**Глава 11. Политика безопасности**

Безопасность — это гораздо более широкая тема, чем просто использование межсетевых экранов, обнаружение вторжений и аутентификация. Эти компоненты являются важной частью программы безопасности, но в целом безопасность требует выполнения множества других задач, для которых требуются различные знания и навыки. В этой главе рассмотрим ключевые аспекты безопасности, которые должны быть учтены при реализации программы безопасности в компании, а также общие рекомендации по созданию эффективной политики безопасности.

Безопасность должна быть задачей каждого сотрудника, однако важно, чтобы были выделены специалисты, которые сосредоточат все свои усилия на этой области, ведь безопасность — это быстро меняющаяся дисциплина. Наиболее подходящими кандидатами для работы в области безопасности являются старшие системные администраторы, которые обладают нужным мышлением и опытом.

**Основные идеи:**

* **Легкость соблюдения политики безопасности**: Лучшие политики безопасности — это те, которые просты для пользователей. Например, если вы хотите, чтобы люди использовали шифрование для электронной почты, важно, чтобы это было так же удобно, как и отправка обычного письма. В противном случае пользователи будут избегать использования этой функции.
* **Эволюция моделей доступа**: С течением времени способы доступа к компьютерам и сетям эволюционировали, и текущие тенденции показывают, что шифрование и строгая аутентификация становятся важными элементами защиты, заменяя традиционные подходы физической безопасности.

**11.1. Основы политики безопасности**

Существует два основных подхода к политике безопасности: **безопасность периметра** и **глубокая защита**.

1. **Безопасность периметра**: Этот подход можно сравнить с крепостью с высокими стенами, где защита сосредоточена на входе в сеть. Внутри сети считается, что все безопасно, если периметр защищен. Однако с развитием беспроводных сетей и более сложных сетевых соединений с партнерами, этот подход становится недостаточным.
2. **Глубокая защита**: Здесь безопасность встроена в каждый уровень системы. Это означает наличие межсетевых экранов, антивирусных программ, шифрования данных, а также аутентификации на каждом уровне взаимодействия с системой. Этот подход гораздо более гибкий и надежный, поскольку он предлагает защиту на всех уровнях, не ограничиваясь только входом в сеть.

**Принципы эффективной безопасности:**

* **Простота и минимализм**: Как и в других областях, архитектура безопасности должна быть простой, удобной для использования и поддержания. Сложные системы повышают вероятность возникновения ошибок и уязвимостей.
* **Встраивание безопасности в систему**: Элементы безопасности должны быть интегрированы в систему с самого начала, а не добавляться поверх уже существующих решений. Это обеспечит более устойчивую защиту и позволит избежать сложностей при интеграции новых решений.
* **Баланс между безопасностью и удобством**: Существует мнение, что повышение безопасности делает систему неудобной. Однако с развитием технологий можно достичь такого уровня безопасности, который будет не только эффективным, но и удобным. Например, использование единой авторизации значительно облегчает жизнь пользователям, позволяя им избежать множества паролей, при этом улучшая безопасность.

### 11.1.1. Задавайте правильные вопросы

Перед тем как приступить к реализации программы безопасности, необходимо четко определить, что именно вы пытаетесь защитить, от кого и какие риски существуют для компании. Ответы на эти вопросы должны быть результатом обсуждения с руководством компании. Документирование этих решений важно, чтобы обеспечить его развитие в будущем, однако важно избегать слишком частых изменений в этом документе.

### 11.1.1.1. Защита информации

Одним из самых ценных активов компании является информация, и поэтому защита информации является ключевым элементом корпоративной безопасности. Информация, которую нужно защитить, может быть классифицирована по нескольким категориям:

1. **Публичная информация**: Включает материалы, которые могут быть свободно распространены, такие как маркетинговые материалы, руководства пользователя, публикации на конференциях или в журналах.
2. **Конфиденциальная информация**: Включает более чувствительные данные, такие как организационные схемы, внутренние новости о финансовых результатах, данные о коммерческой деятельности, материалы о продуктах в разработке, исходный код, а также внутренние политики безопасности.
3. **Строго конфиденциальная информация**: Это самая защищаемая категория. Эта информация доступна только ограниченному кругу лиц, которые действительно нуждаются в ней для выполнения своей работы. Примеры: переговоры по контрактам, информация о сотрудниках, секретные разработки и интеллектуальная собственность клиентов.

Другим важным аспектом является защита информации от злонамеренных изменений, утечек, кражи или уничтожения.

### 11.1.1.2. Доступность обслуживания

Защита доступности обслуживания является важной задачей безопасности. Если компания зависит от доступности определенных ресурсов, то важной частью работы безопасности является предотвращение DoS-атак (атаки на отказ в обслуживании), которые могут нарушить нормальную работу сервисов. Это особенно важно для компаний, предоставляющих интернет-услуги, потому что сотрудники не склонны атаковать свои собственные системы, пока не столкнутся с подобной угрозой.

### 11.1.1.3. Кража ресурсов

Компании также могут потребовать защиту от кражи ресурсов. Например, если вычислительные мощности компании используются на полную мощность, то важно предотвратить их использование злоумышленниками. Это также касается медицинского оборудования, управляемого компьютерами, где возможность доступа к вычислительным ресурсам может быть критичной для безопасности и здоровья людей. Сайты электронной коммерции также могут подвергаться угрозам, связанным с кражей ресурсов, когда пираты могут скрывать свои серверы в инфраструктуре компании, что приведет к замедлению работы систем и потере клиентов.

### 11.1.2. Документируйте политики безопасности компании

Политики безопасности являются основой всех действий группы безопасности. Они должны быть формализованы и разработаны в сотрудничестве с различными отделами компании. Важно вовлекать в этот процесс:

* **Отдел кадров** для разработки политик допустимого использования, мониторинга и неприкосновенности личной информации, а также для определения санкций за нарушения.
* **Юридический отдел** для разработки политик, связанных с отслеживанием нарушителей и привлечением правоохранительных органов при необходимости.

Все политики должны быть утверждены высшим руководством. Это обеспечит соблюдение решений, принятых руководством, и позволит группе безопасности работать уверенно и в рамках интересов компании. Политики могут со временем развиваться и обновляться в ответ на новые угрозы или ситуации, однако для начала можно рассмотреть следующие общие политики.

#### Основные политики безопасности:

1. **Политика допустимого использования (AUP)**:
   * Определяет, кто имеет право использовать компьютерные и сетевые ресурсы компании и для каких целей.
   * Включает примеры недопустимого использования этих ресурсов.
   * Пользователи должны подписать эту политику перед получением доступа к ресурсам.
2. **Политика мониторинга и неприкосновенности личной информации**:
   * Описывает, какие данные мониторятся: использование ресурсов, электронная почта, веб-страницы, журналы событий и т.д.
   * Указывает уровень неприкосновенности личной информации, который гарантируется пользователю.
   * Политика должна учитывать местные законы, регулирующие мониторинг.
   * Пользователи должны подписать эту политику.
3. **Политика удаленного доступа**:
   * Описывает риски, связанные с удаленным доступом, и меры по защите данных, такие как пароли и PIN-коды.
   * Включает процедуры оповещения о потерянных или украденных данных для быстрого блокирования доступа.
   * Требует подписания политики всеми пользователями удаленного доступа.
4. **Политика сетевых соединений**:
   * Описывает, как компания устанавливает сетевые соединения с внешними организациями и какие ресурсы доступны третьим сторонам.
   * Устанавливает требования безопасности для таких соединений.
   * Политика должна быть внедрена на уровне руководства и предусматривать участие группы безопасности с самого начала.
5. **Политика ведения журналов**:
   * Описывает, что должно заноситься в журналы, сколько времени они хранятся и как используются для расследования инцидентов безопасности.
   * Журналы должны быть настроены так, чтобы не занимали слишком много места и содержали только необходимую информацию.

### 11.1.2.1. Получите поддержку высшего руководства

Для успешной реализации программы безопасности крайне важно получить поддержку высшего руководства. Руководство должно быть вовлечено в создание политик и правил безопасности, чтобы принимать решения, соответствующие интересам бизнеса, и понимать причины принятых решений. Чтобы завоевать доверие и авторитет, специалисты по безопасности должны уметь ясно объяснять риски и преимущества решений на языке, понятном для бизнеса, а не использовать технический жаргон.

В случае разногласий между группой безопасности и руководством, важно понять мотивы и ограничения, которые повлияли на принятие того или иного решения. Иногда безопасность может идти вразрез с бизнес-целями, и важно найти баланс между созданием защищенной системы и сохранением гибкости для развития бизнеса.

После того как решения по безопасности будут согласованы, они должны быть задокументированы, одобрены руководством и опубликованы в компании. Идеально, если директор по безопасности находится на высоком уровне и имеет опыт как в области защиты информации, так и в ведении бизнеса. Директор по безопасности возглавляет многофункциональную группу, которая разрабатывает и реализует политики и процедуры защиты информации в интересах компании.

### 11.1.2.2. Централизуйте полномочия

Возникающие вопросы и новые ситуации требуют централизованного подхода для принятия решений в области безопасности. Это позволяет поддерживать программу безопасности единой и эффективной. Для этого необходимо создать совет по политике безопасности или центральный орган, который будет отвечать за следующие аспекты:

* **Деловые решения**,
* **Создание политики**,
* **Архитектура безопасности**,
* **Реализация политики безопасности**,
* **Реакция на инциденты**,
* **Проверка и мониторинг соблюдения стандартов безопасности**.

Без центрального органа будет трудно внедрить стандарты безопасности и оперативно реагировать на происшествия. В крупных компаниях могут существовать как локальные органы безопасности для отдельных подразделений, так и корпоративный орган для установления общих стандартов. Важно, чтобы эти подразделения были четко отделены друг от друга, особенно если у них разные политики безопасности и архитектурные стандарты. Взаимосвязи между ними должны рассматриваться как соединения с третьими сторонами, с соблюдением политик каждой из сторон.

