**Оглавление**

[1 блок вопросов 2](#_Toc132480753)

[1. Определение администрирования, администрирования ИС. Функции администратора ИС. 2](#_Toc132480754)

[2. Основные категории пользователей ИС (различные категории). Административный персонал ИС. Стандартный пакет нормативных документов администратора ИС. 2](#_Toc132480755)

[3. Системное администрирование. Сетевое администрирование 3](#_Toc132480756)

[4. Задачи администрирования ИС. Основные проблемы, с которыми сталкивается администратор сети. 3](#_Toc132480757)

[5. Идентификация. Аутентификация. Авторизация. Пример процесса идентификации, аутентификации и авторизации. 4](#_Toc132480758)

[6. Технологии идентификации. 5](#_Toc132480759)

[7.Технологии аутентификации. Протоколы аутентификации. Использование цифрового сертификата, смарт-карт, usb-ключей. 6](#_Toc132480760)

[8. Организация администрирования ИС. Управление проектами в ИС. 8](#_Toc132480761)

[9. Аудит ИС. Тестирование ИС. 10](#_Toc132480762)

[10. Эксплуатация и сопровождение ИС. Управление рисками и инцидентами. Оценка рисков. 12](#_Toc132480763)

[11. Управление безопасностью. Виды функциональной безопасности ИС. Проверка полномочий, проверка подлинности. Фундаментальные принципы обеспечения безопасности. 14](#_Toc132480764)

[12. Многоуровневая безопасность. Классы и уровни допуска или доступа к информации. Методы обеспечения сохранности информации. 15](#_Toc132480765)

[13. Резервное копирование и восстановление данных. Виды резервного копирования. 16](#_Toc132480766)

[14. Безопасность ИС. Основные аспекты информационной безопасности. Виды и группы угроз ИБ, классы отказов. 17](#_Toc132480767)

[15. Непреднамеренные и преднамеренные действия пользователей, предоставляющие угрозу безопасности ИС. Модель нарушителя ИБ. Типы нарушителей, классификация. Мотивы нарушений. 18](#_Toc132480768)

[16. Системы защиты ИС. Основные методы защиты информации. Средства обеспечения ИБ. Модели администрирования сети и способы обеспечения безопасности (централизованное, распределенное, администрирование по ОС, смешанная модель). 19](#_Toc132480769)

[17. Концепция управления ИТ-службами ITSM (идея, ключевые элементы, идеология). Преимущества внедрения концепции ITSM. 22](#_Toc132480770)

[18. Библиотека ITIL, история создания, идея, определение, составляющие или дисциплины ITIL. 22](#_Toc132480771)

[19. Что понимается под открытыми системами. Свойства открытых систем. Структура среды ИС. Эталонная модель открытых систем. Протокол. Интерфейс. Инкапсуляция. Основные элементы модели взаимодействия открытых систем. 24](#_Toc132480772)

[20. Средства анализа и управления сетями. Стандарт Telecommunication Management Network. 26](#_Toc132480773)

[21. Архитектуры систем управления сетями. Схема менеджер – агент. Структуры распределенных систем управления. Одноранговая и иерархическая модели управления сетями. 28](#_Toc132480774)

[22. Общие требования при выборе аппаратной платформы и конфигурации ИС. Причины сложности оценки конфигурации системы (аппаратных и программных средств). 30](#_Toc132480775)

[23. Инсталляция информационной системы. Основные этапы. Домен. Имена доменов. Отношения доменов. Модели доменов. 31](#_Toc132480776)

[2 блок вопросов 34](#_Toc132480777)

[1 Решения для индивидуальной и коллективной работы пользователей корпоративных информационных систем. Назначение решений: интегрированные средства коммуникаций, рабочие области коллективной деятельности, мгновенный доступ к информации и людям, автоматизация бизнес-процессов. 34](#_Toc132480778)

[2 Основные элементы ИТ-инфраструктуры, позволяющие реализовать эффективную поддержку коллективной работы. Решения Microsoft Windows. 35](#_Toc132480779)

[3 Платформы для построения корпоративных порталов. Расписать (Microsoft, IBM, Oracle). 37](#_Toc132480780)

[4 Определение БД. Определение СУБД. Расписать два уровня администрирования в СУБД. Функции администратора СУБД. 39](#_Toc132480781)

[5 Какие группы пользователей СУБД выделяют? Дискреционное управление доступом. Средства дискреционной защиты в СУБД. Мандатное управление доступом. Средства мандатной защиты в СУБД. 40](#_Toc132480782)

[6 Определение транзакции. Суть механизма транзакций? Основные уровни восстановления БД. 41](#_Toc132480783)

[7 Языковые средства разграничения доступа. Основные команды языка SQL. Концепция и реализация механизма ролей БД. 41](#_Toc132480784)

[8 Преимущества СУБД InterBase. Назначение утилиты gbak, gfix, gsec в InterBase. 43](#_Toc132480785)

[9 Преимущества создания резервных копий БД встроенными средствами СУБД. Теневые копии (shadow) БД. Основные рекомендации по ремонту БД. 44](#_Toc132480786)

[10 Определение каталога и службы каталогов. Назначение и функции служб каталога. Основные службы каталогов и стандарты, используемые в современных сетях. 45](#_Toc132480787)

[11 Ключевые преимущества Active Directory. Область действия, пространство имен ActiveDirectory. Объект. Контейнер. Дерево. 47](#_Toc132480788)

[12 Домен. Доменное дерево. Лес. Организационные единицы. Сайт, узел. 48](#_Toc132480789)

[13 Функциональная структура Active Directory. Физическая структура Active Directory. Логическая структура Active Directory. 49](#_Toc132480790)

[14 Какие сведения собираются на этапе предпроектного исследования для проектирования службы каталогов. Типовой план проектирования структуры ActiveDirectory. Какие объекты содержит БД ActiveDirectory. 50](#_Toc132480791)

[15 Доверительные отношения между доменами. Типы доверительных отношений. Контроллеры доменов, функции контроллера домена, их роли. 52](#_Toc132480792)

[16 Брандмауэры. Определение, общая информация, схема работы, Demilitarized Zone. 55](#_Toc132480793)

[17 Методы виртуализации операционных системы. Характеристика метода, примеры фирм и программ. 56](#_Toc132480794)

[18 Модель управления для администрирования сетевых систем FCAPS. 59](#_Toc132480795)

[19 Системы управления MS (Management System), NMS (Network Management System). Схема работы NMS. 60](#_Toc132480796)

[20 Базовая модель поиска ошибок при администрировании ИС. 60](#_Toc132480797)

[21 Стратегии определения ошибок при администрировании ИС. Два подхода к поиску неисправностей. Типы стратегий. Технологии работы NMS. 62](#_Toc132480798)

[3 блок вопросов 63](#_Toc132480799)

[1. Системы HelpDesk. Системы ServiceDesk. 63](#_Toc132480800)

[2. Протоколы POP3, IMAP, SMTP. Методы шифрования SSL, TLS. Форматы почтовых сообщений. 64](#_Toc132480801)

[3. Реестр Windows. Планировщик заданий. Настройка сети в Windows. Службы ОС в Windows. 65](#_Toc132480802)

[4. Язык сценариев Power Shell. Командлеты в PowerShell. Примеры. Конвейер в PowerShell. Примеры. 66](#_Toc132480803)

[5. Системы удаленного доступа к компьютеру и управлению программным обеспечением. 67](#_Toc132480804)

[6. Системы конфигурирования ИС. Сиcтема управления версиями GIT (цели использования git, принцип работы, репозиторий, типы репозиториев). 67](#_Toc132480805)

[7. Управление пакетами (dpkg, apt-get, Aptitude). 68](#_Toc132480806)

[8. Интерфейсы Ethernet (выполнить определение Ethernet интерфейсов в ОС, логическое имя, настройка интерфейса). 68](#_Toc132480807)

[9. Адресация IP (временное назначение IP адреса, динамическое присвоение и статическое присвоение IP адреса, интерфейс Loopback – обратная петля). 68](#_Toc132480808)

[10. TCP/IP (IP адрес, сетевая маска, адрес сети, адрес рассылки, адрес шлюза, адрес сервера имен). TCP. UDP.ICMP 69](#_Toc132480809)

[11. Протокол динамического выделения адресов (DHCP). NTP протокол. 70](#_Toc132480810)

[12. Удаленное администрирование (OpenSSH, Puppet, Zentyal). 70](#_Toc132480811)

[13. Авторизация по сети на примере ОС Ubuntu Server (OpenLDAP, Samba и LDAP, Kerberos, Kerberos и LDAP, назначение, алгоритм работы). 71](#_Toc132480812)

[14. Администрирование баз данных в UbuntuServer (MySQL, PostgreSQL). 72](#_Toc132480813)

1 блок вопросов

1. Определение администрирования, администрирования ИС. Функции администратора ИС.

Администрирование – процедуры управления, регламентирующие некоторые процессы или их часть

Администрирование ИС заключается в предоставлении пользователям соответствующих прав использования возможностей работы с системой; обеспечение целостности данных, а также создании многопользовательских приложений.

Функциональные области управления, относящиеся к системному администрированию, определены в спецификациях ISO, и ориентированы на:

1. решение проблемных ситуаций (диагностика, локализация и устранение неисправностей, регистрация ошибок, тестирование);
2. управление ресурсами (учёт, контроль использования ресурсов, выставление счетов за использованные ресурсы и ограничение доступа к ним);
3. управление конфигурацией, направленное на обеспечение надёжного и эффективного функционирования всех компонентов информационной системы;
4. контроль производительности (сбор и анализ информации о работе отдельных ресурсов, прогнозирование степени удовлетворения потребностей пользователей/приложений, меры по увеличению производительности);
5. защита данных (управление доступом пользователей к ресурсам, обеспечение целостности данных и управление их шифрованием).

2. Основные категории пользователей ИС (различные категории). Административный персонал ИС. Стандартный пакет нормативных документов администратора ИС.

Три основные категории пользователей: пользователи, разработчики, админыВыделяют пять категорий административного персонала, обеспечивающего эксплуатацию информационной системы.

1. Администратор 1. В его функции входит: оптимизация настроек; мониторинг производительности; модернизация, техническое обслуживание и профилактика ИС, а также организация резервного копирования данных ИС.
2. Администратор 2. Его деятельность нацелена на регистрацию новых пользователей и отслеживание изменения статуса всех пользователей (ведение и хранение учетных карт) ИС; консультацию пользователей; смену и восстановление паролей, а также решение других проблем, связанных с ИС.
3. Администратор 3 осуществляет: организацию размещения данных; назначение и изменение прав доступа; планирование резервного копирования и хранение резервных копий, а также (совместно с администратором 1) восстановление данных.
4. Администратор безопасности системы выполняет следующие задачи: участвует в разработке матрицы доступа к ресурсам; контролирует соблюдение политики безопасности ИС при её эксплуатации; отслеживает информацию об уязвимостях системы и своевременно принимает соответствующие меры; периодически тестирует ИС на предмет выявления её защищенности.
5. Аудитор проводит настройку подсистемы регистрации; организует архивирование и хранение журналов регистрации, осуществляет анализ журналов регистрации ИС.

Документация

1) положение о локальной сети ПК

2) Инструкция адмистратору сервера

3) Инструкция админу БД

4) Инструкция пользователю

5) Инструкция админу ИБ

6) Инструкция аудитору

7) Инструкция оформления доступа к серурсам

8) Инструкция по бекапу

9) Инструкция по антивирусам

10) Инструкция о паротной защите

3. Системное администрирование. Сетевое администрирование

Системное администрирование

Основной целью системного администрирования является приведение сети в соответствие с целями и задачами, для которых она предназначена. Достигается эта цель путём управления сетью, позволяющего минимизировать затраты времени и ресурсов, направляемых на управление системой, и в тоже время максимизировать доступность, производительность и продуктивность системы.

Сетевое администрирование

Сетевое администрирование (NetworkManagement) возникает, когда у администратора сети появляется потребность и возможность оперировать единым представлением сети, как правило, это относится к сетям со сложной архитектурой. При этом осуществляется переход от управления функционированием отдельных устройств к анализу трафика в отдельных участках сети, управлению её логической конфигурацией и конкретными рабочими параметрами, причём все эти операции целесообразно выполнять с одной управляющей консоли. Задачи, решаемые в данной области, разбиваются на две группы:

Контроль над работой сетевого оборудования;

Управление функционированием сети в целом.

4. Задачи администрирования ИС. Основные проблемы, с которыми сталкивается администратор сети.

Администрирование ИС осуществляется лицом, управляющим этой системой. Такое лицо называется администратором.

Если ИС большая, эти обязанности могут выполнять несколько человек (группа администраторов).

Администратор ИС осуществляет её запуск и останов. Он может использовать табличные пространства для:

1. управления распределением памяти для объектов ИС;
2. установления квот памяти для пользователей ИС;
3. управления доступностью данных, включая режимы (состояния) online или offline;
4. копирования и восстановления данных;
5. распределения данных по устройствам для повышения производительности.

В процессе своей деятельности администратор ИС взаимодействует с другими категориями её пользователей, а также и с внешними специалистами, не являющимися пользователями ИС

5. Идентификация. Аутентификация. Авторизация. Пример процесса идентификации, аутентификации и авторизации.

Идентификация – процедура распознавания субъекта по его уникальному идентификатору, присвоенному данному субъекту ранее и занесенному в базу данных в момент регистрации субъекта в качестве легального пользователя системы.

Аутентификация – процедура проверки подлинности входящего в систему объекта, предъявившего свой идентификатор. В зависимости от степени доверительных отношений, структуры, особенностей сети и удаленностью объекта проверка может быть односторонней или взаимной.

В большинстве случаев она состоит в процедуре обмена между входящим в систему объектом и ресурсом, отвечающим за принятие решения ("да" или «нет»). Данная проверка, как правило, производится с применением криптографических преобразований, которые нужны, с одной стороны, для того, чтобы достоверно убедиться в том, что субъект является тем, за кого себя выдает, с другой стороны - для защиты трафика обмена субъект система от злоумышленника. Таким образом, идентификация и аутентификация являются взаимосвязанными процессами распознавания и проверки подлинности пользователей.

Авторизация - процедура предоставления субъекту определенных прав доступа к ресурсам системы после успешного прохождения им процедуры аутентификации. Для каждого субъекта в системе определяется набор прав, которые он может использовать при обращении к её ресурсам.

Идентификация — мы указываем свой логин для входа, при этом будет осуществлена проверка, существует ли такой пользователь. Если пользователь существует, то его необходимо аутентифицировать

Аутентификация — мы указываем свой пароль, если пароль верный, то пользователь аутентифицирован и мы получаем возможность входа в систему. Если влезать более глубоко, то после проверки пароля, так же происходит механизм авторизации, имеет ли право аутентифицированный пользователь входить в систему. Например, на контроллере домена Windows Active Directory, Вы, по умолчанию, не сможете войти в систему локально, если пользователь не входит в группу Доменные Администраторы. То есть в данном примере пользователь будет идентифицирован и аутентифицирован (введены верные имя пользователя и пароль), но не будет авторизован (нет прав для локального входа на контроллер домена).

Авторизация — мы пытаемся открыть файл, если нам даны права на только чтение файла, то мы его сможем открыть и прочитать. Но записать какие-либо изменения в файл мы не сможем, так как мы не авторизированы на запись в файл

6. Технологии идентификации.

Технологии идентификации

В последнее десятилетие интенсивно развивается направление электронной цифровой идентификации, в которой сбор информации происходит с минимальным участием человека. Технологии автоматической идентификации наиболее полно соответствуют требованиям компьютерных систем и систем управления, где нужно четко распознавать объекты в реальном масштабе времени.

**Штрих - кодовая идентификация**

Штрих-коды в основном используются производителями товаров для автоматизации товародвижения. В настоящее время штриховые коды EAN/UPC лежат в основе всемирной многоотраслевой коммуникационной системы, развитие которой обеспечивается двумя крупнейшими специализированными международными организациями -EAN International и AIM International. Наиболее широко распространен тринадцатиразрядный код EAN-13, разработанный в 1976г. для удовлетворения требований пищевой промышленности на базе кода UPC (Universal Product Code), введенного в США еще в 1973г.

**Радиочастотная идентификация**

В средствах радиочастотной идентификации (RFID - Radio Frequency Identification Device) разработчики постарались развить все достоинства штрих-кодовой идентификации и преодолеть практически все недостатки и ограничения. В настоящее время данная технология интенсивно внедряется во многие отрасли мирового хозяйства. RFID позволяет получать информацию о предмете без прямого контакта. Дистанции, на которых может происходить считывание и запись информации, могут варьироваться от нескольких миллиметров до нескольких метров в зависимости от используемых технологий (главным образом, от несущей частоты, находящейся в пределах от 125 кГц до 5,8 ГГц). Большинство применяемых для идентификации сотрудников корпораций смарт-карт с применением компонент производства Ангстрем, HID, Atmel, Mifare, EM Microelectronic Marin, Microchip и др. чаще всего используют несущие частоты 125 кГц или 13,56МГц.

**Биометрическая идентификация**

Данная технология основана на применении статистического анализа биологических наблюдений и явлений. Биометрическая характеристика - это измеримая физиологическая или поведенческая черта человека.

Биометрические характеристики можно разделить на две группы:

* Физиологические биометрические характеристики (называемые физическими или статическими) - характеристики, основанные на данных, полученных путём измерения анатомических данных человека(отпечатки пальцев, форма лица, кисти, структура сетчатки глаза и др.).
* Поведенческие биометрические характеристики (также называемые динамическими биометрическими характеристиками) - биометрические характеристики, основанные на данных, полученных путём измерения действий человека. Характерной чертой для поведенческих характеристик является их протяжённость во времени (типичные примеры - голос, подпись).

**Идентификации на основе карт с магнитной полосой**

Карты с магнитной полосой уже более двух десятилетий используются в системах контроля физического доступа. Магнитные карты срабатывают при проведении в определенном направлении и с определенной скоростью по щели считывателя. Повременные магнитные полосы изготовлены из материалов, требующих сильных магнитных полей для записи и уничтожения информации, с целью сохранности информации от случайного размагничивания.

7.Технологии аутентификации. Протоколы аутентификации. Использование цифрового сертификата, смарт-карт, usb-ключей.

Для того, чтобы понять, что такое AAA и, в частности, аутентификация, обратимся к простому примеру: Ваш сотовый телефон. Телефон -это устройство, куда для начала работы Вы вкладываете SIM-карту. Когда Вы включаете телефон, на дисплее появляется надпись: "введите PIN-код". После правильного ввода PIN-кода (как правило, это 4 легко запоминаемые цифры) телефон начинает работать.

Налицо так называемая двухфакторная аутентификация. Вам надо иметь персональный носитель (SIM-карту) и знать личный PIN-код. Они связаны между собой. Причем эта связь закладывается администратором оператора сотовой связи при предпродажной подготовке контрактов с определенным тарифом и самих SIM-карт. Сам телефонный аппарат по аналогии с корпоративными информационными системами играет роль компьютера. Аналогом SIM-карты может являться микропроцессорная смарт-карта или устройство eToken, к которому привязан личный PIN-код. Только в отличие от сотового телефона PIN-код для доступа к информационной системе предприятия содержит, как правило, не менее 5-7 символов различных регистров (не только цифр). Да и алгоритмы аутентификации и шифрования там намного сложнее, чем используемые в сотовой связи A3 (алгоритм аутентификации), А8 (алгоритм генерации криптоключа), А5/2 (алгоритм шифрования оцифрованной речи для обеспечения конфиденциальности переговоров).

