МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«МИРЭА – Российский технологический университет»

РТУ МИРЭА

ЛЕКЦИОННЫЕ МАТЕРИАЛЫ (ПРЕЗЕНТАЦИИ К ЛЕКЦИОННЫМ МАТЕРИАЛАМ)

Безопасность систем баз данных

(наименование дисциплины (модуля) в соответствии с учебным планом)

Уровень	специалист
	(бакалавриат, магистратура, специалитет)
Форма обучения	очная
	(очная, очно-заочная, заочная)
Направление(-я) подготовки	10.03.01 «Информационная безопасность автоматизированных систем»
	(код и наименование)
Институт	Кибербезопасности и цифровых технологий
	(полное и краткое наименование)
Кафедра	Информационно-аналитические системы кибербезопасности (КБ-2)
	(полное и краткое наименование кафедры, реализующей дисциплину (модуль))
Лектор	К.т.н., доцент Шукенбаев Айрат Бисенгалеевич
	(сокращенно – ученая степень, ученое звание; полностью – ФИО)

Используются в данной редакции с учебного года 2023/2024
(учебный год цифрами)

Проверено и согласовано «____» _____20___г.

_____ А.А. Бакаев
(подпись директора Института/Филиала с расшифровкой)

Москва 2024 г.

Ощущение полной безопасности наиболее опасно.
Илья Нисонович Шевелев
Везде, где есть жизнь, есть и опасность.
Ральф Уолдо Эмерсон

Безопасность систем баз данных.

Тема лекции: **Аутентификация пользователей базы данных**

Аутентификация, основанная на знании, Аутентификация, основанная на наличии, Аутентификация, основанная на биометрических характеристиках. Аутентификация пользователей в Oracle. Внешняя аутентификация пользователей в Oracle. Аутентификация на основе инфраструктуры сертификатов. Аутентификация в СУБД MS SQL Server.

Под *несанкционированным доступом к информации (НСД)*, согласно руководящим документам ФСТЭК (Гостехкомиссии), понимается доступ к информации, нарушающий установленные правила разграничения доступа и осуществляемый с использованием штатных средств, предоставляемых СВТ и АС.

Получение доступа к ресурсам информационной системы предусматривает выполнение трех процедур*: идентификации, аутентификации* и *авторизации*.

Идентификация – это присвоение пользователям идентификаторов и проверка предъявляемых идентификаторов по списку присвоенных.

Идентификация – **это присвоение** объекту уникального имени - идентификатора, и сравнение идентификатора со всем перечнем **присвоенных** идентификационных имен. Идентификатор должен однозначно характеризовать объект, т.е. у двух разных объектов не должно быть одинаковых идентификаторов

Идентификация (identification – отождествление, опознание, установление личности) - это присвоение объекту уникального имени - идентификатора, и сравнение идентификатора со всем перечнем присвоенных идентификационных имен. Идентификатор должен однозначно характеризовать объект, т.е. у двух разных объектов не должно быть одинаковых идентификаторов

Под **аутентификацией** понимается проверка и подтверждение подлинности образа идентифицированного субъекта, объекта, процесса.

Аутентификация (authentication - «реальный, подлинный», «он самый») – это проверка принадлежности пользователю предъявленного им идентификатора. Часто аутентификацию также называют подтверждением или проверкой подлинности.

Авториза́ция (authorization «разрешение; уполномочивание») — предоставление определенному лицу или группе лиц прав на выполнение определённых действий; а также процесс проверки (подтверждения) данных прав при попытке выполнения этих действий.

Сущность процедуры идентификации состоит в назначении пользователю, т. е. объекту – потребителю ресурсов сервера баз данных – имени.

Имя пользователя – это некоторая уникальная метка, соответствующая принятым соглашениям именования и обеспечивающая однозначную идентификацию объекта реального мира в пространстве отображаемых объектов.

Сущность процедуры аутентификации состоит в подтверждении подлинности пользователя, представившего идентификатор.

Сущность процедуры авторизации состоит в определении перечня конкретных информационных ресурсов, с которыми аутентифицированному пользователю разрешена работа.

Часто процедуры идентификации и аутентификации в автоматизированных системах называют **Login-процедурами**.

