**Теоретические вопросы:**

**1. 149-ФЗ «Об информации, информационных технологиях и о защите информации». Ключевые моменты.**

149-ФЗ «Об информации, информационных технологиях и о защите информации»

[149-ФЗ](http://www.consultant.ru/document/cons_doc_LAW_61798/) — главный закон об информации в России. Он определяет ключевые термины, например, говорит, что информация — это любые данные, сведения и сообщения, представляемые в любой форме. Также там описано, что такое сайт, электронное сообщение и поисковая система. Именно на этот закон и эти определения нужно ссылаться при составлении документов по информационной безопасности.

В 149-ФЗ сказано, какая информация считается конфиденциальной, а какая — общедоступной, когда и как можно ограничивать доступ к информации, как происходит обмен данными. Также именно здесь прописаны основные требования к защите информации и ответственность за нарушения при работе с ней.

Ключевые моменты закона об информационной безопасности:

1. Нельзя собирать и распространять информацию о жизни человека без его согласия.
2. Все информационные технологии равнозначны — нельзя обязать компанию использовать какие-то конкретные технологии для создания информационной системы.
3. Есть информация, к которой нельзя ограничивать доступ, например сведения о состоянии окружающей среды.
4. Некоторую информацию распространять запрещено, например ту, которая пропагандирует насилие или нетерпимость.
5. Тот, кто хранит информацию, обязан ее защищать, например, предотвращать доступ к ней третьих лиц.
6. У государства есть [реестр запрещенных сайтов](https://eais.rkn.gov.ru/). Роскомнадзор может вносить туда сайты, на которых хранится информация, запрещенная к распространению на территории РФ.
7. Владелец заблокированного сайта может удалить незаконную информацию и сообщить об этом в Роскомнадзор — тогда его сайт разблокируют.

**2. 152-ФЗ «О персональных данных». Ключевые моменты.**

## 152-ФЗ «О персональных данных»

[Этот закон](http://www.consultant.ru/document/cons_doc_LAW_61801/) регулирует работу с персональными данными — личными данными конкретных людей. Его обязаны соблюдать те, кто собирает и хранит эти данные. Например, компании, которые ведут базу клиентов или сотрудников.

Ключевые моменты закона:

1. Перед сбором и обработкой персональных данных нужно спрашивать согласие их владельца.
2. Для защиты информации закон обязывает собирать персональные данные только с конкретной целью.
3. Если вы собираете персональные данные, то обязаны держать их в секрете и защищать от посторонних.
4. Если владелец персональных данных потребует их удалить, вы обязаны сразу же это сделать.
5. Если вы работаете с персональными данными, то обязаны хранить и обрабатывать их в базах на территории Российской Федерации. При этом данные можно передавать за границу при соблюдении определенных условий, прописанных в законе — жесткого запрета на трансграничную передачу данных нет.

Серверы облачной платформы VK Cloud (бывш. MCS) находятся на территории РФ и соответствуют всем требованиям 152-ФЗ. В публичном облаке VK можно хранить персональные данные в соответствии с УЗ-2, 3 и 4. Для хранения данных с УЗ-2 и УЗ-1 также есть возможность сертификации, как в формате частного облака, так и на изолированном выделенном гипервизоре в ЦОДе VK.

При построении гибридной инфраструктуры для хранения персональных данных на платформе VK Cloud (бывш. MCS) вы получаете облачную инфраструктуру, уже соответствующую всем требованиям законодательства. При этом частный контур нужно аттестовать, в этом могут помочь специалисты VK, что позволит быстрее пройти необходимые процедуры.

**3. 98-ФЗ «О коммерческой тайне». Ключевые моменты.**

## 98-ФЗ «О коммерческой тайне»

[Этот закон](http://www.consultant.ru/document/cons_doc_LAW_48699/) определяет, что такое коммерческая тайна, как ее охранять и что будет, если передать ее посторонним. В нем сказано, что коммерческой тайной считается информация, которая помогает компании увеличить доходы, избежать расходов или получить любую коммерческую выгоду.

Ключевые моменты закона о защите информации компании:

1. Обладатель информации сам решает, является она коммерческой тайной или нет. Для этого он составляет документ — перечень информации, составляющей коммерческую тайну.
2. Некоторые сведения нельзя причислять к коммерческой тайне, например, информацию об учредителе фирмы или численности работников.
3. Государство может затребовать у компании коммерческую тайну по веской причине, например, если есть подозрение, что компания нарушает закон. Компания обязана предоставить эту информацию.
4. Компания обязана защищать свою коммерческую тайну и вести учет лиц, которым доступна эта информация.
5. Если кто-то разглашает коммерческую тайну, его можно уволить, назначить штраф или привлечь к уголовной ответственности.

**4. 63-ФЗ «Об электронной подписи». Ключевые моменты.**

## 63-ФЗ «Об электронной подписи»

[Этот закон](http://www.consultant.ru/document/cons_doc_LAW_112701/) касается электронной подписи — цифрового аналога физической подписи, который помогает подтвердить подлинность информации и избежать ее искажения и подделки. Закон определяет, что такое электронная подпись, какую юридическую силу она имеет и в каких сферах ее можно использовать.

Ключевые моменты закона:

1. Для создания электронной подписи можно использовать любые программы и технические средства, которые обеспечивают надежность подписи. Вы не обязаны использовать для этого какое-то конкретное государственное ПО.
2. Подписи бывают простые, усиленные неквалифицированные и усиленные квалифицированные. У них разные технические особенности, разные сферы применения и разный юридический вес. Самые надежные — усиленные квалифицированные подписи, они полностью аналогичны физической подписи на документе.
3. Те, кто работает с квалифицированной подписью, обязаны держать в тайне ключ подписи.
4. Выдавать электронные подписи и сертификаты, подтверждающие их действительность, может только специальный удостоверяющий центр.

**5. 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации». Ключевые моменты.**

## 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»

[Этот закон](http://www.consultant.ru/document/cons_doc_LAW_220885/) касается компаний, которые работают в сферах, критически важных для жизни государства — таких, что сбой в их работе отразится на здоровье, безопасности и комфорте граждан России.

К таким сферам относится здравоохранение, наука, транспорт, связь, энергетика, банки, топливная промышленность, атомная энергетика, оборонная промышленность, ракетно-космическая промышленность, горнодобывающая промышленность, металлургическая промышленность и химическая промышленность. Также сюда относят компании, которые обеспечивают работу предприятий из этих сфер, например, предоставляют оборудование в аренду или разрабатывают для них ПО.