Рассмотрим основные методы аутентификации по принципу нарастающей сложности. Начнем с самого простого и общеизвестного метода - аутентификация по паролю. Поскольку данная технология, как правило, используется без изменения параметров в течение длительного времени (неделя, месяц, год - в зависимости от политик безопасности предприятия), то она получила название "аутентификация по многоразовым паролям".

**Протоколы аутентификации удаленных пользователей.**

Часть протоколов сетевой аутентификации были разработаны специально для обеспечения удаленного доступа к информационным ресурсам посредством открытых каналов связи (к примеру, телефонные линии, Internet).

Такими протоколами являются:

PAP (Password Authentication Protocol);

CHAP (Challenge Handshake Authentication Protocol);

EAP (Extensible Authentication Protocol);

RADIUS (Remote Authentication Dial-in User Service);

TACACS (Terminal Access Controller Access Control System).

**Аутентификация по предъявлению цифрового сертификата**

Механизмы аутентификации с применением сертификатов обычно используют протокол с запросом и ответом. Согласно этому протоколу, сервер аутентификации направляет пользователю последовательность символов, называемую запросом, а программное обеспечение клиентского компьютера для генерирования ответа вырабатывает с помощью закрытого ключа пользователя цифровую подпись под запросом от сервера аутентификации. Общий процесс подтверждения подлинности пользователя состоит из следующих стадий:

1. получение открытого ключа СА (одноразовый процесс),
2. получение по некоторому незащищенному каналу от этого пользователя его сертификата открытого ключа.

Аутентификация с открытым ключом используется как защищенный механизм аутентификации в таких протоколах как SSL, а также может использоваться как один из методов аутентификации в рамках рассмотренных протоколов Kerberos и RADIUS.

**Использование смарт-карт и usb-ключей**

Несмотря на то, что криптография с открытым ключом согласно спецификации Х.509 может обеспечивать строгую аутентификацию пользователя, сам по себе незащищенный закрытый ключ подобен паспорту без фотографии. Закрытый ключ, хранящийся на жёстком диске компьютера владельца, уязвим по отношению к прямым и сетевым атакам. Достаточно подготовленный злоумышленник может похитить персональный ключ пользователя и с помощью этого ключа представляться этим пользователем. Защита ключа с помощью пароля помогает, но недостаточно эффективно -пароли уязвимы по отношению ко мно¬гим атакам. Несомненно, требуется более безопасное хранилище.

**Смарт-карты**

Смарт-карты - пластиковые карты стандартного размера банковской карты, имеющие встроенную микросхему. Они находят всё более широкое применение в различных областях, от систем накопительных скидок до кредитных и дебетовых карт, студенческих билетов и телефонов стандарта GSM.

Для использования смарт-карт в компьютерных системах необходимо устройство чтения смарт-карт. Несмотря на название - устройство чтения (или считыватель), - большинство подобных оконечных устройств, или устройств сопряжения (IFD), способны как считывать, так и записывать информацию, если позволяют возможности смарт-карты и права доступа. Устройства чтения смарт-карт могут подключаться к компьютеру посредством последовательного порта, слота PCMCIA или USB. Устройство чтения смарт-карт также может быть встроено в клавиатуру. Как правило, для доступа к защищенной информации, хранящейся в памяти смарт-карты, требуется пароль, называемый PIN-кодом.

**USB-ключи**

USB-ключи достаточно привлекательны, поскольку USB стал стандартным портом для подключения периферийных устройств и организации не нужно приобретать для пользователей какие бы то ни было считыватели.

Аутентификацию на основе смарт-карт и USB-ключей сложнее всего обойти, так как используется уникальный физический объект, которым должен обладать человек, чтобы войти в систему. В отличие от паролей, владелец быстро узнаёт о краже и может сразу принять необходимые меры для предотвращения её негативных последствий. Кроме того, реализуется двухфакторная аутентификация. Микропроцессорные смарт-карты и USB-ключи могут повысить надёжность служб PKI: смарт-карта может использоваться для безопасного хранения закрытых ключей пользователя, а также для безопасного выполнения криптографических преобразований. Безусловно, данные устройства аутентификации не обеспечивают абсолютную безопасность, но надёжность их защиты намного превосходит возможности обычного настольного компьютера.

8. Организация администрирования ИС. Управление проектами в ИС.

**ОРГАНИЗАЦИЯ АДМИНИСТРИРОВАНИЯ ИС**

Администрирование связано также с планированием размещения оборудования (компьютеров) и созданием необходимого микроклимата в помещениях с компьютерами, особенно в серверной. В серверных рекомендуется создавать специальную централизованную систему кондиционирования воздуха, располагая разнесённые сервера в одном месте, так как каждое превышение температуры на 8оС выше стандартных 21оС на 50% уменьшает надёжность работы компьютеров. Отсутствие надлежащей организации микроклимата и размещения оборудования в таких помещениях приводит к тому, что более 70% охлаждающего воздуха не доходит до оборудования, а больше половины его улетучивается через щели в кабелепроводах и каналах, а 14% расходуется впустую из-за неверной ориентации створок для направления воздуха в нужном направлении. При этом охлаждённый воздух может уходить под фальшпол, в подвесной потолок, через вентиляционные щели на термостат кондиционера, приводя к снижению уровня охлаждения и др. Они утверждают, что техническое обслуживание и сопровождение шести маленьких серверов электронной почты на территории трёх штатов, обходится гораздо дороже, чем поддержка одного-двух крупных серверов в стойке рядом с сетевым администратором, поскольку повернуться на стуле несравненно проще и быстрее, чем отправляться для устранения локальной проблемы даже в соседнее здание, а уж тем более в другой штат. Так как ИС является динамическим информационным отображением предметной области, то желательно, чтобы администратор своевременно получал информацию о перспективах развития объекта, для которого создаётся информационная система. Руководство организации и администратор согласовывают цели и направления, сроки создания ИС и её развития, очередность подключения пользователей

**УПРАВЛЕНИЕ ПРОЕКТАМИ В ИС**

Основной функцией управления проектами является планирование выполнения необходимых для

реализации управления работ (создание рабочего и иных планов работ).

Рабочий план должен соответствовать общим требованиям, согласно которым в нем должны

присутствовать следующие компоненты:

● указание цели;

● определение требуемых задач;

● распределение обязанностей;

● указание сроков, а также:

● требуемые ресурсы;

● источники материально-технической поддержки;

● бюджетные ассигнования;

● определение количественного аспекта;

● сочетание с другими компонентами;

● промежуточная отчётность и др.

Планирование любых, в том числе связанных с ИС, работ предполагает выполнение определённых реальных стадий и этапов с чётко обозначенными началом и окончанием. Так, например, управление проектом создания ИС связано с вопросами: планирования и организации работ; создания коллективов разработчиков; контроля за сроками и качеством выполняемых работ.

Обычно выделяют восемь этапов процесса планирования.

Этап 1. Целеполагание (формулировка целей). Он нацелен на выявление результатов, которые хотелось бы получить (достичь)? Это – самый трудный и не формализуемый этап.

Этап 2. Подбор способов достижения поставленных целей, их анализ и оценка. Обычно существует несколько способов достижения цели. Важно не только их выявить, но и определить наилучший из них.

Этап 3. Составление перечня необходимых действий. Определение конкретных действий, необходимых для осуществления (реализации) выбранного на предыдущем этапе варианта достижения поставленных целей.

Этап 4. Составление программы работ (плана мероприятий). На этом этапе устанавливают порядок выполнения намеченных на предыдущем этапе действий с учётом того обстоятельства, что многие из них связаны между собой.

Этап 5. Анализ ресурсов. В процессе его выполнения определяют необходимые для реализации плана выполнения намеченных работ интервалы времени, материальные (в том числе программно-технические), финансовые, информационные и кадровые ресурсы.

Этап 6. Анализ разработанного варианта плана. Здесь следует установить: решает ли разработанный план цели, поставленные на первом этапе; являются ли приемлемыми затраты ресурсов; есть ли соображения по улучшению плана, возникшие в ходе его разработки при движении от второго к пятому этапам. В результате проведения этой работы может оказаться целесообразным вернуться к этапам 2, 3, и даже к первому этапу.

Этап 7. Подготовка детального плана действий. На этом этапе необходимо детализировать разработанный на предыдущих этапах план, выбрать согласованные сроки выполнения отдельных видов работ, рассчитать необходимые ресурсы, установить ответственных за отдельные участки работы.

Этап 8. Контроль выполнения плана, внесение необходимых изменений (в случае необходимости)

9. Аудит ИС. Тестирование ИС.

Информационный аудит – это проверка и оценка практики использования ИТ-систем в организации, осуществляемая специализированной независимой организацией.

Выделяют две причины необходимости проведения такого аудита.

Первая причина – информационным технологиям большинства Российских компаний свойственен эволюционный путь создания и дальнейшего их развития. Он характеризуется тем, что информационные системы включаются в инфраструктуру ИТ или модернизируются по мере возникновения необходимости и (или) по мере возможности (в том числе и финансовой). В итоге в ИТ-инфраструктуре формируется сложная (порой разнородная) и поэтому плохо управляемая совокупность программно-технических и системных платформ. Даже если ИС прошла все стадии создания, последующие изменения бизнес-процессов или введение новых приложений могут привести к тому, что параметры её программно-аппаратных платформ перестанут соответствовать требованиям бизнеса.

Вторая причина связана с зависимостью успешности бизнеса от способности управленцев вовремя получать и быстро обрабатывать нужную информацию. Очевидно, что современный руководитель любого звена не в состоянии одновременно быть компетентным в различных областях, обеспечивать получение и обработку разноплановой информации.

**Под тестированием понимается процесс исполнения программы с целью обнаружения** ошибок.

Регрессионное тестирование – это тестирование, проводимое после усовершенствования функций программы или внесения в неё изменений. Одно из средств тестирования QA (ныне – Quality Works) представляет интегрированную, многоплатформенную среду разработки автоматизированных тестов любого уровня, включая тесты регрессии для приложений с графическим интерфейсом пользователя.

Критерии тестирования включают:

• описание тестов;

• фиксацию повторения действий оператора (возможность фиксировать данные, вводимые оператором с помощью клавиатуры, мыши и т.д., редактировать их и воспроизводить в тестовых примерах);

• автоматический запуск тестовых примеров;

• регрессионное тестирование (возможность повторения и модификации ранее выполненных тестов для определения различий в системе и/или среде);

• автоматизированный анализ результатов тестирования и исключительных ситуаций в процессе тестирования, включая сравнение ожидаемых и реальных результатов, сравнение файлов, статистический анализ результатов; обращения к операторам, процедурам и переменным; защиту от несанкционированного доступа и др.;

• анализ производительности. Анализируемые параметры производительности могут включать использование центрального процессора, памяти, обращения к определённым элементам данных и (или) сегментам кода, временные характеристики и т.д.

Результаты оценки должны быть стандартным образом документированы и, при необходимости, утверждены. Отчёт по результатам оценки должен содержать следующую информацию:

● введение (общий обзор процесса и перечень основных результатов);

● предпосылки (цель оценки и желаемые результаты, период времени, в течение которого выполнялась оценка, определение ролей и соответствующего опыта специалистов, выполнявших оценку);

● подход к оценке (описание общего подхода, включая информацию, определяющую контекст и масштаб оценки, а также любые предположения и ограничения);

● информация об ИС, которая должна включать:

1) наименование системы;

2) данные о Заказчике и Исполнителях, включая контактную информацию;

3) конфигурацию технических средств;

4) стоимостные данные;

5) описание ИС, включающее поддерживаемые данным средством процессы создания и сопровождения ИС, программную среду (поддерживаемые языки программирования, операционные системы, совместимость с базами данных), функции, входные/выходные данные и область применения;

● этапы оценки (конкретные действия, выполняемые в процессе оценки, должны быть описаны со степенью детализации, необходимой как для понимания масштаба и глубины оценки, так и для её повторения при необходимости);

● конкретные результаты должны быть представлены в терминах критериев оценки. В тех случаях, когда отчёт охватывает ряд средств или результаты данной оценки будут сопоставляться с аналогичными результатами других оценок, необходимо обратить особое внимание на формат представления результатов, способствующий такому сравнению. Субъективные результаты отделяют от объективных и сопровождают необходимыми пояснениями;

● выводы и заключения;

● приложения, в которых присутствуют формулировка задачи оценки и уточненный список критериев.

В процессе реализации проекта важное место занимают вопросы идентификации, описания и контроля конфигурации отдельных компонентов и всей системы в целом.

10. Эксплуатация и сопровождение ИС. Управление рисками и инцидентами. Оценка рисков.

**Эксплуатация ИС** *Эксплуатация* включает работы по внедрению компонентов ПО в эксплуатацию, в том числе конфигурирование БД и рабочих мест пользователей, обеспечение эксплуатационной документацией, проведение обучения персонала и т.д., и непосредственно эксплуатацию, в том числе локализацию проблем и устранение причин их возникновения, модификацию ПО в рамках установленного регламента, подготовку предложений по совершенствованию, развитию и модернизации системы.

Продуктивность и иные характеристики деятельности организации после внедрения в ней разработанной ИС могут первоначально ухудшиться, так как на освоение новых средств и внесение необходимых изменений в процессы разработки и эксплуатации требуется некоторое время. Таким образом, ожидаемые результаты должны рассматриваться с учётом вероятной отсрочки в улучшении проектных и эксплуатационных характеристик.

Техническое обслуживание и модернизация. Если собственно техническое обслуживание (очистка от пыли, смазка вентиляторов, подтяжка креплений, контроль состояния аккумуляторов, изменение физической топологии сети и т. п.) может осуществляться службой технической поддержки, то грамотное формулирование заявок на изменение аппаратной конфигурации, организация закупки дополнительных лицензий или обновленной версии программного обеспечения – задача администратора.

Важным вопросом сопровождения ИС является мониторинг работы сетевого и иного вычислительного оборудования. Эту задачу оперативного управления ИС выполняет администратор системы.

В первую очередь принято обращать внимание на критически важные инциденты. Затем рекомендуется осуществлять контроль сроков исполнения, оптимизировать контролируемы параметры и др.

**УПРАВЛЕНИЕ РИСКАМИ И ИНЦИДЕНТАМИ**Определение рисков - сложная задача.

Успешное выявление и ликвидация рисков зависит от умения их распознавать.

Выделяю восемь наиболее опасных рисков:

1) недостаточное внимание к проекту со стороны руководства заказчика

(компании) и недостаточное в нём участие;

2) неконкретная постановка задачи или непонимание сторонами конечных целей проекта;

3) изменения, вносимые заказчиком в процессе реализации проекта;

4) недостаточная квалификация работников;

5) отсутствия мотивации сотрудников заказчика, противодействие персонала;

6) срыв сроков;

7) технические проблемы;

8) недостаточное или нестабильное финансирование.

Риски относящиеся к эксплуатации ИС, управление которой осуществляютадминистраторы ИС:

– недостаточное внимание руководства организации, эксплуатирующей ИС, к главным вопросам эксплуатации и администрирования ИС;

– непонимание им важности данной работы, влекущее за собой некорректные указания по данным вопросам;

– недостаточную квалификацию администраторов и пользователей ИС;

– технические и финансовые проблемы.

К рискам администрирования ИС относят:

– сокращение установленных в соответствующих планах (графиках) сроков выполнения работ;

– увеличение стоимости сопровождения, эксплуатации и администрирования ИС из-за системных и иных ошибок, недостаточного уровня поддержки со стороны руководства и администраторов ИС;

– сложность эксплуатации системы;

– несоблюдение условий безопасности ИС и хранящихся в ней данных;

– сбои;

– увольнение администраторов и специалистов, осуществляющих

эксплуатацию и поддержку ИС и др.Количественную оценку большинства организационно-управленческих рисков для ИТпроектов (ИС) оценить трудно, так же как и его экономическую эффективность, так как они обычно носят характер качественного улучшения и выполняются в условиях относительно низкой неопределённости. При этом обычно все наиболее важные риски случаются до начала выполнения проекта.

Качественную оценку рисков в виде низкий, средний, высокий, некоторые специалисты считают возможным перевести в качественно-количественные показатели. При этом они определяют высокую вероятность появления риска в 70% и выше (или 3 балла), среднюю – от 40 до 70% (2 балла) и низкую – менее 40% (1 балл). Другой критерий предполагает, что если воздействие приведёт к потере менее 1% бюджета или затянет сроки исполнения проекта менее чем на 5% отведённого времени, то его можно считать низким. Соответственно при 1–5% бюджета и 5– 10% дополнительного времени – средним. Если бюджет превышен больше чем на 5%, а сроки – более чем на 10%, то высоким.

11. Управление безопасностью. Виды функциональной безопасности ИС. Проверка полномочий, проверка подлинности. Фундаментальные принципы обеспечения безопасности.

Важным компонентом администрирования системы является обеспечение информационной безопасности: составление плана доступа пользователей к ресурсам (в соответствии с принятой в компании политикой информационной безопасности) и контроль его исполнения.

К функциям обеспечения безопасности относятся также отслеживание появления различных уязвимостей в используемых операционных системах, организация получения и установки “заплаток” (patches).

Функционально безопасность ИС можно разделить на технологическую, логическую и физическую безопасности.

• Для обеспечения технологической безопасности в информационных системах используют “зеркальные” серверы, двойные жёсткие диски, надёжные системы бесперебойного питания и др.

• Логическая безопасность заключается в использовании программных средств борьбы с компьютерными вирусами, защиты от несанкционированного доступа, идентификации и кодирования информации.

• Физическая безопасность включает персонал, меры и преграды, препятствующие проникновению несанкционированных лиц на недоступные для них объекты.

**Проверка полномочий** основана на том, что для каждого пользователя или процесса информационной системы устанавливаться набор санкционированных действий, которые он может выполнять по отношению к определенным объектам.

**Проверка подлинности** означает достоверное подтверждение того, что пользователь или процесс, пытающийся выполнить санкционированные действия, действительно является тем, за кого он себя выдает

12. Многоуровневая безопасность. Классы и уровни допуска или доступа к информации. Методы обеспечения сохранности информации.

Многоуровневая безопасность означает, во-первых, что в системе хранится информация, относящаяся к разным классам безопасности, и, во-вторых, – часть пользователей не имеет доступа к информации, относящейся к высшему классу безопасности. Субъект имеет доступ к объекту, если уровень его допуска такой же или ниже, чем класс объекта. При этом пользователь, имеющий низший уровень допуска, должен иметь возможность выполнять свою работу в системе, содержащей в базе данных совершенно секретные данные, но не должен иметь доступа к ним. Информация и данные подвергаются классификации, а каждый субъект получает определённый уровень допуска к соответствующим классам данных (объектов)

Классы и уровни допуска совместно называются классами или уровнями

доступа.

В военных и государственных ведомствах применяют следующую иерархию классов (сверху вниз):

• совершенно секретно;

• секретно;

• конфиденциально;

• без грифа секретности.

В частных компаниях возможны уровни иерархии (сверху вниз):

• секретно;

• для ограниченного распространения;

• конфиденциально;

• для служебного пользования;

• для неограниченного распространения

Защита данных от несанкционированного доступа предполагает:

1. Обеспечение парольного входа в систему: регистрация пользователей, назначение и изменение паролей.

2. Обеспечение защиты конкретных данных: определение прав доступа групп пользователей и отдельных пользователей, определение допустимых операций над данными для отдельных пользователей, выбор/создание программно-технологических средств защиты данных; шифрование информации с целью защиты данных от несанкционированного использования.

3. Тестирование средств защиты данных.

4. Фиксация попыток несанкционированного доступа к информации.

5. Исследование возникающих случаев нарушения защиты данных и проведение мероприятий по их предотвращению.

