. Она резко повысила роль орудий труда, технологии, общих и профессиональных знаний. Постепенно все большее значение приобретает не только характер и размеры средств производства, но и эффективность их применения, научная организация труда. Теперь уже от этих факторов в первую очередь зависит плодотворность труда.

Научно-техническая революция повышает роль информации и науки, их технологического применения в производстве.

Важно подчеркнуть, что возможность превращения потенциальной силы труда в реальную производительность труда зависит от характера господствующих производственных отношений, а также воздействия юридических и политических институтов. Революции в развитии производительных сил (неолитическая, промышленная, научно - техническая) знаменуют качественные этапы повышения производительности труда.

На эффективность трудовой деятельности человека существенно влияет режим труда и отдыха. Рациональным режимом является режим, при котором обеспечивается высокая производительность труда и устойчивая работоспособность без признаков чрезмерного утомления в течение длительного времени.

Правильность режима труда и отдыха оценивается на основе исследования состояния физиологических функций человека и динамики его работоспособности в процессе рабочего дня. Чем эффективнее режим, тем длительнее период устойчивой работоспособности, короче периоды вработываемости и спада работоспособности.

На производстве чередование периодов труда и отдыха достигается введением обеденного перерыва в середине рабочего дня и кратковременных регламентированных перерывов, устанавливаемых с учетом динамики работоспособности, тяжести и напряженности труда.

Так при работах, требующих большого напряжения и внимания, быстрых и точных движений, целесообразны частые, но короткие (5-10-минутные) перерывы. При работах, связанных со значительными усилиями и участием крупных мышц, рекомендуются более редкие, но продолжительные (10-12-минутные) перерывы. При особо тяжелых работах (кузнецы, металлурги) следует сочетать работу в течение 15-20 мин с отдыхом той же

продолжительности.

Кроме регламентируемых перерывов, существуют микропаузы-перерывы, возникающие самопроизвольно между операциями. Они поддерживают оптимальный темп работы и высокую работоспособность и составляют 9-10% рабочего времени.

Работоспособность и жизнедеятельность организма зависит от суточного режима труда и отдыха, то есть от чередования периодов работы, отдыха и сна. В соответствии с суточным циклом работоспособности наивысший уровень ее отмечается в утренние и дневные часы: с 8 до 12 и с 14 до 17. В вечерние часы работоспособность понижается, достигая своего минимума ночью. Эти закономерности должны учитываться при определении сменности работы, начала и окончания работы в сменах, перерывов на отдых и сон. Динамика работоспособности изменяется в течение недели: наивысшая работоспособность приходится на 2-й, 3-й и 4-й день работы, в последующие дни она понижается. В понедельник работоспособность понижена вследствие вработываемости.

Элементами рационального режима труда и отдыха является производственная гимнастика, психофизиологическая разгрузка. В основе производственной физкультуры лежит феномен активного отдыха, описанный И.М. Сеченовым: утомленные мышцы лучше отдыхают при работе других мышечных групп. Задачей производственной физкультуры является возобновление рабочего стереотипа в начале рабочей смены и сохранение его в течение рабочего дня. С этой целью применяется вводная гимнастика (5-7 мин), физкульт-паузы (по 5-10 мин 1-4 раза в смену) и физкультурные минутки (2-3 мин).

Для снятия усталости и нервно-психологического напряжения используются специально оборудованные помещения, где эффект психоэмоциональной разгрузки достигается за счет интерьера помещения, функциональной музыки и других факторов [8].

4.2. Чрезвычайные ситуации

В теории БЖД ЧС — это совокупность событий, результат наступления которых характеризуется одним или несколькими из следующих признаков:

- а) опасность для жизни и здоровья значительного числа людей;
- б) существенное нарушение экологического равновесия в районе чрезвычайной ситуации;
- в) выход из строя систем жизнеобеспечения и управления, полное или частичное прекращение хозяйственной деятельности;
- г) значительный материальный и экономический ущерб;
- д) необходимость привлечения больших, как правило, внешних по отношению к району ЧС сил и средств для спасения людей и ликвидации последствий;
- е) психологический дискомфорт для больших групп людей [8].

Характерно, что ЧС возникает внешне неожиданно, внезапно. Конкретизация определения ЧС достигается введением количественных мер опасностей.

Классификация ЧС. По причинам ЧС бывают природные, техногенные, антропогенные, экологические, социальные.

К природным (стихийным) ЧС относятся опасные природные явления или процессы, имеющие чрезвычайный характер и приводящие к нарушению повседневного уклада жизни более или менее значительных групп населения, человеческим жертвам, уничтожению материальных ценностей. К ним относятся землетрясения, наводнения, цунами, извержения вулканов, селевые потоки, оползни, обвалы, ураганы и смерчи, массовые лесные и торфяные пожары, снежные заносы и лавины. К числу стихийных бедствий относятся также засухи, длительные проливные дожди, сильные устойчивые морозы, эпидемии, эпизоотии,

эпифитотии, массовое распространение вредителей лесного и сельского хозяйства.

Стихийные бедствия могут происходить: в результате быстрого перемещения вещества (землетрясения, оползни); в процессе высвобождения внутриземной энергии (вулканическая деятельность, землетрясения); при повышении общего уровня рек, озер и морей (наводнения, цунами); под воздействием необычайно сильного ветра (ураганы, циклоны). Некоторые стихийные бедствия (пожары, обвалы, оползни и др.) могут возникнуть в результате действий самих людей, но последствия их всегда являются результатом действия сил природы. Для каждого стихийного бедствия характерно наличие присущих ему поражающих факторов, неблагоприятно воздействующих на состояние здоровья человека [8].

Стихийные бедствия являются трагедией всего государства и, особенно, для тех районов, где они возникают. В результате стихийных бедствий страдает экономика страны, так как при этом разрушаются производственные предприятия, уничтожаются материальные ценности и, самое главное, возникают потери среди людей, гибнет их жилье и имущество. Кроме того, стихийные бедствия создают крайне неблагоприятные условия для жизни населения, что может быть причиной вспышек массовых инфекционных заболеваний. Количество людей, пострадавших от стихийных бедствий, может быть весьма значительным, а характер поражений очень разнообразным. Больше всего люди страдают от наводнений (40% от общего урона), ураганов (20%), землетрясений и засух (по 15%). Около 10% общего ущерба приходится на остальные виды стихийных бедствий.

