LeaderSSL®

Всё, что нужно знать о безопасности сайтов и SSL-сертификатах

Оглавление

1. Бесплатные сертификаты: почему не стоит их использовать

Бесплатные сертификаты: почему не стоит их использовать

Бесплатные SSL-сертификаты – казалось бы, очень выгодный и удобный способ защиты своего сайта. Действительно, зачем что-то покупать, когда все это можно получить совершенно бесплатно в различных Центрах Сертификации? Бесплатные сертификаты привлекают владельцев бизнеса, однако в конечном счете они приводят к убыткам. Почему? Давайте посмотрим далее.

Бесплатным SSL-сертификатам редко доверяют крупные компании

Чтобы крупные корпорации включили корневой ключ центра сертификации в свои продукты, этот центр сертификации должен отвечать многочисленным условиям, реализация которых требует значительных финансовых инвестиций. Привлечь такие инвестиции без предложения платных продуктов практически невозможно. Именно по этой причине центры сертификации, предоставляющие бесплатные сертификаты, нередко имеют в своей линейке продуктов платные решения, которые отличаются дополнительными преимуществами: быстротой выпуска, возможностью включения субдоменов, расширенной аутентификацией и т.д.

Бесплатные сертификаты не подходят для сайтов с приемом платежей

Бесплатные SSL-сертификаты не рекомендуется использовать для защиты интернет-магазинов, сайтов банков, микрофинансовых организаций, а также любых других сайтов, принимающих платежи, поскольку посетители не могут видеть информацию о компании, которой выдан сертификат. Пользователи меньше доверяют обезличенным сертификатам, что негативно отразится на продажах.

Бесплатные SSL-сертификаты поставляются только в виде DV (Domain Validation)

Бесплатные сертификаты выпускаются только с проверкой по домену. Такой тип проверки недоступен для Code Signing, OV и EV продуктов, что значительно ограничивает их использование.

Бесплатные сертификаты: почему не стоит их использовать

Сравнение SSL-сертификатов по брендам

Показатель сравнения	Let's Encrypt	PositiveSSL	PositiveSSL Wildcard	Sectigo (Comodo) EV
Стоимость выпуска	Бесплатно	1 200* руб.	10 500* руб.	12 600* руб.
Стоимость перевыпуска	Бесплатно	Бесплатно	Бесплатно	Бесплатно
Защита основного домена (одного)	Да	Да	Да + все поддомены	Да
Дополнительная защита домена с «www»	—	Да	Да	Да
Наименование организации в браузере	—	—	—	Да
Поддержка поддоменов	Да	—	Да	—
Вывод замочка	Да	Да	Да	Да
Логотип доверия	—	Да	Да	Да
Повышение продаж	Нет	Да (минимальное)	Да (минимальное)	Да (максимальное)
Повышение позиций сайта в выдаче Google	Да	Да	Да	Да
Подходит для использования	Некоммерческие сайты, блоги	Некоммерческие сайты, блоги	Сети сайтов компаний, организаций	Сайты банков, интернет-магазины
Тип проверки	По домену	По домену	По домену	Расширенная проверка
Мобильная поддержка	Да	Да	Да	Да

Бесплатные сертификаты: почему не стоит их использовать

Показатель сравнения	Let's Encrypt	PositiveSSL	PositiveSSL Wildcard	Sectigo (Comodo) EV
Страхование	—	Среднее	Среднее	Высокое
Поддержка браузеров	Только крупные браузеры	Все браузеры (99.9%)	Все браузеры (99.9%)	Все браузеры (99.9%)
Длина ключа	256bit	256bit	256bit	256bit
Шифрование	SHA2	SHA2	SHA2	SHA2
Защита страниц сайта от изменений	Да	Да	Да	Да
Гарантии**	—	10,000$	10,000$	250,000$
		Рекомендуется для физ. лиц		**Рекомендуется для организаций**

*При покупке в ЛидерТелеком: Бесплатный тестовый период 14 дней - без введения данных карт и предоплат

**При взломе сертификата будет выплачена компенсация покрыты любые расходы компании и потери со стороны клиентов. С бесплатными сертификатами гарантий нет и любые потери будут компенсироваться за ваш счет.

Все это говорит о том, что бесплатные SSL-сертификаты – это «сыр в мышеловке». Лучше всего использовать проверенные платные решения от известных центров сертификации. Цены на SSL-сертификаты сегодня доступны всем клиентам, в чем Вы можете убедиться лично, посетив сайт ЛидерТелеком.

2. Как SSL-сертификаты защищают от интернет-мошенничества

Жертвой интернет-мошенников может стать каждый. Если вы являетесь клиентом онлайн-банка, пользуетесь платежными системами или совершаете покупки в Интернете - обратите внимание на эти простые рекомендации, которые помогут обезопасить вас от разного типа мошенничества онлайн. Подробнее читайте по ссылке.