Примером проблемы может стать ситуация, когда два подразделения компании имеют различные политики мониторинга. Это может привести к тому, что одна группа безопасности будет случайно просматривать трафик сотрудника другого подразделения, что нарушит ожидания по поводу неприкосновенности личной информации и может привести к юридическим последствиям.

На техническом уровне важность централизованного контроля очевидна: если сеть компании соединена с автономной сетью, над которой нет контроля, то угроза безопасности значительно возрастает. Проблемы с отслеживанием нарушителей или управления безопасностью в таких условиях могут привести к уязвимостям в системе.

### 11.1.3. Основы для технического персонала

Как технический специалист в области безопасности, вы должны учитывать несколько ключевых принципов:

* **Обеспечение рабочих потребностей сотрудников**: ваша задача — обеспечить, чтобы пользователи системы могли эффективно выполнять свою работу, не сталкиваясь с чрезмерными ограничениями безопасности, которые мешают их деятельности.
* **Актуальные угрозы и уязвимости**: всегда будьте в курсе новых угроз и уязвимостей, чтобы своевременно обновлять систему безопасности и защищать ее от новых типов атак.
* **Система аутентификации и авторизации**: это один из критически важных элементов безопасности, за который вы будете отвечать, выбирая продукты и технологии для обеспечения безопасности доступа.

#### 11.1.3.1. Обеспечивайте потребности бизнеса

При проектировании системы безопасности важно учитывать потребности бизнеса. Безопасность не должна быть настолько строгой, чтобы мешать функционированию компании. Если система безопасности слишком сложна или неудобна, сотрудники могут найти способы ее обойти, что приведет к ослаблению защиты.

Более безопасная, но неудобная система может быть обойдена, что сделает ее менее безопасной, чем система с меньшими мерами безопасности, но с простотой в использовании. Поэтому важно находить баланс между уровнем безопасности и удобством работы, чтобы сотрудники могли выполнять свою работу, не прибегая к обходным путям.

**11.1.4. Вопросы руководства и организации**

Группа безопасности нуждается в поддержке руководства для эффективной работы в различных областях, таких как:

* **Поддержка достаточного уровня персонала** для обеспечения безопасности в зависимости от размера компании.
* **Координация с другими руководителями** для создания группы реагирования на происшествия, готовой к экстренным ситуациям.
* **Установление отношений с внешними проверяющими компаниями** и создание рабочего графика, соответствующего потребностям компании.

Кроме того, руководитель группы безопасности должен организовать взаимодействие с различными подразделениями компании, чтобы внедрять успешные методы безопасности и реагировать на угрозы.

**11.1.4.1. Ресурсы**

Группа безопасности требует доступ к различным ресурсам для успешной работы. Одним из ключевых факторов является наличие **связей в отрасли**, что позволяет быть в курсе событий и угроз. Эти связи помогают:

* Быстро реагировать на новые атаки,
* Оценивать работу компании по сравнению с другими,
* Определять, сколько компания должна тратить на безопасность и какие технологии внедрять.

Для создания и поддержания таких связей важно активно участвовать в **конференциях** и **межфирменных рабочих группах** по безопасности. Это позволяет не только быть в курсе отраслевых событий, но и повышать доверие среди коллег и профессионалов.

Группа безопасности требует людей с разнообразными навыками, и в зависимости от размера компании, эти обязанности могут выполняться одним человеком или целой командой. В крупных компаниях руководитель группы безопасности должен нанимать специалистов на различные позиции, такие как:

* **Разработчик политик безопасности**: отвечает за создание корпоративных политик и работу с различными подразделениями для их внедрения.
* **Архитектор безопасности**: проектирует систему безопасности компании, следит за инфраструктурой и новыми технологиями, решая, когда компания должна переходить на новые технологии.
* **Конструктор безопасности**: реализует проекты, проектирует инфраструктуру и обучает операторов.
* **Операторы безопасности**: занимаются ежедневной эксплуатацией системы безопасности, управляют аутентификацией и авторизацией.
* **Аудитор безопасности**: проводит проверку безопасности, включая тестирование на соответствие требованиям и возможные уязвимости.
* **Менеджер рисков**: оценивает технические риски и помогает компании принимать решения по допустимым отклонениям от стандартов безопасности.

**11.1.4.2. Реагирование на происшествия**

Создание процесса реагирования на происшествия — это важный этап, который должен быть подготовлен заранее. Вот ключевые моменты для эффективного реагирования:

1. **Подготовка до кризиса**. Группу реагирования на происшествия необходимо сформировать заранее, до того как возникнет реальная угроза. Это предотвращает хаос в момент инцидента.
2. **Процесс сообщения о происшествиях**. Важно заранее определить механизмы, по которым инциденты будут сообщаться группе реагирования. Это включает:
   * Как сообщения о происшествиях поступают в компанию.
   * Кто первым получает сообщение и как он должен действовать.
   * Как работать в нерабочие часы, если необходимо реагировать круглосуточно.
3. **Интеграция в стандартные процедуры**. Первоначальные сообщения о проблемах должны быть частью стандартных процедур для всех сотрудников. Важно, чтобы пользователи знали, как правильно сообщить о безопасности, даже если не имеют полного представления о том, является ли это инцидентом.
4. **Обработка инцидентов**. Человек, получивший сообщение о происшествии, должен уметь оценить его важность. В случае сомнений нужно передать сообщение соответствующему сотруднику группы реагирования на инциденты. От своевременной передачи информации зависит скорость реакции и эффективность решения проблемы.

**11.1.4.3. Внешние проверки**

Внешние проверки безопасности играют важную роль в обеспечении объективной оценки работы группы безопасности. Преимущества привлечения сторонних консультантов:

1. **Независимость и свежий взгляд**. Внешние аудиторы могут предоставить объективное мнение о состоянии безопасности, не будучи подверженными внутренним предвзятостям.
2. **Отстраненность от текущей работы**. Консультанты, не вовлеченные в ежедневную работу компании, могут предложить более свежие идеи и оценку рисков.
3. **Доступ к новым данным**. Эксперты могут предоставить информацию о последних новинках в отрасли и ресурсах, которые используют аналогичные компании.

Внешние аудиторы не должны заниматься проектированием или обслуживанием систем безопасности компании. Их задача — оценить безопасность компании извне, выполняя **глубокие атаки** на конкретные области, такие как базы данных или сетевые инфраструктуры, а не фокусироваться только на механизмах защиты.

**Глубокие атаки**

* Эти атаки позволяют тестировать безопасность сети и системы в условиях, близких к реальной атаке.
* Внешняя группа может предложить способы атаки, которые не были учтены внутренней группой безопасности.

**Социальная инженерия**

* Этот метод атакует человеческий фактор, пытаясь получить информацию или доступ через манипуляцию.
* Важно периодически тестировать сотрудников на уязвимость к таким атакам.

**Сканирование и тестирование**

* Внешние консультанты могут провести сканирование сетей и точек удаленного доступа, а также выполнить тестирование на проникновение (при наличии разрешения).
* Тестирование на проникновение требует четко определенных ограничений и согласования с руководством, чтобы избежать случайного ущерба компании.

**Координация действий**

* В процессе внешней проверки консультанты должны координировать свои действия с внутренними сотрудниками для предотвращения непредвиденных последствий.
* На проведение таких проверок должно быть получено одобрение высшего руководства.

Сторонние проверки — это важная часть общего подхода к безопасности компании, дополняющая внутренние проверки и предоставляющая дополнительные гарантии надежности системы.

**11.1.4.4. Многофункциональные группы**

Группа обеспечения безопасности не должна работать изолированно от других подразделений компании. Для успешной реализации политик безопасности необходимо:

1. **Сильные связи с другими подразделениями**. Группа безопасности должна быть в курсе всех новых разработок и изменений в компании, которые могут повлиять на безопасность. Особенно важны связи с группами системных администраторов, чтобы они поддерживали инициативы безопасности и не принимали решения, которые могут ослабить защиту.
2. **Юридический отдел**. Сотрудничество с юридическим отделом, особенно с IP-менеджером (менеджером по интеллектуальной собственности), крайне важно. IP-менеджер играет ключевую роль в защите интеллектуальной собственности компании, и взаимодействие с ним позволяет избежать проблем с безопасностью данных, хранимых в электронной форме, а также помогает на стадии планирования партнерских переговоров и слияний.
3. **Многофункциональная группа защиты информации**. В состав такой группы входят представители юридического, рискового, аварийного планирования, операционного, кадрового, маркетингового, инжинирингового и других отделов компании. Они вместе обсуждают, как наилучшим образом защитить интеллектуальную собственность компании и какие изменения в безопасности потребуются для каждого подразделения.
4. **Роль IP-менеджера**. Этот специалист часто участвует в защите информации при партнерских соглашениях, слияниях и приобретениях, а также в создании контрактных соглашений, которые могут включать требования к безопасности. Хорошие отношения с этим человеком позволяют эффективно планировать безопасность и вовремя учитывать изменения.

**11.1.4.5. Продавайте безопасность эффективно**

Продажа безопасности — это искусство убеждения, аналогичное продаже страхования. В случае с безопасностью трудно увидеть немедленную отдачу, но важно показать, как безопасность помогает предотвратить возможные потери.

