Федеральное государственное образовательное бюджетное
учреждение высшего образования
«Финансовый университет при Правительстве Российской Федерации»
(Финуниверситет)

Самарский финансово-экономический колледж
(Самарский филиал Финуниверситета)

УТВЕРЖДАЮ
Заместитель директора по учебно-методической работе
_____ Л.А Косенкова
«21» февраля 20 22 г.

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ПЛАНИРОВАНИЮ И ОРГАНИЗАЦИИ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ ПО ПРОФЕССИОНАЛЬНОМУ МОДУЛЮ «ПМ.07 СОАДМИНИСТРИРОВАНИЕ БАЗ ДАННЫХ И СЕРВЕРОВ»

СПЕЦИАЛЬНОСТЬ: 09.02.07 ИНФОРМАЦИОННЫЕ СИСТЕМЫ И ПРОГРАММИРОВАНИЕ

Самара – 2022

Методические указания по планированию и организации самостоятельной работы студентов разработаны на основе рабочей программы по профессиональному модулю «Соадминистрирование баз данных и серверов», с учетом требований федерального государственного образовательного стандарта среднего профессионального образования по специальности 09.02.07 Информационные системы и программирование, утвержденного приказом Министерства образования науки Российской Федерации от 09.12.2016 года № 1547, с учетом Профессионального стандарта, утвержденного приказом Министерства труда и социальной защиты Российской Федерации от 11 февраля 2014 г. № 647н «Об утверждении профессионального стандарта 06.011 Администратор баз данных» (зарегистрирован Министерством юстиции Российской Федерации 24 ноября 2014 г., регистрационный № 34846)
Присваиваемая квалификация: администратор баз данных

Разработчики:

Платковская Е.А. _____ Преподаватель Самарского филиала Финуниверситета

Методические указания по планированию и организации самостоятельной работы студентов рассмотрены и рекомендованы к утверждению на заседании предметной (цикловой) комиссии естественно-математических дисциплин

Протокол от «24» сентября 20 22 г. № 5

Председатель ПЦК _____ М.В. Писцова

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Данные методические указания составлены для самостоятельного изучения дисциплины по профессиональному модулю ПМ.07 Соадминистрирование баз данных и серверов в соответствии с требованиями ФГОС и предназначены для реализации государственных требований к минимуму содержания и уровню подготовки выпускников по специальности 09.02.07 Информационные системы и программирование (квалификация «администратор баз данных»).

В результате изучения профессионального модуля студент должен освоить основной вид деятельности Осуществление интеграции программных модулей и соответствующие ему общие компетенции и профессиональные компетенции

Перечень общих компетенций:

Код	Наименование общих компетенций
ОК 1.	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам
ОК 2.	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.
ОК 3	Планировать и реализовывать собственное профессиональное и личностное развитие.
ОК 4	Планировать и реализовывать собственное профессиональное и личностное развитие.
ОК 5	Планировать и реализовывать собственное профессиональное и личностное развитие.
ОК 6	Проявлять гражданскопатриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей
ОК 7	Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.
ОК 8	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности
ОК 9	Использовать информационные технологии в профессиональной деятельности.
ОК 10	Пользоваться профессиональной документацией на государственном и иностранном языке
ОК 11	Планировать предпринимательскую деятельность в профессиональной сфере

Перечень профессиональных компетенций

Код	Наименование видов деятельности и профессиональных компетенций
ВД 7	***Соадминистрирование баз данных и серверов***
ПК 7.1	Выявлять технические проблемы, возникающие в процессе эксплуатации баз данных и серверов
ПК 7.2	Осуществлять администрирование отдельных компонент серверов
ПК 7.3	Формировать требования к конфигурации локальных компьютерных сетей и серверного оборудования, необходимые для работы баз данных и серверов
ПК 7.4	Осуществлять администрирование баз данных в рамках своей компетенции
ПК 7.5	Проводить аудит систем безопасности баз данных и серверов, с использованием регламентов по защите информации.

В результате освоения профессионального модуля студент должен:

Иметь практический опыт	В участии в соадминистрировании серверов; разработке политики безопасности SQL сервера, базы данных и отдельных объектов базы данных; применении законодательства Российской Федерации в области сертификации программных средств информационных технологий
уметь	проектировать и создавать базы данных; выполнять запросы по обработке данных на языке SQL; осуществлять основные функции по администрированию баз данных; разрабатывать политику безопасности SQL сервера, базы данных и отдельных объектов базы данных; владеть технологиями проведения сертификации программного средства
знать	модели данных, основные операции и ограничения; технологию установки и настройки сервера баз данных; требования к безопасности сервера базы данных; государственные стандарты и требования к обслуживанию баз данных

Объем дисциплины и виды учебной работы

Вид учебной работы	**Объем часов**
Всего часов	**618**
- на освоение МДК	428
на практики:	
- учебную	36
- производственную	144
Самостоятельная работа	70
Промежуточная аттестация и экзамен по модулю	10
Консультация	2

ВНЕАУДИТОРНАЯ САМОСТОЯТЕЛЬНАЯ РАБОТА СТУДЕНТОВ

№ п/п	Содержание внеаудиторной самостоятельной работы	Кол-во часов	Календарные сроки исполнения	Формы контроля
МДК. 07.01 Управление и автоматизация баз данных				
1.	Работа с конспектами лекций, учебной и специальной литературой.	10	7 семестр	Проведение опросов по темам.
2.	Подготовка к практическим занятиям, оформление результатов практических занятий, отчётов и подготовка к их защите.	28	7 семестр	Проверка преподавателем выполненных заданий
3	Составление таблицы «Характеристики серверов баз данных», изучение теоретического материала и подготовка к контрольной работе.	4	7 семестр	Проверка преподавателем выполненных заданий
МДК.07.02 Сертификация информационных систем				
5	Выполнение индивидуальных заданий по теме «Защита и сохранность информации баз данных»	6	7 семестр	Проверка преподавателем выполненных заданий
6	Выполнение реферата, презентации, доклада по темам: Уровни качества программной продукции. Требования к конфигурации серверного оборудования и локальных сетей. Оформление требований. Техническое задание. Системы сертификации. Процедура сертификации. Сертификаты безопасности: виды, функции, срок действия. Проверка наличия сертификата безопасности. Платформы и центры сертификации. Сертификат разработчика.	20	7 семестр	Выступление с подготовленной презентацией, докладом, рефератом
7	Процесс подписи и проверки кода. SSL сертификат: содержание, формирование запроса, проверка данных с помощью сервисов.	2	7 семестр	Проверка преподавателем выполненных заданий
	Итого	**70**		

Методические указания

Вопросы для подготовки к опросу по теме Модели и типы данных.

1. Что такое база данных?
2. Базовые свойства реляционных отношений.
3. Что такое ключ реляционного отношения?
4. Как задаются связи между реляционными отношениями?

Вопросы для подготовки к опросу по теме Режимы запуска и остановка базы данных.

1. Что такое статические и динамические библиотеки?
2. В чем заключается модульный принцип программирования?
3. Что относится к программным модулям?
4. Как осуществляется открытие групповой политики?
5. Как создают объекты групповой политики?

Вопросы для подготовки к опросу по теме Технология установки и настройка сервера MySQL в операционных системах.

6. Каково назначение средств диагностики оборудования?
7. Как осуществляется установка и эксплуатация сервера?
8. В чем состоит назначение серверного ПО?
9. Что включает в себя клиентское ПО?