Фишинг: как не попасть на деньги

Фишинг - это вид интернет-мошенничества, при котором злоумышленники получают доступ к конфиденциальным данным пользователей, например, к логинам, паролям и номерам банковских карт. Доступ к таким данным получают с помощью специально созданных страниц и сайтов, внешне очень похожих на оригинальные. Осуществляя ввод своих данных на таких подставных сайтах, пользователи дают возможность злоумышленникам получить доступ к нужной информации.

Один из пользователей платежной системы QIWI рассказал нам, как стал жертвой мошенников. При выводе денежных средств с Forex, Роман попал на фишинговый сайт. Ценой этому стали 100 тысяч рублей, которые были украдены. Впоследствии Роман вспомнил, что у него не была включена двухфакторная авторизация по смс. Этот наглядный пример показывает, как важно защитить свои данные всеми возможными способами.

Многие фишинговые сайты не так просто отличить от настоящих. Особенно это становится затруднительным при использовании мобильных устройств. Тогда как же определить, является ли сайт оригинальным и можно ли ему доверять свои данные?

Первое отличие фишингового сайта

- это его url-адрес (то, что пишется в адресной строке браузера). Так, существует множество сайтов с адресами, похожими на https://qiwi.com/. Многие из таких сайтов могут быть недоступны большую часть времени и активироваться лишь на несколько часов в сутки:

- t.qiwi.com
- qiwi-visa.com
- qivvi.co
- qiwi.hk

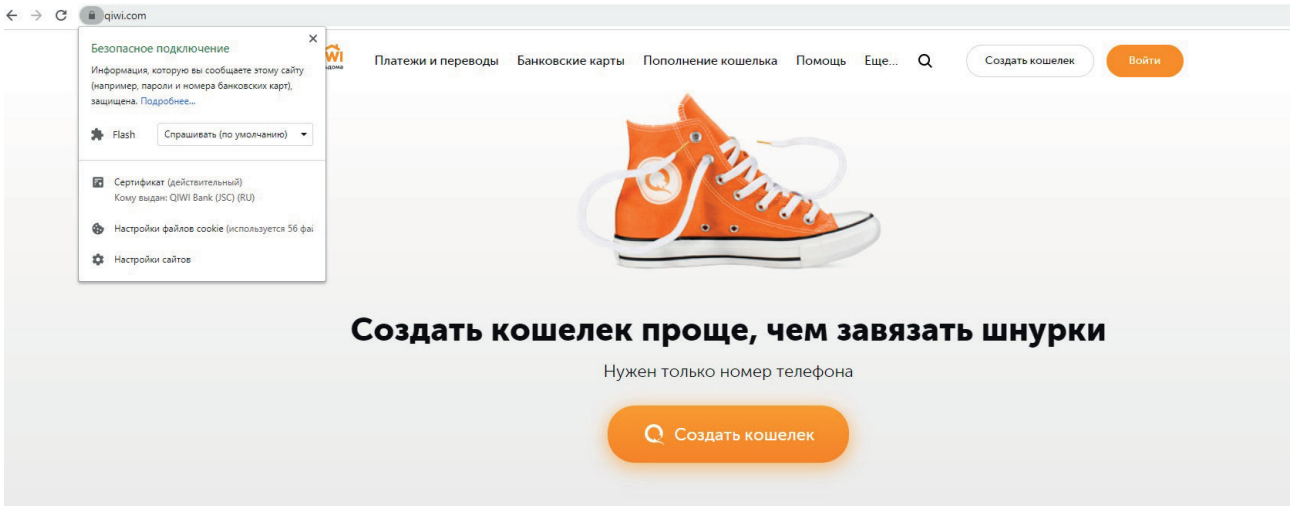
Как SSL-сертификаты защищают от интернет-мошенничества

Почему же люди заходят на такие сайты? Обычно, первые строчки в результатах поиска - это контекстная реклама - оплаченные ссылки, которые могут не иметь ничего общего с оригинальными сервисами. Заходя на такие сайты можно не заметить, что адрес сайта отличается, так как название сервиса обычно совпадает с оригиналом.