Эффективность процедур идентификации и аутентификации существенным образом влияет на эффективность системы безопасности в целом. Процедура идентификации начинается с установления соединения пользователя с системой. Пользователь должен идентифицировать себя и представить системе некоторые параметры процедуры аутентификации. Если подсистема аутентификации принимает предъявленные значения параметров, то Login-процесс завершается успешно и устанавливается сессия взаимодействия пользователя с ИС.

Для защищенных ИС подсистема аудита обязана регистрировать как успешные, так и неуспешные Login-процессы.

Можно выделить три типа принципов, лежащих в основе конкретных процедур аутентификации:

— аутентификация, основанная на знании;
— аутентификация, основанная на наличии;
— аутентификация, основанная на проверке характеристик.

Аутентификация, основанная на знании

Достоинством процедур аутентификации, основанной на знании, является ее **простота**.

Для обеспечения надежной защиты от кражи паролей пользователи системы должны быть проинструктированы о:

— недопустимости ввода пароля из командной строки;
— необходимости хранения пароля в тайне от других пользователей, включая администраторов операционной системы;
— необходимости немедленной смены пароля после его компрометации;
— необходимости регулярной смены пароля;
— недопустимости записи пароля на бумагу или в файл.

Для обеспечения надежной защиты от кражи паролей пользователи системы должны быть проинструктированы о:
— недопустимости ввода пароля из командной строки;
— необходимости хранения пароля в тайне от других пользователей, включая администраторов операционной системы;
— необходимости немедленной смены пароля после его компрометации;
— необходимости регулярной смены пароля;
— недопустимости записи пароля на бумагу или в файл.

Существует целый ряд методов, позволяющих несколько уменьшить угрозу компрометации паролей пользователей

1. *Ограничение срока действия пароля*
2. *Ограничения на содержание пароля*

Обычно используются следующие условия:
— длина, пароля не должна быть меньше некоторого количества символов;
— в литературе по компьютерной безопасности и в документации по операционным системам обычно рекомендуется запрещать использование паролей короче 6-8 символов;
— в пароль должно входить по крайней мере 5-7 различных символов;
— в пароль должны входить как строчные, так и заглавные буквы;
— пароль пользователя не должен совпадать с его именем;
— пароль не должен присутствовать в списке «легко угадываемых» паролей, хранимом в системе.

3. *Блокировка терминала*.

Параметрами данного метода являются:
— максимально допустимое количество неудачных попыток входа в систему с одного терминала;
— интервал времени, после которого счетчик неудачных попыток входа обнуляется;
— длительность блокировки терминала (может быть сделана неограниченной – в этом случае блокировка терминала может быть снята только администратором системы).

Блокировка пользователя
Генерация паролей операционной системой
Пароль и отзыв
Разовый пароль.

Аутентификация, основанная на наличии

В информационных системах используется комплексная процедура, состоящая из двух этапов.

На первом этапе пользователь системы предъявляет предмет: электронный ключ, смарт-карту или специализированную микросхему (токен), которые вводятся в соответствующее устройство считывания.

На втором этапе пользователь вводит свой персональный идентификационный номер (PIN) для доказательства того, что он является действительным владельцем предмета и имеет право доступа к определенным информационным ресурсам.

Для затруднения такого подбора используются следующие меры защиты:

— защита ключевого носителя от копирования;

— блокировка или уничтожение ключевой информации после определенного количества неудачных попыток ввода пароля на доступ к ключу.

Если в качестве носителя ключевой информации применяются ***электронные ключи Touch Memory*** или ***пластиковые карты Memory Card***, эти меры защиты неприменимы.

Аутентификация, основанная на биометрических характеристиках

Аутентификация, основанная на проверке характеристик, чаще всего строится на биометрических характеристиках человека (отпечатки пальцев, рисунок радужной оболочки глаза и т. п.).