Практические задания МДК. 07.01 Управление и автоматизация баз данных

Задание 1: Разработать БД, отображающую музыкальные произведения, их исполнителей, авторов и музыкальные стили

Объекты:

1. Произведение – play; соответствует музыкальному произве- дению как таковому, может не исполненному никем.
2. Person – содержит данные об авторах, исполнителях, вооб- ще всех персонах, как то связанных с музыкальными произведе- ниями.
3. Стиль – style – содержит данные об музыкальных стилях.
4. Ispoolnenie – содержит данные об исполнении музыкального произведения каким либо исполнителем.

Атрибуты:

- Произведения (proizv):

1. id_play – числовой тип integer; код про изведения искусст-венный атрибут, введен для идентификации произведения.
2. Название (play) – текстовый тип varchar(50).
3. id_avts – числовой тип integer; код автора слов используется для указания на автора, сочинившего слова.
4. id_avtm – числовой тип integer; код автора музыки исполь- зуется для указания на автора, сочинившего музыку.

- Стиль (style):

1. id_style – искусственный атрибут, используется для обозна- чения стиля числовой тип integer.

2. Название (style) – текстовый тип varchar(50).

- ispolnenie:

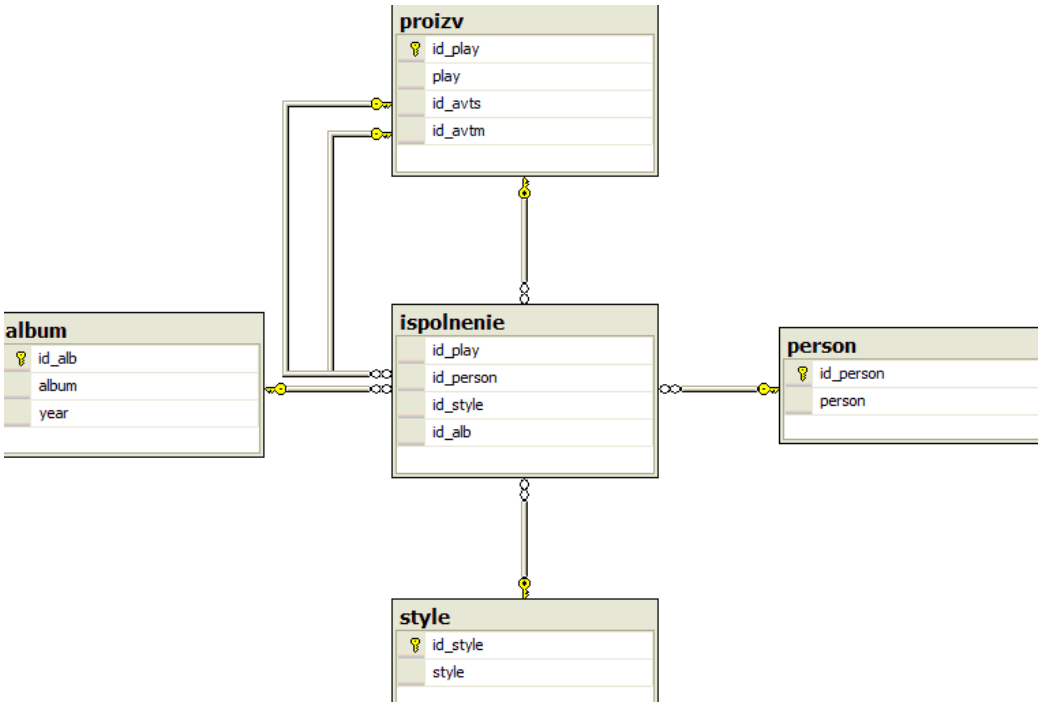
1. id_play – код исполнения – искусственный атрибут, введендля обознаяения произведения.
2. id_avt – код исполнителя, ссылка на таблицу person– число-вой тип integer.
3. id_style – числовой тип integer ссылка на значение кодов персон в табл person.

Связи:

1. Произведение связано с ispolnenie связью один к многим, так как одно произведение может иметь много вариантов исполне- ний.

2. Группа связана с ispolnenie связью один к многим, так как одна группа может записать много исполнений произведений.
3. Стиль связан с ispolnenie связью один к многим, так как в одном стиле может быть сделано много исполнений.
4. Альбом связан с ispolnenie связью один к многим, так как один альбом может содержать много исполнений.

Диаграмма связей в БД



Таблицы, соответствующие выделенным отношениям

Таблица album

Table - dbo.proizv | Table - dbo.ispolnenie | Table - dbo.person | Table - dbo.style | **Table - dbo.album**

id_alb	album	year
1	Стихия огня	2006
2	Смутное время	1997
3	Неформат	2000
4	See You The Other Side	1996
5	Aska	2005
6	Крылья	2005
NULL	NULL	NULL

Таблица person

Table - dbo.proizv | Table - dbo.ispolnenie | **Table - dbo.person** | Table - dbo.style | Table - d

id_person	person
1	Aska
2	Catharsis
3	Легион
4	Ария
5	Korn
6	Маврин
NULL	NULL

Таблица proizv

Table - dbo.proizv | Table - dbo.ispolnenie | Table - dbo.person | Table - dbo.style | Table - dbo.

id_play	play	id_avts	id_avtm
1	Вольная птица	3	3
2	Я свободен	4	6
3	Стая	6	6
4	Twisted Transistor	5	5
5	Angels of war	1	1
6	Крылья	2	2
NULL	NULL	NULL	NULL

Таблица style

Table - dbo.proizv | Table - dbo.ispolnenie | Table - dbo.person | **Table - dbo.style** | Table - dbo.album

id_style	style
1	Heave metall
2	Classik rock
3	Melodik metall
4	NU metall
NULL	NULL

Таблица ispolnenie

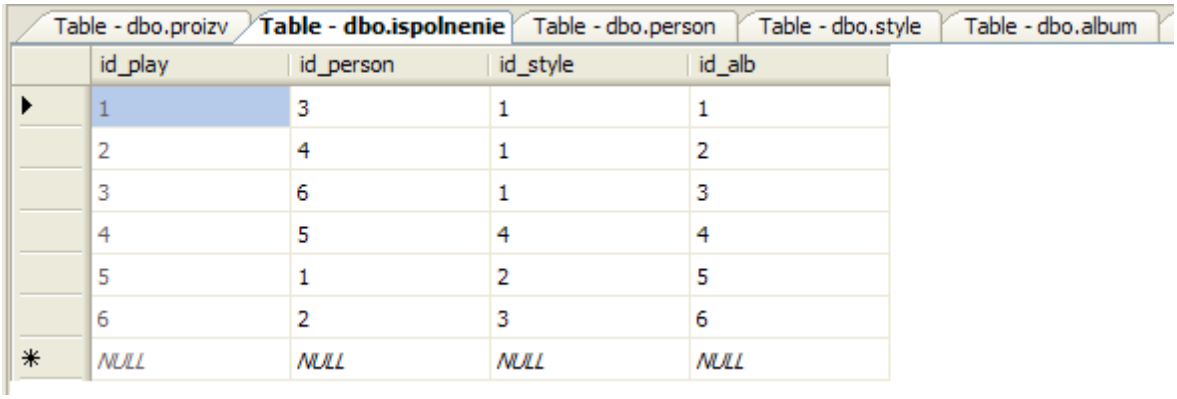


Table - dbo.proizv | **Table - dbo.ispolnenie** | Table - dbo.person | Table - dbo.style | Table - dbo.album

	id_play	id_person	id_style	id_alb
▶	1	3	1	1
	2	4	1	2
	3	6	1	3
	4	5	4	4
	5	1	2	5
	6	2	3	6
*	NULL	NULL	NULL	NULL

Задание 2.