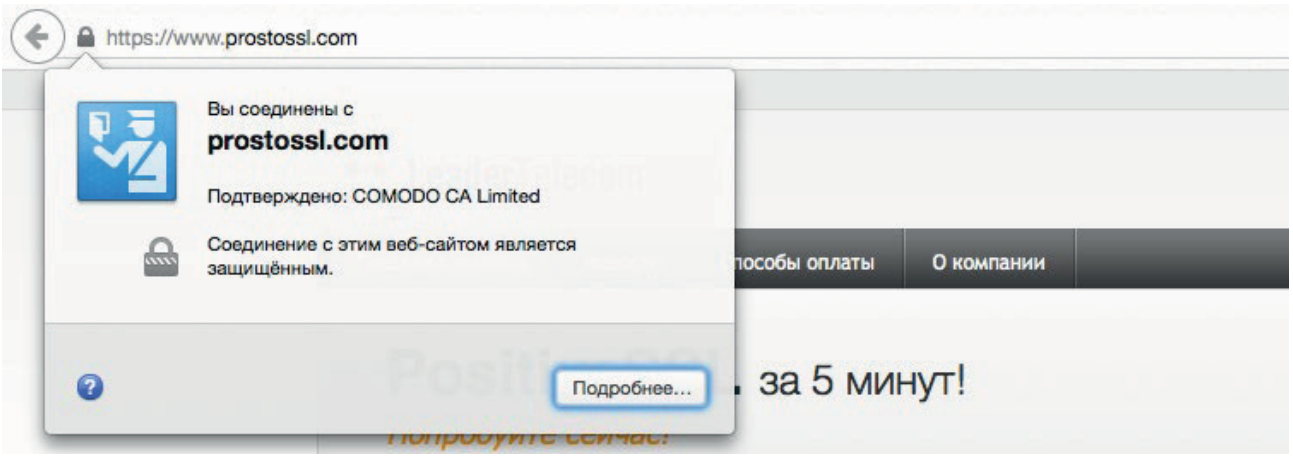
Второе отличие фишингового сайта

- это отсутствие SSL-сертификата. Все страницы сайта, на которых пользователь может вводить конфиденциальную информацию, должны использовать безопасный протокол передачи данных https. Большинство подставных сайтов используют обычное соединение http, а это значит, что таким сайтам доверять нельзя.

Когда вы находитесь на защищенной странице сайта, в адресной строке отображается значок «Замок» в браузере, при нажатии на который можно узнать информацию о сертификате.



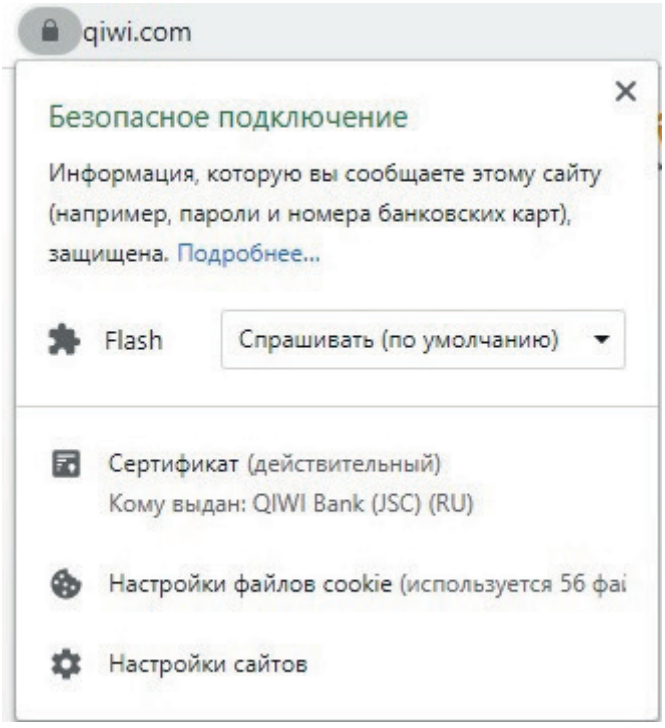
В настоящее время существуют фишинговые сайты, которые используют защищенное соединение со значком «Замок». В таком случае нужно обращать внимание на тип сертификата: DV-сертификат будет подтверждать защиту данных в рамках подставного сайта, но не подтверждение принадлежности сайта нужной организации (например, Qiwi). Обычно при таком типе сертификата замочек в браузерной строке отображается серым.



EV-сертификат

говорит о безопасном соединении и при нажатии на значок „Замок“ отображается название организации. EV-сертификаты являются наиболее доверительными.

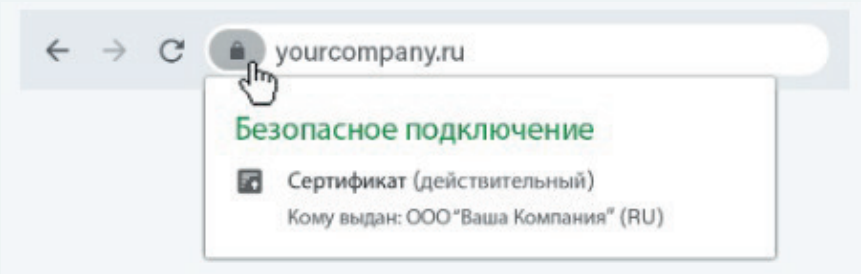
Наличие такого сертификата демонстрирует название компании в браузере, что для большинства пользователей интернета давно является символом и гарантом безопасности.



В помощь организациям: SSL-сертификат

Правильным шагом для любой организации, чья деятельность связана с обработкой конфиденциальных данных своих пользователей - это приобретение EV SSL-сертификата для гарантии безопасности.

EV SSL сертификаты - максимум доверия!



- Для организаций, которым важен престиж и максимальное доверие
- Расширенная проверка по организации (EV)
- Защищает один или несколько доменов
- Отображение имени компании в браузере

Получите максимум доверия с EV (Extended Validation) сертификатом с расширенной проверкой

ЗАКАЗАТЬ СЕРТИФИКАТ

При использовании такого сертификата вся информация кодируется и превращается в набор символов, который становится бесполезным для злоумышленников.

