МДК.02.01.

Раздел 2. Управление доступом в компьютерных системах

$9. Система безопасности сетевых операционных систем

План:

9.1. Система безопасности СОС семейства Windows

9.1.1. Подсистема шифрования Windows Server 20xx
9.1.2. Аутентификация Windows Server 20xx
9.1.3. Сертификация Windows Server 20xx

9.2. Система безопасности СОС семейства *nix

9.2.1. Ключевые аспекты безопасности
9.2.2. Слабые места и проблемы защиты
9.2.3. Средства безопасности

9.3. Система безопасности мобильных ОС - доклады

9.4. Система безопасности SQL Server

9.4.1. Знакомство с SQL Server
9.4.2. Типы безопасности SQL Server
9.4.3. Роли и права доступа
9.4.4. Дополнительные меры безопасности

9.1.1. Подсистема шифрования Windows Server

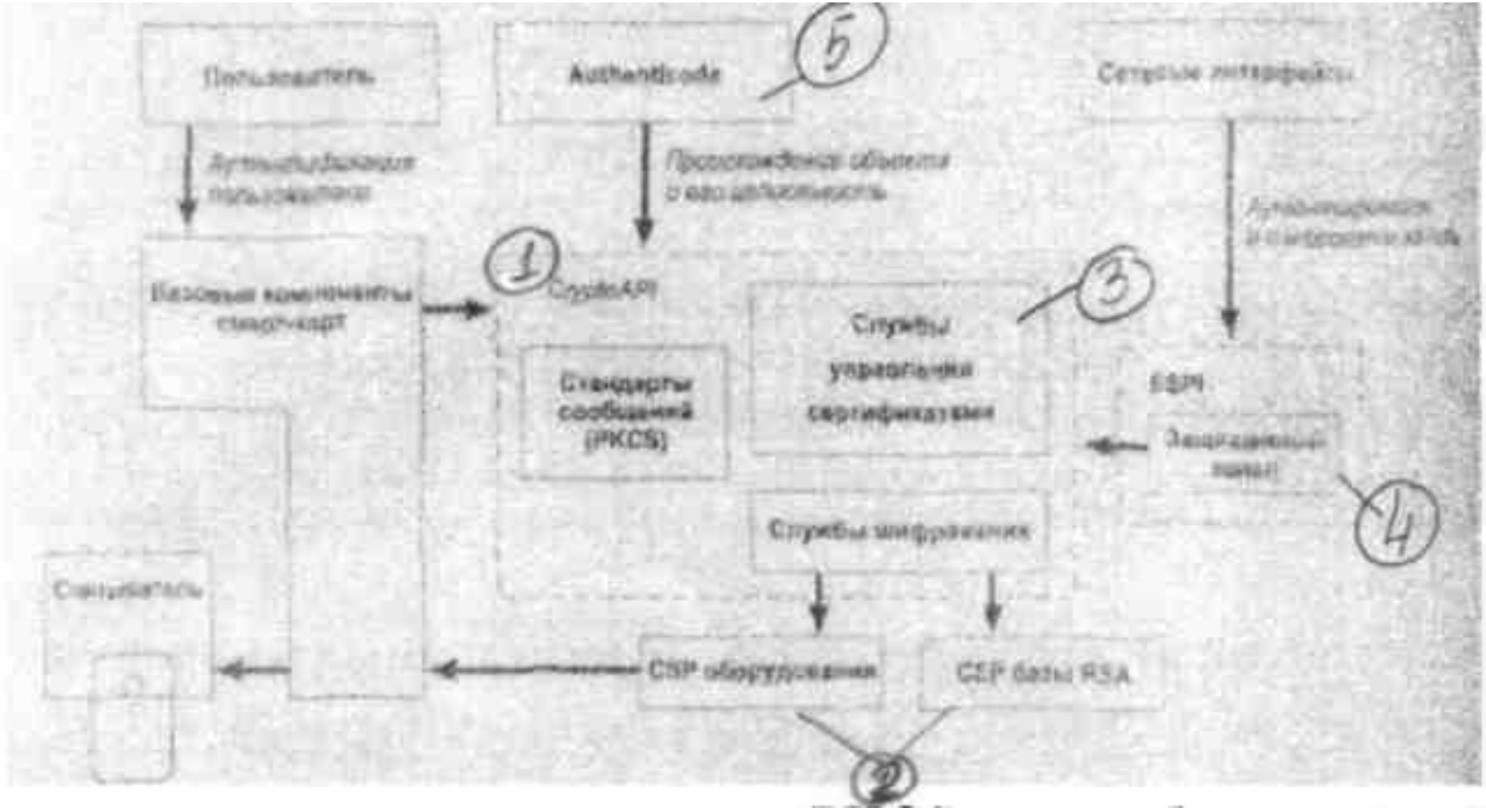

Схема поддержки ассиметричного шифрования

1 - Библиотека Crypto API – является основой архитектуры поддержки прикладных программ шифрования информации с открытым ключом, которая позволяет работать со всеми устанавливаемыми поставщиками услуг шифрования (Cryptographic Service Providers, CSP) – 2, реализуемые программно или аппаратно.

Услугами служб шифрования пользуются службы управления сертификатами – 3.

4 – защищенный канал поддерживает сетевую аутентификацию и шифрование в соответствии со стандартами TLS и SSL.

Служба – 5 - предназначена для проверки и подписи объектов и используется при получении информации через Интернет

Модель распределенной безопасности

1. Прямой доверенный путь между рабочими станциями, сервером и контроллером домена, устанавливается службой Net Logon.

Имеется возможность установки защищенного канала с другими доменами

2. Перед выполнением запрошенных клиентом операций сетевые службы имперсонализируют описание безопасности этого клиента

3. Ядро Windows поддерживает объектно – ориентированное управление доступом, сравнивая SID в маркере доступа с правами доступа. Ядро проверяет разрешения при каждой попытке доступа к объекту.

9.1.2. Аутентификация Windows Server

Протокол Kerberos (RFS IS10) – позволяет выполнять одну регистрацию в системе при организации доступа ко всем ресурсам сети и ***обеспечивает:***

- ***взаимную аутентификацию***
- ***ускоренную аутентификацию***
- ***транзитное доверие на аутентификацию.***

Протокол Kerberos реализован в виде поставщика безопасности, доступ к которому осуществляется с применением интерфейса поддержки поставщика безопасности SSPI (Security Support Provider Interface)

