**Области применения и примеры реализации информационных технологий управления корпорацией**

* Бухгалтерский учет
* Управление финансовыми потоками
* Управление складом, ассортиментом, закупками
* Управление производственным процессом
* Управление маркетингом
* Документооборот
* Системы поддержки принятия решений, системы интеллектуального анализа данных
* Предоставление информации о предприятии

**Администрирования и разграничение прав доступа пользователя**

Администрирование пользователей состоит в создании учетной информации пользователей (определяющей имя пользователя, принадлежность пользователя к различным группам пользователей, пароль пользователя), а также в определении прав доступа пользователя к ресурсам сети - компьютерам, каталогам, файлам, принтерам и т.п.

**Области администрирования**

Сетевое администрирование распространяется на пять основных областей, с которыми должен быть хорошо знаком администратор сети:

* управление пользователями – создание и поддержка учетных записей пользователей, управление доступом пользователей к ресурсам;
* управление ресурсами – установка и поддержка сетевых ресурсов;
* управление конфигурацией – планирование конфигурации сети, ее расширение, а также ведение необходимой документации;
* управление производительностью – мониторинг и контроль за сетевыми операциями для поддержания и улучшения производительности системы;
* поддержка – предупреждение, выявление и решение проблем сети.

**Обязанности администратора**

Учитывая области сетевого управления, можно составить список задач, за выполнение которых отвечает администратор сети:

* создание учетных записей пользователей и управление ими;
* защита данных;
* обучение и поддержка пользователей (при необходимости);
* модернизация существующего программного обеспечения и установка нового;
* архивирование;
* предупреждение потери данных;
* мониторинг и управление пространством для хранения данных на сервере;
* настройка сети для достижения максимальной производительности;
* резервное копирование данных;
* защита сети от вирусов;
* решение сетевых проблем;
* модернизация и замена компонентов сети (при необходимости);
* добавление в сеть новых компьютеров.

**Разграничение прав доступа и установление подлинности пользователей**

Разграничение доступа в информационной системе заключается в разделении информации, циркулирующей в ней, на части и организации доступа к ней должностных лиц в соответствии с их функциональными обязанностями и полномочиями.

Задача разграничения доступа: сокращение количества должностных лиц, не имеющих к ней отношения при выполнении своих функций, т. е. защита информации от нарушителя среди допущенного к ней персонала.

При этом деление информации может производиться по степени важности, секретности, по функциональному назначению, по документам и т.д.

Принимая во внимание, что доступ осуществляется с различных технических средств, начинать разграничение можно путем разграничения доступа к техническим средствам, разместив их в отдельных помещениях. Все подготовительные функции технического обслуживания аппаратуры, ее ремонта, профилактики, перезагрузки программного обеспечения и т.д. должны быть технически и организационно отделены от основных задач системы.

Информационная система в целом, а также комплекс средств автоматизации и организация их обслуживания должны быть построены следующим образом:

* техническое обслуживание комплекса средств автоматизации в процессе эксплуатации должно выполняться отдельным персоналом без доступа к информации, подлежащей защите;
* перезагрузка программного обеспечения и всякие его изменения должны производиться специально выделенным для этой цели проверенным специалистом;
* функции обеспечения безопасности информации должны выполняться специальным подразделением в организации -- владельце комплекса средств автоматизации, компьютерной сети, автоматизированной системы управления или информационной системы в целом;
* организация доступа пользователей к устройствам памяти (хранения) информационной системы должна обеспечивать возможность разграничения доступа к информации, хранящейся на них, с достаточной степенью детализации и в соответствии с заданными уровнями (политиками) полномочий пользователей;
* регистрация и документирование технологической и оперативной информации должны быть разделены.

Разграничение доступа пользователей-потребителей информационной системы может осуществляться также по следующим параметрам:

* по виду, характеру, назначению, степени важности и секретности информации;
* способам ее обработки: считать, записать, внести изменения, выполнить команду;
* условному номеру терминала;
* времени обработки и др.

При проектировании и планировании эксплуатации базового информационного и вычислительного комплекса с учетом комплекса средств автоматизации производятся:

* разработка или адаптация операционной системы с возможностью реализации разграничения доступа к информации, хранящейся в памяти вычислительного комплекса;
* изоляция областей доступа;
* разделение базы данных на группы;
* процедуры контроля перечисленных функций.

