Министерство образования и науки Российской Федерации
Санкт-Петербургский политехнический университет Петра Великого
Институт компьютерных наук и технологий

Работа допущена к защите

Руководитель ООП

_____А.А. Ефремов

«___»_____ 2018г.

**ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА БАКАЛАВРА**

# Модернизация информационной инфраструктуры предприятия

по направлению 09.03.02 Информационные системы и технологии

Выполнил
студент гр. B43503/6 А.А. Попов
*<подпись>*

Руководитель ВКР
доцент, к.т.н В.Е. Баранов
*<подпись>*

Консультант
по нормконтролю *<подпись>*

Санкт-Петербург
2018

**РЕФЕРАТ**

с.68

**МОДЕРНИЗАЦИЯ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ ПРЕДПРИЯТИЯ**

СЕТЕВАЯ ИНФРАСТРУКТУРА, СТРУКТУРИРОВАННАЯ КАБЕЛЬНАЯ СЕТЬ, ЛОКАЛЬНО-ВЫЧИСЛИТЕЛЬНАЯ СЕТЬ, СЕТЕВОЕ ОБОРУДОВАНИЕ, СЕРВЕРНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ, LAN, TCP\IP

В данной работе выполнен проект модернизации сетевой инфраструктуры предприятия в соответствии с масштабами и задачами организации, выбраны наиболее актуальные и оптимальные решения относительно создания кабельной сети и использования программного обеспечения для серверов и пользователей. Показаны типовые решения вопросов информационной безопасности, быстродействия и масштабируемости сети.

**ABSTRACT**

p. 68

NETWORK INFRASTRUCTURE, STRUCTURED CABLE NETWORK, LOCAL-AREA NETWORK, NETWORK HARDWARE, SERVER SOFTWARE, INFORMATION SECURITY, LAN, TCP\IP

In a result of work was made a project of modernization of the enterprise network infrastructure in accordance with the scale and business of the organization. The most relevant and optimal solutions for the creation of cable network and the use of software for servers and users, typical solutions of information security, network performance and scalability issues are shown.

# СОДЕРЖАНИЕ

## СПИСОК СПЕЦИАЛЬНЫХ АББРЕВИАТУР

СКС – структурированная кабельная система

ЛВС – локально-вычислительная сеть

ПО – программное обеспечение

АРМ – автоматизированные рабочие места

LAN – Local Area Network

TCP\IP – Transmission Control Protocol/Internet Protocol (Протокол управления передачей/Протокол Internet)

# ВВЕДЕНИЕ

Актуальность представленной работы обусловлена тем, что в современном мире ни одно предприятие от концерна мирового значения до маленького офиса на окраине города не обходится без использования компьютерных технологий для выполнения стоящих перед ним задач. Посредством компьютеров, объединенных в сети на локальном и далее на глобальном уровне, осуществляется обмен информацией, которая непосредственно относится к деятельности той или иной компании.

Объектом исследования является абстрактное предприятие, имеющее определенные производственные мощности, административный аппарат, филиалы и осуществляющее деловое взаимодействие с прочими предприятиями и фирмами, оказывающими необходимые для функционирования услуги.

Предметом исследования является информационная инфраструктура вышеописанного предприятия, а именно:

- структурированная кабельная система

- локально-вычислительная сеть

- серверное оборудование и программное обеспечение

- автоматизированные рабочие места пользователей

- безопасность и отказоустойчивость системы

- масштабируемость системы

Целью исследования является разработка проекта сетевой инфраструктуры отвечающего потребностям предприятия и требованиям безопасности, как информационной, так и непосредственно при эксплуатации системы, а также поэтапное описание работ по реализации данного проекта на месте.

В представленной работе решены следующие задачи:

1. Произведена оценка объемов работ необходимых для реализации проекта модернизации информационной инфраструктуры предприятия

2. Рассмотрены типовые решения, применяемые в настоящее время в данной области, выбраны наиболее оптимальные и подходящие для конкретного случая

3. Произведены расчеты предполагаемой нагрузки на сеть, приведен перечень используемых материалов, оборудования отвечающего за функциональность сети, программного обеспечения

4. Предусмотрены меры безопасности, оберегающие сеть от внешних атак, утечки данных, а также обеспечивающие безопасность пользователей.

5. Создан проект сети в соответствии с современными нормами и требованиями обеспечивающий возможность масштабирования инфраструктуры и дальнейшей модернизации без необходимости кардинальной переделки сети

6. Поэтапно рассмотрен процесс реализации проекта

В первой главе приводится описание условного предприятия, на котором будет проводиться модернизация, рассматриваются общепринятые в мире типовые решения по организации сетевой инфраструктуры, и на их основе принимается решение о том какой вариант наиболее подходит для воплощения на предприятии. Приводится описание плана модернизации и оценка

объемов работ, приводится перечень необходимых технологий, материалов, программного обеспечения и прочих мероприятий по обеспечению функционирования информационной инфраструктуры согласно плану.

Во второй главе подробно рассматриваются описанные в плане модернизации, представленном в первой главе, технические решения и описан процесс их внедрения. Приведено описание и технические характеристики устанавливаемого оборудования, кабельной инфраструктуры, описан процесс настройки программного обеспечения серверной и клиентской частей.

Третья глава отведена для подробного рассмотрения вопросов безопасного функционирования сети и управления пользователями и подключенными к сети устройствами. Безопасность сети обеспечивается как на виртуальном уровне – защита от внешних атак, вирусов, несанкционированной установки программного обеспечения пользователями, так и на физическом уровне, а именно недоступность сетевого оборудования для всех кроме представителей отдела информационных технологий на предприятии в компетенции которых обслуживание и настройка данного оборудования. Также сюда относится безопасное оборудование рабочих мест пользователей, исключающее случайные повреждения сетевых и питающих кабелей, а также мероприятия по электробезопасности.

Четвертая глава отведена под расчеты пропускной способности сети, нагрузки на оборудование и сервера, скорости передачи данных, производительности сети.

В заключении приведены выводы о проделанной работе.

# Глава 1. Проект модернизации информационной инфраструктуры предприятия

## 1.1 Описание условного предприятия

В качестве объекта исследования выбрано условное предприятие находящееся на территории РФ и обладающего рядом определенных параметров, позволяющих наиболее подробно рассмотреть технологии построения сетей и модернизации информационной инфраструктуры.

Данное предприятие занимается некоей производственной наукоемкой деятельностью, также самостоятельно осуществляет реализацию собственного продукта.

В состав предприятия входят следующие подразделения:

- Научные лаборатории

- Производственный цех

- Офис, включающий в себя несколько отделов:

Администрация, бухгалтерия, отдел конструкторских разработок, отдел разработчиков ПО, отдел закупок, технические службы. Более подробно офисные отделы будут рассмотрены во второй главе.

- Отдел информационных технологий

- Автопарк

- Подразделение охраны

Согласно вводной, на предприятии уже имеется некая локально-вычислительная сеть, которая не отвечает современным требованиям и масштабам организации, в связи с чем принимается решение о ее полной модер-

низации с обязательной возможностью дальнейшего масштабирования. Одним из условий проведения мероприятий модернизации  является безостановочность процессов проходящих на предприятии, то есть все работы должны проходить с минимумом помех для каждого из подразделений организации. Также дальнейшее обслуживание сети предполагает соответствие этому же принципу.

План модернизации информационной инфраструктуры должен включать наиболее оптимальные решения из имеющихся на данный момент на рынке. Типовые решения будут рассмотрены в следующем параграфе.

## 1.2 Понятия СКС и ЛВС. Типовые решения

Прежде чем приступать к описанию типовых решений при построении компьютерных сетей стоит более подробно остановиться на таких понятиях как СКС (структурированная кабельная система) и ЛВС (локально-вычислительная сеть), являющихся базовыми для сетевой инфраструктуры любого типа.

Структурированной кабельной системой называют совокупность коммутационных элементов, таких как кабели, разъемы, коннекторы, кроссовые панели и коммутационные шкафы. Также понятие СКС подразумевает методику совместного использования вышеперечисленных элементов, позволяющую создавать легкоуправляемые и масштабируемые структуры связи в сетях. [4, с.15]

Грамотно построенная СКС подразумевает оснащение каждого рабочего места и точки подключения оборудования на предприятии розетками электропитания, точкой подключения к локальной и телефонной сети. СКС организуется по принципу избыточности, что означает создание вышеперечисленных точек подключения во всех рабочих помещениях, даже если они на данный момент не задействованы в рабочем процессе. Это требует предусмотреть и рассчитать наперед, как именно будет использоваться то или иное помещение и организовать сеть таким образом, чтобы при подключении пользователей не возникало необходимости проводить дополнительные работы по монтажу силовых и коммутационных кабелей.

Система строится при помощи стандартных кабелей соединенных стандартными разъемами и коммутируемых по стандартным коммутационным схемам на стандартном оборудовании. Это позволяет при необходимости легко менять конфигурацию сети – добавлять компьютеры и целые рабочие места, подключать дополнительные сегменты сети, сетевое оборудование, менять соединения между пользователем и коммутатором, а также изымать или заменять оборудование без прерывания рабочего процесса.

Структурированная кабельная система устроена по иерархическому принципу – в основе лежит главная магистраль, от которой отходят многочисленные ответвления. Все соединения кабелей любого назначения осуществляются в изолированных от доступа посторонних распределительных пунктах (коммутационных центрах). Типичная иерархическая структура СКС выглядит следующим образом:

- горизонтальные кабельные подсистемы в пределах одного этажа

- вертикальные кабельные подсистемы в пределах здания от этажа к этажу

- магистральная кабельная подсистема в пределах территории предприятия от здания к зданию

- кабельная подсистема рабочих мест

Обязательным условием является использование кабелей с идентичными характеристиками в рамках одной кабельной линии. Согласно нормативам максимальная длина кабеля в горизонтальных кабельных подсистемах должна составлять не более 90 метров от одной точки подключения до другой во избежание потерь мощности или сигнала. Исключение составляют участки сети, построенные с использованием оптоволоконного кабеля. [4, с.35]

Выбор кабеля обусловлен необходимой пропускной способностью сети и электронагрузкой на оборудование. Подробные расчеты будут приведены в четвертой главе. Краткая характеристика используемых в типичных системах кабелей выглядит следующим образом:

- оптоволоконные трассы используются на городском уровне, и обычно с их помощью организуется взаимодействие сети предприятия с внешней сетью. В случае если бюджет на модернизацию сети позволяет, при помощи оптоволокна прокладываются магистральные кабельные подсистемы.

- витая пара 5 категории на основе медного провода, как экранированная, так и неэкранированная, используется при построении горизонтальных и вертикальных кабельных подсистем.