1. **Привлечение высшего руководства**. Чтобы продать безопасность, необходимо показать, как она помогает компании выполнять обязательства перед акционерами и клиентами, а также как может служить конкурентным преимуществом. Примером может быть уверенность клиентов в том, что их конфиденциальная информация защищена, что повышает доверие и укрепляет репутацию.
2. **Внимание к интересам других подразделений**. Важно понимать, что безопасность должна быть полезной не только для группы безопасности, но и для других подразделений, таких как юридический отдел. Например, хороший уровень безопасности помогает защитить интеллектуальную собственность и выполняет обязательства по правовым требованиям.
3. **Данные о конкурентных усилиях в безопасности**. Чтобы убедить руководство, полезно собрать информацию о том, как конкуренты или аналогичные компании в отрасли инвестируют в безопасность. Это поможет оценить, правильно ли компания распределяет ресурсы на обеспечение безопасности.
4. **Метрики безопасности**. Для более объективной оценки эффективности работы группы безопасности следует разработать метрики, которые помогут измерить эффективность реализуемых политик. Это может включать данные о неудачных атаках, тенденциях в области угроз и возможных убытках от инцидентов.
5. **Привлечение сторонних консультантов**. Внешняя оценка рисков и независимые аудиты могут дать важные данные для принятия обоснованных решений о безопасности, что поможет убедить руководство в необходимости инвестиций в защиту информации.

### Будьте всегда в курсе: связи и технологии

Связи в сфере безопасности могут предоставить ценную информацию об актуальных угрозах, уязвимостях и развивающихся технологиях. Посещение конференций по безопасности помогает наладить связи и опережать конкурентов. На таких мероприятиях важно не только познакомиться с коллегами, но и стать активным участником сообщества. Это поможет выстроить доверительные отношения и получать знания из первых уст. Нужно также следить за новыми технологиями, понимать их принципы работы и потенциальные преимущества. Важно уметь отличать действительные полезные разработки от продуктов, которые обещают больше, чем могут предложить. Для этого полезно обращаться к экспертам и читать соответствующую литературу, например, книгу Мэтта Кертина о безопасности программного обеспечения.

### Создайте метрику

Метрика безопасности помогает продемонстрировать руководству эффективность работы группы безопасности и ее вклад в защиту компании. Это аналогично продаже страхования — чем более убедительные данные о безопасности, тем легче получить финансирование. Существуют внешние группы, которые могут проводить независимые проверки и предоставлять информацию о потенциальных угрозах и уязвимостях. Можно использовать системы, такие как системы обнаружения вторжений, для сбора статистики о безопасности периметра. Построив такие графики, можно наглядно показать результат работы, например, количество уязвимостей, требующих устранения, и количество обновлений программного обеспечения.

Хорошая метрика помогает не только информировать руководство, но и установить доверие к работе команды безопасности, демонстрируя прогресс и зоны для улучшений.

### Профили организаций

В этом разделе рассмотрены этапы разработки программы безопасности в зависимости от размера и специфики компании. Приводятся примеры для малых, средних и крупных компаний, а также для специфических организаций, таких как университеты и сайты электронной коммерции. Эти примеры помогут понять, как должна развиваться программа безопасности в зависимости от роста компании.

### Малая компания

В малых компаниях с ограниченным числом сотрудников акцент на безопасность обычно минимален. Важно разработать политику допустимого использования, а также подумать о защите личной информации. Системные администраторы могут справляться с основными задачами безопасности и контролировать все процессы. Особое внимание стоит уделить защите периметра, особенно если компания только начинает свою деятельность. Если инженеры работают с интернетом для получения актуальной информации, важно найти баланс между безопасностью и доступом к необходимым данным.

### Средняя компания

Средние компании требуют более сложной структуры безопасности. Здесь должен быть выделенный архитектор безопасности, который будет координировать работу группы. Важно создать централизованную систему безопасности, обеспечив четкие процессы отчетности. В компании должна быть внедрена система жесткой аутентификации, а также обеспечена защита от внешних угроз, включая работу с удаленными офисами и третьими сторонами. Необходима комплексная программа проверки безопасности, включающая различные подразделения компании, такие как юридический, информационный и кадровый отделы. Программа безопасности должна быть адаптирована под специфику бизнеса.

### Крупная компания

В крупных компаниях возникают проблемы из-за их размера, включая сложность управления инцидентами и согласования политик безопасности. Здесь важно иметь несколько сотрудников, каждый из которых отвечает за свою часть системы безопасности. Компания должна быть разделена на несколько подразделений, каждое из которых имеет свою политику безопасности. Каждое подразделение должно быть оснащено необходимыми механизмами защиты и программами информирования о безопасности. Крупные компании часто имеют более строгие требования к физической и электронной безопасности, так как количество сотрудников и подразделений значительно увеличивает риски утечек информации. Слияния и поглощения создают дополнительные вызовы для унификации политик безопасности и интеграции оборудования.

### Компания электронной коммерции

Компания, работающая преимущественно через Интернет, имеет специфические требования безопасности. В частности, важно разделять корпоративные машины и машины для сетевого обслуживания, которые используются для ведения бизнеса через Интернет. Для управления доступом к этим машинам необходимо разработать отдельные политики.

В компании электронной коммерции должен быть хотя бы один постоянный профессионал в области безопасности. Из-за особенностей бизнес-модели такого рода компаниям часто требуется более быстрое расширение персонала безопасности, чем другим организациям аналогичного размера. Важно также разрабатывать политики, связанные с защитой информации клиентов, например, данных о кредитных картах и контактной информации. Одной из главных задач является предотвращение DoS-атак на инфраструктуру сетевого обслуживания.

### Университет

Университетская среда значительно отличается от бизнес-среды. В бизнесе обычно предполагается, что люди с правомочным доступом работают в интересах компании, но в университете доступ к сети не всегда доверяется, что связано с более открытым физическим доступом и более свободной атмосферой.

В университете выделяются административные сети с ограниченным доступом и жестким контролем безопасности, а также открытые учебные сети. Университеты обычно имеют открытый доступ в Интернет, что важно для исследовательской работы. Однако из-за ограниченного бюджета на компьютерные системы и безопасность, университеты часто сталкиваются с трудностями в защите данных.

В университете должна быть разработана политика допустимого использования и мониторинга, а также защита личной информации пользователей. Важно задаваться вопросом, что нужно защитить, от кого и какие затраты это потребует. В случае с учебными сетями важно предотвратить потерю данных или нарушение работоспособности. Для ключевых серверов и административных сетей необходимы более серьезные меры безопасности.

### Глава 12. Этика

Этика, в отличие от морали, определяет принципы поведения, которыми руководствуется группа людей, а не общие представления о добре и зле. В данной главе рассматриваются этические вопросы, связанные с системными администраторами и другими сотрудниками с привилегированным доступом в организациях.

#### 12.1. Основы

Организации обычно устанавливают различные этические политики как для всех сотрудников, так и для привилегированных пользователей, таких как системные администраторы, руководители и администраторы баз данных. Системный администратор, имеющий доступ к конфиденциальной информации, должен строго соблюдать этические нормы компании и служить примером для других сотрудников.

В последнее время появились правовые акты, такие как закон Сарбейнса–Оксли, HIPAA и другие, которые усилили ответственность корпораций за соблюдение этических стандартов в сфере информационных технологий. Эти нормативные документы прямо затронули профессию системного администратора, призвав к более строгому соблюдению этических норм и повышению ответственности за работу с конфиденциальной информацией.

**12.1.1. Согласие, основанное на полученной информации**

Принцип согласия, основанного на полученной информации, первоначально был сформулирован специалистами по врачебной этике и справедлив для системных администраторов так же, как и для врачей. В контексте медицинской этики это согласие включает два основных этапа: пациент должен быть полностью информирован о вариантах лечения, возможных преимуществах и недостатках этих вариантов, а также вероятности их успеха. Информация должна быть представлена понятным образом, а пациент должен иметь возможность принять решение о лечении или отказаться от него без какого-либо принуждения.

Такое согласие невозможно, если человек не получил должной информации, не способен понять последствия или не может дать согласие, например, если он находится в коме и у него нет близких родственников. В таких случаях существует три основных условия: во-первых, процедура должна иметь высокую вероятность успеха; во-вторых, должны быть учтены интересы пациента; в-третьих, должны быть использованы все возможности для получения согласия на основе информации.

Эти принципы могут быть применены и к задачам системных администраторов. Например, соглашение об уровне обслуживания (SLA) может указать, что обслуживание будет доступно только в определенные часы, и пользователи должны быть об этом информированы. Если сервер предназначен для выполнения длительных задач, например симуляций, и у программы нет функции сохранения на контрольных точках, из-за перезагрузки можно потерять значительное количество работы. В таком случае SLA может предусматривать, что пользователи будут уведомлены о неизбежной перезагрузке — это и есть согласие, основанное на полученной информации. В других случаях, например при более краткосрочных задачах, SLA может предусматривать лишь предупреждение за 15 минут.

**12.1.2. Профессиональный кодекс поведения**

Гильдия системных администраторов (SAGE) и Лига профессиональных системных администраторов (LOPSA) разрешили опубликовать последнюю редакцию Этического кодекса системных администраторов, который является отличным примером профессионализма и высокого уровня этики для системных администраторов. Этот кодекс служит основой для разработки корпоративных правил поведения. Он не является сводом обязательных законов или перечнем санкций, а скорее рекомендациями и принципами, которых должны придерживаться профессионалы.

**Этический кодекс системного администратора:**

* **Профессионализм:** Я буду соблюдать профессиональные нормы на рабочем месте, не позволяя личным чувствам или убеждениям влиять на мое отношение к людям.
* **Личная сознательность:** Я буду честным в своей профессиональной деятельности и позитивно воспринимать критику. При необходимости обращусь за помощью к коллегам.
* **Неприкосновенность личной информации:** Я буду доступать к личной информации только когда это необходимо для выполнения моих обязанностей и буду защищать конфиденциальность.
* **Законы и политики:** Я буду изучать и обучать актуальным законам и политиками, касающимся моей работы.
* **Общение:** Я буду обсуждать компьютерные вопросы с коллегами и пользователями в наших общих интересах, выслушивая потребности всех сторон.
* **Целостность системы:** Я буду обеспечивать целостность, надежность и доступность систем, за которые я ответственен.
* **Образование:** Я буду расширять свои знания и делиться ими с другими.
* **Ответственность перед сообществом:** Я буду поддерживать целостность сетевых и компьютерных ресурсов, сотрудничая с более широким сообществом.
* **Социальная ответственность:** Я буду способствовать созданию и принятию актуальных политик, соответствующих этическим принципам.
* **Нравственная ответственность:** Я постараюсь поддерживать здоровую рабочую атмосферу, учитывать безопасность и благополучие моего сообщества и общества в целом, а также буду честно критиковать других и признавать заслуги коллег.

