***Глава 7***

***Сети***

Сеть компании – основа ее инфраструктуры. Плохо созданная сеть влияет на любое

восприятие всех остальных компонентов системы. Сеть нельзя считать изолиро-

ванным элементом. Решения, принимаемые при проектировании сети и в процес-

се ее внедрения, влияют на то, как инфраструктурные сервисы будут внедрены.

Таким образом, с теми, кто несет ответственность за проектирование этих сервисов,

обязательно стоит консультироваться в процессе проектирования сети.

***7.1. Основы***

При создании сети ваша основная цель – предоставить надежную, хорошо до-

кументированную, простую в обслуживании сеть, которая отличается значи-

тельной пропускной способностью и потенциалом роста.

Подходы к проектированию глобальных вычислительных и локальных сетей

значительно различаются. Со временем циклически меняющиеся тенденции

делают их более похожими, затем менее похожими, затем вновь более сходны-

ми.

**7.1.1. Модель OSI**

Модель OSI (Open Systems Interconnection – эталонная модель взаимодействия

открытых систем) для сетей получила широкое распространение.

Сетевые устройства определяют путь, который проходят данные по физической

сети, состоящей из кабелей, беспроводных каналов и сетевых устройств (**уро-**

**вень 1**). Сетевое устройство, принимающее решение, основываясь на аппаратном, или MAC-, адресе узла-отправителя либо получателя, относится

к устройствам **уровня 2**. Устройство, принимающее решение, основываясь

на IP-адресе (или AppleTalk, или DECnet) узла-отправителя либо получателя,

известно как устройство **уровня 3**. Устройство, использующее транспортную

информацию, такую как номера портов TCP, – это устройство **уровня 4**.

**Уровень 5** плохо вписывается в мир TCP/IP. **Уровень 6** – это формат данных:

ASCII, HTML, MP3 или MPEG. Также обычно сюда относят шифрование и сжа-

тие данных.

**Уровень 7** – это, собственно, протокол приложения: HTTP (HyperText Transfer

Protocol – протокол передачи гипертекста) для Веб; SMTP для отправки элект-

ронной почты; IMAP4 для доступа к почтовым ящикам, FTP (File Transfer

Protocol – протокол передачи файлов) для передачи файлов и т. д.

**Модель OSI** – полезное руководство для понимания того, как должны работать

сети, но в реальном мире границы уровней часто нарушаются. Например, VPN-

подключение, осуществляемое через HTTP-прокси, посылает трафик уровней

3 и 4 по протоколу 7-го, прикладного уровня.

**7.1.2. Понятная архитектура**

Сетевая архитектура должна быть максимально понятной и простой для вос-

приятия. Должна существовать возможность кратко описать подход, приме-

нявшийся при проектировании сети, и проиллюстрировать проект нескольки-

ми простыми рисунками. Понятная архитектура значительно упрощает реше-

ние проблем с сетью.

Понятная архитектура охватывает как физическую, так и логическую тополо-

гию сети, а также сетевые протоколы, используемые узлами и сетевым обору-

дованием. Понятная архитектура также просто определит стратегию роста

в отношении как добавочных сегментов локальной сети, так и подключения

новых удаленных офисов.

Лучше ограничивать количество сетевых протоколов в каждой отдельной

глобальной вычислительной сети. Если необходимо, для этих протоколов можно создать туннели поверх TCP/IP с помощью разных вложенных протоколов. К тому же такой подход обходится дешевле, чем организация отдельной глобальной вычислительной сети для каждого протокола.

**7.1.3. Топологии сетей**

Топологии сетей сменяют друг друга вместе с технологиями и структурой рас-

ходов по мере того, как компании развиваются, открывают крупные удаленные

офисы или поглощают другие компании. Здесь мы расскажем о некоторых

распространенных топологиях.

В глобальных, университетских и локальных сетях часто встречается топология

«звезда», в которой одна компания, здание или часть сетевого оборудования

находится в центре звезды, а остальные компании, здания или сети подключа-

ются к центру. Для топологии звезды свойственно одно уязвимое место: при отказе

центра нарушается связь между лучами звезды. Иначе говоря, если все узлы

в здании подключены к одному коммутатору, то при его отказе отключатся они

все. Если все сети, входящие в глобальную сеть, подключены к одному зданию,

в котором отключили электричество, они потеряют связь друг с другом, но внут-

ри каждой удаленной сети связь будет работать. Однако топология звезды по-

нятна, проста, а ее внедрение часто экономически эффективно.

Распространен вариант топологии звезды, состоящий из нескольких звезд,

центры которых связаны друг с другом избыточными высокоскоростными ка-

налами. Такой подход ограничивает негативные последствия отказа

центра одной из звезд. Компании с географически удаленными отделениями

часто используют такой подход для сосредоточения всего удаленного трафика

от одного географического региона в одном или двух дорогостоящих дистанци-

онных каналах.

Топология «кольцо» тоже широко распространена и чаще всего применяется

для отдельных низкоуровневых топологий, таких как кольца SONET. Кольце-

вая топология также встречается в локальных и университетских сетях,

а иногда бывает полезна и в глобальных вычислительных сетях. В кольцевой

топологии каждый элемент сети – будь то сетевое оборудование, здание или

корпоративная сеть – подключен к двум другим так, что схема подключений

в сети образует кольцо. Выход из строя любого канала

в сети не влияет на состояние связи между функционирующими составляющи-

ми кольца. Однако при увеличении числа элементов кольца, особенно в глобаль-

ных сетях, может потребоваться разделить конфигурацию подключений на

несколько сетей.

Другая архитектура, используемая компаниями, которые заботятся об избы-

точности и надежности, выглядит как топология из нескольких звезд, но каж-

дый краевой узел. связан резервным подключением с центром другой звезды.

Если откажет центральный узел какой-либо звезды,

ее краевые узлы переходят на резервное подключение, пока основное не будет

восстановлено. Такая гибридная модель позволяет организации добиться ком-

промисса между расходами и надежностью для каждой сети.

Существует множество вариантов сетевых топологий, в том числе топология хаоса, которой по большей части описывается топология Интернета. Топо-

логия хаоса возникает в случае, если каждый узел в качестве маршрута для

доступа к остальной части сети может использовать один или несколько произ-

вольных узлов.

Архитектуру, которую невозможно изобразить или описать без дополнительной

помощи, нельзя назвать понятной. Тем не менее Интернет продолжает существование, потому что он высокоадаптивен и отказоустойчив.

То, что обычно изображается как схема сети, – это логическая топология сети.

Она обычно показывает только сетевые устройства, такие как маршрутизаторы,

работающие на уровне 3 и выше, и представляет как единый элемент каждую

подсеть, работающую с одним и более устройствами уровня 2, такими как ком-

мутаторы. Для отдельной сети могут быть построены различные логические схемы в зависимости от того, на какие конкретно особенности нужно обратить внимание аудитории.

Простое практическое правило ограничения сложности сети заключается в том,

что архитектор корпоративной сети и старшие сетевые администраторы долж-

ны быть способны без посторонней помощи схематично изобразить ключевые

функции и основную структуру топологии сети. Если нужны дополнительные

источники информации, то архитектуру нельзя назвать ясной и понятной.

Логическая топология сети не может разрабатываться изолированно. Она под-

вержена влиянию других аспектов вычислительной инфраструктуры и сама

влияет на них.

**Плоская топология** – единая большая сеть, состоящая только из устройств

уровня 2. В терминах TCP/IP, это одна коммутируемая зона, один большой

домен широковещательной рассылки. Без маршрутизаторов. Под доменом

широковещательной рассылки подразумевается, что широковещательный

запрос, отправляемый в эту сеть одной машиной, принимают все машины сети.

В плоской топологии существует только один блок сетевых адресов, в который

входят все машины. Все сервисы, такие как файловый сервис, печать, элект-

ронная почта, аутентификация и сервис имен, предоставляются серверами этой

сети.

В топологии на основе местоположения сети уровня 2 назначаются исходя из

их физического местоположения.

В топологии на основе функциональных групп каждый член функциональной

группы подключен к одной и той же (плоской) сети, независимо от размещения,

наиболее разумным способом. Также групповые сети, как правило, включают в себя файловый сервис, сервис имен и сервис аутентификации, что подразумевает рас-

пространение сети и на информационный центр. Одно (или больше) устройство

уровня 3 соединяет групповую сеть с основной корпоративной сетью, в которой

также предоставляются сервисы для групповой сети, такие как электронная

почта, доступ к интрасети и к Интернету.

**7.1.4. Промежуточный кабельный узел**

**Промежуточный кабельный узел** (Intermediate Distribution Frame, IDF) – это

«умное» название для коммутационного шкафа. Распределительная система

состоит из нескольких сетевых шкафов и кабелей, которые подключают на-

стольные компьютеры к сети.

Инновации в сетевом оборудовании требуют высококачественных медных или

оптоволоконных подключений, способных справляться с возросшими скоро-

стями. Если вы используете новейшие кабели с наилучшими характеристиками

при создании кабельной системы, можно ожидать, что они проработают по

крайней мере 5 лет, прежде чем устареют по сравнению с сетевыми технологи-

ями. Но если вы пытаетесь сэкономить, используя старые, дешевые кабели

с худшими характеристиками, то вам придется пережить связанные с модер-

низацией расходы и перерывы в работе раньше, чем если бы вы выбрали более

качественные кабели.

**Категории кабелей**

Кабели категории 3 рассчитаны на 10-мегабитные Ethernet-подключения

дальностью до 100 м.

Кабели категории 5 рассчитаны на 100-мегабитные

Fast Ethernet-подключения дальностью до 100 м.

Кабели категории 6 рассчитаны на 1000-мегабитные Gigabit Ethernet-подключения дальностью до 90 м.

Кабели категории 7 требуются для нового стандарта

10-гигабитных Ethernet-подключений. Все они обратно совместимы.

Обычно их наименования сокращаются до Cat3, Cat5 и т. д.

Более современные IDF упрощают подключение кабеля от сетевого разъема

к нужной сети. Достаточно просто подключить короткий патч-корд от гнезда

RJ-45, представляющего этот разъем, к гнезду RJ-45 Ethernet-коммутатора

в нужной сети.

Подключение между IDF можно организовать двумя способами. Первый спо-

соб – проложить связки кабелей через все здание. Однако при большом коли-

честве IDF такое количество каналов обойдется дорого и будет сложным в об-

служивании. Другой способ – создать централизованное место для коммутации

и проложить связки кабелей от IDF только до этого центра. В таком случае для

соединения двух любых IDF будет достаточно только создать кросс-подключение

в центре. Такой центр называется центральным кабельным узлом (Main

Distribution Frame, MDF).

У вас должен быть по меньшей мере один IDF на этаж или больше, если

этажи широкие. Размещать IDF в здании следует строго по одной вертикали,

на одном и том же месте каждого этажа. При вертикальном размещении про-

кладывать кабели между IDF и MDF будет проще и дешевле, а впоследствии при

необходимости будет легче добавить дополнительные кабели между IDF.

Нумерация IDF должна включать номер здания, этажа и шкафа. Нумерация

шкафов должна быть единообразной для всех этажей всех зданий. Сетевые

разъемы, обслуживаемые IDF, должны быть помечены ярлыком с номерами

IDF и розетки. Если в одной розетке расположено несколько сетевых разъемов,

то обычно после номера розетки используются буквы. Номера и литеры розеток

должны соответствовать номерам и литерам розеток на разъемах в IDF.