Сравнительная характеристика алгоритмов уничтожения информации

Алгоритм	Содержание алгоритма
Руководство по защите информации МО США (NISPOM) DoD 5220.22-M, 1995г.	Количество циклов записи - 3. Цикл 1 - запись произвольного кода. Цикл 2 - запись дополнения к нему. Цикл 3 - запись случайных кодов.
NIST SP 800-88 Guidelines for Media Sanitization	обзор проблематики гарантированного уничтожения данных)
NAVSO P-5239-26 - используется ВМС США	предусматривает 3 цикла перезаписи, сначала все "1", затем все "#7FFFFF", затем псевдослучайная последовательность, после чего происходит процедура верификации)
AFSSI S020 - стандарт ВВС США	первый цикл - все "0", затем все "F", затем псевдослучайные числа, а затем верификация 10%перезаписанных данных)
Стандарт VISR, 1999г. (Германия)	Количество циклов записи - 3. Цикл 1 - запись нулей. Цикл 2 - запись единиц. Цикл 3 - запись кода с чередованием нулей и единиц.
ГОСТ Р50739-95г. (Россия). Этот алгоритм соответствует второму классу защищенности из шести по классификации ФСТЭК	Количество циклов записи - 2. Цикл 1 - запись нулей. Цикл 2 - запись случайных кодов.
Алгоритм Брюса Шнейера	Количество циклов записи - 7. Цикл 1- запись единиц. Цикл 2 - запись нулей. Циклы 3..7 - запись случайных кодов
Алгоритм Питера Гутманна	Количество циклов - 35. Циклы 1..4 - запись произвольного кода. Циклы 5..9 - запись специальных комбинаций Циклы 10..25 - последовательная запись комбинаций от 00 до FFh.

Практическая реализация данного механизма аутентификации неизбежно создает следующие проблемы:

— поскольку псевдопользователи не являются людьми и, следовательно, не имеют биометрических характеристик, для их аутентификации должен поддерживаться альтернативный механизм;

— при двух последовательных входах в систему одного и того же человека его биометрические характеристики никогда в точности не совпадают;

— большинство биометрических характеристик человека постепенно меняются со временем, что заставляет регулярно корректировать эталонный образ идентифицирующей информации;

— биометрические характеристики человека могут испытывать резкие кратковременные изменения;

— аутентификация пользователя на основе биометрических характеристик требует применения дорогостоящей аппаратуры для получения образа используемой характеристики и сложных вычислительных алгоритмов для сравнения этого образа с эталонным.

Криптограф Цутому Мацумото.

***Брюс Шнáйер (Bruce Schneier** — американский криптограф, писатель и специалист по компьютерной безопасности. Автор нескольких книг по безопасности, криптографии и информационной безопасности. Основатель криптографической компании Counterpane Internet Security, Inc., член совета директоров Международной ассоциации криптологических исследований и член консультативного совета Информационного центра электронной приватности, также работал на Bell Labs и Министерство обороны США.*

Аутентификация пользователей в Oracle

В СУБД промышленного уровня процедура аутентификации может быть полностью внешней, т.е. реализуемой средствами операционной системы (например, *в IBM DB2*), либо внутренней (например в *Oracle*).

CONNECT

Oracle использует два класса методов аутентификации — на основе паролей и на основе цифровых сертификатов

CREATE USER

GRANT CREATE SESSION TO *имя_пользователя*;

```
SQL> CONNECT SYSTEM/MANAGER@EDUC;
Connected
SQL> CONNECT USER ul IDENTIFIED by ulPSW
User created;
SQL> CONNECT ul/ulPSW@EDUC
EROR: ORA-010117: invalid username/password; logon denied
Warning: You are no longer connected to Oracle/
SQL> CONNECT SYSTEM/MANAGER@EDUC;
Connected
SQL> GRANT CREATE SESSION TO ul;
GRANT succeeded/
SQL> CONNECT ul/ulPSW@EDUC;
Connected
```

Листинг 1. Регистрация пользователя в Oracle и предоставление ему минимальных прав доступа.

Метод аутентификацией *BASIC_ORACLE*

С помощью профиля можно применить правила управления паролями, которые могут быть выбраны как опции при настройке (профиль — это объект базы данных, в котором, в частности, могут быть указаны ограничения на использование паролей):

— блокировка учетной записи пользователя;

— время жизни пароля и прекращение его действия по истечении срока.

— предыстория паролей. Администратор базы данных может корректировать правила повторного использования пароля с помощью оператора *CREATE PROFILE*;

— контроль уровня сложности пароля.

Листенер (слушатель) Oracle Net Listener — служба, которая действует только на сервере и прослушивает входящие запросы на подключение. Oracle предоставляет утилиту lsnrctl, управляющую процессом листенера. Место слушателя в сетевой обработке Oracle можно кратко описать следующим образом.