**12.1.3. Руководства пользователя**

В каждой организации должен быть набор руководств по допустимому использованию компьютеров. Эти руководства могут касаться ряда вопросов, таких как:

* При каких обстоятельствах допускается использование оборудования работодателя в личных целях?
* Какие виды личного использования запрещены?
* Можно ли сотруднику посещать интернет-магазины с рабочего места?
* Разрешено ли писать в блог с работы?
* Как насчет использования рабочего компьютера для просмотра сайтов «для взрослых»?
* Как меняются правила, если сотрудник использует оборудование компании дома?

Правила должны также определять и запрещать опасные или мешающие действия, а также объяснять, как сообщать о таких случаях и как эти сообщения обрабатываются. Иногда такие указания становятся частью политики допустимого использования, обсуждавшейся в главе 11.

В учебных заведениях правила поведения могут существенно отличаться от корпоративных. Это связано с требованиями свободы обучения и тем, что для студентов университетский комплекс может быть домом.

Для составления политик можно обратиться к образцам, которые часто доступны на веб-сайтах различных деловых и учебных ассоциаций. Например, архивы, как Dijker 1999, могут стать отличной основой для создания собственных корпоративных политик.

**12.1.4. Правила поведения привилегированных пользователей**

Некоторые пользователи нуждаются в привилегированном доступе для выполнения своих задач. Например, права root или администраторские права позволяют работать с драйверами устройств, устанавливать программы для других сотрудников и выполнять другие важные задачи. Привилегированные пользователи требуют особых правил поведения, поскольку их доступ может быть использован не по назначению. Эти правила должны включать следующие моменты:

* Признание того, что привилегированный доступ требует особой ответственности.
* Обязательство использовать привилегированный доступ только по служебной необходимости. Руководство должно четко определить, что именно включает в себя служебная необходимость.
* Признание того, что ошибки могут случаться, и обеспечение процедур минимизации ущерба. Например, системные администраторы должны делать резервные копии перед внесением изменений.
* Определение процедур на случай, если привилегированный доступ приводит к обнаружению конфиденциальной информации, которая иначе не была бы известна. Например, если системный администратор случайно видит информацию о сетевых азартных играх на рабочем месте, политика должна четко объяснять, как поступить в такой ситуации.
* Определение действий в случае получения важной, но не преступной информации, например, о предстоящем слиянии компании. Политика должна быть ясной в этом вопросе.
* Указание последствий за ошибки. Оптимальная политика — отсутствие наказания за непреднамеренные ошибки, если они были честно и своевременно сообщены. Чем раньше ошибка будет замечена, тем быстрее она будет исправлена и тем меньше ущерба будет нанесено.
* Предупреждение о возможных санкциях за нарушение политики, включая увольнение.
* Привилегированные пользователи должны подписать расписку, подтверждающую, что они ознакомлены с нормами поведения для привилегированных пользователей. Эта расписка должна храниться у руководителя или в отделе кадров, в зависимости от организации.
* Для повышения безопасности группа системных администраторов должна отслеживать, кто имеет привилегированный доступ к каким системам. Это особенно важно, когда нужно отключить привилегии для сотрудников, покидающих организацию. В некоторых случаях политика требует, чтобы привилегированный доступ пересматривался ежегодно, с обязательным подписанием документа, иначе доступ будет прекращен.

**12.1.5. Соблюдение авторских прав**

В организациях должны быть политики, которые обязывают сотрудников соблюдать законы об авторском праве. Проблема компьютерного пиратства является актуальной, и многие люди не понимают, что использование программы без лицензии, даже для личных нужд, является нарушением закона. Например, «одолжь» программу без разрешения правообладателя — это кража.

Компании часто проявляют особое внимание к пиратскому программному обеспечению, поскольку использование таких программ может привести к финансовым и репутационным последствиям. На компании могут быть наложены штрафы или санкции за использование нелицензионных программ. Чтобы избежать подобных проблем, организации должны придерживаться строгих политик:

1. **Примеры нарушений:** Политика должна содержать 3–4 примера распространённых нарушений, например:
   * Программное обеспечение с индивидуальной лицензией должно быть приобретено для каждого компьютера.
   * Установочный диск не должен использоваться на нескольких машинах.
   * Руководства и материалы для программного обеспечения должны храниться в одном месте с компьютером, на котором оно установлено.
2. **Контроль за установкой программ:** В некоторых компаниях запрещено устанавливать программы без явного одобрения руководства. Также могут быть указаны программы, которые сотрудники могут загружать самостоятельно (например, новые версии Adobe Acrobat или веб-браузеров).
3. **Политика по пиратскому ПО:** Следует включить пункт, напоминающий о том, что пиратское ПО не является приемлемым решением для сокращения расходов. Пример текста: «Мы все стараемся снизить расходы, но пиратское программное обеспечение не является легитимным способом экономии. Никому в этой компании не разрешается заниматься пиратством».
4. **Купить лицензионное ПО:** Для соблюдения политики лучше всего закупать популярные программы с корпоративными лицензиями для всех рабочих станций, что минимизирует риск нарушения. Если это невозможно, можно требовать, чтобы все заявки на новые рабочие станции или серверы включали также необходимые лицензии на операционные системы и приложения.
5. **Бесплатное и открытое ПО:** При использовании открытого программного обеспечения важно внимательно изучить лицензию. Некоторые компании назначают отдельные группы для управления соблюдением лицензий на открытое ПО.
6. **Ответственность за нарушение:** Важно донести до сотрудников, что при предъявлении иска о нарушении авторских прав, ответственность, как правило, возлагается на человека, совершившего нарушение. Политика должна указать, что системный администратор, установивший лицензию на новый компьютер без должного согласования, может быть обвинен в нарушении.

**12.1.6. Работа с правоохранительными органами**

Организациям следует разработать политику взаимодействия с правоохранительными органами, чтобы системные администраторы знали, что делать, если правоохранительные органы обращаются к ним за помощью в расследованиях. Ситуации могут быть стрессовыми, и важно знать, как действовать правильно:

1. **Процедуры взаимодействия:** Важно работать с правоохранительными органами через руководство. Системный администратор должен всегда проверять личность сотрудника правоохранительных органов, прежде чем предоставлять какую-либо информацию. Для этого можно запросить номер телефона сотрудника и позвонить по коммутатору, чтобы удостовериться в его личности.
2. **Социальная инженерия:** Важно быть осторожными, так как некоторые злоумышленники могут представляться сотрудниками правоохранительных органов с целью украсть информацию через тактику социальной инженерии. Эта техника включает в себя сбор небольшой информации, а затем её использование для получения более важной информации.
3. **Опасность подделки:** Если системный администратор не проверяет личность представителя правоохранительных органов, это может привести к утечке информации компании. Поэтому важно придерживаться протокола, проверяя каждую деталь, прежде чем передавать какие-либо данные.

Создание таких четких процедур и политик поможет избежать серьезных юридических проблем и обеспечить безопасность корпоративных данных в случае контактов с правоохранительными органами.

**Указания поступить незаконно/безнравственно**

Важно понимать, что делать, если ваш руководитель просит вас совершить что-то незаконное или противоречащее правилам компании. Главное — записывать все события, связанные с такими требованиями. Начните с проверки, может быть, вы неправильно поняли требование. Если оно незаконно или нарушает политику компании, вежливо откажитесь его выполнять. Если руководитель настаивает, можно обратиться к вышестоящему руководству или в отдел кадров.

Полезный метод — попросить оформить требование в письменной форме или по электронной почте. Это дает вам документ, который можно будет использовать для разъяснений или подтверждения. Если человек отказывается предоставить такое требование, это может быть сигналом, что он не хочет брать на себя ответственность.

**Пример с просьбой прочитать чужую электронную почту**

Предположим, руководитель просит вас прочитать чужую почту для получения информации о проекте. Важно уточнить просьбу и проверить, противоречит ли она политике компании. Если требование нарушает правила, вежливо напомните об этом руководителю. В случае сомнений можно обсудить ситуацию с коллегами или вышестоящим руководством.

**Заключение**

Этика — это принципы, которые регулируют поведение людей. Важно иметь четкие нормы и политики для всех сотрудников, чтобы они знали, как поступать в сложных ситуациях. Этический кодекс помогает повысить профессионализм и улучшить имидж работников.

**Глава 13. Службы поддержки**

Служба поддержки — это место, где пользователи могут получить помощь по вопросам, связанным с компьютерами, сообщить о проблемах и запросить новые услуги. Это может быть физическое помещение или виртуальная служба с электронным доступом. Служба поддержки играет ключевую роль в организации, так как она формирует первое впечатление о компании и поддерживает отношения с пользователями. Пользователи часто воспринимают службу поддержки как основное лицо организации.

**Основы работы службы поддержки**

Для успешной работы службы поддержки необходимо правильно ее организовать. Важно обеспечить достаточное количество сотрудников для работы с обращениями, определить область их ответственности, наладить рабочие процессы и иметь механизм для передачи проблем на более высокий уровень, если они не могут быть решены. Также необходимо внедрить системы для отслеживания запросов и решения проблем.

**13.1.1. Организация службы поддержки**

Служба поддержки существует в каждой организации, и она может быть как физической, так и виртуальной. В некоторых случаях служба поддержки является неофициальной, где системные администраторы помогают пользователям в свободное время. Когда количество системных администраторов растет, требуется формализовать службу поддержки. Это нужно делать заранее, чтобы избежать проблем, когда организация уже достаточно разрослась.