Если на предприятии из этой сферы будет простой, это негативно отразится на жизни всего государства. Поэтому к IT-инфраструктуре и безопасности информационных систем на этих предприятиях предъявляют особые требования.

Ключевые моменты закона об информационной безопасности критически важных структур:

1. Для защиты критической инфраструктуры существует Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА).
2. Объекты критически важной инфраструктуры обязаны подключиться к ГосСОПКА. Для этого нужно купить и установить специальное ПО, которое будет следить за безопасностью инфраструктуры компании.
3. Одна из мер предупреждения — проверка и сертификация оборудования, ПО и всей инфраструктуры, которая используется на критически важных предприятиях.
4. Субъекты критической информационной инфраструктуры обязаны сообщать об инцидентах в своих информационных системах и выполнять требования государственных служащих. Например, использовать только сертифицированное ПО.
5. Все IT-системы критически важных предприятий должны быть защищены от неправомерного доступа и непрерывно взаимодействовать с ГосСОПКА.
6. При разработке IT-инфраструктуры критически важные предприятия должны руководствоваться [239 приказом ФСТЭК](https://fstec.ru/en/53-normotvorcheskaya/akty/prikazy/1592-prikaz-fstek-rossii-ot-25-dekabrya-2017-g-n-239). В нем прописаны основные требования к защите информации на таких предприятиях.
7. Государство имеет право проверять объекты критически важной инфраструктуры, в том числе внепланово, например, после компьютерных инцидентов вроде взлома или потери информации.

**6. Аппаратные средства защиты информации.**

Программно-аппаратные средства защиты информации— это сервисы безопасности, встроенные в сетевые операционные системы.

К аппаратным средствам защиты информацииотносятся электронные и электронно-механические устройства, включаемые в состав технических средств КС и выполняющие (самостоятельно или в едином комплексе с программными средствами) некоторые функции обеспечения информационной безопасности. Критерием отнесения устройства к аппаратным, а не к инженерно-техническим средствам защиты является обязательное включение в состав технических средств КС.

К основным аппаратным средствамзащиты информации относятся:

* устройства для ввода идентифицирующей пользователя информации (магнитных и пластиковых карт, отпечатков пальцев и т. п.);
* устройства для шифрования информации;
* устройства для воспрепятствования несанкционированному включению рабочих станций и серверов (электронные замки и блокираторы).

Примеры вспомогательных аппаратных средств защитыинформации:

* устройства уничтожения информации на магнитных носителях;
* устройства сигнализации о попытках несанкционированных действий пользователей КС и др.

**7. Программные средства защиты информации.**

Под программными средствами защиты информациипонимают специальные программы, включаемые в состав программного обеспечения КС исключительно для выполнения защитных функций. К основным программным средствамзащиты информации относятся:

* программы идентификации и аутентификации пользователей КС;
* программы разграничения доступа пользователей к ресурсам КС;
* программы шифрования информации;
* программы защиты информационных ресурсов (системного и прикладного программного обеспечения, баз данных, компьютерных средств обучения и т. п.) от несанкционированного изменения, использования и копирования.

Примеры вспомогательных программных средствзащиты информации:

* программы уничтожения остаточной информации (в блоках оперативной памяти, временных файлах и т. п.);
* программы аудита (ведения регистрационных журналов) событий, связанных с безопасностью КС, для обеспечения возможности восстановления и доказательства факта происшествия этих событий;
* программы имитации работы с нарушителем (отвлечения его на получение якобы конфиденциальной информации);
* программы тестового контроля защищенности КС и др.

**8. Сервисы безопасности.**

К сервисам безопасностиотносятся: идентификация и аутентификация, управление доступом, протоколирование и аудит, криптография, экранирование.

Под идентификацией,применительно к обеспечению информационной безопасности компьютерной сети, понимают однозначное распознавание уникального имени субъекта компьютерной сети. Идентификация предназначена для того, чтобы пользователь или вычислительный процесс, действующий по команде определенного пользователя, могли идентифицировать себя путем сообщения своего имени.

Аутентификацияозначает подтверждение того, что предъявленное имя соответствует данному субъекту (подтверждение подлинности субъекта). С помощью аутентификации вторая сторона убеждается, что пользователь, пытающийся войти в операционную систему, действительно тот, за кого себя выдает.

Средства управления доступомпозволяют специфицировать и контролировать действия, которые пользователи и вычислительные процессы могут выполнять над информацией и другими компьютерными ресурсами, то есть речь идет о логическом управлении доступом, который реализуется программными средствами.

Логическое управление доступом обеспечивает конфиденциальность и целостность объектов путем запрещения обслуживания неавторизированных пользователей. Контроль прав доступа осуществляется посредством различных компонент программной среды – ядром сетевой операционной системы, дополнительными средствами безопасности, системой управления базами данных, посредническим программным обеспечением.

Протоколированиемназывается процесс сбора и накопления информации о событиях, происходящих в компьютерной сети.

Возможные события принято делить на три группы:

1 внешние события, вызванные действиями других сервисов; 2 внутренние события, вызванные действиями самого сервиса; 3 клиентские события, вызванные действиями пользователей и администраторов.

Аудитомназывается процедура анализа накопленной в результате протоколирования информации. Этот анализ может осуществляться оперативно в реальном времени или периодически.

Экран **–** это средство разграничения доступа клиентов из одного сетевого множества к серверам, принадлежащим другому сетевому множеству. Функция экрана заключается в контроле всех информационных потоков между двумя множествами систем. Примерами экранов являются межсетевые экраны (брандмауэры (firewalls)), устанавливаемые для защиты локальной сети организации, имеющей выход в открытую среду.

Метод криптографии– одно из наиболее мощных средств обеспечения конфиденциальности и контроля целостности информации. Основной элемент криптографии – шифрование (или преобразование данных в нечитабельную форму ключей шифрования расшифровки). В состав криптографической системы входят: один или нескольких алгоритмов шифрования, ключи, используемые этими алгоритмами шифрования, подсистемы управления ключами, незашифрованный и зашифрованный тексты.

Дополнительным методом защиты шифруемых данных и проверки их целостности является цифровая подпись.

**9. Методы резервного копирования базы данных.**

Резервное копирование бд является процессом выгрузки данных из базы данных, протокола транзакций или из файла на устройства резервной копии, которые создаются и поддерживаются системой.

