**Конспект: Глава 7. Сети**

Сеть – это основа инфраструктуры компании. Ошибки, допущенные при проектировании сети, могут негативно сказаться на всех компонентах системы. Сеть не существует в изоляции: решения, принятые при её создании, влияют на внедрение инфраструктурных сервисов. Поэтому при проектировании сети важно консультироваться с ответственными за эти сервисы.

Сетевые технологии стремительно развиваются, и методы их внедрения со временем меняются. Однако основные принципы, такие как надёжность, документирование и масштабируемость, остаются неизменными.

Основная цель при проектировании сети – создать надёжную, документированную, простую в обслуживании систему с высокой пропускной способностью и возможностями для роста. На эту цель влияет множество факторов, включая физическую структуру сети, логическую топологию, маршрутизацию, мониторинг и управление сетью.

Подходы к проектированию локальных и глобальных сетей различаются, но со временем становятся то ближе, то дальше друг от друга. Например, в локальных сетях ранее использовали топологию FDDI (двойное кольцо), которая затем была вытеснена Fast Ethernet с шинной архитектурой. В это время в глобальных сетях набирали популярность кольцевые архитектуры, такие как SONET и MONET. Позже, с развитием технологий, 10-гигабитные локальные сети снова стали использовать кольцевую архитектуру.

### 7.1.1. Модель OSI

Модель OSI (Open Systems Interconnection) представляет собой эталонную модель взаимодействия открытых систем, широко используемую для описания сетей. Она разбивает сеть на логические уровни, каждый из которых отвечает за определённые функции.

Физический уровень (1) включает физическое подключение устройств через кабели, оптоволокно или беспроводные каналы. Канальный уровень (2) отвечает за MAC-адресацию и управление потоком данных. Сетевой уровень (3) занимается логической адресацией (например, IP-адресами) и маршрутизацией. Транспортный уровень (4) отвечает за доставку данных, проверку ошибок и восстановление соединений. Сеансовый уровень (5) управляет сессиями связи. Уровень представления (6) отвечает за форматы данных, шифрование и сжатие. Прикладной уровень (7) включает протоколы приложений, такие как HTTP, SMTP и FTP.

Техники часто упрощают модель OSI для сетей TCP/IP. Например, физический кабель относится к уровню 1, устройства для локальных сетей – к уровню 2, маршрутизаторы – к уровню 3, а используемые протоколы – к уровню 4. Уровень 5 редко используется в TCP/IP. Уровень 6 охватывает форматы данных, шифрование и сжатие, а уровень 7 включает прикладные протоколы, такие как HTTP и FTP.

На практике границы уровней модели OSI часто размываются. Например, VPN через HTTP-прокси использует трафик уровней 3 и 4 в рамках протокола прикладного уровня (7). Модель OSI полезна для понимания принципов работы сети, но не всегда строго соблюдается в реальных системах.

### 7.1.2. Понятная архитектура

Сетевая архитектура должна быть простой и понятной. Её проектирование должно легко описываться несколькими словами и иллюстрироваться простыми схемами. Понятная архитектура облегчает решение проблем: вы всегда знаете, как проходит трафик между точками, и можете быстро определить, какие каналы влияют на сети. Ясное понимание маршрутов трафика позволяет эффективно управлять сетью, тогда как сложная и непонятная архитектура оставляет всё на волю случая.

Простота архитектуры охватывает физическую и логическую топологии, а также используемые сетевые протоколы. Она позволяет легко масштабировать сеть, добавляя новые сегменты локальной сети или подключая удалённые офисы.

Мы рекомендуем минимизировать количество сетевых протоколов в одной глобальной сети. Большинство компаний в последние годы переходят на использование TCP/IP, отказавшись от комбинирования его с такими протоколами, как Novell IPX или AppleTalk. Если необходимо поддерживать устаревшие протоколы, их можно инкапсулировать в туннели поверх TCP/IP, что обходится дешевле и упрощает инфраструктуру.

### 7.1.3. Топологии сетей

Сетевые топологии меняются вместе с развитием технологий и компаний. Рассмотрим основные типы:

**Топология звезды.**  
Центральное устройство или сеть соединяет все остальные узлы.

* Преимущества: простота, экономическая эффективность, удобство масштабирования.
* Недостатки: уязвимость центра — при его отказе связь нарушается.
* Улучшения: дублирование центра и избыточные подключения между узлами.
* Распространённый вариант — несколько звёзд, соединённых высокоскоростными каналами, что минимизирует последствия отказов.

**Топология кольца.**  
Каждый узел соединён с двумя соседними, формируя кольцо.

* Преимущества: устойчивость к отказам одного из каналов.
* Недостатки: сложность управления при увеличении числа узлов.

**Топология хаоса.**  
Каждый узел может использовать один или несколько произвольных маршрутов для связи.

* Пример: Интернет.
* Особенности: высокая адаптивность и отказоустойчивость, сложность описания.

**Логическая топология.**  
Отображает сетевые устройства и их взаимодействие. Она должна быть понятной, чтобы архитектор мог изобразить её без помощи.

### Примеры топологий на логическом уровне:

* **Плоская топология:** единая сеть уровня 2 без маршрутизаторов, один домен широковещательной рассылки.
* **Топология на основе местоположения:** сети уровня 2 организуются по физическим зонам, например, этажам здания, с использованием маршрутизаторов уровня 3.
* **Топология на основе функциональных групп:** группы пользователей подключаются к одной сети, независимо от их местоположения.

### Взаимосвязь логики и физики сети:

Логическая топология зависит от физической и влияет на неё. Например, маршрутизация, сервисы (электронная почта, доступ в Интернет) и другие элементы должны быть интегрированы в архитектуру сети.

**Промежуточный кабельный узел (IDF)**

Промежуточный кабельный узел, или IDF (Intermediate Distribution Frame), представляет собой сетевой коммутационный шкаф, который используется для подключения настольных компьютеров к сети через систему сетевых шкафов и кабелей. Технологии подключения развиваются постепенно, поэтому важно заранее продумывать выбор оборудования. Использование качественных медных или оптоволоконных кабелей позволяет избежать частой модернизации и дополнительных затрат. Например, выбор кабеля категории 5 вместо устаревшего кабеля категории 3 помогает в будущем сократить расходы на замену инфраструктуры.

Современные IDF оборудованы патч-панелями, которые упрощают подключение кабелей через разъемы RJ-45. Это удобнее по сравнению со старыми системами, где использовались коммутационные блоки, требующие ручного подключения проводов. Для подключения нескольких IDF существует два подхода: либо прокладывать отдельные связки кабелей между узлами, что дорого и неудобно, либо организовать центральный узел (MDF), куда подключаются все IDF, что позволяет значительно упростить кросс-подключения.

Размещение IDF в здании должно быть тщательно продумано. Обычно на каждом этаже требуется по одному IDF, и их размещение рекомендуется планировать строго по одной вертикали. Это облегчает прокладку кабелей между узлами и упрощает обслуживание. Нумерация IDF должна быть систематичной, включать номера здания, этажа и шкафа. Также важно маркировать сетевые разъемы, чтобы упростить диагностику и устранение проблем.

Оборудование IDF должно быть расположено только в сетевых шкафах. Размещение серверов или стороннего оборудования не рекомендуется, так как это увеличивает риск повреждений и затрудняет обслуживание. На этапе строительства здания необходимо предусмотреть запас сетевых разъемов, поскольку прокладка дополнительных кабелей впоследствии обходится значительно дороже.

IDF должны быть закрыты для предотвращения несанкционированного доступа. Важно регулярно проводить инструктажи для сотрудников, которые работают с этими узлами. Оборудование IDF нуждается в защите электропитания от перебоев и скачков напряжения. Использование источников бесперебойного питания (ИБП) помогает избежать проблем с сетью во время отключений электроэнергии. Дополнительно требуется охлаждение шкафов IDF, так как сетевое оборудование выделяет много тепла.

Для удобства управления оборудованием IDF необходимо настроить удаленный консольный доступ с использованием строгой аутентификации. Размещение сетевых разъемов и прокладка кабелей на этапе строительства позволяет сэкономить средства и обеспечить устойчивую работу сети в будущем.

**Точки разграничения и документирование сети**

Точка разграничения представляет собой границу между вашей организацией и поставщиком услуг, таким как телефонная компания или интернет-провайдер. Это может быть распределительный шкаф оптоволоконной линии, коммутационные блоки, стойка с щитом, сетевое устройство или даже пластиковая коробка на стене с разъемом для кабеля. Важно знать местоположение точки разграничения, так как телефонная компания несет ответственность только за проводку до этой точки. Если возникают проблемы с линией, необходимо указать технику точку разграничения, чтобы не тратить время на проверку других участков сети. Также стоит иметь возможность тестировать проводку от этой точки до сетевого оборудования.

Сетевое документирование включает в себя несколько видов документации, с основным акцентом на маркировку. Сетевые карты делятся на физические и логические. Карта физической сети отображает путь проводки, местоположение конечных точек и радиус действия беспроводных точек. Если в физической сети предусмотрена избыточность, необходимо четко обозначить и задокументировать разные пути. Также важно обозначить типы и объем подключения для каждого канала, например, количество витых пар или оптоволоконных кабелей между зданиями, их класс и точку подключения.