Ряд советских и зарубежных специалистов, приводя данные о потерях при крупнейших бедствиях, предполагают, что в будущем в связи с ростом и концентрацией населения аналогичные по силе катастрофы

будут сопровождаться увеличением числа жертв в десятки раз.

Техногенными ЧС принято считать внезапный выход из строя машин, механизмов и агрегатов во время их эксплуатации, сопровождающийся серьезными нарушениями производственного процесса, взрывами, образованием очагов пожаров, радиоактивным, химическим или биологическим заражением больших территорий, групповым поражением (гибелью) людей. К техногенным ЧС относятся аварии на промышленных объектах, строительстве, а также на железнодорожном, воздушном, автомобильном, трубопроводном и водном транспорте, в результате которых образовались пожары, разрушения гражданских и промышленных зданий, создавалась опасность радиационного загрязнения, химического и бактериального заражения местности, произошло растекание нефтепродуктов и агрессивных (ядовитых) жидкостей на поверхности земли и воды и возникли другие последствия, создающие угрозу населению и окружающей среде.

Характер последствий техногенных катастроф зависит от вида аварии, ее масштабов и особенностей предприятия, на котором возникла авария (от вида транспорта и обстоятельств, при которых произошла авария).

Антропогенные ЧС являются следствием ошибочных действий персонала. Этот класс ЧС может происходить на тех же объектах, что и техногенные ЧС. Отличие состоит лишь в том, что техногенные ЧС не связаны с человеческим фактором непосредственно.

К чрезвычайным ситуациям экологического характера можно отнести: интенсивную деградацию почвы и ее загрязнение тяжелыми металлами (кадмий, свинец, ртуть, хром и т. д.) и другими вредными веществами; загрязнение атмосферы вредными химическими веществами, шумом, электромагнитными полями; кислотные дожди; разрушение озонового слоя и т. д.

К социальным ЧС относятся события, происходящие в социуме (грабежи, насилия), межнациональные конфликты, сопровождающиеся применением силы; противоречия между государствами с применением оружия.

По скорости распространения опасности ЧС могут быть классифицированы на: внезапные (землетрясения, взрывы, транспортные аварии и т. д.); стремительные (пожары, гидродинамические аварии с образованием волны прорыва, аварии с выбросом газообразных СДЯВ и т. д.); умеренные (паводковые наводнения, извержения вулканов, аварии с выбросом радиоактивных, веществ); плавные с медленно распространяющейся опасностью (засухи, эпидемии, аварии на промышленных очистных сооружениях, загрязнение почвы и воды вредными химическими веществами и т. д.).

По масштабности ЧС можно подразделить на пять типов: локальные (объектовые), местные, региональные, национальные и глобальные. При локальных (объектовых) ЧС последствия ограничиваются пределами объекта народного хозяйства и могут быть устранены за счет его сил и ресурсов.

Местные ЧС имеют масштабы распространения в пределах населённого пункта, в том числе крупного города административного района, нескольких районов или области и могут быть устранены за счет сил и ресурсов области.

В региональных ЧС последствия ограничиваются пределами нескольких областей или экономического района и могут быть ликвидированы за счет сил и ресурсов республики. Национальные ЧС имеют последствия, охватывающие несколько экономических районов или республик, но не выходящие за пределы страны. Ликвидация таких ЧС осуществляется силами и ресурсами государства, зачастую с привлечением иностранной помощи.

При глобальной ЧС ее последствия выходят за пределы страны и распространяются на другие государства. Эти последствия устраняются как силами каждого государства на своей территории, так и силами международного сообщества. Границы между всеми перечисленными типами и классами ЧС в определенной мере условны. Как уже отмечалось, некоторые стихийные бедствия — оползни, опустынивание, в отдельных случаях землетрясения, лесные и торфяные пожары и т. д.— могут иметь как чисто природное, так и природно-антропогенное происхождение. То же самое можно сказать и при систематизации ЧС по другим признакам.

Последствия ЧС могут быть самыми разнообразными. Они зависят от вида, характера чрезвычайной ситуации и масштаба ее распространения.

Основными видами последствий ЧС являются: гибель, заболевания людей, разрушения, радиоактивное загрязнение, химическое заражение, бактериальное заражение. Следует подчеркнуть, что на людей, находящихся в экстремальных условиях ЧС, наряду с различными поражающими факторами действуют и психотравмирующие обстоятельства, представляющие собой обычно комплекс сверхсильных раздражителей, вызывающих нарушение психической деятельности в виде так называемых реактивных (психогенных) состояний. При этом психогенное воздействие экстремальных условий складывается не только из прямой, непосредственной угрозы жизни человека, но и опосредованной, связанной с ожиданием ее реализации вне зон поражения. Если радиусы воздействия опасных и вредных факторов ЧС можно с той или иной, степенью достоверности определить заблаговременно расчет путем, то радиус психологического воздействия в реальной действительности может иметь самые различные значения. В ряде случаев он, возможно, будет во много раз превосходить радиусы воздействия других поражающих факторов.

Территория, на которую воздействуют опасные и вредные факторы

ЧС, с расположенными на ней населением, животными, зданиями и сооружениями, инженерными сетями и коммуникациями называется очагом поражения. Очаги поражения бывают простые (однородные) и сложные (комбинированные) [8].

Простым очагом поражения называют очаг, возникший под воздействием одного поражающего фактора, например, разрушения от взрыва, пожара, только химическое или бактериальное заражение. Сложные очаги поражения возникают в результате действия нескольких поражающих факторов чрезвычайной ситуации. Например, взрыв на химическом предприятии влечет за собой разрушения, пожары, химическое заражение окружающей местности; землетрясение и ураган помимо разрушения сооружений, могут вызвать затопление прибрежной полосы, пожары от повреждения электрических сетей, химическое заражение в результате утечки СДЯВ при разрушении емкостей и т. д.