Дана информация об установленном оборудовании.

Отдел	НачОтдела	ЦехИнвНомер	Модель	Стоимость	СрокСлужбы
Цех1	Сидоров	2	1К62	160000	4.5
Цех1	Сидоров	3	1Т62	160000	2
Цех2	Петров	2	2Ф14	260000	5

1. Строим диаграмму зависимостей

А) В качестве потенциального ключа приняты атрибуты (От- дел, ЦехИнвНомер. По значению данных атрибутов можно оп- ределить любой кортеж (строку, запись).

В) Частичные зависимости:

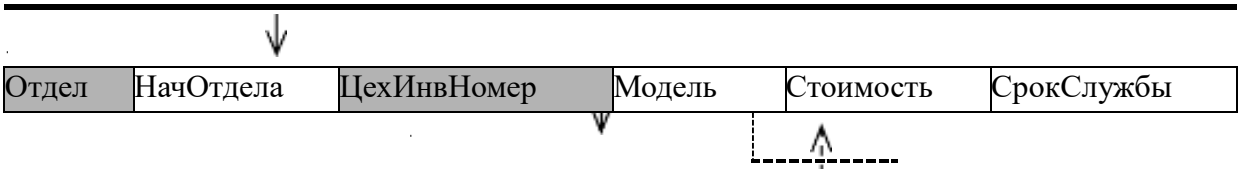
Отдел → НачОтдела, ЦехИнвНомер→ Модель

Данная зависимость Отдел → НачОтдела показывает, что по номеру отдела можно определить его начальника. Зависимость ЦехИнвНомер→ Модель показывает, что по цеховому номеру станка можно определить его модель, то есть цеховой номер станка подразумевает некоторый конкретный станок, который имеет неко- торую модель.

С) Транзитивная зависимость:

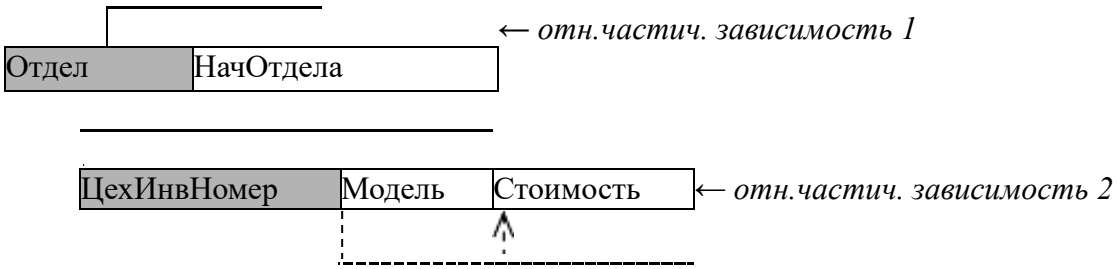
Модель → Стоимость.

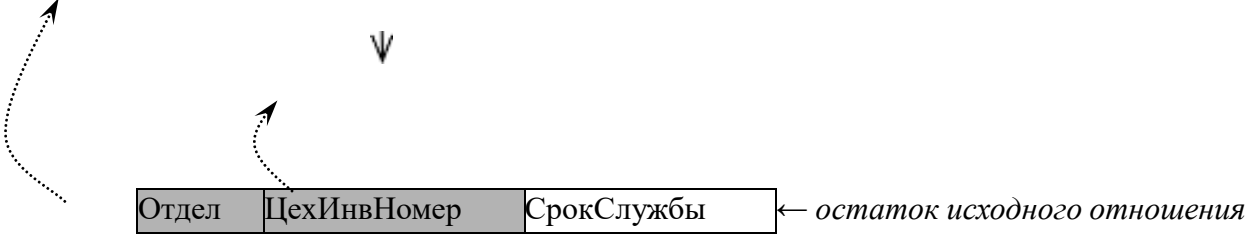
Данная зависимость подразумевает то, что стоимость станка определяется его моделью, что соответствует условиям предметной области.



Задание 3. Приведение ко 2 нормальной форме

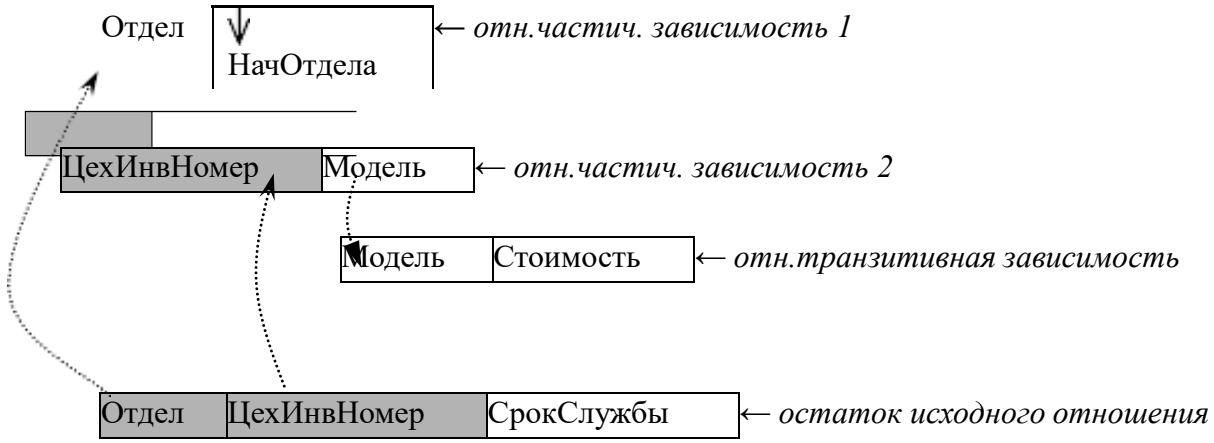
Для приведения ко 2 ф.н. выделяем объекты «Отдел» и «Мо-дель» в отдельные отношения.



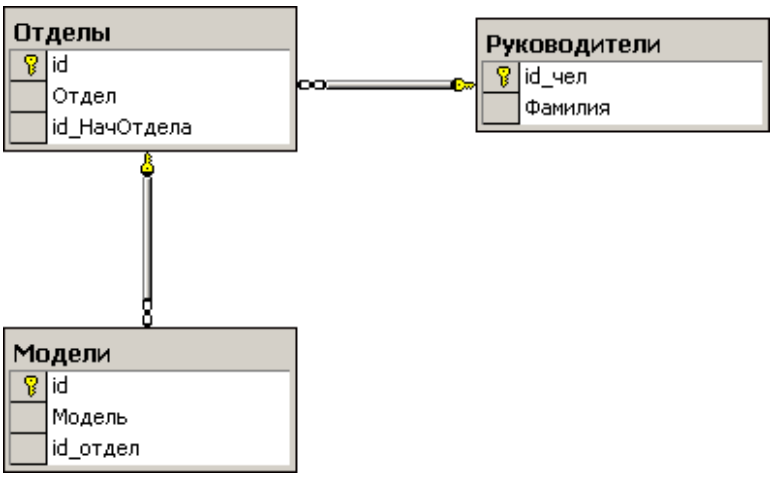


Задание 4. Приведение к 3 нормальной форме

Для приведения к 3NF выделяем транзитивную зависимость «Модель-Стоимость» в отдельное отношения.



