Задание подготовлено в рамках проекта АНО «Лаборатория модернизации образовательных ресурсов» «Кадровый и учебно-методический ресурс формирования общих компетенций обучающихся по программам СПО», который реализуется с использованием гранта Президента Российской Федерации на развитие гражданского общества, предоставленного Фондом президентских грантов.

**Разработчик**

Плюснина Елена Викторовна, ГБПОУ «Тольяттинский социально-экономический колледж»

**Назначение задания**

Обработка информации. Уровень II

09.02.07 Информационные системы и программирование (специалист по информационным системам)

МДК.07.02 Сертификация информационных систем

Тема: Сертификация информационных систем

Один из ваших клиентов планирует переводить сайты на протокол https. Он предполагает, что будет несколько доменов и субдоменов, зарегистрированных на одно физическое лицо. Через сайты планируется продажа цифрового контента.

**Выберите тип SSL сертификата под задачи вашего клиента.**

**Запишите ваше предложение по типу сертификата и кратко (2-3 предложения) обоснуйте его.**

Следует выбрать сертификат \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,

поскольку \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Виды SSL Сертификатов**

**1.** **SSL сертификаты для одного домена -** самые простые в управлении, но при наличии большего числа доменов не такие эффективные, как два следующих типа. Они обеспечивают безопасность только для одного доменного имени и отлично подходят для веб-сайтов с простой структурой или для отдельных частей веб-сайта.

Данный сертификат SSL (Secure Socket Layer) защищает только одно доменное имя. Это правило применяется ко всем типам проверки (DV SSL, OV SSL, EV SSL).

## Типы SSL сертификатов с защитой одного домена

SSL - cертификат c проверкой домена (DV) - является идеальным выбором для защиты вашего блога, личного сайта или сайта малого бизнеса. Поскольку никаких документов не требуется, процесс получения сертификата очень быстрый и простой. Вы можете подтвердить право собственности на свой домен с помощью административного адреса электронной почты. Но в то же время, если у вас есть веб-сайт электронной коммерции или сайт, который собирает личные данные пользователя, вам следует подумать о приобретении сертификатов с проверкой организации (OV) или Extended Validation (EV), которые сделают ваш сайт более надежным.

SSL-сертификат c проверкой организации (Organization Validation (OV) рекомендуется тем, у кого есть Интернет магазин, сайт компании. Центр сертификации (ЦС) проверит, ведет ли Ваш бизнес законную деятельность. Поскольку проверка выполняется вручную, срок выпуска OV SSL осуществляется от 2 рабочих дней.

Расширенная проверка (EV или extended validation) - нужна не только связь с официально зарегистрированной компанией, но и её полное соответствие мировым стандартам финансовой отрасли. EV сертификаты SSL однозначно рекомендуется, если целью вашего веб-сайта является обеспечение крупных продаж или выполнение финансовых транзакций, вам следует рассмотреть возможность приобретения сертификата расширенной проверки. Поскольку этот тип SSL-сертификата активирует зеленую адресную строку (с названием вашей организации) и даст вашему сайту более высокий уровень доверия!

Технические параметры SSL-сертификатов

* 256-битное шифрование;
* Печать защиты сайта;
* Неограниченный и бесплатный перевыпуск сертификата в любое время;
* Неограниченные серверные лицензии;
* 15-дневный период тестирования;
* 99,9% совместимость со всеми основными браузерами;
* Защищает две версии основного домена [www.domain.com](http://www.domain.com/), так и domain.com;
* Устанавливает безопасное соединение между браузером и сервером.

**2.** [**Wildcard SSL сертификаты для защиты поддоменов**](https://www.emaro-ssl.ru/certificates/wildcard/) - прекрасный вариант для веб-сайтов с более сложной структурой, которые, например, состоят из нескольких разделов, находящихся на разных поддоменах одного основного домена. Это достаточно выгодный вариант, так как одним [Wildcard](https://www.emaro-ssl.ru/certificates/wildcard/) сертификатом можно покрыть до ста поддоменов и соответственно сэкономить на покупке множества отдельных сертификатов.