Форма очагов поражения в зависимости от природы источника опасных факторов может быть круглой — при землетрясениях, взрывах, полосной — при ураганах, смерчах, затоплениях, селевых потоках, лавинах и др., неправильной формы при пожарах, цунами, оползнях и т. п.

Независимо от происхождения и типа в развитии чрезвычайных ситуаций можно выделить четыре характерных стадии (фазы): зарождения, инициирования, кульминационную и затухания (ликвидации последствий).

На стадии зарождения складываются условия, предпосылки будущей ЧС: активизируются неблагоприятные природные процессы; накапливаются проектно-производственные дефекты сооружений и многочисленные технические неисправности; происходят сбои в работе оборудования, инженерно-технического персонала и т. п.

Установить продолжительность стадии зарождения, причем весьма приблизительно, можно только с помощью регулярной статистики отказов,

сбоев, «локальных» аварий, данных наблюдений сейсмических, метеорологических, противоселевых и других станций.

На стадии инициирования чрезвычайного события наиболее существенно влияние человеческого фактора. Так, статистика свидетельствует, что свыше 60% аварий происходит из-за ошибок персонала.

4.3. Техносфера

Объем и состав техносферы. Мировое хозяйство можно рассматривать как видовую реализованную экологическую нишу человечества. По многим пространственным и потоковым параметрам она совпадает с биосферой, экологическая емкость которой ограничена. Поэтому неизбежны конкурентные отношения между активными элементами техногенной среды и биосферы, между общественным производством и планетарной биотой. Хотя эти отношения намного сложнее, чем межвидовые взаимоотношения в природе, многие их черты выглядят как конкурентное вытеснение биосферы.

Техносфера - это глобальная совокупность орудий, объектов, материальных процессов и продуктов общественного производства. Техносферу можно определить также как пространство геосфер Земли, находящееся под воздействием производственной деятельности человека и занятое ее продуктами.

Понятие о природных ресурсах. Это солнечная энергия, свет, пища, вода, тепло, почва, т.е. все то, что необходимо для жизни на Земле. В данном разделе природные ресурсы будут рассмотрены с позиций использования их в общественном производстве [8].

Природные ресурсы являются основной частью экономических ресурсов, т.е. кроме факторов среды они являются факторами производства.

Ресурсы - это вещества, материалы, силы и потоки вещества, энергии и

информации, которые:

- образуют входные звенья природных или хозяйственных циклов, являются их необходимыми участниками и, в связи с этим, носителями функции полезности;
- имеют измеряемое количественное выражение: массу, объем, плотность, концентрацию, интенсивность, мощность, стоимость;
- при изменениях во времени подчиняются фундаментальным законам сохранения.

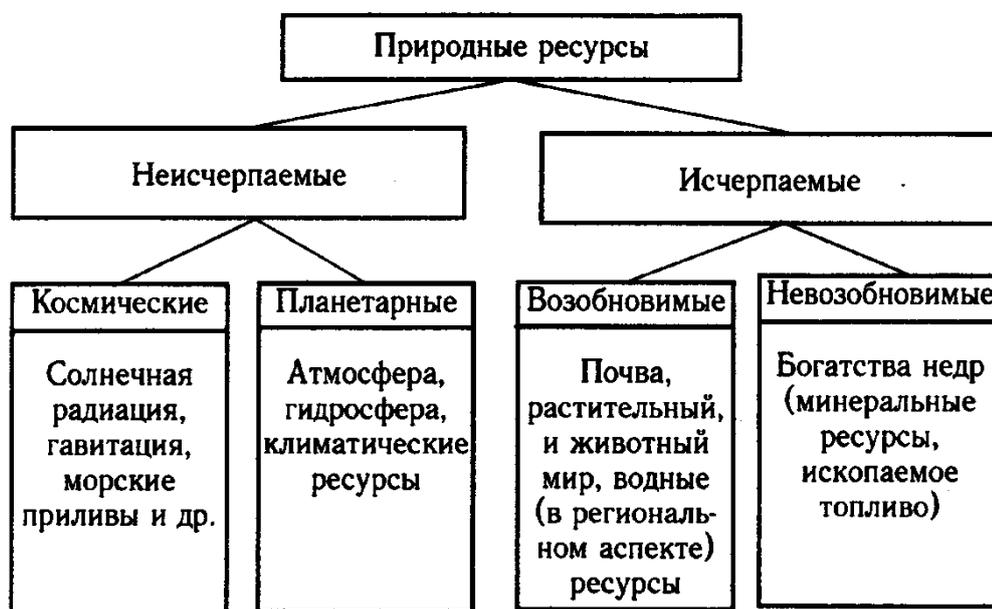


Рис. 12. Схема классификации природных ресурсов

Все естественные материальные и энергетические ресурсы, используемые человеком, принято называть природными ресурсами. При этом часто забывают, что большинство из них является ресурсами не только для человека, но в основном и в первую очередь ресурсами живой природы.

Классификация ресурсов. Существует несколько классификаций природных ресурсов.

Естественная классификация основана на разделении ресурсов по компонентам природной среды: земельные, минеральные, водные, климатические, растительные, животного мира и т.п.

В хозяйственной классификации ведущее значение имеет отраслевая принадлежность: ресурсы топливно-энергетического комплекса, металлургии, химической промышленности, сельского хозяйства, лесоперерабатывающей промышленности и т.д.

С эколого-экономической точки зрения важна классификация природных ресурсов по признакам исчерпаемости. К практически неисчерпаемым (в пределах времени существования техносферы) часто относят космические (солнечную радиацию, гравитацию) и планетарные ресурсы (наличие атмосферы, гидросферы, геотермальной энергии). Однако в конкретных земных и, тем более, техносферных условиях действует закон ограниченности (исчерпаемости) всех природных ресурсов.