При проектировании и эксплуатации комплекса средств автоматизации, автоматизированной системы управления и информационной системы в целом (сети) на их базе производятся:

* разработка и реализация функциональных задач по разграничению и контролю доступа к аппаратуре и информации как в рамках данного комплекса средств автоматизации, так и информационной системы в целом;
* разработка аппаратных средств идентификации и аутентификации пользователя;
* разработка программных средств контроля и управления разграничением доступа;
* разработка отдельной эксплуатационной документации на средства идентификации, аутентификации, разграничения и контроля доступа.
* В качестве идентификаторов личности для реализации разграничения широко распространено применение кодов паролей, которые хранятся в памяти пользователя и комплекса средств автоматизации. В помощь пользователю в системах с повышенными требованиями большие значения кодов паролей записываются на специальные носители – электронные ключи или карточки.
* Разделение привилегий на доступ к информации заключается в том, что из числа допущенных к ней должностных лиц выделяется группа, которой предоставляется доступ только при одновременном предъявлении полномочий всех членов группы.
* **Задача указанного метода** – существенно затруднить преднамеренный перехват информации нарушителем. Примером такого доступа может быть сейф с несколькими ключами, замок которого открывается только при наличии всех ключей. Аналогично в информационной системе может быть предусмотрен механизм разделения привилегий при доступе к особо важным данным с помощью кодов паролей.
* Данный метод несколько усложняет процедуру, но обладает высокой эффективностью защиты. На его принципах можно организовать доступ к данным с санкции вышестоящего лица по запросу или без него.
* Сочетание двойного криптографического преобразования информации и метода разделения привилегий позволяет обеспечить высокоэффективную защиту информации от преднамеренного несанкционированного доступа.

**Управление доступом к информации в сети передачи и в автоматизированной системе управления**

Управление доступом к информации в сети передачи осуществляется при ее подготовке, в процессе эксплуатации и завершения работ.

При подготовке сети передачи информации и автоматизированной системы управления к эксплуатации управление доступом заключается в выполнении следующих функций:

* уточнении задач и распределении функций элементов сети и автоматизированной система управления и обслуживающего персонала;
* контроле ввода адресных таблиц в элементы сети;
* вводе таблиц полномочий элементов сети, пользователей, процессов и т.д.;
* выборе значений, распределении и рассылке ключей шифрования по назначению;
* проверке функционирования систем шифрования и контроля полномочий.

В процессе эксплуатации управление доступом предполагает:

* контроль соблюдения полномочий элементами сети, процессами, пользователями и т. д.; своевременное обнаружение и блокировку несанкционированного доступа;
* контроль соблюдения правил шифрования данных и применения ключей шифрования;
* сбор, регистрацию и документирование информации о несанкционированном доступе с указанием места, даты и времени события;
* регистрацию, документирование и контроль всех обращений к информации, подлежащей защите, с указанием даты, времени и данных отправителя и получателя информации;
* выбор, распределение, рассылку и синхронизацию применения новых значений ключей шифрования;
* изменение и ввод при необходимости новых полномочий элементов сети, процессов, терминалов и пользователей;
* проведение организационных мероприятий по защите информации в сети передачи и автоматизированной системе управления.

Нарушение полномочий выражается:

* в обращении с запросом или выдаче отправителем команд, не предусмотренных в списке получателей элемента сети;
* несовпадении значений предъявленного и хранимого на объекте-получателе паролей;
* получении им зашифрованной информации, не поддающейся расшифровке, и т.д.

Управление доступом может быть трех видов:

* **централизованное управление**

Установление полномочий производится администрацией организации или фирмы-владельца автоматизированной системы управления, сети или информационной системы в целом. Ввод и контроль полномочий осуществляется представителем службы безопасности информации с соответствующего объекта управления;

* **иерархическое децентрализованное управление**

Центральная организация, осуществляющая установление полномочий, может передавать некоторые свои полномочия подчиненным организациям, сохраняя за собой право отменить или пересмотреть решения подчиненной организации или лица;

* **индивидуальное управление**

В этой ситуации не существует статической иерархии в управлении распределением полномочий. Отдельному лицу может быть разрешено создавать свою информацию, гарантируя при этом ее защиту от несанкционированного доступа. Владелец информации может по своему усмотрению открыть доступ к ней другим пользователям, включая передачу права собственности. Все указанные виды управления могут применяться одновременно в зависимости от характера деятельности и задач организации-владельца автоматизированной системы управления, сети или информационной системы в целом.