Логическая карта сети отображает топологию, сетевые номера, имена, скорости, протоколы маршрутизации и административные домены. Оба типа карт должны соответствовать масштабу сети и определять её внешние границы.

Маркировка является ключевым элементом документирования сети. Особенно важными являются ярлыки на патч-панелях и междугородных каналах, которые должны быть четкими и последовательными. На ярлыках для патч-панелей нужно указывать их физическое местоположение и точное подключение каждого кабеля с обеих сторон. Для междугородных линий ярлыки должны включать информацию о направлении линии, контактные данные для устранения проблем и идентификатор цепи. Подобные ярлыки помогут быстро найти нужную информацию при возникновении неисправностей, например, отслеживая кабель от модулей обслуживания канала до монтажных блоков на точке разграничения.

Временные проводки также должны быть промаркированы, однако маркировку следует поддерживать только в случае стабильности окружающей среды. Неверные ярлыки могут создать больше проблем, чем их отсутствие. Одним из компромиссных решений является использование кабелей с уникальными серийными номерами на обоих концах. Эти номера облегчают отслеживание кабелей и могут включать информацию о типе и длине кабеля. Например, можно использовать разноцветные ярлыки на коннекторах для дополнительной идентификации типа кабеля.

Маркировка кабелей – это сложный процесс, однако для этого хорошо подходят самоклеящиеся ярлыки, которые можно быстро прикрепить и, при необходимости, заменить. Кроме того, в процессе документирования важно учитывать онлайн-документирование, которое является частью конфигурации сетевых устройств. Использование комментариев и стандартных имен для устройств в сети помогает значительно упростить администрирование, делая его более интуитивно понятным.

**Простая маршрутизация**

Маршрутизацию следует оставлять для маршрутизаторов, а не для узлов сети. Конфигурация узлов должна включать стандартный шлюз, чтобы упрощать процесс маршрутизации. Важно, чтобы маршрутизация в пределах одной площадки была простой, предсказуемой и доступной для диагностики.

В UNIX-системах поддерживаются протоколы маршрутизации, такие как RIP и RIPv2, что позволяет узлам определять, куда отправлять пакеты. Однако раньше, когда большинство узлов использовали UNIX-системы с одним сетевым интерфейсом, протокол RIP не был оптимальным, так как он нагружал процессор и сеть для создания таблицы маршрутизации, которая на самом деле указывала, что используется только один интерфейс для всех пакетов. Это могло привести к сбоям, если узлы передавали неверную маршрутную информацию.

Если маршрутизатор поддерживает такую возможность, важно отключить отправку протоколов маршрутизации в локальные сети, где они не нужны. Это предотвращает ошибки в конфигурации, которые могут привести к неправильной маршрутной информации.

Узел с одним сетевым интерфейсом должен иметь только один стандартный маршрут и не должен принимать динамическую маршрутную информацию. Узел с несколькими сетевыми интерфейсами должен принимать трафик, адресованный ему, и не должен отправлять пакеты от других узлов. Его маршрутизация должна быть статичной и максимально простой. Если узел подключен к нескольким сетям, трафик для одной из них должен направляться через соответствующий интерфейс, а трафик для других сетей — через стандартный маршрутизатор.

Иногда может понадобиться добавить дополнительные статические маршруты для направления трафика по рекомендуемым путям, например, для отправки трафика через маршрутизатор в другой сети. Однако по возможности следует избегать сложных конфигураций.

Простая маршрутизация позволяет избежать непредсказуемых ситуаций, упрощая решение сетевых проблем. Если все узлы настроены одинаково, их поведение будет одинаковым. Внедрение динамической маршрутизации может привести к непредсказуемому поведению всей сети, поэтому стоит ограничить участие узлов в динамической маршрутизации, используя соответствующие механизмы безопасности и аутентификации.

**Сетевые устройства**

Для любой современной сети необходимы специализированные сетевые устройства, такие как маршрутизаторы и коммутаторы, а не универсальные узлы, сконфигурированные для маршрутизации. Эти устройства должны быть специально разработаны для выполнения своей основной задачи — передачи пакетов или управления трафиком, а не для выполнения дополнительных функций.

До появления сетевых маршрутизаторов маршрутизация осуществлялась с помощью UNIX-систем с несколькими сетевыми картами. Однако вскоре на рынок вышли устройства от Cisco и других компаний, оптимизированные для маршрутизации, которые значительно повысили производительность сети. Эти устройства снижают задержки, лучше интегрируются с системами управления сетью и мониторинга, а также менее склонны к поломкам, так как имеют меньше подвижных частей.

Маршрутизация пакетов в специализированных устройствах происходит в ядре, что обеспечивает приоритет для этой задачи и минимизирует влияние на другие функции. Например, если маршрутизацию выполняет файловый сервер, увеличение сетевого трафика будет снижать производительность файлового сервиса. Это связано с тем, что ядро, выполняющее маршрутизацию, отнимает ресурсы у других процессов, что не всегда видно при обычной диагностике.

Когда появились брандмауэры, они также изначально представляли собой серверы или рабочие станции с дополнительным программным обеспечением для фильтрации трафика. Позже на рынке появились аппаратные брандмауэры, которые справлялись с большим объемом трафика без потери скорости. Несмотря на то, что программные брандмауэры догнали аппаратные по функциональности, они часто подвергаются риску из-за добавления на тот же сервер других сервисов, что может привести к уязвимостям в безопасности.

Мы предпочитаем использовать аппаратные брандмауэры, так как они выполняют свою задачу по фильтрации трафика, не отвлекаясь на другие функции. Программные решения, хотя и гибкие, часто становятся сложными в обслуживании и поддержке, особенно когда разработчик покидает компанию.

Также следует учитывать, что обновления для сетевых устройств и серверов имеют разные графики. Сетевые устройства обычно требуют меньше обновлений и изменений, в то время как серверы приложений часто обновляются и перезагружаются. Это несоответствие может создавать неудобства при работе с оборудованием.

Наблюдается тревожная тенденция, когда крупные компании, такие как Microsoft, Novell и Apple, поощряют использование универсальных машин в качестве маршрутизаторов или брандмауэров. Однако мы считаем, что это ошибка, и не следует повторять прежние ошибки с использованием универсальных машин для специализированных задач.

**Оверлейные сети**

Оверлейная сеть — это логическая топология, которая накладывается на физическую топологию. Примеры оверлейных сетей включают VLAN, Frame Relay и ATM. Этот подход позволяет создавать физически простые, но функционально сложные сети, которые обеспечивают необходимую гибкость и сложность на логическом уровне, при этом сохраняя простоту на физическом слое.

Применение оверлейных сетей позволяет строить однородные и стабильные физические сети, а затем накладывать на них более сложные логические структуры. Например, для глобальной вычислительной сети можно установить единое подключение к ATM или распределенную сеть Frame Relay. После этого можно настроить коммутаторы ATM или Frame Relay так, чтобы между различными площадками создавались виртуальные каналы. Если две удаленные площадки обменяются большим объемом трафика, достаточно просто изменить конфигурацию коммутатора, добавив виртуальный канал между этими площадками.

Одним из популярных вариантов является полная ячеистая топология, где каждая площадка соединена с остальными через виртуальные каналы. Преимущество такого подхода в том, что основная площадка не перегружена трафиком, и компаниям не нужно устанавливать новые физические каналы, что экономит средства.

Для глобальных вычислительных сетей также часто используется туннелирование с шифрованием, например, в виде виртуальных частных сетей (VPN). В этом случае каждая площадка оснащена брандмауэром, VPN-устройством и подключением к Интернету, что позволяет создать ГВС через Интернет. Это позволяет интернет-провайдерам использовать одну стабильную инфраструктуру для множества клиентов.

На уровне локальной сети оверлейные сети обычно означают использование простых физически однородных топологий с протоколом VLAN (IEEE 802.1q) для создания виртуальных подсетей, которые могут быть необходимы пользователям. Для соединения различных участков локальной сети, например, IDF и MDF, могут использоваться высокоскоростные избыточные каналы, которые служат связующим звеном на уровне канала Ethernet с применением протокола STP (Spanning Tree Protocol), обеспечивающего отказоустойчивость.

**7.1.11. Количество поставщиков**

Использование оборудования от множества разных поставщиков может усложнить управление сетью. Чем больше поставщиков предоставляют оборудование, тем больше возникает проблем с интеграцией и взаимодействием между устройствами. Это увеличивает нагрузку на администраторов сети, которым нужно изучить различные конфигурации и особенности оборудования, следить за обновлениями программного обеспечения и отслеживать ошибки. Для повышения надежности и упрощения обслуживания сети рекомендуется минимизировать количество поставщиков, что также может помочь получить скидки за увеличение объема поставок.