Возобновимые ресурсы - это вещества и силы, которые создаются на Земле благодаря текущему потоку солнечной энергии: тепло, атмосферная влага, вода осадков и всех пресных вод, течение рек и гидроэнергия, энергия ветров, волн и течений, почва, все живые организмы, биосфера, наконец, сам человек. Для различных возобновимых, особенно для биологических ресурсов, существуют пределы скорости изъятия и степени истощения, после превышения которых уже невозможно возобновление, так как нарушается его естественный режим. Чаще всего это относится к численности популяции или биоразнообразию экосистем. Но это может быть отнесено и к биосфере в целом [8].

Разумеется, исчерпаемы и все невозобновимые ресурсы. К ним относится подавляющее большинство полезных ископаемых: горные материалы, руды, минералы, осадочные породы, ископаемое топливо. Правда, некоторые минеральные ресурсы и сейчас медленно образуются при геохимических процессах в недрах, глубинах океана или на поверхности земной коры - залежи солей, руды переходных металлов, железомарганцевые конкреции, известняки, продукты выветривания, но не уголь и углеводороды. В отношении полезных ископаемых большое значение имеют доступность и

качество ресурса, а также количественное соотношение между оцененными потенциальными, реальными разведанными и эксплуатационными запасами.

Принципиальное отличие техносферы от биосферы заключается в том, что биосфера использует исключительно контролируемые ею возобновимые ресурсы, тогда как человек в техносфере, кроме захвата значительной части биосферных ресурсов, использует и огромную массу невозобновимых ресурсов, значительная часть которых не нужна биоте биосферы, но влияет на ее функционирование.

Несмотря на указанное отличие ресурсы биосферы и техносферы непрерывно взаимодействуют между собой. Преждевременное изъятие погребенных в литосфере веществ и ввод их в оборот нарушает оптимальный баланс круговорота веществ в природе. Кроме того, использование невозобновимых ресурсов всегда влечет за собой цепь частных последствий, важных для биосферы: преобразование ландшафтов, изъятие площадей природных экосистем, деградацию почв, изменение распределения грунтовых вод и др.

Хотя человечество на протяжении всей своей истории сталкивается с ограниченностью природных ресурсов, оно до сих пор не осознало последствий их бесконтрольного использования. В настоящее время экономика мирового хозяйства чрезвычайно природоемка, что и обуславливает техногенный тип развития и истощение природных ресурсов.

Выводы по главе IV

Рассмотрены вопросы производительность труда и работоспособность человека. А также чрезвычайные ситуации и техносфера.

ЗАКЛЮЧЕНИЕ

Целью выпускной работы является проектирование локальной компьютерной сети для школы №3 на базе оборудования Cisco.

В результате выполнения выпускной квалификационной работы получены следующие основные результаты:

- изучены теоретические основы построения локальных сетей;
- разработана функциональная схема локальной вычислительной сети для школы;
- планирована структура вычислительной сети;
- разработана структура локальной компьютерной сети школы;
- определены основные административные блоки;
- рассмотрены вопросы защиты информации в сети и отказоустойчивость.

Реализация предложенного проекта позволит сократить бумажный документооборот внутри школы, повысить производительность труда, сократить время на обработку информации. Как следствие, образуются дополнительные временные ресурсы для разработки и реализации новых инновационных проектов.

По результатам данного проекта и подключением к глобальной сети Internet школа получает практически неограниченные информационные возможности, оперативное получение новостей.

ЛИТЕРАТУРА

1. Каримов И.А.: Постановление Президента Республики Узбекистан «О мерах по дальнейшему внедрению развитию современных информационно-коммуникационных технологий» / Собрание законодательства Республики Узбекистан, 2012 г., № 13, стр. 139. Ташкент, 2012.
2. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. Учебник. –4-е издание. СПб. Питер. 2009 г.
3. Бройдо В.Л. Вычислительные системы, сети и телекоммуникации. СПб.: Питер. 2003.
4. Бройдо В.Л. Архитектура ЭВМ и вычислительных систем. Учебник. 2.е издание. М.: Форум. 2008.
5. Ватаманюк А. Создание, обслуживание и администрирование сетей. СПб.: Питер. 2010.
6. Новиков Ю.В., Карпенко Д.Г. Аппаратура локальных сетей: Функции, выбор, разработка. – М.: ЭКОМ, 1998. – 288 с.
7. Буза М.К. Архитектура компьютеров. Учебник для вузов.- Минск.Новое знание.2006,-559с.
8. Русак О.Н., Малаян К.Р., Занько Н.Г. Безопасность жизнедеятельности. Учебное пособие. Омега. С. Петербург-М.-Краснодар. 2004
9. www.ziyonet.uz
10. www.intuit.ru
11. <http://www.osp.ru/lan/2005/11/030.htm>
12. <http://www.xserver.ru/computer/protokol/razn/13/>
13. <http://www.osp.ru/win2000/2001/07/010.htm>

ПРИЛОЖЕНИЕ

НАСТРОЙКА ОТКАЗОУСТОЙЧИВОГО СЕРВЕРА НА БАЗЕ ТОМСАТ

Настройка DRBD

В первую очередь следует настроить DRBD и убедиться, что он работает правильно.

/dev/sda – это системный диск, на котором установлена ОС,

/dev/sdb, которое предполагается использовать в качестве устройства DRBD, постоянно реплицируя его с аналогичным диском на другой ноде.

```
# fdisk -l
```

```
Disk /dev/sda: 8589 MB, 8589934592 bytes
255 heads, 63 sectors/track, 1044 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
   Device Boot      Start         End      Blocks   Id
System
/dev/sda1    *           1           978     7855753+   83
Linux
/dev/sda2                979        1043     522112+   82
Linux swap / Solaris
Disk /dev/sdb: 8589 MB, 8589934592 bytes
255 heads, 63 sectors/track, 1044 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
Disk /dev/sdb doesn't contain a valid partition table
```

DRBD управляется с помощью одного конфигурационного файла – /etc/drbd.conf. Структуру файла можно представить тремя секциями.

Global section – секция может быть описана только один раз и содержит в себе глобальные настройки, распространяемые на все ресурсы.

Common section – секция полезна, если используется несколько ресурсов и необходимо предоставлять ряд настроек для конкретных ресурсов.