Служба поддержки должна быть частью планирования развития компании. Признаком необходимости создания формальной службы является то, что системные администраторы начинают испытывать трудности с выполнением своих проектов из-за частых отвлечений на запросы пользователей. Также возможен переход от неформальной помощи к официальной службе, что требует усилий для упрощения переходного периода и объяснения новых процедур.

Службы поддержки могут быть виртуальными, с возможностью обращения по электронной почте или через текстовые и голосовые сообщения. Системы самостоятельной помощи также могут быть полезными, но не должны заменять живое общение с людьми. Важно иметь простую документацию, которая будет доступна для пользователей через веб-сайт или блог. Веб-системы могут снизить нагрузку на сотрудников, но не способны полностью заменить человеческое взаимодействие.

**13.1.2. Будьте дружелюбны**

Служба поддержки должна быть дружественной. Физическая служба поддержки должна иметь приятный и гостеприимный интерьер, а виртуальная — использовать успокаивающие цвета и понятный интерфейс. Важно, чтобы лица сотрудников были дружелюбными, а их личностные качества подходили для работы с клиентами. Атмосфера, создаваемая администратором, будет определять атмосферу в команде.

Администраторы, создающие доброжелательную атмосферу, привлекают соответствующий персонал, что, в свою очередь, влияет на отношение к пользователям. Легче с самого начала создать атмосферу дружелюбия, чем позднее исправлять репутацию. Важно быть примером для своего коллектива и всегда демонстрировать открытость и доброжелательность.

**13.1.3. Отражение корпоративной культуры**

Служба поддержки должна соответствовать корпоративной культуре организации. Если она не поддерживает ценности компании, это может повлиять на восприятие ее работы. Например, в строгих и формальных компаниях сотрудники службы поддержки не должны носить слишком непринужденную одежду, как футболки с надписями, иначе они могут быть восприняты как недисциплинированные, несмотря на качество их работы. В то же время, если организация имеет креативную атмосферу, сотрудники службы поддержки могут работать в более свободной обстановке.

Очень важно учитывать культуру организации при создании службы поддержки, чтобы она гармонировала с ожиданиями пользователей. Культура поддержки должна соответствовать тем, кто будет ею пользоваться, чтобы сотрудники могли эффективно взаимодействовать с пользователями.

**13.1.4. Достаточность персонала**

Для эффективной работы службы поддержки необходимо, чтобы в ней было достаточно персонала для своевременного обслуживания всех пользователей. Недостаток сотрудников приведет к тому, что пользователи будут искать помощь в других местах.

Численность персонала службы поддержки может сильно варьироваться в зависимости от типа организации. В университетах на одного сотрудника службы поддержки может приходиться тысячи студентов, в то время как в корпорациях или компаниях электронной коммерции соотношение может быть другим. Важно найти баланс между количеством пользователей и количеством сотрудников. Это можно сделать, отслеживая интенсивность вызовов и время обслуживания, а не просто пытаясь поддерживать фиксированное соотношение пользователей и сотрудников.

Управление на основе интенсивности вызовов позволяет искать более разнообразные решения, например, внедрение автоматизированных систем, которые позволяют пользователям выполнять задачи без вмешательства сотрудников. Метрики, такие как время ожидания ответа, могут помочь выявить, какие процессы наиболее эффективны, и где можно улучшить обслуживание.

**13.1.5. Определение полномочий поддержки**

В службе поддержки должна быть четко прописанная политика, которая определяет полномочия сотрудников. Это документ, который разъясняет, за что отвечает группа системных администраторов, и что не входит в их обязанности. Полномочия охватывают следующие аспекты:

1. **Что поддерживается**: Например, поддержка ограничивается только компьютерами или включает также локальную сеть, поддержку конкретных операционных систем или всех. Необходимо также четко определить, как решаются проблемы с неподдерживаемыми платформами.
2. **Кто поддерживается**: Какие подразделения или группы пользователей получают поддержку. Это может включать сотрудников конкретных офисов, подразделений, а также работу с удаленными пользователями и филиалами.
3. **Где предоставляется поддержка**: Служба поддержки может обслуживать пользователей в одном здании, на нескольких площадках или поддерживать путешествующих сотрудников.
4. **Когда предоставляется поддержка**: Установление четких часов работы службы поддержки и решения, что делать в нерабочее время. Например, создание механизма для обращения к системным администраторам вне рабочих часов.
5. **Как долго будет длиться выполнение запроса**: Установление нормативов для времени, которое нужно для выполнения разных типов запросов, таких как срочные задачи или более длительные проекты.

Документ должен быть доступен всем сотрудникам и четко объяснять, что входит в обязанности службы поддержки и какому типу запросов следует уделять внимание. Это помогает избежать перегрузки сотрудников и повысить эффективность работы.

**13.1.6. Указания по получению помощи**

Пользователи должны четко знать, как получить помощь от службы поддержки. Это можно указать в документах, которые разъясняют, как обращаться за помощью — по телефону, электронной почте или через систему заявок. Также важно, чтобы были указаны контактные данные (например, номер телефона, адрес электронной почты, веб-сайт).

Этот документ должен быть кратким, с ясными указаниями, чтобы избежать недоразумений. В идеале информация о способах получения поддержки должна быть размещена на видном месте на устройствах пользователей (например, на стикере или в фоновом изображении рабочего стола).

**13.1.7. Определение процессов для персонала**

Важным элементом работы службы поддержки является четко определенный и документированный процесс, которому должны следовать сотрудники при оказании помощи. Это особенно важно в крупных организациях, где процессы могут быть сложными и требуют формализации.

Для крупных служб поддержки часто используются сценарии, которые помогают структурировать диалог с пользователем и обеспечивают последовательность действий при обработке запросов. Например, сценарий для запроса удаленного доступа или сброса пароля может включать требования безопасности, такие как подтверждение личности пользователя.

Четкие процессы помогают поддерживать порядок и эффективность работы службы поддержки.

**13.1.8. Процесс передачи проблемы на более высокий уровень**

Передача проблемы на более высокий уровень — это процесс, в рамках которого проблема передается от одного сотрудника поддержки к более опытному специалисту, если она не может быть решена на первом уровне. Обычно, сотрудники первого уровня должны справляться с 80-90% запросов, а сложные проблемы передаются на второй уровень, где работают более опытные специалисты.

Часто используется правило, согласно которому все запросы, на решение которых требуется более 15 минут, должны быть переданы на второй уровень. Это помогает освободить время сотрудников первого уровня для более быстрых задач, однако стоит учитывать, что передача больших объемов запросов на более высокие уровни может снизить время, которое у специалистов второго уровня есть для работы над проектами.

Для решения проблемы перегрузки второго уровня можно назначить сотрудника второго уровня, который будет работать с сотрудниками первого уровня, обучая их и помогая в решении более сложных вопросов. Это не только помогает снизить количество ошибок и улучшить качество обслуживания, но и способствует улучшению взаимодействия между уровнями поддержки.

Процесс передачи на более высокий уровень также может быть использован, когда пользователи недовольны обслуживанием на первом уровне. В таких случаях всегда должна быть возможность для передачи запроса к руководству службы поддержки, чтобы улучшить решение проблем и избежать недовольства пользователей.

**13.1.9. Письменное определение экстренных случаев**

Очень важно для службы поддержки четко определить, что является экстренным случаем, и прописать это в документах. Это поможет системным администраторам точно понимать, когда нужно предоставить срочную помощь, а когда можно отложить решение проблемы.

Без такой политики сотрудники службы поддержки могут столкнуться с ситуацией, когда каждый пользователь считает свою проблему экстренной, что может привести к перегрузке системы. Прописанная политика позволяет администратору отказывать в экстренности запроса, если это необходимо, и передавать вопрос более высокому руководству.

Определение экстренного случая должно быть привязано к специфике бизнеса. Например:

* В производственной компании экстренным случаем будет ситуация, когда останавливается сборочная линия.
* В интернет-провайдере — это проблемы с доступом, которые влияют на качество обслуживания пользователей.
* В учебных заведениях экстренным случаем может быть сбой, который нарушает важные образовательные процессы, такие как экзамены или зачисление студентов.

**13.1.10. Программа отслеживания заявок**

Для эффективной работы службы поддержки необходима программа для отслеживания заявок. Без такой программы задачи могут быть потеряны, а процессы становятся непрозрачными для руководства.

Основные функции программы включают:

* Назначение приоритета заявкам, что помогает оптимизировать рабочий процесс и оправдать ожидания пользователей.
* Ведение логов, которые фиксируют все действия по заявкам. Эти данные могут быть полезны для анализа и улучшения работы службы поддержки.
* Автоматизация сбора данных по удовлетворенности пользователей, что помогает отслеживать качество обслуживания и выявлять области для улучшения.

Программа должна поддерживать автоматическое отображение сценариев для обработки заявок, облегчая сбор информации и выполнение задач. Это особенно важно для крупных организаций, где есть большое количество запросов, и их обработка требует четкой системы управления.

**13.2. Тонкости службы поддержки**

**13.2.1. Статистические усовершенствования**

Собирая статистику, можно значительно улучшить работу службы поддержки. Важно отслеживать количество заявок, переданных на более высокий уровень, чтобы выявить области, требующие дополнительного обучения сотрудников. Это также помогает демонстрировать эффективность работы службы поддержки перед руководством и обосновать потребность в дополнительном бюджете.

С ростом компании становится проще собирать статистику, поскольку методы работы становятся более автоматизированными. Это важно не только для текущей работы, но и для планирования, особенно когда речь идет о поддержке новых технологий или сервисов. Использование ретроспективной статистики позволяет предсказывать возможные затраты на поддержку и оценивать эффективность существующих решений.

**13.2.2. Поддержка в нерабочее время и в режиме 24/7**

С увеличением зависимости бизнеса от технологий, поддержка в режиме 24/7 становится необходимостью. Даже если организация не может обеспечить круглосуточную поддержку, существует несколько экономичных способов этого достичь. Например, можно настроить голосовую почту, которая отправляет уведомление на пейджер. Сотрудники могут передавать пейджер по очереди, чтобы решить проблему как можно быстрее, или просто уведомить компетентных людей о возникшей ситуации.