- электрический силовой кабель выбирается в соответствии с тем, какую нагрузку на сеть дает подключаемое к нему оборудование, точные данные рассчитываются исходя из характеристик конкретного подключаемого устройства.

Принципиальное отличие структурированной кабельной системы от локальной вычислительной сети заключается в том, что СКС по сути своей пассивна, она выполняет транспортную функцию для передачи информации. ЛВС же включает в себя разнообразное активное оборудование, подключаемое на уже смонтированную кабельную систему.

Локальная вычислительная сеть это совокупность компьютеров, каналов связи, сетевых адаптеров, работающих под управлением сетевой операционной системы и сетевого программного обеспечения, располагается на небольшой территории, обычно в пределах одной организации. Локальные сети используются повсеместно и организациями любого типа, в жилых домах, офисных центрах и отдельных офисах, в учебных заведениях, на предприятиях любого рода деятельности. Отличительной чертой локальной сети от всех остальных сетей является принадлежность к одной конкретной организации, которая осуществляет ее обслуживание, а также использует сеть для объединения всех компьютеров в отделах компании, совместного использования ресурсов (например, принтеров, сетевых хранилищ информации) и обмена информацией. ЛВС бывают проводными и беспроводными. На рассматриваемом в работе условном предприятии беспроводные сети будут представлены лишь фрагментарно, как участки общей сети. Основные каналы передачи информации будут основаны на проводной сети, как наиболее надежной и быстродействующей системе, так как отправка сигнала по проводам это более простой и надежный способ передачи информации, нежели по воздуху. [1, с.317]

Проводную ЛВС можно построить при помощи различных технологий передачи данных, основываясь на медном или оптоволоконном кабеле. Как правило, проводные ЛВС в настоящее время работают на скорости от 100 Мбит\с до 1 Гбит\с, впрочем, современные технологии позволяют организовать каналы передачи информации со скоростью до 100 Гбит\с. Вопрос целесообразности финансовых и трудозатрат на организацию подобной сети решается для каждой организации конкретно исходя из ее потребностей.

Наиболее распространенный стандарт, по которому создаются локальные вычислительные сети, имеет индекс IEEE 802.3 и называется Ethernet. Это значит что каждый компьютер, подключенный к ЛВС, передает данные согласно протоколу Ethernet на коммутирующее устройство, которое передает сигнал далее на магистральную линию связи. Сетевой коммутатор имеет определенное количество портов, рознящееся в зависимости от модели, к каждому порту подключается один компьютер или иное устройство (например, принтер). Работа коммутатора заключается в передаче информационных пакетов между подключенными к нему компьютерами и устройствами. Для правильной передачи пакета используется адрес устройства, прикрепленный к каждому передаваемому пакету.

Локальные сети могут быть организованы посредством нескольких топологических схем. Под топологией сети подразумевается способ соединения отдельных ее компонентов. Существует три основных топологических схемы:

- схема типа звезда

- схема типа кольцо

- схема типа общая шина

В данной работе будет рассмотрена только схема типа звезда, так как две другие схемы не обеспечивают достаточной надежности, безопасности, быстродействия и удобства монтажа и использования сети и являются в целом устаревшими.

Топологическая схема типа звезда представляет собой некий центральный узел, в зависимости от масштаба сети им может являться как сервер, так и сетевой коммутатор, вокруг которого объединены кабельной системой клиенты сети и обмен информацией между клиентами происходит через этот самый центральный узел. Подобная схема в рамках сети предприятия может быть продублирована неограниченное количество раз в соответствии с необходимостью подключения тех или иных устройств. На практике это означает, что от центрального коммутационного узла и серверного парка посредством магистральной шины подключаются коммутационные устройства, к которым подключаются как прямые клиенты, так и дальнейшие коммутационные устройства, что позволяет обеспечить быстродействие и удобство управления сетью, а также ее масштабируемость. [3, с.145]

Слабым местом данной топологической схемы является центральный коммутационный узел сегмента сети. В случае его недоступности или выхода из строя все подключенные к нему клиенты и устройства теряют связь друг с другом и с центральным сервером. Эта проблема решается при помощи программ мониторинга, отслеживающих состояние коммутационных устройств в реальном времени, а также в физической изоляции данных устройств от всех, кто не уполномочен их обслуживать.

Локальные сети также подразделяются на две модели:

- одноранговая сеть

- сеть типа клиент-сервер

Сети, использующие модель клиент-сервер наиболее распространены и актуальны на сегодняшний день. Целесообразно привести основной список терминов, относящихся к данной архитектуре.

- Прикладной программный интерфейс (Application Programming Interface, API) Набор функций и протоколов, обеспечивающих взаимодействие клиентов и серверов

- Клиент это объект, запрашивающий информацию по сети. Как правило, это персональный компьютер, рабочая станция, или оборудование, запрашивающие информацию у сервера

- Промежуточное программное обеспечение Набор драйверов, прикладных программных интерфейсов и прочего программного обеспечения, позволяющего улучшить взаимодействие между клиентским приложением и сервером

- Реляционная база данных, база данных, в которой доступ к информации ограничен выбором строк, удовлетворяющих определенным критериям поиска

- Сервер (как правило, высокопроизводительная рабочая станция), хранящий и обрабатывающий информацию, с которой взаимодействуют клиенты сети

- Язык структурированных запросов (Structured Query Language, SQL) язык для создания, управления и изменения баз данных и их массивов

Как предполагает термин, окружение клиент-сервер состоит из клиентов и серверов. Клиентские машины, как правило, представляют собой персональные компьютеры или рабочие станции, сервера, а также принтеры, системы IP телефонии, а также оборудование и прочую вычислительную технику.

Клиентская станция обычно имеет наиболее удобный графический интерфейс пользователя, предполагающий наличие окон, мыши, клавиатуры и возможность подключение прочих устройств типа флеш накопителей. Наиболее известные примеры подобных интерфейсов — интерфейсы операционных систем Microsoft Windows, Linux и MacOs. На их базе разработаны средства управления серверами и клиентскими машинами Клиентские приложения предполагают простоту использования и знакомые инструментальные средства, например, электронные таблицы.

Каждый сервер в окружении клиент-сервер предоставляет клиентам набор услуг. Высокопроизводительный сервер обеспечивает коллективный доступ нескольких клиентов к одной и той же базе данных. Помимо клиентов и серверов в окружение клиент-сервер входит сеть. Вычислительная модель клиент-сервер по определению является распределенной, типа «звезда». Пользователи, приложения и ресурсы располагаются на разных компьютерах и соединены общей локальной, сетью.

Требующий особого внимания сегмент ЛВС это сетевое оборудование. Существует определенный список устройств, относящихся к сетевому оборудованию. Ниже приведен список устройств опционально используемых при построении любой локальной сети с кратким описанием функционала. Концептуально он состоит из двух частей – активного сетевого оборудования и пассивного сетевого оборудования.

К активному сетевому оборудованию относят следующие устройства:

- сетевой адаптер — плата, которая устанавливается в компьютер и обеспечивает его подсоединение к локальной вычислительной сети

- повторитель (репитер) — прибор, как правило, с двумя портами, предназначенный для повторения сигнала с целью увеличения длины сетевого сегмента;

- концентратор (активный хаб, многопортовый репитер) — прибор с 4-32 портами, применяемый для объединения пользователей в сеть;

- мост — прибор с 2 портами, обычно используемый для объединения нескольких рабочих групп ЛВС, позволяет осуществлять фильтрацию сетевого трафика, разбирая сетевые (MAC) адреса;

- коммутатор (свитч) — прибор с несколькими (4-32) портами, обычно используемый для объединения нескольких рабочих групп ЛВС (иначе называется многопортовый мост);

- маршрутизатор (роутер) — используется для объединения нескольких рабочих групп ЛВС, позволяет осуществлять фильтрацию сетевого трафика, разбирая сетевые (IP) адреса;

- ретранслятор — для создания усовершенствованной беспроводной сети с большей площадью покрытия и представляет собой альтернативу проводной сети. По умолчанию устройство работает в режиме усиления сигнала и выступает в роли ретрансляционной станции, которая улавливает радиосигнал от базового маршрутизатора сети или точки доступа и передает его на ранее недоступные участки.

- медиаконвертер — прибор, как правило, с двумя портами, обычно используемый для преобразования среды передачи данных (коаксиал-витая пара, витая пара-оптоволокно);

- сетевой трансивер — прибор, как правило, с двумя портами, обычно используемый для преобразования интерфейса передачи данных (RS232-V35, AUI-UTP).

Пассивным сетевым оборудованием называют оборудование, не получающее питание от электрической сети или других источников, и выполняющее функции распределения или снижения уровня сигналов.

Например, кабельная система:

-кабель (коаксиальный и витая пара), вилка/розетка (RG58, RJ45, RJ11, GG45)

- патч-панель для коаксиальных кабелей (RG-58) и т. д.

Также, к пассивному оборудованию иногда относят оборудование трассы для кабелей: кабельные лотки, монтажные шкафы и стойки, телекоммуникационные шкафы. [1, с. 379]

Активное сетевое оборудование обменивается данными посредством протоколов маршрутизации, наборов правил, используемых маршрутизаторами для определения возможных маршрутов следования данных в локальной сети

. Применение протокола маршрутизации позволяет избежать ручного ввода всех допустимых маршрутов, что, в свою очередь, снижает количество ошибок, обеспечивает согласованность действий всех маршрутизаторов в сети, позволяет принимать адекватные меры безопасности на уровне ключевых узлов сети и серверов, увеличивает производительность и быстродействие сети, а также облегчает труд группы ИТ или прочих лиц уполномоченных обеспечивать связь между сегментами предприятия.

. Сетевые устройства поддерживающие вышеуказанные протоколы называются сетевыми коммутаторами (switch), подразделяются на управляемые и неуправляемые/

Управление сетевыми устройствами осуществляется при помощи серверного программного обеспечения силами группы информационных технологий.

Администрирование сети это меры по организации функционирования сети в соответствии со спецификой и запросами предприятия. При помощи средств администрирования – специального программного обеспечения, которое позволяет производить настройку, маршрутизацию, управление пользователями и устройствами, хранение и обработку данных, обеспечение мер безопасности и взаимодействие с другими сетями.

Осуществляет настройку и дальнейшее управление сетью при помощи сетевого оборудования и подобранного оптимального программного обеспечения лицо или подразделение ответственное за серверный парк, состояние сети, обычно системный администратор или группа информационных технологий.