Wildcard Сертификаты (Wildcard Certificate) являются самым удобным способом предоставления SSL защиты и шифрования для главного домена и его поддоменов гарантируя доверие и защиту трансакций. Выгодный по стоимости и технически эффективный. Благодаря его функциональности Вы можете создавать поддомены, позже, без перевыпуска сертификата. Сертификат Wildcard работает по той же схеме, что и обычные сертификаты, позволяя Вам обеспечить защищенное соединение между Вашим вебсайтом и браузерами. Вы можете приобрести Wildcard SSL-сертификат двух типов: [с проверкой домена](https://www.emaro-ssl.ru/certificates/dv-ssl/) и [с проверкой компании](https://www.emaro-ssl.ru/certificates/ov-ssl/).

**3.** **Мультидоменные SSL сертификаты** - наиболее выгодный продукт для больших компаний, обладающих несколькими ресурсами на разных доменах. Он способен защитить до ста доменых имен, хотя при покупке его стоимость обычно включают только три, а остальные нужно покупать дополнительно. Как и Wildcard, мультидоменный SSL сертификат, поможет Вам сэкономить деньги и время на получение отдельных цифровых сертификатов.

Мультидоменный SSL - сертификат, также известный как (сертификат Unified Communications или сертификат SAN SSL) представляет собой тип сертификата, который использует альтернативные имена субъекта (SAN) для защиты нескольких веб-сервисов. В поле SAN сертификата может быть включено любое количество разных доменных имен, что позволяет сертификату работать с любым из включенных доменных имен.

Вы можете легко добавить SAN к своим SSL сертификатам DV, OV или EV для защиты нескольких доменов или поддоменов.

SSL сертификат (MDC) идеально подходит для организаций с несколькими уникальными доменами, размещенными на одном сервере. Вы можете сэкономить время и деньги, сохраняя при этом высокий уровень доверия и безопасности. Сравните стоимость покупки множества отдельных сертификатов для защиты всех ваших доменов с покупкой одного мультидоменного сертификата. Этот исключительный SSL-сертификат идеально подходит для любой среды, где необходима защита нескольких доменных имен. Вы можете добавлять, редактировать или удалять домены в любом промежутке времени действия сертификата.

SSL MDC сертификаты поддерживают до 256-бит шифрования и 2048-бит секретных ключей, которые обеспечивают пользователям полную защиту передаваемой информации.

**Какой SSL-сертификат выбрать?**

Итак, мы определились с тем, что SSL-сертификаты различаются между собой не только брендом и ценой. Сегодняшний ассортимент предложений предусматривает широкий круг задач, для которых может потребоваться SSL.

Например, если вы просто хотите уберечь пользователей вашего веб-сайта от навязчивых предупреждений браузера о посещении непроверенного сайта, будет достаточно за несколько минут получить простой [DV (Domain Validation)](https://1cloud.ru/services/ssl/dv) сертификат. Если же вы используете свою интернет-площадку для операций, требующих повышенного уровня сохранности данных компании и клиентов - стоит задуматься об [EV (Extended Validation)](https://1cloud.ru/services/ssl/ev) сертификате. А если вы используете не один, а несколько веб-адресов для сайта или сайтов компании - для вас на рынке представлены сертификаты [Wildcard](https://1cloud.ru/services/ssl/wc) и [SAN](https://1cloud.ru/services/ssl/san).

**Каковы особенности типов SSL-сертификатов?**

Рассмотрим подробнее виды предлагаемых сегодня на рынке SSL-сертификатов. Их отличия условно можно разделить на две группы

По методу проверки:

Сертификаты с проверкой домена (Domain Validation - DV) подтверждают, что пользователь находится именно на том веб-сайте, на доменный адрес которого осуществил переход, то есть удостоверяет веб-сервер, который обслуживает сайт. Такой сертификат не содержит информации о компании-владельце сайта, а потому не может считаться достаточно безопасным для оказания коммерческих услуг. DV рекомендуется к использованию на площадках, где не требуется строгая гарантия безопасности.

Так выглядит адресная строка пользовательского браузера при посещении им сайта с установленным DV-сертификата SSL. При щелчке на значке зашифрованного соединения отображается только информация о доменном имени, для которого выпущен сертификат:

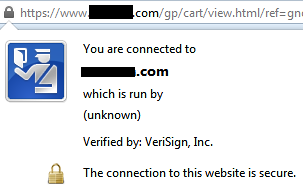
Details of the certificate: subject: CN = www.yourdomain.com

domain_validation

Сертификаты с проверкой организации (Organization Validation - OV) являются подтверждением не только доменного имени, но и организации-владельца веб-сайта. Подлинность последней проверяется по регистрационным данным юридического лица, которые необходимо предоставить провайдеру SSL при заказе сертификата. OV-сертификаты на сегодняшний день, пожалуй, наиболее популярны среди клиентов.