13. Резервное копирование и восстановление данных. Виды резервного копирования.

Функционально безопасность ИС можно разделить на технологическую, логическую и физическую безопасности. Для обеспечения технологической безопасности в информационных системах используют “зеркальные” серверы, двойные жёсткие диски, надёжные системы бесперебойного питания и др. Логическая безопасность заключается в использовании программных средств борьбы с компьютерными вирусами, защиты от несанкционированного доступа, идентификации и кодирования информации. Физическая безопасность включает персонал, меры и преграды, препятствующие проникновению несанкционированных лиц на недоступные для них объекты.

Важной особенностью систем хранения данных является непрерывная их защита (Continuous Data Protection, CDP). Для защиты данных, хранящихся на файл-сервере, применяют резервное копирование, ленточный автозагрузчик и др. Открытые файлы не копируются на ленту. Операция резервного копирования создаёт дополнительную нагрузку на сервер. В этом случае резервное копирование можно осуществлять в нерабочее время (ночью, в выходные и праздничные дни и др.), то есть в специально выделяемый для этого период времени – окно резервного копирования.

С целью обеспечения достоверности и постоянной работоспособности ИС периодически вручную или автоматически осуществляется копирование ИС.

Основными причинами, побуждающими выполнение процедур копирования, являются различные структурные изменения в ИС:

• создание или удаление табличного пространства;

• добавление или переименование (перемещение) файла данных в существующем табличном пространстве;

• добавление, переименование (перемещение) или удаление журнала повторения и др.

При этом резервное копирование может осуществляться непосредственно перед изменениями и после них.

ВИДЫ

1. Непротиворечивое (холодное) резервное копирование, когда копии создаются, в случае закрытой для пользователей ИС. Копия ИС, созданной в автономном режиме, содержит: все файлы данных, журналы повторов и управляющие файлы. После остановки ИС, все её файлы копируются на один из “backup” дисков. По окончании копирования осуществляется перезагрузка ИС.

2. Резервное (горячее) копирование в оперативном режиме, к примеру, когда ИС всё время находиться в оперативном режиме и доступна пользователям.

14. Безопасность ИС. Основные аспекты информационной безопасности. Виды и группы угроз ИБ, классы отказов.

Безопасность информационной системы – свойство, заключающееся в способности системы обеспечить конфиденциальность и целостность информации, т.е. защиту информации от несанкционированного доступа с целью ее раскрытия, изменения или разрушения.

В соответствии с общепринятым современным подходом выделяют следующие аспекты информационной безопасности:

• доступность (возможность за приемлемое время получить требуемую информационную услугу);

• целостность (актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения);

• конфиденциальность (защита от несанкционированного ознакомления)

Все угрозы информационным системам можно объединить в обобщающие их три группы.

1. Угроза раскрытия — возможность того, что информация станет известной тому, кому не следовало бы ее знать.

2. Угроза целостности — умышленное несанкционированное изменение (модификация или удаление) данных, хранящихся в вычислительной системе или передаваемых из одной системы в другую.

3. Угроза отказа в обслуживании — возможность появления блокировки доступа к некоторому ресурсу вычислительной системы.

Выделяют следующие классы отказов:

1. Отказ пользователей – возникает по следующим причинам:

• нежелание работать с информационной системой;

• невозможность работать с системой в силу отсутствия соответствующей подготовки;

• невозможность работать с системой в силу отсутствия технической поддержки.

2. Внутренний отказ информационной системы – возникает по следующим причинам:

• отступление (случайное или умышленное) от установленных правил эксплуатации;

• ошибки при (пере)конфигурировании системы; • отказы программного и аппаратного обеспечения;

• разрушение данных;

• разрушение или повреждение аппаратуры.

3. Отказ поддерживающей инфраструктуры – возникает по следующим причинам:

• нарушение работы (случайное или умышленное) систем связи, электропитания, водоснабжения, кондиционирования;

• разрушение или повреждение помещений;

• невозможность или нежелание выполнения обслуживающим персоналом и/или пользователями своих обязанностей (гражданские беспорядки, аварии на транспорте, террористический акт или его угроза, забастовка и т.п.).

15. Непреднамеренные и преднамеренные действия пользователей, предоставляющие угрозу безопасности ИС. Модель нарушителя ИБ. Типы нарушителей, классификация. Мотивы нарушений.

Пользователем ИС могут быть осуществлены следующие непреднамеренные действия, представляющие угрозу безопасности ИС:

– доведение до состояния частичного или полного отказа системы, разрушение аппаратных, программных, информационных ресурсов системы (порча оборудования, носителей информации, удаление, искажение файлов с важной информацией или программ);

– неправомерное включение оборудования или изменение режимов работы устройств и программ;

– запуск сервисных программ, способных при некомпетентном использовании вызывать потерю работоспособности системы или необратимые изменения в системе

Пользователем ИС могут быть осуществлены следующие преднамеренные действия, представляющие угрозу безопасности ИС :

– физическое разрушение системы или вывод из строя наиболее важных ее компонентов;

– отключение или вывод из строя подсистем обеспечения функционирования вычислительных систем (электропитания, охлаждения и вентиляции, линий связи и т. п.);

– дезорганизация функционирования системы (изменение режимов работы устройств или программ, создание мощных активных радиопомех и т. п.);

Формализованное описание или представления комплекса возможностей нарушителя по реализации тех или иных угроз безопасности информации называют моделью нарушителя, при разработке которой делаются предположения:

– о категориях лиц, к которым может принадлежать нарушитель;

– о мотивах действий нарушителя;

– о квалификации нарушителя и его технической оснащенности;

– о характере возможных действий нарушителя.

По отношению к ИС нарушители могут быть:

Внутренние нарушители - могут быть лица из следующих категорий персонала:

• пользователи системы;

• персонал, обслуживающий технические средства (инженеры, техники);

• сотрудники отделов разработки и сопровождения программного обеспечения (прикладные и системные программисты);

• технический персонал, обслуживающий здание (уборщики, электрики, сантехники и другие сотрудники, имеющие доступ в здание и помещения, где расположены компоненты ИС);

• сотрудники службы безопасности ИС;

• руководители различных уровней должностной иерархии. Посторонние лица, которые могут быть внешними нарушителями:

• клиенты;

• посетители;

• представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации (энерго-, водо-, теплоснабжение и т. п.);

• представители конкурирующих организаций или лица, действующие по их заданию;

• лица, случайно или умышленно нарушившие пропускной режим (без цели нарушения безопасности ИС).

Можно выделить три основных мотива нарушений:

• безответственность;

• самоутверждение;

• корыстный интерес.

16. Системы защиты ИС. Основные методы защиты информации. Средства обеспечения ИБ. Модели администрирования сети и способы обеспечения безопасности (централизованное, распределенное, администрирование по ОС, смешанная модель).

Система защиты — это совокупность специальных мер правового и административного характера, организационных мероприятий, программно-аппаратных средств защиты, а также специального персонала, предназначенных для обеспечения информационной безопасности .

Основные методы защиты информации:

1. Создание препятствий — методы физического преграждения злоумышленнику пути к защищаемой информации (аппаратуре, носителям информации и т. д.).

2. Управление доступом — метод защиты информации регулированием использования всех ресурсов компьютерной информационной системы (элементов баз данных, программных и технических средств).

3. Защита от несанкционированного доступа к ресурсам компьютера — это комплексная проблема, подразумевающая решение следующих вопросов:

– присвоение пользователю, терминалам, программам, файлам и каналам связи уникальных имен и кодов (идентификаторов);

– выполнение процедур установления подлинности при обращениях к информационной системе, то есть проверка того, что лицо или устройство, сообщившее идентификатор, в действительности ему соответствует;

– проверка полномочий, то есть проверка права пользователя на доступ к системе или запрашиваемым данным;

– автоматическая регистрация в специальном журнале всех как удовлетворенных, так и отвергнутых запросов к информационным ресурсам с указанием идентификатора пользователя, терминала, времени и сущности запроса, то есть ведение аудита.

4. Маскировка — метод защиты информации путем ее криптографического закрытия.

5. Регламентация — метод защиты информации, создающий такие условия автоматизированной обработки, хранения и передачи защищаемой информации, при которых возможности несанкционированного доступа к ней сводились бы к минимуму. 6. Принуждение — метод защиты, при котором пользователи и персонал системы вынуждены соблюдать правила обработки, передачи и использования защищаемой информации под угрозой материальной, административной или уголовной ответственности.

**Средства обеспечения информационной безопасности в зависимости от способа их реализации можно разделить на следующие классы методов: -**

аппаратные методы, реализующие физическую защиту системы от несанкционированного доступа, аппаратные функции идентификации периферийных терминалов системы и пользователей, режимы подключения сетевых компонентов и т. д.

К техническим средствам физической защиты информации (ЗИ) относят механические, электронно-механические, электромеханические, оптические, акустические, лазерные, радио и другие устройства, системы и сооружения, предназначенные для создания физических препятствий на пути к защищаемой информации и способные выполнять самостоятельно или в комплексе с другими средствами функции защиты информации.

- организационные методы подразумевают рациональное конфигурирование, организацию и администрирование системы. В первую очередь это касается сетевых информационных систем, их операционных систем, полномочий сетевого администратора, набора обязательных инструкций, определяющих порядок доступа и работы в сети пользователей;

- технологические методы, включающие в себя технологии выполнения сетевого администрирования, мониторинга и аудита безопасности информационных ресурсов, ведения электронных журналов регистрации пользователей, фильтрации и антивирусной обработки поступающей информации;

- программные методы - это самые распространенные методы защиты информации (например, программы идентификации пользователей, парольной защиты и проверки полномочий, брандмауэры, криптопротоколы и т. д.)

**Администрирование сети можно организовать одним из четырех основных способов:**

• централизованно на всем предприятии;

• по отделам или группам («распределенное» администрирование);

• по операционным системам;

• в виде сочетания предыдущих способов.

Модели администрирования небольших и крупных, сложных систем могут совпадать. Они будут отличаться масштабами, но не по сути

**Централизованное администрирование**

В модели с централизованным администрированием один человек, группа или отдел занимается администрированием всей сети организации, ее пользователей и ресурсов. Главным и очень серьезным недостатком централизованной схемы является ее недостаточная масштабируемость и отсутствие отказоустойчивости. Производительность центрального компьютера всегда будет ограничителем количества пользователей, работающих с данным приложением, а отказ центрального компьютера приводит к прекращению работы всех пользователей. Эта модель хорошо подходит небольшим и средним организациям, но может оказаться медленной и неэффективной для крупного или географически разбросанного предприятия. Однако с точки зрения безопасности централизованное администрирование является наилучшим. Оно гарантирует, что системная политика и процедуры являются однообразными для всей организации.

**Распределенное администрирование**

При распределенном администрировании управление сетью осуществляется на уровне отдела или рабочей группы. Хотя администрирование на этом уровне может быстро откликаться на нужды пользователей, часто это достигается за счет безопасности сети. При наличии нескольких администраторов политика администрирования в разных рабочих группах будет отличаться. Чем больше групп имеется в системе, тем больше доверительных отношений им требуется, что повышает возможность того, что в систему проникнет злоумышленник и воспользуется этими доверительными отношениями, чтобы добраться до совершенно секретной информации.

**Администрирование по операционным системам**

Когда администрирование домена производится по операционным системам, средства обеспечения безопасности значительно различаются в зависимости от используемых операционных систем. Например, если имеется свой администратор у сервера Windows NТ Server, свой — у сервера Novell Net Wаге и свой — у систем UNIX, то администратор каждой системы будет сам обеспечивать ее безопасность. Однако потребуется кто-то, кто будет разрешать различия во мнениях администраторов в случае возникновения проблем.

**Смешанная модель администрирования**

Смешанная модель администрирования сочетает элементы централизованной и распределенной моделей. Центральный администратор (или группа) гарантирует проведение политики безопасности на всем предприятии, а администраторы на уровне отделов или рабочих групп выполняют повседневную работу. При этом обычно требуется больше затрат на штат, чем может себе позволить небольшая организация, поэтому применение смешанной модели администрирования, как правило, ограничивается крупными предприятиями.

17. Концепция управления ИТ-службами ITSM (идея, ключевые элементы, идеология). Преимущества внедрения концепции ITSM.

Концепция Управления ИТ-службами — Information Technology Service Management (ITSM) предлагает новый взгляд на организацию функционирования ИТ-подразделений, порядок управления этими подразделениями, пути повышения эффективности использования ресурсов.

Основная идея внедрения ITSM состоит в том, чтобы ИТ-отдел перестал быть вспомогательным элементом для основного бизнеса компании, ответственным только за работу отдельных серверов, сетей и приложений, «где-то и как-то» применяющихся в компании.

Ключевыми элементами ITSM являются: процессы, персонал, технологии.

Идеология ITSM держится на трех китах:

1) формализация процессов функционирования информационных технологий;

2) профессионализм и четкая ответственность сотрудников ИТ-отдела за определенный круг задач;

3) технологическая инфраструктура обеспечения качества услуг:

- Собственно информационные технологии, служба поддержки пользователей;

- служба управления конфигурациями и изменениями;

- система контроля услуг;

- служба тестирования и внедрения новых услуг и т.д.

Положительными сторонами ITSM для пользователей является

* Улучшение качества обслуживания;
* Сокращение времени простоев, которые связаны с ИТ;
* Возможность обращения в централизованную службу поддержки по любым вопросам;
* Контроль над выполнением своих запросов;
* Обеспечение выполнения запросов в соответствии с установленным уровнем услуг.

18. Библиотека ITIL, история создания, идея, определение, составляющие или дисциплины ITIL.

Библиотека Information Technology Infrastructure Library (ITIL) — библиотека передового опыта была создана в результате осознания того факта, что достижение организациями своих корпоративных целей все более зависит от ИТ.

С течением времени акцент переместился с разработки ИТ-приложений на управление ИТ-услугами.

ИТ-приложения лишь тогда способствуют достижению корпоративных целей, когда система доступна пользователям, и при возникновении ошибок и необходимости модификации поддержка может быть оказана службой сопровождения.

С ростом важности задач, ставящихся руководством компаний перед ИТотделами, и расширением используемых ими средств столь популярная в бизнесе тема реинжиниринга бизнес-процессов пришла и в ИТ.

В конце 80-х годов в Европе была предложена IT Infrastructure Library — библиотека передового опыта ИТ, вобравшая наилучшие решения по организации ИТ.

ITIL был разработан Центральным Компьютерным и Телекоммуникационным Агентством (CCTA - Central Communications and Telecom Agency) по указанию английского правительства в целях использования ИТ-службами.

Библиотека ITIL создавалась для систематического и последовательного распространения передового опыта по Управлению ИТ-услугами. Этот подход основывается на качестве услуг и разработке эффективных и рациональных процессов.

Можно дать следующие определения ITIL:

• ITIL - строго регламентированная система требований и рекомендаций по организации деятельности по управлению предоставлением информационных сервисов (сервисов ИТ или услуг ИТ) в соответствии с определенным уровнем качества и затрат.

• ITIL - это не продукт, не программа, не система. ITIL - это методология. Она позволит вам обеспечить эффективное функционирование служб Информационных Технологий (ИТ), удовлетворение нужд бизнеспользователей, стабильное и предсказуемое развитие информационной системы.

• ITIL - является набором всесторонних, непротиворечивых и согласованных документов, построенных на основе знаний и опыта мировых организаций, и предназначенным для управления обслуживанием информационных систем (ИС).

Подход ITIL заключается в разделении процесса управления ИТ на несколько дисциплин. Каждая дисциплина нацелена на решение определенных задач (или выполнение функций), но во взаимодействии с остальными. Они охватывают такие области, как:

• управление изменениями (Change Management);

• управление проблемами (Problem Management);

• управление конфигурацией (Configuration management);

• управление уровнем сервиса (Service Level Management);

• управление планированием (Capacity Management);

• управление стоимостью (Cost Management) и множество других.

19. Что понимается под открытыми системами. Свойства открытых систем. Структура среды ИС. Эталонная модель открытых систем. Протокол. Интерфейс. Инкапсуляция. Основные элементы модели взаимодействия открытых систем.

Открытая система – система реализующая открытые спецификации на интерфейсы, службы и форматы данных достаточные для того чтобы обеспечить:

1. Возможность переноса (мобильность) прикладных систем, разработанных с минимальными изменениями на широкий диапазон систем.

2. Совместную работу (интероперабельность) с другими прикладными системами на локальных и удаленных платформах.

3. Взаимодействие с пользователями в стиле облегчающем переход от системы к системе.

**Общие свойства открытых ИС**:

• расширяемость/масштабируемость - обеспечение возможности добавления новых функций ИС или изменения некоторых уже имеющихся при неизменных остальных функциональных частях ИС;

• мобильность/переносимость - обеспечение возможности переноса программ и данных при модернизации или замене аппаратных платформ ИС и возможности работы с ними специалистов, пользующихся ИТ, без их переподготовки при изменениях ИС;

• взаимодействие - способность к взаимодействию с другими ИС (технические средства, на которых реализована информационная система, объединяются сетью или сетями различного уровня - от локальной до глобальной)

• стандартизуемость - ИС проектируются и разрабатываются на основе согласованных международных стандартов и предложений, реализация открытости осуществляется на базе функциональных стандартов (профилей) в области информационных технологий;

• дружественность к пользователю - развитые унифицированные интерфейсы в процессах взаимодействия в системе "человек-машина" позволяют работать пользователю, не имеющему специальной "компьютерной" подготовки.

**Структура среды информационной системы**

Обобщенная структура любой ИС может быть представлена двумя взаимодействующими частями:

1. функциональная часть, включающая прикладные программы, которые реализуют функции прикладной области;

2. среда или системная часть, обеспечивающая исполнение прикладных программ.

С этим разделением тесно связаны две группы вопросов стандартизации:

1. стандарты интерфейсов взаимодействия прикладных программ со средой ИС, прикладной программный интерфейс (Application Program Interface - API);

2. стандарты интерфейсов взаимодействия самой ИС с внешней для нее средой (External Environment Interface - EEI).

Эти две группы интерфейсов определяют спецификации внешнего описания среды ИС - архитектуру, с точки зрения конечного пользователя, проектировщика ИС, прикладного программиста, разрабатывающего функциональные части ИС.

**Эталонная модель среды открытых систем**

Основным достоинством этой модели является детальное описание связей в среде с точки зрения технических устройств и коммуникационных взаимодействий. Вместе с тем она не принимает в расчет взаимосвязь с учетом мобильности прикладного программного обеспечения. Эталонная модель среды открытых систем (OSE/RM) определяет разделение любой информационной системы на приложения (прикладные программы и программные комплексы) и среду, в которой эти приложения функционируют. Между приложениями и средой определяются стандартизованные интерфейсы (API), которые являются необходимой частью профилей любой открытой системы. Кроме того, в профилях ИС могут быть определены унифицированные интерфейсы взаимодействия функциональных частей друг с другом и интерфейсы взаимодействия между компонентами среды ИС.

• **Протоколом** является набор алгоритмов (правил) взаимодействия объектов одноименных уровней различных систем.

• **Интерфейс** - это совокупность правил, в соответствии с которыми осуществляется взаимодействие с объектом данного или другого уровня. Стандартный интерфейс в некоторых спецификациях может называться услугой.

• **Инкапсуляция** - это процесс помещения фрагментированных блоков данных одного уровня в блоки данных другого уровня.