Проект модернизации сетевой инфраструктуры составляется и утверждается с учетом принятых в конкретной организации требований к масштабам и задачам сети си-

лами группы информационных технологий, дирекции, технологов и лиц, ответственных за направления деятельности предприятия. [5, с. 57]

## 1.3 Составление проекта модернизации

Требования к сетевой инфраструктуре выдвигаются исходя из нужд подразделений компании и характера их взаимодействия. Технические задания на выполнение конкретных частей проекта составляются специалистами в сфере информационных технологий с учетом корпоративных и государственных нормативных актов и стандартов, руководствуясь выбором оптимальных и надежных решений соответствующих требованиям предприятия, после чего утверждаются дирекцией предприятия.

Планирование – первая и самая ответственная часть проекта модернизации. На данной стадии возможно предусмотреть все нюансы эксплуатации и обслуживания сетевого оборудования, а также поэтапного процесса монтажа и ввода в строй.

В рамках мероприятий планирования составляется подробная схема сети относительно зданий занимаемых предприятием, отделов и спецификой их работы. На основании данной схемы составляются технические задания, в соответствии с которыми будет производиться монтаж и настройка всех компонентов локальной сети. Составляются подробные схемы СКС, ЛВС и серверного оборудования, утверждается схема взаимодействия компонентов сети и нагрузка на оборудование.

В соответствии с рассчитанным уровнем предполагаемой нагрузки на сеть выбирается наиболее оптимальное оборудование и соответствующее его характеристикам и условиям эксплуатации программное обеспечение.

Выбор оборудования и компонентов сети должен учитывать все особенности каждого элемента сетевой инфраструктуры. Отдельно составляются технические задания на следующие этапы:

- Подбор необходимого инструмента, подготовительные работы

- Монтаж СКС, создание магистралей и точек подключения клиентов сети, а также пунктов коммутации

- Установка и настройка сетевого оборудования: коммутационных узлов, серверного парка, автоматизированных рабочих мест

- Настройка серверного парка, распределение ролей физических серверов, проверка безошибочного взаимодействия с элементами сети

- Установка и настройка пользовательских рабочих мест в соответствии с возможностью масштабирования и обеспечения мер безопасности, подключение компьютеров с периферийными устройствами, телефонии.

- Установка программного обеспечения, настройка обновлений, установка прав и ограничений. Проверка соответствия настройкам политик установленных на серверах. Обеспечение информационной безопасности.

- Криптография, цифровые подписи и прочие меры кибербезопасности, использование их в сетевой инфраструктуре предприятия. Способы аутентификация пользователей и клиентов сети.

- Безопасность и эргономика АРМ

# Глава 2. Реализация проекта

## 2.1 Создание СКС на предприятии

Структурированная кабельная система является основой будущей сети. Существует международный стандарт ISO/IEC 14763-1 согласно которому осуществляется проектирование, монтаж и обслуживание телекоммуникационных кабельных систем общего назначения подходящих для услуг разного вида (имеется в виду использование в различных технологических отраслях использующих кабельные сети и технику их использующую), построенных на основе медного или оптоволоконного кабеля. Стандарт специально разработан для использования в сетях охватывающих одно или несколько зданий с масштабируемым количеством точек подключения к оборудованию и конечным пользователям. На данный момент готовится уже третья редакция стандарта, получившая обозначение ISO/IEC 11801-1 состоящая из шести частей, каждая из которых регламентирует создание СКС для нужд различных по масштабу и нагрузке на сеть предприятий. [4, с. 64]

К этапу составления плана модернизации ИТ инфраструктуры условного предприятия относятся подразделы ISO/IEC 11801-1,2,3: общие требования к кабельным системам, использующим витую пару и оптоволокно, кабельные системы для корпоративных сетей в офисных зданий, кабельные системы для производственных помещений в целях автоматизации и контроля промышленных процессов.

Использование оптоволокна при организации сети предприятия не связанного с обработкой большого массива данных нецелесообразно виду дороговизны кабеля и сложности его монтажа. Оптоволокно в кабельной структуре предприятия будет представлено только входящим каналом связи, предоставляемым провайдером.

В случаях если расстояние между корпусами предприятия составляет более 100 метров в точке подключения конкретного здания к общей сети, или

же необходим канал связи с большой пропускной способностью, целесообразно использовать оптоволоконный кабель для прокладки внутренней магистрали. Но в данной работе этот вариант рассмотрен не будет.

Стандарт ISO/IEC 11801-1 включает 10 классов симметричных кабельных систем, отличающихся диапазоном частот и параметрами, определяющими качество сигнала. Полный список приводить нецелесообразно, стоит выделить лишь интересующий нас класс. Все внутренние магистрали, как главные, соединяющие сетевое оборудование, так и отдельные отрезки кабеля (линки), которыми к сети подключены конечные пользователи, планируется проложить, используя медную витую пару категории 5e. Это соответствует классу D, витая пара пятой категории позволяет обеспечить скорость передачи данных до 1 Гбит\с на расстоянии в 100 метров.

Согласно стандарту структурированная кабельная система подразделяется на подсистемы и функциональные элементы:

к горизонтальной подсистеме относятся

-телекоммуникационные разъемы

-кабели консолидации

-точки консолидации

-горизонтальные кабели

-распределительный пункт этажа

к магистральной подсистеме здания относятся

-магистраль здания

-распределительный пункт здания

к магистральной подсистеме комплекса относятся

-магистраль комплекса

-распределительный пункт комплекса

Также при создании плана СКС стандартом предписано учитывать условия среды, в которой используется сетевое оборудование и кабели. Классы среды разделены согласно роду деятельности организации эксплуатирующей СКС: коммерческий, легкая промышленность и промышленный. Также составлена классификация среды, учитывающая такие параметры как:

-механические условия

-проникающие условия

-климатические и химические условия

-электромагнитные условия

Грамотно построенная структурированная кабельная система позволяет решить многие задачи предприятия помимо организации локальной вычислительной сети и обеспечения сотрудникам доступа в Интернет. СКС используется для передачи различной информации и электропитания для всех устройств, как сетевых, так и прочих подключенных на рабочих местах:

- телекоммуникационных систем, включая беспроводные точки доступа, распределенные антенные системы;

- систем управления энергией, в том числе, освещением, распределением и учетом расхода электроэнергии;

- систем экологического контроля, например, температуры и влажности;

- систем контроля персонала: контроль доступа, видеокамеры, пассивные инфракрасные детекторы, мониторинг очереди, электронные указатели;

- мультимедийных сервисов, например, аудиовизуальные проекторы;

- систем мониторинга;

- интеллектуальной системы здания. [6, с. 7]

Помимо вышеуказанного стандарта нормативными актами, используемыми при проектировании и реализации СКС, являются отечественные ГОСТ 18620-86 и СНиП 3.05.06-85. В них подробно рассматривается система маркировки кабелей, обеспечивающая удобство эксплуатации и обслуживания кабельной системы.

В процессе создания технического задания на создание структурированной кабельной системы составляется подробная схема помещений предприятия. На ней указываются все соответствующие подсистемам и функциональным элементам СКС точки, размещенные в соответствии со средой эксплуатации СКС и потребностями подразделения, подключаемого к конкретному участку системы. На основании полученной схемы составляются технические задания на монтаж отдельных элементов СКС.

Для удобства эксплуатации и управления сетью создаются системы оптической индикации и средства механической блокировки и цветовой идентификации. Они позволяют осуществлять постоянный мониторинг кабельной сети вплоть до отдельных портов на коммутационных панелях. Благодаря этому администратор сети имеет возможность автоматически обнаружить факт отключения или подключения устройств к сети. Также существует воз-

можность использовать средства компьютерного контроля состояния портов, в случае если используемое сетевое оборудование поддерживает данные функции.

Очень важным средством контроля и идентификации является маркировка кабельных магистралей и сетевого оборудования. Маркирующий элемент, используемый в процессе создания и эксплуатации СКС, вне зависимости от его назначения и выполняемой функции должен отвечать следующему комплексу требований:

- обладать такими размерами, цветом и контрастностью, которые обеспечивают легкость прочтения нанесенной на него информации;

- иметь срок службы, совпадающий или превышающий нормативную продолжительность эксплуатации маркируемого компонента во всем разрешенном диапазоне изменения влияющих факторов;

- обеспечивать возможность нанесения маркирующих надписей требуемого объема не только вручную, но и на принтере;

- желательно, чтобы наряду с символьной и текстовой маркировкой элемент позволял производить также цветовую кодировку;

- обладать простотой установки в сочетании с высокой механической прочностью и устойчивостью к воздействию неблагоприятных факторов окружающей среды (влага, экстремально высокие и низкие температуры, ультрафиолетовое излучение и т. д.);

- иметь достаточно широкий ряд типоразмеров для выполнения маркировки устройств одинакового функционального назначения с разными габаритами. [

Построенная с учетом всех нормативных актов и с использованием качественных материалов структурированная кабельная система обладает высокой эксплуатационной надежностью. Аварийные и нештатные ситуации ситуации возникают преимущественно в результате механических, термических и химических повреждений сетевого оборудования и кабельных магистралей, и может быть сформулирован в следующей форме:

- обрыв или повреждение кабеля, организационно относящегося к горизонтальной или магистральной подсистемам;

- выход из строя розеточного модуля информационной розетки рабочего места пользователя;

- неисправности элементов коммутационного оборудования в монтажных шкафах или помещениях кроссовых различного уровня;

- повреждение линков на рабочих местах пользователей и в технических помещениях различного уровня. [6, с. 15]

При возникновении аварийной ситуации первая основная задача группы информационных технологий заключается в скорейшем определении ее причины. Затем локализуется место повреждения. Для этого привлекаются различные измерительные приборы и индикаторы, а также метод визуального осмотра. Затем принимается решение о выборе метода восстановления доступа к сети конкретного пользователя или группы. Для этого применяются ремонт, соответствующие переключения на резервный тракт передачи и организация временной связи. После этого немедленно или в более подходящее время организуются и производятся работы по восстановлению нормальной работоспособности сети.

Кабельная сеть это одна из частей сложной системы информационной структуры предприятия, требующая от обслуживающего персонала высокой квалификации. СКС, находящаяся в ведении группы информационных технологий состоит не только из сетевых кабелей, но также включает в себя комплекс силовой электропроводки для питания техники и пользователей. Соответственно весь технический персонал подразделения должен иметь допуски по работе с электроустановками в обязательном порядке.

## 2.2 Компоненты ЛВС

В данной главе будет более подробно рассмотрен комплекс оборудования, лежащий в основе ЛВС предприятия. Как было сказано выше, локальная вычислительная сеть это совокупность технических средств и инженерных решений, к которым относят: каналы связи, это структурированная кабельная система, рассмотренная в предыдущей главе, компьютеры, сетевые адаптеры, сетевое программное обеспечение и операционные системы.