Так выглядит информация о сертификате в адресной строке посетителя сайта. Как вы видите, здесь отображена весьма подробная информация об организации-владельце сайта, позволяющая определить её подлинность.

Details of the certificate: CN = www.yourdomain.com, O = Company Name, OU = Management, L = Moscow, S = MSK, C = RU



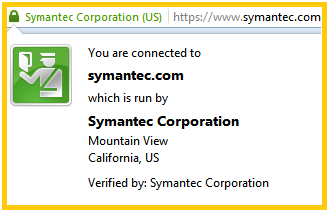
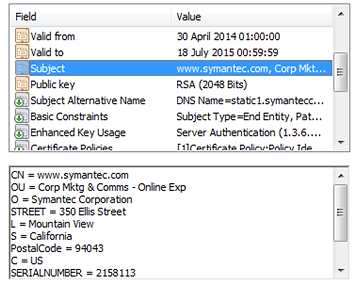
Сертификат с расширенной проверкой (Extended Validation - EV) имеет самый высокий уровень доверия со стороны других интернет-узлов. Он является оптимальным решением для сайтов, работа которых требует строгой конфиденциальности передаваемых данных (например, при совершении финансовых транзакций). Само название этого типа сертификатов подразумевает расширенную периодическую проверку данных владельца сайта для предотвращения их подмены.

Примечание: при первоначальном внедрении SSL-сертификатов в глобальную сеть, центры сертификации предоставляли только сертификаты с проверкой данных организации. Появление типа Domain Validation - следствие коммерческого интереса, постепенно заставившего вендоров выпускать «упрощённые» сертификаты с проверкой только домена. Отчасти, это сыграло и продолжает играть на руку интернет-мошенникам, пользующимся тем, что обычно интернет-браузер не предупреждает пользователя о возможных проблемах с подлинностью сайта, если первоначально предоставленный этим сайтом сертификат будет иметь хотя бы минимальный уровень доверия.

EV-сертификат призван на борьбу с вышеописанной проблемой. Это достигается путём отображения непосредственно в адресной строке клиента информации об организации-владельце сайта в виде дополнительного ярлыка, выделенного зелёным цветом (Green Bar). Такой ярлык сложно не заметить. Теперь пользователю не обязательно кликать по иконке сертификата браузере для получения подробной информации о нём - самое важное подтверждение он получит, просто взглянув на адресную строку. Опция Green Bar поддерживается всеми популярными интернет-браузерами на всех актуальных операционных системах. сертификат расширенной проверки, доступен только юридическим лицам.

Примечание: опция Green Bar недоступна для DV- и OV-сертификатов. Ею удостоены только SSL-сертификаты с расширенной проверкой.