IDF всегда должны быть закрыты, а доступ посторонних к ним – запрещен. Без

должной подготовки и понимания того, что вы делаете, в коммутационном

шкафу слишком легко все испортить. Если приходится вносить большое коли-

чество изменений, а штат сотрудников отличается высокой текучестью, реко-

мендуется проводить частые, но краткие инструктажи по работе с коммутаци-

онными шкафами. Если эти занятия проводятся в одно и то же время в одном и

том же месте каждый месяц, то люди, имеющие доступ к коммутационным

шкафам, но редко с ними работающие, смогут по необходимости посещать за-

нятия, чтобы быть в курсе происходящего.

Еще одна причина закрывать IDF на замок – безопасность. IDF – слишком удоб-

ное место для размещения устройств слежения за сетью, так как туда редко

заглядывают люди и там можно легко спрятать «жучок» среди другого обору-

дования. Кроме того, IDF – слишком легкая добыча для желающих нарушить

работу сети.

В шкафу для IDF должно размещаться только сетевое оборудование для его

зоны обслуживания. Серверы, размещенные в не предназначенных для этого

местах (коммутационных шкафах и т. д.), сильнее подвержены сбоям, вызван-

ным случайными толчками или отключениями кабелей, а при возникновении

проблем их сложнее найти.

Коммутационные шкафы должны быть обеспечены защитой электропитания.

Сетевое оборудование, так же как и компьютерное, должно быть защищено от

всплесков напряжения и перебоев в электроснабжении. Если ваш информаци-

онный центр питается через ИБП, то также надо защитить и сетевое оборудова-

ние в коммутационных шкафах, которое является продолжением вычислитель-

ного центра.

Шкафы IDF должны иметь дополнительное охлаждение помимо того, что обес-

печивает система кондиционирования здания. Сетевое оборудование компакт-

но, поэтому на ограниченном пространстве плотно размещается большое коли-

чество нагревающихся устройств. Сетевые устройства обычно неприхотливы

и надежны, но и для них существуют ограничения. В небольшом шкафу IDF

будет слишком жарко без дополнительного охлаждения.

Более экономично устанавливать сетевые разъемы на этапе строительных работ,

а не добавлять их потом по одному по мере надобности. Следовательно, имеет

смысл установить на каждом столе на один или два разъема больше, чем, по

вашему мнению, может когда-либо понадобиться вашим пользователям. При

проводке кабелей в офисе не так дороги сами кабели, как высоки строительные

расходы на прокладку их в стенах.

Вместо того чтобы пытаться учитывать, например, что в офисах инженеров

должно быть больше сетевых разъемов, чем в офисах отдела маркетинга, лучше

устанавливайте одно и то же количество разъемов на каждом столе и столько

же на потолке. Распределение мест никогда не бывает постоянным. Со временем

инженеры будут работать там, где предполагалось разместить отдел маркетин-

га, и вам понадобится приводить кабели в этих помещениях в соответствие

стандартам остальных инженерных помещений.

Чтобы оценить поставщика, осведомитесь об отзывах клиентов и предыдущих

заказчиках, к которым можно было бы сходить, чтобы расспросить их и посмотреть на качество работы. Посмотрите на произведенные работы, оцените

аккуратность монтажа в IDF. Попросите посмотреть журнал тестовых распеча-

ток поставщика. Прокладка кабелей – дорогостоящая операция, в ней ни на

чем нельзя экономить. Устранение проблем позже обойдется гораздо дороже,

чем в то время, пока монтажники проводят работы в вашей компании.

Короткий кабель от разъема до устройства называется патч-кабелем. Рекомендуется приобретать готовые патч-кабели, а не делать их самостоятельно. Некачественный кабель может создавать проблемы с надежностью, которые возникают случайным образом и трудно отслеживаются.

Еще один момент, который необходимо учитывать при монтаже сетевых разъ-

емов, – это их ориентация. Разъемы устанавливаются в так называемых рас-

пределительных коробках или розетках, что и определяет, как будет расположен

разъем. В потайных розетках подключенный кабель будет торчать из стены,

и потребуется место, чтобы кабель не изгибался на излом. Удостоверьтесь, что

места достаточно.

**7.1.5. Центральный кабельный узел**

**Центральный кабельный узел** (Main Distribution Frame, MDF) соединяет все

IDF. Между MDF и IDF всегда должно быть достаточно запасных кабелей, так

как довольно часто требуются новые подключения, а прокладка дополнитель-

ного оптоволокна или кабеля между этажами стоит дорого, и лучше сделать все

за один раз. MDF, как и IDF, – продолжение вашего вычислительного центра.

Ему необходим тот же уровень физической безопасности, защиты электропита-

ния и охлаждения.

Очень часто MDF является частью вычислительного центра. В таких случаях

MDF часто называют **сетевым рядом или сетевыми стойками**. Патч-панели

в этих стойках подключены к патч-панели на верхней части каждой стойки

в информационном центре.

Если вычислительный центр занимает несколько зданий, IDF и MDF, как пра-

вило, располагают одним из двух способов. В небольших комплексах каждый

IDF подключен к одному MDF в центральном здании. Либо во всех зданиях

устанавливаются MDF, каждый из которых затем подключается к центрально-

му MDF.

**7.1.6. Точки разграничения**

**Точка разграничения** – это граница между вашей организацией и поставщиком

услуг, например телефонной компанией или интернет-провайдером. Точка

разграничения может представлять собой распределительный шкаф оптоволо-

конной линии, коммутационные блоки, щит в стойке, сетевое устройство или

даже небольшую пластиковую коробку на стене с разъемом для кабеля. Теле-

фонная компания отвечает лишь за проводку кабеля до своей точки разграни-

чения. Если у вас проблемы с линией, вы должны узнать, где находится соот-

ветствующая точка разграничения, и сказать об этом технику, чтобы он не

пытался проверить и починить другую эксплуатируемую линию.

**7.1.7. Документирование**

Сетевая документация бывает нескольких видов, и самое основное – маркиров-

ка. Необходимость в документировании и его основные виды вряд ли изменят-

ся со временем.

Частью сетевой документации должны быть карты как физической, так и ло-

гической сети. Карта физической сети должна отображать, где проходит про-

водка, местоположение конечных точек и радиус действия беспроводных точек.

Если в схеме физической сети предусмотрена избыточность, необходимо четко

обозначить и задокументировать физически разные пути. Необходимо обозна-

чить объем и тип подключения для каждого канала.

Карта логической сети должна отображать топологию логической сети, сетевые

номера, имена и скорость. Эта карта также должна показывать все протоколы

маршрутизации и административные домены, существующие в сети. Карты

физической и логической сетей должны создаваться в масштабе сети организа-

ции и определять ее внешние границы.

**Маркировка** – основная и самая главная составляющая сетевого документиро-

вания. Особенно важное значение имеют понятные и последовательные ярлыки

на патч-панелях и междугородных каналах. Для патч-панелей должно быть

четко обозначено физическое местоположение соответствующей патч-панели

или разъемов. Все подключения к патч-панели должны быть четко и последо-

вательно промаркированы с обоих концов. Такой ярлык, наклеенный непосредственно рядом с индикатором сбоя устройства, может значительно

облегчить жизнь.

Еще один ключевой аспект документирования – онлайн-документирование,

являющееся частью конфигурации самих сетевых устройств. При каждом воз-

можном случае стоит использовать поля комментариев и имен устройств, обес-

печивая таким образом документирование для администраторов сети.

**7.1.8. Простая маршрутизация**

У узла с одним сетевым интерфейсом должен быть один стандартный маршрут.

Он не должен принимать никакую динамическую маршрутную информацию.

Узел с несколькими сетевыми интерфейсами не должен отправлять пакеты от

других узлов, но при этом обязан принимать только трафик, адресованный ему.

Для такого узла необходима статичная таблица маршрутизации, он не должен

принимать динамическую маршрутную информацию, а его конфигурация

должна быть максимально простой. Если узел с несколькими сетевыми интер-

фейсами подключен к сетям A, B и C и ему необходимо связаться с другим узлом

в сети B, необходимо использовать сетевой интерфейс, подключенный к сети B.

Это самый простой, самый очевидный и самый прямой способ.

Простая маршрутизация является более детерминированной, благодаря чему

упрощает и делает более предсказуемым решение сетевых проблем. Если все

узлы сети сконфигурированы одинаково, они должны и вести себя одинаково.

Если узлы получают динамическую маршрутную информацию, может произой-

ти непредвиденное.

Если узлы занимаются маршрутизацией, это может привести к снижению быс-

тродействия. По мере роста количества маршрутов в сети проводить обновление

протоколов маршрутизации становится все сложнее. Если подсеть содержит ровно один маршрутизатор, нет необходимости трансляции протокола маршрутизации в эту подсеть.

**7.1.9. Сетевые устройства**

«Строительным материалом» для любой современной сети должны быть выде-

ленные сетевые устройства, такие как маршрутизаторы и коммутаторы, а не

универсальные узлы сети, сконфигурированные для маршрутизации. Эти сете-

вые устройства должны быть созданы специально для выполнения одной зада-

чи, связанной с передачей пакетов или управлением трафиком, а также с самим

устройством.

Маршрутизация пакетов производится в ядре – это означает, что ей отводится

наивысший приоритет по сравнению со всеми другими функциями. Если роль

маршрутизатора у вас выполняет файловый сервер, вы заметите, что чем боль-

ше сетевого трафика обрабатывается, тем медленнее работает файловый сервис.

У компьютерного и сетевого оборудования разные графики обновления. После

установки сетевого устройства обновлений программного обеспечения и измене-

ний в конфигурации начинают избегать и откладывать их до самых крайних

случаев. Серверы приложений обновляются, переконфигурируются и перезагру-

жаются чаще. Несоответствие этих графиков на одной машине становится при-

чиной неудобств для каждого сотрудника, имеющего дело с данной машиной.

Хотя в сообществах с системами UNIX уже не используют рабочие станции

и серверы в качестве маршрутизаторов, наблюдается тревожная тенденция,

в соответствии с которой такие поставщики, как Майкрософт, Novell и Apple,

поощряют использование универсальных машин в качестве маршрутизаторов,

брандмауэров или сервисов удаленного доступа.

**7.1.10. Оверлейные сети**

**Оверлейная сеть** – логическая топология, наложенная на физическую тополо-

гию. Примерами таких сетей являются VLAN, Frame Relay и ATM. Этот принцип

позволяет создавать простые физические архитектуры, которые могут поддерживать любую необходимую сложность логического наложения и при этом

сохранять простоту на физическом слое.

Можно создать очень простую (а значит, стабильную) однородную физическую

сеть, а затем построить оверлейные сети на этой прочной основе, чтобы получить

возможность для более сложных подключений. На уровне глобальной вычис-

лительной сети это может означать, что у всех площадок установлено единое

подключение к ATM или распределенная сеть Frame Relay. Затем коммутаторы

ATM или Frame Relay конфигурируются таким образом, чтобы между площад-

ками был создан виртуальный канал. Если какая-либо пара удаленных площадок обменивается трафиком большого объема, достаточно просто изменить конфигурацию коммутатора, добавив виртуальный канал между этими площадками. Одной из распространенных конфигураций является полная ячеистая топология, в которой каждая площадка с помощью виртуального канала подключена ко всем остальным площадкам. Преимуществом такой сети является тот факт, что основная площадка не перегружена проходящим через нее трафиком, а компании не приходится нести дополнительные затраты и проходить через процедуру установки нового физического канала.

На уровне локальной сети оверлейная сеть, как правило, означает создание

простой однородной физической топологии и использование VLAN-протоколов

IEEE 802.1q для наложения подсетей, необходимых пользователям.