Центр распределения ключей Kerberos (KDC, Kerberos Key Distribution Center) – устанавливается на каждый контроллер домена

Области применения протокола Kerberos:

- Аутентификация в Active Directory
- При организации удаленного доступа
- Защищенное обновление адресов DNS
- Служба печати
- Взаимная аутентификация IPSec –хостов
- Запросы резервирования для службы качества обслуживания
- Аутентификация интрасети в IIS (Internet Information Services)
- Аутентификация запросов сертификата открытого ключа
- Удаленное управление сервером и рабочими станциями

Безопасность IP. Протокол IPSec (IPSecurity)

ПБ IP гарантирует защиту трафика от: НСД; перехвата, просмотра и копирования; модификации данных во время пути по сети

Преимущества безопасности IP:

- Централизованное администрирование ПБ
- Прозрачность безопасности IP
- Гибкость конфигурирования ПБ
- Туннелирование
- Усиленная служба аутентификации
- Поддержка ключей большой длины, динамический повторный обмен ими
- Безопасная связь для частных пользователей внутри домена, между доверенными доменами
- Взаимодействие с другими платформами и продуктами за счет открытости стандарта IPSec
- Установка безопасной связи с компьютерами не являющимися частью домена за счет ассиметричного шифрования
- Взаимодействие с другими механизмами защиты
- Не мешает другим службам

Возможности системы при использовании IPSec (IPSecurity)

- Выбор протокола защиты
- Решить какой алгоритм использовать для служб
- Устанавливать и поддерживать криптографические ключи
- IPSec может защищать пути между компьютерами, между шлюзами, между шлюзами и компьютерами

Сертификаты с открытым ключом – средство идентификации пользователей в незащищенных сетях и предоставляют информацию, необходимую для проведения защищенных частных коммуникаций.

Задачи решаемые сертификатами:

- Аутентификация

  - пользователя для защищенного веб-узла по протоколам TLS, SSL

  - сервера по протоколу TLS

  - регистрация в домене
- Конфиденциальность (с помощью протоколов TLS, SMIME, IP Security)
- Шифрование
- Цифровые подписи

9.1.3. Сертификация Windows Server

Виды центров сертификации

1. ***ЦС предприятия*** – требует наличия Active Directory, для проверки идентификационной информации запрашивающего сертификат, публикует списки отозванных сертификатов в Active Directory.