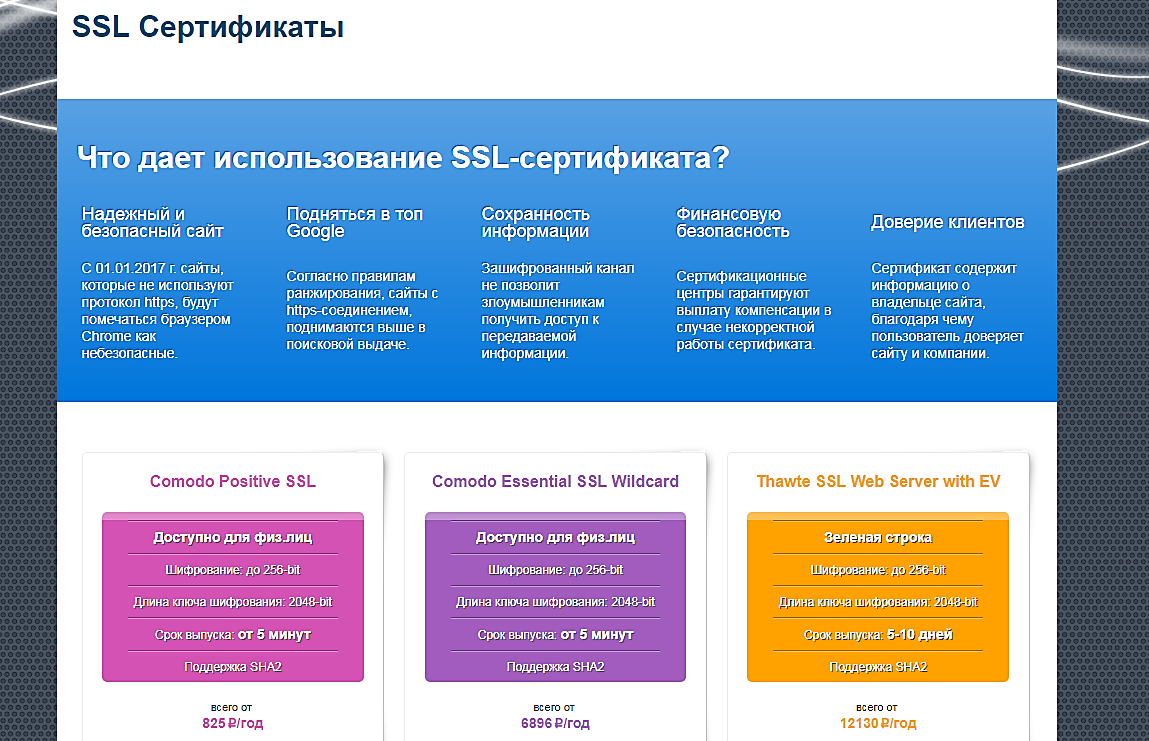
Ниже представлен пример отображения сведений об EV-сертификате в клиентском браузере.

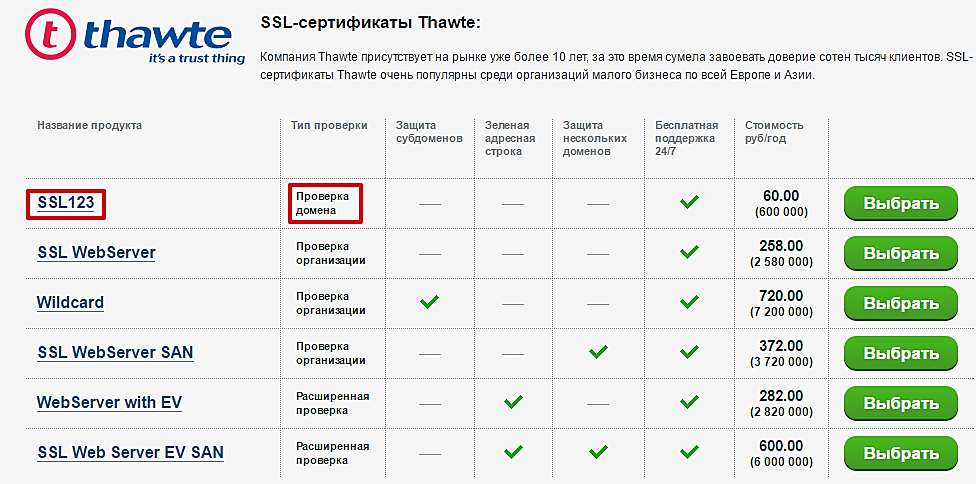


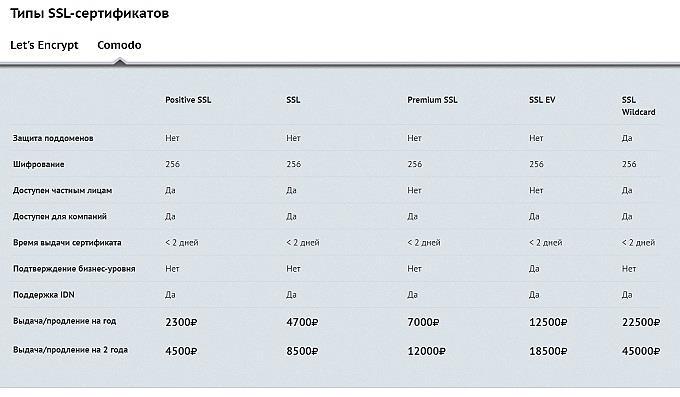
Мы рассмотрели типы SSL-сертификатов по методу проверки сайта. Помимо этого различия, немаловажным является и разграничение сертификатов по сертифицируемым доменам. Этот параметр определяет список доменов (поддоменов) сайта, на которые будет распространяться приобретённый сертификат.