Другим вариантом является создание системы, в которой руководители групп пользователей могут контактировать с администратором службы поддержки, который по очереди будет находить системных администраторов для решения проблемы. Такой подход позволяет избежать перегрузки одного администратора и минимизировать затраты на круглосуточную поддержку.

**13.2.3. Лучшая реклама службы поддержки**

Для того чтобы политики службы поддержки были доступны и понятны пользователям, важно обеспечить их публикацию на веб-портале организации. Однако, чтобы привлечь внимание пользователей к этой информации, нужно позаботиться о том, чтобы они знали о наличии этих ресурсов и заинтересовались ими. Для этого можно использовать различные способы: рассылки по электронной почте, публикации в форме "полиции месяца", постеры и объявления в местах общего пользования, таких как стены в офисах или у входных дверей.

Рекламные сообщения должны быть понятными и актуальными для пользователей. Например, сообщение о плановом выключении сервера будет восприниматься гораздо серьезнее, чем абстрактное уведомление о техническом обслуживании. Важно повторять важные уведомления, особенно если они касаются временных изменений или планового обслуживания, чтобы пользователи не пропустили нужную информацию.

Сообщения, которые приходят в нужный момент, будут наиболее эффективными. Например, если сервер будет отключен через месяц, регулярное напоминание о нем поможет пользователям подготовиться и минимизировать неудобства.

**13.2.4. Различные службы поддержки для предоставления обслуживания и решения проблем**

С ростом организации создание отдельных групп службы поддержки для разных типов заявок может быть полезным. Это разделение позволяет эффективно управлять разными задачами и помогает избежать перегрузки сотрудников. Например, можно выделить одну группу для заявок на новые услуги, другую — для решения проблем, которые могут возникать после активации услуги, и третью — для более сложных технических задач.

Преимущества такого разделения включают:

1. **Управление и отчетность**: Разделение сотрудников на несколько групп под руководством разных администраторов позволяет эффективно управлять и организовывать работу. Каждый администратор управляет группой с определенным фокусом, что снижает нагрузку и повышает эффективность.
2. **Специализация и обучение**: Сотрудники могут быть обучены для выполнения конкретных задач, что снижает затраты на обучение универсальных специалистов. Это выгодно, так как сотрудники с узкой специализацией будут более эффективны в своей работе.
3. **Процесс предоставления услуг**: Независимо от того, какой тип заявки поступает, процесс должен быть стандартизирован для всех пользователей. Для сбора данных и предоставления услуг можно обучить сотрудников задавать правильные вопросы, а также внедрить систему веб-заявок для упрощения процесса и исключения ошибок при вводе данных.

Кроме того, использование системы заявок на веб-портале помогает снизить количество ошибок, связанных с ручным вводом данных. Также такие системы могут автоматически отклонять непоследовательные запросы, что повышает точность и эффективность обработки заявок.

**13.3. Заключение**

Служба поддержки является лицом организации для пользователей, и ее репутация критически важна для имиджа компании. Как только организация достигает определенного размера, создание службы поддержки становится важным шагом, который затем может развиваться и делиться на более узкие направления по мере роста компании.

Для эффективного функционирования службы поддержки необходимо заранее определить, какие услуги поддерживаются, кто получает поддержку, когда и в течение какого времени пользователи могут ожидать решения своей заявки. Важно также собрать статистику, которая помогает планировать финансирование и набор персонала.

Разделение службы поддержки на разные группы для решения разных типов задач помогает улучшить качество обслуживания. Важную роль играет правильная настройка процессов для передачи проблем на более высокий уровень и использование программного обеспечения для отслеживания заявок и статистики.

В завершение, служба поддержки должна быть не только эффективной, но и ориентированной на клиента. Своевременная и понятная коммуникация с пользователями влияет на восприятие компании как дружелюбной или недружелюбной, а правильно выстроенные процессы и статистика помогают обеспечить высокий уровень обслуживания.

**Глава 14. Работа с пользователями**

После Второй мировой войны США столкнулись с избытком производственных мощностей, что привело к возникновению огромного выбора товаров. В ответ на этот выбор появилась жесткая конкуренция между компаниями, и они начали искать способы улучшить свои системы продаж. Исследования показали, что успешные продавцы использовали структурированный процесс, который можно было преподавать, что привело к формализации обучения продажам. Этот процесс стал основой для улучшения качества работы в других сферах, включая системное администрирование.

**14.1. Основы**

Системные администраторы часто сталкиваются с запросами пользователей, которые могут включать проблемы с сетью, печатью или программным обеспечением. Правильное и эффективное реагирование на эти запросы критично для репутации компании. В этой главе представлен структурированный процесс работы с запросами пользователей, состоящий из девяти этапов, разделенных на четыре фазы:

* **Фаза A: Приветствие**
  + **Этап 1**: Приветствие.
* **Фаза B: Определение проблемы**
  + **Этап 2**: Классификация проблемы.
  + **Этап 3**: Описание проблемы.
  + **Этап 4**: Проверка проблемы.
* **Фаза C: Планирование и выполнение**
  + **Этап 5**: Предложение решений.
  + **Этап 6**: Выбор решения.
  + **Этап 7**: Выполнение решения.
* **Фаза D: Проверка**
  + **Этап 8**: Проверка исполнителем.
  + **Этап 9**: Проверка пользователем.

Этот процесс помогает системным администраторам более эффективно решать проблемы, организуя работу и избегая ошибок. Он вводит общую терминологию, что способствует лучшему взаимопониманию внутри команды. Новый персонал может обучаться по этой модели, что делает их работу более структурированной и ориентированной на решение проблем.

Важно понимать, что этот метод не заменяет технический опыт, но служит полезным инструментом для организации работы и обучения. Понимание этого процесса пользователями также помогает им эффективно взаимодействовать с системными администраторами, предоставляя необходимую информацию и даже помогая в решении проблем.

**14.1.1. Фаза A/Этап 1: Приветствие**

Первая фаза состоит из этапа, который на первый взгляд кажется простым — это момент, когда пользователь сообщает о своей проблеме. На этом этапе важно создать положительное и дружелюбное первое впечатление. Встретить пользователя можно разными способами: через телефон, веб-форму, электронную почту или даже через автоматизированные средства, такие как автоответчики. Задача заключается в том, чтобы эффективно и удобно собрать необходимую информацию о запросе пользователя, при этом обеспечить доступность разных методов связи.

Встретить пользователя можно также с помощью табличек, наклеек на компьютерах, баннеров на веб-страницах и других средств. Важно, чтобы пользователь знал, куда обратиться в случае возникновения проблемы, и имел доступ к нужной информации.

**14.1.2.1. Этап 2: Классификация проблемы**

На этом этапе важно классифицировать запрос, чтобы определить, кто должен с ним работать. Это может быть автоматизированный процесс или процесс, выполняемый человеком. Классификация может зависеть от типа проблемы, например, проблемы с компьютером или сетью. В случае автоматизированного подхода запросы могут быть перенаправлены в нужную группу на основе определенных критериев, таких как адрес электронной почты или идентификационный номер.

Если классификация выполняется вручную, может потребоваться задать дополнительные вопросы для уточнения проблемы. Важно, чтобы пользователю сообщили о том, к какой категории отнесена его проблема. Это позволит избежать ошибок и улучшит взаимодействие. Если классификация была выполнена неправильно, то нужно вежливо исправить это и предложить правильный вариант, направив пользователя в нужный отдел.

На этом этапе также может происходить перенаправление запросов или их отклонение, если они не соответствуют политике компании. В крупных компаниях процесс классификации может включать взаимодействие с несколькими отделами или службами, особенно если проблема сложная, например, связана с сетями или серверами. В этом случае системный администратор может помочь пользователю сориентироваться в сложной структуре компании и перенаправить запрос в нужный отдел.

**14.1.2.2. Этап 3: Описание проблемы**

На этом этапе пользователь должен предоставить подробное описание своей проблемы, и эта информация записывается регистратором (человеком или системой). Навыки, которые необходимы на этом этапе, включают умение слушать и задавать правильные вопросы, чтобы собрать всю необходимую информацию. Важно выявить и зафиксировать все детали, которые могут помочь в воспроизведении и решении проблемы.

**Характеристики хорошего описания проблемы:**

1. **Полнота информации** — нужно указать все аппаратные и программные средства, связанные с проблемой, а также их местоположение, время работы и другие важные моменты.
2. **Конкретика** — описание должно быть четким, чтобы можно было легко воспроизвести ситуацию. Например, вместо «не могу печатать» лучше указать: «Компьютер talpc.example.com (с ОС Windows Vista) не может печатать документы MS-Word 2006 на принтере 'rainbow' в комнате 314».
3. **Избыток информации** — обычно лучше предоставить больше данных, чем их недостаток. Например, при сообщении о проблемах с маршрутизацией в сети лучше указать два IP-адреса, которые не могут соединиться между собой, но работают с другими узлами.
4. **Помощь в сборе информации** — пользователи часто не могут предоставить все необходимые данные. Поэтому сотрудник или система должны задавать уточняющие вопросы, например, о времени возникновения проблемы или конкретном устройстве.

**Примеры плохого и хорошего описания:**

* **Плохое описание:** «Помогите! Я не могу печатать». Это слишком общее и неполное описание.
* **Хорошее описание:** «Компьютер talpc.example.com, ОС Windows Vista, не может печатать на цветном принтере 'rainbow' в комнате 314. Вчера все работало нормально. На других принтерах печатать можно».