Однако сотрудничество с одним поставщиком также имеет свои риски. Нет поставщика, который производил бы лучшую продукцию во всех областях, и полная зависимость от одного поставщика может привести к проблемам с взаимодействием оборудования в случае, если компания решит работать с другим поставщиком. Оптимальным решением является выбор поставщиков по уровням или типам устройств. Например, можно использовать маршрутизаторы от одного поставщика, центральные коммутаторы от другого, а хабы и коммутаторы в офисах — от третьего.

**7.1.12. Стандартные протоколы**

Сеть организации должна строиться с использованием стандартных протоколов, поскольку проприетарные решения связывают вас с конкретным поставщиком, что затрудняет интеграцию с оборудованием других производителей. Это усложняет получение скидок, мешает внедрению инновационных решений и делает вашу инфраструктуру уязвимой для проблем поставщика. Стандарты должны быть проверенными временем и обеспечивать совместимость с оборудованием различных производителей. Использование стандартов IETF, например, снижает риски несовместимости между версиями. В идеале стоит убедить поставщика сделать свои протоколы открытыми, а если они эксклюзивны, попросить его предоставить стандарт или описание, подтверждающее их взаимодействие с другими решениями.

**7.1.13. Мониторинг**

Мониторинг сети — ключевой элемент для обеспечения высокой производительности и надежности сети. Он позволяет своевременно выявлять проблемы, оптимизировать сеть и планировать будущие потребности. Сетевой мониторинг включает два основных типа: мониторинг в реальном времени и сбор статистики для анализа тенденций. Оба типа мониторинга имеют большое значение для провайдеров интернет-услуг, а для корпоративных сетей они также полезны, но не всегда критичны для основного бизнеса.

Мониторинг в реальном времени должен уведомлять администраторов о неисправностях, таких как отказ сетевого интерфейса или проблемы с маршрутизацией. Также важно учитывать аномалии, такие как неожиданные всплески или падения трафика, которые могут свидетельствовать о проблемах с сетью или устройствах. Сбор статистических данных позволяет предсказать будущие потребности в пропускной способности сети и оптимизировать ее расширение. Для интернет-провайдеров и компаний, предоставляющих интернет-услуги, важно собирать данные о трафике и определять места для оптимизации и увеличения пропускной способности.

Сбор статистики по сбоям, ошибкам и отказам помогает выявить проблемы и следить за их устранением. Анализ данных помогает обнаружить аномалии в работе сети, что позволяет заранее планировать меры по устранению проблем и оптимизации работы сети.

**7.2. Тонкости**

В дополнение к базовым задачам существуют несколько важных аспектов, которые могут помочь улучшить вашу сеть. Важно найти баланс между внедрением новых технологий и использованием проверенных и надежных решений. Также, если потребуется создать несколько административных единиц, следует следовать рекомендациям, чтобы минимизировать возможные проблемы.

**7.2.1. Передовые технологии или надежность**

Одной из главных целей построения сети является обеспечение ее надежности. Более старые решения, которые прошли обширные проверки как с аппаратной, так и с программной стороны, часто отличаются высокой стабильностью, поскольку все ошибки уже исправлены. В отличие от этого, новые решения с улучшенными характеристиками и высокой скоростью подключения могут быть еще не полностью протестированы, что влечет за собой определенные риски.

Чтобы снизить этот риск, можно провести сертификацию новых решений в лаборатории до их внедрения. Это даст уверенность в успешности развертывания перед массовым использованием нового оборудования. Важно документировать процесс установки и стандарты конфигурации. Постепенное развертывание и тестирование в лаборатории помогут обеспечить большую уверенность в новых решениях.

Можно разделить пользователей на разные группы по уровню готовности к риску. Некоторые пользователи могут быть готовы пожертвовать частью надежности в обмен на новые возможности. В этом случае также важно тестировать новое оборудование до внедрения, чтобы избежать проблем.

В некоторых случаях такие группы пользователей могут быть под ответственностью другого отдела. Этот отдел может иметь клиентские группы, которые требуют внедрения новых технологий сразу после их появления. Если это возможно, можно доверить им решение проблем, а самому использовать их опыт. Таким образом, вы можете учиться на их ошибках и избежать повторения их проблем.

Если вы решаете внедрять новейшие технологии, важно уведомить сотрудников, что из-за новизны технологий возможны сбои и простои. Это важно делать заранее, чтобы избежать разочарования пользователей и снижения репутации сети. В случае, если руководство согласится на риски, такие предупреждения должны быть сделаны для конечных пользователей и их руководителей, чтобы избежать обвинений в простоях. Даже в этом случае новое оборудование должно быть тщательно настроено и протестировано в лаборатории перед внедрением в рабочую среду.

**7.2.2. Несколько административных единиц**

В некоторых случаях создание единой административной единицы для управления сетью может быть невозможно по политическим, практическим или соображениям безопасности. В таких ситуациях необходимо использовать другую модель управления сетью. Если различные организации управляют разными частями сети, которые не подчиняются единому органу управления, требуется создание четких границ между этими частями, используя пограничные протоколы маршрутизации, такие как BGP, а также системы безопасности, включая брандмауэры.

Такой подход позволяет обеспечить стабильность маршрутизации и установить известные уровни безопасности для каждой административной единицы независимо от других. Чаще всего используется следующее разделение: одна группа отвечает за подключение к глобальной вычислительной сети, а другая — за подключение к локальной сети. Это оправдано, поскольку для управления этими сетями требуются различные навыки и квалификация.

Если требуется создать несколько административных единиц, это нужно сделать корректно. Действия и решения одной группы администраторов должны быть полностью независимыми от действий других групп, и они не должны оказывать влияния на работу или надежность других сетей. Для этого важно провести совещания для разработки общепринятых стандартов и утвердить комиссию из представителей каждой группы, которая будет отвечать за внедрение ключевых стандартов.

**7.3. Заключение**

В этой главе рассмотрены различные аспекты разработки и создания сети. Сетевые технологии быстро развиваются, и некоторые из этих аспектов будут изменяться со временем. Однако другие аспекты создания сети остаются неизменными и всегда будут актуальны.

Несмотря на быстрое развитие технологий, у вас есть возможность использовать стабильные основы для построения надежной сети, что позволит не только обеспечить её устойчивость, но и идти в ногу с развитием технологий.

**Глава 8. Пространства имен**

В этой главе рассматриваются принципы организации и управления пространствами имен. Пространство имен — это набор уникальных ключей и связанных с ними атрибутов. Примеры пространств имен включают регистры, доступные принтеры, имена хостов, Ethernet-адреса, списки сервисов и номеров портов, карты расположения домашних каталогов и так далее. Каждый элемент в пространстве имен имеет определенные атрибуты, такие как UID (для UNIX) или SID (для Windows) для регистрационных записей, IP-адреса, серийные номера оборудования, MAC-адреса и другие.

Термин "пространство имен" может быть как абстрактным, так и конкретным. Например, имена пользователей — это пространство имен, представленное списком идентификаторов пользователей в каждой многопользовательской операционной системе. Хотя пространства имен для разных компаний могут отличаться, поскольку набор пользователей у каждой компании уникален.

**Типы пространств имен**

Пространства имен бывают разных типов:

1. **Плоские пространства имен**. В таких пространствах нет иерархии. Примером может служить каталог WINS в Windows или набор идентификаторов UID в UNIX.
2. **Иерархические пространства имен**. В таких пространствах элементы организованы в виде дерева, например, дерево каталогов в файловой системе. В таких пространствах файлы с одинаковыми именами могут находиться в разных подкаталогах.

**Значение формализации управления**

Чем более сложная система, тем важнее формализовать управление пространствами имен. В небольших системах один человек может управлять пространствами имен и держать информацию в памяти, но в крупных компаниях необходимо делегировать управление нескольким подразделениям. Управление пространствами имен в больших системах требует четкой структуры, чтобы избежать беспорядка.

**8.1. Основы управления пространствами имен**

Для эффективного управления пространствами имен необходимы следующие основы:

* **Политики**: Пространствам имен нужно подчиняться общим политикам, которые регулируют имена, долговечность, локальность и защищенность.
* **Процедуры**: Нужно разработать процедуры для добавления, изменения и удаления элементов из пространства имен.
* **Централизованное управление**: Управление пространствами имен должно быть централизованным, чтобы избежать несоответствий и ошибок.

**8.1.1. Политики для пространств имен**

Пространства имен должны быть организованы на основе формальных политик, а не полагаться только на устные соглашения. Чем больше и сложнее ваша организация, тем важнее зафиксировать эти политики в письменном виде. Письменные политики служат основой для взаимодействия между системными администраторами и для обучения новых сотрудников. Эти политики также регулируют отношения с клиентами и должны быть основой требований при автоматизации управления пространствами имен.

**8.1.1.1. Назначение имен**

Политика по назначению имен для пространств имен должна решать несколько ключевых вопросов:

* **Какие имена разрешены?** Определяет, какие символы, длина и формат допустимы для имен в пространстве.
* **Какие имена запрещены?** Устанавливает, какие имена являются недопустимыми по различным причинам (например, из-за технических ограничений или политических норм).
* **Как выбираются имена?** Объясняет, какой процесс или методы выбора применяются для создания уникальных имен.
* **Как решается проблема перекрытия имен?** Предусматривает процедуры и правила для разрешения конфликтов имен.
* **Когда допускается переименование?** Определяет условия и порядок, при которых возможно изменение имени элемента в пространстве имен.