Задание 5. Строим связь отношений в Enterprise Manager



Задание 6. Формируем запрос, позволяющий получать требуемуюинформацию

SELECT M.Модель, O.Отдел, R.Фамилия FROM dbo.Модели M INNER **JOIN** Отделы O

ON M.id_отдел = O.id

INNER **JOIN** Руководители R

ON O.id_НачОтдела = R.id_челРезультат:

1К62	Цех1	Иванов
1Т65	Цех2	Петров
С1Е12	Цех2	Петров

Задание: Изучить теоретический материал и заполнить таблицу «Характеристики серверов баз данных».

Сервера баз данных	**Oracle 9 (Oracle)**	**MS SQL Server 2000 (MS)**	**Informix (Informix)**	**Sybase (Sybase)**	**Db2 (IBM)**
Основные характеристики					
Функциональные возможности					
Масштабируемость					

Выполнение индивидуальных заданий по теме «Защита и сохранность информации баз данных»

1. Используя указанную преподавателем доменную или локальную учетную запись Windows, с помощью SQL Server Management Studio подключитесь к используемому экземпляру SQL Server. Проверьте установленный на сервере режим аутентификации.

2. В окне Object Explorer (по умолчанию — левая часть окна Management Studio) откройте список учетных записей (logins). На выполнение каких серверных ролей авторизована используемая вами учетная запись?

3. В каких базах данных сервера вашей учетной записи сопоставлены пользователи? На выполнение каких ролей они авторизованы?

4. В среде Management Studio создайте новую базу данных. Откройте список пользователей и ролей. Убедитесь, что учетная запись, под которой вы работаете, сопоставлена пользователю dbo, авторизованному на роль db owner.

5. Используя приведенный ниже скрипт, создайте в базе данных таблицы. Перед тем как запустить скрипт, уберите символы комментария («--») из первой строки и после ключевого слова use укажите имя вашей базы данных.

```
use MyTestl GO
CREATE TABLE dbo.Book (
book_id int IDENTITY (1, 1) primary key,
Title varchar(50) NOT NULL, —название книги Author varchar(50), — автор Publisher var-
char(50), — издательство [Year] smallint) — год издания GO
CREATE TABLE dbo.Status (
Status_id int IDENTITY (1, 1) primary key, Status_name varchar(50) NOT NULL ) — статус:
выдана, в библиотеке и т.д.
GO
CREATE SCHEMA libr GO
CREATE TABLE libr.Book_in_lib (
lib_id int primary key , —номер экземпляра book_id int references dbo.Book , status_id int
references dbo.[Status])
```

Обратите внимание, что приведенный скрипт создает не только три таблицы, но и схему libr. В SQL Server схема является контейнером логического уровня, к которому относятся объекты базы данных. Во вновь созданной БД уже будет несколько схем: dbo, sys, information_schema и т. д. Схема dbo — это схема по умолчанию для новых пользовательских объектов, sys и infor- mation schema используются системными объектами. Оператором CREATE SCHEMA в БД можно создавать новые схемы.

Защищаемым объектом, на действия с которым пользователю предоставляются разрешения, может быть база данных, схема или объект базы данных. Определенное для схемы разрешение неявным образом распространяется на все объекты схемы, разрешение для базы данных — на все схемы и объекты этих схем.

6. Для указанной преподавателем учетной записи SQL Server (при самостоятельном выполнении работы создайте учётную запись Windows и учётную запись SQL Server для нее) создайте пользователя в вашей базе данных, в качестве схемы по умолчанию выберите dbo. В Management Studio это можно сделать из графического интерфейса (контекстное меню узла Security для выбранной БД, там New...-> User) или выполнив оператор CREATE USER. Например (если схема не указана, подразумевается dbo):

USE MyTestl до

CREATE USER ns FOR LOGIN [HOME s]

Добавьте этого пользователя в роль db_datareader. Это можно сделать или через графический интерфейс или с помощью системной хранимой процедуры sp_addrolemember, первым параметром которой будет имя роли, а вторым — имя пользователя.

EXEC sp_addrolemember 'db_datareader', 'ns 1 Введите в таблицы тестовый набор данных. Подключитесь к серверу с учетной записью другого пользователя. Убедитесь, что можно получить доступ к базе данных и читать записи из всех таблиц, а добавлять или изменять данные нельзя.

7. Создадим новую роль уровня базы данных и добавим ей разрешение на удаление (DELETE), изменение (UPDATE) и добавление данных (INSERT) в объектах схемы libr. Добавим нашего пользователя к этой роли. Указанные действия надо выполнять с правами администратора или владельца базы данных. Как и в предыдущем случае, все это можно сделать в графическом интерфейсе или запуском скрипта.

CREATE ROLE libr_writer GO

GRANT INSERT, UPDATE, DELETE ON SCHEMA :: libr TO

libr_writer

Go

EXEC sp_addrolemember 'libr_writer', 'ns'

Используемый в приведенном скрипте оператор GRANT позволяет предоставить разрешения. Оператор DENY позволяет запретить выполнение каких-то действий, а оператор REVOKE отменяет установленные оператором GRANT или DENY настройки разрешений. Таким образом, у разрешения может быть три состояния: «разрешено», «запрещено», «не задано».

Действие можно выполнить, только если оно разрешено непосредственно пользователю или одной из ролей, на которые он авторизован. Запрещение более приоритетно, чем разрешение: если пользователь авторизован на выполнение двух ролей, одной из них действие разрешено, а другой — запрещено, то пользователь это действие

выполнить нс сможет. В SQL Server Management Studio можно просмотреть эффективные разрешения для пользователя (рис. 5.5).

Конкретный набор возможных разрешений зависит от типа объекта.

Выполните описанные действия. Убедитесь, что пользователь с ограниченными правами может изменять данные в таблице Book_in_lib, относящейся к схеме libr.

8. Иногда нужно предоставить пользователю права на изменение отдельных столбцов. Как отмечается в документации SQL Server, на столбец могут быть предоставлены только разрешения SELECT, REFERENCES и UPDATE.

Например:

GRANT UPDATE ON dbo.Book(Title) TO libr_writer

Выполните аналогичные действия в своей базе данных, проверьте, что пользователь получил указанные разрешения.

9. Самостоятельно по справке ознакомьтесь с форматом оператора CREATE VIEW, особое внимание обратите на задаваемые дополнительные параметры. Создайте представление, выбирающее из таблицы Book книги, изданные не ранее 2000 года. Предоставьте пользователю с ограниченными правами возможность изменять и добавлять подобные книги. Возможности изменять прочие записи таблицы и добавлять книги, изданные до 2000 года, он иметь не должен.

Выполнение реферата, презентации, доклада по темам:
Уровни качества программной продукции.
Требования к конфигурации серверного оборудования и локальных сетей.
Оформление требований.
Техническое задание.
Системы сертификации.
Процедура сертификации.
Сертификаты безопасности: виды, функции, срок действия.
Проверка наличия сертификата безопасности.
Платформы и центры сертификации.
Сертификат разработчика.

Правила оформления реферата

Реферат должен содержать следующие составляющие:
- тему работы;
- содержание;
- текст работы;
- выводы;
- список литературы.

Студент должен предоставить реферат в печатном виде в папке скоросшивателе.

Процесс подписи и проверки кода.
SSL сертификат: содержание, формирование запроса, проверка данных с помощью сервисов.

Сертификаты разработчика (Code Signing сертификаты) — это сертификат, которым подписывается программное обеспечение или скрипты, который подтверждает автора программы и гарантирует, что код не был изменен, после того, как была наложена цифровая подпись.

