# 1 Показать и объяснить, какой режим аутентификации используется для экземпляра SQL Server.

* Режим проверки подлинности Windows является режимом по умолчанию. Поскольку эта модель безопасности SQL Server тесно интегрирована с Windows, часто ее называют встроенной функцией безопасности. Для входа в SQL Server в список надежных элементов вносятся определенные учетные записи пользователей и группы Windows. Пользователям Windows, которые уже прошли аутентификацию, не нужно представлять дополнительные учетные данные.
* Режим смешанной аутентификации поддерживает проверку подлинности как средствами Windows, так и средствами SQL Server. Пары имен пользователей и паролей хранятся в SQL Server.

# 

# 1. Поясните схему безопасности в SQL Server.

Существует два вида схем безопасности в Microsoft SQL Server: безопасность SQL Server и доверенная проверка подлинности (также известная как проверка подлинности Windows). Безопасность SQL Server — стандартная комбинация имени пользователя для регистрации и пароля, а доверенная проверка подлинности предполагает, что устройство, которое пытается подключиться к экземпляру SQL Server, одобрено процедурой проверки подлинности домена, и результаты этой проверки переданы экземпляру SQL Server: считается, что домен, в котором размещен экземпляр SQL Server, доверяет учетной записи пользователя — проверка выполнена ранее.

# 2. Что такое принципалы и подзащитные?

**Участники** – **security principals** – объекты, которым может быть выдано право доступа к определенным объектам базы данных, имеют уникальный SID

**Объекты** – **securables** – это объекты, доступ к которым контролируется

# 3. Перечислите встроенные роли сервера, покажите, какие они имеют привилегии.

Bulkadmin – копирование

Dbcreator – создание БД

Diskadmin – упр-е дисковыми файлами

Processadmin – управление процессами

Securityadmin – безопасность

Serveradmin – конфигурация сервера

Setupadmin – процедуры запуска

Sysadmin – любые действия, безотзывная

# 4. Перечислите встроенные роли базы данных, покажите, какие они имеют привилегии.

public

db\_accessadmin

db\_backupoperator

db\_datareader и db\_datawriter

db\_denydatareader и db\_denydatawriter

db\_dlladmin

db\_owner

https://docs.microsoft.com/ru-ru/sql/relational-databases/security/authentication-access/database-level-roles?view=sql-server-ver15

# 5. Что такое имперсонификация?

Администратор или другой привилегированный пользователь может зайти в систему от имени другого пользователя и проверить, есть ли у того доступ тем или иным приложениям.

# 6. Что такое цепочка владения?

пропускает проверку привилегий для улучшения производительности для двух объектов с одинаковым владельцем

# 7. Поясните схему аудита в SQL Server.

Аудит – отслеживание и протоколирование событий, происходящих на сервере

Аудит SQL Server:

* аудит сервера для событий на уровне сервера
* аудит баз данных для событий на уровне базы данных

# 8. Куда могут записываться события аудита в SQL Server?

Журнал аудита:

* файл файловой системы
* журнал Windows Application Log
* Windows Security Log

# 9. Поясните свойства серверного аудита.

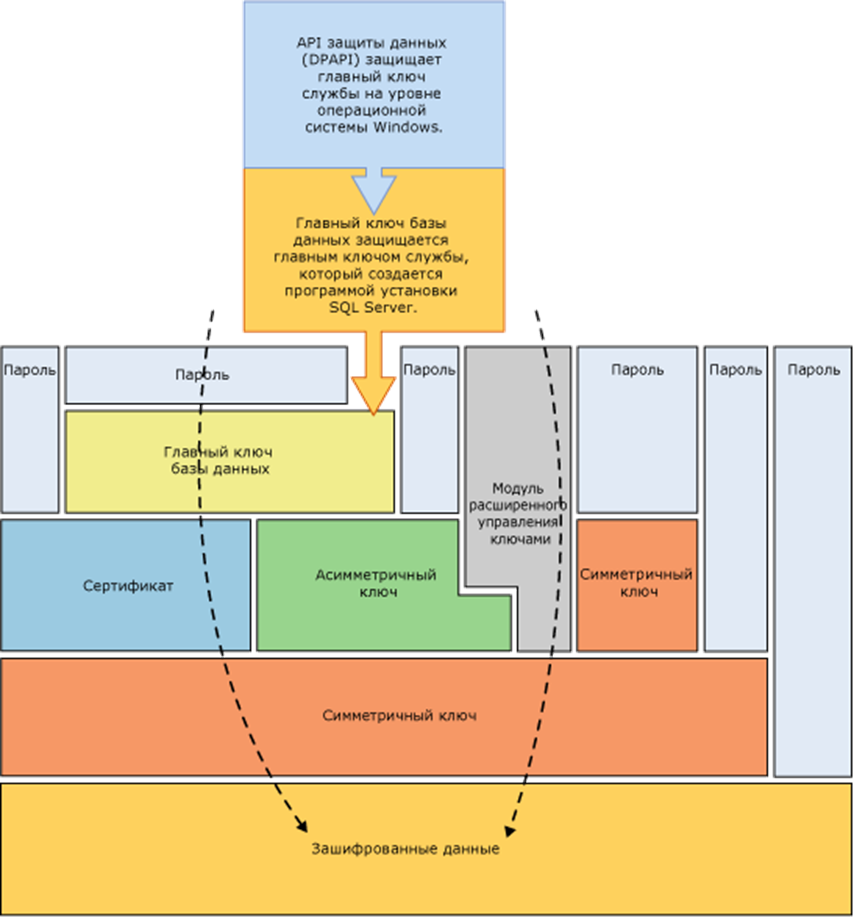
# 10. Поясните группы событий серверного аудита.

# 11. Поясните свойства аудита БД.

# 12. Поясните группы событий аудита БД.

# 

# 13. Поясните схему ключей шифрования в SQL Server.



# 14. Какие представления каталога, связанные с шифрованием, вы знаете?

[sys.asymmetric\_keys](https://docs.microsoft.com/ru-ru/sql/relational-databases/system-catalog-views/sys-asymmetric-keys-transact-sql?view=sql-server-ver15)

[sys.cryptographic\_providers](https://docs.microsoft.com/ru-ru/sql/relational-databases/system-catalog-views/sys-cryptographic-providers-transact-sql?view=sql-server-ver15)

[sys.certificates](https://docs.microsoft.com/ru-ru/sql/relational-databases/system-catalog-views/sys-certificates-transact-sql?view=sql-server-ver15)

[sys.key\_encryptions](https://docs.microsoft.com/ru-ru/sql/relational-databases/system-catalog-views/sys-key-encryptions-transact-sql?view=sql-server-ver15)

[sys.column\_encryption\_key\_values](https://docs.microsoft.com/ru-ru/sql/relational-databases/system-catalog-views/sys-column-encryption-key-values-transact-sql?view=sql-server-ver15)

[sys.openkeys](https://docs.microsoft.com/ru-ru/sql/relational-databases/system-catalog-views/sys-openkeys-transact-sql?view=sql-server-ver15)

[sys.column\_encryption\_keys](https://docs.microsoft.com/ru-ru/sql/relational-databases/system-catalog-views/sys-column-encryption-keys-transact-sql?view=sql-server-ver15)

[sys.security\_policies (Transact-SQL)](https://docs.microsoft.com/ru-ru/sql/relational-databases/system-catalog-views/sys-security-policies-transact-sql?view=sql-server-ver15)

[sys.column\_master\_keys](https://docs.microsoft.com/ru-ru/sql/relational-databases/system-catalog-views/sys-column-master-keys-transact-sql?view=sql-server-ver15)

[sys.security\_predicates (Transact-SQL)](https://docs.microsoft.com/ru-ru/sql/relational-databases/system-catalog-views/sys-security-predicates-transact-sql?view=sql-server-ver15)

[sys.crypt\_properties](https://docs.microsoft.com/ru-ru/sql/relational-databases/system-catalog-views/sys-crypt-properties-transact-sql?view=sql-server-ver15)

[sys.symmetric\_keys](https://docs.microsoft.com/ru-ru/sql/relational-databases/system-catalog-views/sys-symmetric-keys-transact-sql?view=sql-server-ver15)