4 метода рез копирования:

1 полное копирование бд

2 дифференциальное рез коп

3 рез коп протокола транзакций

4 рез коп файла или файловой группы

Полное рез коп захватывает то состояние бд, которое она имеет на момент начала копирования. В процессе полного копирования бд система копирует данные, а также схему всех таблиц бд и соответствующие файловые структуры. Если полное копирование бд выполняется динамически, то система бд записывает любые действия, которые имеют место в процессе выполнения рез копирования, поэтому даже все неподтверждённые транзакции в протоколе транзакций будут записаны на устройство рез копии.

Дифференцированное рез коп создаёт копию только частей бд, которые изменялись с момента последнего полного копирования бд(как и в случае полного копирования бд любые действия, имеющие место в процессе дифференцированного копирования, также копируются) преимуществом дифференцированного рез копирования является скорость. Этот тип рез коп минимизирует время, требуемое для копрования, потому что количество копируемых данных значительно меньше, чем в случае полного рез коп.

Рез коп протокола транзакций учитывает только изменения, записанные в протокол. Поэтому такая форма рез коп не основывается на физ частях(страницах) бд, а только на логических операциях, т.е на изменениях, выполненных операторами: insert update delete. Поскольку объём данных мал, этот процесс может быть выполнен значительно быстрее, чем полное и дифференцированное рез коп. 2 осн причины для чего стоит делать коп протокола транзакций: 1 сохранение данных, которые были изменены с момента последнего копирования протокола транзакций или бд на защищённое устройство; 2 это правильное закрытие протокола транзакций перед началом новой порции действий с этим протоколом.

Рез коп файла или файловой группы даёт вам возможность копировать указанные файлы бд вместо копирования всей бд. В этом случае копируются только заданные вами файлы. Отдельные файлы могут быть восстановлены из копии бд, позволяя выполнить восстановление после сбоя, который повлиял лишь на небольшое подмножество файлов бд

**10. Резервное копирование данных с помощью в SQL Server Management Studio.**

Как сделать резервное копирование в SSMS:

1. Открываем SQL Server Management Studio (SSMS) и подключаемся к серверу.
2. В Object Explorer переходим к Databases → выбираем нужную базу данных
3. Кликаем правой кнопкой мыши → Tasks → Back Up…
4. В разделе Backup type выбираем Full.
5. Указываем путь для сохранения .bak файла
6. Нажимаем OK – резервное копирование запустится.

Дифференциальное резервное копирование (Differential Backup):

1. Повторяем действия из полного резервного копирования.
2. В Backup type выбираем Differential.
3. Указываем путь для сохранения .bak файла.
4. Нажимаем OK – копия создана.

Резервное копирование журнала транзакций (Transaction Log Backup):

1. Повторяем действия из полного резервного копирования.
2. В Backup type выбираем Transaction Log.
3. Указываем путь .trn файла.

Нажимаем OK. Если выходит ошибка то пишем код : use название\_базы; go alter database название\_базы set recover full; go

**11. Восстановление данных с помощью в SQL Server Management Studio.**

1 Откройте SSMS и подключитесь к вашему серверу базы данных; 2. Перейдите в «Объекты» → «Базы данных», правой кнопкой мыши щелкните на области с базами данных, и выберите «Восстановить базу данных»; 3 В окне восстановления выберите «Восстановить из устройства», затем укажите путь к первой полной резервной копии, которая была сделана в предыдущем задании;

Восстановление из полной резервной копии (Full Backup)

RESTORE DATABASE имя\_базы

FROM DISK = ‘путь’ – или FROM название резерв устройства

WITH REPLACE, RECOVERY;

(FROM DISK — путь к резервной копии.

WITH REPLACE — перезаписать существующую базу данных (если она уже существует).

WITH RECOVERY — позволяет завершить восстановление базы данных. После этого база готова к использованию.)

Восстановление базы данных из дифференциальной резервной копии (Differential Backup)

1. Восстановите полную копию:

RESTORE DATABASE HR\_DepartmentDB1

FROM DISK = 'D:\Backups\HR\_DepartmentDB1\_Full.bak'

WITH NORECOVERY;

(WITH NORECOVERY — не завершать восстановление базы данных, чтобы можно было применить другие резервные копии (например, дифференциальные).)

1. Восстановите дифференциальный бэкап:

RESTORE DATABASE HR\_DepartmentDB1

FROM DISK = 'D:\Backups\HR\_DepartmentDB1\_Diff.bak'

WITH RECOVERY;

(WITH RECOVERY — завершает процесс восстановления, и база данных готова к использованию.)

Восстановление базы данных из журнала транзакций (Transaction Log Backup)

1. Восстановите полную копию базы данных:

RESTORE DATABASE HR\_DepartmentDB1

FROM DISK = 'D:\Backups\HR\_DepartmentDB1\_Full.bak'

WITH NORECOVERY;

1. Восстановите дифференциальный бэкап, если он имеется:

RESTORE DATABASE HR\_DepartmentDB1

FROM DISK = 'D:\Backups\HR\_DepartmentDB1\_Diff.bak'

WITH NORECOVERY;

1. Восстановите журнал транзакций:

RESTORE LOG HR\_DepartmentDB1

FROM DISK = 'D:\Backups\HR\_DepartmentDB1\_Log.trn'

WITH RECOVERY;

**12. Реализация режима аутентификации в SQL Server Management Studio.**

SQL Server предоставляет два основных режима аутентификации: Windows Authentication и SQL Server Authentication. Настройка и выбор режима аутентификации в SSMS важны для управления доступом и безопасности базы данных.

Windows Authentication

– В этом режиме SQL Server использует учетные данные Windows для аутентификации пользователей.

– Доступ предоставляется только тем пользователям, которые имеют права в Windows.

– Рекомендуется для организаций, использующих Active Directory, так как она упрощает управление безопасностью.

SQL Server Authentication

– В этом режиме аутентификация происходит с использованием логина и пароля, определенных в SQL Server.

– В этом случае учетные записи SQL Server не зависят от учетных записей Windows.

– Этот режим используется, если требуется доступ из разных операционных систем или для серверов, не подключенных к Active Directory.

**13. Понятие имени входа, создание имени входа SQL Server при помощи графического интерфейса и из скрипта T-SQL.**

Имя входа – это субъект безопасности, с помощью которого система безопасности может проверить подлинность лица или сущности. Пользователям требуется имя входа для подключения к SQL Server.