2. ***Изолированный (автономный) ЦС*** – не зависит от Active Directory. Запрос сертификата только в веб-страниц.

9.2.1. Ключевые аспекты безопасности

Проблемы модели безопасности Linux:

- Ориентация на удобство применения, но не предполагает простой защиты
- Всего 2 варианта статуса пользователя (не обладающий привилегиями и суперпользователь)
- Разрабатывается большим сообществом программистов (разная квалификация, отношение к работе и т.д.) – может быть компенсировано открытым исходным кодом.

Слабые места защиты:

- Человеческий фактор
- Ошибки в программах
- Частичная безопасность – по умолчанию (полная Б настраивается)

1. Фильтрация пакетов (брандмауэр или утилита iptables)
2. Ненужные службы (файлы /etc/inetd.conf или /etc/xinetd.d для Red Hat)
3. Программные «заплаты»
4. Резервные копии
5. Пароли
6. Бдительность (состояние сетевых соединений, таблиц процессов)

9.2.2. Слабые места и проблемы защиты

1. Плохое управление паролями

файлы /etc/passwd и /etc/shadow - содержат данные об учетных записях пользователей и их правах).

доступ к /etc/passwd /etc/group – читают все, запись root; /etc/shadow – недоступен рядовым пользователям.

2. Модули PAM – подключаемые модули аутентификации (программы аутентификации отдает аутентификацию модулю, которые можно добавлять, удалять и перенастраивать в любое время)

Настройка через каталог /etc/pam.d:

тип_модуля: auth (право группового доступа), account (действия не связанные с аутентификацией), session (действия после доступа к службе), password (ввод пароля)

управляющий_флаг: required (положительный результат), requisite, sufficient, optional (результат работы модуля не существенен)

путь_к_модулю:

аргумент:

3. Скрытые пароли

файла /etc/passwd – открыт для чтения, имеет 7 полей, 2-е – зашифрованный пароль пользователя.

/etc/shadow - файл скрытых паролей, доступен только суперпользователю

4. Групповые и совместно используемые учетные записи – не рекомендуется применять

Контроль предоставления прав суперпользователя – утилита **sudo.**

9.2.3. Средства безопасности

1. Система **Syslog** – запись журнальной информации о процессах ядра и польз-их процессах в файл с его дальнейшей рассылкой

2. Защищенные терминалы (регистрация root только с определенных терминалов)

3. Отключение служб (демонов) **rshd и rlogin**, читающих файлы .rhosts и hosts.equiv (компьютеры – эквивалентные, что позволяет осуществлять вход и копирование файлов без пароля)

4. Отключение демонов: rexeced – выполняющий удаленное выполнение команд; tftpd – реализующий протокол TFTP; fingerd – выводящий отчет о заданном пользователе.

5. **NIS –** сетевая информационная служба – система распространения БД, используемая для рассылок файлов /etc/group, /etc/passwd, /etc/hosts, рекомендуется не использовать повседневно

6. Команда **showmounte** – информация о том, какие файловые системы экспортируются и кому, необходимо задавать список управления доступом для каждой ФС.

7. Программа **sendmail** - сетевая система, компоненты которой выполняются с правами суперпользователя, наиболее уязвима для злоумышленников, рекомендуется использовать последнюю версию

Инструментальные средства защиты

1. Команда **nmap** - сканер сетевых протоколов (способна проверять «по-хакерски» - не устанавливая реального соединения)
2. Утилита **ncliff** – отслеживает изменения в состоянии портов и известных узлов
3. **SAINT** – интегрированный пакет для безопасного администрирования сети, ищет наиболее распространенные случаи неправильного конфигурирования и проверяет наличие известных ошибок.
4. **Nessus –** сетевой сканер, ничему не доверяющий
5. Утилита **crack** – поиск ненадежных паролей
6. Программа **tcpd** – защита Интернет служб
7. Утилита **tripwire** – контролирует права доступа и контрольные суммы важных системных файлов, обнаруживая замененные, поврежденные или подделанные файлы.
8. **TCT** – набор утилит, помогающих анализировать систему после проникновения нарушителя

9. Программа **COPS** – система проверки компьютеров и паролей, содержит утилиты, осуществляющие мониторинг компонентов подсистемы защиты

Компоненты проверки:

- Права доступа к файлам, каталогам и устройствам;
- Содержимое файлов /etc/group, /etc/passwd
- Содержимое сценариев запуска системы
- Возможность записи в начальные каталоги

10. **Kerberos** – система аутентификации

11. **PGP** – криптографические утилиты, ориентированные на обеспечение безопасности электронной почты

12. **OPIE** – универсальные одноразовые пароли

13. Пакет **SSH** – использует криптографическую аутентификацию для подтверждения личности и шифрует любые соединения

Содержит:

Демон **sshd** – аутентификация пользователей 3 способами:

- Метод А. Автоматический доступ без проверки пароля если имя удаленного компьютера с которого регистрируется пользователь указано в файлах -/.rhosts, -/.shosts, /etc/hosts.equiv или /etc/shosts.equiv
- Метод Б. в дополнение к методу А применяется шифрование с открытым ключом для проверки адреса удаленного компьютера
- Метод В. Шифрование для идентификации самого пользователя
- Метод Г. Простой ввод регистрационного пароля (наиболее удобен для повседневного использования)

9.3. Безопсность мобильных ОС

Состояние на 2011 год.

- Android
- Apple iPhoneOS
- Maemo/MeeGo
- Microsoft Windows Mobile
- Palm webOS
- RIM BlackBerry OS
- Samsung Bada OS
- Symbian OS