Основные элементы модели взаимодействия открытых систем:

1. Уровень

2. Объекты

3. Соединения

4. Физические средства соединения

Функциональные профили модели – подмножества стандартов взаимодействия открытых систем, предназначенные для конкретных нужд пользователей. При создании и развитии сложных, распределенных, тиражируемых программных и информационных систем требуется гибкое формирование и применение согласованных (гармонизированных) совокупностей базовых и рабочих стандартов, нормативных документов разного уровня, выделение в них требований и рекомендаций, необходимых для реализации заданных функций ИС. Для унификации и регламентирования такие совокупности базовых стандартов должны адаптироваться и конкретизироваться применительно к определенным классам проектов, процессов функций и компонентов разрабатываемых систем. В связи с этим выделилось и сформировалось понятие профиля программной или информационной системы как основного инструмента функциональной стандартизации.

20. Средства анализа и управления сетями. Стандарт Telecommunication Management Network.

Любая сложная вычислительная сеть требует дополнительных специальных средств управления помимо тех, которые имеются в стандартных сетевых операционных системах. Это связано с большим количеством разнообразного коммуникационного оборудования, работа которого критична для выполнения сетью своих основных функций. Распределенный характер крупной корпоративной сети делает невозможным поддержание ее работы без централизованной системы управления, которая в автоматическом режиме собирает информацию о состоянии каждого концентратора, коммутатора, мультиплексора и маршрутизатора и предоставляет эту информацию оператору сети. Обычно система управления работает в автоматизированном режиме, выполняя наиболее простые действия по управлению сетью автоматически, а сложные решения предоставляя принимать человеку на основе подготовленной системой информации. Система управления должна быть интегрированной. Это означает, что функции управления разнородными устройствами должны служить общей цели обслуживания конечных пользователей сети с заданным качеством. 2 Сами системы управления представляют собой сложные программноаппаратные комплексы, поэтому существует граница целесообразности применения системы управления - она зависит от сложности сети, разнообразия применяемого коммуникационного оборудования и степени его распределенности по территории. В небольшой сети можно применять отдельные программы управления наиболее сложными устройствами, например коммутатором, поддерживающим технику VLAN. Обычно каждое устройство, которое требует достаточно сложного конфигурирования, производитель сопровождает автономной программой конфигурирования и управления. Однако при росте сети может возникнуть проблема объединения разрозненных программ управления устройствами в единую систему управления, и для решения этой проблемы придется, возможно, отказаться от этих программ и заменить их интегрированной системой управления.

Применительно к системам управления сетями наиболее проработанным и эффективным для создания многоуровневой иерархической системы является стандарт **Telecommunication Management Network** (TMN), разработанный совместными усилиями ITU-T, ISO, ANSI и ETSI. Хотя этот стандарт и предназначался изначально для телекоммуникационных сетей, но ориентация на использование общих принципов делает его полезным для построения любой крупной интегрированной системы управления сетями. Стандарты TMN состоят из большого количества рекомендаций ITU-T (и стандартов других организаций), но основные принципы модели TMN описаны в рекомендации М.3010. 4 На каждом уровне иерархии модели TMN решаются задачи одних и тех же пяти функциональных групп, (управления конфигурацией, производительностью, ошибками, безопасностью и учетом), однако на каждом уровне эти задачи имеют свою специфику. Чем выше уровень управления, тем более общий и агрегированный характер приобретает собираемая о сети информация, а сугубо технический характер собираемых данных начинает по мере повышения уровня меняться на производственный, финансовый и коммерческий.

Нижний уровень - уровень элементов сети (Network Element layer, NE) - состоит из отдельных устройств сети: каналов, усилителей, оконечной аппаратуры, мультиплексоров, коммутаторов и т. п. Элементы могут содержать встроенные средства для поддержки управления - датчики, интерфейсы управления, а могут и представлять вещь в себе, требующую для связи с системой управления разработки специального оборудования - устройств связи с объектом, УСО. Современные технологии обычно имеют встроенные функции управления, которые позволяют выполнять хотя бы минимальные операции по контролю за состоянием устройства и за передаваемым устройством трафиком. Подобные функции встроены в технологии FDDI, ISDN, frame relay, SDH. В этом случае устройство всегда можно охватить системой управления, даже если оно не имеет специального блока управления, так как протокол технологии обязывает устройство поддерживать некоторые функции управления. Устройства, которые работают по протоколам, не имеющим встроенных функций контроля и управления, снабжаются отдельным блоком управления, который поддерживает один из двух наиболее распространенных протоколов управления - SNMP или CMIP. Эти протоколы относятся к прикладному уровню модели OSI. 6

Следующий уровень - уровень управления элементами сети (network element management layer) - представляет собой элементарные системы управления. Элементарные системы управления автономно управляют отдельными элементами сети - контролируют канал связи SDH, управляют коммутатором или мультиплексором. Уровень управления элементами изолирует верхние слои системы управления от деталей и особенностей управления конкретным оборудованием. Этот уровень ответственен за моделирование поведения оборудования и функциональных ресурсов нижележащей сети. Атрибуты этих моделей позволяют управлять различными аспектами поведения управляемых ресурсов. Обычно элементарные системы управления разрабатываются и поставляются производителями оборудования. Примерами таких систем могут служить системы управления CiscoView от Cisco Systems, Optivity от Bay Networks, RADView от RAD Data Communications и т. д. 7

Выше лежит уровень управления сетью (Network management layer). Этот уровень координирует работу элементарных систем управления, позволяя контролировать конфигурацию составных каналов, согласовывать работу транспортных подсетей разных технологий и т. п. С помощью этого уровня сеть начинает работать как единое целое, передавая данные между своими абонентами.

Следующий уровень - уровень управления услугами (Service management layer) - занимается контролем и управлением за транспортными и информационными услугами, которые предоставляются конечным пользователям сети. В задачу этого уровня входит подготовка сети к предоставлению определенной услуги, ее активизация, обработка вызовов клиентов. Формирование услуги (service provisioning) заключается в фиксации в базе данных значений параметров услуги, например, требуемой средней пропускной способности, максимальных величин задержек пакетов, коэффициента готовности и т. п. В функции этого уровня входит также выдача уровню управления сетью задания на конфигурирование виртуального или физического канала связи для поддержания услуги. После формирования услуги данный уровень занимается контролем за качеством ее реализации, то есть за соблюдением сетью всех принятых на себя обязательств в отношении производительности и надежности транспортных услуг. Результаты контроля качества обслуживания нужны, в частности, для подсчета оплаты за пользование услугами клиентами сети. Например, в сети frame relay уровень управления услугами следит за заказанными пользователем значениями средней скорости CIR и согласованной пульсации Вс, фиксируя нарушения со стороны пользователя и сети

Уровень бизнес-управления (Business management layer) занимается вопросами долговременного планирования сети с учетом финансовых аспектов деятельности организации, владеющей сетью. На этом уровне помесячно и поквартально подсчитываются доходы от эксплуатации сети и ее отдельных составляющих, учитываются расходы на эксплуатацию и модернизацию сети, принимаются решения о развитии сети с учетом финансовых возможностей. Уровень бизнес-управления обеспечивает для пользователей и поставщиков услуг возможность предоставления дополнительных услуг. Этот уровень является частным случаем уровня автоматизированной системы управления предприятием (АСУП), в то время как все нижележащие уровни соответствуют уровням автоматизированной системы управления технологическими процессами (АСУТП), для такого специфического типа предприятия, как телекоммуникационная или корпоративная сеть. Но если телекоммуникационная сеть действительно чаще всего является основой телекоммуникационной компании, то корпоративную сеть и обслуживающий ее персонал обычно трудно назвать предприятием. Тем не менее на некоторых западных фирмах корпоративная сеть выделена в автономное производственное подразделение со своим бюджетом и со своими финансовыми договорами на обслуживание, которое данное подразделение заключает с основными производственными подразделениями предприятия.

21. Архитектуры систем управления сетями. Схема менеджер – агент. Структуры распределенных систем управления. Одноранговая и иерархическая модели управления сетями.

Выделение в системах управления типовых групп функций и разбиение этих функций на уровни еще не дает ответа на вопрос, каким же образом устроены системы управления, из каких элементов они состоят и какие архитектуры связей этих элементов используются на практике.

Схема менеджер – агент

• Агент – это устройство или программа, которые устанавливаются в элементах компьютерной сети для централизованного управления этими элементами и всей сетью. Агенты являются частью системы сетевого управления. Каждый агент собирает данные и управляет определенным элементом сети. Менеджеры, называемые серверами системы управления, собирают данные от своих агентов, обобщают их и хранят в базе данных.

• Менеджер - это основная управляющая программа, которая устанавливается на отдельном компьютере, который выполняет также роль консоли управления для оператора или администратора системы. Менеджер взаимодействует с агентами по стандартному протоколу, например SNMP. Агент является посредником между управляемым ресурсом и основной управляющей программой

Агент поставляет менеджеру обработанную и представленную в нормализованном виде информацию. На основе этой информации менеджер принимает решения по управлению, а также выполняет дальнейшее обобщение данных о состоянии управляемого ресурса, например, строит зависимость загрузки порта от времени.

Операторы, работающие за рабочими станциями, могут соединиться с любым из менеджеров и с помощью графического интерфейса просмотреть данные об управляемой сети, а также выдать менеджеру некоторые директивы по управлению сетью или ее элементами.

В основе любой системы управления сетью лежит элементарная схема взаимодействия агента с менеджером. На основе этой схемы могут быть построены системы практически любой сложности с большим количеством агентов и менеджеров разного типа.

В крупной корпоративной сети полностью централизованная система управления, построенная на базе единственного менеджера, вряд ли будет работать хорошо по нескольким причинам.

Во-первых, такой вариант не обеспечивает необходимой масштабируемости по производительности, так как единственный менеджер вынужден будет обрабатывать весь поток сообщений от всех агентов, что при нескольких тысячах управляемых объектов потребует очень высокопроизводительной платформы для работы менеджера и перегрузит служебной управляющей информацией каналы передачи данных в той сети, где будет расположен менеджер.

Во-вторых, такое решение не обеспечит необходимого уровня надежности, так как при отказе единственного менеджера будет потеряно управление сетью.

В-третьих, в большой распределенной сети целесообразно располагать в каждом географическом пункте отдельным оператором или администратором, управляющим своей частью сети, а это удобнее реализовать с помощью отдельных менеджеров для каждого оператора.

В случае одноранговых связей каждый менеджер управляет своей частью сети на основе информации, получаемой от нижележащих агентов. Центральный менеджер отсутствует. Координация работы менеджеров достигается за счет обмена информацией между базами данных каждого менеджера. Одноранговое построение системы управления сегодня считается неэффективным и устаревшим.

Гораздо более гибким является иерархическое построение связей между менеджерами. Каждый менеджер нижнего уровня выполняет также функции агента для менеджера верхнего уровня. Такой агент работает уже с гораздо более укрупненной моделью (MIB) своей части сети, в которой собирается именно та информация, которая нужна менеджеру верхнего уровня для управления сетью в целом. Обычно для разработки моделей сети на разных уровнях проектирование начинают с верхнего уровня, на котором определяется состав информации, требуемой от менеджеров-агентов более низкого уровня, поэтому такой подход назван подходом «сверху вниз». Он сокращает объемы информации, циркулирующей между уровнями системы управления, и приводит к гораздо более эффективной системе управления.

22. Общие требования при выборе аппаратной платформы и конфигурации ИС. Причины сложности оценки конфигурации системы (аппаратных и программных средств).

Выбор аппаратной платформы и конфигурации системы представляет собой чрезвычайно сложную задачу.

• Это связано с характером прикладных систем, который в значительной степени может определять рабочую нагрузку вычислительного комплекса в целом.

• Часто оказывается просто трудно с достаточной точностью предсказать саму нагрузку, особенно в случае, если система должна обслуживать несколько групп разнородных по своим потребностям пользователей

Во-первых, как правило нагрузка на систему в среднем сглаживается особенно при наличии большого коллектива пользователей (хотя почти всегда имеют место предсказуемые пики). Например, известно, что нагрузка на систему достигает пиковых значений через 1-1.5 часа после начала рабочего дня или окончания обеденного перерыва и резко падает во время обеденного перерыва. С большой вероятностью нагрузка будет нарастать к концу месяца, квартала или года.

Во-вторых, универсальный характер большинства наиболее сложных для оценки систем - систем разделения времени, предполагает и большое разнообразие, выполняемых на них приложений, которые в свою очередь как правило стараются загрузить различные части системы.

**Почему оценка конфигурации системы так сложна? Причины:**

1. Подобная оценка прогнозирует будущее: предполагаемую комбинацию устройств, будущее использование программного обеспечения, будущих пользователей.

2. Сами конфигурации аппаратных и программных средств сложны, связаны с определением множества разнородных по своей сути компонентов системы, в результате чего сложность быстро увеличивается. Несколько лет назад существовала только одна вычислительная парадигма: мейнфрейм с терминалами. В настоящее время по выбору пользователя могут использоваться несколько вычислительных парадигм с широким разнообразием возможных конфигураций системы для каждой из них.

3. Скорость технологических усовершенствований во всех направлениях разработки компьютерной техники (аппаратных средствах, функциональной организации систем, операционных системах, ПО СУБД, ПО "среднего" слоя (middleware)) уже очень высокая и постоянно растет. Ко времени, когда какое-либо изделие широко используется и хорошо изучено, оно часто рассматривается уже как устаревшее.

4. Доступная потребителю информация о самих системах, операционных системах, программном обеспечении инфраструктуры (СУБД и мониторы обработки транзакций) как правило носит очень общий характер. Структура аппаратных средств, на базе которых работают программные системы, стала настолько сложной, что эксперты в одной области редко являются таковыми в другой.

5. Информация о реальном использовании систем редко является точной. Более того, пользователи всегда находят новые способы использования вычислительных систем как только становятся доступными новые возможности.

23. Инсталляция информационной системы. Основные этапы. Домен. Имена доменов. Отношения доменов. Модели доменов.

1. Планирование информационной системы

Перед установкой системы необходимо знать ответы на следующие вопросы:

• Какие задачи по обработке информации решает информационная система?

• Сколько и какие компьютеры используются в информационной системе?

• Как построена сеть (топология, маршрутизация и т.п.)?

• Какова политика безопасности в информационной системе?

2. Приемка систем

Необходимо задать критерии приемки новых систем и провести соответствующие испытания до их приемки. Для этого рассматриваются следующие пункты:

• требования к производительности и нагрузочной способности компьютеров;

• подготовка процедур восстановления и перезапуска систем после сбоев, а также планов действий в экстремальных ситуациях;

• подготовка и тестирование повседневных операционных процедур в соответствии с заданными стандартами;

• указание на то, что установка новой системы не будет иметь пагубных последствий для функционирующих систем, особенно в моменты пиковой нагрузки на процессоры (например, в конце месяца); • подготовка персонала к использованию новых систем.

3.Учетные записи пользователей и группы

Создание учетных записей и групп занимает важное место в обеспечении безопасности информационной системы, поскольку, назначая им права доступа, администратор получает возможность ограничить пользователей в доступе к конфиденциальной информации компьютерной сети, разрешить или запретить им выполнение в сети определенного действия, например, архивацию данных или завершение работы компьютера. Каждый пользователь сети должен иметь в одном из доменов свою учетную запись. В учетную запись заносятся имя пользователя, пароль, различные ограничения на работу в сети.

4. Имена доменов

У каждого компьютера в сети должно быть уникальное имя. Например – КОМ-1. Рекомендуется использовать не более 15 символов для имени компьютера. Если на компьютере планируется использовать выход в глобальную сеть Интернет и установлен сетевой протокол TCP/IP, то имя компьютера может содержать до 63 символов, включающих только числа 0-9, буквы A-Z, a-z и дефисы. Можно использовать и другие символы, но только если это не будет мешать другим пользователям найти компьютер в сети.

5. Отношения доменов

В сети, состоящей из двух и более доменов, каждый домен действует как отдельная сеть со своей базой данных учетных записей. Однако даже в наиболее жестко структурированной организации некоторым пользователям из одного домена могут понадобиться какие-нибудь ресурсы из другого домена. Обычное решение этой проблемы, связанной с настройкой уровней доступа пользователей между различными доменами, называется установлением доверительных отношений.

Существуют четыре модели структуры доверительных отношений между доменами.

Это модели:

• с одним доменом;

• одним главным доменом;

• несколькими главными доменами;

• полностью доверительными отношениями.

**Модель с одним доменом**

Это самая простая модель; все серверы и клиенты входят в один домен. Локальные и глобальные группы совпадают, а все администраторы могут администрировать все серверы. Поскольку домен один, нет нужды в доверительных отношениях. Сеть с одним доменом является эффективной и полезной моделью для небольшого предприятия, где не так уж много серверов и пользователей. Модель с одним доменом не подходит, если:

• пользователи используют различные наборы ресурсов и имеют различные потребности;

• предприятие разрастается и отделы располагаются в нескольких зданиях, на разных этажах или вообще далеко друг от друга;

• время, затрачиваемое на просмотр ресурсов сети, огромно.

**Модель с одним главным доменом**

Модель с одним главным доменом подходит для организации, в которой сравнительно мало пользователей и возможно логичное объединение ресурсов в группы, когда число ресурсов возрастает. Все учетные записи пользователей, а также глобальные группы создаются в главном домене. Но каждый домен подразделения может завести свои локальные группы. Первейшей функцией главного домена является централизованное ведение учетных записей. Обязательно также наличие хотя бы одного резервного контроллера домена, так как база данных всех учетных записей пользователей хранится только на основном и резервных контроллерах главного домена. Все остальные домены (домены ресурсов) действуют в основном как распорядители ресурсов. У каждого из них имеется свой набор ресурсов, которые доступны во всей сети, но могут администрироваться на месте. Модель с одним главным доменом это естественное развитие модели с одним доменом. Однако эта модель перестает быть пригодной, если число пользователей становится слишком большим. Производительность значительно снижается, так как подлинность каждой учетной записи проверяет один главный домен.

**Модель с несколькими главными доменами**

Такая модель подходит для организаций с большим числом пользователей и централизованной структурой управления. В ней обеспечивается централизованное администрирование двух и более главных доменов, а ресурсы распределены между доменами ресурсов. В этой модели имеется небольшое число главных доменов, между которыми установлены двусторонние доверительные отношения. Учетные записи пользователей хранятся в главных доменах и распределены между ними сравнительно равномерно. Делить учетные записи пользователей между главными доменами можно исходя из логического объединения пользователей в группы или чисто формально, например, по именам в алфавитном порядке. Для каждого пользователя имеется только одна учетная запись в одном из главных доменов. Все домены ресурсов доверяют каждому главному домену, но наличие доверительных отношений между доменами ресурсов совсем не обязательно. Управление ресурсами, такими как принтеры и файлы, осуществляется на уровне доменов ресурсов.

**Модель с несколькими главными доменами и полностью доверительными отношениями**

Модель с несколькими главными доменами и полностью доверительными отношениями имеет смысл в относительно небольших организациях, которые переросли модель с одним доменом, но она не подходит для случая, когда доменов становится слишком много. У каждого домена должны быть установлены двусторонние доверительные отношения со всеми остальными доменами. Таким образом, число доверительных отношений растет экспоненциально с увеличением числа доменов. Число доверительных отношений, которые требуется установить в сети с п доменами, равно п\*(п-1). Если у вас пять доменов, то понадобится двадцать доверительных отношений, добавление еще одного домена приведет к необходимости установить дополнительно десять доверительных отношений.

2 блок вопросов

1 Решения для индивидуальной и коллективной работы пользователей корпоративных информационных систем. Назначение решений: интегрированные средства коммуникаций, рабочие области коллективной деятельности, мгновенный доступ к информации и людям, автоматизация бизнес-процессов.