Результат использования EV SSL-сертификата для организации - это рост продаж для всех сфер Ecommerce до 10-40%, подтвержденный независимыми исследователями.

Более подробную информацию о EV SSL-сертификатах вы можете получить на нашем сайте по ссылке https://www.leaderssl.ru/products/ev

3. Какой SSL-сертификат выбрать?

Различия между DV и OV сертификатами

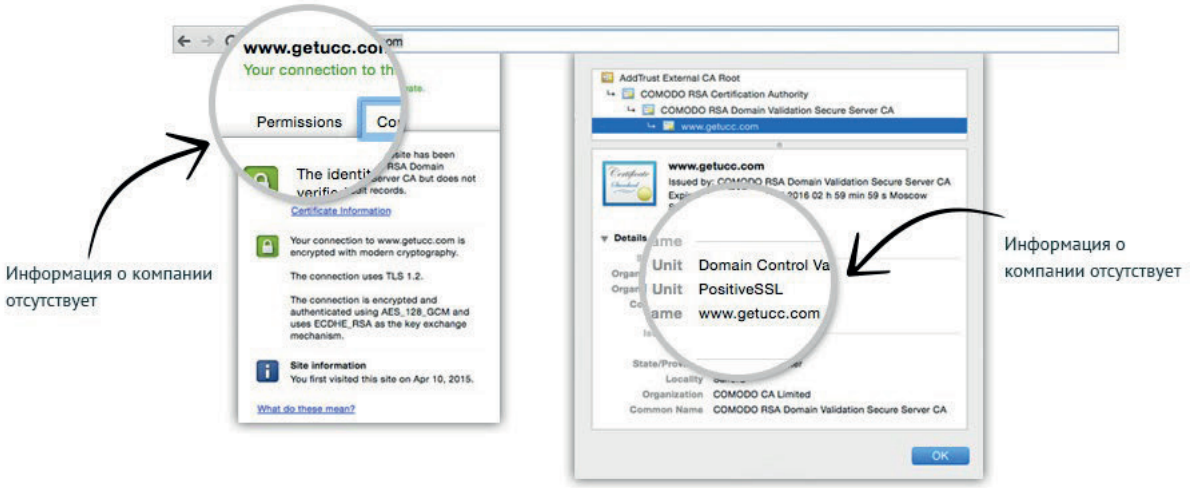
Какой SSL-сертификат выбрать: DV или OV?

Многие сомневаются какой SSL-сертификат выбрать. SSL-сертификаты могут быть трех типов: DV, OV и EV. В рамках текущей статьи мы остановимся на двух первых типах сертификатов, DV (с проверкой по домену) и OV (с проверкой по организации), и покажем вам, чем они отличаются и почему стоит перейти с DV на OV.

DV-сертификаты

(от английского Domain Validation). Для их выпуска используется самый базовый уровень SSL валидации. Центр сертификации просто убеждается в том, что вы являетесь владельцем определенного домена, что проверяется при помощи информации, которая содержится в WHOIS. Конечно, такой сертификат позволяет обеспечить надежное кодирование данных на вашем сайте, однако он не проверяет тот факт, что вы являетесь владельцем законного бизнеса. Это – вполне подходящее, и, что самое главное, очень быстрое решение для защиты своего сайта при помощи HTTPS. Пользователи, видя замочек в адресной строке браузера, будут доверять вашему сайту в разы больше, чем до этого, ведь для них такой знак является фактором доверия.

Пример DV-сертификата:



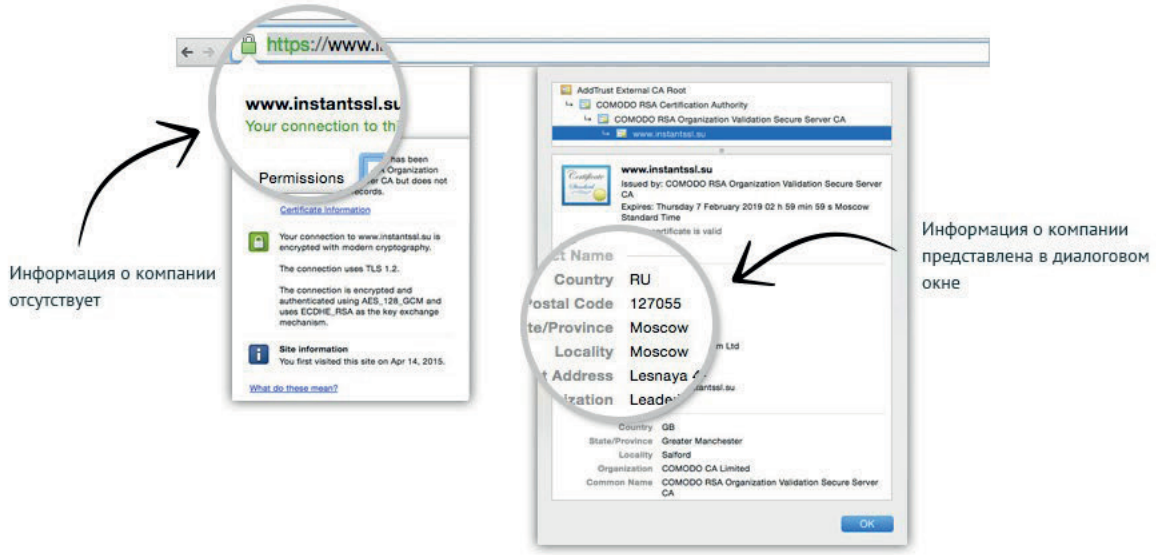
Все было бы хорошо, если бы не одно но: DV-сертификат могут использовать злоумышленники на фишинговых сайтах. Доверчивые пользователи видят заветный замочек и вводят данные, которые в результате оказываются в руках мошенников. То, что канал передачи данных защищен, еще не говорит о том, что данные уйдут в нужном направлении. Пользователь должен быть уверен, что сайт принадлежит именно той компании, у которой он хочет произвести покупку или выполнить другие действия, связанные с вводом важной информации.