С помощью TNS Listener Oracle база данных регистрирует информацию о службах, экземплярах и обработчиках служб.

Клиент устанавливает начальное соединение со слушателем.

Слушатель принимает и проверяет запрос на подключение клиента и передает его обработчику службы базы данных. Как только слушатель передает запрос клиента, он устраняется из процесса обслуживания данного подключения.

Файл listener.ora, который по умолчанию размещается в каталоге $ORACLE_HOME/network/admin в системах UNIX и в каталоге $ORACLE_HOME\network\admin в системах Windows, содержит информацию о конфигурации Listener Oracle. Поскольку служба слушателя действует только на сервере, клиентские компьютеры не содержат никакого файла listener.ora. Типичный файл listener.ora приведен в листинге ниже.

Все параметры конфигурации в этом файле имеют значения по умолчанию. Поэтому службу листенера не обязательно конфигурировать вручную. После создания первой базы данных на сервере служба TNS Listener Oracle автоматически запускается, и файл конфигурации слушателя, listener.ora, помещается в каталог, определенный по умолчанию. При создании новой базы данных ее информация о сетевых подключений и службах автоматически добавляется в файл конфигурации tns listener Oracle**. При запуске экземпляра база данных автоматически регистрируется в слушателе, и слушатель начинает прослушивать запросы на подключение к этой базе данных**.

Файл пароля для администраторов базы данных необязателен и может быть установлен с помощью утилиты *ORAPWD*. Файл пароля ограничивает привилегии администрирования только тех пользователей, которые знают пароль и имеют специальные роли — *SYSOPER* и *SYSDBA*.

Роль SYSOPER предоставляет возможность выполнять операторы *STARTUP, SHUTDOWN, ALTER DATABASE OPEN/MOUNT, ALTER DATABASE BACKUP, ARCHIVE LOG* и *RECOVER*, а также включает привилегию *RESTRICTED SESSION*.

Роль SYSDBA включает все системные привилегии с опцией *ADMIN OPTION*.

Средства управления паролями Oracle.

Среди средств управления паролями в Oracle следует отметить блокировку учетных записей, уменьшение и окончание их срока действия, сохранение истории паролей и предварительную проверку надежности пароля (*proactive checking*).

Для активизации управления паролями следует запустить сценарий *utlpwdmg.sql*

resource__limit в файле init.ora

Используемая по умолчанию функция выполняет комплексную проверку надежности пароля согласно приведенным ниже критериям:

— пароль содержит не менее четырех символов;

— пароль не совпадает с учетным именем;

— пароль содержит, по крайней мере, по одной букве, цифре, и знаку пунктуации;

— новый пароль отличается от прежнего, по крайней мере, тремя символами.

Предлагаемые по умолчанию параметры пароля для команды *CREATE PROFILE*

Параметр	*Значение по умолчанию*	*Единица измерения*
Failed_login_attempts	3	Безразмерное число
Password_life_time	60	День
Password_reuse_time	180	День
Password_reuse_max	Не ограничено	Безразмерное число
Password_lock_time	1	Безразмерное число
Password_grace_time	10	День
Password_verify_function	По умолчанию	Функция

```
myauthfunction (p_userid IN varchar2(30), p_new_password
IN varchar2(30), p_old_password IN varchar2(30)
return Boolean;
```

```
SQL> CONNECT SYSTEM/VFNFGER@EDUC;
Connected.
Connected
```

Листинг 2. Пример задания профиля пользователя и проверки ограничений на свойства нового пароля

Внешняя аутентификация пользователей в Oracle

Чтобы использовать эту опцию, необходимо установить в файле базы данных ***init.ora*** параметр ***OSAUTHENTPREFIX***. Это укажет СУБД Oracle, что пользователь, имя которого имеет тот же префикс, должен рассматриваться как подлежащий внешней идентификации.

Например, если для параметра ***OSAUTHENTPREFIX*** установлено значение ***ops$*** и имеются два пользователя — ***ops$jones*** и ***smith***, то для системы Oracle не требуется пароль от пользователя ***ops$jones***, но необходим ввод пароля для пользователя ***smith***. Данным параметром может быть установлен любой желаемый префикс (включая пустую строку). В таком случае указывается пустое значение в двойных кавычках.