При использовании VLAN и наложенных сетей очень сложно создать точные диа-

граммы сетевых топологий. Рекомендуем создать две диаграммы: одну, изобража-

ющую физическую топологию, и вторую, представляющую логические сети.

**7.1.11. Количество поставщиков**

Использование оборудования от большого количества разных поставщиков

может излишне усложнить управление сетью. Чем больше поставщиков предо-

ставляют вам сетевое оборудование, тем больше проблем с взаимодействием

у вас, скорее всего, появится. Кроме того, увеличивается нагрузка на админис-

траторов сети, которым придется изучить конфигурации и особенности разного

оборудования, а также следить за обновлением программного обеспечения

и отслеживать ошибки. Если свести количество поставщиков к минимуму,

можно повысить надежность и упростить обслуживание сети. Кроме того, это

поможет компании получить дополнительные скидки на оборудование благо-

даря увеличению объема поставок.

Однако сотрудничество с одним эксклюзивным поставщиком тоже имеет свои

недостатки. Не может быть такого, чтобы один поставщик производил лучшую

продукцию во всех областях. При сотрудничестве исключительно с одним поставщиком ваш протокол остается непроверенным на взаимодействие, что может

привести к неприятным сюрпризам при первом же контракте с новым постав-

щиком.

**7.1.12. Стандартные протоколы**

Сеть организации должна быть создана с использованием стандартных прото-

колов. Это правило со временем не меняется. Проприетарные протоколы поставщиков привязывают вас к одному конкретному поставщику, осложняя при

этом интеграцию оборудования от других производителей. Привязка к одному

поставщику усложняет получение скидок и мешает внедрить продукцию других

компаний, лишая вас возможности использовать ее преимущества. Кроме того,

на вас сказываются деловые проблемы вашего поставщика.

Если вам нужны возможности, предоставляемые исключительно проприетар-

ными протоколами поставщика, старайтесь убедить поставщика открыть стан-

дарт. В идеале стандарты должны быть проверенными, а не новыми, чтобы

обеспечить совместимость со всем оборудованием. Использование проверенных

временем стандартов IETF означает, что любое выбранное вами оборудование

или программное обеспечение будет совместимо с этими стандартами.

**7.1.13. Мониторинг**

Мониторинг сети необходим для построения быстрой и надежной сети, для масштабирования сети в соответствии с растущими потребностями, для поддержания безотказности сети. Сетевой мониторинг представлен двумя основными типами. Первый – мониторинг и оповещение о работоспособности в реальном времени. Второй тип – сбор данных для анализа тенденций изменения, который проводится с целью предсказания будущего спроса и составления счетов за пользование.

Мониторинг сети в реальном времени должен быть внедрен во все используемые

у вас системы уведомления о неисправностях. Как минимум, такой мониторинг

должен оповещать вас об изменениях состояния сетевого интерфейса. Другими

словами, система мониторинга должна сообщать об отказах сетевого интерфей-

са и, предпочтительно, о восстановлении его работоспособности.

Самая распространенная и самая важная цель сбора статистических данных –

прогнозирование будущих потребностей. В большинстве сетей достаточно

просто вести мониторинг всех нужных сетевых интерфейсов, отслеживая про-

ходящий через них объем трафика и проводя анализ тенденций изменения. Это

позволит определить момент, в который понадобится увеличение пропускной

способности. В других сетях (особенно в компаниях, связанных с интернет-ус-

лугами) предпочитают собирать данные о трафике в сети, определяя, с кем не-

обходимо осуществить прямое подключение, какой должна быть пропускная

способность таких подключений и где должны находиться такие пункты гео-

графически, чтобы можно было оптимизировать трафик в сети.

Сбор статистических данных по сбоям, ошибкам и отказам также может ока-

заться полезным и информативным, отображая моменты появления проблем

и их исчезновения. С помощью анализа статистических данных можно выделять

аномалии в поведении систем, которые могут свидетельствовать о наличии

проблем, или создавать статистику работоспособности для руко-

водства или пользователей.

**7.1.14. Одна административная единица**

Грамотное создание сетей, их обслуживание и решение связанных с ними про-

блем одновременно в нескольких организациях – задача сложная. Сеть должна

быть единым организмом, передающим трафик последовательно и координи-

рованно. Сеть должна регулироваться единым набором правил и инструкций,

которые единообразно используются по всей сети. Чем больше независимых

групп управляют движением трафика, тем выше риск, что работа сети станет

несогласованной и нескоординированной. Использование одной администра-

тивной единицы означает наличие одной организованной административной

группы с единой структурой управления. Если разные отделы группы админис-

траторов подчиняются структурам управления, которые пересекаются лишь на

уровне генерального директора, различные подразделения компании неизбеж-

но начнут двигаться в разных направлениях, следуя своим собственным инструкциям и правилам.

С отсутствием одной административной единицы связаны и проблемы безопас-

ности. Если разные части сети контролируют различные группы, у каждой

такой группы будут свои правила относительно подключения других сетей к их

участку сети и обеспечения безопасности таких подключений. Это приводит

к невозможности контролировать уровень безопасности сети, так как сеть – еди-

ное целое и ее безопасность определяется ее слабейшим звеном.

***7.2. Тонкости***

Помимо базовых задач существует несколько дополнительных аспектов, кото-

рые помогут вам улучшить свою сеть. Вы должны добиться баланса между

рискованным внедрением новых передовых технологий и использованием более

старых, но и более надежных технологий и оборудования. И наконец, если вы

окажетесь в ситуации, которая потребует от вас создания нескольких админис-

тративных единиц, вы можете последовать нашим советам, чтобы снизить

опасность возникающих проблем.

**7.2.1. Передовые технологии или надежность**

Как правило, самое важное качество сети, которого все добиваются, – это на-

дежность. Более старые решения, которые прошли множество проверок как

в аппаратном аспекте, так и в отношении прошивки, обычно отличаются повы-

шенной надежностью. Все ошибки в них уже исправлены. С другой стороны,

новые возможности и увеличенная скорость подключения, как правило, доступ-

ны только в новых продуктах, которые, возможно, еще не прошли полевые

испытания. И именно вы должны добиться нужного баланса.

Существует множество способов для управления этим риском. Вы можете про-

водить в лаборатории собственную сертификацию новых решений до их внед-

рения, а затем приступить к их постепенному развертыванию.

Вы можете создать отдельные клиентские группы, различающиеся между собой

степенью риска, на который они готовы пойти.

В некоторых случаях клиентские группы, которые согласны пойти на риск,

находятся в ведении другого отдела системного администрирования. А у этого

отдела могут быть клиентские группы с бизнес-требованиями, такими как не-

обходимость использовать некоторые новые технологии, как только они стано-

вятся доступными. Если это возможно, предоставьте им разбираться с пробле-

мами и используйте свой шанс позволить другим вместо вас исправлять ошиб-

ки. Учитесь на их опыте.

Если вы используете новейшие технологии, удостоверьтесь, что каждый сотруд-

ник, который может столкнуться с проблемами на первых этапах внедрения

этих технологий, знает, что из-за их новизны возможны сбои и простои в рабо-

те. Если не сделать этого заранее, ваши пользователи расстроятся, а репутация

вашей сети в целом серьезно пострадает. Если кто-либо из руководства одобря-

ет подобный риск, обязательно сообщите об этом конечным пользователями

и их непосредственным руководителям, чтобы в возможных простоях не обви-

няли лично вас. И даже в этом случае оборудование необходимо сначала настро-

ить и протестировать в лаборатории.

**Технологии**

**Ведущие технологии**. Самые современные технологии. Вы возглавля-

ете движение в эру новых технологий.

**Передовые технологии**. Это означает, что вы внедряете инновации

раньше, чем они становятся ведущими технологиями. Слово «передо-

вой» также означает «ближайший к неприятельскому фронту».

**Ударные технологии**. Удар – именно то, что получают юзеры, если они

постоянно находятся на передовой.

**7.2.2. Несколько административных единиц**

По различным причинам создать одну административную единицу может быть невозможно. Если разные организации управляют различными частями сети и не подчиняются единому уставу или единому органу управления, сети необходима другая

модель. Между различными частями сети должны быть явные границы, создан-

ные с использованием пограничных протоколов маршрутизации, таких как

BGP, и систем безопасности, в число которых входят брандмауэры. Это позволит

обеспечить стабильность маршрутизации и создать известные уровни безопас-

ности в каждой административной единице независимо от других.

Достаточно часто используется следующее разделение: одна группа – для воз-

можности подключения к глобальной вычислительной сети, а другая – для

обеспечения подключения к локальной сети. Такой подход разумен, так как

для поддержки этих сетей требуется разная квалификация. То же самое каса-

ется создания отдельной группы для управления подключением к Интернету

или для сетевой безопасности.

***7.3. Заключение***

Так как сетевые технологии стремительно меняются, некоторые из этих аспек-

тов со временем также претерпят значительные изменения. Но остальные ас-

пекты создания сети являются неизменными (константами).

Итак, хотя многие ключевые факторы, определяющие способ создания сети,

постоянно меняются, у вас есть возможность в качестве основы для своей сети

использовать некий фундамент, который упростит создание надежной сети

и позволит вам двигаться в ногу со временем.

**7.3.1. Константы создания сети**

Необходимость четкой архитектуры.

Надежность.

Грамотное документирование и ярлыки.

Соответствие IDF и MDF высочайшим стандартам проводки.

Надежные системы энергопитания и охлаждения для IDF и MDF.

Последовательное размещение IDF на всех этажах и во всех зданиях.

Точки разграничения.

Если возможно, создание одной административной единицы. В противном

случае четкое разграничение обязанностей.

Стандартные открытые протоколы (IETF и IEEE).

Простая маршрутизация узлов.

Выделенное сетевое оборудование для передачи пакетов.

Минимальное количество поставщиков.

По возможности отказ от использования ударных технологий.

**7.3.2. Изменчивые аспекты создания сети**

Необходимый тип проводки в помещении и между помещениями.

Топологии физических и логических сетей.

Сетевые устройства и протоколы.

Возможности подключения к глобальной вычислительной сети.

Структура подключения к Интернету.

Методы избыточности.

Технологии мониторинга.

***Глава 8***

***Пространства имен***

**Пространство имен** – это набор уникальных ключей и связанных с ними

атрибутов. В пространстве имен для каждого элемента предусмотрены атрибуты.

Для регистрационных записей существуют идентификаторы UID (UNIX) или

SID (Windows), домашние каталоги, владельцы и т. д. Атрибуты имени хоста,

как правило, включают в себя IP-адреса, серийные номера оборудования, ин-

формацию о пользователе (владельце), MAC-адрес Ethernet и т. д.

Термин пространство имен может сбить с толку, поскольку относиться он

может как к абстрактному понятию, так и конкретному явлению. В любой среднестатистической

компании есть абстрактное понятие пространства имен для имен пользователей.

Однако пространство имен одной компании будет отличаться от пространства

имен любой другой компании. В этом смысле компании обладают разными пространствами имен для имен пользователей. По большей части термин «пространство имен» относится к определенной (конкретной) базе данных пространства имен.

Пространства имен бывают самых разных видов. Некоторые из них являются

плоскими, то есть не имеют копий. Другие пространства имен являются иерархическими, например дерево каталогов. В каждом отдельном каталоге не могут существовать два файла с одинаковым именем. Но два файла с одним и тем же именем example.txt могут находиться в разных подкаталогах.

Чем крупнее и сложнее система, тем важнее формализовать управление про-

странством имен. Небольшие системы требуют значительно меньшей формализации своих пространств имен. Но мегакорпорации должны разделять и делегировать ответственность между несколькими подразделениями и сотрудниками.