Угрозы и атаки на смартфонах

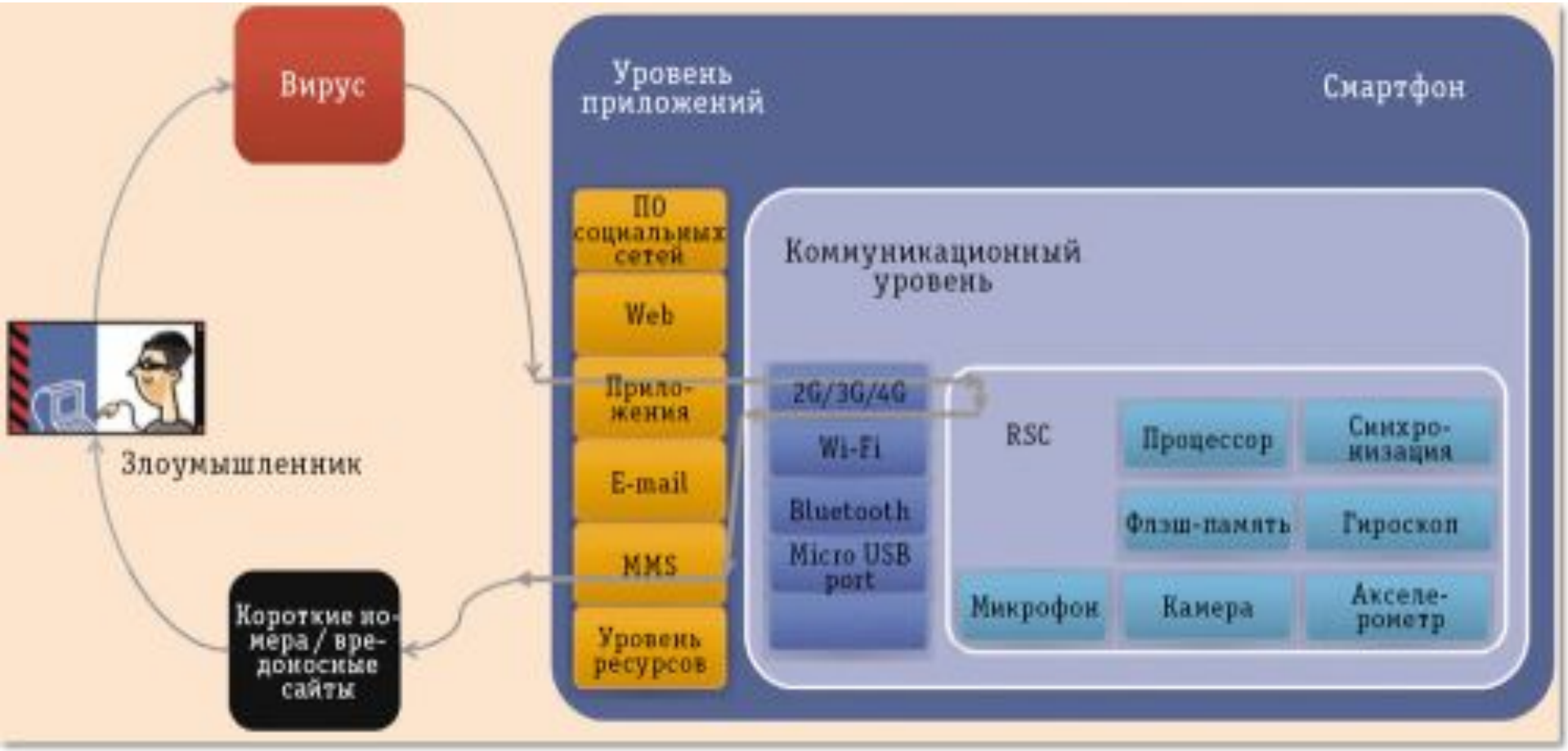

Рис. Модель угрозы безопасности на смартфоне. Пользователь загружает вирус на смартфон с помощью клиента социальной сети через сеть мобильной связи. Вирус перехватывает управление ресурсами смартфона и отправляет MMS-сообщения на платн короткий номер

Угрозы и атаки на смартфонах

Последствия

- **Ухудшение обслуживания**
- **Угроза ресурсам** (перепрограммирование флэшпамяти, выяснение содержимого карты памяти MicroSD, раскрыть местонахождение пользователя по GPS, включение камеры или микрофон аппарата когда передается информация со смартфона на компьютер по сети Wi-Fi или Bluetooth.

Вирус с полным контролем над смартфоном, - эффективное устройство для шпионажа.

- **Вредоносные программы**
- Вирусы (игры, заплаты безопасности или другое ПО).
- Трояны (запись разговоров или перехват мгновенных сообщений, регистрация местонахождение с помощью GPS или передают посторонним детализацию вызовов и другие приватные сведения)
- SMS-трояны (в фоновом режиме и отправляют SMS-сообщения на платные номера)
- Шпионские программы собирают информацию о пользователях без их ведома.

9.4.1. Знакомство с SQL Server

Windows Server	SQL Server	Назначение	Примечание
User (пользователь)	**Login (вход в систему)**	Объект содержащий имя, пароль и другие атрибуты представляющие пользователя)	В SQL термин **Login** относится к сервисам SQL
User name (имя пользователя)	**Login name (идентиф. польз.)**	Идентификатор или имя пользователя	В Win кроме символов: «»/\[]:;+=<> В SQL кроме \
Password			
------	**User**	Идентификатор пользователя БД (имя под которым пользователь известен конкретной БД)	В SQL термин **User** относится к сервисам SQL 128 символов, кроме \
Group (группа)	**Role (роль)**	Атрибуты множества пользователей	Пользователь принадлежит к любому числу групп или ролей В SQL типы ролей: Стандартная роль сервера Стандартная роль БД Роль на уровне БД
Group name	**Role name**	Идентификатор группы или роли	Имена глобальных групп 20 сим. Имена локальных групп 256 сим.

9.4.2. Типы безопасности SQL Server

Средства безопасности включают в себя мониторинг и управление корпоративными БД в соответствии с указаниями менеджеров компании.

Стратегия безопасности разрабатывается для ограничения наборов данных, доступных работникам для просмотра, и времени доступа к информации.

Модель безопасности SQL Server.

1 уровень: вход в систему и разграничение прав доступа пользователя

2 уровень: представления и хранимые процедуры

3 уровень: внешняя безопасность

Типы безопасности:

1. Стандартная: SQL Server полностью отвечает за установку и поддержку бюджетов пользователей и серверов, выполняет аутентификацию пользователя и наложение ограничений, связанных с паролем и входом в систему.

Применяется, когда компьютер Windows Server не используется для выполнения функций файлового сервера и в случае, когда подключение к серверу производится с помощью нескольких различных протоколов.

2. Интегрированная: за управление доступом пользователей отвечает операционная система Windows с помощью списка контроля доступа (Access Control List,ACL), что обеспечивает доступ с единым паролем ко всем ресурсам домена Windows. При присоединении к SQL Server решение о предоставлении доступа принимается на основании, атрибутов бюджета пользователя в системе Windows.

3. Смешанная: SQL проверяет установил ли пользователь доверительное соединение с Windows, если соединение не найдено, то SQL исполняет собственную проверку.

Уровни бюджетов пользователя в SQL Server.