Именно по этой причине мы рекомендуем приобрести OV-сертификат.

OV-сертификаты

(от английского Organization Validation) предназначены для компаний и организаций. В частности, они полезны для ведения электронной коммерции, интернет-продаж. Такие сертификаты требуются для сайтов, на которых пользователи вводят важную информацию (номера кредитных карт, контактные данные и т.д.). OV-сертификат удостоверяет владельца сайта и содержит в себе название компании. Процесс валидации таких сертификатов является более долгим и углубленным. Центр сертификации проверяет не только тот факт, что вы являетесь владельцем домена, но и тот факт, что вы – владелец реально существующей компании. Компания должна присутствовать на сайте государственного регистрирующего органа и в доверенном интернет-справочнике (к примеру, dnb.com). Мошенники не смогут получить такой сертификат, поскольку у них не получится пройти валидацию. Основное преимущество получения OV-сертификата – ваша компания будет отмечена в сертификате.

Пример OV-сертификата:



Соответственно, вам стоит задуматься о переходе с DV-сертификата на OV-сертификат, если:

- **Вам нужно максимально защитить важные данные пользователей**
- **Вы хотите, чтобы название вашей компании выводилось в сертификате (а значит, пользователи будут больше доверять вам)**

- **Вы планируете расширять свой бизнес и выводить его на новый уровень**
- **Вы хотите, чтобы люди знали, что сайт принадлежит законному владельцу компании, т.е. деньги или важные данные не попадут к мошенникам**

Если вы хотите перейти с DV-сертификата на OV-сертификат, обязательно обратитесь к специалистам компании ЛидерТелеком. Наши знания, опыт и отлаженный процесс взаимодействия с УЦ сделают выпуск сертификата с проверкой по организации легким и удобным.

Более подробная информация о DV SSL-сертификатах:
https://www.leaderssl.ru/products/dv

Информация о OV SSL-сертификатах:
https://www.leaderssl.ru/products/ov

4. Какой SSL-сертификат выбрать?

Различия между OV и EV сертификатами

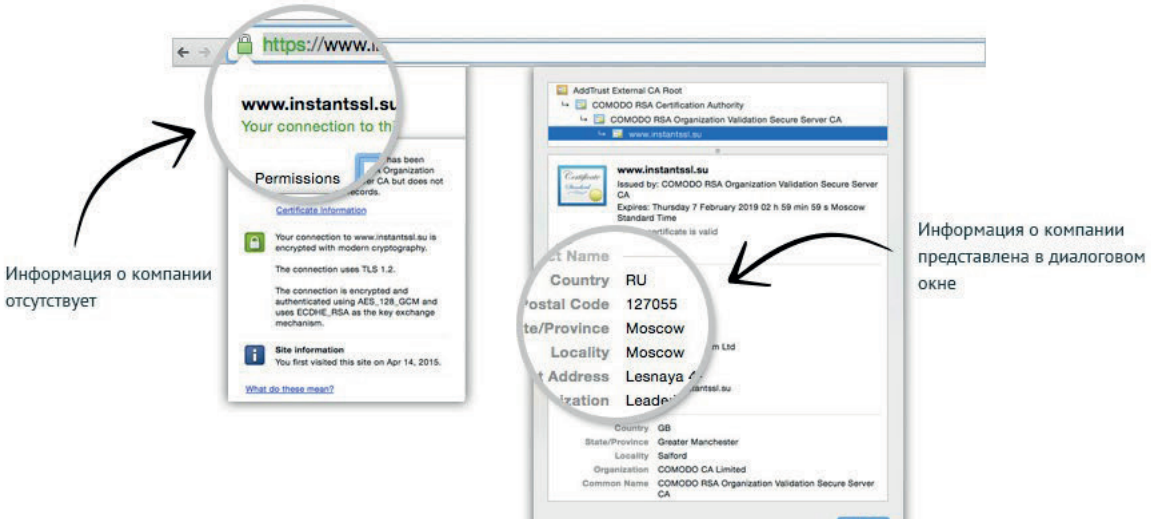
Какой SSL-сертификат выбрать: OV или EV?