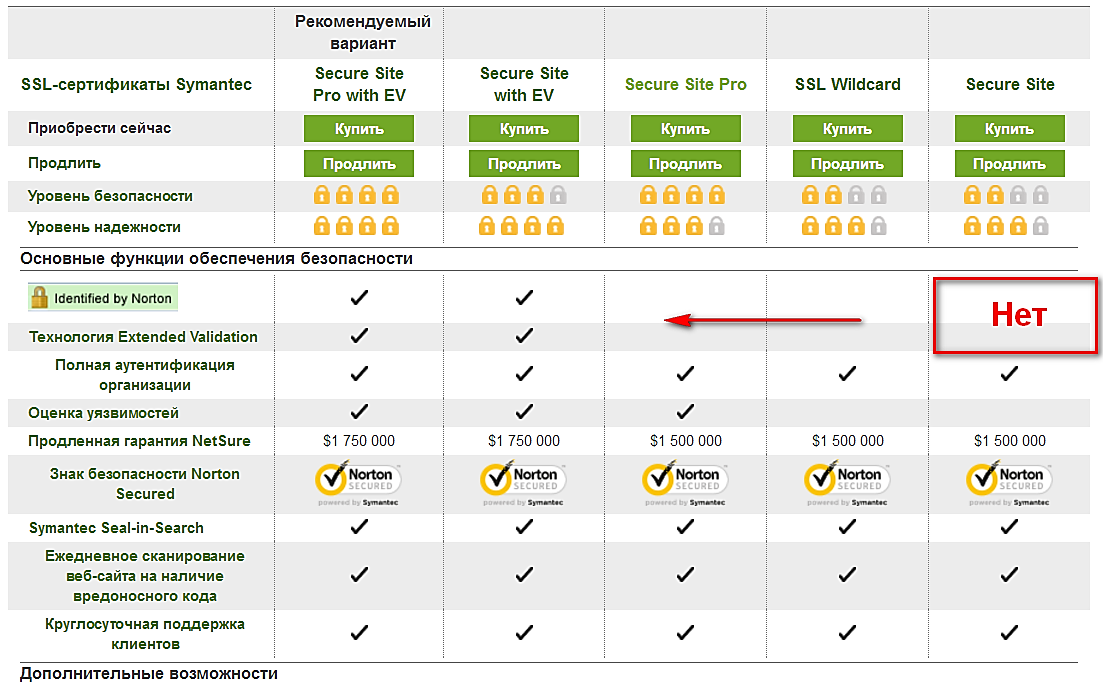
По сертифицируемым доменам:

* [Сертификат на один домен](https://1cloud.ru/services/ssl/dv) (Single Certificate) - работает для одного доменного имени, указанного при заказе. То есть, например, домен yourcompany.com, для которого приобретён сертификат, будет защищён, но используемые поддомены (sub.yourcompany.com), при их наличии, уже не будут.
* [Wildcard SSL](https://1cloud.ru/services/ssl/wc) - может использоваться для домена, указанного при регистрации, и всех его поддоменов (sub1.yourcompany.com, sub2.yourcompany.com, sub3.yourcompany.com). Wildcard поддерживает и работу интернет-площадки на распределённых серверах.
* UC (Unified Communications) или [SAN (Subject Alternative Name)](https://1cloud.ru/services/ssl/san) сертификаты могут использоваться сразу для нескольких или многих доменов и серверов









*Использованы материалы источников:*

[*https://www.emaro-ssl.ru/blog/ssl-type/*](https://www.emaro-ssl.ru/blog/ssl-type/)*;* [*https://1cloud.ru/blog/vidy-sertifikatov-ssl*](https://1cloud.ru/blog/vidy-sertifikatov-ssl)*.*

Инструмент проверки

|  |  |
| --- | --- |
| Выбран сертификат Domain **Validation** SSL | 1 балл |
| Приведены обоснования: |  |
| Осуществляет проверку домена с субдоменами | 1 балл |
| Требуется сертификация домена, а не организации… | 1 балл |
| …следовательно, может быть зарегистрирован на физическое лицо | 1 балл |
| ***Максимальный балл*** | ***4 балла*** |