Создание имени входа через графический интерфейс в SQL Server Management Studio (SSMS):

1. Откройте SQL Server Management Studio (SSMS) и подключитесь к серверу.
2. В Object Explorer выберите сервер, к которому вы хотите добавить имя входа.
3. Разверните папку Security.
4. Кликните правой кнопкой мыши на Logins и выберите New Login.
5. В появившемся окне Login - New заполните необходимые поля:

– Login name — введите имя входа (например, sqluser1).

– Если выбрали Windows Authentication, введите имя пользователя Windows (например, Domain\Username).

1. Перейдите на вкладку Server Roles и назначьте роли для этого логина, если нужно (например, sysadmin, dbcreator и т.д.).
2. Перейдите на вкладку User Mapping, чтобы назначить пользователя в конкретных базах данных и предоставить необходимые роли (например, db\_datareader, db\_datawriter).

Создание имени входа с помощью T-SQL скрипта

CREATE LOGIN sqluser1

WITH PASSWORD = 'password123';

-- Создание Windows Login

CREATE LOGIN [Domain\Username]

FROM WINDOWS;

(CREATE LOGIN sqluser1 — создает имя входа с именем sqluser1.

WITH PASSWORD = 'password123' — задает пароль для этого входа.

В примере с Windows Login используется имя Domain\Username для создания входа, который использует учетные данные Windows.)

Пример назначения ролей при создании логина:

CREATE LOGIN sqluser1

WITH PASSWORD = 'password123';

ALTER SERVER ROLE sysadmin ADD MEMBER sqluser1;

(В этом примере для логина sqluser1 сразу добавляется роль sysadmin, что дает ему полный доступ ко всем базам данных и возможность управления сервером.)

**14. Фиксированные серверные роли.**

1. Sysadmin – Полный доступ ко всем объектам сервера и всем базам данных, включая права на выполнение любых операций. Члены этой роли могут выполнять любые действия на сервере.
2. Serveradmin– Разрешения на управление конфигурацией SQL Server и настройками сервера (например, настройка серверных параметров).
3. Setupadmin – Разрешение на установку и настройку серверных объектов, таких как создание и удаление серверных объектов (например, связывание серверов).
4. Processadmin – Разрешение на управление процессами SQL Server, включая остановку и запуск экземпляров SQL Server и их процессов.
5. Dbcreator – Создание, удаление и изменение баз данных. Пользователи этой роли могут выполнять операции, такие как создание баз данных и изменение их структуры.
6. Backupadmin – Разрешение на выполнение операций резервного копирования и восстановления баз данных.
7. Public – Эта роль автоматически назначается всем пользователям. Она предоставляет минимальные права доступа, обычно для чтения метаданных, но не дает прав на выполнение операций.

**15. Пользователи баз данных. Создание пользователя базы данных SQL Server при помощи графического интерфейса и из скрипта T-SQL.**

Пользователи баз данных. Схемы После создания логинов следующая задача - спуститься на уровень базы данных и создать пользователей базы данных. Пользователи баз данных – это специальные объекты, которые создаются на уровне базы данных и используются для предоставления разрешений в базе данных (на таблицы, представления, хранимые процедуры и т.д.).

Логины и пользователи баз данных - это совершенно разные объекты.

Разделение логинов и пользователей баз данных обеспечивает большую гибкость. Например, пользователь, который входит от имени одного и того же логина, сможет работать в разных базах данных от имени разных пользователей.

Создать пользователя базы данных можно:

1 В среде Management Studio, вызвав команду «Создать пользователя…» в контекстном меню подузла «Безопасность | Пользователи» узла конкретной базы данных дерева обозревателя объектов. В открывшемся окне «Пользователь базы данных - Создать» (рисунок 35), необходимо указать два обязательных параметра: имя нового пользователя и выбрать соответствующий ему логин (Windows или SQL Server).

При помощи команды CREATE USER.

Изменение свойств пользователя и его удаление производится из того же контейнера в Management Studio, что и создание пользователя, а также при помощи команд ALTER USER/DROP USER.

**16. Роли базы данных. Встроенные роли базы данных.**

Роли базы данных

Обычно после создания логина и пользователя базы данных следующее, что нужно сделать, - предоставить пользователю разрешения в базе данных. Один из способов сделать это - воспользоваться ролями базы данных.

Роли базы данных - это специальные объекты, которые используются для упрощения предоставления разрешений в базах данных. В отличие от серверных ролей, которые могут быть только встроенными, роли баз данных могут быть как встроенными, так и пользовательскими. Встроенные роли баз данных обладают предопределенным набором разрешений, а пользовательские роли можно использовать для группировки пользователей при предоставлении разрешений.

Обычно пользовательские роли используются только для логинов SQL Server, поскольку для группировки логинов Windows обычно удобнее и проще использовать группы Windows.

Вначале перечислим встроенные роли баз данных:

public - эта специальная роль предназначена для предоставления разрешений сразу всем пользователям базы данных. Специально сделать пользователя членом этой роли или лишить его членства невозможно. Все пользователи базы данных получают права этой роли автоматически;

db\_owner - этой роли автоматически предоставляются полные права на базу данных. Изначально права этой роли предоставляются только специальному пользователю dbo, а через него - логину, который создал эту базу данных;

db\_accessadmin - роль для сотрудника, ответственного за пользователей базы данных. Этот сотрудник получит возможность создавать, изменять и удалять объекты пользователей баз данных, а также создавать схемы. Других прав в базе данных у него нет;

db\_securityadmin- эта роль дополняет роль db\_accessadmin. Сотрудник с правами этой роли получает возможность назначать разрешения на объекты базы данных и изменять членство во встроенных и пользовательских ролях. Прав на создание и изменение объектов пользователей у этой роли нет;

db\_backupoperator - эта роль дает право выполнять резервное копирование базы данных;

db\_ddladmin - эта роль применяется в редких ситуациях, когда пользователю необходимо дать право создавать, изменять и удалять любые объекты в базе данных, не предоставляя прав на информацию, которая содержится в существующих объектах;

db\_datareader и db\_datawriter - эти встроенные роли дают право просматривать и изменять соответственно (в том числе добавлять и удалять) любую информацию в базе данных. Очень часто пользователю необходимо дать права на чтение и запись информации во всех таблицах базы данных, не предоставляя ему лишних административных разрешений (на создание и удаление объектов, изменение прав и т. п.). Самый простой вариант в этой ситуации - воспользоваться этими двумя ролями.

db\_denydatareader и db\_denydatawriter- эти роли противоположны ролям db\_datareader и db\_datawriter. Роль db\_ denydatareader явно запрещает просматривать какие-либо данные, а db\_denydatawriter запрещает внесение изменений. Явный запрет всегда имеет приоритет перед явно предоставленными разрешениями. Обычно эти роли используются в ситуации, когда «разрешаем всем, а потом некоторым запрещаем».

