# 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

**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

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

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

**Bulkadmin** – могут выполнять инструкцию BULK INSERT (Массовая вставка)

**Dbcreator** – могут создавать, изменять, удалять и восстанавливать любые базы данных.

**Diskadmin** – используется для управления файлами на диске.

**Processadmin** – управление процессами

**Securityadmin** – управляют именами входа и их свойствами

**Serveradmin** – могут изменять параметры конфигурации на уровне сервера, а также выключать сервер

**Setupadmin** – могут добавлять или удалять связанные серверы с помощью инструкций Transact-SQL

**Sysadmin** – могут выполнять любые действия на сервере.

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

**public**

**db\_accessadmin** - могут добавлять или удалять права удаленного доступа к базе данных для имен входа и групп

**db\_backupoperator** - могут создавать резервные копии базы данных

**db\_datareader** - могут считывать все данные из всех пользовательских таблиц и представлений.

**db\_datawriter** - могут добавлять, удалять или изменять данные во всех пользовательских таблицах.

**db\_denydatareader** - не могут считывать никакие данные из пользовательских таблиц или представлений в базе.

**db\_denydatawriter** - не могут добавлять, изменять или удалять данные в пользовательских таблицах базы данных.

**db\_owner** - могут выполнять все действия по настройке и обслуживанию базы данных, а также удалять (drop) базу данных в SQL Server.

<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 к 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.

* Детальный анализ аппаратных и программных компонентов сервера;
* Оценка надежности оборудования;
* Проверка актуальности серверного ПО;
* Оценка состояния работающих служб;
* Анализ сетевых настроек на сервере;
* Оценка показателей отказоустойчивости.
* Анализ эффективности работы.

# 10. Поясните группы событий серверного аудита.

**APPLICATION\_ROLE\_CHANGE\_PASSWORD\_GROUP** - при изменении пароля для роли приложения

**BACKUP\_RESTORE\_GROUP** - вызывается командой резервного копирования или восстановления

**FAILED\_LOGIN\_GROUP** - участник выполнил попытку входа в SQL Server , которая завершилась неудачно.

**LOGOUT\_GROUP** - участник отключился от SQL Server.

**TRANSACTION\_GROUP** - вызывается для операций BEGIN TRANSACTION, **ROLLBACK TRANSACTION и COMMIT TRANSACTION** как при явных вызовах этих инструкций, так и при неявных операциях с транзакциями

# 11. Поясните свойства аудита БД.

1. Организация быстрой и слаженной работы всех элементов базы данных;
2. Обновление базы до актуального на момент оценки состояния;
3. Устранение ошибок, влияющих на работу базы данных;
4. Определение и устранение причин, вызывающих ошибки в базе данных;
5. Оптимизация затрат временных ресурсов в работе с базой данных.

# 12. Поясните группы событий аудита БД.

**AUDIT\_CHANGE\_GROUP** - возникает при создании, изменении или удалении любого аудита

**USER\_CHANGE\_PASSWORD\_GROUP** - возникает при изменении пароля пользователя автономной базы данных с помощью инструкции ALTER USER

**FAILED\_DATABASE\_AUTHENTICATION\_GROUP** - попытка участника войти в автономную базу данных завершилась ошибкой

**DATABASE\_OPERATION\_GROUP** - вызывается при выполнении различных операций в базе данных

**DATABASE\_CHANGE\_GROUP** - вызывается при создании, изменении или удалении базы данных

# 13. Поясните схему ключей шифрования в SQL Server.

Используемые в SQL Server ключи шифрования представляют собой сочетание открытых, закрытых и симметричных ключей, которые используются для защиты конфиденциальных данных. Симметричный ключ создается во время инициализации SQL Server, при первом запуске экземпляра SQL Server. Этот ключ используется SQL Server для шифрования конфиденциальных данных, которые хранятся в SQL Server. Открытые и закрытые ключи создаются операционной системой и используются для защиты симметричного ключа. Пара из открытого и закрытого ключей создается для каждого экземпляра SQL Server, который сохраняет конфиденциальные данные в базе данных.

# 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) -Возвращает строку для каждого асимметричного ключа.

[**sys.cryptographic\_providers**](https://docs.microsoft.com/ru-ru/sql/relational-databases/system-catalog-views/sys-cryptographic-providers-transact-sql?view=sql-server-ver15)- Возвращает одну строку для каждого зарегистрированного поставщика служб шифрования.

[**sys.certificates**](https://docs.microsoft.com/ru-ru/sql/relational-databases/system-catalog-views/sys-certificates-transact-sql?view=sql-server-ver15) - Возвращает строку для каждого сертификата в базе данных.

[**sys.key\_encryptions**](https://docs.microsoft.com/ru-ru/sql/relational-databases/system-catalog-views/sys-key-encryptions-transact-sql?view=sql-server-ver15) - Возвращает по одной строке для каждого симметричного ключа шифрования, созданного с помощью инструкции CREATE SYMMETRIC KEY с предложением ENCRYPTION BY.

[**sys.openkeys**](https://docs.microsoft.com/ru-ru/sql/relational-databases/system-catalog-views/sys-openkeys-transact-sql?view=sql-server-ver15) - Это представление каталога возвращает сведения о ключах шифрования, открытых в текущем сеансе.

[**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)- Возвращает по одной строке для каждого главного ключа базы данных, добавленного с помощью инструкции [создания главного ключа](https://docs.microsoft.com/ru-ru/sql/t-sql/statements/create-column-master-key-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) - Возвращает по одной строке для каждого симметричного ключа, созданного инструкцией CREATE SYMMETRIC KEY.