Основным каналом связи в ЛВС рассматриваемого предприятия является витая пара категории 5е, позволяющая обмениваться данными на скорости до 1Гбит\мин. Все сетевое оборудование, лежащее в основе ЛВС, имеет порты с разъемами на 8 контактов, соответствующих количеству жил в витой паре. Коннектор формата RG-45 обжимается на каждом оконечнике кабеля в соответствии с цветовой схемой указанной в стандартах. Подробно со схемой обжимки можно ознакомиться в Приложении 1.

Кабель подключается к разъему рабочей станции, будь то персональный компьютер или какое-либо иное оборудование (принтеры, промышленное или научное оборудование), соединяя ее с сетевым коммутатором, обеспечивающим связь с сервером. Каждое устройство для успешного обмена данными обладает сетевой картой, конфигурации которых разнятся, но все обладают возможностью работать по единым протоколам передачи данных. Важно чтобы сетевые карты соответствовали пропускной способности сети и были способны обработать сигнал соответствующей скорости.

Коммутацию элементов локальной сети осуществляют специальные сетевые устройства, называемые сетевыми коммутаторами (switch). Ранее для этих целей широко использовались сетевые концентраторы, однако на данный момент подобное оборудование практически не используется. Коммутаторы делятся на два типа – управляемые и неуправляемые. Неуправляемое

устройство автоматически передает пакеты данных с одного порта на другой в соответствии с сопоставлением адресов устройств получателей.

Управляемый коммутатор в режиме по умолчанию работает как неуправляемый, однако обладает микропроцессором, позволяющим осуществлять ручное управление трафиком. Управление осуществляется посредством протокола Telnet или SSH, или WEB-интерфейса, также может быть использовано графическое меню, текстовое меню или командная строка. Подобные устройства позволяют разделять локальную сеть с помощью VLAN, внося в память устройства данные о принадлежности конкретных адресов к определенным сегментам сети. Это позволяет сократить количество широковещательного трафика, установить доступ устройств к определенным подсетям и повысить уровень безопасности сети. Также при помощи протоколов резервирования можно создавать сложные топологии, если существует необходимость обрабатывать большие потоки данных.

Сотрудники предприятия, использующие для работы компьютеры, или какую либо иную технику, подключенную к сети предприятия, являются клиентами ЛВС. Автоматизированные рабочие места (АРМ) оборудованы компьютерами с сетевыми картами, поддерживающими формат передачи данных принятый в сети, а также периферийными устройствами (клавиатура, мышь, монитор и пр.). Доступ к работе на АРМ осуществляется при помощи учетных записей на сервере. При помощи серверного программного обеспечения осуществляется автоматический удаленный контроль технического состояния рабочих станций, что позволяет оперативно решать проблемы, возникшие у пользователей.

Основой любой локальной вычислительной сети является сервер. В случае, когда сеть обширна, создается серверный парк, состоящий из нескольких серверов, наделенных специальными ролями в управлении сетью, оборудованием, пользователями и программами. При определении задач возложен-

ных на локальную сеть, а также с учетом нагрузки и потребностей предприятия выбирается соответствующий серверный компьютер, который обладает необходимым количеством и мощностью процессоров, объемом оперативной и встроенной памяти. Объединив несколько серверов в общую сеть и распределив между ними соответствующие роли можно построить мощную, быстродействующую и отказоустойчивую вычислительную систему, способную обеспечивать нужды большого предприятия. Также сервер с большим объемом памяти может быть использован для запуска на нем виртуальных машин и создания виртуальных серверов, что позволяет создать максимально гибкую и удобную сетевую инфраструктуру.

Выбор программного обеспечения также зависит от потребностей организации. Также немаловажным фактором становится стоимость программ, а также сложность эксплуатации и обслуживания. Наиболее распространенными семействами операционных систем, используемых как на серверных, так и на клиентских компьютерах являются Windows, Linux и прочие UNIX-based системы, а также MacOS. Каждый системный продукт имеет свои преимущества и недостатки. Зачастую в сетевой инфраструктуре используются различные сочетания операционных систем, например на клиентских машинах установлена ОС Windows, серверный парк же использует как Windows сервера, так и машины с установленной на ней ОС Linux.

Поскольку ЛВС это сложная многоуровневая система, состоящая из множества элементов, требуется постоянное и грамотное управление всеми компонентами системы, обеспечивающее бесперебойное функционирование и оперативный ремонт в случае аварийных ситуаций. Администрирование локальной сети, а также надзор за техническим состоянием всего относящегося к ней оборудования, возлагается на группу информационных технологий входящую в штат предприятия. В перечень обязанностей входит поиск, правильное определение, а также устранение неполадок и сбоев в работе определенной сети, конфигурация компонентов системы, настройка параметров

сетевых операционных систем, учет работы сети и управление производительностью, обеспечение информационной безопасности. Для осуществления всех вышеуказанных мероприятий группа информационных технологий наделяется определенными полномочиями по доступу ко всему, что касается ЛВС и ее функционирования. Первичным средством контроля является маркировка кабельных магистралей и оборудования, а также ограничение доступа посторонних в технические помещения, относящиеся к локальной сети. Также в распоряжении сетевого администратора находится специализированное программное обеспечение, позволяющее осуществлять контроль действий пользователей, защиту сети от вирусных атак извне и изнутри, осуществление мероприятий по информационной безопасности.

В данной главе был приведен перечень основных компонентов ЛВС и их краткое описание. Далее каждый из компонентов сети будет рассмотрен в контексте реализации плана модернизации предприятия. Все регламенты, технические решения и описанные сетевые продукты ложатся в основу составления итогового проекта модернизации.

## 2.3 Сетевое оборудование

После составления схем сети, технических заданий и прокладки основных кабельных магистралей, настает очередь установки и настройки соответствующего задачам сети сетевого оборудования.

Сетевое оборудование будет использоваться как пассивное, так и активное. Одной из немаловажных задач является простота обслуживания сетевой инфраструктуры, в связи с этим необходимо не перегружать топологию сети лишними устройствами, а так же использовать технику с большим ресурсом работы.

Наиболее распространенным и известным производителем сетевого оборудования является фирма Cisco. Не смотря на высокую стоимость продуктов данной компании, они обладают всеми необходимыми свойствами для обеспечения комфортного и бесперебойного функционирования сетевой инфраструктуры. Принято решение рассмотреть в качестве основного сетевого оборудования коммутаторы фирмы Cisco. Ниже приводится список необходимого оборудования с краткими характеристиками.

Первым сетевым оборудованием, пропускающим входящий сигнал от провайдера и обрабатывающим его для дальнейшего использования внутри сети предприятия, является сетевой шлюз. Также шлюз является обратным выходом для данных передающихся из локальной сети в глобальную. Главной особенностью сетевого шлюза как устройства является его способность осуществлять сопряжение сетей использующих разные протоколы, например локальной и глобальной. Вариантов установки сетевого шлюза существует большое количество, это может быть как отдельное устройство, так и специализированное программное обеспечение, или же они могут быть объединены. В сетевой инфраструктуре условного предприятия решено использовать отдельный физический сервер, на который устанавливается операционная система Windows Server 2012. После установки системы выбираются роли

сетевого шлюза, а также настраивается прокси-сервер и межсетевой экран. Данный сервер выполняет ключевую роль в сети, позволяя осуществить обмен данными с внешним миром, а также управлять службами безопасности и блокировать нежелательный трафик.

За маршрутизацию внутри сети отвечает специальное устройство, называемое маршрутизатором или роутером. Данное устройство осуществляет пересылку пакетов между различными сегментами сети, а также для связи сетей использующих отличные друг от друга протоколы передачи данных. Маршрутизатор работает на сетевом уровне модели OSI и при построении маршрута руководствуется таблицами маршрутизации. В качестве маршрутизатора принято решение использовать физический сервер на котором размещен сетевой шлюз. Для этого необходимо установить на сервере виртуальную машину с операционной системой Linux, после чего сконфигурировать ее для выполнения функций маршрутизации. [1, с. 406]

Самым многочисленным сетевым оборудованием в инфраструктуре являются сетевые коммутаторы (switch). Ключевой особенностью сетевого коммутатора является его способность передавать данные непосредственно получателю, не нагружая излишне сетевые каналы и исключая возможность несанкционированного доступа к данным тех лиц, для которых они не предназначаются. Для этого коммутатор работает на канальном уровне модели OSI, осуществляя физическую адресацию при помощи закодированного в биты адреса отправителя и получателя. Это повышает производительность и безопасность сети, избавляя остальные сегменты сети от необходимости и возможности обрабатывать данные, которые им не предназначались. Поскольку рассматриваемое условное предприятие состоит из множества подразделений с разными целями, задачами и техническим оснащением, целесообразно использовать управляемые сетевые коммутаторы, это позволит гибко настраивать доступ к сети для каждого конкретного клиента с учетом его индивидуальных особенностей. Разновидностей сетевых коммутаторов также

существует огромное количество, поэтому нецелесообразно описывать конкретную модель. Принцип работы же у каждого устройства одинаковый, поэтому выбор модели зависит лишь от стоимости и надежности устройства.

[2, с. 325]

## 2.4 Серверный парк

Для эффективного осуществления контроля над серверным оборудованием и обеспечением гибкой поддержки функционирования ИТ инфраструктуры предприятия необходима консолидация серверов и виртуализация их ресурсов, обеспечение мониторинга ИТ-инфраструктуры, защита её от информационных угроз и качественное обслуживание. Ревизия и объединение ресурсов серверов обязательные мероприятия по приведению сети в порядок. Инвентаризация аппаратных средств, находящихся в подразделениях и филиалах предприятия, помогает осознать картину в целом. Это позволяет оценить степень износа оборудования и прогнозировать плановое обслуживание и замену серверов.

Дисбаланс серверной загрузки - обычное явление для сетевой инфраструктуры. Не смотря на точные расчеты нагрузки и ресурсов перед созданием сети, при длительной эксплуатации появляются некоторые нюансы. С течением времени происходит обновление операционных систем и прочего программного обеспечения, вводятся новые корпоративные приложения, изменяется количество пользовательских рабочих мест и т. д. Это неизбежно приводит к дисбалансу нагрузок. Серверы становятся либо недозагружены (ценные ресурсы простаивают), либо перегружены (что влечет за собой угрозу стабильной работе и риск для бизнес-процессов).

Данную проблему может решить виртуализация серверного парка, что позволяет наиболее оптимальным образом перераспределять нагрузку. Это способствует снижению потребности в мощности серверов, исчезает необходимость замены серверов, а модернизация оборудования обходится гораздо дешевле. Стоит отметить, что в случае, когда каждое каждой роли согласно плану соответствует отдельный физический сервер, виртуализация позволяет обходиться без покупки новых физических серверов.