В настоящее время требования, предъявляемые к корпоративным информационным системам, сводятся не только к обеспечению эффективной индивидуальной работы пользователей, но и к возможности коллективной работы при условии доступа к нужной информации в любом месте и в любое время.

Поддержка индивидуальной и коллективной работы пользователей корпоративных информационных систем может быть реализована на базе следующих решений:

* интегрированные средства коммуникаций;
* рабочие области коллективной деятельности;
* мгновенный доступ к информации и людям;
* автоматизация бизнес-процессов.

***Интегрированные средства коммуникаций.*** Сотрудники предприятий для доступа к информации используют городские и сотовые телефоны, смартфоны, КПК, персональные компьютеры, ноутбуки и Internet-киоски. ИТ-инфраструктура предприятия должна обеспечивать взаимодействие всех перечисленных устройств.

Решения Microsoft упрощают и интегрируют разнообразные средства коммуникаций, доступные группам и индивидуальным сотрудникам. Электронная почта, мгновенный обмен сообщениями, голосовая почта, телефоны, мобильные устройства и средства проведения конференций через Internet объединяются унифицированным программным обеспечением. Функции такого ПО должны быть доступны независимо от места нахождения пользователей или типа сетевого соединения. Microsoft предоставляет интеллектуальное ПО, которое управляет коммуникациями, с учетом возможностей линий связи, в реальном масштабе времени. Данное программное обеспечение способствует созданию эффективных коммуникаций как внутри предприятия, так и с партнерами, поставщиками и клиентами.

***Рабочие области коллективной деятельности.*** Для поддержки коллективной работы Microsoft предлагает использовать службу Windows SharePoint Services, которая устанавливается в Microsoft Windows Server 2003. Данная служба предоставляет надежные и простые в использовании рабочие области для групп, легко интегрируется с Microsoft Windows Server, позволяя ИТ-службе создавать рабочие области коллективной работы. Эти области облегчают проведение совещаний, управление проектами, создание документов и др. Windows SharePoint Services можно интегрировать с корпоративными бизнес-приложениями и, следовательно, получать к ним доступ посредством привычного пользователю интерфейса.

***Мгновенный доступ к информации и людям.*** Корпоративным пользователям требуются эффективные средства поиска информации во множестве источников. Для решения данной задачи Microsoft предлагает использовать портальные технологии и управление контентом. С помощью функциональности MySites в SharePoint пользователи могут создавать свои сайты под личные задачи. Такой сайт является единой точкой доступа к документам пользователя, новостям, электронной почте и другим приложениям.

***Автоматизация бизнес-процессов.*** При автоматизации внутренних бизнес-процессов предприятия появляется необходимость исключения бумажного документооборота из информационных потоков. Решения Microsoft позволяют использовать привычные программы, такие как Microsoft Windows Server, для обращения к корпоративной информации и приложениям. При интеграции ERP-систем с программами Microsoft Windows Server сотрудники предприятия могут обращаться к бизнес-приложениям прямо из Microsoft Windows Server. Поддержка XML в Microsoft Windows Server предоставляет большие возможности по формированию индивидуальных схем информационных потоков и позволяет применять гибкие средства управления процессами на основе документов.

2 Основные элементы ИТ-инфраструктуры, позволяющие реализовать эффективную поддержку коллективной работы. Решения Microsoft Windows.

Основные элементы ИТ-инфраструктуры, которые позволяют реализовать эффективную поддержку коллективной работы следующие:

* Exchange Server 2007 – поддержка доступа к электронной почте и информации практически из любого места, с любого устройства и в любое время;
* технологии Microsoft Windows Server – доступные, простые в эксплуатации и масштабируемые средства поддержки коллективной работы (от совместной деятельности в рамках отдела до взаимодействия между предприятиями). Эти технологии включают Microsoft Windows Server Portal Server (SPPS) 2003 и Windows SharePoint Services (SPS):
  + Microsoft Windows Server Portal Server 2007 – надежный, масштабируемый, простой в использовании и управлении портал для поддержки коллективной работы, который служит связующим звеном между людьми и информацией. SPPS 2003, построенный на платформе Microsoft Windows Server, позволяет организациям интегрировать бизнес-процессы и приложения, а также полный набор средств персонализации и коллективной работы пользователей;
  + Microsoft Windows Server Services 2.0 позволяет создавать Web –сайты, через которые члены группы могут обмениваться документами и совместно работать над проектами;
* InfoPath 2007 – гибкое и эффективное средство создания динамических форм и их заполнения в рамках группы или организации, которое способствует успешному ведению бизнеса, расширяя возможности коллективной работы и улучшая процесс принятия решений. Информацию, собираемую с помощью InfoPath 2007, можно передавать в Web-сервисы и бизнес-приложения, так как InfoPath 2007 поддерживает любые пользовательские XML-схемы;
* ISA Server 2004 – межсетевой экран и прокси-сервер, который обеспечивает безопасный доступ к данным и защищает конфиденциальную информацию, хранящуюся в корпоративной сети;
* Microsoft Windows Server – средства работы с документами, тесно интегрированные со средствами совместной работы SharePoint;
* служба управления правами Windows (Windows Rights Management Services, WRMS) – обеспечивает надежную защиту и контроль доступа на уровне отдельных документов;
* Microsoft Windows Server Communications Server 2007 в сочетании с Office Communicator 2007 – мощное, масштабируемое корпоративное решение для мгновенного обмена сообщениями, проведения аудио- и видеоконференций по IP-сетям в режиме реального времени с функциональностью определения присутствия. Live Meeting – отдельный Web-сервис, не требующий для установки в организации выделенного сервера и позволяющий проводить конференции через Internet;
* платформа Windows Server 2003 со службой каталогов Active Directory – основа ИТ-инфраструктуры, обеспечивающей максимальную эффективность работы сотрудников.

3 Платформы для построения корпоративных порталов. Расписать (Microsoft, IBM, Oracle).

1. ***Microsoft Share Point*** представляет собой рабочую платформу для создания сайтов и корпоративных порталов, интегрированные функции которой предоставляют широкие возможности коммуникации между людьми.

• Share Point Online — облачная служба, размещенная в Microsoft и предназначенная для предприятий любых размеров. Вместо локальной установки и развертывания Share Point Server любая организация может просто подписаться на план Office 365 или отдельную службу Share Point Online, чтобы сотрудники могли создавать сайты для доступа к документам и данным совместно с коллегами, партнерами и клиентами.

• Share Point Server — организации могут развернуть систему Share Point Server и управлять ею локально. В ее состав входят все функции SharePoint Foundation, а также дополнительные функции и возможности, такие как управление корпоративным контентом, бизнес-аналитика, поиск в корпоративной среде, личные сайты и канал новостей.

• Share Point Foundation — технология Share Point Foundation, которая использовалась в качестве основы для всех сайтов Share Point, больше не предоставляется отдельно для выпуска Share Point 2016. Share Point Foundation (прежнее название — Windows Share Point Services) предлагается бесплатно для локального развертывания. Share Point Foundation можно использовать для создания сайтов различного типа, совместной работы над веб-страницами, документами, списками, календарями и данными. Share Point Foundation используется для перечисленных ниже операций:

— координирование расписаний;

— организация документов;

— участие в обсуждениях с помощью рабочих областей группы, блогов, вики-сайтов и библиотек документов.

• Share Point Designer 2013 — бесплатная программа (последний выпуск в 2013 г.) для создания функциональных решений с поддержкой рабочих процессов и редактирования внешних типов контента для работы с внешними данными на основе служб Business Connectivity Services.

• Синхронизация One Drive для бизнеса — программа для настольных систем, с помощью которой можно синхронизировать документы с сайта группы или из One Drive для бизнеса с компьютером для работы в автономном режиме.

***2. IBM Web Sphere Portal.*** Передовые портальные решения IBM способствуют повышению удобства работы с веб-приложениями, позволяют защитить и сохранить инвестиции в существующие системы, повышают производительность и создают возможности для дальнейшего роста компании.

• Максимальное удобство веб-интерфейса — можно воспользоваться всеми достижениями технологии Web 2.0 для реализации современных бизнес-моделей.

• Расширение бизнес-активов — позволяет создавать и внедрять собственные, ориентированные на потребности рынка решения на основе новых и существующих бизнес-активов, используя их повторно и меняя их назначение при необходимости.

• Повышение эффективности работы — программное обеспечение Web Sphere является проверенным, надежным, масштабируемым и высокопроизводительным фундаментом для корпоративных приложений, процессов и транзакций.

• Обеспечение развития компании — позволяет «подключать» рассчитанные на конкретные бизнес-потребности инструменты, которые ускорят получение отдачи от решения и позволят использовать новые коммерческие возможности рынка, одновременно снижая затраты на развертывание порталов.

• Новая версия продукта Web Sphere Portlet Factory содержит еще более простые шаблоны, использует новые возможности технологии Web 2.0 и поддерживает средства визуальной разработки настольных веб-приложений.

***3. Oracle Portal.*** Эффективно решает все три основные задачи, предоставляя корпоративным пользователям интуитивный доступ к необходимым данным и сервисам, а также позволяет бесшовно интегрировать корпоративные приложения.

Перечислим основные составляющие Oracle Portal:

• средства построения порталов на основе портальных компонентов;

• библиотеки готовых компонентов;

• средства управления содержанием с поддержкой коллективной работы;

• средства для сквозного полнотекстового поиска информации на портале, в интернете (Интранете), в базах данных и в хранилищах неструктурированной информации;

• средства интеграции внешних систем, приложений, различных видов источников данных;

• средства для анализа бизнес-информации (Business Intelligence);

• средства однократной регистрации и управления информационной безопасностью;

• средства поддержки мобильного беспроводного доступа;

• интегрированное средство разработки веб-приложений. Архитектура Oracle Web Center Portal состоит из следующих ключевых компонентов:

• Application Development Framework (ADF) — технология разработки приложений;

• Web Center Portal: Framework — функциональное развитие технологии ADF для специфичных функциональных требований портала;

• Web Center Portal: Spaces — готовый к использованию, предна- строенный инструмент создания порталов совместной работы;

• Web Center Portal: Services — набор социальных инструментов портала;

• Composer — инструмент создания и модификации страниц, структуры портала без программирования;

• Discussion Server — реализация форумов;

• Analytics — механизм сбора статистики работы пользователей с объектами портала;

• Activity Graph — инструмент визуализации активностей пользователей;

• Personalization Server — набор функций для выполнения задач кастомизации портального интерфейса как пользователем, так и ГГ-специалистами;

• Portals — механизм создания отдельных порталов для пользователей и групп пользователей, «портал в портале»;

• Composite Applications — среда исполнения и интеграции композитных приложений.

4 Определение БД. Определение СУБД. Расписать два уровня администрирования в СУБД. Функции администратора СУБД.

**Базой данных (БД)** называется электронное хранилище информации, доступ к которому имеет один или несколько компьютеров

**Система управления базами данных (СУБД)** – это набор программ, которые управляют структурой БД и контролируют доступ к данным, хранящимся в БД. СУБД служит посредником между пользователем и БД. Сама структура БД хранится в виде набора файлов, и единственный способ получить доступ к данным в этих файлах – через СУБД.

**Два уровня администрирования в СУБД**

Во всех СУБД различаются (хотя и называются по-разному) два уровня администрирования: системный администратор (администратор СУБД) и администраторы базы данных (БД). Одна копия программного продукта СУБД может поддерживать одновременное существование многих БД.

Разные БД могут быть связаны с разными проектами и даже с разными организациями, поэтому у каждой БД должен быть свой администратор. Функции системного администратора относятся ко всей системе в целом, его права и привилегии распространяются на все объекты и на всех субъектов в системе. Функции администратора БД относятся не только к подмножеству системных ресурсов, выделенных конкретной БД, его права и привилегии распространяются на объекты, относящиеся к данной БД, и на субъектов, имеющих к ним доступ.

**Функции администратора:**

• инсталляция СУБД - является функцией только системного администратора;

• управление памятью - Администратор должен обеспечить такое выделение памяти, чтобы с одной стороны, ее было достаточно для хранения и эффективного доступа к данным, а с другой - минимальное количество выделенной памяти оставалось неиспользованным;

• управление разделением данных между пользователями - Администратор, имея исчерпывающее представление о дисциплинах разделения, применяемых СУБД, выступает в роли консультанта прикладных программистов, сводя к минимуму взаимное блокирование приложениями друг друга;

• копирование и восстановление БД - Копирование и восстановление являются необходимыми для гарантирования сохранности данных даже при полном крахе системы;

• управление безопасностью в системе - Оно состоит в регистрации пользователей в системе, выделении пользователям привилегий и бюджетов;

• передача данных между СУБД и другими системами - .Данные, хранящиеся в БД, могут потребоваться для использования в других БД, работающих в другой инсталляции, или в приложениях, не зависящих от СУБД;

• управление производительностью - включает в себя три аспекта: настройку параметров функционирования самой СУБД, отдельных БД и отдельных приложений.

5 Какие группы пользователей СУБД выделяют? Дискреционное управление доступом. Средства дискреционной защиты в СУБД. Мандатное управление доступом. Средства мандатной защиты в СУБД.

Группы пользователей:

* Пользователи
* Администратор БД
* Разработчики и администраторы приложений

**Дискреционное управление доступом** – решение, позволяющее работать с конфиденциальными данными только лицам с определенным уровнем полномочий и закрывать доступ для остальных пользователей.

В программах дискреционное управление доступом реализуется в виде матрицы. В столбцах указываются объекты, права доступа к которым регламентируются (АРМ, базы данных, программы и приложения, удаленные устройства, Интернет), а в строках – пользователи. Для каждого из них определяется список разрешенных действий для пользователей с определенным уровнем доступа с объектами:

* чтение;
* копирование и запись;
* внесение изменений;
* выполнение (для программ);
* передача прав другим пользователям.

**Мандатное управление доступом** (mandatory access control) — это разграничение доступа субъектов к объектам данных, основанное на характеризуемой меткой конфиденциальности информации, которая содержится в объектах, и на официальном разрешении (допуске) субъектов обращаться к информации такого уровня конфиденциальности.

При этом подходе с каждым зарегистрированным в системе пользователем (субъектом) и каждым защищаемым объектом системы связывается мандат, определяющий действия, которые может выполнять данный субъект над данным объектом

6 Определение транзакции. Суть механизма транзакций? Основные уровни восстановления БД.

**транзакции** – пакет запросов, который последовательно производит изменения БД и либо принимается, если все изменения записи подтверждены, либо отвергается, если хоть один запрос завершился неуспешно.

Транзакция, по сути, это механизм, который позволяет совершать различные действия над базой данных, как единый логический блок, и который переводит базу данных из одного целостного состояний в другое. Или не переводит, если транзакция была отвергнута.

**Основные уровни восстановления БД**

1. Оперативное восстановление. Характеризуется возможностью восстановления на уровне отдельного логического элемента работы при аномальном окончании управления данными (ошибка в программе, ошибка в аргументе и т.д.).

2. Промежуточное восстановление. Если возникают аномалии в системе (системно-программные ошибки, сбой аппаратного обеспечения, не связанный с разрушением базы данных), то требуется восстановить состояние всех выполняемых логических элементов работы на момент возникновения сбоя.

3. Длительное восстановление. При разрушении базы данных в результате дефекта на диске осуществляют восстановление с помощью копии базы данных. Затем воспроизводят результаты выполненных с момента снятия копии логических элементов работы и возвращают систему в состояние на момент разрушения.

7 Языковые средства разграничения доступа. Основные команды языка SQL. Концепция и реализация механизма ролей БД.

**Языковые средства разграничения доступа. Основные команды sql**

Раздаются права командой GRANT. Права можно не только дать, но и отнять. Делается это командой REVOKE, которая является копией GRANT, только с обратным действием.

Основные команды:

Команда SELECT является основой запроса. Большинство SQL-запросов начинаются с нее

Команда WHERE позволяет использовать условие, которые может быть верным или нет для каждой записи НД

Команда ORDER BY позволяет сортировать записи по определенному полю как в возрастающем, так и в убывающем порядке

Оператор IN позволяет определить набор значений

Оператор BEETWEEN работает примерно так же, как IN, но задает не список, а диапазон значений

Оператор LIKE работает только с символьными и строковыми полями

Агрегатные функции используются в запросах SQL, чтобы из группы записей сформировать одиночное значение одного поля. Имеются следующие агрегатные функции:

AVG – Функция возвращает среднее арифметическое значение из всех значений данного поля.

MIN – Функция возвращает минимальное значение указанного поля. Синтаксис аналогичен

функции AVG.

SUM – Функция возвращает максимальное значение указанного поля. Синтаксис аналогичен

функции AVG.

COUNT – Функция возвращает общее количество строк, сформированных запросом.

Команда GROUP BY позволяет группировать записи по какому-то определенному значению, и применяется совместно с агрегатными функциями

Команда DISTINCT (Отличие) предназначена для удаления избыточных (дублирующих) данных

Команда HAVING позволяет определить условия, чтобы удалить определенные группы из полученного набора данных, точно так же как команда WHERE делает это для отдельных записей.

**Концепция и реализация механизма ролей БД.**

Когда в организации работает множество пользователей, они, как правило, разбиваются на группы. Например, несколько бухгалтеров с одинаковыми правами. Чтобы не терять время на создание одинаковых прав для нескольких пользователей, для примера, в InterBase имеется механизм ролей. При пользовании этим механизмом, существует четыре последовательности действий:

1. Создать роль.

2. Присвоить этой роли необходимые права.

3. Назначить нужным пользователям эту роль.

4. При соединении с БД указать не только имя пользователя и пароль, но и его роль.

8 Преимущества СУБД InterBase. Назначение утилиты gbak, gfix, gsec в InterBase.

**Использование встроенных механизмов InterBase имеет следующие преимущества:**

InterBase позволяет осуществлять резервное копирование БД параллельно с работой других пользователей.

Во время резервного копирования InterBase считывает каждую запись из таблиц, параллельно занимаясь «сборкой мусора», поэтому в резервной копии не останется устаревших версий записей.

Оставшиеся данные переупаковываются, то есть, резервная копия не будет содержать тех «дырок», что были в базе данных. Можно сказать, что данные дефрагментируются.

Индексы пересчитываются, что приводит к оптимизации работы базы данных.

Созданная резервная копия может быть использована для миграции базы на другие серверы (InterBase новых версий, Firebird или Yaffil), а также при восстановлении позволяет исправить некоторые параметры БД, например, размер страниц.

**Для чего нужна утилита gbak?**

Как для создания резервной копии, так и для восстановления БД InterBase предлагает утилиту командной строки gbak

**Назначение утилиты gsec в InterBase**

GSEC – это утилита командной строки, обеспечивающая интерфейс к базе данных безопасности. Вы должны иметь права SYSDBA или суперпользователя (root для Unix), чтобы использовать GSEC. Данную утилиту можно использовать в интерактивном режиме или режиме командной строки.

di[splay] Показывает информацию обо всех пользователях из базы ISC4.GDB

di[splay] name Показывает информацию о пользователе name

a[dd] name -pw passwd [option argument option argument ...] Добавляет пользователя с именем name, паролем passwd и дополнительной информацией

mo[dify] name [options] Изменяет атрибуты пользователя

de[lete] name Удаляет информацию о пользователе с именем name из ISC4.GDB

h[elp] Показывает синтаксис команд GSEC

q[uit] Завершает сеанс

**Назначение утилиты gfix**

Эта утилита является одним из основных инструментов администратора БД. Утилита gfix позволяет:

 Выполнять принудительную чистку (sweep) базы данных;

 Изменять интервал автоматической чистки;

 Закрывать базу данных для получения монопольного доступа, и затем снова открывать ее;

 Переводить базу в режимы «чтение/запись» или «только чтение»;

 Переключаться между синхронным и асинхронным вводом (Forced Writes);

 Изменять диалект БД;

 Устанавливать размер кэша;

 Отыскивать повисшие транзакции и отменять или подтверждать их;

 Активировать или удалять теневые копии;

 Производить ремонт поврежденных баз данных.