Resource section – секция описания ресурса, в ней также должна быть подсекция on host, для каждой кластерной ноды.

```
# vim /etc/drbd.conf
```

```
global { usage-count yes; }
common { syncer { rate 20M; } }
resource r0 {
    protocol C;
    startup {

    }
    disk {
        on-io-error detach;
    }
    net {
    }
    on node1.company.ru {
        device /dev/drbd0;
        disk /dev/sdb;
        address 192.168.146.150:7789;
        meta-disk internal;
    }
    on node2.company.ru {
        device /dev/drbd0;
        disk /dev/sdb;
        address 192.168.146.134:7789;
        meta-disk internal;
    }
}
```

Конфигурационный файл /etc/drbd.conf

minor-count	По умолчанию модуль DRBD загружается с minor-count 32, если используется много устройств и номеров не хватает их можно явно указать здесь;
dialog-refresh	Обновление экрана каждые n секунд, может быть полезно при подключение к серверу по последовательному интерфейсу;
disable-ip-verification	Позволяет отключить одну из проверок drbdadm;

usage-count	Участвовать в глобальном подсчете пользователей DRBD или нет;
common {...}	Секция, опции которой наследуют все ресурсы;
syncer	Позволяет задать пропускную способность при синхронизации устройств по сети, разработчики рекомендуют использовать 30% от возможностей сети. Например, если у вас 100 Мбит сеть, то $100 * 0.3 = 30$ Мб;
resource r0 {...}	Секция описания ресурса;
protocol	Задаёт протокол для DRBD, подробнее о них написано выше;
handlers {...}	Задаёт обработчики, например что делать в случае потери соединения первичной ноды;
startup { ...}	Секция для опций используемых в процессе загрузки DRBD;
wfc-timeout	Ожидание таймаута соединения;
degr-wfc-timeout	Ожидание таймаута подключения, в случае если в кластере одна рабочая нода;
wait-after-sb	Ожидание после split brain, ситуация когда все ноды могут попытаться запустить сервис одновременно, думая что другие ноды недоступны. В свою очередь это может повлечь за собой повреждение данных;
disk { ...}	Секция с настройками оповещения верхних уровней, если замечено, что происходят I/O ошибки при обращении к диску;
on-io-error detach	Нода перестает работать с носителем данных если на нем происходят I/O ошибки;
fencing	Процесс блокировки ресурсов с нод статус которых сомнителен;
net {...}	Секция задаёт различные опции сети, такие как размеры

	буфера, максимальное число запросов обрабатываемых DRBD. В обычных ситуациях значений по умолчанию достаточно;
on host { ... }	Секция описания нод;
device	Указывает на устройство DRBD, они расположены в /dev/ и начинаются с 0;
disk	Физический диск или раздел, который будет задействован в работе DRBD;
address	IP-адрес и порт этой ноды, нужно указывать именно ее IP-адрес а не shared IP;
meta-disk	Meta данные могут храниться на отдельном разделе/диске а могут на диске описанном в опции disk;
max-buffers	Число буферов используемых для хранения данных, пока те записываются на диск;
max-epoch-size	Максимальное число запросов на запись. Должно соответствовать max-buffers;
timeout ping-int	Эти значения можно повысить если наблюдаются обрывы связи;

```
[root@node1 ~]# drbdadm create-md r0
```

```
[root@node2 ~]# drbdadm create-md r0
```

```
v08 Magic number not found
v07 Magic number not found
v07 Magic number not found
v08 Magic number not found
Writing meta data...
initialising activity log
NOT initialized bitmap
New drbd meta data block sucessfully created.
success
```

После запуска DRBD на первичной ноде, она перейдет в режим ожидания вторичной. И не запустится пока не получит от нее отклик.

```
*****
DRBD's startup script waits for the peer node(s) to appear.
- In case this node was already a degraded cluster before the
  reboot the timeout is 0 seconds. [degr-wfc-timeout]
- If the peer was available before the reboot the timeout will
  expire after 0 seconds. [wfc-timeout]
  (These values are for resource 'r0'; 0 sec -> wait forever)
To abort waiting enter 'yes' [ 58]:
```

```
[root@node2 ~]# service drbd start
```

```
[root@node1 ~]# cat /proc/drbd
```

```
version: 8.0.13 (api:86/proto:86)
GIT-hash: ee3ad77563d2e87171a3da17cc002ddfd1677dbe build by
builddsvn@c5-i386-
build, 2008-10-02 13:31:44
 0: cs:Connected st:Secondary/Secondary
ds:Inconsistent/Inconsistent C r---
   ns:0 nr:0 dw:0 dr:0 al:0 bm:0 lo:0 pe:0 ua:0 ap:0
   resync: used:0/61 hits:0 misses:0 starving:0 dirty:0
changed:0
   act_log: used:0/127 hits:0 misses:0 starving:0 dirty:0
changed:0
```

```
0: cs:Connected st:Secondary/Secondary ds:Inconsistent/Inconsistent C r---
```

st: означает статус, обе ноды в secondary режиме.

Затем необходимо node1 перевести в primary, делается это командой:

```
[root@node1 ~]# drbdadm -- --overwrite-data-of-peer primary r0
```

После этого начнется процесс синхронизации нод.