Правила назначения имен могут диктоваться различными факторами, включая технические ограничения, корпоративный стиль или внешние стандарты. Например, в UNIX-системах логины могут состоять только из алфавитно-цифровых символов, а в DNS имена не могли начинаться с цифры до принятия RFC 1123.

**Методы выбора имен**

Существует несколько методов назначения имен:

1. **Шаблонный метод**. Все имена формируются по строгому шаблону. Например, рабочие станции могут иметь имена вида pc-1234, а логины — инициалы + шесть первых букв фамилии + случайный набор цифр для уникальности.
2. **Тематический метод**. Все имена соответствуют определенной теме. Например, серверы могут носить имена планет или персонажей научной фантастики.
3. **Функциональный метод**. Имена отражают функциональные обязанности устройства или пользователя. Например, серверы могут иметь имена типа dns1, webserver01, а учетные записи могут быть связаны с ролями: admin, guest, secretary.
4. **Описательный метод**. Имена содержат описания, которые помогают понять, для чего предназначен объект. Например, test-data для раздела диска или laserjet-printer для принтера. Крупные компании могут использовать географические наименования, такие как nyc-marketing или sjc-web-03.
5. **Метод без шаблона**. Имена выбираются без единого шаблона, что может привести к перекрытию и путанице.

**Проблемы и особенности методов**

Методы назначения имен, такие как шаблонный и функциональный, часто несовместимы между собой, и изменить схему назначения имен в сложной системе бывает сложно. Наиболее распространено комбинированное использование нескольких методов, например, функциональные имена могут сочетаться с описательными для улучшения понимания назначения объектов (например, nyc-marketing для отдела маркетинга в Нью-Йорке).

Использование определенных методов для назначения имен также влияет на корпоративную культуру. Для легкости работы в компании, где поддерживается непринужденная атмосфера, можно использовать тематические имена (например, имена принтеров в честь кофе), в то время как более строгие организации часто используют шаблонные имена.

**Аспект безопасности**

Некоторые методы назначения имен также могут повлиять на безопасность. Например, использование шаблонных или слишком очевидных имен может привлечь внимание злоумышленников, которые будут искать машины системных администраторов. В таком случае лучше избегать уникальных или слишком характерных имен и использовать псевдонимы для скрытия настоящих названий машин.

**Практические рекомендации**

При назначении имен для рабочих станций и серверов стоит следовать рекомендациям, например, в случае настольных машин, делать имена, отражающие имена пользователей, что упростит администрирование. Однако в некоторых случаях может быть полезно использовать псевдонимы, такие как ajaypc, чтобы избежать совпадений с именами пользователей в каталоге.

**8.1.1.2. Контроль доступа**

Политика контроля доступа к пространствам имен должна решать несколько важных вопросов:

1. **Какие защита и уровень безопасности требуются?**  
   Пространство имен должно быть защищено на нужном уровне в зависимости от его назначения и содержания. Например, для паролей требуется высокая степень безопасности, чтобы предотвратить несанкционированный доступ.
2. **От чего мы пытаемся защитить имена и зачем?**  
   Основная цель — защитить имена от несанкционированного изменения, доступа или утечек, что может привести к злоупотреблениям или утрате конфиденциальности. Например, данные, как логины и пароли, должны быть защищены от внешних угроз.
3. **Нужно ли защищать имена или только их атрибуты?**  
   Важно защитить не только сами имена, но и их атрибуты, такие как пароли, идентификаторы пользователей и другие чувствительные данные. Например, в UNIX-файле /etc/shadow, где хранятся пароли, требуется значительно больше защиты, чем в файле /etc/passwd, где содержатся только идентификаторы пользователей и другие атрибуты.
4. **Кто имеет право добавлять, изменять или удалять записи?**  
   Это зависит от прав и ролей пользователей. Например, системные администраторы могут изменять и удалять учетные записи, а пользователи могут изменять только свои данные или ограниченные атрибуты, если это разрешено политиками безопасности.
5. **Может ли владелец записи изменять определенные поля своей записи?**  
   В большинстве случаев владельцы записей могут изменять только те данные, которые связаны с их ролью или ответственностью, такие как собственные учетные данные (например, изменять свой логин или настройки), но не могут изменять данные других пользователей.
6. **От кого нужно защищать содержимое пространства имен?**  
   Пространство имен может быть защищено от различных категорий пользователей. Например, доступ к паролям или учетным записям должен быть ограничен только системными администраторами, а пользователи могут иметь доступ только к своим данным.
7. **Пример контекста доступа к пространствам имен:**  
   Например, в UNIX-системах логины могут использоваться в открытых источниках (например, на визитных карточках), но полный список пользователей не должен публиковаться, чтобы предотвратить спам. Также нельзя раскрывать пароли, связанные с этими логинами.
8. **Политики контроля изменений и резервного копирования:**  
   Политики изменения должны предусматривать возможность отмены изменений, а резервное копирование — гарантировать сохранность данных. Пространства имен, хранящиеся в текстовом формате, могут подвергаться контролю изменений с помощью систем, таких как SubVersion или SourceSafe. Важно, чтобы методы резервного копирования были настроены таким образом, чтобы в случае утраты или изменения данных можно было восстановить пространство имен.
9. **Методы защиты от изменений:**  
   В некоторых случаях пространство имен может быть защищено от изменений с помощью контроля доступа к файлам или базам данных. Для защиты от несанкционированных изменений можно использовать шифрование, а также более сложные механизмы аутентификации, чем просто пароль.

**Важные аспекты:**

* Уровень безопасности пространства имен должен зависеть от важности данных. Для критичных данных, как пароли, необходимо использовать строгие методы защиты, такие как шифрование и аутентификация.
* Контроль доступа должен включать не только ограничение прав на изменение данных, но и управление правами доступа для чтения, что также важно для предотвращения утечек информации.
* При проектировании системы важно понимать, кто может делать изменения, как и когда, а также как можно восстановить данные в случае ошибок или атак.

**8.1.1.3. Долговечность пространства имен**

Политика долговечности пространства имен должна решать вопрос, когда необходимо удалять записи из пространства имен. Важно учитывать следующие моменты:

1. **Когда удалять записи?** Некоторые записи в пространстве имен могут иметь срок действия, который заканчивается в определенный день или после периода бездействия. Например, учетные записи могут удаляться, если они не обновляются в течение года или если IP-адрес не используется в течение нескольких месяцев.
2. **Долговечность имен**  
   Имена, присвоенные пользователям, часто оказываются долговечными. После того как имя закрепляется за пользователем, его изменение становится сложным. Например, адрес электронной почты, указанный на визитках, может быть трудно изменить, и потребуется перераспределить новые карточки с измененным адресом. Это требует особого подхода к управлению именами, особенно в контексте сохранности информации и ее долгосрочной актуальности.
3. **Технологии маскировки имен**  
   Для решения проблемы долговечности имен можно использовать технологии маскировки. Например, можно скрыть реальные имена серверов или файловых систем за псевдонимами. Это позволяет изменять расположение или имена ресурсов, не влияя на пользователей. Примером может служить использование псевдонимов в DNS, таких как www, который может быть настроен на разные серверы, обеспечивая гибкость в изменении инфраструктуры.
4. **Решения для гибкости**  
   Использование псевдонимов и автоматических систем монтирования позволяет скрывать привязку ресурсов к конкретным именам и местоположению. Например, в UNIX можно использовать символические ссылки или автоматическое монтирование для абстракции реального местоположения файлов, предоставляя пользователям доступ по фиксированным путям, не зависящим от изменений в инфраструктуре.

**8.1.1.4. Вопросы сферы действия**

Политика по сфере действия пространства имен должна отвечать на вопросы, касающиеся географической и организационной области, в которой пространство имен будет применяться. Важными факторами являются:

1. **Диаметр (географическая область применения)**  
   Диаметр пространства имен определяется тем, на сколько систем оно распространяется. Пространство имен может быть локализовано на одном узле, в одном кластере, в одном отделе или использоваться глобально в рамках всей организации. Например, в случае с протоколом RADIUS, который используется для аутентификации на различных устройствах, одна база данных может обслуживать пользователей по всему миру.
2. **Плотность (количество сервисов, использующих пространство имен)**  
   Плотность пространства имен определяется количеством различных сервисов и систем, которые используют одно пространство имен. Например, уникальный идентификатор сотрудника может использоваться не только для логина в систему, но и для его электронной почты, доступа к VPN и других сервисов.
3. **Проблемы с именами в разных пространствах**  
   При использовании разных пространств имен в различных отделах компании может возникнуть ситуация, когда один и тот же идентификатор (например, tal) будет обозначать разных людей в разных отделах. Это может привести к проблемам при попытке переноса учетных записей между различными системами, так как каждое пространство имен может требовать уникальности имен.
4. **Глобальные и локальные пространства имен**  
   Иногда используется глобальное плоское пространство имен, что упрощает управление, но может создавать проблемы, если разных учетных записей для разных пользователей не хватает уникальности. В таких случаях можно использовать иерархические пространства имен, как в случае с DNS, где для каждого подразделения создается отдельная зона имен, что позволяет избежать конфликтов имен в разных частях организации.