9 Преимущества создания резервных копий БД встроенными средствами СУБД. Теневые копии (shadow) БД. Основные рекомендации по ремонту БД.

**Преимущества создания резервных копий БД встроенными средствами СУБД**

Использование встроенных механизмов InterBase имеет следующие преимущества:

• InterBase позволяет осуществлять резервное копирование БД параллельно с работой других пользователей.

• Во время резервного копирования InterBase считывает каждую запись из таблиц, параллельно занимаясь «сборкой мусора», поэтому в резервной копии не останется устаревших версий записей.

• Оставшиеся данные переупаковываются, то есть, резервная копия не будет содержать тех «дырок», что были в базе данных. Можно сказать, что данные дефрагментируются.

• Индексы пересчитываются, что приводит к оптимизации работы базы данных.

• Созданная резервная копия может быть использована для миграции базы на другие серверы (InterBase новых версий, Firebird или Yaffil), а также при восстановлении позволяет исправить некоторые параметры БД, например, размер страниц.

Сервер InterBase имеет механизм теневого (shadow) копирования базы данных. Такое копирование создает «зеркало» базы данных на случай какого-либо аппаратного или сетевого сбоя, или случайного удаления или повреждения базы данных операционной системой. В этом случае имеется возможность вручную или даже автоматически перейти с основной базы данных на теневую копию, и продолжить работу системы. Однако теневое копирование ни в коем случае не может заменить резервное копирование утилитой gbak, так как все ошибки и мусор, присутствующие в основной базе данных, будут присутствовать и в ее теневой копии. Shadow – файлы являются дополнительным средством безопасности данных, но никак не панацеей от всех возможных бед. Теневые копии можно создавать и в другой папке того диска, на котором находится основная база данных, однако при этом теряются все преимущества использования shadow копий. Обычно такие копии создают на другом жестком диске, физически подключенном к серверному ПК.

**Основные рекомендации по ремонту БД**

• Прежде всего, отключите от базы всех пользователей, не позволяйте им вносить изменения в БД

• Сделайте копию рабочей базы данных средствами файловой. Все попытки восстановления делайте с полученной копией, не трогая оригинал.

• Проведите полную проверку (gfix –v –full ). Если выводятся сообщения об ошибках контрольных сумм, можно добавить переключатель –i, чтобы игнорировать эти ошибки.

• Далее можно попытаться исправить разрушенные данные, помечая их как недоступные: gfix –mend –full –ignore

• После этого вновь выполните проверку на наличие разрушенных структур , как в № 3, но без –i.

• Затем попробуйте снова выполнить резервное копирование утилитой gbak, например: gbak –b –v –i

• Если это удалось, то все хорошо. Иначе попробуйте сделать еще одно резервное копирование, добавив параметр –g (не собирать мусор). Если разрушения связаны с повисшими limboтранзакциями, то –limbo.

• В большинстве случаев, такие меры позволяют сделать нормальную резервную копию. Попробуйте восстановить ее командой gbak –create –v

10 Определение каталога и службы каталогов. Назначение и функции служб каталога. Основные службы каталогов и стандарты, используемые в современных сетях.

**Каталог** представляет собой иерархическую структуру, в которой хранятся сведения об объектах в сети.

**Служба каталогов,** например доменные службы Active Directory (AD DS), предоставляет методы хранения данных каталога и предоставления этих данных сетевым пользователям и администраторам.

**Основные функции службы каталогов.**

Централизация. Смысл централизации - уменьшение количества каталогов в сети. Включение информации обо всех сетевых ресурсах в централизованный каталог создает единственную точку управления, что упрощает администрирование ресурсов и позволяет эффективнее делегировать административные задачи.

Масштабируемость. Служба каталогов должна допускать рост сети, не создавая при этом слишком больших издержек, - то есть она должна поддерживать какой-либо способ разбиения базы данных каталога на разделы, чтобы не утратить контроль над базой данных из-за ее чрезмерного разрастания и при этом сохранить преимущества централизации.

Стандартизация. Служба каталогов должна предоставлять доступ к своей информации по открытым стандартам.

Расширяемость. Служба каталогов должна тем или иным способом позволять администраторам и приложениям расширять в соответствии с потребностями организации набор информации, хранимой в каталоге.

Разделение физической сети. Благодаря службе каталогов топология физической сети должна быть прозрачной для пользователей и администраторов.

Безопасность. Служба каталогов должна поддерживать защищенные средства хранения, управления, выборки и публикации информации о сетевых ресурсах.

**Основные службы каталогов и стандарты, используемые в современных сетях.**

Active Directory (AD) - служба каталогов, поставляемая с Microsoft Windows, начиная с Windows 2000 Server. Active Directory содержит каталог, в котором хранится информация о сетевых ресурсах и службы, предоставляющие доступ к этой информации.

Х.500 и Directory Access Protocol (DAP). X.500 - спецификация International Organization for Standardization (ISO), определяющая, как должны быть структурированы глобальные каталоги. Х.500 также описывает применение DAP для обеспечения взаимодействия между клиентами и серверами каталогов;

Lightweight Directory Access Protocol (LDAP). Протокол LDAP был разработан в ответ на критические замечания по спецификации DAP, которая оказалась слишком сложной для применения в большинстве случаев.

Novell Directory Services (NDS). Служба каталогов для сетей Novell NetWare, совместимая со стандартом Х.500;

Windows NT и SAM. Ядром Windows NT NOS (Network Operating System - сетевая операционная система) является база данных SAM (Security Accounts Management - управление безопасными учетными записями). Она представляет центральную базу данных учетных записей, включающую все учетные записи пользователей и групп в домене. Эти учетные записи используются для управления доступом к совместным ресурсам, принадлежащим любому серверу в домене Windows NT.

11 Ключевые преимущества Active Directory. Область действия, пространство имен ActiveDirectory. Объект. Контейнер. Дерево.

**Ключевые преимущества Active Directory**

**Единая точка аутентификации.** Все учетные записи хранятся в общей базе данных, к которой при авторизации обращаются все ПК, включенные в сеть. Каждый пользователь домена включается в определенную группу. Последняя имеет свой уровень доступа к документам, приложениям, хранилищу данных и т. п. в зависимости от выполняемых ею обязанностей. Новый сотрудник, принятый на работу в компанию, получает учетную запись в соответствующей группе пользователей и тот же уровень доступа. При увольнении работника его исключают из списка и блокируют возможность доступа.

**Единая точка управления.** Каталог Active Directory позволяет распределить всех пользователей и ПК согласно имеющейся иерархии отделов и филиалов. К каждому из них применяются общие групповые политики. Они заключаются в одних и тех же настройках доступа и безопасности для каждого отдела. При добавлении нового ПК или пользователя его относят в одну из групп. При этом дополнительных настроек не требуется, они применяются автоматически. Групповые политики AD позволяют назначать сетевые принтеры, настраивать офисные приложения, устанавливать уровень безопасности браузера и т. п.

**Высокий уровень защиты данных.** Службы AD помогают значительно повысить безопасность хранения информации. Высокий уровень защищенности обеспечивается двумя направлениями:

* единым хранилищем учетных записей, которые располагаются на выделенных серверах домена;
* использованием для аутентификации в доменной среде протокола Kerberos, более безопасного, чем NTLM в рабочих группах.

**Высокие возможности интеграции**. Все службы Active Directory соответствуют стандарту LDAP – «легко расширяемому протоколу доступа к каталогам». Он позволяет осуществлять аутентификацию, поиск, сравнение, а также работу с учетными записями. LDAP поддерживается, например почтовыми и прокси-серверами, а также другими приложениями, не обязательно продуктами Microsoft®. К преимуществам такой интеграции относятся единые логин и пароль для всех приложений, с которыми работает пользователь. Это дает возможность подключаться и аутентифицироваться по корпоративным точкам доступа по Wi-Fi или внешнему VPN.

**Область действия, пространство имен Active Directory.**

Область действия (scope) Active Directory достаточно обширна. Она может включать отдельные сетевые объекты (принтеры, файлы, имена пользователей), серверы и домены в отдельной глобальной сети. Она может также охватывать несколько объединенных сетей. Active Directory может быть настроена на управление как отдельным компьютером, так и компьютерной сетью или группой сетей.

Пространство имен – это такая ограниченная область, в которой может быть распознано данное имя. Распознавание имени заключается в его сопоставлении с некоторым объектом или объемом информации, которому это имя соответствует. Active Directory образует пространство имен, в котором имя объекта в каталоге может быть поставлено в соответствие самому этому объекту.

**Объект. Контейнер. Дерево.**

**Объект** представляет собой уникальную сущность внутри Каталога и обычно обладает многими атрибутами, которые помогают описывать и распознавать его.

**Контейнер** – объект, содержащий другие объекты.

**Дерево** содержит один или несколько доменов, также связанных в иерархию транзитивными отношениями доверия.

12 Домен. Доменное дерево. Лес. Организационные единицы. Сайт, узел.

**Домен** формирует область административной ответственности. База данных домена содержит учетные записи пользователей, групп и компьютеров. Большая часть функций по управлению службой каталогов работает на уровне домена (аутентификация пользователей, управление доступом к ресурсам, управление службами, управление репликацией, политики безопасности).

**Дерево** является набором доменов, которые используют единое связанное пространство имен. В этом случае "дочерний" домен наследует свое имя от "родительского" домена. Дочерний домен автоматически устанавливает двухсторонние транзитивные доверительные отношения с родительским доменом. Доверительные отношения означают, что ресурсы одного из доменов могут быть доступны пользователям других доменов.

**Лес** объединяет деревья, которые поддерживают единую схему. В лесу между всеми доменами установлены двухсторонние транзитивные доверительные отношения, что позволяет пользователям любого домена получать доступ к ресурсам всех остальных доменов, если они имеют соответствующие разрешения на доступ. По умолчанию, первый домен, создаваемый в лесу, считается его корневым доменом, в корневом домене хранится схема AD.

**Организационные единицы OU** – это объекты в Active Directory, которые могут определяться пользователем и к которым может применяться групповая политика.

**Сайт** представляет область сети, где все контроллеры домена связаны быстрым, недорогим и надежным сетевым подключением.

**Узлом** (сайтом) называется такой элемент сети, который содержит серверы Active Directory. Узел обычно определяется как одна или несколько подсетей, поддерживающих протокол TCP/IP и характеризующихся хорошим качеством связи, которое подразумевает высокую надежность и скорость передачи данных.

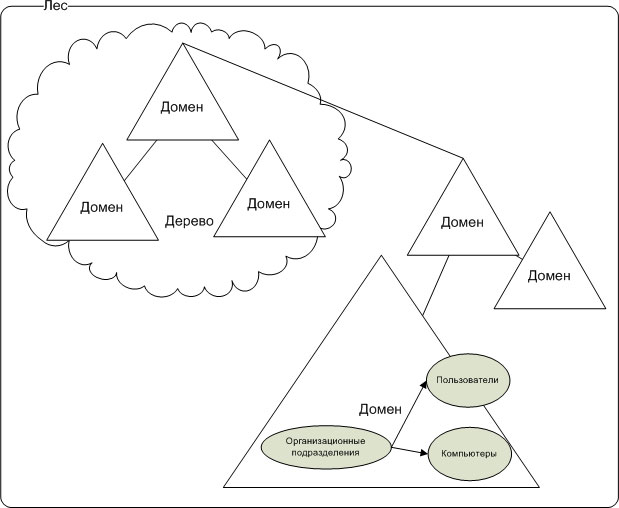
13 Функциональная структура Active Directory. Физическая структура Active Directory. Логическая структура Active Directory.

**Функциональная структура AD. Многоуровневая архитектура AD.**

Функциональную структуру Active Directory можно представить в виде многоуровневой архитектуры, в которой уровни являются процессами, предоставляющими клиентским приложениям доступ к службе каталога. Active Directory состоит из трех уровней служб и нескольких интерфейсов и протоколов, совместно работающих для предоставления доступа к службе каталога. Три уровня служб охватывают различные типы информации, необходимой для поиска записей в базе данных (БД) каталога. Выше уровней служб в этой архитектуре находятся протоколы и API интерфейсы, осуществляющие связь между клиентами и службой каталога.



**Логическая структура Active Directory** является моделью службы каталога, которая определяет каждого участника безопасности на предприятии, а также организацию этих участников.



**Физическое проявление службы Active Directory** состоит в наличии отдельного файла данных, расположенного на каждом контроллере домена. Физическая реализация службы Active Directory описывается местоположением контроллеров домена, на которых расположена служба. При реализации службы Active Directory можно добавлять столько контроллеров доменов, сколько необходимо для поддержания служб каталога в данной организации.

14 Какие сведения собираются на этапе предпроектного исследования для проектирования службы каталогов. Типовой план проектирования структуры ActiveDirectory. Какие объекты содержит БД ActiveDirectory.

**Какие сведения собираются на этапе предпроектного исследования для проектирования службы каталогов**

1. На данном этапе предпроектного исследования собираются основные сведения по существующей инфраструктуре в компании.
2. Для планирования структуры Active Directory - информация о доменной структуре и ее типе, структуре групп пользователей и распределении их по доменам, количестве существующих контроллеров доменов внутри каждого домена. Определение существующих доверительных отношений между доменами, односторонних и двухсторонних доверительных отношений и доменов, которые не должны включаться в леса Active Directory, пространства имен DNS, существующих в организации, и перечня существующих доменных имен организации, зарегистрированных в сети Интернет.
3. Для планирования сайтов Active Directory - информация о существующей структуре сайтов, о топологии сети, о каналах связи и их пропускной способности.
4. Для планирования переноса текущей структуры сетевых сервисов на платформу Active Directory - информация о топологии используемых сетевых сервисов DHCP, WINS, DNS.
5. Для обеспечения возможности резервного восстановления данных во время миграции - схема резервного копирования информации.
6. Для определения возможной расширяемости решения - исследование возможных вариантов изменения схемы при росте организации или ее реорганизации, определение области Active Directory (исследование подразделений, включая удаленные филиалы организации, необходимых для включения в Active Directory).
7. Для планирования миграции приложений, использующих Active Directory - список приложений, связанных с Active Directory, и возможных ограничений, накладываемых ими на структуру Active Directory, определение механизмов идентификации пользователей.

**Типовой план проектирования структуры Active Directory.**

Проектирование структуры Active Directory начинается с компонентов высшего уровня, а затем проектируются компоненты низших уровней. Это означает, что первый шаг состоит в создании проекта леса, затем следует проект доменов, проект DNS и, наконец, проект организационной единицы (OU)

Планирование структуры лесов

Планирование доменов для каждого леса

Планирование использования сайтов для каждого леса

Планирование структуры организационных единиц для каждого домена

Планирование реорганизации существующих доменов и их перевод на новую платформу Active Directory

Тестирование внедряемых решений и установка стенда

**Какие объекты содержит БД AD**

1. Разделы (сегменты). Разделы Active Directory называются контекстами именования (NC - Naming Contexts) и содержат следующие сегменты: раздел домена каталога, раздел конфигурации каталога, раздел схемы каталога, раздел глобального каталога, разделы приложений каталога.
2. Домены. Домен служит в качестве административной границы, он определяет и границу политик безопасности. Каждый домен имеет, по крайней мере, один контроллер домена (оптимально иметь два или более). Домены Active Directory организованы в иерархическом порядке. Первый домен на предприятии становится корневым доменом леса, обычно он называется корневым доменом или доменом леса.
3. Деревья доменов. Домены, которые создаются в инфраструктуре Active Directory после создания корневого домена, могут использовать существующее пространство имен Active Directory совместно или иметь отдельное пространство имен. Чтобы выделить отдельное пространство имен для нового домена, нужно создать новое дерево домена.
4. Леса. Лес определяет границу безопасности для предприятия, являясь общим для всех контроллеров домена в лесу. Все домены и доменные деревья существуют в пределах одного или несколько лесов Active Directory.
5. Сайты. Сайт представляет область сети, где все контроллеры домена связаны быстрым, недорогим и надежным сетевым подключением. Независимость логических компонентов от сетевой инфраструктуры возникает вследствие использования сайтов в Active Directory: они обеспечивают соединение между логическими компонентами Active Directory и физической сетевой инфраструктурой.
6. Организационные единицы. Организационные единицы предназначены для того, чтобы облегчить управление службой Active Directory. Они служат для создания иерархической структуры в пределах домена и используются, чтобы сделать более эффективным управление единственным доменом (вместо управления несколькими доменами Active Directory).

15 Доверительные отношения между доменами. Типы доверительных отношений. Контроллеры доменов, функции контроллера домена, их роли.

**Домен. Доверительные отношения. Типы доверительных отношений.**

Домен — это единая область, в пределах которой обеспечивается безопасность данных в компьютерной сети под управлением ОС Windows

Поскольку домены разграничивают зоны безопасности, специальный механизм, называемый доверительными отношениями (trust relationships), позволяет объектам в одном домене [доверяемом (trusted domain)] обращаться к ресурсам в другом [доверяющем (trusting domain)].

**Типы доверительных отношений:**

Доверие к родительскому и дочернему доменам

Доверие к корневому домену дерева

Доверие к внешнему домену

Доверие к сокращению

Доверие к сфере

Доверие к лесу

**Контроллеры доменов и их роли**

Контроллер домена — это компьютер-сервер, управляющий доменом и хранящий реплику каталога домена (локальную БД домена). Поскольку в домене может быть несколько контроллеров домена, все они хранят полную копию той части каталога, которая относится к их домену.

Каждый контроллер домена хранит полную копию всей информации Active Directory, относящейся к его домену, а также управляет изменениями этой информации и реплицирует их на остальные контроллеры того же домена.

Все контроллеры в домене автоматически реплицируют между собой все объекты в домене. Какие-либо изменения, вносимые в Active Directory, на самом деле производятся на одном из контроллеров домена. Затем этот контроллер домена реплицирует изменения на остальные контроллеры в пределах своего домена. Задавая частоту репликации и количество данных, которое Windows будет передавать при каждой репликации, можно регулировать сетевой трафик между контроллерами домена.

Важные обновления, например отключение учетной записи пользователя, контроллеры домена реплицируют немедленно.

Active Directory использует репликацию с несколькими хозяевами (multimaster replication), в котором ни один из контроллеров домена не является главным. Все контроллеры равноправны, и каждый из них содержит копию базы данных каталога, в которую разрешается вносить изменения. В короткие периоды времени информация в этих копиях может отличаться до тех пор, пока все контроллеры не синхронизируются друг с другом.

Наличие в домене нескольких контроллеров обеспечивает отказоустойчивость. Если один из контроллеров домена недоступен, другой будет выполнять все необходимые операции, например записывать изменения в Active Directory.

Контроллеры домена управляют взаимодействием пользователей и домена, например находят объекты Active Directory и распознают попытки входа в сеть.

Хозяин схемы (Schema Master). Первый контроллер домена в лесу принимает роль хозяина схемы и отвечает за поддержку и распространение схемы на остальную часть леса. Он поддерживает список всех возможных классов объектов и атрибутов, определяющих объекты, которые находятся в Active Directory. Если схему нужно обновлять или изменять, наличие Schema Master обязательно.

Хозяин именования доменов (Domain Naming Master). Протоколирует добавление и удаление доменов в лесу и жизненно необходим для поддержания целостности доменов. Domain Naming Master запрашивается при добавлении к лесу новых доменов. Если Domain Naming Master недоступен, то добавление новых доменов невозможно; однако при необходимости эта роль может быть передана другому контроллеру.