***8.1. Основы***

**Основы пространств имен очень просты:**

Пространствам имен необходимы политики по именам, долговечности, ло-

кальности и защищенности.

Пространствам имен необходимы процедуры: добавление, изменение и уда-

ление.

Пространствам имен необходимо централизованное управление.

**8.1.1. Политики для пространств имен**

Пространства имен должны подчиняться общим политикам, а не отдельным

технологическим системам. Чем крупнее ваш отдел системных администрато-

ров, тем важнее оформить политики в письменном виде, а не просто полагаться

на устные традиции. Письменные политики должны быть основой требований, составляемых при создании автоматизированного обслуживания пространств имен. Кроме того, письменные политики регулируют отношения с клиентами.

**8.1.1.1. Назначение имен**

Политика по назначению имен для пространств имен должна отвечать на сле-

дующие вопросы. Какие имена разрешены в пространстве имен? Какие имена

запрещены в пространстве имен? Каким образом выбираются имена? Каким

образом решается проблема перекрытия имен? В каких случаях допускается

переименование?

Необходимы правила, какие имена могут стать частью пространства имен.

Некоторые правила диктуются технологией.

При выборе имен можно использовать несколько методов:

**1. Шаблонный.** Все имена составляются по строгому шаблону. Например, все

настольные рабочие станции получают имена pc- и четырехзначное число.

**2. Тематический**. Все имена соответствуют определенной теме. Например,

все серверы можно назвать в честь планет.

**3. Функциональный**. Имена соответствуют функциям. Учетные записи могут

соответствовать должностям и ролям (admin, secretary, guest); имена узлов

могут отражать обязанности машины (dns1, cpuserver22, web01) или группы

доступа (webmaster, marketing).

**4. Описательный**. Описательные имена обычно отражают фактическую ин-

формацию, а не правила. Подходящими примерами здесь являются метки

разделов диска, описывающие пользователей или данные, для которых

предназначен данный раздел диска (S:\Otdel\Finance, test data). Имена принтеров могут сообщать, какой используется принтер с драйвером (laserjet,

photo, 11Ч14) или где этот принтер установлен (testlab, inkjet, CEO-desktop).

**5. Нет метода**. Иногда шаблоном является отсутствие шаблона. Каждый

выбирает что-нибудь свое. Конфликты и перекрытия имен решаются по

принципу обслуживания в порядке поступления.

Эти четыре метода малосовместимы. После того как вы выберете одну опреде-

ленную схему, изменить ее будет достаточно сложно. Многие организации из-

бегают использования только одного метода, объединяя несколько методик. Но,

как правило, один метод берется за основу, а другой является вторичным.

Функциональные имена могут упростить конфигурацию программного обеспе-

чения. Службе поддержки будет проще обслуживать программное обеспечение,

если почтовый сервер носит имя pochta, а календарный сервер – calendar. Однако,

если такие серверы придется переносить на другие узлы, могут возникнуть

сложности. Лучше всего ввести функциональные псевдонимы, указывающие

на такие узлы. Такие псевдонимы, как DNS CNAME, отлично подходят для неинтер-

активных служебных машин, таких как почтовый сервер, веб-сервер, DNS

и т. д.

Метод, используемый для назначения имен, отражает корпоративную культу-

ру. Если вы хотите установить свободную и непринужденную рабочую атмос-

феру, latte – отличное имя для принтера. Для строгой корпоративной кульуры больше подойдет pc и четырёхзначный номер.

Имена обладают и аспектом безопасности. Внимание мошенников скорее при-

влечет имя sourcecodedb, чем имя server05. Кроме того, мошенники давно уже

поняли, что системные администраторы, как правило, нарушают правила на-

значения имен в своих собственных системах. Цель мошенников – как можно

дольше оставаться незамеченными. Поэтому они избегают узлов, за которыми

может быть установлено пристальное наблюдение, например настольных машин

системных администраторов. Если они обнаружат сеть, в которой все имена

узлов составлены по четкому шаблону, за исключением нескольких машин, мошенники решат, что последние и есть машины системных администраторов. Мошенники будут стараться избегать этих узлов, чтобы снизить свои шансы быть обнаруженными.

**8.1.1.2. Контроль доступа**

Политика по контролю доступа к пространству имен должна отвечать на следу-

ющие вопросы.

- Какие защита и уровень безопасности требуются данному пространству

имен?

- От чего мы пытаемся защитить имена и зачем?

- Нужно ли защищать имена в пространстве или только их атрибуты?

- Кто имеет право добавлять, изменять или удалять целые записи?

- Может ли владелец записи изменять определенные поля своей записи?

- От кого необходимо защитить содержимое пространства имен?

Это зависит от пространства имен. Доступ к просмотру пространства имен стоит запретить всем, если речь идет о списке паролей. Доступ к некоторым пространствам имен ограничивается узким кругом лиц.

Ответ зависит от каждого конкретного пространства имен, а также может зави-

сеть от контекста. Например, отдельные логины в UNIX-системе можно спо-

койно указывать в исходящих письмах, на визитных карточках, в рекламе

и т. д. Однако полный список таких идентификаторов не стоит нигде публико-

вать, так как его могут использовать спамеры для рассылки нежелательных

писем.

Пользователи должны иметь возможность менять только определенные параметры, и лишь отдельные сотрудники могут иметь право создавать или удалять учетные записи. С другой стороны, интернет-провайдеры часто позволяют пользователю создать учетную запись при условии, что он предоставит номер своей кредитной карты, и удаление учетной записи также производится пользователем.

Еще один аспект защиты включает в себя политики по контролю изменений

и резервному копированию. Важно иметь возможность отменить изменения.

Пространства имен, которые хранятся в формате нешифрованного текста, мож-

но включить в систему контроля изменений, например в SubVersion (UNIX) или

SourceSafe (Windows) для сетевого управления. Политики по резервному копи-

рованию должны особое внимание уделять пространствам имен. Резервное

копирование – главный страховой полис.

Каким образом пространство имен защищено от изменений – это другой вопрос.

В некоторых случаях пространство имен хранится в текстовом файле и измене-

ния можно предотвратить с помощью соответствующего контроля доступа

к файлам. В других случаях изменения вносятся через базу данных, которая

включает собственную систему контроля доступа. Важно помнить, что степень

защищенности пространства имен определяется методами, используемыми для

его изменения. Метод, используемый для обновления пространства имен, дол-

жен быть более защищенным, чем системы, чья безопасность зависит от данно-

го пространства имен.

**8.1.1.3. Долговечность пространства имен**

Политика по долговечности пространства имен должна отвечать на следующий

вопрос: когда необходимо удалять записи в данном пространстве имен? Срок

действия некоторых записей в пространстве имен должен заканчиваться в ус-

тановленный день или через определенный период бездействия. Можно указать,

что учетные записи должны обслуживаться одним из сотрудников, который

будет обновлять запрос раз в год. При отсутствии обновления учетные записи

должны удаляться. IP-адресов может быть недостаточно, и в слабо контроли-

руемой среде можно завершить срок действия IP-адреса, который был передан

пользователю, если система сетевого мониторинга показывает, что этот IP-адрес

не использовался в течение определенного количества месяцев.

Грамотные технологии позволяют вам маскировать имена, которые не должны

быть взаимосвязаны. Средство автоматического монтирования UNIX можно

использовать для того, чтобы пользователи обращались к репозиторию как

к /home/docs при скрытом имени файлового сервера. Расположение документов

не должно быть привязано к имени сервера. Тот факт, что они взаимосвязаны,

не должен касаться ваших пользователей.

Никогда не называйте веб-сервер www. Дайте ему общее имя, а www сделайте псевдонимом. Пользователям сообщите только псевдоним www, и тогда вы сможете спокойно переносить функциональность сервера на другой узел. Если вы постоянно используете псевдонимы и другие технологии, должным образом скрывающие имена, вы сможете без проблем переносить функциональность с одного узла на другой.

**8.1.1.4. Вопросы сферы действия**

Политика по сфере действия пространства имен должна отвечать на следующий

вопрос: где будет применяться данное пространство имен? Степень глобальности

или локальности того или иного пространства имен определяется двумя факто-

рами: диаметром (географически, то есть насколько широко оно используется)

и плотностью (сколько сервисов его используют).

**Диаметр** – это число систем, использующих конкретную базу данных пространства имен: один узел, кластер, отдел, вся организация и т. д. И хотя вся ваша

организация может пользоваться Microsoft ActiveDirectory, конкретная база

данных пространства имен – например, имена пользователей и пароли, – может

использоваться только машинами вашего подразделения. У иных подразделений

есть другие списки пользователей и паролей для своих машин.

Для сайтов, использующих сетевую информационную службу NIS, которые

часто являются UNIX-системами, характерно применение пространства имен

диаметром в один кластер UNIX-узлов. Каждый кластер имеет свои базы данных

пространства имен.

**Плотность** пространства имен определяется количеством служб, которые его

используют. Например, компания может создать уникальный идентификатор

для каждого сотрудника и использовать его для адреса электронной почты человека, логина, идентификатора входа во внутрисетевые службы, имени в модемных пулах, службах VPN и т. д. Даже несмотря на то что эти системы используют различные базы данных и протоколы – ActiveDirectory, NIS, RADIUS и т. д., – идентификатор применяется везде.

Иногда глобальное плоское пространство имен нежелательно. В некоторых

случаях используемая технология обеспечивает иерархическое пространство

имен. Например, именам узлов необязательно быть уникальными в масштабе

всей корпорации, потому что DNS обеспечивает зоны и подзоны. При наличии

зон DNS в подразделениях каждое подразделение может иметь машину www. –

в идеале псевдоним реального сервера с более уникальным именем. Подразде-

ление может даже называть свои настольные ПК как pc и номер, и сайтам не

придется координироваться друг с другом, чтобы обеспечить использование

непересекающихся номеров.

**8.1.1.5. Целостность**

Политика целостности пространства имен должна отвечать на следующий вопрос: целостность каких атрибутов должна сохраняться при использовании

одного имени в нескольких пространствах имен?

**Высокая целостность** означает, что имя, применяемое в одном месте, будет

иметь те же самые атрибуты во всех других местах, где оно существует. Напри-

мер, вы можете создать такую политику: если у кого-то есть учетная запись

UNIX, цифровой идентификатор пользователя UID должен быть одним и тем

же везде, где у человека есть учетные записи.

**8.1.1.6. Повторное использование**

Политика повторного использования пространства имен должна отвечать на

следующий вопрос: через какое время после удаления или прекращения срока

действия имя может использоваться повторно? Обычно можно немедленно

повторно использовать имя. Например, вы можете сразу повторно использовать

имя принтера без необходимости перенастройки компьютера.

Однако с адресом электронной почты следует быть более осторожным. Возмож-

но, ваша политика предполагает, что после удаления адреса электронной почты

никто не может пользоваться им в течение 6 месяцев, чтобы снизить вероятность

получения новым владельцем электронной почты, адресованной другому лицу.

Эта политика предотвращает следующий злонамеренный прием: в некоторых

компаниях есть автоматизированная процедура перенаправления почты с имен-

ных адресов.

Политика повторного использования может быть реализована программно.

Однако в небольших и редко изменяющихся пространствах имен системному

администратору просто следует учитывать последствия повторного использо-

вания. Например, если вас просят дать компьютеру пользователя имя, которое

недавно использовалось для популярного сервера, вы можете предложить дру-

гое имя, чтобы предотвратить путаницу. Путаница будет особенно серьезной,

если все еще используется большое количество бумажной документации, содер-

жащей имя сервера.