**Дополнительные советы:**

* **Позитивный подход** — важно общаться с пользователем так, чтобы он не чувствовал себя неудобно или виноватым. Например, вместо того чтобы спрашивать: «Вы проверили, включен ли принтер?» лучше сказать: «Пожалуйста, подтвердите, что принтер подключен к розетке и что кабель надежно закреплен с обеих сторон».
* **Гибкость в решении срочных проблем** — в случае срочных запросов (например, если нужно срочно распечатать отчет) можно предложить временное решение, например, использовать другой принтер, если основной не работает.
* **Передача информации** — в крупных организациях может быть несколько человек, которые записывают и обрабатывают запросы. В таких случаях важно иметь четкие схемы для сбора информации в зависимости от типа проблемы, чтобы обеспечить точность и скорость обработки запроса.
* **Использование системы отслеживания заявок** — программа отслеживания может автоматически записывать важную информацию в зависимости от категории проблемы (например, IP-адрес для сетевых проблем, имя принтера для печатных проблем).

Весь процесс должен быть организован так, чтобы избежать недоразумений и ошибок в описании проблемы, а также минимизировать время на решение задачи.

**14.1.2.3. Этап 4: Проверка проблемы**

На этом этапе системный администратор пытается воспроизвести проблему, чтобы лучше понять, что именно происходит. Проверка проблемы важна по нескольким причинам, в том числе для правильной диагностики и избегания работы над неверным направлением. В случае, если проблему невозможно воспроизвести, вероятно, она была неправильно описана, и необходимо вернуться к этапу 3.

**Важные аспекты:**

1. **Важность воспроизведения проблемы**: Ничто не дает лучшего понимания проблемы, чем наблюдение её в действии. Иногда описание проблемы пользователем может быть неточным, что может привести к поиску решения в неверном направлении. Это особенно важно при работе с удаленной помощью, где невозможно непосредственно увидеть проблему.
2. **Метод воспроизведения**: Процесс воспроизведения проблемы должен быть записан для дальнейшего использования, например, в тестовом скрипте. В системах с командной строкой, как UNIX, это проще реализовать, чем в графических интерфейсах, где такие действия сложнее автоматизировать.
3. **Широта проверки**: Проверка не должна быть слишком узкой или слишком широкой. Узкие тесты могут не покрыть всех аспектов проблемы, в то время как слишком широкие могут привести к потере времени на лишние проверки. Важно правильно сфокусироваться на ключевых элементах проблемы.
4. **Независимые проблемы**: В процессе воспроизведения может быть обнаружена другая, не связанная с текущей проблемой неисправность. Эти проблемы стоит фиксировать, даже если они не критичны, для последующего исправления.
5. **Прямая проверка**: Иногда для проверки проблемы не требуется полностью воспроизводить ситуацию. Например, если проблема с принтером, можно проверить очередь печати, чтобы убедиться, что новые задачи не добавляются. В других случаях нужно точно воспроизвести проблему, возможно, на устройстве пользователя.
6. **Проблемы локальные или глобальные**: Если проблему удалось воспроизвести на устройстве пользователя, может быть полезно проверить, проявляется ли она в других системах, чтобы понять, локальна ли проблема или затрагивает более широкую область. В случае сложных продуктов может быть полезно иметь лабораторию для тестирования и воспроизведения таких проблем.

**Заключение:**

Проверка проблемы — важный этап, который помогает не только точно понять её суть, но и минимизировать ошибки, связанные с недоразумениями в описаниях. Системные администраторы должны тщательно подходить к этому процессу, используя все доступные средства для точной диагностики.

**14.1.3.1. Этап 5: Предложение решений**

На этом этапе специалист по проблеме (Subject Matter Expert — SME) предлагает возможные решения для устранения проблемы. Количество решений зависит от типа проблемы — для некоторых решений может быть одно, а для других — несколько.

**Основные моменты:**

1. **Выбор решения**: Важно предложить «лучшее» решение, которое зависит от контекста и ситуации. Например, в финансовых учреждениях может быть достаточно быстрого решения (перезагрузки системы), в то время как в исследовательских системах потребуется более глубокий анализ проблемы.
2. **Стоимость решений**: Некоторые решения требуют больше затрат, например, при необходимости личного присутствия специалиста. Для удаленной поддержки существуют коммерческие и некоммерческие решения, которые могут существенно снизить затраты.
3. **Передача задачи другим специалистам**: Если системный администратор не знает вариантов решения проблемы, лучше передать задачу более опытным коллегам. Командная работа и обмен знаниями помогают быстрее найти правильное решение и минимизировать время, затраченное на исправление неполадок.

Этап предложения решений помогает сориентироваться в возможных вариантах исправления проблемы, ориентируясь на целесообразность и стоимость каждого из них.

**14.1.3.2. Этап 6: Выбор решения**

На этом этапе из множества возможных решений выбирается одно для первой попытки или для повторной попытки, если этапы проблемы проходят несколько раз. Этот выбор осуществляется специалистом в области проблемы (Subject Matter Expert – SME).

**Основные моменты:**

1. **Легкость выбора решения**: Выбор решения может быть либо простым, либо сложным. В некоторых случаях можно сразу выбрать наилучший вариант, в других — необходимо учитывать несколько факторов. Очень важно определить приоритет возможных решений, потому что одновременно несколько решений могут не быть реализуемы.
2. **Привлечение пользователя к выбору решения**: Пользователь должен участвовать в определении приоритетности решений, поскольку он лучше понимает свои временные ограничения. Например, продавец потребительских товаров, для которого потеря доступа к компьютеру в рабочее время критична, может предпочесть краткосрочное решение, такое как временная "заплатка". В исследовательской среде же можно сразу выбрать более долгосрочное решение, не беспокоясь о немедленном восстановлении работы.
3. **Участие опытных пользователей**: Важно привлекать более опытных пользователей, если они есть. Это может помочь им лучше понять процесс и даже позволить решать проблемы в будущем. Однако важно избегать излишней технической детали для неопытных пользователей, чтобы не вызвать у них панику или путаницу.
4. **Обучение и вовлеченность пользователей**: Вовлечение пользователей в этот процесс имеет долгосрочную выгоду, поскольку это может помочь обучить их работать с проблемами самостоятельно в будущем. Это также помогает снизить барьер между технической поддержкой и пользователями, создавая более тесную командную атмосферу и устраняя стереотипы о "противостоянии" между ними.

**14.1.3.3. Этап 7: Выполнение решения**

На этом этапе решение проблемы должно быть выполнено. Успех на этом этапе зависит от навыков и опыта того, кто выполняет решение.

**Основные моменты:**

1. **Исполнитель задачи**: Исполнитель — это системный администратор, оператор или работник, выполняющий необходимые действия для реализации решения. Это может быть как специалист, так и пользователь, особенно если система имеет ограниченные возможности для удаленного управления.
2. **Роль пользователя в реализации решения**: В некоторых случаях решение зависит от пользователя, особенно если он работает удаленно и имеет ограниченные возможности для вмешательства. В таком случае важно наладить диалог с пользователем, чтобы убедиться, что он правильно выполнил необходимые действия. Это требует внимательности, так как неопытные пользователи могут сделать ошибку, а опытные — не всегда точно описывают свои действия.
3. **Коммуникация с пользователем**: Важно наладить правильную коммуникацию в зависимости от уровня знаний пользователя. Для опытных пользователей стоит избегать излишне подробных инструкций, а для неопытных — не использовать сложную терминологию. Правильные вопросы, такие как «Какое сообщение появилось, когда вы это ввели?», помогут понять, где произошла ошибка, если она случилась.
4. **Диалог и обратная связь**: Важно не только выполнить решение, но и убедиться, что оно действительно работает, а пользователь доволен результатом. Это требует диалога и дополнительной проверки.
5. **Развитие навыков общения**: Умение эффективно общаться с пользователями и понимать их потребности — это навык, который можно развивать. Курсы по активному слушанию и межличностной коммуникации могут помочь развить этот навык и улучшить взаимодействие с пользователями.

Этап выполнения решения — это не только технический процесс, но и коммуникационный, где важно не только правильно выполнить задачи, но и убедиться, что результат удовлетворяет пользователя.

**14.1.4.1. Этап 8: Проверка исполнителем**

На этом этапе исполнитель, который работал на этапе 7, проверяет, были ли успешными принятые меры для устранения проблемы. Проверка имеет смысл только в случае, если процесс воспроизведения проблемы на этапе 4 был точно записан и воспроизведен. Если проблема все еще присутствует, следует вернуться к предыдущим этапам, возможно, даже к этапу 5 или раньше, чтобы найти более точное решение.

**Основные моменты:**

* **Проверка выполнения решения**: Это важный шаг, где исполнитель должен удостовериться, что проблема была решена правильно.
* **Точное воспроизведение проблемы**: Без точной записи или воспроизведения проблемы предыдущими шагами, проверка может быть неэффективной.
* **Возврат к предыдущим этапам**: Если проблема не решена, необходимо вернуться к предыдущим этапам для поиска корректных решений.

**14.1.4.2. Этап 9: Проверка пользователем/Закрытие**

На последнем этапе пользователь должен подтвердить, что проблема решена. Если пользователь не удовлетворен результатом, работа не считается завершенной.

**Основные моменты:**

* **Роль пользователя**: Пользователь играет ключевую роль на этом этапе, так как именно он определяет, решена ли проблема. Если пользователь не удовлетворен, задача не завершена.
* **Возврат к предыдущим этапам**: Если пользователь сообщает, что проблема не решена, может потребоваться вернуться к этапам воспроизведения, планирования или классификации проблемы.
* **Необходимость повторной проверки**: Пользовательская проверка может выявить недочеты или ошибки, связанные с неправильным объяснением проблемы или с неправильной интерпретацией решения. Это может привести к необходимости возврата к более ранним этапам, таким как классификация или описание проблемы.

**14.1.5. Риск пропуска этапов**

Пропуск любого этапа процесса может привести к неудаче всего решения. Недостаток опыта, ошибочная интерпретация или даже излишняя спешка могут стать причиной проблем.