Важной частью виртуализации является развертывание виртуальных машин на базе физических серверов. С выход программного обеспечения VMWare vSphere 4 технология облачных вычислений теперь включает в себя возможность консолидировать сервера в виде «облака» виртуальных машин. Из чего состоит конкретная физическая начинка «облака» не очень важно. Это означает что сервера разных производителей и разных марок, с различной производительностью объединяются в «облака» виртуальных машин. Эти «облака» могут соответствовать определенным физическим местам, где расположены конкретные сервера, и даже включать в себя удаленные друг от друга серверы. В результате системный администратор управляет одним или несколькими отказоустойчивыми «облаками» виртуальных машин. При возникновении проблем с одним из облаков вся нагрузка в виде запущенных на сервере приложений автоматически переносится на доступные ресурсы серверов в сети предприятия.

Для успешной работы «облака» потребуются и хорошая сетевая инфраструктура уровня Gigabit Ethernet, включая систему хранения данных NAS с резервированными контроллерами, и гигабитные коммутаторы, объединяющие серверы и сеть предприятия. Приложения, которым необходим прямой доступ к оборудованию, не могут работать на виртуальных серверах, их необходимо размещать на физических серверах. Особенно важные и ресурсоемкие приложения рекомендуется оставлять на специально отведенных физических серверах. Другими словами, «облако» виртуальных машин легко создать на современной ИТ-инфраструктуре, и такую работу стоит выполнять тщательно и вдумчиво – перенос старых физических серверов в одно место не имеет смысла. [1, с. 354]

Альтернативой радикальной модернизации серверного оборудования предприятия является аренда облака на стороне, например в датацентре. Это необязательно делать в масштабах всего предприятия. Для территориально распределенного предприятия аренда «облака» может быть реализована от-

дельно в тех регионах, где собственная ИТ-инфраструктура наиболее изношена. В этом случае вся серверная начинка в виде виртуальных машин переносится в «облако», арендованное у коммерческого провайдера. На компанию арендодателя в данном случае помимо представления отказоустойчивых каналов связи ложится ответственность за отказоустойчивость и целостность содержимого «облака», а предприятие-арендатор платит за «облако» согласно выбранному тарифному плану.

Само собой, аренда и собственное локальное «облако» способны успешно дополнять друг друга. Особо актуальным подобный подход является для случаев, когда нагрузка на вычислительную среду непостоянна. Например, российским ИТ-специалистам очень знакомо понятие отчетного периода, когда все бухгалтерские и административные системы предприятия работают на пике производительности. Аренда «облака» в этом случае успешно решает задачу доступности вычислительных ресурсов, если мощность собственного серверного парка оказывается недостаточной. После того, как арендованное «облако» включено в логическую виртуальную инфраструктуру предприятия, виртуальные машины могут автоматически выбрать пространстводля работы и, при недостатке ресурсов в локальном «облаке», способны мигрировать в арендованное облако. По завершении ресурсоемкой работы, виртуальные машины возвращаются обратно в локальное «облако».

В дополнении к объединению и виртуализации серверного парка неотъемлемым элементом сложной сетевой инфраструктуры с большим количеством серверов является построение оптимальной системы мониторинга, резервирования и восстановления данных. Уровень готовности информационных систем в целом во многом зависит от используемых средств управления сетевой инфраструктурой. Ведь до сих пор далеко не везде используются интегрированные системы управления и мониторинга. При построении многих сетей администраторы по-прежнему пытаются решить данные задачи с помощью наборов из множества инструментов - консолей, анализаторов

и т. д., скачанных из сети или входящих в состав стандартного серверного программного обеспечения. При этом время системных администраторов расходуется крайне нерационально — ведь на каждую ситуацию, связанную со сбоем, приходится подбирать и задействовать свой набор ПО.

Назначение универсальной системы — обеспечение качественного и бесперебойного функционирования всех компонентов информационной инфраструктуры предприятия (включая АРМ), а также выработка и принятие обязательных решений по поддержке и развитию ИТ-систем. Важно абстрагироваться от уровня мониторинга конкретных операционных систем (Windows, Linux, UNIX), аппаратной архитектуры (x86, RISC), приложений и сетевой инфраструктуры, от «точечных» средств мониторинга и перейти к универсальному, глобальному уровню управления (уровню предприятия). Например далеко не всегда сбои в системе возникают именно по вине сервера, причиной могут являться сбои в сетевой инфраструктуре или каналообразующем сетевом оборудовании, и все это необходимо отслеживать и анализировать моментально, используя комплексные средства мониторинга
.

Наиболее современными, удобными и преобладающими на рынке мониторинговыми комплексами на сегодняшний день являются IBM Tivoli или HP OpenView. При помощи этих продуктов возможно создавать единую унифицированную информационную среду, позволяющую управлять информационными технологиями, анализом сетевой инфраструктуры предприятия, а также для территориально распределенных сетей обмена данными. Указанные меры позволяют осуществлять контроль ключевого оборудования сетевой инфраструктуры — серверов, активного сетевого оборудования, постоянный мониторинг состояния системы, нагрузки сетевых узлов и каналов связи, сбор статистики о трафике и действиях пользователей, контроль пороговых значений параметров работы оборудовании. [3, с. 259]

На рассматриваемом в работе условном предприятии целесообразно собрать серверную инфраструктуру из нескольких физических серверов, на основе которых будет реализована система виртуальных машин, а также обеспечены все обязательные элементы для управления локальной сетью. Ниже приведен список серверов с указанием их ролей.

- Gate. Сервер, выполняющий роль шлюза, на нем же размещается сетевой экран и прочие средства по управлению входящим и исходящим трафиком.

- NAS. Network attached storage, сетевое хранилище данных.

- HyperV. Гипервизор, сервер для размещения на нем виртуальных машин.

- Mail. Отдельный почтовый сервер

- Backup. Сервер, выполняющий функции резервного копирования, служит для сбора бэкапов и дальнейшего их развертывания в возникновения случае аварийной ситуации и потери данных.

- Сервер для осуществления расчетов предназначенный для научного подразделения предприятия

Все сервера обеспечены системой RAID которая обладает функциями резервного копирования и моментального переноса рабочих процессов с одного сервера на другой в случае возникновения технических неполадок или любых других проблем.

## 2.5 Автоматизированные рабочие места пользователей

АРМ, в основе которых лежит персональный компьютер, – наиболее простой и распространенный вариант автоматизированного рабочего места для сотрудников любого предприятия. Данное АРМ является системой, предоставляющей каждому пользователю возможность работать используя все технические средства компьютера и локальной сети к которой он подключается на все время работы.

Создание АРМ на базе персональных компьютеров обеспечивает:

- простоту и удобство по отношению к пользователю;

- простоту адаптации к конкретным функциям пользователя;

- компактность размещения и невысокие требования к условиям эксплуатации;

- высокую надежность;

- сравнительно простую организацию технического обслуживания.

Эффективным режимом работы АРМ является его функционирование в рамках локальной вычислительной сети в качестве рабочей станции. Особенно целесообразен такой вариант, когда требуется распределить информационно-вычислительные ресурсы между несколькими пользователями.

Любая конфигурация АРМ должна отвечать общим требованиям в отношении организации информационного, технического и программного обеспечения.

Программное обеспечение АРМ ориентировано на конкретную предметную область, в которой работает тот или иной пользователь. Например, для обработки документации предполагается такая структуризация информации, позволяющая осуществить необходимое манипулирование различными структурами, удобную и быструю корректировку данных в массивах.

Техническое обеспечение АРМ обязано гарантировать высокую надежность технических средств, организацию удобного пользователям режима работы, способность обрабатывать за определенное время конкретный объем данных. Поскольку АРМ является индивидуальным пользовательским средством его организация должна отвечать задачам эргономики, удобства использования и возможность легкого, в том числе удаленного обслуживания.

Программное обеспечение прежде всего ориентируется на профессиональный уровень пользователя, сочетаясь с его функциональными потребностями, квалификацией и специализацией. Пользователь со стороны программной среды должен ощущать постоянную поддержку своего желания работать в любом режиме. Взаимодействие пользователя с техническими средствами АРМ предусматривает обеспечение максимального комфорта при работе с любыми приложениями и данными, что достигается путем выбора оптимальных продуктов, своевременного обновления и совершенствования программного обеспечения.

## 2.6 Программное обеспечение

Назначение серверных операционных систем — это управление приложениями, обслуживающими всех пользователей корпоративной сети, а в некоторых случаях и внешних пользователей. К данным приложениям относятся современные системы управления базами данных, средства управления сетями и анализа событий в сети, службы каталогов, средства обмена сообщениями и групповой работы, Web-серверы, почтовые серверы, корпоративные брандмауэры, серверы приложений самого разнообразного назначения, серверные части бизнес-приложений. Требования к производительности и надежности указанных операционных систем очень высоки; нередко сюда входят и поддержка кластеров (набора ряда однотипных компьютеров, выполняющих одну и ту же задачу и делящих между собой нагрузку), и возможности дублирования и резервирования, и переконфигурации программного и аппаратного обеспечения без перезагрузки операционной системы.

Выбор конкретной операционной системы для сервера производился из операционных систем компании Microsoft семейства Windows, как наиболее подходящих для поставленных задач и удобства администрирования. На сегодняшний день рынок серверных ОС Microsoft представлен несколькими основными системами:

Windows Server 2008 – серверная операционная система корпорации Microsoft, выпущенная 25 февраля 2008 года. В основу Windows Server 2008 положена операционная система Windows Server 2003, а также усовершенствования, реализованные в пакете обновления и выпуске Windows Server 2003 R2. В Windows Server 2008 добавлены новые функции, а также усовершенствованы многие возможности базовой ОС. Среди них следует отметить работу с сетью, расширенные функции безопасности, обеспечение удаленного доступа к приложениям, централизованное управление ролями сервера, средства мониторинга производительности и надежности, отказоустойчи-

вость кластеров, развертывание и файловую систему. При помощи данной операционной системы можно разрабатывать, доставлять и управлять гибким взаимодействием с пользователями и приложениями, организовывать сетевые инфраструктуры с высоким уровнем безопасности и увеличивать технологическую эффективность и организованность в своей организации.

Windows Server 2012 — версия серверной операционной системы от Microsoft. Была выпущена 4 сентября 2012 года на смену Windows Server 2008 R2 как серверная версия Windows 8. Выпускается в четырёх редакциях.