**8.1.1.7. Выводы**

Политики назначения имен, контроля доступа, долговечности, охвата, целост-

ности и повторного использования должны быть записаны, одобрены управляю-

щим и техническим персоналом и доступны для ознакомления пользователям

и системным администраторам, четко устанавливая таким образом правила ва-

ших пространств имен. Так можно избежать многих проблем. Небольшие сайты

могут себе позволить работать без такой документации потому, что в данном

случае требуется совсем немного системных администраторов, которые работают

вместе, и такая политика является частью их культуры. Однако такой нефор-

мальный подход становится препятствием расширяемости. Сайты со временем

становятся крупнее и вдруг оказываются под управлением большего количества

системных администраторов, не посвященных в «стандартные» методы работы.

Документирование упомянутых политик может предотвратить многие разногла-

сия. Таким образом, новый системный администратор, несогласный с ними,

может обсудить любые предлагаемые изменения. Без документации каждый

системный администратор волен полагать, что его способ – правильный (более

подробно процедуры документирования рассмотрены в главе 9).

**8.1.2. Процедуры изменения пространства имен**

Всем пространствам имен требуются процедуры добавления, изменения и уда-

ления их элементов. Эти процедуры должны документироваться так же, как

и политики, но документация может быть недоступной пользователям. Опять

же, малая группа сможет работать без явного письменного указания этих про-

цедур. Эти действия осуществляются только людьми, создавшими систему,

и поэтому не требуют документации. Однако с ростом системы и привлечением

новых системных администраторов появляется беспорядок. Документация

может выполнять двойную функцию, предоставляя как основу для обучения,

так и пошаговую инструкцию при выполнении задачи.

Если что-то можно кратко и понятно задокументировать, то это можно автома-

тизировать.

**8.1.3. Централизация управления пространством имен**

Управление пространством имен должно быть максимально централизованным,

насколько это возможно для любой конкретной среды. С централизацией при-

ходит целостность. Иначе пространства имен становятся разрозненными на

различных серверах или даже в различных директориях на одном сервере.

Лучше иметь один узел, поддерживающий ваши пространства имен, и распро-

странять их по другим узлам.

GNU-приложение cfengine Марка Барждеса (Burgess 1995) – отличное средство

под UNIX для поддержки контрольных копий пространств имен и файлов

и распространения их по узлам. Преимуществами этого средства являются

автоматическое поддержание любой конфигурации узла UNIX и возможность

программирования других конфигураций для определенных узлов. Microsoft

ActiveDirectory и OpenDirectory в Mac OS X были созданы по другому принци-

пу – клиенты должны отправлять запросы на LDAP-серверы, которые центра-

лизованно хранят информацию о пространствах имен.

***8.2. Тонкости***

**8.2.1. Одна большая база данных**

**Централизация** – хорошая практика, а централизация всех пространств имен

в базе данных SQL даже лучше. Вы можете разработать клиент (веб-приложение

или приложение с оконным интерфейсом), который позволит операторам вносить

большинство изменений. Затем программы могут передавать данные другим

системам, например ActiveDirectory, LDAP, NIS, конфигурациям принтера

и т. д.

**8.2.2. Дальнейшая автоматизация**

После завершения основ дальнейшая автоматизация упрощается. Если первич-

ная автоматизация была сделана правильно, более высокие ее уровни могут

быть интерфейсами первичной автоматизации и обеспечивать, например, до-

полнительную проверку данных или возможность повторять процесс много-

кратно.

Если вы способны повторно проводить процесс по элементам пространств имен,

автоматизация может управляться последними. Например, простая итерация

по пространству имен passwd может быть основой системы, которая проверяет

различные параметры безопасности, например содержимое файла .rhosts. Мно-

гие сайты имеют один список рассылки на подразделение, и эти списки рассы-

лок могут автоматически генерироваться из корпоративной директории.

Учетная база данных всех систем может быть одним из ваших наиболее мощных

пространств имен, если поддерживается его актуальность, а этот процесс мож-

но частично автоматизировать.

**8.2.3. Обновление, управляемое пользователем**

Автоматизация также может пойти в другом направлении: к большей самосто-

ятельности пользователей. В каждой среде есть много возможностей для авто-

матизации служб. Периодически просматривайте свои журналы запросов

и проведенных работ, обсудите с пользователями, что бы они хотели автомати-

зировать. В разделе 3.1.3.3 описана система DHCP, которая автоматизирует

выдачу IP-адресов.

**8.2.4. Эффективное использование пространств имен**

Всеобъемлющие пространства имен могут быть полезны не только в вашей

компьютерной инфраструктуре, но и в других инфраструктурах. Существует

тенденция по снижению нагрузки по администрированию некомпьютерной

инфраструктуры за счет ее привязки к пространствам имен компьютерной ин-

фраструктуры.

***8.3. Заключение***

Во-первых, мы должны осознать, какую роль выполняют пространства имен в системе. Очевидно, что всем пространствам имен присущи определенные качества. Про-

странствам имен требуются правила для присвоения имен, контроля доступа,

долговечности, сферы действия, целостности и повторного использования.

После определения правил можно установить процедуры. Правила необходимо

сформулировать до установки процедур, потому что первые должны определять

последние.

Установление записанных правил и процедур для пространств имен улучшает

согласованность в работе команды системных администраторов и дает пользо-

вателям представление о том, на что они вправе рассчитывать. Пространства

имен могут значительно выиграть от централизованного управления и автома-

тизации.

Пространства имен являются частью базовой инфраструктуры компьютерной

среды. Эффективно управляемые пространства имен являются одной из клю-

чевых систем, которые обеспечивают стабильную работу других систем. Напри-

мер, вы можете поддерживать систему электронной почты без эффективно

управ­ляемого пространства имен, но это будет сложно, утомительно и непонят-

но пользователям системы.

Для эффективной работы по поддержке пространств имен требуется автомати-

зация, а хорошие пространства имен могут помочь в дальнейшей автоматизации,

если они обеспечивают стандартизированные методы, или API. Перенос всех

пространств имен в единую крупную систему баз данных позволяет нам получить

максимальное преимущество.

После создания основы появляются новые возможности. Создание всех про-

странств имен из единой системы баз данных может быть выгодным. Можно

обеспечить лучшую автоматизацию, в том числе такую, которая позволит поль-

зователям удовлетворять свои потребности без вмешательства системного ад-

министратора. Наконец, мы позитивно отметили тенденцию привязки неком-

пьютерной инфраструктуры, такой как кадры, офисная АТС и системы доступа

по смарт-картам, к централизованным базам данных.

***Глава 9***

***Документация***

Документирование означает ведение записей о том, где что находится, объяснение того, что и как выполняется, и обеспечение доступности полезной информации для пользователей. Обычно системные администраторы не любят писать документацию: времени едва хватает на текущие задачи, зачем еще писать документацию? Причина в том, что документация во многом помогает и ее недостаток снижает возможности системных администраторов эффективно работать.

Применяйте документацию как средство для облегчения вашей работы.

Документация – это способ создания «памяти» организации, которая позволяет

команде системных администраторов повышать свой уровень знаний и навыков.

Считайте документацию RAID-массивом для системных администраторов: она

обеспечивает избыточность группы.

За счет одновременного хранения и распространения знаний документация позволяет организации развивать своих людей.

***9.1. Основы***

**9.1.1. Что документировать**

Наиболее важные для документирования процессы чаще всего являются либо

сложными и неприятными, либо теми, которые вы постоянно объясня-

ете кому-то. Иногда предмет документирования принадлежит обеим категори-

ям, например доступ к корпоративной сети в поездках.

Если процесс имеет множество этапов, требующих точного порядка выполнения, – особенно если в случае ошибки вам приходится звать на помощь своего руководителя, – имеет смысл задокументировать его как можно скорее. Вы избавите кого-нибудь от множества трудностей, и этим «кем-нибудь» можете быть вы сами.

Документирование нелюбимых вами задач упрощает поиск других людей для

их выполнения. Часто самым сложным элементом является собственно разра-

ботка процесса, а затем его выполнение становится проще.

Должностные инструкции обычно состоят из двух частей – списков обязаннос-

тей и требуемых навыков. Создайте список обязанностей, перечислив процессы,

которые вы не любите выполнять и которые были задокументированы. Создай-

те список требуемых навыков, рассмотрев каждый документ и определив навы-

ки и технологии, с которыми системный администратор должен быть знаком,

чтобы понимать документацию. В принципе, все должностные инструкции

пишутся сами собой.

**9.1.2. Простой шаблон для начала**

Самый сложный этап создания документа – это начало. Вот простой принцип:

определите четыре основных элемента документа – название, метаданные, что

и как. Создайте шаблон или план документа и заполните его разделы с начала

до конца.

1. **Название**: простое название, понятное другим.

2. **Метаданные:** контактная информация автора документа – обычно ваша,

дата последней редакции или история изменений. Люди, читающие доку-

мент, смогут обратиться к автору с вопросами, а когда вы получите повы-

шение, ваши преемники будут помнить вас как человека, давшего им этот

документ. Дата последней редакции и история изменений помогут людям

понять, является ли документ все еще актуальным.

3. **Что**: предложение, описывающее содержание документа или цель, кото-

рой человек должен достичь, следуя указаниям. Достаточно одного-двух

предложений.

4. **Как**: шаги, предпринимаемые для выполнения задачи.

Затем тщательно проверьте уровень качества документа. Точность имеет очень

важное значение. Опечатка или пропущенный шаг может привести к тому, что

человек создаст больше проблем, чем предполагалось решить с помощью доку-

мента.

Выполните шаги, указанные в документе, самостоятельно вводя каждую ко-

манду. Затем попросите кого-нибудь другого выполнить задачу, используя до-

кумент, и предоставить вам отчет, где он встретил какие-то затруднения.

После успешного использования этой документации несколькими сотрудника-

ми создайте на ее основе более емкое «краткое руководство», обобщающее шаги.

Это руководство просто поможет опытным системным администраторам ничего

не забыть. У системных администраторов должна быть возможность вырезать

и вставлять командные строки из этого документа в консоль, чтобы ускорить

процесс.

**9.1.3. Простые источники для документации**

Один из способов упрощения ваших задач по документированию – сделать по-

метки при следующем выполнении задачи. Даже если это замедлит процесс, это

будет проще, чем написание документа по памяти.

**9.1.3.1. Сохранение скриншотов**

Научитесь пользоваться средством для снятия скриншотов. Когда вы в следу-

ющий раз будете делать что-то, что хотите описать в документации, снимайте

скриншоты при выполнении каждого шага. Если вы создадите документ из

скриншотов, все, что вам останется, – это добавить одну-две строки текста

к каждому изображению, описывающие, что выполняется на данном этапе.

Таким образом вы получите детализированный и наглядный мультимедийный

документ.

**9.1.3.2. Сохранение содержимого командной строки**

Если вы чаще работаете с командной строкой, чем с графическим интерфейсом,

копируйте и вставляйте в документ содержимое окна терминала или консоли.

Некоторые программы терминалов или консолей содержат функцию сохранения

в файл, UNIX-команда script сохраняет в файл весь сеанс.

UNIX-команда history возвращает список последних выполненных команд. Эти

сохраненные команды при преобразовании в автоматизированный скрипт могут

быть начальной точкой документации процесса. Документация является первым

шагом к автоматизации: если вы не знаете точно, как вы что-то делаете, вы не

сможете это автоматизировать.

**9.1.3.3. Применение электронной почты**

Две основные проблемы в непосредственном применении электронной почты

для документации заключаются в том, что электронную почту трудно исполь-

зовать совместно и что она, скорее всего, окажется плохо организованной.