Как уже говорилось ранее, в отличие от серверных ролей, роли баз данных вы можете создавать самостоятельно. Это можно сделать из контекстного меню узла «Безопасность | Роли | Роли базы данных» обозревателя объектов в Management Studio или при помощи команды CREATE ROLE

Работа с разрешениями производится одинаково для всех объектов базы данных:

‒ на вкладке «Разрешения» свойств этого объекта (эта вкладка предусмотрена не для всех объектов, для которых можно предоставить разрешения);

‒ на странице «Защищаемые объекты» окна свойств пользователя или роли;

‒ при помощи команд GRANT (предоставить разрешение), DENY (явно запретить что-то делать) и REVOKE (отменить явно предоставленное разрешение или запрет).

**17. Создание роли базы данных при помощи графического интерфейса и из скрипта T-SQL.**

Создание роли базы данных через графический интерфейс

1. Подключитесь к серверу и выберите нужную базу данных.
2. В Object Explorer разверните папку Databases и выберите базу данных, в которой хотите создать роль.
3. Перейдите в раздел Security → Roles → Database Roles.
4. Кликните правой кнопкой мыши на Database Roles и выберите New Database Role.
5. В появившемся окне введите имя роли в поле Role name.
6. На вкладке Securables можно настроить разрешения для этой роли, добавив объекты, к которым будет предоставлен доступ.
7. На вкладке Members добавьте пользователей, которым будет назначена эта роль.

Создание роли базы данных с помощью скрипта T-SQL:

-- Создание роли базы данных

CREATE ROLE [имя\_роли];

-- Назначение прав роли

GRANT SELECT, INSERT, UPDATE, DELETE ON [таблица] TO [имя\_роли];

-- Добавление пользователей в роль

ALTER ROLE [имя\_роли] ADD MEMBER [имя\_пользователя];

**18. Предоставление прав на объекты в базе данных.**

Работа с разрешениями производится одинаково для всех объектов базы данных:

‒ на вкладке «Разрешения» свойств этого объекта (эта вкладка предусмотрена не для всех объектов, для которых можно предоставить разрешения);

‒ на странице «Защищаемые объекты» окна свойств пользователя или роли;

‒ при помощи команд GRANT (предоставить разрешение), DENY (явно запретить что-то делать) и REVOKE (отменить явно предоставленное разрешение или запрет).

GRANT предоставляет права пользователям, которые могут передавать их другим (если указано WITH GRANT OPTION).

DENY используется для явного отказа в праве, которое не может быть переопределено даже с помощью команды GRANT.

REVOKE удаляет права, но не блокирует повторное предоставление этих прав.

Основные операции предоставления прав

Команда GRANT:

-- Предоставление прав на выборку (SELECT) из таблицы Employees для роли SalesTeam

GRANT SELECT ON dbo.Employees TO SalesTeam;

Команда DENY:

-- Отказ в праве на обновление (UPDATE) данных в таблице Employees для пользователя user2

DENY UPDATE ON dbo.Employees TO user2;

Команда REVOKE:

-- Отмена прав на выборку (SELECT) из таблицы Employees для роли SalesTeam

REVOKE SELECT ON dbo.Employees TO SalesTeam;

Типы прав на объекты базы данных:

1. SELECT — право на выборку данных из таблицы или представления.
2. INSERT — право на добавление новых строк в таблицу.
3. UPDATE — право на изменение существующих данных в таблице.
4. DELETE — право на удаление строк из таблицы.
5. EXECUTE — право на выполнение хранимой процедуры или функции.
6. ALTER — право на изменение структуры объекта базы данных (например, изменение таблицы или представления).
7. REFERENCES — право на создание внешних ключей, ссылающихся на объект.
8. CONTROL — полное управление объектом, включая возможность предоставления прав другим пользователям.

**19. Понятие порта ПК. Основные порты, используемые в компьютерах и их характеристики.**

Порт — это аппаратный интерфейс для подключения внешних устройств к компьютеру. Он служит для обмена данными между компьютером и внешними устройствами, такими как клавиатуры, мыши, принтеры, мониторы, сетевые устройства и другие периферийные устройства. Порты могут быть как физическими (например, разъемы на корпусе), так и виртуальными (например, логические порты для сетевых соединений).

Основные типы портов и их характеристики:

1. Порты ввода/вывода (I/O порты)

– USB (Universal Serial Bus) – Протокол для подключения периферийных устройств. Стандарты: USB 1.1, 2.0, 3.0, 3.1, USB4. Скорость передачи данных: от 12 Мбит/с (USB 1.1) до 40 Гбит/с (USB4). Подключаемые устройства: клавиатуры, мыши, флешки, внешние диски и другие устройства.

– COM (RS-232, последовательный порт)– Используется для подключения старых периферийных устройств (модемы, принтеры). Скорость передачи данных: обычно до 115200 бит/с.

– LPT (параллельный порт)– Применяется для подключения старых принтеров и сканеров. Скорость передачи данных: до 1 Мбит/с.

1. Сетевые порты

– Ethernet (RJ-45) – Используется для проводных соединений с сетью. Стандарты: Fast Ethernet (100 Мбит/с), Gigabit Ethernet (1 Гбит/с), 10 Gigabit Ethernet (10 Гбит/с). Наиболее распространенный порт для подключения к локальной сети (LAN).

– Wi-Fi (беспроводное подключение) – Используется для подключения к сети Wi-Fi. Порты для Wi-Fi обеспечивают подключение через радиочастотные каналы, обычно без физического подключения кабелей.

– Bluetooth (BT) –Используется для беспроводного подключения различных устройств на короткие расстояния. Диапазон скорости передачи данных — до 3 Мбит/с (для Bluetooth 3.0) и до 24 Мбит/с (для Bluetooth 5.0).

1. Аудио и видео порты

– HDMI– Для передачи высококачественного видео и аудио по одному кабелю. Скорость передачи данных: до 48 Гбит/с (для HDMI 2.1). Используется для подключения мониторов, телевизоров, проекторов и других устройств.

– DisplayPort – Протокол для передачи видео и аудио сигналов. Скорость передачи данных: до 32.4 Гбит/с (DisplayPort 2.0). Широко используется для подключения мониторов высокого разрешения.