Эти аспекты необходимо учитывать при проектировании системы управления именами, чтобы обеспечить их гибкость, долгосрочность и совместимость с различными сервисами и технологиями.

**8.1.2. Процедуры изменения пространства имен**

Каждое пространство имен требует четко прописанных процедур для добавления, изменения и удаления его элементов. Это необходимо для того, чтобы поддерживать порядок и обеспечить безопасность в процессе работы с именами. Некоторые аспекты:

1. **Документация процедур**  
   Процедуры изменения пространства имен должны быть документированы, хотя доступ к этой документации может быть ограничен. В малых системах, где над управлением пространством имен работает небольшая группа людей, эти процедуры могут быть неформальными и не требовать четкой документации. Однако по мере роста системы и расширения команды администраторов, документация становится необходимой для предотвращения путаницы и обеспечения четкости действий.
2. **Автоматизация изменений**  
   Если процессы изменения можно документировать простым и понятным образом, это уже открывает возможность для автоматизации. Автоматизация процессов не обязательно должна быть сложной, и часто существуют простые способы автоматизировать задачи по управлению пространством имен, что помогает сократить количество ошибок и повысить эффективность.

**8.1.3. Централизация управления пространством имен**

Централизованное управление пространством имен — это ключевой аспект для поддержания целостности системы. При централизованном управлении пространство имен хранится и обновляется в одном месте, что позволяет избежать разрозненности и несогласованности данных. Важные моменты:

1. **Целостность через централизацию**  
   Если управление пространством имен не централизовано, то данные о пользователях и других сущностях могут быть распределены по множеству серверов или даже в различных директориях одного сервера. Это создает риск рассинхронизации данных и усложняет управление. Централизованное хранилище помогает избежать этих проблем, улучшая целостность и упрощая процессы администрирования.
2. **Средства для централизованного управления**  
   Существуют различные инструменты для централизованного управления пространствами имен:
   * **GNU cfengine**: это мощный инструмент для управления конфигурацией системы на UNIX, который позволяет поддерживать контрольные копии пространств имен и распространять их по различным узлам сети.
   * **Microsoft ActiveDirectory** и **OpenDirectory в Mac OS X**: эти системы используют LDAP-серверы для централизованного хранения информации о пользователях и других элементах пространства имен, предоставляя клиентам доступ к данным.

Централизованное управление позволяет более эффективно управлять данными и системами, обеспечивая их согласованность и безопасность.

**8.2. Тонкости**

В этой части главы обсуждаются способы улучшения управления пространствами имен с помощью дальнейшей автоматизации и централизованного подхода. Вот ключевые моменты:

**8.2.1. Одна большая база данных**

Централизованное хранение всех пространств имен в одной базе данных SQL — это одна из лучших практик. Этот подход позволяет:

* Разработать интерфейсы (веб-приложения или оконные приложения) для внесения изменений в пространство имен.
* Синхронизировать эти изменения с другими системами, такими как ActiveDirectory, LDAP, NIS и другие.
* Современные решения с открытым исходным кодом, такие как PostgreSQL или MySQL, снижают затраты на реализацию этого подхода.

Использование такой базы данных упрощает управление и обеспечивает высокую степень контроля над всей инфраструктурой.

**8.2.2. Дальнейшая автоматизация**

После того как установлены основные процессы, можно продолжить автоматизацию на более высоком уровне. Это может включать:

* Использование первичной автоматизации как интерфейса для дополнительных проверок или повторных процессов.
* Пример: автоматическая проверка безопасности через итерацию по пространству имен (например, файл .rhosts), генерация списков рассылки из корпоративной директории.

Повторная автоматизация делает процессы более гибкими и эффективными, минимизируя человеческие ошибки.

**8.2.3. Обновление, управляемое пользователем**

Автоматизация может быть направлена на повышение самодостаточности пользователей, позволяя им:

* Запрашивать изменения и обновления в пространстве имен без необходимости вмешательства системного администратора.
* Например, система DHCP автоматически управляет выдачей IP-адресов, а пользователи могут управлять собственными учетными записями, что снижает нагрузку на администрацию.

Регулярное взаимодействие с пользователями помогает определить, какие процессы можно автоматизировать для улучшения рабочего процесса.

**8.2.4. Эффективное использование пространств имен**

Пространства имен могут быть полезны не только в компьютерных системах, но и в других сферах. Примеры применения:

* Снижение административной нагрузки на системы, такие как офисные АТС, системы голосовой почты и смарт-карты, через интеграцию с LDAP.
* В корпоративной базе данных LDAP можно автоматически создавать учетные записи для новых сотрудников, настраивать их электронную почту, телефонные номера и доступы.

Это приводит к улучшению эффективности работы и интеграции различных инфраструктур.

**8.3. Заключение**

В этой главе мы рассмотрели важность пространств имен в системе и их роль в обеспечении стабильной работы инфраструктуры. Основные моменты:

* Необходимо установить четкие правила и процедуры для управления пространствами имен.
* Централизация и автоматизация процессов управления пространствами имен значительно повышают целостность и эффективность работы.
* Пространства имен являются неотъемлемой частью эффективной работы других систем, таких как система электронной почты.
* Возможности для дальнейшей автоматизации увеличиваются с централизованным управлением.

В итоге, эффективное управление пространствами имен позволяет упростить взаимодействие пользователей с системами, уменьшить нагрузку на администраторов и улучшить совместную работу различных частей инфраструктуры.

**Глава 9. Документация**

Документация играет важную роль в системном администрировании, несмотря на то, что многие системные администраторы не склонны к ее написанию. Она необходима для организации работы, повышения ее эффективности и обеспечения доступа к важной информации для других сотрудников. Вот основные идеи, рассмотренные в главе.

**Документирование в системном администрировании** — это процесс записи информации о местоположении ресурсов, описания того, как выполняются задачи, а также обеспечение доступности этой информации для пользователей. Документация помогает не только системным администраторам, но и всей организации в целом. Несмотря на неохоту к документированию, оно существенно облегчает решение задач и улучшает взаимодействие между коллегами.

**9.1. Основы**

Основные задачи документирования включают:

* **Создание документации**: Это включает в себя простые методы записи информации о системах, процессах и правилах, которые упрощают работу и уменьшают нагрузку на администраторов.
* **Хранение документации**: Важно, чтобы документация была легко доступна. Это может быть как физическая документация, так и электронные ресурсы, доступные всем нуждающимся.
* **Обеспечение доступа**: Документация должна быть доступна для тех, кому она может понадобиться. Это не только администраторы, но и пользователи, которые могут самостоятельно решать проблемы, с которыми сталкиваются.

**Преимущества документации:**

1. **Облегчение работы**: Документация позволяет системным администраторам выполнять задачи более эффективно, сокращая время на решение однотипных проблем.
2. **Передача знаний**: Она помогает передавать информацию новым сотрудникам или менее опытным коллегам, делая их работу более продуктивной.
3. **Упрощение отпусков и выходных**: Документирование процессов позволяет системным администраторам брать отпуска, не опасаясь, что их отсутствие приведет к сбоям в работе.
4. **Предотвращение ошибок**: Документация помогает сократить количество повторяющихся ошибок и улучшить процесс их исправления.

**Документация как инструмент организации**

Документация помогает создать «память» организации, что важно для повышения квалификации и опыта команды. Она действует как «RAID-массив» для системных администраторов, обеспечивая резервирование знаний и предотвратив «ловушку незаменимости». Отказ от документации может привести к перегрузке сотрудника и невозможности полноценного ухода в отпуск или развития, поскольку без документов его навыки и знания становятся несменяемыми.

**Важность документации в организации**

В этой главе также подчеркивается важность того, чтобы документация была доступна не только администраторам, но и другим сотрудникам компании. Это способствует повышению общей эффективности работы и улучшению оперативности в решении задач.

**9.1.1. Что документировать**

Основной принцип выбора процесса для документирования — это его сложность и частота, с которой вы объясняете его другим. Если процесс:

1. **Сложный и неприятный**: Такие процессы обычно требуют точного выполнения шагов, и ошибки могут иметь неприятные последствия. Примером может служить подготовка рабочего места для нового сотрудника, включая настройку компьютера и создание учетных записей.
2. **Часто объясняемый другим**: Если вы постоянно объясняете, как что-то сделать, то это также сигнализирует о необходимости документации.

Документирование сложных процессов облегчает их выполнение другими людьми, избавляя вас от необходимости постоянно объяснять или исправлять ошибки. Например, если вам нужно передать выполнение задач кому-то другому, наличие документации позволяет нанять менее опытного сотрудника, обучая его со временем. Это также поможет в разгрузке команды и улучшении качества работы.

Создайте **список обязанностей**, включив в него процессы, которые вы не любите выполнять и которые были задокументированы. Составьте **список требуемых навыков**, определив, какие навыки и технологии должны быть знакомы системному администратору для выполнения каждой из задач.