1 уровень: идентификатор пользователя или вход в систему

2 уровень: пользователь БД

SYSUSERS таблица для хранения объекты-пользователи (для каждой БД)

Стандартные идентификаторы:

SA приписан к роли sysadmin – абсолютные права

Administrators – доступ к серверам членам административной группы Windows

9.4.3. Роли и права доступа

Варианты подключения к серверу:

- *Use Windows authentication* – подключение под именем пользователя Windows
- *Use SQL authentication* – подключение под именем SQL Server

Роль – именованный набор прав в рамках сервера или конкретной БД.

Для конкретной БД – неограниченное число ролей.

Для каждой БД роль создается заново.

Модель БД (Model database).

Операции управления пользователями

Название операции	SQL Server Enterprise Manager	Transact – SQL процедуры
Добавление входа на сервер	Login/new login -security access -server roles -database access	SP_ADDLOGIN
Добавление нового пользователя		SP_ADDUSER
Удаление идентификаторов	Кнопка DELETE	SP_DROPLOGIN SP_DROPUSER
Создание роли	Database Roles – контекстное меню new database role – окно database role properties	SP_SETAPROLE Предварительно выполняется процедура SP_ADDAPROLE (создание роли)
Удаление ролей	Кнопка DELETE	SP_DROLE (стандартной роли) SP_DROPROLE (роли приложения)
Управление ролями		GRANT DENY REVOKE

Стандартные роли сервера

Роль	Права
Sysadmin	Любые действия на конкретном сервере
Securityadmin	Управление идентификаторам и пользователей, создавать БД, читать журнал
Serveradmin	Назначение параметров конфигурации сервера
Setupadmin	Создание объектов репликации, управление процедурами
Diskadmin	Управление файлами БД
dbcreator	Создание и модификация БД

Стандартные роли базы данных

Роль	Права
Db_owner	Любые действия и работы по сопровождению и конфигурации БД
Db_accessadmin	Добавление пользователей БД (windows и SQL)
Db_datareader	Извлечение информации из любой БД
Db_datawriter	Добавление, обновлять и удалять пользовательские таблицы БД
Db_ddladmin	Добавление, удаление и обновление объектов БД
Db_securityadmin	Управление ролями и их членами, выполнение выражение на доступ к объектам
Db_backupoperator	Выполнение операций резервирования БД
Db_denydatareader	Модификация схемы БД (без чтения)
Db_denydatawriter	Запрет модификации информации

Роль Public – роль на уровне БД (приписаны все пользователи зарегистрированные в БД, автоматически попадают все пользователи и группы Windows)

Удалить роль нельзя.

Имеет минимальный набор прав: просмотр содержимого таблиц, выполнение ограниченного числа хранимых процедур для получения информации из БД master и пользовательских БД.

Роль для приложения – исключает неавторизованный доступ к данным вне рамок приложения.

Особенности:

- Для нее не определены члены, запускается только из приложения и дает набор прав только на время работы приложения
- Для активизации роль приложение должно передать серверу пароль
- До выхода из приложения пользователь имеет только права данной роли

Права доступа – права, дающие возможность доступа к объекту: выборка данных, добавление новых строк, обновление данных и т.д.

Владелец объекта может самостоятельно принимать решение о предоставлении прав доступа конкретным пользователям

Типы прав доступа:

- Право на выполнение инструкций SQL (statement permission) – набор прав на выполнение выражений
- Право на работу с объектами (object permission) – определяет набор прав пользователя при работе с данными или выполнении хранимых процедур
- Предопределенные права (predefined permission) – определяют набор действий для пользователей включенных в определенные стандартные роли или владельцам объектов БД

Представления – ограничивают данные доступные пользователям.

Хранимые процедуры – используются для обеспечения уровня безопасности, полностью скрывающего информацию, доступную пользователю или деловым процессам, происходящим при манипулировании данными.

9.4.4. Дополнительные меры безопасности

1. Определение работника ответственного за безопасность
2. Организация физической безопасности
3. Организация защиты локальной сети: отсоединение узлов не имеющих реально подключенных компьютеров и токенов безопасности для генерации паролей
4. Организация защищенного удаленного доступа: определение безопасных IP-адресов, использование брандмауэра, изменение пароля для файл – серверов, аудит удаленных транзакций
5. Обеспечение безопасности приложений: реализация дерева прав доступа, аудит ограничения на суммы денежных переводов.