Основные функции принципиально такие же как и в предыдущей версии системы. К отличиям можно отнести то что в новой серверной ОС добавлена служба Dynamic Access Control. Работа этой службы направлена на улучшение централизованной защиты на уровне доменов файлов, а также на обеспечение безопасности папок поверх всех имеющихся разрешений файлов. Windows Server 2012 является наиболее подходящей операционной системой в качестве обновления – с момента своего выпуска она была доработана, исправлены ошибки и стала полноценной заменой семейству Windows Server 2008

К операционным систем рабочих станций не предъявляются столь высокие требования в плане надежности и возможности работы многими пользовательскими сеансами. Но при этом они должны в первую очередь обеспечивать удобный интерфейс для общения пользователя и всех аппаратных средств, как самого компьютера, так и средств расположенных в сети.

В качестве клиентских операционных сетей рассматривались продукты компании Microsoft, как наиболее подходящие для данной сети предприятия. Не смотря на то, что лицензионные продукты компании Microsoft платные, в отличие от систем семейства UNIX, они более привычны для пользователей и более удобны для настройки и обслуживания техническим персоналом.

На данный момент самой современной системой является Windows 10, однако более старая система Windows 7 не теряет своей актуальности благодаря удобству и простоте работы с ней. В сети предприятия планируется использовать обе данных системы на клиентских компьютерах.

Обязательным моментом при использовании программного обеспечения является наличие лицензий на каждый системный продукт, что позволит избежать проблем с законом.

## 2.7 Администрирование сети

Чтобы обеспечивать максимально производительную, удобную и безотказную работу сети необходимо осуществлять мероприятия по нескольким направлениям. Это не является вопросом настройки всего оборудования или программного обеспечения, а сбалансированная совместная работа того и другого в комплексе, плюс управление использованием сети в организации. Даже при наличии хорошего оборудования необходимо грамотно сконфигурировать его и провести все необходимые мероприятия по обеспечению безопасности, в том числе по защите от человеческого фактора.

Очень важно иметь точную схему и документацию сети. Должна существовать актуальная топологическая схема сети и подробная информация обо всем сетевом оборудовании, его конфигурациях и используюемых протоколах, IP-адресах, каналах связи WAN, серверах и сегментах пользовательских локальных сетей. Без этой всеобъемлющей информации трудно будет понять, что следует изменить или что изменилось в результате перехода от одной сетевой конфигурации к другой.

При внесении изменений в сеть важно знать и уметь оценивать работу сети в текущий момент. Создание базовой линии - это запись всех параметров работы сети, чтобы сравнивать параметры работы сети после внесения изменений и делать выводы о положительном или отрицательном влиянии внесенных изменений. Можно создать базовую линию своей сети с помощью инструмента System Monitor. После сбора всех необходимых данных можно получить представление о рабочих возможностях сети.

При настройке сети не стоит забывать о том, что все вносимые изменения должны иметь обоснование и укладываться в рамки заданных параметров. Особенно в организациях с большим количеством клиентов и развитой сетью, где множество людей задействовано в процессе настройки и поддержания работоспособности сети. Также необходимо позаботиться о документировании всех проводимых работ.

При проведении реорганизации сети и ее дальнейшем росте важно следить за тем чтобы не создавать скопления концентраторов или маршрутизаторов, так как будучи неучтенными, они представляют собой точки возможных сбоев в работе сети, и ими невозможно управлять. В сетях со слишком сложной топологией больше времени тратится на поиск причин возникающих аварийных ситуаций и меньше времени остается на конструктивное планирование того, как лучше удовлетворить потребности пользователей и исправление неисправностей. Также не следует забывать и об обеспечении безопасности. Не внесенный в документацию маршрутизатор в удаленной части сети может позволить проникнуть в сеть злоумышленникам. [1, с. 658]

# Глава 3. Безопасность

## 3.1 Информационная безопасность сети и пользователей

Современные сетевые операционные системы, полностью защищенные от атак и угроз также представляют мощные средства защиты от несанкционированного доступа к сетевым ресурсам. Однако возникают случаи, когда даже такая защита становится уязвимой и не срабатывает. Используются программные продукты для защиты информации. Практика показывает, что несанкционированный пользователь или программные продукты, называемые вирусами, имеющий достаточный опыт в области системного и сетевого программирования, задавшийся целью подключиться к сети, даже имея ограниченный доступ к отдельным ресурсам, рано или поздно все равно может получить доступ к некоторым защищенным ресурсам сети. Поэтому возникает необходимость в создании дополнительных аппаратных и программных средств защиты сетевых ресурсов от несанкционированного доступа или подключения. К аппаратным средствам защиты относятся различные брандмауэры, сетевые экраны, фильтры, антивирусные программы, устройства шифрования протокола и т. д. К программным средствам защиты можно отнести: слежения сетевых подключений (мониторинг сети); средства архивации данных; антивирусные программы; криптографические средства; средства идентификации и аутентификации пользователей; средства управления доступом; протоколирование и аудит. Также необходимо физически защитить кабельные магистрали и сетевое оборудование от несанкционированного доступа и случайных повреждений, вызванных человеческим фактором.

[7, с. 147]

## 3.2 Средства защиты данных

Для защиты информации в локальной сети традиционно используются следующие меры и средства:

Технические средства - электрические, электромеханические и электронные устройства. Технические средства подразделяются на:

- аппаратные - устройства, встраиваемые непосредственно в аппаратуру, или устройства, которые сопрягаются с аппаратурой локальных сетей по стандартному интерфейсу

- физические - реализуются в виде автономных устройств и систем (электронно-механическое оборудование охранной сигнализации и наблюдения. Замки на дверях, решетки на окнах).

Программные средства - программы, специально предназначенные для выполнения функций, связанных с защитой информации. А именно программы для идентификации пользователей, контроля доступа, шифрования информации, удаления остаточной (рабочей) информации типа временных файлов, тестового контроля системы защиты и др. К преимуществам программных средств — универсальность, гибкость, надежность, простота установки, способность к модификации и развитию.

Недостатки - ограниченная функциональность сети, использование части ресурсов файл-сервера и рабочих станций, высокая чувствительность к случайным или преднамеренным изменениям, возможная зависимость от типов компьютеров (их аппаратных средств).

Организационные средства складываются из организационно-технических (подготовка помещений с компьютерами, монтаж кабельной системы с учетом требований ограничения доступа к ней и др.) и организационно-правовых (нормативные акты и правила работы, устанавливаемые руководством конкретного предприятия). Преимущества организационных средств состоят в том, что они позволяют решать множество разнообразных проблем, просты в реализации, быстро реагируют на нежелательные действия в сети, имеют неограниченные возможности модификации и развития. К недостаткам относят высокую зависимость от субъективных факторов, в том числе от общей организации работы в конкретном подразделении.

Надежно обезопасить доступ к информации предприятия каким либо одним из вышеперечисленных способов невозможно. Необходим комплексный подход к использованию и развитию всех средств и способов защиты информации. Ниже более подробно рассмотрим каждый элемент комплекса мер безопасности.

Среди программных средств защиты информации в локальных сетях можно выделить и подробнее рассмотреть следующие:

- средства архивации данных — средства, осуществляющие слияние нескольких файлов и даже каталогов в единый файл — архив, одновременно с сокращением общего объёма исходных файлов путем устранения избыточности, но без потерь информации, то есть с возможностью точного восстановления

- антивирусные программы – программы. разработанные для защиты информации от вирусов;

- криптографические средства — включают способы обеспечения конфиденциальности информации, в том числе с помощью шифрования и аутентификации;

- средства идентификации и аутентификации пользователей — аутентификацией (установлением подлинности) называется проверка принадлежности субъекту доступа предъявленного им идентификатора и подтверждение его подлинности. Другими словами, аутентификация заключается в проверке является ли подключающийся субъект тем, за кого он себя выдает. А идентификация обеспечивает выполнение функций установления подлинности и определение полномочий субъекта при его допуске в систему, контролирования установленных полномочий в процессе сеанса работы, регистрации действий и др.

- средства управления доступом — средства, имеющие целью ограничение регистрации входа-выхода объектов на заданной территории через «точки прохода»;

- протоколирование и аудит — протоколирование обеспечивает сбор и накопление информации о событиях, происходящих в информационной системе. Аудит — это процесс анализа накопленной информации. Целью компьютерного аудита является контроль соответствия системы или сети требуемым правилам безопасности, принципам или индустриальным стандартам.

Аудит обеспечивает анализ всего, что может относиться к проблемам безопасности, или всего, что может привести к проблемам защиты.

Специализированные программные средства защиты информации от несанкционированного доступа обладают в целом лучшими возможностями и характеристиками, чем встроенные средства сетевых операционных систем. Кроме программ шифрования и криптографических систем, существует много других доступных внешних средств защиты информации. [7, с. 159]

## 3.3 Безопасность рабочих мест пользователей

Начальникам соответствующих структурных подразделений предприятия требуется в надлежащей степени организовать рабочие места в соответствии со всеми требованиями законодательства, касающимися трудовой деятельности за компьютеризированными системами.

Основными вредными факторами при осуществлении трудовой деятельности за персональными компьютерами являются:

- высокая степень электромагнитного воздействия;

- высокий уровень статического электричества;

- низкая степень ионизации воздуха;

- нагрузки, связанные с длительным сидячим положением тела;

- очень высокая нагрузка на органы зрения;

- сопутствующие длительной сидячей работе факторы: боли и дискомфорт в пояснице и позвоночнике, венозная недостаточность, стресс и депрессии.

Охрана труда при работе за компьютером предусматривает соблюдение следующих правил:

- по организации и оснащению трудового места;

- по освещенности;

- по регламентации перерывов в работе.

Нормативные положения СанПиНа предъявляют определенные требования к площади рабочего места при работе за персональным компьютером в совокупности более 4 часов за смену для мониторов ЭЛТ от 6 квадратных метров и более, для мониторов ЖК от 5 квадратных метров и более.

Существует набор правил по организации рабочего места оснащенного компьютером:

- в помещении с компьютерами рекомендуется, чтобы окна выходили на север или северо-восток;

- при отсутствии в помещении естественного солнечного освещения необходимо оборудовать искусственное освещение в соответствии с нормами и правилами освещенности рабочих мест;

- в случае если мониторы расположены в ряд, люминесцентные лампы следует смонтировать в виде сплошных или прерывистых линий;

- при расположении ПК по периметру, источники освещения должны располагаться непосредственно над рабочими местами. [7, с. 163]

# Глава4. Расчет сетевых показателей

## 4.1 Расчет пропускной способности ЛВС

Не смотря на высокие мощности современных компьютеров, позволяющих им обмениваться информацией и обрабатывать ее с большой скоростью, показателем хорошей пропускной способности сети нельзя считать ту скорость, с которой два компьютера могут обмениваться данными между собой. Скорость работы сети оценивается в зависимости от ее пропускной способности. Сеть Ethernet обладающая пропускной способностью 10 Мбит/с может одновременно обслуживать либо несколько компьютеров, генерирующих большой поток данных, либо множество компьютеров, создающих небольшой трафик в сети. Ранее пропускная способность локальной сети, равная 10 Мбит/с, была более чем достаточна для обслуживания множества компьютеров, поскольку существующие на то время скорости работы центральных процессоров компьютеров и плат интерфейса не позволяли обмениваться данными с большими скоростями. Однако с ростом производительность микропроцессоров и общего усиления компьютеров изменилась и интенсивность использования сетей. В результате сеть Ethernet с пропускной способностью 10 Мбит/с уже не может быть использована в качестве магистральной даже при организации небольших сетей, поскольку она не справляется с резко возросшим потоком данных. Подходящей для использования в сетях среднего размера является технология Fast Ethernet, обладая пропускной способностью в 100 Мбит/с. Но и способности этой технологии в настоящее время не удовлетворяют большинству крупных предприятий и фирм, вследствие чего наиболее оптимальной технологией для нашего условного предприятия является Gigabit Ethernet.