Хозяин RID (Relative Identifier (RID) Master). Отвечает за выделение диапазонов относительных идентификаторов (RID) всем контроллерам в домене. SID в Windows Server 2003 состоит из двух частей. Первая часть - общая для всех объектов в домене; для создания уникального SID к этой части добавляется уникальный RID. Вместе они уникально идентифицируют объект и указывают, где он был создан.

Эмулятор основного контроллера домена (Primary Domain Controller (PDC) Emulator). Отвечает за эмуляцию Windows NT 4.0 PDC для клиентских машин, которые еще не переведены на Windows 2000, Windows Server 2003 или Windows XP и на которых не установлен клиент службы каталогов. Одна из основных задач эмулятора PDC - регистрировать устаревшие клиенты. Кроме того, к эмулятору PDC происходит обращение, если аутентификация клиента оказалась неудачной. Это дает возможность эмулятору PDC проверять недавно измененные пароли для устаревших клиентов в домене, прежде чем отклонять запрос на вход.

Хозяин инфраструктуры (Infrastructure Master). Регистрирует изменения, вносимые в контролируемые объекты в домене. Обо всех изменениях сначала сообщается Infrastructure Master, и лишь потом они реплицируются на другие контроллеры домена. Infrastructure Master обрабатывает информацию о группах и членстве в них для всех объектов в домене. Еще одна задача Infrastructure Master - передавать информацию об изменениях, внесенных в объекты, в другие домены.

**функции контроллеров доменов:**

Каждый контроллер домена хранит полную копию всей информации Active Directory, относящейся к его домену, а также управляет изменениями этой информации и реплицирует их на остальные контроллеры того же домена.

Все контроллеры в домене автоматически реплицируют между собой все объекты в домене.

Важные обновления, например отключение учетной записи пользователя, контроллеры домена реплицируют немедленно.

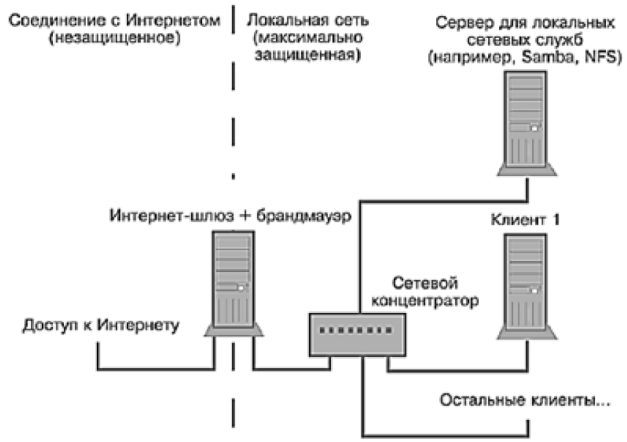
Active Directory использует репликацию с несколькими хозяевами (multimaster replication), в котором ни один из контроллеров домена не является главным.

Наличие в домене нескольких контроллеров обеспечивает отказоустойчивость.

Контроллеры домена управляют взаимодействием пользователей и домена, например находят объекты Active Directory и распознают попытки входа в сеть.

16 Брандмауэры. Определение, общая информация, схема работы, Demilitarized Zone.

Под брандмауэром будем понимать совокупность методов, повышающих надежность обмена информацией, проходящей по TCP/IP через фильтр пакетов. Такой фильтр анализирует все сетевые пакеты, приходящие на компьютер, а также пакеты, которые уходят с компьютера в сеть. В зависимости оттого, все ли правила соблюдаются, пакеты могут быть пропущены или заблокированы.



Demilitarized Zone – сегмент сети, содержащий общедоступные сервисы и отделяющий их от частных. В качестве общедоступного может выступать, например, веб-сервис: обеспечивающий его сервер, который физически размещён в локальной сети (Интранет), должен отвечать на любые запросы из внешней сети (Интернет), при этом другие локальные ресурсы (например, файловые серверы, рабочие станции) необходимо изолировать от внешнего доступа.

Цель ДМЗ – добавить дополнительный уровень безопасности в локальной сети, позволяющий минимизировать ущерб в случае атаки на один из общедоступных сервисов: внешний злоумышленник имеет прямой доступ только к оборудованию в ДМЗ.

17 Методы виртуализации операционных системы. Характеристика метода, примеры фирм и программ.

Виртуализация — это общий термин, охватывающий абстракцию ресурсов для многих аспектов вычислений. Некоторые наиболее характерные примеры виртуализации приведены ниже.

***Паравиртуализация***

Паравиртуализация — техника виртуализации, при которой гостевые операционные системы подготавливаются для исполнения в виртуализированной среде, для чего их ядро незначительно модифицируется. Операционная система взаимодействует с программой гипервизора, который предоставляет ей гостевой API, вместо использования напрямую таких ресурсов, как таблица страниц памяти. Код, касающийся виртуализации, локализуется непосредственно в операционную систему. Паравиртуализация требует, чтобы гостевая операционная система была изменена для гипервизора, и это является недостатком этого метода, так как подобное изменение возможно лишь в случае, если гостевые ОС имеют открытые исходные коды, которые можно модифицировать согласно лицензии. �В то же время паравиртуализация предлагает производительность почти как у реальной невиртуализированной системы, а также возможность одновременной поддержки различных операционных систем, как и при полной виртуализации.

***Виртуализация инфраструктуры***

В данном случае, будем понимать под этим термином создание ИТ-инфраструктуры, не зависимой от аппаратной части. Например, когда нужный нам сервис находится на гостевой виртуальной машине и нам в принципе не особо важно, на каком физическом сервере он располагается.

Виртуализация серверов, десктопов, приложений – существует множество методов для создания подобной независимой инфраструктуры. В этом случае на одном физическом или хост-сервере посредством специального ПО, именуемого "гипервизор", размещается несколько виртуальных или "гостевых" машин.

Современные системы виртуализации, в частности, VMware и Citrix XenServer в большинстве своем работают по принципу bare metal, то есть ставятся прямо на "голое железо".

Виртуальная система, построена не на bare metal гипервизоре, а на сочетании операционной системы Linux CentOS 5.2 и VMware Server на базе серверной платформы Intel SR1500PAL, 2 процессора Intel Xeon 3.2/1/800, 4Gb RAM, 2xHDD 36Gb RAID1 и 4xHDD 146Gb в RAID10 общим объемом 292Gb. На хост-машине размещены четыре виртуальные машины:

* почтовый сервер Postfix на базе операционной системы FreeBSD (Unix). Для доставки почты конечному пользователю использовался протокол POP3.
* прокси-сервер Squid на базе все той же системы FreeBSD.
* выделенный контроллер домена, DNS, DHCP на базе Windows 2003 Server Standard Edition.
* управляющая рабочая станция на базе Windows XP для служебных целей.

***Виртуализация серверов***

Виртуальная машина — это окружение, которое представляется для «гостевой» операционной системы, как аппаратное. Однако на самом деле это программное окружение, которое симулируется программным обеспечением хостовой системы. Эта симуляция должна быть достаточно надёжной, чтобы драйверы гостевой системы могли стабильно работать. При использовании паравиртуализации, виртуальная машина не симулирует аппаратное обеспечение, а, вместо этого, предлагает использовать специальное Application Programming Interface (API).

Bochs

FAUmachine

KVM

Parallels (Параллелз Софтвер)

Qemu

SVISTA

twoOStwo

VirtualBox

Virtual Iron

Microsoft Virtual PC

Microsoft Virtual Server

VMware (VMware ESX Server)

Xen

Аналитики Gartner отмечают: «Виртуализация х86 серверной инфраструктуры выступает отправной точкой для двух важнейших современных отраслевых тенденций – модернизации инфраструктуры и облачных вычислений». Более того, «она коренным образом меняет подход предприятий к развертыванию, управлению и предоставлению IT». Исследователи убеждены, что «виртуализация х86 серверной инфраструктуры является сейчас ключевым направлением развития информационных технологий, делая стратегическое развитие серверной виртуализации в сторону облачных вычислений более очевидным для IT-директоров крупных предприятий».

***Виртуализация уровня ОС***

Виртуализация на уровне операционной системы — виртуализирует физический сервер на уровне ОС, позволяя запускать изолированные и безопасные виртуальные серверы на одном физическом сервере.

Solaris Containers/Zones

FreeBSD Jail

Linux-VServer

FreeVPS

OpenVZ

Virtuozzo (Parallels) Виртуоззо Рисерч

VDSmanager

***Виртуализация ресурсов***

Разделение ресурсов (partitioning) — это разделение единого, обычно достаточно большого для этого, ресурса (например дисковое пространство или пропускной канал сети) на некоторое количество меньших, легче используемых ресурсов того же типа.

Например, к реализации разделения ресурсов можно отнести Проект Crossbow, позволяющий создавать несколько виртуальных сетевых интерфейсов на основе одного физического.

Агрегация, распределение или добавление множества ресурсов в большие ресурсы или объединение ресурсов. Например, симметричные мультипроцессорные системы объединяют множество процессоров; RAID и дисковые менеджеры объединяют множество дисков в один большой логический диск; RAID и сетевое оборудование использует множество каналов, объединённых так, чтобы они представлялись, как единый широкополосный канал. На мета-уровне компьютерные кластеры делают все вышеперечисленное. Иногда сюда же относят сетевые файловые системы абстрагированные от хранилищ данных на которых они построены, например, Vmware VMFS, Solaris ZFS, NetApp WAFL

***Виртуализация приложений***

Виртуализация прикладных приложений — включает в себя рабочую среду для локально выполняемого приложения, использующего локальные ресурсы. Виртуализируемое приложение запускается в небольшом виртуальном окружении, которое включает в себя ключи реестра, файлы и другие компоненты, необходимые для запуска и работы приложения. Такая виртуальная среда работает как прослойка между приложением и операционной системой, что позволяет избежать конфликтов между приложениями. К виртуализации прикладных приложений можно отнести такие системы как Softgrid и Thinstall.

18 Модель управления для администрирования сетевых систем FCAPS.

(F) Fault Management (управление отказами) - обнаружение отказов в устройствах сети, сопоставление аварийной информации от различных устройств, локализация отказов и инициирование корректирующих действий.

(С) Configuration Management (управление конфигурированием) - возможность отслеживания изменений, конфигурирования, передачи и установки программного обеспечения на всех устройствах сети.

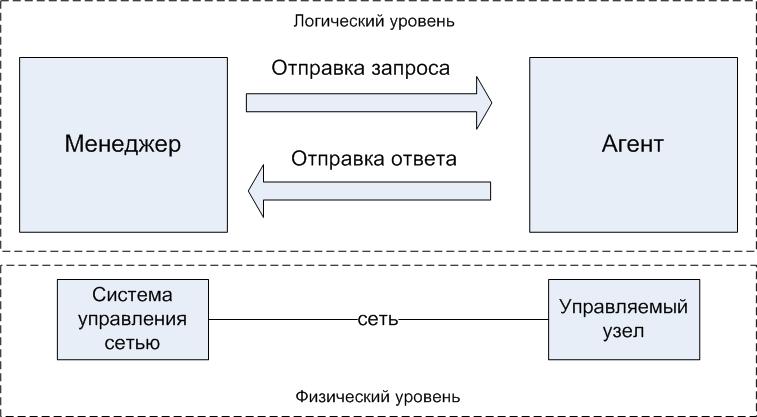
(A) Accounting Management (управление учетом) - возможность сбора и передачи учетной информации для генерации отчетов об использовании сетевых ресурсов.

(Р) Performance Management (управление производительностью) - непрерывный источник информации для мониторинга показателей работы сети (QoS, ToS) и распределения сетевых ресурсов.

(S) Security Management (управление безопасностью) - возможность управления доступом к сетевым ресурсам.

19 Системы управления MS (Management System), NMS (Network Management System). Схема работы NMS.

Системы управления сетью - Network Management System (NMS) являются системами, реализующими уровень NML модели TMN. Физически NMS представляет собой комбинацию программного обеспечения с аппаратной частью, на которой это программное обеспечение имеет серверную часть.



20 Базовая модель поиска ошибок при администрировании ИС.

1. Убедиться в том, что ошибки действительно есть. Другими словами, после сообщения пользователя о некорректной работе ИС надо убедиться в том, что этот пользователь выполняет все процедуры корректно и правильно оценивает работу ИС. Например, некая операция действительно занимает много времени, а пользователь считает, что ИС медленно работает.
2. Провести инвентаризацию. Это означает, что необходимо выяснить, все ли части ИС на месте: все кабели существуют, все части ИС взаимодействуют и правильно соединены. При этом NMS может помочь провести автоматический опрос параметров работы оборудования и программного обеспечения, дать план системы. У администратора системы должна быть исполнительная документация по ИС с картой сети и списками всех параметров загрузки серверов, рабочих станций, коммутационного оборудования (worksheet). Нужно убедиться в том, что «все на месте» и соответствует документации.
3. Сделать копии ИС (backup). Причем желательно это делать «быстрыми средствами» (например, не утилитой копирования СУБД, а утилитами ОС «том в том» или «диск в диск»).
4. Сделать перезагрузку всех компонент ИС (restart). Есть два режима перезагрузки: холодный режим (с отключением питания) и горячий режим (без отключения питания). При холодном рестарте заново загружается все ПО оборудования, все драйверы, все процессы ОС и СУБД, заново инициализируется память серверов. Поэтому при ошибочных ситуациях надо использовать холодный рестарт. Однако если есть ошибки оборудования, то оно после этого может вообще не загрузиться. Перед перезагрузкой нужна не забыть завершить работу всех процессов различных ОС и СУБД (обычно команды типа Down или Shutdown).
5. После перезагрузки необходимо упростить работу ИС, например, завершить работу всех резидентных программ, не обязательных для работы в простейшем варианте ИС.
6. Если система загрузилась, нужно проверить права и привилегии работающих пользователей (например, одно приложение запускается и работает нормально с данными правами пользователя, а другое нет).
7. Надо убедиться, что версии программного обеспечения являются текущими. Следует работать не на последней версии продуктов, а на стабильной, хорошо отлаженной. Нужно убедиться в том, что никто из пользователей не поставил себе никаких обновлений программного обеспечения. Хотя при правильных действиях АС и NMS такой возможности у пользователя не должно быть.
8. Только после всех перечисленных действий надо собирать информацию об ошибке. Для этого следует проанализировать журналы ИС (логи). Выявить симптомы проблемы, а также тех, кто был ею затронут, проанализировать использование процессов во время возникновения ошибки, изменения, произошедшие в системе, после которых появились сообщения об ошибке в журналах
9. Необходимо разработать план по изоляции ошибки. Для этого строятся гипотезы о причинах ошибки в ИС. Это могут быть ошибки каналов связи (80% всех ошибок), аппаратные ошибки, ошибки системного программного обеспечения, прикладного программного обеспечения. Всегда следует учитывать, что тираж аппаратных средств больше, чем тираж программных продуктов. Например, процессоров Intel выпускается больше, чем установок какой-либо одной ОС, поэтому аппаратных ошибок будет меньше, чем программных Аналогично тираж системного программного обеспечения больше, чем тираж прикладного ПО, поэтому в первом меньше ошибок, чем в последнем. Просто чем больше тираж продукта, тем лучше он отлажен.
10. После разработки плана по изоляции ошибки следует ранжировать гипотезы по вероятности их подтверждения. Начинать проверку целесообразно не с самой вероятной гипотезы, а с той, которую можно быстрее всего проверить. Тем самым можно быстро отсечь часть гипотез и сузить процесс проверки.
11. Затем гипотезы проверяются по очереди (строго по одной в единицу времени), в определенной последовательности. В восходящем направлении — от рабочей станции к коммутационной аппаратуре или серверу либо в нисходящем направлении — от сервера или коммутационной аппаратуры к рабочей станции. Для проверки используются только специальные проверенные версии программныхпродуктов, специальные тестовые кабели и проверенные надежные тестовые диагностические средства.
12. Наконец, последним действием является документирование проблемы и способа ее решения в специальном журнале. Обязательно должны быть созданы инструкции службам администратора системы по действиям, предотвращающим повторное появление проблемы.

21 Стратегии определения ошибок при администрировании ИС. Два подхода к поиску неисправностей. Типы стратегий. Технологии работы NMS.

***Существуют два подхода к поиску неисправностей - теоретический и практический.***

При ***теоретическом*** подходе специалист-теоретик анализирует ситуацию до тех пор, пока не будет найдена точная причина ошибки. При таком решении, например, сетевой проблемы требуется современный высокопроизводительный протокольный анализатор для набора и анализа огромного количества сетевого трафика в течение значительного времени. Затем сетевому специалисту необходим длительный теоретический анализ данных Этот процесс надежен, однако не многие компании могут себе позволить, чтобы их ИС или сеть не функционировала в течение нескольких часов или даже дней.

При ***практическом*** подходе опыт специалиста-практика подсказывает, что при возникновении неисправности целесообразно начинать менять сетевые платы, кабели, аппаратные средства и программное обеспечение до тех пор, пока система не начнет работать. Это вовсе не означает, что все компоненты системы функционируют должным образом, главное, что они вообще функционируют. К сожалению, во многих руководствах по эксплуатации в разделе поиска неисправностей фактически рекомендуется прибегнуть к стилю специалиста-практика, вместо предоставления подробной инструкции по устранению технических неисправностей. Этот подход быстрее предыдущего. Однако он очень ненадежен и первопричина неработоспособности системы может быть так и не устранена.

Стратегия управления ошибками может быть ***проактивной*** либо ***реактивной***. С ростом объема ИС возрастает потребность в ее надежности и, соответственно, возрастает потребность в предварительном мониторинге производительности системы, предупреждениях пользователям о возможных проблемах, постоянной бдительности администратора системы. Такая стратегия предупреждения ошибок называется ***проактивной***. Стратегия, при которой АС не предупреждает появление ошибок, а разбирается с ошибками по мере их возникновения, называется ***реактивной***. АС должен приложить усилия и воспользоваться средствами MS или NMS для перехода от реактивной стратегии к проактивной.

***При этом возможны две технологии работы NMS - пассивная и активная.***

***Пассивная технология.*** С помощью протокола SNMP устройства оповещают управляющую систему о выполнении заранее предусмотренного и заданного параметрами системы условия, например, отличие какого-либо параметра от номинального значения. Эта технология должна применяться администратором системы при идентификации проблем, не связанных с аппаратными сбоями, например, при изменении производительности, проблемах интерфейсов и т. д.

***Активная технология.*** Система NMS тестирует ИС (например, с помощью утилиты PING) и опрашивает каждое из устройств на регулярной основе. Если какое-либо устройство не реагирует в заданный администратором системы интервал времени или его параметры отличаются от желаемых, посылается сообщение администратору системы о сбое устройства.

3 блок вопросов

1. Системы HelpDesk. Системы ServiceDesk.

В ИТ инфраструктуре для максимально быстрой ликвидации проблем – аварий, проблем с оборудование, и тд. создаются специальные отделы, которые контактируют с сотрудниками и согласовывают ликвидацию проблем с ИТ подразделеним. Этот отдел может называться Центр обслуживания пользователей (Service Desk) или Центр поддержки пользователей (Help Desk).

Задачей Service Desk является регистрация заявок пользователей, предоставление им требуемой помощи и привлечение сотрудников ИТ подразделения для скорейшего устранения проблем. Дополнительно эта служба анализирует статистику инцидентов и время их устранения. Это необходимо для оценки и повышения качества предоставления ИТ услуг.