Обычно имеется большое сообщение и несколько входящих и исходящих сооб-

щений меньшего размера, в которых что-то решается или обсуждается. Объеди-

ните эти отдельные сообщения в один файл и поместите его там, где ваши кол-

леги смогут его найти.

В своей папке отправленной почты вы можете поискать сообщения, которыми

можно воспользоваться, чтобы собрать документ на определенную тему. Поль-

зуйтесь возможностью своего клиента электронной почты сортировать сообще-

ния по сеансам или темам, чтобы найти сообщения, подходящие для преобра-

зования в документацию. Если по какой-то теме было более одного или двух

обменов сообщениями, переписка, скорее всего, содержит достаточно информа-

ции для преобразования в документ.

**9.1.3.4. Изучение системы заявок**

Другим хорошим источником потенциальной документации является система

заявок на устранение неисправностей или обработки запросов в вашей органи-

зации. В некоторых таких системах есть средства создания базы решений или

документов решений, которые могут отправляться при поступлении новых

запросов, похожих на уже решенные.

На многих сайтах используются программы с поддержкой базы решений, но эта

возможность никогда не применяется и даже не включается. После первых

нескольких применений пользоваться ею становится проще, поэтому включите

ее и начните пользоваться ею прямо сейчас.

Если вы знаете, что при написании документации будете пользоваться своей

системой заявок, то можно упростить процесс и сделать информацию в запросах

более полезной. Если ваши системные администраторы отмечают, как они ре-

шают проблему, в том числе сохраняют команды и результаты и включают их

в журнал обработки заявки, это быстро повышает ценность таких журналов для

совместно используемой документации.

Вы можете дополнить свою систему заявок пометкой «база знаний» и полем для

комментария, где будете отмечать процессы, которые нужно описать в докумен-

тации.

**9.1.4. Преимущества контрольных листов**

Хорошим способом начать создание документации и вообще более эффективно

работать является использование контрольных листов, или списков действий,

организованных таким образом, что каждая строка или абзац содержит только

один шаг. Каждый завершенный этап можно будет отметить значком.

Контрольные листы позволяют вам выполнять сложные задания с уверенностью

в том, что вы завершили все этапы. Пропуск шага будет очевиден, если вы от-

мечаете их по мере завершения. Контрольный лист может применять кто-то

менее опытный, чтобы убедиться в том, что каждый элемент процесса был за-

вершен.

Типичные контрольные листы включают:

1. Задачи, которые необходимо выполнить при каждом найме на работу ново-

го сотрудника.

1. Задачи, которые необходимо выполнить при каждом увольнении сотруд-

ника.

1. Задачи по установке каждой операционной системы, которая используется

в организации.

1. Процессы по архивации и внешнему хранению данных в соответствии с тре-

бованиями юридического отдела.

1. Процессы по обеспечению безопасности ОС перед вводом машины в эксплу-

атацию.

Добавьте контрольные листы к обычной документации, особенно для часто

выполняемых задач. После нескольких применений полного документа чело-

веку понадобится только контрольный список.

**9.1.5. Хранение документации**

Создание места для хранения документов, или хранилища документов, явля-

ется важным шагом в процессе документирования. Централизованное разме-

щение обеспечивает начальную точку для организации и обновления докумен-

тов.

Если существует центральное хранилище, люди будут приносить различные документы, написанные ими. У большинства системных администраторов есть одна или

больше директорий со справочными документами, и они с радостью поделятся

ими, если появится место, где их можно разместить.

Самым простым методом создания хранилища документов является создание

директории с документацией на диске с общим доступом. Начните ее заполнение

с файла README, описывающего все правила и политики, которым необходи-

мо следовать при создании документации для включения в данное хранилище.

По мере создания системными администраторами документов вносите их в со-

ответствующую поддиректорию, создавая ее по необходимости, и используйте

информативные имена для файлов с документацией.

В хранилище документов полезно ввести контроль исходного кода, помогающий

при поиске более ранних версий документов, если кто-нибудь внесет изменения,

которые окажутся неверными, или файл будет случайно удален. Обычно гораздо

проще проверить наличие дубликата в хранилище исходного кода, чем восста-

навливать копию с резервного носителя.

Веб-сайт может быть отличным хранилищем документов, но поддержка табли-

цы содержания вручную и другие задачи могут потребовать больше работы, чем

вы сэкономите за счет наличия документов. Одно из решений – настроить веб-

сервер, чтобы он выводил содержимое директорий.

**9.1.6. Системы wiki**

**Wiki** – это веб-хранилище документов, которое обеспечивает простое добавление

и редактирование документов любому, кто имеет соответствующий доступ.

Документы могут содержать обычный текст, текст на языке разметки гипер-

текста (HTML) или текст с особыми тегами или командами wiki. Часто в wiki

имеется встроенная система контроля исходного кода для проверки создаваемых

и удаляемых файлов документации и хранения истории изменений.

Наиболее сильная сторона wiki заключается в том, что кто угодно может редак-

тировать любую страницу. Если что-то неправильно или устарело, то человек,

заметивший ошибку, может исправить ее либо оставить замечание, чтобы кто-

нибудь проверил и поправил информацию.

Все изменения отслеживаются по пользователю, поэтому любой нарушитель будет определен. В корпоративной среде такие происшествия будут редкими за счет общественного давления. Если они случаются, страницы могут быть

возвращены к предыдущему состоянию при помощи полных историй изменения.

Можно защитить страницы, чтобы редактировать их могли только определенные

люди.

Поддерживаются многие условные обозначения электронной почты, например \*этот

текст будет полужирным\* и \_этот текст подчеркнут\_. URL автоматически преобразуют-

ся в гиперссылки. Имена других страниц wiki распознаются и преобразуются

в ссылки. Страницы wiki обычно именуются на языке CamelCaps, известном

также как WikiWords или StudlyCaps, поэтому программы легко могут их вы-

явить. При применении слова WikiWord, не связанного ни с какой существую-

щей страницей wiki, будет сформирована ссылка с предложением пользователю

создать страницу.

Возможность создавать заранее подготовленные страницы для объектов, кото-

рые, по вашему мнению, вам скоро понадобятся, очень полезна. Она чрезвычай-

но полезна, но, пока вы с ней не столкнетесь, вы можете и не подозревать о ее

важности. Можно создать таблицу содержания хранилища документов и вносить

в нее документы по мере их создания.

Вместе эти функции создают идеальное средство для совместной работы. Оно

может быть очень удобным для того, чтобы посмотреть, как быстро документы

обретают форму и хранилище начинает выглядеть реальным и полезным. Это

побуждает других людей вносить свой вклад и поддерживает динамику.

**9.1.7. Средство поиска**

Функционирующей системе документации необходимо средство поиска. Люди

часто помещают данные туда, где другим трудно их найти. К счастью, для веб-

хранилищ существует много встраиваемых поисковых систем. Эти средства

варьируются от пакетов с открытым исходным кодом до аппаратных средств,

созданных для индексирования данных всей организации. При выборе поиско-

вой системы учитывайте уровень детализации поиска и наличие нужных вам

опций поиска, а также то, какие типы документов доступны для полнотексто-

вого индексирования.

Предпочтительно иметь возможность ограничения поиска по определенным

областям или объектам. Можно задать поиск только по названиям документов

или тексту на страницах, с которыми они связаны ссылками. Другие виды по-

иска могут работать с содержимым самих документов или ключевыми словами

либо тегами, связанными со страницами.

**9.1.8. Проблемы внедрения**

Важнейшим аспектом при создании нового хранилища документов является

обеспечение заинтересованности и участия сообщества, которое будет им пользо-

ваться. Пользователи хранилища являются также и авторами, и если большинство людей не захотят проявлять инициативу, эффективность всего проекта будет

сомнительной. Как ни странно, среди противников этого проекта бывает много

специалистов «старой закалки». Они привыкли к миру общения по электронной

почте и считают, что не стоит тратить свое время на создание общего веб-ресурса.

Естественно, в данном случае стоит привести аргументы в пользу создания единой

папки входящих сообщений для обзора новых материалов. Одним из способов

решения данной проблемы является обеспечение автоматической генерации

раздела «Последние изменения» как элемента wiki. Некоторые системы позво-

ляют периодически рассылать эту страницу по списку заинтересованных людей,

чтобы ее можно было читать, как блог. Предоставление различных способов до-

ступа к информации упрощает принятие людьми новшества.

**9.1.9. Самоуправление или прямое управление**

Лучше заранее решить, должен ли менеджер либо администратор библиотеки

сайта обеспечивать всю необходимую поддержку хранилища документов или

сайт должен быть самоуправляемым.

Если можно включить управление сайтом в чьи-нибудь служебные обязанности,

то при помощи последовательных улучшений можно будет создать гораздо более

полезный сайт. В качестве примера можно привести обзор журналов поиска

и журналов ссылок, по которым обращаются пользователи, чтобы определить

информацию, которую людям трудно найти, а затем более явно выделить ее на

сайте.

Если учреждена должность менеджера сайта, он должен способствовать само-

стоятельному развитию системы, а не быть цензором. Менеджер сайта нужен для поддержки и развития инфраструктуры сайта, перемещения документов в нужные места и повышения удобства пользования.

***9.2. Тонкости***

**9.2.1. Динамическое хранилище документов**

Идея сайта «живой документации», или динамического хранилища документов,

заключается всего лишь в том, что предполагается периодическое обновление

сайта или хранилища для удовлетворения потребностей среды. В отличие от стандартного хранилища документов, «живое» хранилище документации

смещает акцент на взаимодействие пользователя с документами. Пользователь

может комментировать, редактировать, собирать документы в обзоры, отправлять

ссылки на документы коллегам и т. д., а не просто найти и прочитать документ.

Wiki - центральная точка организации информации, содержащая ссылки на другие информационные системы.

**9.2.2 Система управления содержимым**

**Система управления содержимым** CMS (Content-Management System) – это

система публикации для веб-сайтов. Система CMS выпускает статью в определенное время, размещая ее на веб-сайте, обновляя таблицы содержания и разбираясь с другими деталями. На IT-сайте CMS может предоставлять дополнения, расширяющие функции портала, например возможность отображать обзор недавних сбоев.

Для реализации функционирующей CMS требуется ряд элементов. Система

управления содержимым состоит из трех уровней: хранилище, история и пред-

ставление. Уровень хранилища обычно представляет собой базу данных, но

также может быть структурированной файловой системой с метаданными. На

этом уровне хранится содержимое. Уровень истории реализует контроль версии,

разрешения, регистрацию событий и такие функции, как присвоение глобальных

идентификаторов новым документам. Уровень истории может быть реализован

как отдельный журнал или база данных, а может находиться в хранилище.

**9.2.3. Культура отношения**

Сайт «живой документации» требует культуры отношения, иначе люди будут

сомневаться, стоит ли им что-то писать, или сочтут, что они могут писать толь-

ко «одобренные» материалы.

Не стоит позволять всем и каждому редактировать инструкции по проверке резервного генератора, но ведь даже компетентный автор может, например, что-то упустить или исказить в первоначальной публикации. В большинстве случаев эту проблему можно решить, предоставляя возможность оставлять комментарии к странице и преобразовы-

вать комментарии в содержимое, когда сам автор или достаточное число других

комментаторов посчитают их справедливыми. Если случайно будет сделана

ошибка, контроль версий может предоставить доступ к неизмененной версии.

Будьте готовы к тому, что вам придется потратить некоторое время на управле-

ние системой wiki, пока люди не освоятся с ней и не поднимутся до уровня вашей

культуры. Определите, какая степень детализации будет «правильной» для

вашей группы, и, как это бывает с любыми документами, прежде чем все станет

выглядеть так, как вы считаете нужным, будут иметь место какие-то разногла-

сия между обеими сторонами.