Пропускная способность одна из основных характеристик производительности сети. Быстрая передача информации между компьютерами - это основная задача, для решения которой строится любая сеть. Пропускная способность — максимально возможная скорость обработки трафика, определенная стандартом технологии, на которой построена сеть. Критерии, связанные с пропускной способностью сети или части сети, хорошо отражают качество выполнения сетью ее основной функции.

Пропускная способность измеряется либо в битах в секунду, либо в пакетах в секунду.

Пропускная способность сети зависит как от характеристик физической среды передачи (медный кабель, оптическое волокно, витая пара) так и от принятого способа передачи данных (технология Ethernet, FastEthernet, Gigabit Ethernet). Пропускная способность часто используется в качестве характеристики не столько сети, сколько собственно технологии, на которой построена сеть.

Возьмем следующие исходные данные для расчета пропускной способности новой сети:

1. 100 Мбит/с полоса пропускания канала связи между коммутаторами горизонтальной подсистемы и АРМ

2. 1 Гбит/с полоса пропускания канала связи между магистральным коммутатором и коммутаторами горизонтальной подсистемы

3. серверный парк

4. общее число компьютеров – 250 (от 8 до 24 на коммутаторе);

5. 2 мкс задержка пакета, производимая коммутатором

В связи с тем, что вычислительные сети работают по принципу коммутации пакетов, количество переданной информации есть смысл измерять в пакетах, тем более что пропускная способность коммуникационного оборудования, работающего на канальном уровне и выше, также, чаще всего, измеряется именно в пакетах в секунду. Чаще всего, при упоминании пакета, подразумевают пакеты протокола Ethernet, как самого распространенного, имеющие минимальный для протокола размер в 64 байта. Пакеты минимальной длины выбраны в качестве эталонных из-за того, что они создают для коммуникационного оборудования наиболее тяжелый режим работы. Вычислительные операции, производимые с каждым пришедшим пакетом, в очень слабой степени зависят от его размера, поэтому на единицу переносимой информации обработка пакета минимальной длины требует выполнения гораздо большего числа операций, чем для пакета максимальной длины.

Несмотря на то, что количество переданной информации принято измерять в пакетах, измерение пропускной способности в битах в секунду дает более точную оценку скорости передаваемой информации.

При тестировании пропускной способности сети на прикладном уровне легче всего измерять как раз пропускную способность по пользовательским данным. Для этого достаточно измерить время передачи файла определенно-

го размера между сервером и клиентом и разделить размер файла на полученное время.

Исходя из вышесказанного, расчет будут проведены с измерением скорости передачи по сети 1 кадра Ethernet минимальной длины, то есть 64 байта (512 бит).

1. Измеряется скорость передачи 1 кадра Ethernet между любыми двумя точками, подключенными к одному из коммутаторов в пределах одного коммутационного узла:

где β – размер кадра минимальной длины

T1 – время за которое проходит 1 кадр расстояние от хоста к хосту на заданном участке (в пределах одного коммутационного узла)

В общем случае время, за которое кадр заданной длины проходит заданный сегмент сети при одинаковом времени задержки на коммутаторах можно выразить через формулу:

где r – количество коммутаторов;

τ – время задержки на коммутаторе;

ni – количество участков, с определенной максимальной скоростью прохождению пакета;

ti – время прохождения кадра минимальной длины, на участке, с определенной максимальной скоростью;

i – участок, с определенной максимальной скоростью;

θ – общее количество определенных скоростей, встречающихся на участках рассматриваемого сегмента сети;

Время прохождения кадра минимальной длины, на участке, с определенной максимальной скоростью можно найти следующим образом:

где β – размер кадра минимальной длинны;

vi – максимальная скорость на участке между узлами сети;

i – участок, с определенной максимальной скоростью

Таким образом, t1 (время прохождения любого участка между двумя узлами сети, при максимальной скорости 100 Mbps) будет равно:

t1 = 512 / 108 = 0.00000512 с

Общее время прохождения заданного сегмента сети T1 (хост-хост, хост-сервер в пределах одного коммутационного узла):

T1 = 0.000002 + 2 * 0.00000512 = 0.00001224 с

Теперь рассчитаем скорость прохождения данного участка кадром Ethernet минимальной длины:

V1 = 512 / 0.00001224 = 41830065.359477125 б/с ≈ 41.85 Мб/с

Измеряется скорость передачи 1 кадра Ethernet между любыми двумя точками, подключенными к разным коммутаторам, как второй возможный путь прохождения кадра:

1) Найдем время прохождения на малых участках заданного сегмента при максимальной скорости передачи 1000 Мб/с:

t2 = 512 / 109 = 0.000000512 с

2) Время прохождения на малых участках заданного сегмента при максимальной скорости передачи 100 Мб/с мы вычислили ранее:

t1 = 0.00000512 с

3) Количество коммутаторов в заданном сегменте:

r = 3

4) Время задержки на коммутаторах:

τ = 0.000002 с

5) Количество участков поддерживающих скорость 100 Мб/с и 1000 Мб/с соответственно:

n1 = 2

n2 = 2

6) Вычислим время прохождения заданного сегмента сети T2:

T2 = 3 * 0.000002 + ( 2 * 0.00000512 + 2 * 0.000000512 ) = 0.000017264 с

7) Теперь можем найти скорость прохождения кадром всего данного участка:

V2 = 512 / 0.000017264 = 29657089.89805375 б/с ≈ 29.66 Мб/с

Максимальная скорость передачи на участках сегмента (фактически всей старой сети) равна 10 Мб/с, время задержки на коммутаторе 0,000002:

t3 = 512 / 107 = 0.0000512 с

T3 = 0.000002 + 2 * 0.0000512 = 0.0001044 с

V3 = 512 / 0.0001044 = 4904214,55938697 б/с ≈ 4.9 Мб/с

Целесообразно определять общую пропускную способность сети как среднее количество информации, переданной между всеми узлами сети в единицу времени. Общая пропускная способность сети может измеряться как в пакетах в секунду, так и в битах в секунду. При делении сети на сегменты или подсети общая пропускная способность сети равна сумме пропускных способностей подсетей плюс пропускная способность межсегментных или межсетевых связей.

Для начала необходимо составить матрицу трафика сети. На ней будет отображена скорость взаимодействия любых двух узлов сети.

- V1 = 41.85 Мб/с
- V2 = 29.67 Мб/с

После составления матрицы необходимо найти усредненную скорость прохождения 1 кадра Ethernet минимальной длины из матрицы трафика сети:

1. для скорости передачи 1 кадра Ethernet между любыми двумя хостами, подключенными к одному из коммутаторов в коммутационном узле (для значения V1 в таблице (V1 = 41.85 Мб/с)):

где xi – количество возможных соединений между хостами, при скорости прохождения кадра 41.85 Мб/с

i – номер коммутатора

ai – количество хостов, подключенных к i-му коммутатору

N – общее количество коммутаторов

X – общее количество возможных соединений между хостами , при скорости прохождения кадра 41.85 Мб/с

Коммутатор 1, 5: ( 15 – 1 ) * 15 = 210

Коммутатор 2, 3, 4: ( 20 – 1 )*20 = 380

X = 210*2+380*3= 1560

2. для скорости передачи 1 кадра Ethernet между любыми двумя хостами, подключенными к разным коммутаторам (для значения V2 в таблице

(V2 = 29.67 Мб/с))

где yi – количество возможных соединений между хостами, при скорости прохождения кадра 29.67 Мб/с

ai – количество хостов, подключенных к i-му коммутатору

i – номер коммутатора

N – общее количество коммутаторов

O – общее количество хостов

Y – общее количество возможных соединений между хостами , при скорости прохождения кадра 29.67 Мб/с

Коммутатор 1, 5: ( 90 – 15 ) * 15 = 1125

Коммутатор 2, 3, 4: ( 90 – 20 )*20 = 1400

Y = 1125*2+1400*3= 6450

Выполняется проверку:

общее количество всех возможных соединений по результатам расчета равно:

X + Y = 1560 + 6450 = 8010

общее количество всех соединений по матрице равно:

(90*90)-90=8010

Теперь возможно вычислить пропускную способность сети:

A = ( 41.83 * 1560 + 29.66 * 6450 ) / (1560 + 6450 ) = 32.03 Мб/с

Минимальная пропускная способность на участке сети равна 29.67 Мб/с.

## 4.2 Производительность сети

В качестве временной характеристики производительности сети чаще используют такой показатель как время реакции. Время реакции - это полное время, прошедшее с момента завершения запроса или команды компьютерной системе до начала. Время реакции сети характеризует сеть в целом, в том числе качество работы аппаратного и программного обеспечения

Вычисляется время полного оборота кадра в сети для двух случаев:

1. время, затраченное кадром минимальной длины на прохождение пути от любого хоста сети до сервера, равно 0.00001224 с RTT = 2 x 0.00001224 = 0.00002448 с = 24.48 мкс

2. время, затраченное кадром минимальной длины на прохождение пути от любого хоста сети до сервера, подключенным к разным коммутаторам, равно 0.000017264 с.