– 3.5 мм аудио-разъем (mini-jack) –Для подключения наушников, микрофонов, колонок и других аудио устройств. Обычный разъем для аналогового звука.

1. Порты хранения данных

– SATA– Стандарт для подключения жестких дисков и SSD. Скорость передачи данных: до 6 Гбит/с (SATA III).

– eSATA – Внешний интерфейс для подключения устройств хранения данных.

1. Порты для подключения видеокарт и других устройств

– PCI – Стандарт для подключения карт расширения (видеокарт, звуковых карт и других).

**20. Обнаружение открытых на ПК портов утилитой Netstat.**

Netstat (Network Statistics) — это утилита командной строки, которая используется для отображения сетевых соединений, таблиц маршрутизации, статистики интерфейсов, а также открытых портов и сокетов на компьютере. С помощью Netstat можно узнать, какие порты открыты на ПК, а также какие программы или процессы их используют.

Основные функции утилиты Netstat

1. Отображение открытых портов и активных соединений.
2. Информация о протоколах: TCP, UDP, а также их состояние (например, "LISTEN", "ESTABLISHED").
3. Вывод статистики для всех интерфейсов сети, таких как количество принятых и переданных пакетов.
4. Определение процессов, которые используют те или иные порты.

Использование Netstat для обнаружения открытых портов

1. В Windows: нажмите Win + R, введите cmd и нажмите Enter.
2. Основная команда для отображения открытых портов: netstat –an
3. Для более детальной информации об открытых портах с указанием используемых приложений: В Windows можно использовать команду: netstat –ab

Пояснение основных состояний портов:

1. LISTENING — порт открыт, ожидает подключения.
2. ESTABLISHED — установленное активное соединение.
3. CLOSE\_WAIT — соединение закрыто с одной стороны, ожидает завершения передачи данных.
4. TIME\_WAIT — порт завершил соединение, но еще не освободил ресурсы.
5. SYN\_SENT — инициирован запрос на установление соединения.
6. SYN\_RECV — получен запрос на соединение, ожидает подтверждения.

**21 Понятие качества программного продукта (ПП). Критерии качества ПП.**

Понятие качества программного продукта (ПП).

Качество ПП – это совокупность его черт и характеристик, которые влияют на способность ПП удовлетворять заданные потребности пользователя. Это, однако, не означает, что разные ПП должны обладать одним и тем же набором свойств с одинаковыми значениями количественных показателей. Как и в случае технических устройств, показатели качества являются противоречивыми, что означает: улучшение одних показателей качества может быть достигнуто за счет ухудшения других. Качество ПП является удовлетворительным, если количественные показатели свойств гарантируют успешное его использование.

Критерии качества ПП (перечислить и дать характеристику каждого критерия).

Критериями качества ПП являются:

* функциональность;
* надежность;
* легкость применения;
* эффективность;
* сопровождаемость;
* мобильность.

Функциональность – это способность ПП выполнять набор функций, определенных его внешними спецификациями.

Надежность ПП – это способность безотказно выполнять заданные функции при заданных условиях в течение заданного периода времени с высокой степенью вероятности. Таким образом, надежность не означает безошибочности, для надежного ПП важно, чтобы ошибки появлялись при применении ПП достаточно редко и не приводили к катастрофическим последствиям.

Легкость применения – это способность минимизировать затраты пользователя на подготовку и ввод исходных данных и оценку полученных результатов, а также вызывать положительные эмоции пользователя.

Эффективность – это отношение уровня услуг, предоставляемых ПП к объему используемых вычислительных ресурсов. Напомню, что объем используемых вычислительных ресурсов количественно определяется затратами машинного времени и оперативной памяти на выполнение заданных функций.

Сопровождаемость – это такие характеристики ПП, которые позволяют минимизировать усилия по внесению изменений при обнаружении ошибок в ПП и при его модификации. Не последнюю роль в повышении сопровождаемости играют комментарии к тексту программы!

Мобильность – это способность ПП быть перенесенным из одной вычислительной среды (окружения) в другую, в частности, с одной ЭВМ на другую (применяют термин “перенос с одной платформы на другую”.

**22. Понятие сертификации, сертификата соответствия. Основные цели сертификации средств информатизации, информационных технологий и услуг.**

Понятие сертификации, сертификата соответствия.

Сертификация — процедура, выполняемая третьей стороной, независимой от изготовителя (продавца) и потребителя продукции или услуг, по подтверждению соответствия этих продукции или услуг установленным требованиям.

Результатом выполнения процедуры сертификации является так называемый сертификат соответствия.

Сертификат соответствия — документ, выданный по правилам системы сертификации для подтверждения соответствия сертифицированной продукции установленным требованиям.

Основные цели сертификации средств информатизации, информационных технологий и услуг.

Основные цели сертификации средств информатизации, информационных технологий и услуг**:**

1. защита пользователей средств и систем информатизации от приобретения средств и систем, в том числе импортных, которые представляют опасность для жизни, здоровья, имущества, а также для окружающей среды;
2. обеспечение разработчиков систем, а также широкого круга пользователей этих систем достоверной информацией о состоянии отечественного и зарубежного рынков средств информатизации, телекоммуникаций, информационных технологий и услуг;
3. обеспечение информационного обмена между государственными системами информатизации (налоговая служба, правоохранительные органы, службы управления трудом и занятостью, образование, здравоохранение и др.);
4. обеспечение условий для информационного взаимодействия субъектов негосударственной принадлежности с субъектами государственной принадлежности;
5. содействие повышению научно-технического уровня и конкурентоспособности отечественных систем информатизации, информационных технологий и услуг;
6. содействие созданию условий для вхождения России в мировое информационное пространство.

**23. Виды сертификации и их определения.**

Виды сертификации и иx определения.

Добровольная сертификация проводится по инициативе юридических или физических лиц на договорных условиях между заявителем и органом по сертификации в системах добровольной сертификации. Допускается проведение добровольной сертификации в системах обязательной сертификации органами по обязательной сертификации. Нормативный документ, на соответствие которому осуществляются испытания при добровольной сертификации, выбирается, как правило, заявителем. Решение о добровольной сертификации обычно связано с проблемами конкурентоспособности товара, продвижением товаров на рынок (особенно зарубежный); предпочтениями покупателей, все больше ориентирующихся в своем выборе на сертифицированные изделия. Добровольная сертификация не может заменить обязательную сертификацию для товаров и услуг, подлежащих последней.