При этом для параметра ***REMOTE_OS_AUTHENT*** в файле ***init.ora*** должно быть установлено значение ***true*** (значение по умолчанию — false), чтобы система Oracle могла использовать имя пользователя из незащищенного соединения. Так можно защититься от потенциального компьютерного взломщика, выдающего себя за корректного пользователя.

Аутентификация на основе инфраструктуры сертификатов

Хотя аутентификация может осуществляться как для физических пользователей, так и для псевдопользователей — фиктивных пользователей, используемых операционной системой для запуска системных процессов, наибольший интерес с точки зрения обеспечения ЗИ в операционной системе представляет аутентификация физических пользователей.

Аутентификация на основе инфраструктуры сертификатов

Основу механизма аутентификации составляют сертификаты стандарта X.509, которые поддерживаются на сервере, выполняющем функции сертификационного центра.

Утилита **Oracle Security Server** — это программный инструмент, который позволяет администратору базы данных или администратору режима безопасности поддерживать режим безопасности в глобальной среде.

В Oracle Security Server Release 1 сертификаты можно оформлять только для Web-серверов, а в Release 2 — также для клиентов и серверов Net8. Согласно документации Oracle, сертификаты оформляются в Oracle Security Server в соответствии с международными стандартами X.509.

Эти сертификаты используются с протоколом Secure Sockets Layer (SSL). SSL обеспечивает шифрование и проверку целостности данных при передаче по сети.

Oracle позволяет использовать способы аутентификации, базирующиеся на протоколе *RADIUS (DIAMETER).*

RADIUS (Remote Authentication Dial In User Service) — сетевой протокол, предназначенный для обеспечения централизованной аутентификации, авторизации и учёта (Authentication, Authorization, and Accounting, AAA) пользователей, подключающихся к различным сетевым службам.

DIAMETER — сеансовый протокол, созданный, отчасти, для преодоления некоторых ограничений протокола RADIUS. Обеспечивает взаимодействие между клиентами в целях аутентификации, авторизации и учёта различных сервисов (AAA).

1. Сервер RADIUS (DIAMETER) передает пароль серверу приложения.
2. Сервер передает пароль машине клиента.
3. Пароль выводится для конечного пользователя.
4. Пользователь вводит отзыв на полученный пароль.
5. Значение отзыва возвращается на сервер.
6. Сервер контролирует полученное значение и передает на сервер приложения ответ с указанием принять или отклонить запрос на соединение с данным пользователем.