**9.2.4. Классификация и структурирование**

Системы wiki обычно слабо структурированы. Некоторые просто предоставляют

возможность навигации.

Не тратьте много времени на структурирование на начальном этапе. Основным

врагом wiki-проектов является введение слишком жесткого структурирования

на ранних стадиях. Wiki так широко распространились именно благодаря принципу низкого уровня ограничений при внесении записей. Обновление страницы

должно быть таким же легким, как отправка электронного письма, иначе люди

просто не будут пользоваться этой функцией. Гораздо лучше заниматься дове-

дением некоторых страниц до нужной степени удобочитаемости, чем оставить

эту информацию в папках чьей-нибудь почты, где никто не сможет ее найти,

когда хозяин в отпуске.

Различайте написание документации и организацию документации. С ростом

объемов ваших материалов люди все чаще будут пользоваться поиском, а не

категориями, чтобы найти интересующие их данные. Вы всегда можете создать

структурированные категории и реорганизовать страницы или ссылки на них

с ростом wiki.

**9.2.5. Дополнительное применение документации**

Приведем еще несколько способов применения системы «живой документации».

Во многих системах wiki есть шаблоны или дополнения специально для этих

приложений.

**9.2.5.1. Служба самостоятельной помощи**

Пользователи могут применять раздел службы самостоятельной помощи сайта

документации для прямого взаимодействия с сайтом. Например, ссылка **«Создать новую заявку»**, которая позволяет пользователям сделать запрос через систему заявок.

Этот раздел – подходящее место для таких объектов, как новости о запланиро-

ванных отключениях, обновлениях по текущим процессам и явные ссылки на

политики и документы How-To1.

Еще одна функция в разделе службы самостоятельной помощи – это доступ

пользователей к обзору результатов, например графиков загрузки нескольких

маршрутизаторов (Multirouter Traffic Graphics – MRTG), или даже вызываемые

скриптом данные о свободном месте на общих дисках.

**9.2.5.2. Внутренние документы группы**

Создание собственных документов группы является началом формирования «памяти» подразделения, которая является очень важным элементом преемственности в любой группе.

Любая группа или подразделение может получить пользу от создания собствен-

ного раздела на сайте, хотя группа системных администраторов может быть

первопроходцем. Фактически в некоторых группах есть сайты «живой доку-

ментации» в форме хранилища исходного кода, в котором помимо кода можно

собирать спецификации, списки пользователей, материалы по маркетингу.

Поскольку внутренняя документация группы требует бережного отношения,

доступ в этот раздел должен быть органичен, чтобы им обладала только эта

группа и руководящий персонал.

**9.2.5.3. Документы How-To**

На многих сайтах имеются короткие пояснительные документы, называемые

How-To или HOWTO, которые дают возможность пользователям помочь себе

самостоятельно, когда обратиться к системному администратору невозможно.

В каждом документе HOWTO рассматривается одна тема, обычно выполнение

конкретной задачи, адаптированное под среду сайта. В них обычно включают

как вводимые пользователем команды, как и ответы программ, часто со скрин-

шотами. Документ HOWTO создан, скорее, для решения конкретной проблемы,

чем для использования в качестве учебного пособия как такового.

**9.2.5.4. Часто задаваемые вопросы**

Часто задаваемые вопросы (FAQ – Frequently Asked Question) являются средством, знакомым большинству пользователей Интернета. FAQ – это просто список

наиболее распространенных вопросов по конкретной теме, часто организован-

ный в виде разделов и подразделов и обычно развивающийся со временем. Не-

которые дополнения для wiki автоматически создают таблицу содержания,

выводя список вопросов в виде гиперссылок, ведущих к ответам (такой подход

имеет тот недостаток, что затрудняются чтение всех вопросов и ответов по по-

рядку, поиск по списку или его распечатка).

Список FAQ и набор документов HOWTO различаются, главным образом, дли-

ной и форматом. HOWTO – это разбор одной темы, а FAQ – набор вопросов

и ответов. Часто ответ может указывать на документ HOWTO или несколько

документов на выбор, отвечающих запросу пользователя.

**9.2.5.5. Справочные списки**

**Справочные списки** – это списки объектов, которые не используются часто, но

служат для конкретной цели. Например, список корпоративных сокращений

не является чем-то, требуемым ежедневно, но если вы увидите какое-то сокра-

щение впервые, то сможете посмотреть его в списке.

Вот несколько примеров подобных списков:

- Поставщики и их контактная информация.

- Серийные и инвентарные номера аппаратных средств.

- Лицензионные ключи и количество пользователей для программ.

- Списки совместимости: какие оптические мыши совместимы с какими аппа-

ратными средствами, какие драйверы работают с какими контроллерами.

- Каталог сотрудников: ручной или автоматически создаваемый из корпора-

тивной базы данных.

- Корпоративные сокращения.

- Список местных ресторанов, служб такси и т. д.: одна страница на офис.

**9.2.5.6. Процедуры**

Многие организации должны соответствовать международным стандартам ISO

(International Organisation for Standardization), нормам техники безопасности

и гигиены труда OSHA (Occupational Safety and Health Administration) или

положениям закона Сарбейнса–Оксли об управлении. Такие сайты выигрыва-

ют от наличия простого способа создания, поддержки и доступа к процедурам,

контрольным спискам и скриптам, относящимся к актуальным методикам.

Создайте журнал регистрации процедур и записывайте соблюдение процедур.

Документировать процедуры и вести журналы регистрации полезно даже в том

случае, если вы не обязаны это делать. Когда нужно отключить генератор после

восстановления подачи энергии, описание процедуры, позволяющей правильно

это сделать, будет более полезным, чем схема, показывающая все электрические

соединения в вычислительном центре.

**9.2.5.7. Техническая библиотека или информационный сборник**

Документы, полученные от продавцов, поставщиков и клиентов, статьи, кото-

рые вы купили или загрузили из других источников, и, возможно, даже руко-

водство по ремонту кухонной раковины – этот раздел хранилища может быть

сложным для систематизации. На некоторых сайтах просто создаются списки

содержимого в алфавитном порядке, на других назначается библиотекарь, ко-

торый выполняет подробную классификацию документов. Если классификация

будет слишком объемной, это затруднит, а не облегчит поиск документов.

**9.2.6. Ссылки на внешние источники**

Интернет содержит огромное количество полезной информации по технической

и деловой тематике. Большую часть этих данных нельзя воспроизвести на вашем сайте из-за авторских прав или практических соображений, или необходимости своевременного обновления. Однако ссылки на эти данные могут быть очень полезны для ваших пользователей.

Важно, чтобы для таких ссылок применялась служба перенаправления с со-

хранением анонимности. Большинство браузеров, когда запрашивают страни-

цу, включают в запрос ссылку на страницу, которая направила браузер на за-

прашиваемую страницу. Это позволяет сайтам отслеживать, кто дает на них

ссылки и какие из этих ссылок наиболее удачны. Однако имеется проблема

безопасности: если направившая страница находится на внутреннем веб-сайте,

то сайт, на который была ссылка, узнает о существовании этого внутреннего

сайта. Сайт, на который была дана ссылка, может узнать имя вашего внутрен-

него веб-сервера, что не должно стать проблемой, если только ваша безопасность

не основана на простом сокрытии имен узлов. Однако полный URL может рас-

крыть секретные условные названия проектов и другую информацию. Решение этой проблемы состоит

в обеспечении перенаправления хранилищем документов внешних ссылок через

службу, которая удаляет заголовки источников ссылок.

***9.3. Заключение***

Документация предоставляет пользователям нужную информацию, поэтому

они реже беспокоят системных администраторов, что приводит к экономии

времени последних. Документация позволяет системным администраторам

повторять процессы без ошибок и упрощать их, чтобы было легче передавать

поддержку процессов другим людям.

Документацию проще создать, применяя шаблон, с которым вы можете исполь-

зовать скриншоты, сохраненные сеансы работы с терминалом, архивы элект-

ронной почты и системы заявок для помощи в создании содержимого докумен-

тов. Контрольные листы являются хорошим способом документации многоша-

говых процедур, что поможет вам повторять их в одной и той же последователь-

ности, документировать требования других групп к вам или обеспечить младшим

системным администраторам способ отметить выполненные задания и передать

этот отчет руководителю.

Процесс документирования является сложным. Однако, как только вы продела-

ете тяжелую работу по созданию процесса, документацией смогут воспользовать-

ся менее информированные люди. Таким образом, выполнение процесса станет

проще поручить кому-то другому. Наличие документации по процедурам упро-

щает составление должностных инструкций при найме новых сотрудников.

Документы должны находится в хранилище, чтобы их можно было поддержи-

вать и использовать совместно. Очень удобной системой для создания хранилищ

являются wiki, потому что они упрощают создание и обновление документов

и не требуют знания HTML. При помощи дополнений wiki могут предоставлять

дополнительные службы.

Людей может быть трудно привлечь к использованию хранилища документации.

Предоставление помощи, обучения и шаблонов снижает этот барьер.

Хранилища могут быть удобны не только для процедур. Они могут стать служ-

бами самостоятельной помощи и содержать документы HOWTO, списки FAQ,

справочную документацию и инвентарные списки.

Группы системных администраторов с напряженным графиком работы всегда

приветствуют документирование процессов и распространение информации.

Хорошее хранилище может способствовать этому. Документация экономит

время вам и всем остальным, а также позволяет использовать знания всех со-

трудников для улучшения системы.

***Глава 10***

***Аварийное восстановление и целостность данных***

**План аварийного восстановления рассматривает**, какие нештатные ситуации

могут затронуть компанию, и предоставляет план реакции на эти ситуации.

Планирование аварийного восстановления включает реализацию способов

смягчения последствий возможных нештатных ситуаций и подготовку быстро-

го восстановления основных служб. План определяет эти ключевые службы

и указывает, как быстро они должны быть восстановлены.

Определенный уровень планирования аварийного восстановления должен быть

на всех сайтах. Проектировщики аварийного восстановления должны рассмот-

реть, что будет, если с одним из сайтов их организации случится что-то катастрофическое, и как они смогут обеспечить восстановление.

При создании плана аварийного восстановления должны приниматься во вни-

мание как риски, с которыми сталкивается ваш сайт, так и правовые и долговые

обязательства вашей компании.

***10.1. Основы***

Как и любой другой проект, создание плана аварийного восстановления начи-

нается с определения требований: какие нештатные ситуации могут затронуть

ваш сайт, какова их вероятность, стоимость для вашей компании и как быстро

нужно восстановить различные части вашего бизнеса. Как только вы и ваше

руководство поймете, что может случиться, вы сможете получить средства на

проект и начать поиск способов выполнения или, что предпочтительнее, пере-

выполнения этих требований.

**10.1.1. Определение нештатной ситуации**

Нештатная ситуация – это катастрофическое событие, которое вызывает силь-

ный сбой, влияющий на все здание или сайт. Нештатная ситуация может быть

любой: от стихийного бедствия, например землетрясения, до более распростра-

ненной проблемы случайного повреждения ваших кабелей экскаватором. Не-

штатная ситуация – это все, что может значительно повлиять на возможность

вашей компании вести бизнес.

**10.1.2. Анализ рисков**

Первый шаг в построении плана аварийного восстановления – проведение ана-

лиза рисков. **Управление рисками** является подходящей областью для привле-

чения сторонних консультантов, потому что их специализированные навыки

требуются лишь время от времени, а не каждый день.