Обязательная сертификация осуществляется на основании законов и законодательных положений и обеспечивает доказательство соответствия товара (процесса, услуги) требованиям технических регламентов. Для осуществления обязательной сертификации создаются системы обязательной сертификации. Номенклатура объектов обязательной сертификации устанавливается на государственном уровне управления. Для определения обязательности сертификации существует Номенклатура продукции (а так же продукция, имеющая код ТНВЭД), в отношении которой законодательными актами РФ предусмотрена обязательная сертификация. Обязательная сертификация подтверждает только обязательные требования, установленные законом (в частности, продукция и услуги обязаны проходить сертификацию на безопасность). При обязательной сертификации действие сертификата соответствия и знака соответствия распространяется на всей территории РФ.

Декларирование соответствия – это обязательная процедура подтверждения качества продукции. Сам процесс декларирования соответствия в России кардинально не отличается от сертификации, так как декларирование соответствия включает в себя такие же этапы подтверждения качества продукции: проведение лабораторных сертификационных испытаний, оформление протокола испытаний продукции и затем оформляется декларация соответствия. Как показывает практика предприниматели, оформившие декларацию соответствия, дополнительно оформляют и добровольный сертификат на тот же вид продукции. Согласно букве закона, если продукция подлежит декларированию, то сертификат не заменяет наличие декларации. В первую очередь нужно оформить декларацию, а уже потом добровольный сертификат. Перечень продукции подлежащей обязательному декларированию ежегодно дополнятся новыми видами продукции. На данный момент действует Номенклатура продукции, соответствие которой может быть подтверждено декларацией о соответствии.

**24. Понятие сертификата безопасности. Виды сертификатов безопасности.**

Сертификат безопасности — документ, подтверждающий соответствие продукции всем нормам и требованиям безопасности жизнедеятельности, установленным законодательными актами Российской Федерации. Сертификат соответствия также иногда называют сертификатом качества, сертификатом безопасности, таможенным сертификатом и т. д.

Виды сертификатов безопасности.

Выделяют несколько видов сертификатов безопасности:

* промышленный сертификат безопасности (производственной) – разрешительный документ Ростехнадзора, подтверждает, что весь технологический процесс, а также оборудование и различные системы контроля на производстве отвечают всем нормам безопасности. Наличие сертификата дает право на эксплуатацию оборудования и промышленной техники в производственных целях.
* пожарный сертификат безопасности – подтверждает, что сертифицируемая продукция отвечает всем установленным требованиям пожарной безопасности, государственным стандартам, строительным нормам и правилам. С 2009 года под пожарной сертификацией понимается выдача сертификата ГОСТ-Р, устанавливающего требования пожарной безопасности.
* гигиенический сертификат – подтверждает соответствие продукции установленным санитарным правилам и гигиеническим нормам. С 1 июля 2010 года был заменен на регистрационное удостоверение.  Оно выдается на готовые товары, перечень которых утвержден решением комиссии таможенного союза, после проведения испытаний и регистрации в Роспотребнадзоре.

**25. Процесс получения сертификата. Системы сертификации**

**Процесс получения сертификата.**

Процесс получения сертификата включает следующие общие этапы:

1. Формирование пакета документов для подачи заявки. Процесс допускает использование электронных документов, при наличии цифровой подписи с определённой квалификацией.
2. Работа с документами в аккредитованном государством центре сертификации, который имеет разрешение на оказание услуг такого рода и внесён в единый реестр.
3. Подписание соглашения с центром, в котором устанавливаются условия процедуры и оговаривается цена за её проведение.
4. Испытание отобранных образцов продукции, установление соответствия их требованиям стандарта. Итогом проведённых работ является составленный протокол, в котором отражаются все действительно полученные результаты испытаний.
5. Организация и проведение проверки с выездом к заказчику услуг по сертификации для изучения процесса производства, определения соответствия условий производства требованиям стандарта.
6. Принятие окончательного решения об отказе в выдаче или о выдаче сертификата.
7. Оформление и выдача подтверждающего качество документа.

Список необходимых документов может отличаться в зависимости от вида сертификации, поэтому рекомендуется уточнить его у конкретного центра.

**Системы сертификации**

Системы сертификации продукции и товара в России могут осуществляться по одной из утверждённых форм:

* добровольная система сертификации – выполняется по желанию или инициативе продавца или производителя конкретного вида продукции, с целью подтверждения её соответствия разработанным и утверждённым государственным нормам и требованиям. Добровольная сертификация направлена на борьбу за каждого отдельного клиента. Добровольной сертификации подлежит товар или продукция, на которые отсутствуют требования к качеству и безопасности обязательные для выполнения. В свою очередь проведение добровольной сертификации позволяет ограничивать доступ потребителей к некачественной продукции, за счёт определение её качественных характеристик и свойств. Документ, выданный на основании проведённой добровольной сертификации, имеет голубовато-синий цвет и необходим для осуществления мероприятий, связанных с импортом или экспортом различной продукции;
* обязательная система сертификации – распространяется на товары, услуги или продукцию, связанные с обеспечением безопасности здоровья, жизни, имущества и окружающей среды. Главной целью проведения обязательной сертификации является максимальная защита потребителей от возможности приобретения опасных товаров или продукции. Случаи обязательной сертификации оговорены в законодательных нормах и актах РФ. К данным документам относят перечни продукции, относящейся к обязательной сертификации, требования, предъявляемые к декларациям и сертификатам, а также нормы и правила их оформления, получения и выдачи. Документ обязательной сертификации подтверждает соответствие продукции, выдвигаемым к ней требованиям относительности безопасности и качества. Обязательный сертификат имеет светло-жёлтый цвет.

**26. SSL сертификат.**

SSL-сертификат (Secure Sockets Layer) — цифровой сертификат, подтверждающий подлинность сайта. Он даёт возможность установить зашифрованное соединение между сервером и браузером.

Возможности SSL-сертификата.

Возможности SSL-сертификата заключаются в следующем:

* Обеспечение безопасности данных пользователей. SSL-сертификат шифрует передаваемые данные, что не позволяет злоумышленникам считывать или изменять информацию. Это важно, например, при вводе личных данных, таких как номера кредитных карт, или просмотре конфиденциальной информации.
* Подтверждение прав собственности на сайт. SSL-сертификат указывает, кто является владельцем сайта, и не допускает его подделки злоумышленниками.
* Предотвращение создания поддельной версии сайта.
* Обеспечение доверия со стороны пользователей. Если пользователи знают, что их информация защищена, то с большей вероятностью захотят иметь дело с сайтом.
* Повышение позиций в результатах выдачи поисковых систем. Поисковые системы учитывают использование SSL-сертификата при ранжировании сайтов.