Сертификат разработчика Code Signing гарантирует:

- **подлинность источника**, подтверждая посредством цифровой подписи, что ПО на самом деле выпущено указанной в сертификате компанией или физическим лицом;
- **целостность кода**, подтверждая, что с момента подписания код программы не был изменен, поврежден или дополнен.

Во всех современных версиях Windows, начиная с Windows XP SP2, при установке программного обеспечения без такой цифровой подписи вы получите предупреждение. То же самое кстати касается и установки драйверов, которые не имеют соответствующей цифровой подписи.

В случае, если цифровая подпись не найдена, Windows выдаст предупреждение, что у этой программы «Неизвестный издатель» и запускать её не рекомендуется.

В случае, если программа имеет цифровую подпись, то окошко будет выглядеть иначе, и вы также сможете посмотреть информацию о сертификате.

Виды сертификатов разработчика

Сертификаты, по центрам сертификации, которые их выпускают представлены в таблице. В колонках указаны названия центров сертификации, а в строках тип сертификата или технология/платформа для которой он используется.

Платформа \ Центр сертификации	**Syman-tec**	**Thawte**	**Comodo**	**Digicert**	**Globalsign**	**Trustwave**	**Startc**
Microsoft Authenticode Signing	+	+	+	+	+	+	+
Code Signing for Apple	+	+		+	+	+	+
Microsoft Vba Signing	+	+	+	+	+	+	+

Java Code Signing	+	+	+	+	+	+	+
Adobe Air Signing	+	+	+	+	+	+	+
Kernel Mode Signing	+			+	+		+
Android	+						
Windows Phone	+						
Qualcomm BREW	+						
Стоимость, от	500$	250$	90$	220$	220$	330$	200$

Не все центры сертификации дают полную информацию о платформах, на которых работают их сертификаты, поэтому плюсом отмечены только те платформы, поддержка которых в явном виде заявлена центром сертификации.

Microsoft Authenticode. Для подписи 32 и 64 битных файлов (.exe, .cab, .dll, .ocx, .msi, .xpi и .xap файлы). Также позволяет подписывать код для Microsoft® Office, Microsoft VBA, Netscape Object Signing и Marimba Channel Signing. Поддерживает приложения на Silverlight 4

Code Signing for Apple. Позволяет разработчикам подписывать программы для Mac OS, а также обновления для программного обеспечения

Microsoft Office Vba Signing. Подписывает VBA объекты, скрипты и макросы для файлов Microsoft Office .doc, .xls, и.ppt Для Microsoft Office и дополнений, которые используют VBA

Java Code Signing. Для подписи Java апплетов. Позволяет подписывать .jar файлы и Java приложения для настольных и мобильных устройств. Распознается Java Runtime Environment (JRE)

Adobe Air Signing. Для подписи файлов.air Требуется для всех приложений, основанных на AIR

Kernel Mode Signing. Сертификаты разработчика Kernel-Mode позволяют подписывать, так называемые kernel-mode приложения и драйвера устройств. 64 битная версия Windows Vista и Windows 7 требуют, чтобы все kernel-mode приложения были подписаны сертификатом и доверенного центра сертификации.

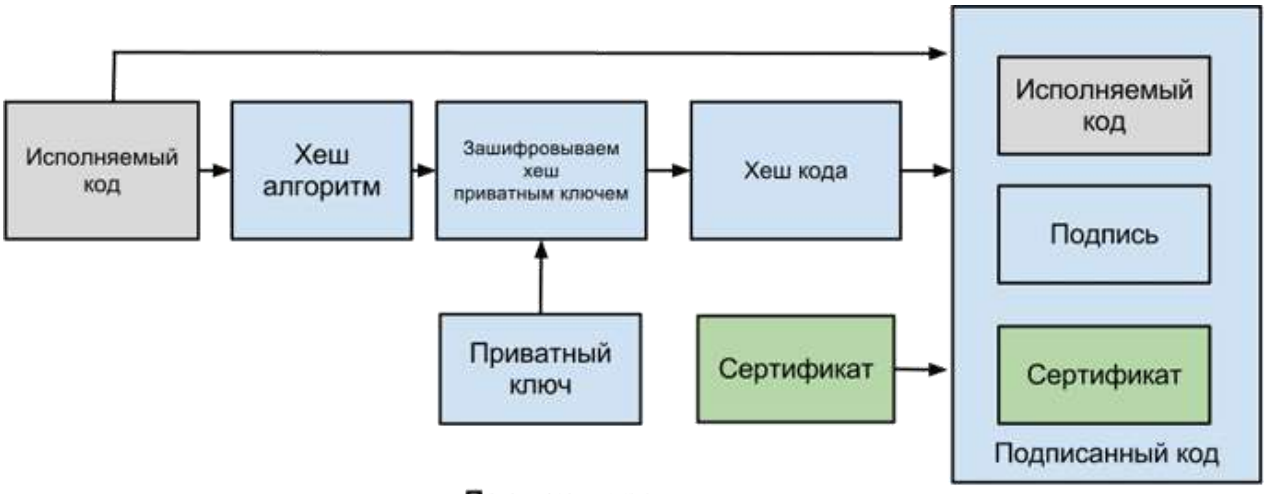
Android. Для подписи и оптимизации .apk файлов для платформы Android

Microsoft Windows Phone. Для цифровой подписи приложений для Windows Phone и Xbox 360. Требуется для сервиса Microsoft App Hub

Qualcomm BREW. Для тех, кто разрабатывает приложения под платформу BREW (Binary Runtime Environment for Wireless)

Принцип работы сертификата разработчика (Code Signing)

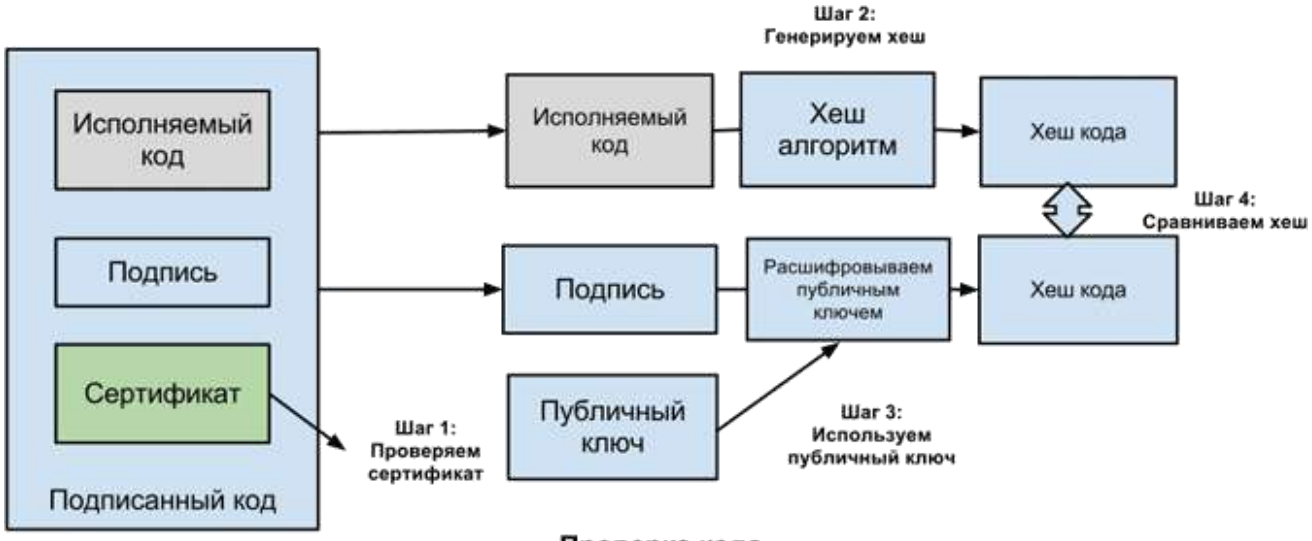
Процесс подписи кода



Подпись кода

1. Издатель (разработчик) запрашивает Code Signing сертификат у центра сертификации
2. Используя SIGNCODE.EXE или другую утилиту для подписи кода издатель, создает хеш кода, используя алгоритмы MD5 или SHA
3. Кодирует хеш, с помощью приватного ключа
4. Создает пакет, который включает в себя: код, зашифрованный хеш и сертификат издателя