RTT = 2 x 0.000017264 = 0.000034528 с = 34.528 мкс

При помощи данных значений составляется матрица:

- TS = 24.49 мкс
- TM = 34.529 мкс

Подсчитывается общее количество значений TS и TM в матрице:

TS

где zi – количество значений TS, при скорости прохождения кадра

41.85 Мб/с

ai – количество хостов, подключенных к i-му коммутатору

si – количество серверов, подключенных к i-му коммутатору

i – номер коммутатора

N – общее количество коммутаторов

Z – общее количество значений TS, при скорости прохождения кадра

41,85 Мб/с

Z = z2 = 20 – 1 = 19

TM

где wi – количество значений TM, при скорости прохождения кадра

29.67 Мб/с

ai – количество хостов, подключенных к i-му коммутатору

si – количество серверов, подключенных к i-му коммутатору

i – номер коммутатора

N – общее количество коммутаторов

O – общее количество хостов в сети

W – общее количество значений TS, при скорости прохождения кадра

29.67 Мб/с

W = w2 = 90 – 20 = 70

Остается найти среднее-время реакции сети B:

B = (0.00002448 * 19 + 0.000034528 * 70 ) / ( 19 + 70 ) = 32.38 мкс

Для данной схемы максимальное значение времени реакции сети будет равно максимальному времени оборота кадра:

RTT= 2 x 0.000017264 = 0.000034528 с = 34.528 мкс

Надежность является одной из важнейших характеристик качества объекта - совокупности свойств, определяющих пригодность его использования по назначению. Но в отличие от точечных характеристик качества (быстродействие, производительность и т.д., которые измеряются для некоторого момента времени), надежность характеризует зависимость точечных характеристик качества либо от времени использования, либо от наработки объекта, т.е. надежность - характеристика временная.

Повышение надёжности сервера достигается резервированием, в том числе с горячим подключением и заменой критически важных компонентов:

- при необходимости вводится дублирование процессоров при помощи RAID технологии (например, это важно для непрерывности выполнения сервером задачи долговременного расчёта — в случае отказа одного процессора вычисления не обрываются, а продолжаются, пусть и на меньшей скорости);
- блоков питания;
- жёстких дисков в составе массива RAID и самих контроллеров дисков;
- вентиляторов, обеспечивающих охлаждение компонентов сервера.

В теории надежности используется термин MTTF (Mean Time To Failure) - средняя наработка до отказа. Приведем значения MTTF для сравнительно ненадежных компонентов (1 год приблизительно 10000 часов):

- блоки питания 30000-100000 часов;
- кулеры 50000-400000 часов;
- материнские платы 50000-300000 часов;
- приводы компакт-дисков 50000-100000 часов;
- жесткие диски 0.5 млн. - 1.5 млн. часов.

При расчёте надежности сервера принимаются следующие допущения:

- отказы устройств являются независимыми и случайными событиями;
- учитываются только устройства, входящие в сервер;
- вероятность безотказной работы подчиняется экспоненциальному закону распределения.

Вероятность безотказной работы системы определяется как:

N – общее количество

Pi – вероятность безотказной работы i-го элемента

Вероятность безотказной работы системы с раздельным резервированием определяется как:

Pi – вероятность безотказной работы i-го элемента;

λi – интенсивность отказов элементов i-го типа;

m – количество резервных элементов;

T – время работы сервера.

Для элементов, используемых в сервере, приняты следующие интенсивности отказов:

- Материнская плата: λ1 = 4.5x10-8 ч-1;
- Процессор: λ2 =4.0x10-7 ч-1;
- Память: λ3 =3.2x10-7 ч-1;
- Жесткий диск: λ4 =8.3x10-7 ч-1;
- CD-ROM/DVD-ROM: λ5 =0.1x10-5 ч-1;
- Контроллер RAID: λ6 =5x10-7 ч-1;
- Сетевая карта: λ7 =1.0x10-7 ч-1 ;
- Блок питания: λ8 =2x10-7 ч-1 ;

Исходя из этих значений, можно подсчитать суммарную интенсивность отказов всех устройств одного типа, а затем и для всех устройств сервера.

$$\lambda_1 = N \times 4.8 \times 10^{-8}$$

$$\lambda_{\text{общ}} = \sum_{i=1}^{N} \lambda_i$$

Рассчитаем вероятность безотказной работы сервера без резервирования и построим график зависимости ВБР от времени работы.

Подсчитаем суммарную интенсивность отказов всех устройств:

$$\lambda_{\text{общ}} = \lambda_1 + \lambda_2 + \lambda_3 + \lambda_4 + \lambda_7 + \lambda_8 =$$
$$= 4{,}5 \times 10^{-8} + 4{,}0 \times 10^{-7} + 3{,}2 \times 10^{-7} + 8{,}3 \times 10^{-7} + 1{,}0 \times 10^{-7} + 2{,}0 \times 10^{-7} = 18{,}95 \times 10^{-7}$$

Вероятность безотказной работы сервера за T=1000 часов

$$P(1000) = e^{-18.95\times10^{-7}\times1000} = 0.9981$$

Вероятность безотказной работы сервера за T=5000 часов

$$P(5000) = e^{-18.95\times10^{-7}\times5000} = 0.9906$$

Вероятность безотказной работы сервера за T=10000 часов

$$P(10000) = e^{-18.95\times10^{-7}\times10000} = 0.9812$$

Рассчитывается вероятность безотказной работы сервера с раздельным резервированием для ниже представленной схемы и зависимости ВБР от времени работы.

Вероятность безотказной работы сервера за T=1000 часов

$$P_{MB} = 1-(1-e^{-4.5\times10^{-6}\times1000})^1 = 0.9999$$
$$P_{CPU} = 1-(1-e^{-4.0\times10^{-7}\times1000})^2 = 0.9999$$
$$P_{RAM} = 1-(1-e^{-3.2\times10^{-7}\times1000})^2 = 0.9999$$
$$P_{HDD} = 1-(1-e^{-8.3\times10^{-7}\times1000})^4 = 0.9999$$
$$P_{CD} = 1-(1-e^{-0.1\times10^{-5}\times1000})^2 = 0.9999$$
$$P_{RAID} = 1-(1-e^{-5.0\times10^{-7}\times1000})^1 = 0.9995$$
$$P_{LAN} = 1-(1-e^{-1.0\times10^{-7}\times1000})^1 = 0.9999$$
$$P_{PU} = 1-(1-e^{-2.0\times10^{-7}\times1000})^2 = 0.9999$$
$$P(1000) = 0.9999\times0.9999\times0.9999\times0.9999\times0.9999\times0.9995\times0.9999\times0.9999 = 0.9988$$

Вероятность безотказной работы сервера за T=5000 часов

$$P_{MB} = 1-(1-e^{-4.5\times10^{-6}\times5000})^{1} = 0.9998$$

$$P_{CPU} = 1-(1-e^{-4.0\times10^{-7}\times5000})^{2} = 0.9999$$

$$P_{RAM} = 1-(1-e^{-3.2\times10^{-7}\times5000})^{2} = 0.9999$$

$$P_{HDD} = 1-(1-e^{-8.3\times10^{-7}\times5000})^{4} = 0.9999$$

$$P_{CD} = 1-(1-e^{-0.1\times10^{-5}\times5000})^{2} = 0.9999$$

$$P_{RAID} = 1-(1-e^{-5.0\times10^{-7}\times5000})^{1} = 0.9975$$

$$P_{LAN} = 1-(1-e^{-1.0\times10^{-7}\times5000})^{1} = 0.9995$$

$$P_{PU} = 1-(1-e^{-2.0\times10^{-7}\times5000})^{2} = 0.9999$$

$$P(5000) = 0.9998\times 0.9999\times 0.9999\times 0.9999\times 0.9999\times 0.9975\times 0.9995\times 0.9999 = 0.9963$$

Вероятность безотказной работы сервера за T=10000 часов

$$P_{MB} = 1-(1-e^{-4.5\times10^{-6}\times10000})^{1} = 0.9995$$

$$P_{CPU} = 1-(1-e^{-4.0\times10^{-7}\times10000})^{2} = 0.9999$$

$$P_{RAM} = 1-(1-e^{-3.2\times10^{-7}\times10000})^{2} = 0.9999$$

$$P_{HDD} = 1-(1-e^{-8.3\times10^{-7}\times10000})^{4} = 0.9999$$

$$P_{CD} = 1-(1-e^{-0.1\times10^{-5}\times10000})^{2} = 0.9999$$

$$P_{RAID} = 1-(1-e^{-5.0\times10^{-7}\times10000})^{1} = 0.9950$$

$$P_{LAN} = 1-(1-e^{-1.0\times10^{-7}\times10000})^{1} = 0.9990$$

$$P_{PU} = 1-(1-e^{-2.0\times10^{-7}\times10000})^{2} = 0.9999$$

$$P(10000) = 0.9995\times 0.9999\times 0.9999\times 0.9999\times 0.9999\times 0.9950\times 0.9990\times 0.9999 = 0.9930$$

# Заключение

В ходе проведенной работы была произведена оценка объемов работ, необходимых для реализации проекта модернизации ИТ инфраструктуры предприятия, рассмотрены типовые решения применяемые при реализации отдельных частей сетевой инфраструктуры. На основании расчетов предполагаемой нагрузки на сеть подобраны оптимальные решения относительно СКС, ЛВС, а также общего парка устройств. Сформулированы политики управления сетью, Предусмотрены меры безопасности, оберегающие сеть от внешних атак, утечки данных, а также обеспечивающие безопасность пользователей.

Приведенные в работе данные можно использовать  при решении реальных рабочих задач, ставящихся перед системным администратором. Описанные технические решения и данные позволяют создать современную сетевую инфраструктуру, рассчитанную на высокую загрузку и отвечающую требованиям любого реально существующего предприятия.

Современные технологии, используемые при развертывании сетевой инфраструктуры, позволяют создать отказоустойчивый, удобный в использовании и обладающий хорошим быстродействием, а также легко масштабируемый комплекс технических средств обеспечивающий максимально быстрое и удобное выполнение любой задачи, стоящей перед предприятием, а также многолетнее пользование сетью без ее принципиальных переделок.

## Список использованной литературы


1. Компьютерные сети. 5-е издание. Э. Таненбаум. Серия «Классика computer science». – СПб.: Питер, 2003, - 992 с.

2. Официальное руководство Cisco по подготовке к сертификационным экзаменам CCNA ICND2 200-101: маршрутизация и коммутация. Академическое издание. Уэнделл Одом. Издательский дом «Вильямс», 2015, 737 с.

3. «Компьютерные сети. Принципы, технологии, протоколы» (5-е издание), В. Олифер, Н. Олифер. ATmega16.- San Jose.: Atmel Corporation, 2010. – 357с.

4. Администрирование структурированных кабельных систем. Семенов А.Б. НОУДПО «Институт АйТи» – М.: ДМК Пресс; М.: Компания АйТи,

2008. – 192 с.: ил.

5. Основы компьютерных сетей. Олифер В.Г., Олифер Н.А. Издательство «Питер», 2009 г., 352 с.

6. Международный стандарт ISO/IEC 14763-1 ISO/IEC 11801-1, 89 с.

7. Абраров Р. Д., Курязов Д. А. Информационная безопасность в компьютерных сетях // Молодой ученый. — 2016. — №9.5, 1341 с.