Анализ рисков включает определение того, с какими нештатными ситуациями

может столкнуться компания и какова вероятность их возникновения. Анали-

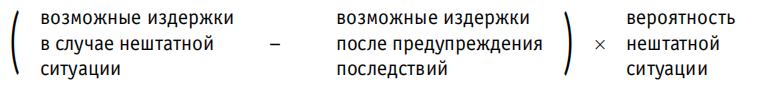
тик определяет возможные издержки компании в случае возникновения каж-

дого типа нештатной ситуации. Затем компания использует эту информацию,

чтобы определить приблизительную сумму денег, которую можно потратить на

попытку смягчить последствия каждого типа нештатной ситуации.

Приблизительный бюджет предупреждения риска определяется по формуле:



В качестве примера можно привести большой сайт, который имеет одну потенциальную точку сбоя, где все локальные сети связываются одним маршрутизатором. Если он откажет, то для его ремонта потребуется один день, и есть 70-процентный шанс, что сбой случится один раз в 24 месяца. Авария приведет к невозможности работы 1000 человек в течение суток. Компания оценивает потерю производительности в 68 тыс. долларов. При выборе резервного маршрутизатора системные администраторы будут располагать бюджетом, равным приблизительно 23,8 тыс. долларов. Также системным администраторам нужно определить стоимость снижения времени неработоспособности до 4 ч – например, за счет повышения уровня контракта на обслуживания. Если цена будет разумной, это еще сильнее снизит объемы возможных убытков компании, а следовательно, и сумму, которую она должна

будет потратить на полное восстановление.

**10.1.3. Правовые обязательства**

У коммерческих организаций есть правовые обязательства перед постав-

щиками, клиентами и акционерами, касающиеся выполнения контрактных

обязательств. Открытые акционерные общества должны соблюдать нормы

фондовых рынков, на которых ведется торговля их акциями. Университеты

имеют контрактные обязательства перед своими студентами. Кроме того, необ-

ходимо соблюдать строительные нормы и правила, а также правила техники

безопасности.

Юридический отдел должен уметь детально разъяснить эти обязательства.

Эти обязательства переводятся в требования для плана аварийного восстановления.

Они определяют, как быстро должна быть восстановлена работоспособность

различных элементов физической и электронной инфраструктуры. Восстанов-

ление работоспособности отдельных составных частей компании до полного

восстановления всей инфраструктуры требует глубокого понимания того, на

какие элементы инфраструктуры полагаются эти части, и подробного плана их

возвращения в рабочее состояние. Соблюдение временных рамок также требует

понимания того, какое время займет восстановление этих компонентов.

**10.1.4. Ограничение ущерба**

**Ограничение ущерба** касается снижения издержек в результате нештатных

ситуаций. Некоторое ограничение ущерба может быть достигнуто бесплатно

или с небольшими затратами за счет планирования и хорошей организации

процессов. Большая часть ограничения ущерба предполагает дополнительные

затраты компании и является предметом анализа прибыли и издержек, который

проводится аналитиком риска.

Ограничение ущерба, вызванного серьезной аварией, дороже и всегда должно

быть предметом анализа прибыли и издержек. Например, вычислительный

центр может быть построен в подземном бункере, аналогичном военному, для

защиты от торнадо и бомбардировок. На сейсмоопасных территориях применя-

ют дорогие механизмы, обеспечивающие взаимное перемещение элементов

стойки, чтобы снизить риск повреждения панелей компьютеров, что является

основной проблемой жестко закрепленных стоек при сильных землетрясениях.

Эти механизмы ограничения ущерба настолько дороги, что, скорее всего, их

применение может быть оправданным только в крупнейших компаниях.

Большинство механизмов ограничения ущерба находятся где-то между «совер-

шенно бесплатными» и «очень дорогими». Системы пожаротушения обычно

относятся к последней категории. Разумно рассмотреть возможность примене-

ния системы пожаротушения, спроектированной для ограничения ущерба

оборудованию вычислительного центра при активации.

Еще одна область, часто заслуживающая внимания, – это отключение питания

в здании или комплексе зданий. С короткими перебоями в подаче электроэнер-

гии, скачками или падением напряжения можно справиться при помощи ис-

точника бесперебойного питания, для более долгих перерывов потребуется ге-

нератор. Чем больше аппаратуры требует защищенного питания – рефрижера-

торы в биотехнологических компаниях, центры обработки вызовов в компани-

ях по работе с клиентами – и чем дольше потребуется поддерживать их работу,

тем дороже это будет стоить.

**10.1.5. Подготовка**

Даже при наличии достаточных мер по контролю ущерба ваша компания может

столкнуться с нештатной ситуацией. Подготовленность к нештатной ситуации означает возможность восстановить работоспособность основных систем в сжатые сроки, определенные вашими правовыми обязательствами.

Восстановление служб после аварии может потребовать перестройки необходи-

мых данных и служб на новом оборудовании, если старое оборудование нерабо-

тоспособно. Таким образом, вам нужно заранее определить источник замены

оборудования из компаний, которые предоставляют эту услугу. Вам также

потребуется наличие другого помещения, куда можно будет переместить это

оборудование, если основное помещение нельзя использовать по соображениям

безопасности, из-за недостатка электроэнергии или плохой связи. Убедитесь,

что компания, предоставляющая рабочее оборудование, знает, куда его нужно

отправлять в случае аварии. Убедитесь, что у вас есть временные обязательства

по замене от поставщика и что вы знаете, какое оборудование компания сможет

поставить по первому требованию. Не забудьте учесть время замены этого обо-

рудования при подсчете общих затрат времени на процесс.

Как только у вас будут машины, вам потребуется восстановить систему. Обыч-

но сначала вы реконструируете систему, а затем восстанавливаете данные. Это

требует наличия резервных копий данных вне сайта – обычно в коммерческой

службе хранения. Вам также потребуется возможность легко определить, какие

кассеты потребуются для восстановления основных служб. Этот этап базовой

подготовки строится на инфраструктуре, которая уже должна быть на вашем

сайте.

Обычно сайту требуется безопасное сохранение важных документов в хранили-

ще. Такие хранилища специализируются на сценариях аварийного восстанов-

ления. Если в вашей компании есть такое хранилище, вы можете применять

его для хранения кассет с резервными копиями данных.

Помните, что в качестве элемента восстановления служб вам могут понадобить-

ся электропитание, телефон и сетевое соединение. Проработайте эти вопросы

с группой обеспечения. Может быть, разумно назначить резервное местополо-

жение офиса для выполнения важнейших функций в качестве элемента ава-

рийного плана.

**10.1.6. Целостность данных**

**Целостность данных** означает обеспечение неизменности данных под действи-

ем внешних источников. Целостность важных данных необходимо обеспечивать

путем определенных операций и ежедневного резервного копирования и архи-

вации. Базы данных, в которых предусмотрены лишь небольшие изменения или только добавление данных, могут проверяться на неожиданно большие изменения или удаления. Учитывайте известные вам особенности данных в ваших системах при создании автоматизации проверки целостности.

Аварийное планирование также включает обеспечение возможности воспроиз-

водства и восстановления в системах полной и достоверной копии корпоратив-

ных данных. Для аварийного восстановления это должна быть недавняя, согла-

сованная копия данных с синхронизацией всех баз данных. Аварийное восста-

новление должно обеспечивать целостность данных.

Промышленный шпионаж и кража интеллектуальной собственности довольно

распространены, и может получиться так, что компании необходимо будет за-

щищать свои права на интеллектуальную собственность в суде. Возможность

быстрого восстановления данных в виде, существовавшем на определенную

дату, может быть использована для доказательства владения интеллектуальной

собственностью. Для применения в качестве доказательства дата полученной

информации должна быть точно известной, а данные должны быть в целостном

состоянии.

***10.2. Тонкости***

Полная подготовка к нештатной ситуации заключается в наличии резервных

версий всего, что может взять работу на себя, когда основная версия откажет.

Другими словами, должен иметься резервный сайт с резервными системами.

Несмотря на высокие затраты, в крупных компаниях, особенно в банках, нали-

чие резервного сайта является необходимостью. Фактически крупные компании

перестали использовать термин «аварийное восстановление» и вместо него

пользуются термином «планирование резервных вариантов» или «планирова-

ние непрерывности бизнеса».

**10.2.1. Резервный сайт**

Для компаний, которым требуется высокая доступность, следующим уровнем

аварийного планирования является наличие полного **резервного сайта**, распо-

ложенного в месте, которое не будет затронуто той же самой чрезвычайной си-

туацией.

Вместо того чтобы постоянно хранить резервное оборудование во втором поме-

щении, его можно использовать в качестве альтернативного варианта для вос-

становления служб. Если у компании есть контракт на поставку оборудования

в случае чрезвычайной ситуации, это оборудование может быть отправлено

в помещение альтернативного вычислительного центра. Если помещение, за-

тронутое чрезвычайной ситуацией, было серьезно повреждено, это может быть

самым быстрым способом восстановить работоспособность служб.

**10.2.2. Нарушения безопасности**

Нарушения безопасности являются растущей проблемой.

В отличие от природных чрезвычайных ситуаций, физический ущерб не нано-

сится, а атака может осуществляться не с физически локального объекта.

Для определения типов мер по защите данных можно провести аналогичный

анализ рисков. В архитектурных решениях есть элемент риска. Можно спра-

виться с риском несколькими способами – за счет построения барьеров вокруг

системы или с помощью мониторинга системы, чтобы можно было быстро ее

отключить в случае атаки.

**10.2.3. Отношения с прессой**

Когда произойдет чрезвычайная ситуация, журналисты, скорее всего, захотят

узнать, что случилось, как это повлияло на компанию и когда службы будут

восстановлены. К сожалению, обычно вы можете дать лишь один ответ на все

три вопроса: «Мы не знаем». Это, пожалуй, является наихудшим ответом, ко-

торый можно дать репортеру.

Во-первых, заключите соглашение с компанией по связям с общественностью (PR – Public Relations) заблаговременно, чтобы вы не пытались привлечь ее к сотрудничеству во время чрезвычайной ситуации.

Во-вторых, заблаговременно планируйте, как вы будете общаться с прессой. Этот план должен включать следующее: кто будет общаться с прессой, что будет и что не будет сказано и каков порядок цепочки управления при отсутствии ответственных за принятие решений. Все, кто будет общаться с прессой, должны пройти подготовку в вашей PR-компании.

***10.3. Заключение***

Самый важный аспект аварийного планирования – понимание того, какие

службы являются наиболее важными для бизнеса и каковы временные рамки

восстановления этих служб. Ответственному за аварийное планирование также

нужно знать, какие чрезвычайные ситуации могут произойти и какие расходы

они вызовут, прежде чем завершить анализ рисков и определить бюджет ком-

пании на ограничение ущерба.

Аварийный план должен строиться с учетом этих критериев. Он должен учи-

тывать время, необходимое для получения нового оборудования, внешних ре-

зервных копий и восстановления всей системы с нуля.

Ответственный за аварийное планирование должен искать как простые способы

ограничения ущерба, так и более сложные и дорогие. Наиболее эффективными

являются средства автоматического действия, включенные в инфраструктуру.

К этой категории относятся системы пожаротушения, обнаружения воды, сей-

смоустойчивые опоры и подходящее оборудование, монтируемое в стойках.

Ответственный за аварийное планирование также должен подготовить план

действий людей в случае чрезвычайной ситуации. Простые планы часто наибо-

лее эффективны. Члены группы должны знать свои персональные обязанности

и проходить практикум несколько раз в год.

Полное резервирование, включающее резервный сайт, является идеалом, ко-

торый большинство компаний не могут себе позволить. Однако, если у компании

есть второй вычислительный центр, существуют способы включить его в ава-

рийный план с разумными расходами.