ServiceDesk, помимо решения инцидентов, также управляет запросами на обслуживание (о предоставлении новых услуг) и запросами о предоставлении информации (отвечает на вопросы «как мне это сделать?»).

Help desk – более узкое понятие, это инструмент технической поддержки пользователей.

Helpdesk появилась как ИТ-ориентированная служба для решения внутренних проблем, а ServiceDesk – услугоориентированная служба, которая развивает концепцию предоставления ИТ как услуг бизнесу. Причем услуги не только ИТ-услуги, ServiceDesk может выполнять функцию общего центра обслуживания для приема и обработки запросов в хозяйственную, финансовую или юридическую службу организации.

1. Протоколы POP3, IMAP, SMTP. Методы шифрования SSL, TLS. Форматы почтовых сообщений.

Post Office Protocol Version 3 - протокол почтового отделения, версия 3 — это сетевой протокол, используемый почтовым клиентом для получения сообщений электронной почты с сервера. Обычно используется в паре с протоколом SMTP. По умолчанию использует TCP-порт 110.

После установки соединения протокол РОР3 проходит три последовательных состояния

* Авторизация клиент проходит процедуру аутентификации
* Транзакция клиент получает информацию о состоянии почтового ящика, принимает и удаляет почту.
* Обновление сервер удаляет выбранные письма и закрывает соединение.

IMAP (англ. Internet Message Access Protocol) – интернет-протокол прикладного уровня для доступа к электронной почте.

IMAP предоставляет пользователю богатые возможности для работы с почтовыми ящиками, находящимися на центральном сервере. Почтовая программа, использующая этот протокол, получает доступ к хранилищу корреспонденции на сервере так, как будто эта корреспонденция расположена на компьютере получателя. Электронными письмами можно манипулировать с компьютера пользователя (клиента) без необходимости постоянной пересылки с сервера и обратно файлов с полным содержанием писем.

SMTP (Simple Mail Transfer Protocol) – это сетевой протокол, предназначенный для передачи электронной почты в сетях TCP/IP, причем передача должна быть обязательно инициирована самой передающей системой.

TLS ( англ. Transport Layer Security) — криптографический протокол, обеспечивающий безопасную передачу данных между пользователями в сети Интернет. TLS-протокол основан на Netscape SSL-протоколе версии 3.0 и состоит из двух частей — TLS Record Protocol и TLS Handshake Protocol. Различие между SSL 3.0 и TLS 1.0 незначительные.

SSL (англ. Secure Sockets Layer — протокол защищённых сокетов) — криптографический протокол, обеспечивающий безопасную передачу данных по сети Интернет. При его использовании создаётся защищённое соединение между клиентом и сервером.

1. Реестр Windows. Планировщик заданий. Настройка сети в Windows. Службы ОС в Windows.

Реестр Windows (англ. Windows Registry), или системный реестр — иерархически построенная база данных параметров и настроек в большинстве операционных систем Microsoft Windows.

Реестр содержит информацию и настройки для аппаратного обеспечения, программного обеспечения, профилей пользователей, предустановки. Большинство изменений в Панели управления, ассоциации файлов, системные политики, список установленного ПО фиксируются в реестре.

Планировщик заданий (англ. Task Scheduler) — компонент Microsoft Windows, который предоставляет возможность запланировать запуск программ или скриптов в определённые моменты времени или через заданные временные интервалы. Компонент впервые появился в Windows 95 Plus! pack под названием System Agent, но был переименован в Task Scheduler в Windows 98.

Настройка локальной сети для ОС Windows:

1. Настройка IP
   1. Через встроенный поиск найти и открыть утилиту «Параметры».
   2. Выбрать пункт «Сеть и Интернет», зайти в раздел Ethernet или Wi-Fi.
   3. Щелкнуть на названии текущего сетевого подключения.
   4. Прокрутить окно вниз до раздела «Параметры IP».
   5. Изменить значение с «Автоматически (DHCP)» на вручную.
   6. Включить режим IPv4 или IPv6 в зависимости от задачи.
   7. Внести IP-адрес, длину префикса подсети и шлюз.
2. Настройка локальной сети
   1. На всех релизах Windows используется следующая команда – **sysdm.cpl**.
   2. В открывшемся окне нужно нажать кнопку «Изменить» и внести выбранные наименования, а после подтвердить их кликом «ОК» в обеих вкладках. После перезагрузки техника гарантированно войдет в общую рабочую группу и сможет обмениваться файлами, подключаться к сетевым устройствам и использовать их функционал.

Службы Windows – это, в основном, приложения, которые работают в фоновом режиме и предлагают свои «услуги». Эти службы выполняют большинство основных функций Windows, например подключение к внешним устройствам или создание стабильного подключения к Интернету.

1. Язык сценариев Power Shell. Командлеты в PowerShell. Примеры. Конвейер в PowerShell. Примеры.

PowerShell — это кроссплатформенная система для автоматизации задач и управления конфигурацией, состоящая из оболочки командной строки и языка сценариев. В отличие от большинства оболочек, которые принимают и возвращают текст, PowerShell построена на основе общеязыковой среды выполнения (CLR) .NET и принимает и возвращает объекты .NET. Это фундаментальное отличие, которое подразумевает использование совершенно новых средств и методов автоматизации.

С помощью Windows PowerShell можно:

• Получать доступ к файловой системе;

• Управлять реестром;

• Управлять службами;

• Управлять процессами;

• Настраивать операционную систему;

• Устанавливать программное обеспечение;

• Устанавливать роли и компоненты сервера;

• Осуществлять администрирование и конфигурирование ролей и компонентов сервера;

• Писать и использовать сценарии для автоматизации управления и администрирования;

• Выполнять другие задачи системных администраторов.

Командлет (cmdlet) – это команда Windows PowerShell, с помощью которой можно осуществлять взаимодействие с объектами операционной системы с целью их управления. Данные команды являются частью языка PowerShell. Командлеты построены по принципу «Глагол-Существительное», разделенные дефисом (-).

Полный список командлетов в Windows PowerShell можно посмотреть с помощью специального командлета Get-Command.

Пример командлета

Get-CimInstance – командлет, который позволяет обращаться к различным классам.

Select-Object – фильтрует вывод информации.

Конвейер – это передача результата работы командлета через вертикальную черту (|) другому командлету.

С помощью конвейера можно выполнять сложные задачи простым и удобным способом без необходимости написания сложных алгоритмов и сценариев.

Пример

Get-CimInstance -ClassName Win32\_Processor | Select-Object -ExcludeProperty "CIM\*"

1. Системы удаленного доступа к компьютеру и управлению программным обеспечением.

Системы удаленного доступа - Программы или функции операционных систем, позволяющие получить удалённый доступ к компьютеру через Интернет или ЛВС и производить управление и администрирование удалённого компьютера в реальном времени. Программы удалённого администрирования предоставляют почти полный контроль над удалённым компьютером: они дают возможность удалённо управлять рабочим столом и всей операционной системой компьютера, возможность копирования или удаления файлов, установки и запуска приложений и т. д.

Примеры: LiteManager, team viewer.

1. Системы конфигурирования ИС. Сиcтема управления версиями GIT (цели использования git, принцип работы, репозиторий, типы репозиториев).

В ходе разработки ПО требуется постоянно вести учёт изменений исходного кода, а также возможность отката к контрольной точке. Для этого были созданы специальные инструменты — системы управления версиями, к коим и относится рассматриваемое ПО git.

Основное отличие Git от любой другой СКВ (включая Subversion и её собратьев) — это подход к работе со своими данными. Концептуально, большинство других систем хранят информацию в виде списка изменений в файлах. Эти системы представляют хранимую информацию в виде набора файлов и изменений, сделанных в каждом файле, по времени (обычно это называют контролем версий,

Git не хранит и не обрабатывает данные таким способом. Вместо этого, подход Git к хранению данных больше похож на набор снимков миниатюрной файловой системы. Каждый раз, когда вы делаете коммит, то есть сохраняете состояние своего проекта в Git, система запоминает, как выглядит каждый файл в этот момент, и сохраняет ссылку на этот снимок. Для увеличения эффективности, если файлы не были изменены, Git не запоминает эти файлы вновь, а только создаёт ссылку на предыдущую версию идентичного файла, который уже сохранён. Git представляет свои данные как поток снимков.

Репозиторий Git представляет собой каталог файловой системы.

В классическом обычном сценарии в репозитории git есть три типа объектов — файл, дерево и «коммит» (англ. commit — фиксация). Файл есть какая-то версия какого-то пользовательского файла, дерево — совокупность файлов из разных подкаталогов, «коммит» — дерево и некая дополнительная информация (например, родительские коммиты, а также комментарий).

Репозиторий Git бывает локальный и удалённый. Локальный репозиторий — это подкаталог .git, создаётся (в пустом виде) командой git init и (в непустом виде с немедленным копированием содержимого родительского удалённого репозитория и простановкой ссылки на родителя) командой git clone.

1. Управление пакетами (dpkg, apt-get, Aptitude).

Dpkg – это пакетный менеджер для Debian систем. Он может устанавливать, удалять и создавать пакеты, но, в отличие от других систем управления пакетами, он не может автоматически загружать и устанавливать пакеты или их зависимости. Эта секция раскрывает использование dpkg для управления локально установленными пакетами.

Apt-get – это мощный консольный инструмент, который работает с Улучшенным инструментарием пакетов (APT) Ubuntu, выполняющий такие функции, как установка новых программных пакетов, обновление имеющихся пакетов, обновления индекса списка пакетов и даже обновление все системы Ubuntu.

Aptitude — оболочка для Advanced Packaging Tool, части системы управления пакетами в операционной системе Debian и её производных. Имеет графический интерфейс (GTK), псевдографический и интерфейс командной строки.

1. Интерфейсы Ethernet (выполнить определение Ethernet интерфейсов в ОС, логическое имя, настройка интерфейса).

Интерфейсы Ethernet идентифицируются системой с использованием имен ethX, где X является числовым значением. Первый интерфейс обычно обозначается как eth0, второй как eth1, и все последующие с увеличивающимися номерами по порядку.

Для быстрого определения всех доступных сетевых интерфейсов вы можете использовать команду ifconfig

Настройки интерфейса Ethernet

ethtool - это программа, которая показывает и изменяет настройки сетевых карт, такие как автоопределение, скорость порта, режим дуплекса и функция Wake-on-LAN (пробуждение системы через сеть). Эта программа не устанавливается по умолчанию, но доступна к установке из репозиториев.

sudo apt-get install ethtool

1. Адресация IP (временное назначение IP адреса, динамическое присвоение и статическое присвоение IP адреса, интерфейс Loopback – обратная петля).

IP-адрес состоит из адреса сети и адреса хоста (или локального адреса). Такой адрес, состоящий из двух частей, позволяет отправителю задавать как сеть, так и конкретный хост в этой сети. Каждой сети присваивается уникальный адрес при подсоединении ее к другим сетям Internet.

Временное назначение IP адреса.

Для временной настройки сети вы можете использовать стандартные команды, такие как ip, ifconfig и route, которые присутствуют также и в других системах на базе GNU/Linux. Эти команды позволят изменить настройки, которые будут применены мгновенно, но они не будут постоянными и будут утеряны после перезагрузки.

Команды для временного назначения IP адреса:

1) Ifconfig – для проверки настройки IP адреса eth0

2) Route – для настройки шлюза по умолчанию

3) ip с опцией flush – для того, чтобы отменить все IP настройки интерфейса

Статический (Фиксированный) – в этом случае происходит настройка DHCP сервера, в ходе которой администратор вручную прописывает соответствие между каждым MAC-адресом и IP-адресом. Таким образом, за каждым устройством закрепляется свой адрес, который будет выдавать сервер.

Динамический – DHCP-сервер выдает клиенту любой адрес из диапазона свободных. Эти адреса не закрепляются за конкретными устройствами.

Динамическим способом раздают IP-адреса, когда состав пользователей и их количество в сети постоянно меняется, например при использовании Wi-Fi в кафе. В этом случае кафе покупает определенное количество IP-адресов и выдает посетителям, которые подключаются к сети.

Loopback — это термин, который обычно используется для описания методов или процедур маршрутизации электронных сигналов, цифровых потоков данных, или других движущихся сущностей от их источника и обратно к тому же источнику без специальной обработки или модификаций. Первоначально он использовался для тестирования передачи или передающей инфраструктуры.

Примеры использования:

* метод проведения теста передачи по линии доступа от обслуживающего центра коммутации, для которого обычно не требуется поддержка персонала на обслуживаемом терминале;
* метод тестирования передачи сигнала между станциями
* *коммутационный кабель*
* *возвратная петля, обратная петля* — вид диагностического теста, при котором сигнал возвращается передающему устройству, пройдя по коммуникационному каналу в обоих направлениях.

1. TCP/IP (IP адрес, сетевая маска, адрес сети, адрес рассылки, адрес шлюза, адрес сервера имен). TCP. UDP.ICMP

Протокол управления передачей и межсетевой протокол (TCP/IP) — это стандартный набор протоколов, разработанный в конце 1970-х Агентством передовых оборонных исследовательских проектов (DARPA) как средство взаимодействия между различными типами компьютеров и компьютерными сетями. TCP/IP является движущей силой интернета и поэтому является самым популярным стеком сетевых протоколов на Земле.

Протокол межсетевых управляющих сообщений (ICMP) — это расширение протокола IP, определенное в RFC 792, поддерживающее сетевые пакеты сообщений управления, информирующих сообщений и сообщений об ошибках.

Пользовательский пакетный протокол (**UDP**) — это протокол без установления соединения, который редко используется для передачи важных данных, поскольку не использует управление потоком и иные методы проверки целостности передаваемых данных.

**IP адрес** – это уникальная идентифицирующая строка, представленная в виде четырех десятичных чисел от 0 до 255, разделенных точками, каждое из которых представляет 8-битный адрес, составляющие полный 32-битный адрес

**Маска подсети (или просто сетевая маска)** — это локальная побитовая маска или набор флагов, которые разделяют IP адрес на часть, значимую для всей сети, и биты, значимые для данной подсети.

**Адрес сети** представляет собой байты, составляющие сетевую часть IP адреса.

**Адрес рассылки** — это IP адрес, который позволяет посылать сетевые данные на все хосты заданной подсети вместо того чтобы задавать определенный хост.

**Адрес шлюза** — это IP адрес, через который можно соединиться с определенной сетью или хостом в сети.

**Адрес сервера имен** представляет IP адрес системы сервиса доменных имен (DNS), которые разрешают сетевые имена хостов в IP адреса.

1. Протокол динамического выделения адресов (DHCP). NTP протокол.

Протокол динамического выделения адресов (DHCP) — это сетевой сервис, который позволяет компьютерам в сети автоматически получать настройки с сервера вместо того, чтобы настраивать каждый сетевой хост вручную. Компьютеры, настроенные быть клиентами DHCP, не управляют тем, какие настройки они получат от DHCP сервера, и эта настройка совершенно незаметна для пользователя компьютера.

NTP — это протокол синхронизации времени по сети. По существу клиенты запрашивают текущее время на сервере и используют его для установки своих собственных часов.

1. Удаленное администрирование (OpenSSH, Puppet, Zentyal).

Удаленным администрированием принято называть подключение ИТ специалиста, чаще всего являющегося сотрудником аутсорсинговой компании, к рабочей станции или серверу клиентской организации удаленным способом, т.е. через локальную сеть или интернет с целью инсталляции, настройки и устранения проблем в работе компьютерной техники и программного обеспечения и для проведения его планового обслуживания.

OpenSSH — это мощный набор инструментов для удаленного управления и передачи данных между сетевыми компьютерами.

Puppet — кроссплатформенное клиент-серверное приложение, которое позволяет централизованно управлять конфигурацией операционных систем и программ, установленных на нескольких компьютерах. Написано на языке программирования Ruby

Zentyal (ранее — eBox Platform) — это дистрибутив Linux, основанный на Ubuntu, с пакетом серверного программного обеспечения с открытым исходным кодом, ориентированный на малые и средние корпоративные сети. Zentyal может выступать в роли сетевого шлюза, единого центра безопасности сети, Office Server, сервера унифицированных коммуникаций, или в роли комбинировании любых из перечисленных функций. Кроме того, Zentyal включает фреймворк, упрощающий разработку новых служб для Unix.

1. Авторизация по сети на примере ОС Ubuntu Server (OpenLDAP, Samba и LDAP, Kerberos, Kerberos и LDAP, назначение, алгоритм работы).

LDAP — это аббревиатура от Lightweight Directory Access Protocol. Как следует из названия, это облегчённый протокол доступа к службам каталогов, предназначенный для доступа к службам каталогов на основе X.500. LDAP работает поверх TCP/IP или других ориентированных на соединение сетевых протоколов. LDAP стандартизирован в качестве протокола IETF, и его описание можно найти в "Lightweight Directory Access Protocol (LDAP) Technical Specification Road Map" ("Описание технической спецификации Lightweight Directory Access Protocol (LDAP)") RFC4510.

OpenLDAP — открытая реализация LDAP, разработанная одноимённым проектом, распространяется под собственной свободной лицензией OpenLDAP Public License. В числе прочих есть реализации для различных модификаций BSD, а также Linux, AIX, HP-UX, macOS, Solaris, Windows и z/OS.

Samba — это реализация протокола Server Message Block (SMB)/Common Internet File System (CIFS) для систем Unix, обеспечивающая поддержку межплатформенного общего доступа к файлам и принтерам с Microsoft Windows, OS X и другими системами Unix.

Самбу можно использовать для:

* Действуйте как сервер для клиентов SMB: делитесь папками и принтерами, включая псевдопринтеры PDF, чтобы все компьютеры в вашей сети могли записывать файлы PDF
* Работа в качестве контроллера домена в сети Windows (аутентификация пользователей и т. д.)
* Выполните более сложные действия, например, используйте контроллер домена Windows для аутентификации пользователей компьютера с Linux/UNIX.

Kerberos — сетевой протокол аутентификации, который предлагает механизм взаимной аутентификации клиента и сервера перед установлением связи между ними. Kerberos выполняет аутентификацию в качестве службы аутентификации доверенной третьей стороны, используя криптографический разделяемый секрет, при условии, что пакеты, проходящие по незащищенной сети, могут быть перехвачены, модифицированы и использованы злоумышленником. Kerberos построен на криптографии симметричных ключей и требует наличия центра распределения ключей. Расширения Kerberos могут обеспечить использование криптографии с открытым ключом на определенных этапах аутентификации.

1. Администрирование баз данных в UbuntuServer (MySQL, PostgreSQL).

Одной из самых популярных СУБД на сегодняшний день является **MySQL,** распространяемая свободно (с некоторыми ограничениями). Эта серверная система способна эффективно функционировать во взаимодействии с интернет-сайтами и веб-приложениями. При этом она проста в освоении, что лишь увеличивает ее популярность.

Помимо универсальности и распространенности СУБД MySQL обладает целым комплексом важных преимуществ перед другими системами. В частности, следует отметить такие качества как:

* Простота в использовании.
* Обширный функционал.
* Безопасность.
* Масштабируемость.
* Скорость.

PostgreSQL – унифицированный сервер баз данных, имеющий единый движок – storage engine. Постгрес использует клиент-серверную модель.

Для каждого клиента на сервере создается новый процесс (не поток). Для работы с такими клиентскими процессами сервер использует семафоры.

Как и любая СУБД PostgreSQL должна обслуживать запросы sql и возвращать результаты клиентским приложениям. Для этого механизм СУБД оптимизатор запросов принимает решение об оптимальном использовании ресурсов и строит план запроса. При этом он может опереться на используемых механизмы ускорения работы (индексов, кэшей в памяти, ресурсам процессора, данные статистики и т.д.).