Запустив 'watch cat /proc/drbd' на отдельной консоли можно в реальном времени наблюдать за процессом синхронизации разделов.

```
[root@node1 ~]# watch cat /proc/drbd
```

```
Every 2.0s: cat /proc/drbd
```

```
Sun Apr 26 20:04:58
```

```
2014
```

```
version: 8.0.13 (api:86/proto:86)
```

```
GIT-hash: ee3ad77563d2e87171a3da17cc002ddfd1677dbe build by  
buildsvn@c5-i386-
```

```
build, 2008-10-02 13:31:44
```

```
0: cs:SyncSource st:Primary/Secondary ds:UpToDate/Inconsistent C r---
```

```
ns:1936384 nr:0 dw:0 dr:1936384 al:0 bm:118 lo:0 pe:0 ua:0 ap:0
```

```
[===>.....] sync'ed: 23.1% (6300/8191)M
```

```
finish: 0:09:28 speed: 11,304 (10,244) K/sec
```

```
resync: used:0/61 hits:120905 misses:119 starving:0 dirty:0 changed:119
```

```
act_log: used:0/127 hits:0 misses:0 starving:0 dirty:0 changed:0
```

После завершения синхронизации нужно убедиться, что статус устройства изменился.

```
[root@node1 ~]# cat /proc/drbd
```

```
version: 8.0.13 (api:86/proto:86)
```

```
GIT-hash: ee3ad77563d2e87171a3da17cc002ddfd1677dbe build by buildsvn@c5-i386-  
build, 2008-10-02 13:31:44
```

```
0: cs:Connected st:Primary/Secondary ds:UpToDate/UpToDate C r---
```

```
ns:8388316 nr:0 dw:0 dr:8388316 al:0 bm:512 lo:0 pe:0 ua:0 ap:0
```

```
resync: used:0/61 hits:523758 misses:512 starving:0 dirty:0 changed:512
```

```
act_log: used:0/127 hits:0 misses:0 starving:0 dirty:0 changed:0
```

Также, статус можно посмотреть с помощью команды `drbdadm`.

```
[root@node1 ~]# drbdadm dstate r0
```

```
UpToDate/UpToDate
```

```
[root@node2 ~]# drbdadm dstate r0
```

```
UpToDate/UpToDate
```

Ресурс полностью синхронизирован и готов к работе.

Теперь необходимо создать файловую систему на диске.

```
[root@node1 ~]# mkfs -t ext3 /dev/drbd0
```

И точку монтирования для диска.

```
[root@node1 ~]# mkdir /mnt/drbd0
```

Диск монтируется командой:

```
[root@node1 ~]# mount /dev/drbd0 /mnt/drbd0/
```

Запросив статус DRBD, можно выяснить смонтировано ли устройство или нет.

```
[root@node1 ~]# service drbd status
```

```
drbd driver loaded OK; device status:
version: 8.0.13 (api:86/proto:86)
GIT-hash: ee3ad77563d2e87171a3da17cc002ddfd1677dbe build by
buildsvn@c5-i386-
build, 2008-10-02 13:31:44
      m:res cs      st      ds      p mounted  fstype
0:r0 Connected Primary/Secondary UpToDate/UpToDate C /mnt/drbd0
      ext3
```

Для проверки работоспособности DRBD необходимо создать файл:

```
[root@node1 ~]# echo 'test content' > /mnt/drbd0/test
```

Отмонтировать устройство

```
[root@node1 ~]# umount /mnt/drbd0/
```

Понизить роль node1 до вторичной ноды

```
[root@node1 ~]# drbdadm secondary r0
```

повысить роль node2 до первичной ноды

```
[root@node2 ~]# drbdadm primary r0
```

Создать директорию, куда будет монтироваться устройство. Очевидно, раз программное обеспечение на обеих нодах будет выполнять одну работу с

одними файлами конфигурации, то расположение контента должно быть идентичным.

```
[root@node2 ~]# mkdir /mnt/drbd0
```

Затем, следует монтировать устройство

```
[root@node2 ~]# mount /dev/drbd0 /mnt/drbd0
```

Проверить статус, можно командой:

```
[root@node2 ~]# service drbd status
```

```
drbd driver loaded OK; device status:
version: 8.0.13 (api:86/proto:86)
GIT-hash: ee3ad77563d2e87171a3da17cc002ddfd1677d8e build by
buildsvn@c5-i386-
build, 2008-10-02 13:31:44
m:res cs      st          ds          p mounted  fstype
0:r0 Connected Primary/Secondary UpToDate/UpToDate C /mnt/drbd0
ext3
```

Если файл существует, то значит настройка выполнена правильно:

```
[root@node2 ~]# cat /mnt/drbd0/test
```

```
Text content
```

Теперь следует вернуть обратно роль первичного сервера node1

```
[root@node2 ~]# umount /mnt/drbd0/
```

```
[root@node2 ~]# drbdadm secondary r0
```

```
[root@node1 ~]# drbdadm primary r0
```

```
[root@node1 ~]# mount /dev/drbd0 /mnt/drbd0
```

Настройка Heartbeat

Необходимо скопировать шаблоны файлов конфигурации в /etc/ha.d/

```
# cp /usr/share/doc/heartbeat-2.1.3/{ha.cf,authkeys,haresources} /etc/ha.d/
```

```
Text content
```

Конфигурационные файлы Heartbeat.

ha.cf	Главный конфигурационный файл;
haresources	Файл ресурсов;
authkeys	Файл аутентификации.

```
[root@node1 ~]# uname -n
```

```
node1.company
```

```
[root@node2 ~]# uname -n
```

```
node2.company
```

Конфигурационный файл /etc/ha.d/authkeys

В файле конфигурации выбирается режим аутентификации и указывается секретная фраза, по которой она будет происходить. Далее на этот файл необходимо установить право на чтение только пользователю root, для этого выполняется команда `chmod`, указанная ниже.

```
# vim/etc/ha.d/authkeys
```

```
auth 2  
2 sha1 NoOneKnowsIt
```

```
# chmod 600 /etc/ha.d/authkeys
```

