Какие бывают типы проверки SSL сертификатов и чем они отличаются?

Основная классификация SSL сертификатов — по типу проверки.

Сертификат предполагает, что ресурсу можно доверять. Поэтому [Certification authority](https://www.firstssl.ru/faq/general-questions/kto-zanimaetsa-vidachey) не выдают их сомнительным сайтам. Сначала они проводят верификацию домена, простую или расширенную проверку организации.

От уровня проверки зависит:

* как быстро вы получите сертификат
* как дорого он обойдётся
* насколько сайту будут доверять посетители

**Валидация домена**, DV выполняется за несколько минут. Нужно только отправить запрос и ответить на письмо от центра выдачи.

После установки DV сертификата в адресной строке появится значок замка. Пользователи будут видеть его и знать, что соединение защищено и домен не фальшивый.

**Проверка организации**, OV требует до 10 дней, копии учредительных документов фирмы, подтверждение доменного имени и номера телефона.

После установки OV сертификата в адресной строке появится значок замка. При клике по изображению или печати доверия можно прочитать информацию о компании. Посетители будут видеть это и знать, что соединение защищено и фирма реально существует.

**Расширенная проверка**, EV занимает до 14 дней. Кроме подтверждения домена и номера телефона нужно предоставить копии официальных документов компании (от свидетельства о гос. регистрации до доп. подтверждающих бумаг).

После установки EV сертификата адресная строка станет зелёной со значком замка и названием фирмы. Посетители будут видеть это и знать, что соединение защищено и деятельность компании легальна.

Сертификаты также делятся по количеству защищаемых доменов. Могут включать или нет защиту поддоменов и национальных доменов, дополнительные функции. Каждый SSL защищает передаваемые данные по протоколу HTTPS.