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.