**Типичные стереотипы о плохих системных администраторах:**

1. **Людоед**: Системные администраторы, которые агрессивно относятся к пользователям, не приветствуют их и сразу начинают раздражать.  
   *Предложение*: Установить стандарт общения и обучать дружелюбному взаимодействию с пользователями.
2. **Гонитель**: Системный администратор, который не передает запросы в нужный отдел и не помогает пользователю найти нужную информацию.  
   *Предложение*: Создание формального дерева решений, чтобы запросы передавались правильно.
3. **Самонадеянный**: Системный администратор, который быстро решает, что понял проблему, не проверив ее полноценно.  
   *Предложение*: Обучение активному слушанию и внимание к деталям.
4. **Безответственный**: Системный администратор, который пропускает проверку проблемы и решает не ту проблему.  
   *Предложение*: Научить системных администраторов воспроизводить проблему, прежде чем передавать ее на более высокий уровень.
5. **Мастер-ломастер**: Системный администратор, который слишком креативно подходит к решению проблемы, не соблюдая правильный процесс.  
   *Предложение*: Обучение использованию различных методов устранения неполадок и наставничество.
6. **Халтурщик**: Системный администратор, который приносит больше вреда, чем пользы, из-за небрежности.  
   *Предложение*: Обучение внимательности и тщательному выполнению команд.
7. **Залетная птица**: Системный администратор, который решает проблему, не проверив ее должным образом.  
   *Предложение*: Установить стандарты проверки работы, прежде чем заявлять, что проблема решена.
8. **Торопыга**: Системный администратор, который ориентирован на скорость закрытия заявок, а не на качество решения проблемы.  
   *Предложение*: Оценивать работу на основе качества решения, а не только времени, затраченного на проблему.

Пропуск этапов или выполнение работы поспешно может привести к негативным последствиям. Важно обучать системных администраторов каждому этапу процесса и соблюдать установленные стандарты, чтобы обеспечить качественную работу с пользователями.

**14.2. Тонкости**

После освоения базового процесса можно улучшить его с помощью ряда методов, улучшая как отдельные этапы, так и весь процесс в целом.

**14.2.1. Обучение, основанное на модели**

Для повышения эффективности работы системных администраторов важно, чтобы обучение основывалось на модели решения проблем. Важно, чтобы после базового обучения более опытный персонал наставлял менее опытных коллег, помогая им усвоить ключевые этапы процесса.

* **Проблемы из-за недостатка обучения**: Без должного обучения могут возникнуть проблемы, такие как неправильное распределение обязанностей или недостаточно полная информация на этапе записи. Это затруднит дальнейшие этапы и приведет к дополнительным обращениям к пользователю.
* **Решение**: Разработка письменных схем, которые четко объясняют, кто за что отвечает, а также стандартных списков данных для классификации, поможет избежать этих проблем.

**14.2.2. Целостное усовершенствование**

Важно не только улучшать отдельные этапы, но и обеспечивать плавный переход между ними. Это поможет создать более профессиональный и последовательный процесс.

* **Сложности передачи задач**: Каждая передача задачи между участниками процесса создает возможность для ошибок. Чем меньше таких передач, тем меньше вероятность ошибок. Особенно это важно в крупных организациях, где рост числа системных администраторов может создавать дополнительные сложности.
* **Решение**: Для повышения эффективности можно выбрать принцип одной точки контакта. Пользователь будет взаимодействовать с одним системным администратором, который будет полностью отвечать за его проблему.

**14.2.3. Более близкое знакомство с пользователями**

Если системный администратор общается с одним и тем же пользователем регулярно, он лучше понимает его потребности и может предоставлять более качественное обслуживание.

* **Как улучшить взаимодействие**: Можно создать подгруппы в отделе, которые будут прикреплены к определенным группам пользователей. Кроме того, системы телефонной поддержки могут направлять вызовы так, чтобы пользователь всегда общался с одним и тем же оператором, если тот свободен. Это помогает создать более персонализированное обслуживание и улучшает взаимодействие.

**14.2.4. Специальные объявления о серьезных отключениях**

Во время крупных отключений сети пользователи могут обращаться с многочисленными вопросами. Для оптимизации этого процесса можно использовать автоответчик.

* **Решение**: Автоответчик может быть настроен таким образом, чтобы перед перечислением опций он сообщал пользователю о текущем состоянии проблемы. Например: «Пожалуйста, имейте в виду, что сетевое соединение с Денвером в данный момент неисправно. Наш провайдер ожидает, что оно будет исправлено к 15 часам. Нажмите 1 для… нажмите 2 для…». Это поможет снизить нагрузку на операторов и информировать пользователей сразу о текущих проблемах.

Эти улучшения помогут создать более эффективный и организованный процесс работы с пользователями, снижая количество ошибок и повышая качество обслуживания.

**14.2.5. Анализ тенденций**

Каждый месяц полезно уделять немного времени для анализа тенденций в запросах пользователей и на основе этого предпринимать соответствующие действия. Это не обязательно должен быть сложный анализ, но он может значительно улучшить процесс работы.

**Важные тенденции для отслеживания:**

1. **Повторяющиеся проблемы**:
   * Если пользователи постоянно обращаются с одной и той же проблемой, нужно выяснить причины. Требуется ли дополнительное обучение для пользователя, или система действительно неисправна?
2. **Часто задаваемые вопросы**:
   * Если много пользователей задают вопросы на одну и ту же тему, возможно, система недостаточно интуитивно понятна. В таком случае стоит подумать об улучшении документации или о переделке интерфейса.
3. **Общие проблемы среди клиентов**:
   * Если несколько клиентов сообщают о похожей проблеме, возможно, стоит оповестить всех пользователей сразу. Это может также означать, что проблема требует более высокого приоритета.
4. **Самообслуживание**:
   * Определенные запросы можно перевести на уровень самообслуживания. Например, если пользователи часто обращаются из-за необходимости привилегированного доступа, можно предоставить им инструменты для решения задач самостоятельно. В UNIX-системах есть возможности, такие как SUID и sudo, которые позволяют безопасно предоставить пользователю ограниченные привилегии для выполнения задач.
5. **Анализ группы пользователей**:
   * Подсчитайте, какие пользователи чаще всего обращаются за помощью. Может быть, определенная группа или отдел генерирует больше запросов, чем другие, и это стоит учитывать для более эффективного распределения ресурсов.
6. **Запросы, требующие много времени**:
   * Некоторые запросы могут требовать значительных временных затрат (например, восстановление удаленных файлов). Если такие запросы часто повторяются, можно инвестировать время в обучение пользователей методам предотвращения таких ситуаций или в приобретение системы для автоматического восстановления.
7. **Метрики производительности**:
   * Важно отслеживать метрики, такие как время, которое тратится на решение проблем. Если время выполнения запросов увеличивается, это может означать либо рост сложности проблем, либо менее эффективную работу администраторов.

**14.2.6. Пользователи, знающие процесс**

Образованные пользователи, которые понимают процесс решения проблем, могут значительно улучшить взаимодействие с системными администраторами.

* **Преимущества подготовленных пользователей**:
  + Они могут предоставить более точную и полную информацию о проблеме, что ускорит её решение. Понимание важности точности информации при обращении в службу поддержки позволяет быстрее сужать проблему до конкретной машины или ситуации.
* **Дополнительное обучение**:
  + Пользователи, которые знакомы с этапами процесса, могут даже решать некоторые проблемы самостоятельно. Это может значительно снизить нагрузку на системных администраторов.
* **Обучение и упрощение процесса**:
  + Обучение пользователей процессу из девяти этапов поможет улучшить взаимодействие между ними и администраторами. С помощью такого обучения пользователи будут более осведомлены о том, как и когда обращаться за помощью, что повысит эффективность и уменьшит количество запросов.

Эти шаги помогут не только оптимизировать процессы, но и улучшить взаимодействие с пользователями, повысив удовлетворенность и снижая нагрузку на специалистов.

**14.2.7. Архитектурные решения, соответствующие процессу**

Архитектура системы может как способствовать, так и препятствовать эффективному процессу классификации и обработки запросов. Сложность системы увеличивает трудности в воспроизведении и идентификации проблем. Например, в большой UNIX-сети, проблема с печатью может быть связана с множеством факторов, таких как DNS, программное обеспечение сервера или клиента, настройки системы пользователя, сеть и даже сам принтер. Чтобы диагностировать такие проблемы, администраторы должны быть экспертами в различных областях, или система должна предусматривать перекрестный контроль на разных уровнях.

При проектировании системы важно учитывать, как она будет обслуживаться в будущем. Принцип «проектирования для обслуживания» должен быть в центре внимания, чтобы гарантировать, что решение проблем будет максимально простым и эффективным.

**14.3. Заключение**

Эта глава посвящена общению и созданию структурированного процесса для обработки запросов пользователей. Процесс разделен на четыре фазы: приветствие, идентификация, планирование и выполнение, а также исправление и проверка. Каждый этап имеет свои подэтапы, которые обеспечивают четкую организацию работы и подготовку к следующему этапу.

Применение этой модели помогает системным администраторам более эффективно и формализованно подходить к решению проблем. Включение модели в обучение администраторов и объяснение её пользователям позволяет создать четкие и понятные процедуры для взаимодействия. Модель также помогает анализировать тенденции в запросах и предоставляет возможность для улучшения качества обслуживания.

Автоматизация процессов отслеживания запросов с помощью специализированных программ значительно снижает трудозатраты и помогает избежать ошибок, связанных с ручной обработкой информации. Такие программы экономят время, улучшая организацию работы.

В целом, модель служит хорошей основой для организации службы поддержки, но не заменяет творческий подход, опыт и нужные ресурсы. Несмотря на то что знание модели улучшает эффективность работы, она должна быть частью общей стратегии и не является универсальным решением для всех ситуаций. Хорошо организованная служба поддержки всегда будет включать и другие важные элементы, такие как обучение, поддержка и внимание к потребностям пользователей.