**Аутентификация, авторизация и администрирование действий пользователей**

**Идентификация** – процедура распознавания пользователя по его идентификатору (имени). Эта функция выполняется, когда пользователь делает попытку войти в сеть. Пользователь сообщает системе по ее запросу свой идентификатор, и система проверяет в своей базе данных его наличие.

**Аутентификация** – процедура проверки подлинности заявленного пользователя, процесса или устройства. Эта проверка позволяет достоверно убедиться, что пользователь (процесс или устройство) является именно тем, кем себя объявляет. При проведении аутентификации проверяющая сторона убеждается в подлинности проверяемой стороны, при этом проверяемая сторона тоже активно участвует в процессе обмена информацией. Обычно пользователь подтверждает свою идентификацию, вводя в систему уникальную, не известную другим пользователям информацию о себе (например, пароль или сертификат).

Идентификация и аутентификация являются взаимосвязанными процессами распознавания и проверки подлинности субъектов (пользователей). Именно от них зависит последующее решение системы: можно ли разрешить доступ к ресурсам системы конкретному пользователю или процессу. После идентификации и аутентификации субъекта выполняется его авторизация.

**Авторизация** – процедура предоставления субъекту определенных полномочий и ресурсов в данной системе. Иными словами, авторизация устанавливает сферу его действия и доступные ему ресурсы. Если система не может надежно отличить авторизованное лицо от неавторизованного, то конфиденциальность и целостность информации в этой системе могут быть нарушены. Организации необходимо четко определить свои требования к безопасности, чтобы принимать решения о соответствующих границах авторизации.

С процедурами аутентификации и авторизации тесно связана процедура администрирования действий пользователя.

**Администрирование** – регистрация действий пользователя в сети, включая его попытки доступа к ресурсам. Хотя эта учетная информация может быть использована для выписывания счета, с позиций безопасности она особенно важна для обнаружения, анализа инцидентов безопасности в сети и соответствующего реагирования на них. Записи в системном журнале, аудиторские проверки и ПО accounting -- все это может быть использовано для обеспечения подотчетности пользователей, если что-либо случится при входе в сеть с их идентификатором.

**Пароль** – это то, что знает пользователь и другой участник взаимодействия. Для взаимной аутентификации участников взаимодействия может быть организован обмен паролями между ними.

Персональный идентификационный номер PIN (Personal Identification Number) является испытанным способом аутентификации держателя пластиковой карты и смарт-карты. Секретное значение PIN-кода должно быть известно только держателю карты.

**Динамический (одноразовый) пароль** – это пароль, который после однократного применения никогда больше не используется. На практике обычно используется регулярно меняющееся значение, которое базируется на постоянном пароле или ключевой фразе.

**Система запрос-ответ**. Одна из сторон инициирует аутентификацию с помощью посылки другой стороне уникального и непредсказуемого значения «запрос», а другая сторона посылает ответ, вычисленный с помощью «запроса» и секрета. Так как обе стороны владеют одним секретом, то первая сторона может проверить правильность ответа второй стороны.

**Сертификаты и цифровые подписи**. Если для аутентификации используются сертификаты, то требуется применение цифровых подписей на этих сертификатах. Сертификаты выдаются ответственным лицом в организации пользователя, сервером сертификатов или внешней доверенной организацией. В рамках Интернета появились коммерческие инфраструктуры управления открытыми ключами PKI (Public Key Infrastructure) для распространения сертификатов открытых ключей. Пользователи могут получить сертификаты различных уровней.

**Необходимый уровень аутентификации** определяется требованиями безопасности, которые установлены в организации. Общедоступные Web-серверы могут разрешить анонимный или гостевой доступ к информации. Финансовые транзакции могут потребовать строгой аутентификации. Примером слабой формы аутентификации может служить использование IP-адреса для определения пользователя. Подмена IP-адреса может легко разрушить механизм аутентификации. Надежная аутентификация является тем ключевым фактором, который гарантирует, что только авторизованные пользователи получат доступ к контролируемой информации.

При защите каналов передачи данных должна выполняться взаимная аутентификация субъектов, т.е. взаимное подтверждение подлинности субъектов, связывающихся между собой по линиям связи. Процедура подтверждения подлинности выполняется обычно в начале сеанса установления соединения абонентов. Термин «соединение» указывает на логическую связь (потенциально двустороннюю) между двумя субъектами сети. Цель данной процедуры – обеспечить уверенность, что соединение установлено с законным субъектом и вся информация дойдет до места назначения.