**9.1.2. Простой шаблон для начала**

Для того чтобы начать документирование, важно сразу определить основные элементы документа. Используйте следующий шаблон:

1. **Название**: Название документа должно быть простым и понятным, чтобы другие могли легко понять, о чём идет речь.
2. **Метаданные**: Включите контактную информацию автора документа (обычно это ваша информация), дату последней редакции и историю изменений. Это важно для того, чтобы люди могли обратиться с вопросами и чтобы будущие пользователи понимали актуальность документа.
3. **Что**: Краткое описание цели документа — что должен достичь человек, следуя инструкциям. Это может быть всего несколько предложений.
4. **Как**: Шаги, которые нужно предпринять для выполнения задачи. Для каждого шага, который может быть непонятным или сложным, добавьте объяснение, почему именно так нужно поступить. Например: "Перемотать ленту (Почему? Потому что это снижает количество ошибок при резервном копировании)."

После составления документа внимательно проверьте его на точность. Ошибки могут привести к проблемам, которые должны были быть решены с помощью инструкции.

Для проверки документа выполните все шаги самостоятельно и попросите кого-то другого выполнить задачу по вашей инструкции, чтобы выявить затруднения. После этого проведите корректировку документа.

Кроме того, на основе этой документации можно создать **краткое руководство**, которое будет использоваться более опытными сотрудниками для быстрого выполнения задачи. Это поможет ускорить рабочий процесс и снизить вероятность ошибок.

**9.1.3. Простые источники для документации**

Есть несколько простых способов собирать материалы для документации, что упрощает процесс и помогает вам в будущем.

**9.1.3.1. Сохранение скриншотов**

Использование скриншотов может значительно упростить создание документации. Когда вы выполняете задачу, снимайте скриншоты на каждом шаге. Потом достаточно добавить краткие пояснения к изображениям. Это создаст наглядную и подробную документацию. Такие визуальные элементы помогают лучше понять процесс, так как люди могут сверить свой экран с изображением в документации, чтобы убедиться, что все делают правильно.

**9.1.3.2. Сохранение содержимого командной строки**

Если ваша работа часто связана с командной строкой, полезно сохранять содержимое терминала. Многие терминалы и консоли позволяют сохранять сеансы в файлы, а команда UNIX script позволяет записывать весь сеанс. Команда history также позволяет получить список недавно выполненных команд, который можно использовать как основу для документации. Эти сохраненные команды можно позже преобразовать в автоматизированные скрипты, что поможет в будущем сделать процесс более автоматизированным.

**9.1.3.3. Применение электронной почты**

Электронная почта часто является хорошим источником информации для документации. Если вы переписываетесь с коллегами по определенной задаче, то такие письма можно собрать и оформить в виде документа. Проблема в том, что электронную почту сложно использовать совместно и она может быть плохо организована. Чтобы решить это, соберите все сообщения, относящиеся к одной задаче, и объедините их в один файл. Сортировка писем по сеансам или темам поможет легче найти нужную информацию для документации.

**9.1.3.4. Изучение системы заявок**

Системы заявок на устранение неисправностей или обработку запросов могут стать отличным источником для документации. В таких системах часто есть возможность создать базу решений, которая поможет при решении аналогичных проблем в будущем. Если вы часто отмечаете, как решаете проблемы в заявках, это поможет быстрее создавать документацию. Можно дополнительно настроить систему так, чтобы важные заявки автоматически попадали в базу знаний, что позволит упростить документирование и ускорить создание полезной информации для коллег.

**9.1.4. Преимущества контрольных листов**

Контрольные листы (или списки действий) — это эффективный инструмент для организации задач и улучшения документации. Каждый пункт в таком списке представляет собой один шаг, и его можно отметить, когда этап выполнен. Это помогает не только структурировать процесс, но и избежать ошибок, гарантируя, что все этапы будут выполнены. Вот некоторые ключевые преимущества контрольных листов:

* **Уверенность в выполнении всех шагов.** Каждый этап можно пометить как завершенный, и это сразу показывает, если какой-то шаг пропущен.
* **Упрощение работы менее опытных сотрудников.** Контрольный лист может быть использован новичками, чтобы убедиться, что они не упустили важные шаги.
* **Ответственность и отчетность.** Важно, чтобы младший персонал сохранял контрольные листы или передавал их руководителю для отчета о выполнении задач.
* **Документация для совместных процессов.** Когда задачи требуют участия нескольких людей или подразделений, подписанный контрольный лист может служить подтверждением того, что все шаги были выполнены правильно.

Типичные контрольные листы могут включать:

* Задачи при найме нового сотрудника.
* Процедуры при увольнении сотрудника.
* Установки операционных систем.
* Архивация данных и обеспечение их хранения.
* Обеспечение безопасности ОС перед вводом в эксплуатацию.

Контрольные листы могут быть дополнением к основной документации для часто выполняемых задач. Они могут со временем стать настолько привычными, что для некоторых процессов достаточно будет просто списка действий.

Если процесс повторяется часто, то можно автоматизировать самые подверженные ошибкам шаги из контрольного листа. Со временем это может привести к автоматизации всей последовательности действий.

**9.1.5. Хранение документации**

Хранение документации в централизованном хранилище — важный этап для эффективной организации работы. Централизованное хранилище помогает обновлять и организовывать документы, а также облегчает их поиск. К тому же, это способствует нахождению документов, о которых вы могли не знать. Например, системные администраторы часто имеют свои собственные документы и записи, и их можно поделиться через центральное хранилище.

Чтобы создать простое хранилище, можно создать каталог с документацией на общем диске. В нем можно разместить файл README, который будет описывать правила и политику создания документации. Затем создаются подкаталоги по темам, например, рабочие станции, принтеры, Linux. Все документы можно аккуратно распределить по этим каталогам с информативными именами файлов. Это облегчит поиск, так как будет достаточно просмотреть содержимое каталога или провести поиск по ключевым словам.

В хранилище полезно использовать систему контроля версий, чтобы отслеживать изменения в документах и находить более старые версии в случае ошибок. Программы с открытым исходным кодом, такие как SubVersion, могут быть полезны для организации простого хранилища с контрольными версиями.

Веб-сайт может быть удобным хранилищем документов, но иногда его настройка может потребовать больше усилий, чем экономия от наличия документов. Хорошим решением может быть настройка веб-сервера для отображения содержимого каталогов, что упростит доступ к документам.

**9.1.6. Системы wiki**

Системы wiki — это веб-инструменты для публикации и совместной работы, которые произвели революцию в хранилищах документов. Название wiki происходит от гавайского слова "wikiwiki", что означает "быстрый". Первая система wiki, WikiWikiWeb, стала основой для всего подхода.

Системы wiki позволяют легко добавлять и редактировать документы любому пользователю с соответствующим доступом. Документы могут быть написаны в обычном тексте, HTML или с использованием собственных тегов wiki. Одна из сильных сторон wiki — это возможность для всех пользователей редактировать страницы. Это позволяет оперативно обновлять и исправлять информацию, сохраняя её актуальность.

Системы wiki поддерживают историю изменений, что позволяет отслеживать, кто и когда внес какие-либо правки. В случае ошибок или недочетов страницы можно вернуть в предыдущую версию. Также существует возможность защиты страниц, чтобы редактировать их могли только определенные пользователи.

Форматирование в wiki проще, чем в HTML, что делает систему доступной для людей без технического опыта. В wiki автоматически создаются гиперссылки, и если упоминается несуществующая страница, система предложит создать её.

Еще одной полезной функцией является создание заранее подготовленных страниц, которые могут понадобиться в будущем. Это позволяет быстро организовать структуру и содержание хранилища документов.

**9.1.7. Средство поиска**

Для эффективной работы с документами необходима система поиска. Веб-хранилища часто предлагают встроенные поисковые системы, которые варьируются от простых решений с открытым исходным кодом до более сложных аппаратных систем для индексирования данных.

Важно, чтобы система поиска позволяла ограничивать поиск по определённым областям, например, по названиям документов или содержимому. Также полезна возможность выполнения сложных запросов, например, поиск документов с определёнными ключевыми словами или метаданными.

Наличие полнотекстового поиска и фильтров для различных типов документов также является важным аспектом при выборе поисковой системы.

**9.1.8. Проблемы внедрения**

Одной из главных проблем при внедрении нового хранилища документов является заинтересованность пользователей, которые будут им пользоваться. Если сотрудники не захотят принимать участие, проект может потерпеть неудачу. Особенно это касается опытных специалистов, которые привыкли к более традиционным методам работы, например, электронной почте.

Один из способов решения этой проблемы — обеспечение автоматической генерации раздела «Последние изменения» в wiki, который будет отправляться заинтересованным людям. Это также можно организовать через RSS-трансляции, чтобы участники могли отслеживать изменения как в блоге.

**9.1.9. Самоуправление или прямое управление**

При создании хранилища документов важно заранее определить, кто будет отвечать за его поддержку — менеджер или администратора сайта, или система будет самоуправляемой. В большинстве случаев используется смешанная модель, где менеджер или руководитель периодически направляет деятельность, корректируя формат разделов или оставляя комментарии.