Процесс проверки подписанного кода



Проверка кода

1. Пользователь скачивает или устанавливает подписанное ПО и платформа или система пользователя проверяет сертификат издателя, который подписан корневым приватным ключом центра сертификации
2. Система запускает код, используя тот же самый алгоритм создания хеша, как издатель и создает новый хеш
3. Используя публичный ключ издателя, который содержится в сертификате, система расшифровывает зашифрованный хеш
4. И сравнивает между собой 2 хеша

Центр сертификации (CA)

Центр сертификации - это организация, которая обладает правом выдачи цифровых сертификатов. Она производит проверку данных, содержащихся в CSR, перед выдачей сертификата. В самых простых сертификатах проверяется только соответствие доменного имени, в самых дорогих производится целый ряд проверок самой организации, которая запрашивает сертификат.

Когда разработчик запрашивает цифровой сертификат — центр сертификации идентифицирует его и выпускает сертификат, связанный с корневым сертификатом центра сертификации. Платформы и устройства содержат в себе корневой сертификат соответствующего центра сертификации. То есть если платформа или устройство доверяет какому-либо центру сертификации, то оно доверят и вашему сертификату, подписанному этим центром сертификации.

В случае если хеши не совпадают вы получите ошибку при запуске такого ПО — это может означать, что ПО было модифицировано вирусом или злоумышленником.

Когда ПО расшифровывает цифровую подпись, оно проверяет также корневой сертификат в системе, источник проверенной информации. В случае использования самоподписного сертификата, вы получите ошибку: «издатель не может быть проверен». Поэтому важно использовать сертификаты того центра сертификации, чьи корневые сертификаты уже установлены в системе у предполагаемого пользователя программы.

Timestamp или ***временная метка*** используется для указания времени, когда цифровая подпись была сделана. Если такая метка присутствует, то приложение, которое проверяет подпись проверит был ли сертификат, связанный с подписью валидным на момент подписи. Если же такой метки нет, и срок сертификата уже закончился, то подпись будет считаться недействительной.

Пример:

Сертификат действителен с: 01.01. 2008 Сертификат действителен до: 31.12.2010 Подпись сделана: 04.07.2009

Подпись проверена: 30.04.2012

С временной меткой (timestamp) подпись пройдет проверку, поскольку на момент подписи сертификат был действителен. Без такой метки сертификат не пройдет проверку, поскольку на момент проверки у сертификата уже закончился срок. То есть такая метка позволяет использовать подписанный код, даже после срок окончания сертификата.

Итак, для выбора сертификата сначала нужно выбрать центр сертификации, который выпускает сертификаты под нужную вам платформу.

Цифровые SSL сертификаты — это сокращение от Secure Socket Layer — это стандартная интернет технология безопасности, которая используется, чтобы обеспечить зашифрованное соединение между веб-сервером (сайтом) и браузером. SSL сертификат позволяет нам использовать https протокол. Это безопасное соединение, которое гарантирует, что информация, которая передается от вашего браузера на сервер остается приватной; то есть защищенной от хакеров или любого, кто хочет украсть информацию. Один из самых распространенных примеров использования SSL — это защита клиента во время онлайн транзакции (покупки товара, оплаты).

SSL сертификаты самый распространенный на данный момент тип сертификатов в Интернет. Чаще всего они используются в интернет-магазинах, то есть на сайтах, где есть функция заказа и где клиент вводит свои персональные данные. Для того, чтобы эти данные в момент передачи из браузера на сервер невозможно было перехватить используется специальный протокол HTTPS, который шифрует все передаваемые данные.

Для того, чтобы активировать возможность работы протокола HTTPS как раз и нужны цифровые SSL сертификаты.

Получение SSL сертификата:

- ***бесплатный способ*** — это так называемый, *самоподписной сертификат* (self- signed), который можно сгенерировать прямо на веб-сервере. Однако на такой сертификат все браузеры будут выдавать ошибку, с предупреждением, что сайт не проверен. То есть для служебных целей и для внутреннего использования такие сертификаты подходят, а вот для публичных сайтов, а тем более для сайтов, которые продают услуги, такие сертификаты противопоказаны.
- ***платные сертификаты***, выдаваемые центром сертификации. Данные в сертификате проверены центром сертификации и при использовании такого сертификата на сайте ваш посетитель никогда не увидит огромную ошибку на весь экран.

Говоря в общем, SSL сертификаты содержат и отображают (как минимум одно из) ваше доменное имя, ваше название организации, ваш адрес, город и страницу. Также сертификат всегда имеет дату окончания и данные о центре сертификации, ответственного за выпуск сертификата. Браузер подключается к защищенному сайту, получает от него SSL сертификат и делает ряд проверок: он не просрочен ли сертификат, потом он проверяет, выпущен ли сертификат известным ему центром сертификации (CA) используется ли сертификат на сайте, для которого он был выпущен.

Если один из этих параметров не проходит проверку, браузер отображает предупреждение посетителю, чтобы уведомить, что этот сайт не использует безопастное соединение SSL. Он предлагает покинуть сайт или продолжить просмотр, но с большой осторожностью.

Принцип работы SSL сертификата

Для того, чтобы получить SSL сертификат первое, что нужно сделать, это *сформировать специальный запрос* на выпуск сертификата, так называемый (Certificate Signing Request). При формировании этого запроса вам будет задан ряд вопросов, для уточнения деталей о вашем домене и вашей компании. После завершения ваш веб сервер создаст 2 типа криптографических ключей — приватный ключ и публичный ключ.