Сегодня SSL-сертификаты являются обязательным условием ведения электронной коммерции. Вряд ли можно представить себе сайт, который вызывал бы доверие в глазах посетителей и при этом был незащищенным. Пользователи просто не станут вводить конфиденциальную информацию на таких ресурсах, даже если у них стоит цель что-либо приобрести. Именно по этой причине владелец любого бизнеса, существующего в сети, должен обеспокоиться заказом SSL-сертификата через проверенную компанию. Вот только встает ожидаемый вопрос: какой тип сертификата лучшего всего выбрать – с проверкой по организации (OV) или с расширенной проверкой (EV)? В чем разница между этими двумя SSL-сертификатами?

OV-сертификат

(от английского Organization Validation) – это сертификат, который подтверждает существование организации. Чтобы его получить, компания должна пройти валидацию. При валидации удостоверяющему центру необходимо убедиться в юридическом (для этого дается ссылка на государственный ресурс) и физическом (для этого дается ссылка на доверенный онлайн-справочник) существовании компании. Соответственно, если сайт защищен OV-сертификатом, то в таком случае его посетители будут видеть замочек в адресной строке браузера, который покажет, что сайт надежно защищен от злоумышленников.

Пример OV-сертификата:



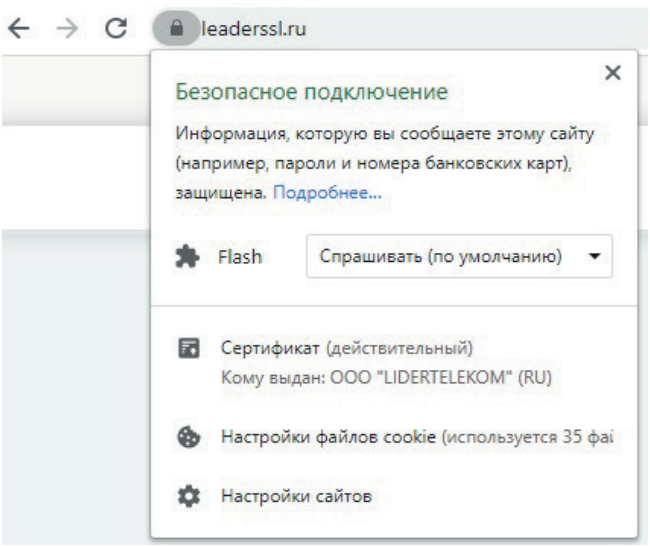
Однако OV-сертификат лишен некоторых дополнительных преимуществ, которые позволяет получить EV-сертификат.

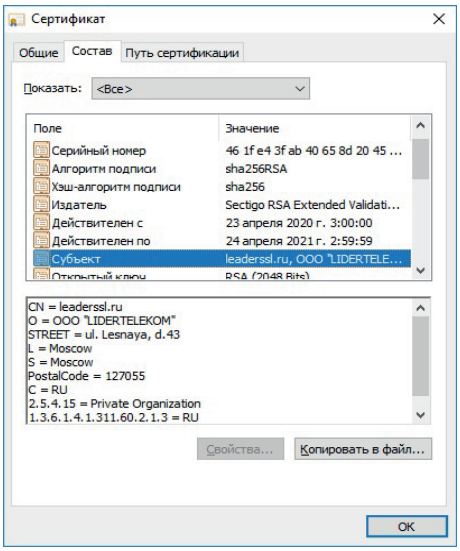
Более подробную ифнормацию о OV SSL-сертифкатах вы можете получить на нашем сайте по ссылке https://www.leaderssl.ru/products/ov

EV-сертификат

(от английского Extended Validation). Это самое эффективное и престижное решение, которое активно применяется в онлайн-бизнесе. Данный сертификат позволяет добиться отображения имени компании в браузере, что является гарантом безопасности и надежности. Посетители видят, что вы - действительно та компания, за которую выдаете себя, а не злоумышленники, наживающиеся на доверчивых пользователях. Получить такой сертификат не намного сложнее, чем OV, но при этом он более престижный и более доверенный. EV-сертификат полезен для вашего бизнеса, поскольку он помогает увеличить продажи вследствие возросшего доверия пользователей.

Пример EV-сертификата:





Какой же сертификат предпочесть, OV или EV? Ответ очевиден – EV. Почему лучше всего обращаться именно к EV-сертификатам для защиты своего сайта:

- **EV-сертификаты включают в себя название компании (выводится в адресной строке браузера) и некоторые дополнительные данные о ней**

- **EV-сертификаты по цене не намного дороже OV-сертификатов, но при этом имеют больше преимуществ**
- **EV-сертификаты используют многие крупные корпорации**

Единственное, что останавливает владельцев сайтов от получения EV-сертификата – это углубленная валидация и более продолжительное время выпуска, чем у любого другого сертификата. Однако если вы доверите этот процесс профессионалам, то в таком случае вам не придется ни о чем волноваться – мы поможем вам решить все вопросы и получить готовый EV-сертификат.

Специалисты компании ЛидерТелеком всегда к вашим услугам!