Если проект хранилища поддерживает самоуправление, то руководитель должен заниматься поддержкой инфраструктуры, помогать пользователям организовать работу с документацией, а не контролировать каждое изменение. Это позволяет создать более эффективную и полезную систему для всех участников.

Система управления содержимым (CMS) — это система для публикации веб-сайтов, которая помогает создавать, редактировать и публиковать материалы. Например, на сайте газеты CMS может помочь репортерам написать статьи, которые затем редактируются и публикуются. В IT-области CMS может включать функции для добавления различных дополнений, таких как обзор сбоев. Для работы CMS необходимо три ключевых уровня: хранилище, история и представление. Хранилище может быть представлено базой данных или структурированной файловой системой. История включает контроль версий, регистрацию событий и другие функции, такие как присвоение уникальных идентификаторов новым документам. Представление представляет собой пользовательский интерфейс, который дает доступ к редактированию и просмотру документов.

Многие современные системы CMS предлагают функции, аналогичные системам wiki, например Drupal и MediaWiki, которые обладают множеством функций CMS.

Важным аспектом успешной работы с системой "живой документации" является культура отношения, которая позволяет избежать сомнений у пользователей относительно того, что и как можно публиковать. Это связано с необходимостью модерируемой публикации. Несмотря на то что не каждый должен иметь возможность редактировать документацию, например, по проверке генераторов, важно, чтобы другие пользователи могли оставлять комментарии, которые позже могут быть включены в основное содержание. В случае ошибок система контроля версий позволит вернуться к предыдущей версии документа. Этот подход способствует более открытой и гибкой работе с документами.

Также важно, чтобы система wiki развивалась и становилась более формализованной по мере накопления материалов. Вначале лучше не загружать систему жесткой структурой, так как это может помешать простоте использования. Позднее, по мере увеличения количества документации, можно создавать шаблоны для повторяющихся документов и постепенно организовывать материалы в категории и разделы.

Система «живой документации» может быть использована для множества целей. Например, в разделе службы самостоятельной помощи пользователи могут найти инструкции по типовым вопросам, таким как настройка VPN или синхронизация с мобильными устройствами. Кроме того, этот раздел может включать мониторинг технических параметров, таких как загрузка маршрутизаторов или информация о свободном месте на дисках. Также на таких страницах могут быть размещены ссылки на средства проверки лицензий, что полезно для учета программного обеспечения.

Системные администраторы часто используют «живую документацию» для создания внутреннего раздела для своей команды. Это позволяет быстро найти информацию о сложных задачах, которые знают только несколько человек в группе, что важно в случае отсутствия сотрудников. Важно, чтобы доступ к таким разделам был ограничен, обеспечивая конфиденциальность и безопасность.

Документы типа How-To предоставляют пользователям пошаговые инструкции по выполнению конкретных задач, таких как настройка клиентских приложений или удаленный доступ к сетям. Эти документы обычно оформляются в доступной и наглядной форме, включая команды и скриншоты, чтобы помочь пользователям самостоятельно решать проблемы без обращения к поддержке.

Списки часто задаваемых вопросов (FAQ) могут быть полезны для быстрого получения ответов на распространенные запросы. FAQ обычно организуется по категориям и развивается со временем в зависимости от вопросов пользователей. Они могут указывать на более подробные документы How-To, если требуется более глубокое объяснение.

Справочные списки, такие как списки контактных данных поставщиков, серийных номеров оборудования или лицензионных ключей, используются реже, но служат важной вспомогательной целью. Например, список совместимости оборудования или каталог сотрудников может быть полезен для оперативного поиска нужной информации.

Процедуры и контрольные списки, необходимые для соблюдения стандартов и нормативных требований, таких как ISO или OSHA, могут быть документированы с помощью «живой документации». Это позволяет отслеживать соблюдение процедур и создавать журнал их выполнения, что особенно важно для организации, работающей с оборудованием или соблюдающей юридические требования.

Наконец, техническая библиотека или информационный сборник включает документацию от поставщиков, клиентов и другие важные материалы. Этот раздел может быть сложным для систематизации, однако важно поддерживать его в актуальном состоянии, чтобы пользователи могли быстро найти нужные документы.

### 9.3. Заключение

Документация предоставляет пользователям нужную информацию, что позволяет значительно снизить количество запросов к системным администраторам и экономить их время. Благодаря документации администраторы могут легко повторять процессы без ошибок и упростить их, что облегчает передачу поддержки процессов другим людям.

Документацию проще создать, используя шаблон, в который можно вставить скриншоты, сохраненные сеансы работы с терминалом, архивы электронной почты и данные из системы заявок. Контрольные листы являются хорошим инструментом для документации многозадачных процедур. Они помогут повторять эти процессы в одном и том же порядке, фиксировать требования других групп и обеспечивать младших системных администраторов инструментами для отчетности и передачи информации руководству.

Процесс документирования является сложным, однако как только будет проделана работа по созданию процесса, документация станет доступной для менее информированных людей. Это позволит легче поручать выполнение процесса другим. Наличие документации по процедурам также упрощает создание должностных инструкций при найме новых сотрудников.

### Глава 10. Аварийное восстановление и целостность данных

План аварийного восстановления рассматривает возможные нештатные ситуации, которые могут затронуть компанию, и предоставляет план реакции на эти ситуации. Планирование аварийного восстановления включает разработку способов смягчения последствий потенциальных нештатных ситуаций и подготовку быстрого восстановления основных служб. План должен определить ключевые службы и установить, как быстро они должны быть восстановлены.

Определенный уровень планирования аварийного восстановления должен присутствовать на всех сайтах компании. Проектировщики аварийного восстановления должны рассмотреть, что будет, если с одним из сайтов случится катастрофа, и как можно обеспечить восстановление. В данной главе рассматривается в первую очередь восстановление электронных данных, но этот аспект должен быть частью более широкой программы, которая также будет учитывать правовые и финансовые обязательства компании.

Планированию аварийного восстановления посвящено множество книг, таких как Fulmer 2000, Levitt 1997 и Schreider 1998, которые мы рекомендуем для более глубокого изучения.

### 10.1. Основы

Как и в любом другом проекте, создание плана аварийного восстановления начинается с определения требований: какие нештатные ситуации могут повлиять на ваш сайт, какова вероятность этих событий, их стоимость для вашей компании и как быстро нужно восстановить различные части бизнеса. После того как вы и ваше руководство поймете, что может произойти, можно будет получить необходимые средства для реализации проекта и начать искать способы выполнения (или даже превыполнения) этих требований.

### 10.1.1. Определение нештатной ситуации

Нештатная ситуация – это катастрофическое событие, которое вызывает значительный сбой, влияющий на всю организацию или сайт. Это может быть что угодно: от стихийного бедствия, например, землетрясения, до более распространенной проблемы, как случайное повреждение кабелей экскаватором. Важно, что нештатная ситуация — это событие, которое серьезно влияет на способность компании продолжать вести бизнес.

### 10.1.2. Анализ рисков

Первый шаг в создании плана аварийного восстановления — это проведение анализа рисков. Управление рисками является областью, где часто привлекаются сторонние консультанты, так как их специализированные знания требуются не постоянно, а лишь в нужные моменты. Крупные компании могут нанимать таких специалистов, при этом сохраняя штатного сотрудника, ответственного за управление рисками.

Анализ рисков включает определение тех нештатных ситуаций, с которыми может столкнуться компания, и оценку вероятности их возникновения. Специалисты анализируют возможные издержки для компании в случае каждой потенциальной ситуации. На основе полученной информации компания определяет, сколько средств она готова выделить для смягчения последствий каждого типа нештатной ситуации.

Пример: если вероятность того, что здание пострадает от наводнения, составляет один шанс из миллиона, а убытки от наводнения составят 10 млн долларов, то сумма, выделенная на предотвращение таких последствий, должна составлять не более 10 долларов. С другой стороны, если вероятность того, что компания окажется в зоне землетрясения с эпицентром в 10 милях от своей локации, составляет один шанс из 3000, а ущерб от землетрясения составит 60 млн долларов, то компания должна иметь бюджет в пределах 20 тыс. долларов для уменьшения ущерба.

Для более простого примера: если сайт зависит от единственного маршрутизатора, который связывает все локальные сети, и если этот маршрутизатор выйдет из строя, то для его ремонта потребуется один день. В случае сбоя все 1000 человек на сайте не смогут работать в течение этого времени, что приведет к убыткам на сумму 68 тыс. долларов. Бюджет для покупки резервного маршрутизатора может составлять около 23,8 тыс. долларов. Системные администраторы могут оценить расходы на уменьшение времени простоя, например, путем улучшения условий контракта на обслуживание, что поможет снизить возможные убытки.

Этот процесс может показаться упрощенным, но каждая нештатная ситуация может проявляться в разных масштабах с различной вероятностью и множеством факторов, влияющих на издержки. Профессиональный аналитик рисков учитывает все эти сложности, когда составляет рекомендации по бюджету на подготовленность к различным типам нештатных ситуаций.