Публичный ключ не является секретным и он помещается в запрос CSR. Вот пример такого запроса:

-----BEGIN CERTIFICATE REQUEST-----
MIIC3zCCAccCAQAwgZkxCzAJBgNVBAYTAlVBMQ0wCwYDVQQIEwRLaWV2MQ0wCwYD
VQQHEwRLaWV2MRQwEgYDVQQKEwtIb3N0QXV0b21hdDEQMA4GA1UECxMHaG9zdGlu ZzEmMCQGCSqGSIb3DQEJARYXc3VwcG9ydEBob3N0YXV0b21hdC5jb20xHDAaBgNV

BAMTE3d3dy5ob3N0YXV0b21hdC5jb20wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAw
ggEKAoIBAQDTg7iUv/iX+SyZl74GcUVFHjFC5IqlTNEzWgLWrsSmxGxlGzXkUKid
NyXWa0O3ayJHOiv1BSX1l672tTqeHxhGuM6F7l5FTRWUyFHUxSU2Kmci6vR6fw5c
cgWOMMNdMg7V5bMOD8tfI74oBkVE7hV95Ds3c594u7kMLvHR+xui2S3z2JJQEwCh
mflIojGnSCO/iv64RL9vjZ5B4jAWJwrruIXO5ILTdis41Z1nNIx3bBqkif0H/G4e
O5WF6fFb7etm8M+d8ebkqEztRAVdhXvTGBZ4Mt2DOV/bV4e/ffmQJxffTYEqWg8w
b465GdAJcLhhiSaHgqRzrprKns7QSGjdAgMBAAGgADANBgkqhkiG9w0BAQUFAAOC
AQEAuCfJKehyjt7N1IDv44dd+V61MIqlDhna0LCXH1uT7R9H8mdlnuk8yevEcCRI
krnWAlA9GT3VkOY3Il4WTGg3wmtq6WAgLkVXQnhIpGDdYAflpAVeMKil8Z46BGIh
KQGngL2PjWdhMVLlRTB/01nVSKSEk2jhO8+7yLOY1MoGIvwAEF4CL1lAjov8U4XG
NfQldSWT1o8z9sDeGsGSf5DAXpcccx0gCyk90HFJxhbm/vTxjJgchUFro/0goVpB
credpKxtkwBMuCzeSyDnkQft0eLtZ9b9Q4+ZNDWsPPKxo/zWHm6Pa/4F4o2QKvPC
Px9x4fm+/xHqkhkR79LxJ+EHzQ==
-----END CERTIFICATE REQUEST-----

Данные которые содержатся в этом ключе можно легко проверить с помощью сервисов CSR Decoder. Как пример: CSR Decoder 1 или CSR Decoder 2. Второй сервис

выдает больше информации о CSR и проверяет ее на валидность, поле Signature в результатах проверки.

Если мы вставим такой запрос в форму для его расшифровки, то увидим, какие данные содержатся в публичном ключе.

CSR Information:

Common Name: tuthost.ua — доменное имя, которое мы защищаем таким сертификатом Organization: TutHost — название организации, которой принадлежит домен Organization Unit: Hosting department — подразделение организации

Locality: Kiev — город, где находится офис организации State: Kiev — область или штат

Country: UA — двухбуквенный код, страны офиса.

Email: support@tuthost.com — контактный email технического администратора или службы поддержки

После того как CSR сгенерирован можно приступать к оформлению заявки на выпуск сертификата. Во время этого процесса центр сертификации (CA — Certification Authority) произведет проверку введенных вами данных, и после успешной проверки выпустит SSL сертификат с вашими данными и даст возможность вам использовать HTTPS. Ваш сервер автоматически сопоставит выпущенный сертификат, со сгенерированным приватным ключем. Это означает, что вы готовы предоставлять зашифрованное и безопасное соединение между вашим сайтом и браузером клиентов.

В SSL сертификате хранится следующая информация:

- полное (уникальное) имя владельца сертификата
- открытый ключ владельца
- дата выдачи ssl сертификата
- дата окончания сертификата
- полное (уникальное) имя центра сертификации
- цифровая подпись издателя

Виды SSL сертификатов

Между собой сертификаты отличаются свойствами и уровнем валидации.

Типы сертификатов по типу валидации:

- Сертификаты, которые подтверждают только доменное имя (Domain Validation — DV).
- Сертификаты, которые подтверждают домен и организацию (Organization Validation — OV).
- Сертификаты, с расширенной проверкой (Extendet Validation — EV).

Сертификаты, подтверждающие только домен - это самые простые сертификаты, это ваш выбор если сертификат вам нужен срочно, так как выпускаются они автоматически и моментально. При проверке такого сертификата отсылается письмо со специальной ссылкой, по которой нужно кликнуть, чтобы подтвердить выпуск сертификата.

Важный момент, что это письмо может быть отправлено только на так называемый approver email, который вы указываете при заказе сертификата. И к адресу approver email есть определенные требования, он должен быть либо в том же домене для которого вы заказываете сертификат, либо он должен быть указан в whois домена. Если вы указываете email в том же домене, что и сертификат, то указывать любой emal тоже нельзя, он должен соответствовать одному из шаблонов: admin@, administrator@, hostmaster@, postmaster@, webmaster@

Еще один *Важный момент:* иногда сертификаты с моментальным выпуском попадают на дополнительную ручную проверку Центром сертификации, сертификаты для

проверки выбираются случайным образом. Так что всегда стоит помнить, что есть небольшой шанс, что ваш сертификат будет выпущен не моментально.

Сертификаты SSL с валидацией домена выпускаются, когда центр сертификации проверил, что заявитель имеет права на указанное доменное имя. Проверка информации об организации не проводится, и никакая информация об организации в сертификате не отображается.

Сертификаты с валидацией организации. В таком сертификате уже будет указано название организации. Такой сертификат частное лицо получить не может. Срок выдачи таких сертификатов как правило от 3 до 10 рабочих дней, зависит от центра сертификации.

После получения запроса на выпуск сертификата с проверкой организации центр сертификации производит проверку, реально ли существует такая организация, как указано в CSR и принадлежит ли ей указанный домен.

Сертификаты с расширенной проверкой. Это самые дорогие сертификаты и получить их сложнее всего. В таких сертификатах есть так называемый «green bar» — то есть при входе не сайт, где установлен такой сертификат в адресной строке браузера посетителя появится зеленая строка, в которой будет указано название организации, получившей сертификат.

Вот как это выглядит на сайте у Thawte.

Такие сертификаты обладают наибольшим уровнем доверия, среди продвинутых посетителей вашего сайта, поскольку сертификат указывает, что компания реально существует, прошла полную проверку и сайт действительно принадлежит ей.

SSL сертификаты с расширенной проверкой (EV) выпускаются только когда центр сертификации (CA) выполняет две проверки, чтобы убедиться, что организация имеет право использовать определенный домен плюс центр сертификации выполняет тщательную проверку самой организации. Процесс выпуска сертификатов EV стандартизирован и должен строго соотвествовать правилам EV, которые были созданы на специализированном форуме CA/Browser Forum в 2007 году.

EV сертификаты используются для всех типов бизнеса, в том числе для государственных и некоммерческих организаций. Для выпуска необходимо 10-14 дней.

Типы SSL сертификатов по своим свойствам:

- ***обычные SSL сертификаты*** - это сертификаты, которые выпускаются автоматически и подтверждают только домен. Подходят для всех сайтов.
- ***SGC сертификаты*** сертификаты с поддержкой повышения уровня шифрования. Актуально для очень старых браузеров, которые поддерживали

только 40 или 56 бит шифрование. При использовании этого сертификата уровень шифрования принудительно повышается до 128 бит.

- ***Wildcard сертификаты*** - нужны в том случае, когда кроме основного домена нужно обеспечить шифрование также на всех поддоменах одного домена. Например, есть домен domain.com и вам нужно установить такой же сертификат на support.domain.com, forum.domain.com и billing.domain.com
- ***SAN сертификаты*** – применяется, если необходимо использовать один сертификат для нескольких разных доменов, размещенных на одном сервере. Обычно в такой сертификат входит 5 доменов и их количество можно увеличивать с шагом в 5.
- ***EV сертификаты*** - это сертификаты с расширенной проверки и зеленой строкой в браузере. Получить их может только юридическое лицо, коммерческая,

некоммерческая или государственная организация.