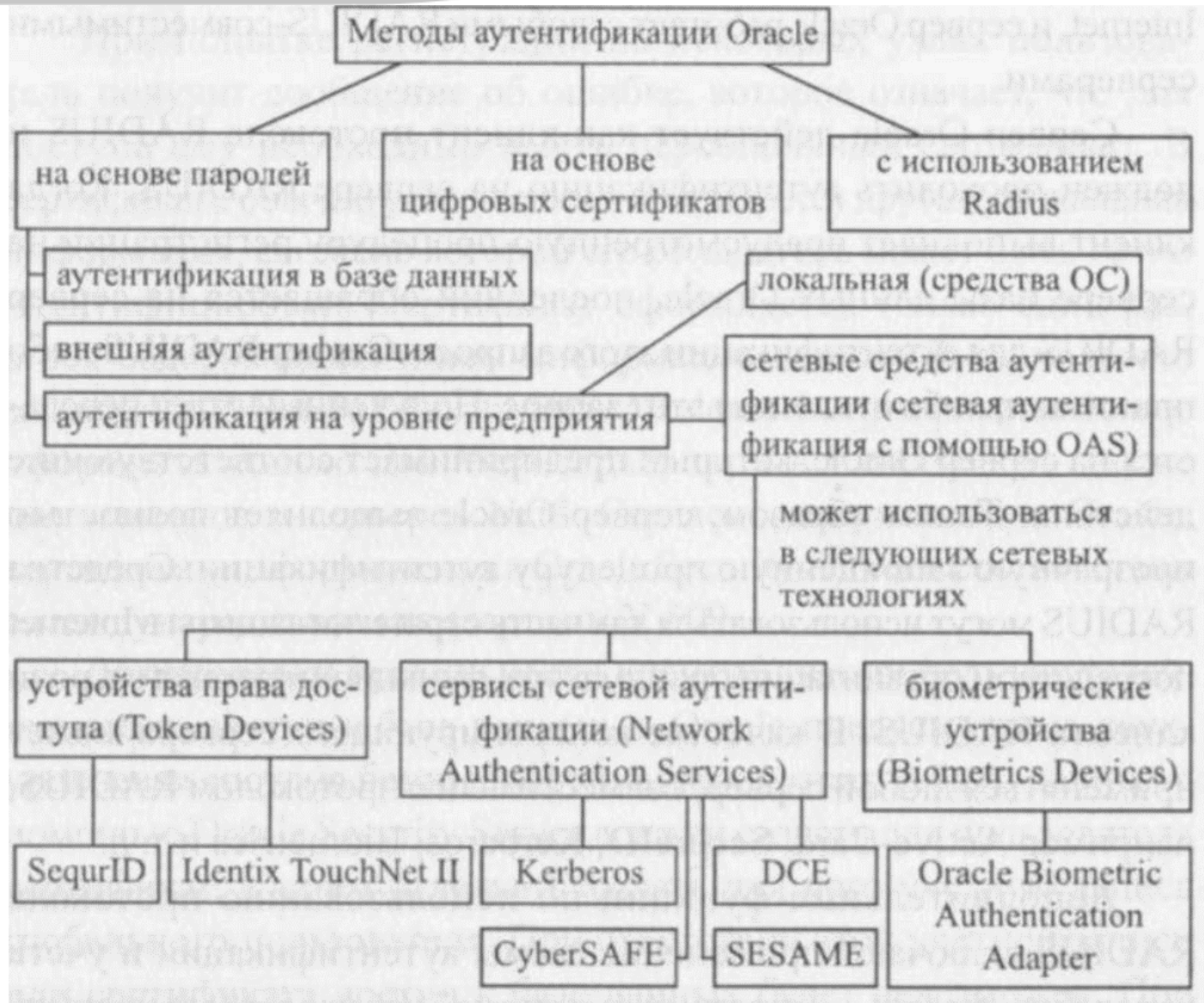

Рис. 1 Методы аутентификации СУБД Oracle

Аутентификация в СУБД MS SQL Server

Выполним анализ наиболее важных понятий безопасности баз данных, после чего рассмотрим конкретные возможности системы безопасности компонента *Database Engine*.

Наиболее важными концепциями безопасности баз данных являются следующие:

- *аутентификация;*
- *шифрование;*
- *авторизация;*
- *отслеживание изменений.*

Аутентификация заключается в предоставлении ответа на следующий вопрос: «Имеет ли данный пользователь законное право на доступ к системе?». Аутентификацию можно реализовать путем запроса, требуя, чтобы пользователь предоставил, например, следующее:

♦ нечто, что известно пользователю;

♦ нечто, что принадлежит пользователю;

♦ физические характеристики пользователя.

Шифрование данных представляет собой процесс кодирования информации таким образом, что она становится непонятной, пока не будет расшифрована пользователем.

Авторизация – это процесс, который применяется к пользователям, уже получившим доступ к системе, пройдя через процесс аутентификации, чтобы определить их права на использование определенных ресурсов.

Отслеживание изменений означает отслеживание и документирование действий несанкционированных пользователей.

Для поддержки авторизации компонент *Database Engine* использует инструкции языка *Transact-SQL* **GRANT, DENY** и **REVOKE**.

Прежде чем приступить к рассмотрению этих **четырех концепций безопасности**, сначала ознакомимся с кратким определением модели безопасности, которая применяется в *SQL Server*. Данная модель безопасности состоит из трех разных категорий, которые взаимодействуют друг с другом:

♦ Принципалы (principals).

- *Windows*
- роли *SQL Server*.

♦ *Защищаемые объекты* (securables).

Разрешения (permissions).

Режимы аутентификации

Система безопасности компонента Database Engine состоит из двух разных подсистем безопасности:

♦ системы безопасности *Windows*;

♦ системы безопасности *SQL Server*.