Конфигурационный файл /etc/ha.d/ha.cf

Это главный конфигурационный файл и поведение Heartbeat задается здесь.

```
# vim /etc/ha.d/ha.cf
```

```
logfacility local0  
keepalive 2  
deadtime 30  
initdead 120  
bcast eth0  
auto_failback on  
node node1.company.ru  
node node2.company.ru  
respawn hacluster /usr/lib/heartbeat/ipfail  
use_logd yes  
logfile /var/log/ha.log  
debugfile /var/log/ha-debug.log
```

debugfile	Задаёт расположение файла для записи отладочной информации;
logfile	Задаёт расположение файла для записи всей остальной информации;
logfacility	Опция для Syslog;
keepalive	Как часто проверять состояние другой ноды, указывается в секундах;
deadtime	Как быстро нужно решить, что удаленная нода вышла из строя, указывается в секундах;
warntime	Через какой промежуток времени после последнего ответа от удаленной ноды генерировать предупреждение;
initdead	На некоторых серверах и ОС, сетевой интерфейс начинает работать правильно только после перезагрузки, для корректной обработки ситуации введен дополнительный счетчик;
udpport UDP	порт для broadcast/unicast запросов;
baud	Скорость для последовательного соединения;
serial	Устройство для последовательного соединения;
bcast	Через какой интерфейс отправлять broadcast-запросы Heartbeat;
mcast	Интерфейс для multicast-запросов, если используется;
ucast	Интерфейс для unicast-запросов, если используется;
auto_failback	Переключаться ли обратно на primary node после ее восстановления: on – переключаться; off – secondary node продолжит работать как primary node; legacy – включить auto_failback в системах, где все ноды еще не поддерживают опцию auto_failback;
stonith	Опция используется только в первой версии Heartbeat;

watchdog	Позволяет включить Watchdog timer, если наш собственный Heartbeat не ответит в течение минуты то сервер будет перезагружен;
node	Задаёт ноду;
ping	Позволяет пинговать сетевое устройство, например свой шлюз, используется для определения работоспособности сети;
respawn	Процессы стартуют и останавливаются вместе с Heartbeat, ipfail определяет какая нода имеет лучшее сетевое подключение, в случае если нода теряет сетевое подключение или испытывает большие затруднения в передаче трафика, ipfail заметит это и роль primary node может быть передана другой ноде;
apiauth	API authorization directive;
debug	Задаёт уровень отладки;
use_logd	Использовать ли logging daemon;
conn_logd_time	Интервал переподключения к logd;
compression	Здесь указывается модуль компрессии.

После того, как файл конфигурации готов, необходимо создать log-файлы.
`# touch /var/log/{ha.log,ha-debug.log}`

Конфигурационный файл /etc/ha.d/haresources

В этом файле описываются ресурсы для управления с помощью Heartbeat.
 Содержимое файла можно прочитать вот так:

```
node1.company.ru IPaddr::192.168.146.140/24 drbddisk::r0 \
Filesystem::/dev/drbd0::/mnt/drbd0::ext3::defaults tomcat
```

При старте Heartbeat, node1 будет primary node с shared IP-адресом 192.168.146.140, drbddisk – это диск, описанный в ресурсе r0 (/etc/drbd.conf),

устройство /dev/drbd0, файловая система /mnt/drbd0, это именно та файловая система, которая будет доступна для приложений, используется тип файловой системы ext3 с опциями по умолчанию. После монтирования ФС необходимо запустить сервис tomcat.

Как видно, именно, здесь задается shared IP-адрес, это тот самый IP-адрес, по которому пользователи должны обращаться к сервисам.

Если первичная нода станет недоступна, то этот IP-адрес будет назначен вторичной ноде, которая станет первичной, и начнет обрабатывать запросы.

Такой подмены пользователи не заметят, и сервис будет предоставляться без перебоев, а именно это так и нужно.

После того, как файлы конфигурации Heartbeat на обеих нодах будут готовы, можно запускать сервис.

Кластер почти готов, поскольку DRBD и Heartbeat готовы к работе, самое время установить Apache tomcat.

Установка ТОМСАТ

Непосредственно перед началом установкой tomcat необходимо поставить виртуальную машину java:

```
# yum install java
```

Далее следует скачать сам apache-tomcat:

```
# wget http://mirror.metrocast.net/apache/tomcat/tomcat-6/v6.0.32/bin/apache-tomcat-6.0.32.tar.gz
```

Затем распаковать скаченный архив в /opt/ tomcat

На этом установка веб сервера завершена и необходимо перейти к его настройке.

Настройка TOMCAT

В файле tomcat-users.xml, в блоке <tomcat-users> добавляются строки:

```
# vim /opt/tomcat/conf
```

```
<!--
  <role rolename="tomcat"/>
  <role rolename="role1"/>
  <user username="tomcat" password="tomcat"
roles="tomcat"/>
  <user username="both" password="tomcat"
roles="tomcat,role1"/>
  <user username="role1" password="tomcat"
roles="role1"/>
-->

<role rolename="admin-gui"/>
  <role rolename="manager-gui"/>
  <role rolename="rc-web-admin"/>
  <user username="admin" password="password"
roles="admin-gui,manager-gui,rc-web-admin"/>
```

Теперь необходимо установить размера выделяемой памяти для java

```
# vim /opt/tomcat/bin/catalina.sh
```

```
# OS specific support. $var _must_ be set to either true
or false.

CATALINA_OPTS="-Xms256m -Xmx1024m"
cyqwin=false
```

Xms - задает минимальный размер кучи

Xmx - задает максимальный размер кучи

Секрет состоит в том, что по умолчанию объем максимально выделяемой памяти равняется 64Мб. Разумеется, это катастрофически мало для серверного приложения и, запуская систему со значениями по умолчанию, оперирование в памяти с файлами объемом в пару десятков мегабайт будет приводить к останову сервлета и зависание сервера.

Далее необходимо найти фразу **Connector port="8080"** в файле server.xml 8080 – это порт, который использовался при установке Tomcat и при желании его можно изменить. Что бы правильно отображалась кириллица на сайте, добавляется текст:

```
# vim /opt/tomcat/conf/server.xml
```

```
<Connector port="80" protocol="HTTP/1.1"
           connectionTimeout="20000" URIEncoding="UTF-
8"
```

Затем создаётся виртуальный хост для чего перед последними строчками `</Engine>` `</Service>` `</Server>` в файле `server.xml` необходимо вставить следующее:

```
<Host name="company.ru" debug="0" appBase="/mnt/drbd0"
unpackWARs="true" autoDeploy="true">
<Alias>www.company.ru</Alias>
<Context path="" docBase="examples" debug="0" reloadable="true">
</Context>
</Host>
```