- ***Сертификаты с поддержкой IDN*** - как правило, не у всех центров сертификации указана эта опция в описании сертификата, но не все сертификаты поддерживаются работу с IDN доменами. Список сертификатов, у которых есть такая поддержка: Thawte SSL123 Certificate, Thawte SSL Web Server, Symantec Secure Site, Thawte SGC SuperCerts, Thawte SSL Web Server Wildcard, Thawte SSL Web Server with EV, Symantec Secure Site Pro, Symantec Secure Site with EV, Symantec Secure Site Pro with EV.

САМОСТОЯТЕЛЬНАЯ РАБОТА

1) Назначение сертификата разработчика и предоставляемые гарантии ПО.
2) В зависимости от каких характеристик классифицируются сертификаты по центрам сертификации?
3) Укажите процессы подписи кода и проверки подписанного кода. Какую информацию мы видим в случае, наличия и отсутствия сертификата разработчика.
4) Назначение SSL сертификата, его содержание.
5) Укажите принцип работы SSL сертификата.
6) Укажите основные отличия разных типов SSL сертификатов в зависимости от уровня валидации и свойств.

Список рекомендуемых источников

Основные источники

1. Беспалов, Д. А. Администрирование баз данных и компьютерных сетей : учебное пособие / Д. А. Беспалов, А. И. Костюк ; Южный федеральный университет. - Ростов-на-Дону ; Таганрог : Южный федеральный университет, 2020. - 127 с. : ил., табл. - URL: https://biblioclub.ru/index.php?page=book&id=612220 (дата обращения: 29.03.2022). - Режим доступа: ЭБС Университетская библиотека онлайн, для зарегистрир. пользователей. - Библиогр. в кн. - ISBN 978-5-9275-3577-4. – Текст : электронный.
2. Илюшечкин, В. М. Основы использования и проектирования баз данных : учебник для среднего профессионального образования / В. М. Илюшечкин. — испр. и доп. — Москва : Издательство Юрайт, 2022. — 213 с. — (Профессиональное образование). — ISBN 978-5-534-01283-5. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://ezpro.fa.ru:3217/bcode/491755
3. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для среднего профессионального образования / О. В. Казарин, А. С. Забабурин. - Москва : Юрайт, 2022. - 312 с. - (Профессиональное образование). - URL: https://ezpro.fa.ru:3217/bcode/497433 (дата обращения: 29.03.2022) Режим доступа: ЭБС Юрайт, для зарегистрир. пользователей. - ISBN 978-5-534-13221-2. - Текст : электронный.
4. Лагоша, О. Н. Сертификация информационных систем : учебное пособие для спо / О. Н. Лагоша. - 2-е изд., стер. - Санкт-Петербург : Лань, 2021. - 112 с. - URL: https://e.lanbook.com/book/156616 (дата обращения: 09.03.2022). - Режим доступа: ЭБС Лань, для зарегистрир. пользователей. - ISBN 978-5-8114-7212-3. - Текст : электронный.
5. Тенгайкин, Е. А. Организация сетевого администрирования. Сетевые операционные системы, серверы, службы и протоколы. Практические работы : учебное пособие для спо / Е. А. Тенгайкин. - 2-е изд., стер. - Санкт-Петербург : Лань, 2022. - 100 с. - URL: https://e.lanbook.com/book/198497 (дата обращения: 29.03.2022). - Режим доступа: ЭБС Лань, для зарегистрир. пользователей. - ISBN 978-5-8114-9783-6. - Текст : электронный.
6. Черников, Б. В. Управление качеством программного обеспечения : учебник / Б. В. Черников. - Москва : ФОРУМ : ИНФРА-М, 2022. - 240 с. - (Среднее профессиональное образование). - URL: https://znanium.com/catalog/product/1850732 (дата обращения: 29.03.2022). - Режим доступа: ЭБС Znanium.com, для зарегистрир. пользователей. - ISBN 978-5-8199-0902-7. - Текст : электронный.

Дополнительные источники

1. Гвоздева, Т. В. Проектирование информационных систем. Стандартизация, техническое документирование информационных систем : учебное пособие для спо / Т. В. Гвоздева, Б. А. Баллод. - 2-е изд., стер. - Санкт-Петербург : Лань, 2021. - 216 с. - URL: https://ezpro.fa.ru:3178/book/176672 (дата обращения: 29.03.2022). - Режим доступа: ЭБС Лань, для зарегистрир. пользователей. - ISBN 978-5-8114-8414-0. - Текст : электронный.
2. Губин, А. Н. Проектная оценка надежности информационных систем : учебное пособие / А. Н. Губин. - Санкт-Петербург : СПбГУТ им. М.А. Бонч-Бруевича, 2019. - 77 с. - URL: https://e.lanbook.com/book/180062 (дата обращения: 09.03.2022). - Режим доступа: ЭБС Лань, для зарегистрир. пользователей. - Текст : электронный.
3. Даева, С. Г. Основы системного администрирования и администрирования СУБД : учебно-методическое пособие / С. Г. Даева. - Москва : РТУ МИРЭА, 2021. - 75 с. - URL: https://e.lanbook.com/book/171547 (дата обращения: 29.03.2022). - Режим доступа: ЭБС Лань, для зарегистрир. пользователей. - Текст : электронный.
4. Журавлев, А. Е. Корпоративные информационные системы. Администрирование сетевого домена : учебное пособие для спо / А. Е. Журавлев, А. В.

Макшанов, Л. Н. Тындыкарь. - Санкт-Петербург : Лань, 2021. - 172 с. - URL: https://e.lanbook.com/book/176675 (дата обращения: 29.03.2022). - Режим доступа: ЭБС Лань, для зарегистрир. пользователей. - ISBN 978-5-8114-8417-1. – Текст : электронный.

5. Мартишин, С. А. Базы данных: Работа с распределенными базами данных и файловыми системами на примере MongoDB и HDFS с использованием Node.js, Express.js, Apache Spark и Scala : учебное пособие / С. А. Мартишин, В. Л. Симонов, М. В. Храпченко. - Москва : ИНФРА-М, 2021. - 235 с. + Доп. материалы - (Среднее профессиональное образование). - URL: https://znanium.com/catalog/product/1189321 (дата обращения: 29.03.2022). - Режим доступа: ЭБС Znanium.com, для зарегистрир. пользователей. - ISBN 978-5-16-015643-9. - Текст : электронный.

Электронные издания (электронные ресурсы)

1. http://www.ed.gov.ru – Министерство образования Российской федерации.
2. http://www.edu.ru – Федеральный портал «Российское образование».
3. http://www.rambler.ru – Русская поисковая система.
4. http://www.yandex.ru – Русская поисковая система.
5. http://biblioteka.net.ru – Библиотека компьютерных учебников.
6. http://www.britannica.com – Библиотека Britannica.
7. http://ict.edu.ru/lib/ - Библиотека портала «ИКТ в образовании»
8. Единое окно доступа к образовательным ресурсам http://window.edu.ru/
9. Министерство образования и науки РФ ФГАУ «ФИРО» http://www.firo.ru/
10. Портал «Всеобуч»- справочно-информационный образовательный сайт, единое окно доступа к образовательным ресурсам –http://www.edu-all.ru/
11. Экономико–правовая библиотека [Электронный ресурс]. — Режим доступа: http://www.vuzlib.net.
12. http://www.consultant.ru. - Справочно-правовая система «Консультант Плюс»
13. http://www.garant.ru - Справочно-правовая система «Гарант».
14. http://www.nalog.ru. - Официальный сайт Федеральной налоговой службы
15. http://znanium.com – Электронно-библиотечная система znanium.com
16. http://www.urait.ru – электронная библиотека издательства ЮРАЙТ