На основе этих двух подсистем безопасности компонент *Database Engine* может работать в одном из следующих режимов аутентификации:

♦ в режиме Windows;

♦ в смешанном режиме.

Режим *Windows* требует, чтобы пользователи входили в систему баз данных исключительно посредством своих учетных записей *Windows*. Такой способ подключения к системе баз данных называется *доверительным соединением* (*trusted connection*).

Смешанный режим позволяет пользователям подключаться к компоненту *Database Engine* посредством аутентификации Windows или аутентификации *SQL Server*.

Разрешения и соответствующие защищаемые объекты

Разрешение	Применение	Описание
SELECT	Таблицы и их столбцы, синонимы, представления и их столбцы, возвращающие табличные значения функции	Предоставляет возможность выборки (чтения) строк. Это разрешение можно ограничить одним или несколькими столбцами, перечислив требуемые столбцы. (Если список столбцов отсутствует, то разрешение применимо ко всем столбцам таблицы)
INSERT	Таблицы и их столбцы, синонимы, представления и их столбцы	Предоставляет возможность вставлять столбцы
UPDATE	Таблицы и их столбцы, синонимы, представления и их столбцы	Предоставляет возможность изменять значения столбцов. Это разрешение можно ограничить одним или несколькими столбцами, перечислив требуемые столбцы. (Если список столбцов отсутствует, то разрешение применимо ко всем столбцам таблицы)
DELETE	Таблицы и их столбцы, синонимы, представления и их столбцы	Предоставляет возможность удалять столбцы
REFERENCES	Определяемые пользователем функции (SQL и среды CLR), таблицы и их столбцы, синонимы, представления и их столбцы	Предоставляет возможность обращаться к столбцам внешнего ключа в родительской таблице, когда пользователь не имеет разрешения SELECT для этой таблицы
EXECUTE	Хранимые процедуры (SQL и среды CLR), определяемые пользователем функции (SQL и среды CLR), синонимы	Предоставляет возможность выполнять указанную хранимую процедуру или определенную пользователем функцию
CONTROL	Хранимые процедуры (SQL и среды CLR), определяемые пользователем функции (SQL и среды CLR), синонимы	Предоставляет возможности, подобные возможностям владельца; получатель имеет практически все разрешения, определенные для защищаемого объекта. Принципал, которому было предоставлено разрешение CONTROL, также имеет возможность предоставлять разрешения на данный защищаемый объект. Разрешение CONTROL на определенной области видимости неявно включает разрешение CONTROL для всех защищаемых объектов в этой области видимости
ALTER	Хранимые процедуры (SQL и среды CLR), определяемые пользователем функции (SQL и среды CLR), таблицы, представления	Предоставляет возможность изменять свойства (за исключением владения) защищаемых объектов. Когда это право предоставляется применимо к области, оно также предоставляет права на выполнение инструкций ALTER, CREATE и DROP на любых защищаемых объектах в данной области
TAKE OWNERSHIP	Хранимые процедуры (SQL и среды CLR), определяемые пользователем функции (SQL и среды CLR), таблицы, представления, синонимы	Предоставляет возможность становиться владельцем защищаемого объекта, для которого оно применяется
VIEW DEFINITION	Хранимые процедуры (SQL и среды CLR), определяемые пользователем функции (SQL и среды CLR), таблицы, представления, синонимы	Предоставляет получателю возможность просматривать метаданные защищаемого объекта
CREATE	Нет данных	Предоставляет возможность создавать защищаемые объекты сервера
CREATE (	Нет данных	Предоставляет возможность создавать защищаемые объекты базы данных

Выбор одного из доступных режимов аутентификации осуществляется посредством среды *SQL Server Management Studio*. Чтобы установить режим аутентификации *Windows*, щелкните правой кнопкой сервер баз данных и в контекстном меню выберите пункт *Properties*. Откроется диалоговое окно *Server Properties*, в котором нужно выбрать страницу *Security*, а на ней *Windows Authentication Mode*. Для выбора смешанного режима в этом же диалоговом окне *Server Properties* вам нужно выбрать *Server and Windows Authentication Mode*.

После успешного подключения пользователя к компоненту *Database Engine* его доступ к объектам базы данных становится независимым от использованного способа аутентификации для входа в базу данных – аутентификации *Window* или *SQL Server* аутентификации.