Теперь необходимо создать скрипт запуска сервиса в `/etc/init.d/`

```
vim /etc/init.d/tomcat
```

```
#!/bin/bash
#
# Init file for SixSigns Tomcat server
#
# chkconfig: 2345 55 25
# description: SixSigns Tomcat server
#
# Source function library.
. /etc/init.d/functions
RUN_AS_USER=root # Adjust run user here
CATALINA_HOME=/opt/tomcat
}
```

```

start() {
    echo "Starting Razuna Tomcat: "
    if [ "$USER" != "$RUN_AS_USER" ]; then
        su - $RUN_AS_USER -c "$CATALINA_HOME/bin/startup.sh"
    else
        $CATALINA_HOME/bin/startup.sh
    fi
    echo "done."
}
stop() {
    echo "Shutting down Razuna Tomcat: "
    if [ "$USER" != "$RUN_AS_USER" ]; then
        su - $RUN_AS_USER -c "$CATALINA_HOME/bin/shutdown.sh"
    else
        $CATALINA_HOME/bin/shutdown.sh
    fi
    echo "done."
}
case "$1" in
    start)
        start
        ;;
    stop)
        stop
        ;;
    restart)
        stop
        sleep 10
        #echo "Hard killing any remaining threads.."
        #kill -9 `cat $CATALINA_HOME/work/catalina.pid`
        start
        ;;
    *) darwin=false
os400=false
case "`uname`" in
    CYGWIN*) cygwin=true;;
    Darwin*) darwin=true;;
    OS400*) os400=true;;
esac

```

Далее для проверки настройки нужно скопировать в каталог /mnt/drbd0/ приложение примеров (которое по умолчанию размещено в каталоге %CATALINA_HOME%\webapps\examples) и убедиться, что оно работает по адресу <http://www.company.ru/examples/servlets>. Разумеется, для тестирования в файле HOSTS клиентской операционной системы нужно создать записи вида

```
192.168.149.140 www.company.ru
```

```
192.168.149.140 www.company.ru
```

Файл hosts в Linux находится в /etc/, в Windows

```
C:\WINDOWS\system32\drivers\etc
```

Тестирование

Производится запуск Heartbeat, который в свою очередь запустит Tomcat.

```
[root@node1 ~]# service heartbeat start
```

```

Starting High-Availability services:
2009/04/26_21:29:04 INFO: Resource is stopped
[ OK ]

```

В выводе команды `ifconfig` можно заметить, что был создан сетевой алиас (`eth0:0`), это виртуальный интерфейс с назначенным ему IP-адресом. В случае выхода первичной ноды, он будет переназначен на вторичной, и она став первичной будет обрабатывать запросы.

```
[root@node1 ~]# ifconfig
```

```
eth0  Link encap:Ethernet HWaddr 00:0C:29:77:9C:9C
      inet addr:192.168.146.150 Bcast:192.168.146.255 Mask:255.255.255.0
      inet6 addr: fe80::20c:29ff:fe77:9c9c/64 Scope:Link
      UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
      RX packets:2743855 errors:0 dropped:0 overruns:0 frame:0
      TX packets:6180468 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:1000
      RX bytes:203601157 (194.1 MiB) TX bytes:691044303 (659.0 MiB)
      Interrupt:59 Base address:0x2000
eth0:0 Link encap:Ethernet HWaddr 00:0C:29:77:9C:9C
      inet addr:192.168.146.140 Bcast:192.168.146.255 Mask:255.255.255.0
      UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
      Interrupt:59 Base address:0x200
```

```
root@node2 ~]# service heartbeat start
```

Теперь надо попробовать в браузере обратиться к веб-серверу. Должна открыться тестовая страница. Затем надо убедиться, что при недоступности одной ноды работу будет выполнять вторая.

Нужно просто отключить Heartbeat на `node1`, в свою очередь он выключит веб-сервер и перейдет в режим `secondary node`.

```
[root@node1 ~]# service heartbeat stop
```

Еще раз запрашивается страница в браузере и все продолжает работать. Виртуальный интерфейс переместился на `Node2`, там же запустился Tomcat и начал сразу же обрабатывать запросы. Вторичная нода стала первичной.

```
[root@node2 ~]# service drbd status
```

```
drbd driver loaded OK; device status:
version: 8.0.13 (api:86/proto:86)
GIT-hash: ee3ad77563d2e87171a3da17cc002ddfd1677dbe build by buildsvn@c5-i386-
build, 2008-10-02 13:31:44
m:res cs          st          ds          p  mounted  fstype
0:r0  Connected  Primary/Secondary UpToDate/UpToDate C /mnt/drbd0 ext3
```

```
[root@node2 ~]# ifconfig
```

```
eth0  Link encap:Ethernet HWaddr 00:0C:29:25:04:55
      inet addr:192.168.146.134 Bcast:192.168.146.255 Mask:255.255.255.0
      inet6 addr: fe80::20c:29ff:fe25:455/64 Scope:Link
      UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
      RX packets:6180400 errors:2 dropped:2 overruns:0 frame:0
      TX packets:2742239 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:1000
      RX bytes:693847272 (661.7 MiB) TX bytes:200769641 (191.4 MiB)
      Interrupt:59 Base address:0x2000
eth0:0 Link encap:Ethernet HWaddr 00:0C:29:25:04:55
      inet addr:192.168.146.140 Bcast:192.168.146.255 Mask:255.255.255.0
      UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
      Interrupt:59 Base address:0x2000
```

После того как node1 будет починена ее можно вернуть на первичную роль.

```
[root@node1 ~]# service heartbeat start
```

```
[root@node2 ~]# service heartbeat stop
```

```
[root@node2 ~]# service heartbeat start
```

Далее проводится более жесткий тест - имитация потери подключения ноды к сети. Для этого выдергивается сетевой кабель из node1, если это физический сервер или просто набирается команду ниже:

```
[root@node1 ~]# ifdown eth0
```

В течение нескольких секунд виртуальный интерфейс должен мигрировать на node2 и работа веб-сервера продолжится. Затем нужно вернуть подключение на node1:

```
[root@node1 ~]# ifup eth0
```

Через несколько секунд node1 опять станет primary node и начнет обслуживать подключения, потому что “auto_fallback on”.