### 10.1.3. Правовые обязательства

Помимо финансовых издержек, которые могут возникнуть в результате нештатных ситуаций, важно учитывать правовые обязательства, которые компания имеет перед различными заинтересованными сторонами, такими как поставщики, клиенты и акционеры. Организации, например, акционерные общества, обязаны соблюдать нормы фондовых рынков, в то время как университеты могут иметь контрактные обязательства перед своими студентами. Также важно учитывать строительные нормы, правила техники безопасности и другие регулирующие требования.

Юридический отдел компании должен разъяснить эти обязательства, которые могут выглядеть, например, как требования по восстановлению поставки продукции в течение недели или возможность задержки квартальной отчетности не более чем на три дня. Эти обязательства формируют требования к плану аварийного восстановления, которые включают восстановление работоспособности инфраструктуры в установленные сроки. Для этого необходимо точно понимать, какие компоненты инфраструктуры критичны для бизнеса и как быстро их нужно восстановить, а также учесть, какое время займет этот процесс. Эти вопросы будут рассмотрены более детально в разделе 10.1.5.

### 10.1.4. Ограничение ущерба

Ограничение ущерба касается минимизации финансовых потерь в случае нештатных ситуаций. Некоторые способы снижения ущерба могут быть реализованы с минимальными затратами или вовсе бесплатно через грамотное планирование и организацию процессов. Например, если территория подвержена небольшим затоплениям, можно разместить ключевые структуры на высоте, что поможет избежать ущерба в будущем. Применение устойчивых стоек для оборудования также может предотвратить повреждения от землетрясений без значительных дополнительных расходов. Внедрение громоотводов в районах с частыми грозами – это еще один пример недорогого метода предотвращения ущерба.

Однако для более серьезных аварий, например, защиты от торнадо или бомбардировок, требуются дорогостоящие решения, такие как строительство подземных бункеров или применение специальных механизмов для снижения повреждений от сильных землетрясений. Эти решения оправданы только для крупных организаций, способных покрыть высокие затраты.

Для большинства компаний решения по ограничению ущерба находятся между "бесплатными" и "дорогими". Например, системы пожаротушения могут быть важным элементом, и стоимость таких систем варьируется в зависимости от их типа. Наиболее популярными являются системы на основе инертных газов и водяные системы с механизмами раннего предупреждения, которые активируются только при необходимости.

### 10.1.5. Подготовка

Независимо от того, насколько эффективно реализованы меры по ограничению ущерба, нештатная ситуация все равно может произойти. Планирование аварийного восстановления должно включать подготовку к этому. Подготовленность означает способность быстро восстановить работоспособность ключевых систем в сроки, установленные правовыми обязательствами.

Процесс восстановления может потребовать переноса данных и сервисов на новое оборудование, если старое окажется неисправным. Необходимо заранее определить поставщиков оборудования и местоположения для его установки в случае аварии. Важно иметь договоренности с компаниями, которые смогут предоставить оборудование по первому требованию, а также учитывать время, необходимое для его замены, при планировании восстановления.

Кроме того, необходимо организовать безопасное хранение резервных копий данных. На многих сайтах это делают с помощью специализированных хранилищ для аварийного восстановления. После того как резервные копии данных будут доступны, восстановление системы может продолжиться. Для этого нужно точно знать, какие кассеты требуются для восстановления и сколько времени потребуется на их получение. Если процесс получения резервных копий занимает слишком много времени, может стать невозможным полное восстановление системы в установленные сроки.

Помимо данных, необходимо учесть такие факторы, как электропитание, телефонные линии и сетевые соединения. Также стоит проработать вариант переноса ключевых функций в другое место, если основное помещение окажется непригодным для работы.

### 10.1.6. Целостность данных

Целостность данных — это способность поддерживать неизменность данных, защищая их от изменений, вызванных внешними источниками. Внешними угрозами могут быть вирусы, умышленные атаки или случайные повреждения данных, связанные с ошибками пользователей, багами в программном обеспечении или сбоями оборудования. Для обеспечения целостности данных необходимо разработать стратегии регулярного резервного копирования и архивации.

Одним из способов проверки целостности является использование контрольных сумм для данных, которые не должны изменяться. Например, для баз данных, в которых изменения ограничены только добавлением новых данных, можно мониторить резкие изменения или удаления. К примеру, системы контроля исходного кода и базы данных генетических последовательностей могут использовать подобные методы для проверки целостности.

Аварийное восстановление требует наличия актуальной и согласованной копии данных, которая синхронизирует все базы данных компании. Важно, чтобы эта копия данных оставалась целостной в случае восстановления, так как любые искажения могут повлиять на процесс восстановления и даже стать проблемой в судебных делах. Например, если необходимо будет доказать права на интеллектуальную собственность, восстановление данных на определенную дату может быть использовано в качестве доказательства, но только при условии, что данные не были изменены.

При реализации механизмов обеспечения целостности данных необходимо следовать рекомендациям разработчиков системы, чтобы подтвердить надежность этих систем до возникновения нештатных ситуаций.

### 10.2. Тонкости

Полная подготовка к нештатным ситуациям включает в себя создание резервных версий всего критически важного оборудования и данных, которые могут занять место основного оборудования в случае его отказа. Одним из таких решений является наличие резервного сайта, который служит для дублирования инфраструктуры и восстановления работы компании.

### 10.2.1. Резервный сайт

Для организаций, которые требуют высокой доступности, создание полного резервного сайта — следующий шаг в процессе аварийного планирования. Резервный сайт должен располагаться в регионе, который не будет затронут теми же обстоятельствами, что и основной офис. Для большинства компаний создание такого сайта может быть слишком дорогостоящим, однако для крупных организаций (например, для банков) это является необходимостью.

Вместо того чтобы постоянно поддерживать резервное оборудование в другом помещении, можно использовать его только в случае чрезвычайной ситуации. Например, если у компании есть контракт с поставщиком оборудования для таких ситуаций, оборудование может быть доставлено в альтернативный вычислительный центр, что позволит быстрее восстановить работу компании.

Еще одной возможностью является использование оборудования менее важных служб с другого сайта для восстановления ключевых сервисов. Это может быть эффективным решением, если компания имеет разделенную инфраструктуру, что облегчает проектирование резервного сайта и сокращает расходы на поддержание его работы.

**10.2.2. Нарушения безопасности**

Нарушения безопасности становятся все более распространенной проблемой, когда злоумышленники могут атаковать систему удаленно, не нанося физического ущерба. Это могут быть различные виды атак: взлом веб-сайтов, похищение баз данных, удаление файлов вирусами и другие. В отличие от природных бедствий, такие инциденты не связаны с физическим ущербом, но они могут быть не менее разрушительными для бизнеса.

Для защиты данных от угроз важно проводить анализ рисков и разрабатывать соответствующие меры безопасности. Возможны два основных подхода:

1. **Построение барьеров** — создание защитных слоев вокруг системы.
2. **Мониторинг системы** — чтобы при атаке можно было быстро отключить систему и минимизировать ущерб.

Организации часто покупают готовые системы, не требуя от поставщика разъяснений о рисках безопасности. Однако, несмотря на то, что ни одна система не является полностью безопасной, поставщик должен объяснить структуру безопасности продукта и предложить план восстановления данных в случае утраты.

Глава 11 посвящена созданию политики безопасности, которая должна учитывать планы по аварийному восстановлению.

**10.2.3. Отношения с прессой**

Во время чрезвычайной ситуации важно правильно взаимодействовать с прессой. Журналисты будут интересоваться, что произошло, как это повлияло на компанию, и когда все будет восстановлено. Ответ "Мы не знаем" — худший, который можно дать, поскольку это может привести к дополнительным проблемам.

Есть два ключевых совета для подготовки:

1. **Заключение соглашения с PR-компанией** заранее. Это поможет избежать паники в кризисной ситуации и обеспечит квалифицированную помощь.
2. **Планирование взаимодействия с прессой**: определите, кто будет общаться с журналистами, что можно и что нельзя говорить, а также как будет организована цепочка принятия решений в отсутствие ответственных лиц.

Важно, чтобы все, кто будет взаимодействовать с прессой, прошли подготовку через PR-компанию.

**10.3. Заключение**

Основное в аварийном планировании — это понимание критически важных для бизнеса служб и временных рамок для их восстановления. Ответственные за планирование должны заранее знать возможные чрезвычайные ситуации и оценивать риски и затраты на их устранение.

Аварийный план должен учитывать:

* Время, необходимое для получения нового оборудования.
* Возможность восстановления всей системы с нуля.
* План для быстрой поставки необходимых резервных копий.

Ответственный за аварийное планирование должен также искать решения, как простые и дешевые, так и более сложные и дорогие. Автоматизация процессов, таких как системы пожаротушения, системы обнаружения воды, устойчивые к сейсмическим воздействиям конструкции — все это поможет ограничить ущерб.

Важно подготовить планы действий для сотрудников в случае чрезвычайной ситуации, а также проводить регулярные тренировки.

Хотя полное резервирование, включая резервный сайт, является идеалом, который не всегда доступен для компании, возможность использования второго вычислительного центра может быть более экономически оправданным решением для включения в аварийный план.