Как работают SSL-сертификаты.

Использование SSL гарантирует, что данные, передаваемые между пользователями и веб-сайтами или между двумя системами, невозможно прочитать сторонним лицам или системам. SSL использует алгоритмы для шифрования передаваемых данных, что не позволяет злоумышленникам считать их при передаче через зашифрованное соединение. Эти данные включают потенциально конфиденциальную информацию, такую как имена, адреса, номера кредитных карт и другие финансовые данные.

Процесс работает следующим образом:

1. Браузер или сервер пытается подключиться к веб-сайту (веб-серверу), защищенному с помощью SSL.
2. Браузер или сервер запрашивает идентификацию у веб-сервера.
3. В ответ веб-сервер отправляет браузеру или серверу копию своего SSL-сертификата.
4. Браузер или сервер проверяет, является ли этот SSL-сертификат доверенным. Если это так, он сообщает об этом веб-серверу.
5. Затем веб-сервер возвращает подтверждение с цифровой подписью и начинает сеанс, зашифрованный с использованием SSL.
6. Зашифрованные данные используются совместно браузером или сервером и веб-сервером.

Данные, входящие в SSL-сертификат, обычно включают:

* Доменное имя, для которого выпущен сертификат.
* Лицо, организация или устройство, для которого выпущен сертификат.
* Центр сертификации, выдавший сертификат.
* Цифровая подпись центра сертификации.
* Связанные поддомены.
* Дата выдачи сертификата.
* Срок действия сертификата.
* Открытый ключ (закрытый ключ не раскрывается).

Типы SSL-сертификатов.

Типы SSL-сертификатов и их уровни проверки:

* EV SSL — с расширенной проверкой;
* OV SSL — подтверждают организацию;
* DV SSL — подтверждают домен;
* Wildcard — с подстановочными символами;
* UCC — с унифицированными коммуникациями;
* MDC — мультидоменный.

Сертификаты с расширенной проверкой (EV SSL)

* Самый высокорейтинговый и дорогой тип SSL-сертификатов. Его получают популярные веб-сайты, которые собирают данные и используют онлайн-платежи. Подходящее решение для интернет-магазинов и сайтов микрофинансовых организаций.
* После установки EV SSL-сертификата в адресной строке браузера отображаются замок, HTTPS, название и страна компании. Данные о владельце веб-сайта в адресной строке помогают отличить сайт от вредоносных. Чтобы настроить сертификат, владелец веб-сайта должен пройти стандартную проверку. Она заключается в подтверждении, что владелец на законных основаниях имеет исключительные права на домен.

Сертификаты, подтверждающие организацию (OV SSL)

* Максимальная защита и доверие: чтобы создать такой сертификат, владелец веб-сайта должен пройти основательную проверку. При использовании сертификата данные о владельце веб-сайта отображаются в адресной строке — так отличить сайт от вредоносного в разы легче.
* OV SSL-сертификаты для сайтов находятся на втором месте по стоимости (после EV). Их главная функция — шифровать конфиденциальные данные пользователей при транзакциях. Такие сертификаты принято выпускать для коммерческих и общедоступных сайтов, чтобы защищать клиентские данные.

Сертификаты, подтверждающие домен (DV SSL)

* Процесс проверки — простой, быстрый и дешёвый. Поэтому DV SSL-сертификаты — это минимальная защита и уровень шифрования. Именно здесь можно найти версии free.
* DV SSL-сертификаты используют, чтобы создавать блоги, а также для информационных веб-сайтов. То есть для страниц, которые не связаны с онлайн-платежами или сбором данных.
* Чтобы пройти проверку, владельцу веб-сайта нужно указать права собственности на домен в электронном письме или телефонном разговоре. В адресной строке браузера отображается только HTTPS и замок (без слов, то есть без обозначения названия компании).

Сертификаты с подстановочными символами (Wildcard)

* Преимущество Wildcard заключается в том, что они позволяют защитить базовый домен и неограниченное количество поддоменов с помощью одного сертификата. Если поддоменов несколько, то выйдет намного дешевле, чем покупать сертификат отдельно для каждого поддомена.
* Wildcard-сертификаты содержат звездочку (\*) — это часть общего имени. Звездочка указывается вместо любого допустимого в составе одного базового домена.

Мультидоменные сертификаты (MDC)

* Используют для защиты нескольких доменных и поддоменных имён, включая сочетания уникальных доменов и поддоменов с разными доменами верхнего уровня (TLD). Исключения — локальные (внутренние) домены.
* По умолчанию мультидоменные сертификаты не поддерживают поддомены. Если нужно защитить сайты www.example.com и example.com с помощью одного мультидоменного сертификата, при его получении важно указать оба имени хоста.

Сертификаты унифицированных коммуникаций (UCC)

* Функция таких сертификатов — защита серверов Microsoft Exchange и Live Communications. Любой владелец веб-сайта может использовать эти сертификаты, чтобы обеспечить защиту нескольких доменных имён с помощью одного сертификата.
* UCC-сертификаты проверяются на уровне организации. Для них в браузере отображается значок замка. Сертификаты унифицированных коммуникаций могут заменить сертификаты с расширенной проверкой, а значит, обеспечить максимум безопасности посетителям веб-сайта.

Этапы получения сертификата

1.Подготовка. Настройте сервер и убедитесь, что ваша запись WHOIS обновлена и соответствует данным, отправляемым в центр сертификации. WHOIS — это сетевой протокол, необходимый для получения в текстовом виде регистрационных данных владельцев IP-адресов и доменных имен. Запись должна правильно отображать название, адрес компании и другие сведения.

2. Создание запроса на сервере на подпись SSL-сертификата (CSR). Запрос заключается в текстовом файле, в котором в зашифрованном виде содержится информация об администраторе домена. Вместе с CSR формируется приватный ключ. За помощью в создании запроса онлайн можно обратиться к вашей хостинговой компании.

3. Отправка запросав центр сертификации для проверки данных вашего домена и организации. У удостоверяющего центра могут возникнуть вопросы — тогда он запросит дополнительные документы.

4. Установка сертификата. После получения файлов на почту SSL-сертификат необходимо настроить на вашем веб-хосте или серверах (если вы обеспечиваете хостинг веб-сайта самостоятельно). Скачайте файлы и проведите установку.