Информация о OV SSL-сертификатах:
https://www.leaderssl.ru/products/ov

Информация о EV SSL-сертификатах:
https://www.leaderssl.ru/products/ev

5. SSL-сертификаты для интернет-магазинов: обязательное дополнение для онлайн-бизнеса

SSL-сертификаты для интернет-магазинов

Вы открыли интернет-магазин своей мечты, который уже приносит Вам некоторый доход, однако Вы пытаетесь найти способы сделать его более прибыльным. Какие возможности по увеличению доходов у Вас имеются? Одно из популярных решений – SSL-сертификат, который позволит Вам продавать больше за счет роста доверия потенциальных покупателей. SSL-сертификат несет в себе сразу три преимущества:

- **увеличивает Ваши доходы за счет увеличения доверия к Вашему сайту;**
- **защищает персональные данные Ваших клиентов от кражи;**
- **позволяет предотвратить появление сайтов-двойников (или, как их еще называют, фишинговых сайтов)*.**

SSL – это современный стандарт для осуществления практически всех финансовых операций в сети.

Интернет-магазины очень сложно представить без использования SSL, ведь они проводят различные финансовые транзакции, запрашивают ввод чувствительных пользовательских данных. Такие сайты очень уязвимы к краже паролей, вследствие чего их необходимо обязательно защищать с помощью SSL.

Рекомендации профессионалов: защита всего интернет-магазина, а не только его отдельных страниц с важными данными. Такой подход дает массу преимуществ:

- **Пользователи сразу же видят, что Ваш сайт защищен – адресная строка браузера имеет замочек и/или наименование компании**
- **Никто не сможет украсть ценную информацию Ваших покупателей (номера кредитных карт, почтовый адрес, личные данные пользователя и т.д.)**
- **Доступ к анализу статистики посещений для аналитических сервисов будет закрыт (никто не узнает, какие страницы посещал Ваш покупатель, что именно он приобретал и т.д.)**

Какой SSL-сертификат выбрать?

Сегодня существует широкий спектр различных SSL-провайдеров: DigiCert, Sectigo (Comodo), Thawte и т.д. Если вы продаете премиальные продукты, то в таком случае Вам лучше всего воспользоваться сертификатом DigiCert Secure Site Pro with EV. Вместе с ним Вы получите специальную печать доверия Norton Seal, которая является знаком качества и безопасности любого интернет-магазина. Ее стоит

**верно только для SSL-сертификатов с зеленой адресной строкой (EV-сертификатов).*

разместить на всех страницах интернет-магазина, а также рядом с формами входа, чтобы посетитель понимал, что на данном сайте все находится под безупречной защитой.

Почему так важно установить печать доверия?

Основные преимущества установки печати доверия на сайте:

- **Пользователи видят, что Ваш сайт является безопасным, а потому вводят свои персональные данные и совершают покупки.**
- **Norton – узнаваемый бренд, который в сознании многих пользователей связан с защитным программным обеспечением. Иконка с надписью «Norton Secured» позволяет привлечь дополнительное доверие со стороны пользователей.**
- **При наведении курсора мыши на печать доверия пользователь сможет увидеть всю информацию о Вашей компании и используемых Вами средствах защиты сайта.**

Если же требуется более дешевое решение, то в таком случае можно обратить свое внимание на Thawte EV-сертификат или Sectigo (Comodo) EV-сертификат. Такой EV-сертификат позволяет добиться вывода замочка, а также наименования компании в ней. Пользователь сразу же замечает такой визуальный сигнал и понимает, что сайту можно доверять, ведь он надежно защищен.

OV SSL-сертификат (с проверкой организации) не рекомендуется для использования в интернет-магазинах. Этот тип сертификатов позволяет вывести замочек в адресной строке браузера, щелчок по которому приведет к отображению данных о компании. Однако далеко не все пользователи настолько технически подкованы, чтобы просматривать данные о компании. Поэтому они могут просто отказаться от покупок на вашем сайте.

DV SSL-сертификат позволяет получить замочек в адресной строке браузера, но не содержит данных о вашей компании. Тем самым Вы добьетесь безопасности транзакций на сайте, однако не сможете защититься от кражи данных через фишинговые сайты. Хакеры вполне могут приобрести такой же DV-сертификат и создать поддельную копию интернет-магазина, направляя пользователей к нему и получая их данные.

Именно по этим причинам мы настоятельно рекомендуем всем владельцам интернет-магазинов приобретать EV SSL-сертификат, который несет в себе многочислен-

ные маркетинговые преимущества, а также позволяет надежно защитить сайт от злоумышленников.

В этом случае посетитель сайта получает невербальный знак, говорящий о том, что сайту стоит доверять (зеленый цвет всегда ассоциируется с получением разрешения). Человек сразу видит, кому принадлежит сайт, поскольку наименование компании выводится в адресной строке браузера. Доверие посетителей к сайту растет, а потому растут и продажи. Как показывает статистика, рост продаж может составить до 10-40%.

Теперь немного математики.

Пусть продажи Вашего сайта достигают 1 млн рублей в месяц. Предположим, что прирост продаж будет равен 1% (минимальный процент). EV-сертификаты стоят от 10 тыс. рублей в год. Получаем увеличение продаж за год:

1 млн х 12 мес. х 0,01 = 120 тыс. руб.

Вычитаем затраты 10 тыс. руб.

Увеличение продаж за вычетом стоимости SSL-сертификата составит 110 тыс. руб.

Все это говорит о том, что SSL-сертификаты представляют собой очень выгодное вложение средств, которое быстро себя окупает.

Еще один важный фактор, влияющий на рост продаж - узнаваемость бренда. Как показало исследование Baymard, люди больше доверяют VeriSign (теперь DigiCert).

При использовании стандартного производителя мы имели профит в 110 тыс. рублей. Теперь давайте рассмотрим, как изменит ситуацию использование сертификата DigiCert. Начальные условия будут теми же самыми. Отличие в том, что DigiCert является более престижным и узнаваемым брендом по сравнению со многими другими центрами сертификации, и такой EV-сертификат стоит 60 тыс. рублей. При этом мы получаем большее доверие посетителей и выше вероятность того, что человек совершит заказ.

В случае с DigiCert при увеличении продаж хотя бы на 3% мы получим следующее:

1 млн х 12 мес. х 0,03 = 360 тыс. рублей.

Вычитаем затраты на сертификат – 60 тыс. рублей.

В итоге мы имеем увеличение продаж на 300 тыс. рублей.

Расчет эффективности использования EV SSL-сертификатов для интернет-магазинов

Без SSL-сертификата	
Продажи в магазине (в руб.)	1 000 000
С установленным SSL-сертификатом стандартного производителя	
Минимальная цена сертификата (руб., год)	10000
Минимальный рост продаж	1%
Рост продаж (руб.,год)	120000
Прирост продаж за вычетом цены SSL-сертификата (руб.,год)	110000
С установленным SSL-сертификатом DigiCert EV	
Минимальная цена сертификата (руб., год)	60000
Минимальный рост продаж	3%
Рост продаж (руб.,год)	360000
Прирост продаж за вычетом цены SSL-сертификата (руб.,год)	300000
Рост прибыли при переходе от стандартного производителя к DigiCert	
Прирост продаж (в руб.)	190000
Прирост продаж (в %)	172,73%

Прирост продаж при использовании EV-сертификатов DigiCert почти в 3 раза выше, чем в случае со стандартными производителями.

Именно по этой причине в Германии и США многие компании отдают свое предпочтение бренду DigiCert. В России самыми популярными сертификатами являются Thawte.

Дополнительные аргументы в пользу SSL-сертификатов:

- **Пользователи нередко считают, что сайт безопасен только в том случае, если он имеет замочек в браузерной строке.** Эта аксиома прописывается во многих учебниках и статьях, посвященных безопасности. Многие пользователи будут предвзято относиться к сайту, если они не увидят небольшого замочка или зеленой строки. Таким образом, если Вы не включите SSL для всего сайта, Вы можете потерять какой-то процент пользователей. Они попросту посчитают ваш сайт опасным и не станут ничего покупать на нем.
- **Google в августе 2014 года сообщил о том, что наличие SSL на каждой странице сайта позволяет добиться роста SEO-показателей ранжирования этих страниц в поисковой выдаче.** Сделано это было как часть общей кампании по защите интернета после некоторых крупных утечек данных. Это еще один плюс в общую копилку аргументов «за» установку SSL-сертификата.
- **Как показали исследования, процент покупок в интернет-магазинах, защищенных SSL, увеличивается примерно до 40%.** Пользователи негативно относятся к сайтам, не имеющим замочка или наименования компании в адресной строке браузера, и потому уходят к конкурентам, которые установили SSL-сертификат. Как следует из недавнего опроса пользователей, проведенного центром сертификации DigiCert, примерно 78% респондентов готовы совершать покупки онлайн, если видят замочек в строке браузера,

Заказать SSL-сертификат лучше всего в проверенной компании, такой как Лидер-Телеком. Мы являемся стратегическим партнером Sectigo (Comodo) и предлагаем SSL-сертификаты этого центра регистрации по самым выгодным ценам.

Также у нас Вы можете заказать SSL-сертификаты DigiCert, которые идеально подходят для ведения серьезного онлайн-бизнеса.

О компании ЛидерТелеком

Более 12 лет мы совершенствовали наш профессионализм и создавали репутацию. Это значит, что Вы можете доверять нашей квалификации и получить своевременный профессиональный ответ на любой вопрос.

Наши сотрудники прошли необходимое обучение и имеют подтверждающие квалификацию сертификаты. Поэтому Вы можете быть уверены, что все SSL-сертификаты будут выпущены без ошибок и вовремя. А любой сертификат, приобретенный в нашей компании, Вы сможете бесплатно протестировать в течение 14 дней.

Мы предоставляем бесплатную быструю, дружелюбную и профессиональную поддержку через e-mail и по телефону:

http://www.leaderssl.ru/
info@leaderssl.ru
8 (495) 225-2235