SSL-сертификат нужен для того, чтобы мошенники не могли перехватить личные данные, которые пользователи вводят у вас на сайте. Личные данные — это логины и пароли от аккаунтов и т.д.

Для работы SSL-протокола требуется, чтобы на сервере был установлен SSL-сертификат.

**SSL-сертификат содержит следующую информацию:**

* доменное имя, на которое оформлен SSL-сертификат;
* *юридическое лицо, которое владеет сертификатом;*
* *физическое местонахождение владельца сертификата (город, страна);*
* *срок действия сертификата;*
* реквизиты компании-поставщика SSL-сертификатa.

SSL-cертификат подтверждает, что домен принадлежит реальной компании и что его владелец вправе пользоваться секретным ключом на законных основаниях.

Сертификат для веб-сервера. Сертификат состоит из двух частей (двух ключей) – public и private. Public-часть сертификата используется для шифрования трафика от клиента к серверу в защищенном соединении; private-часть – для расшифровывания полученного от клиента зашифрованного трафика на сервере.

Для получения сертификата необходимо обратиться в компании, которые выдают SSL-сертификаты. Например, в [RU-CENTER](https://www.nic.ru/dns/service/ssl/) – крупнейший регистратор доменов и один из ведущих хостинг-провайдеров в России.

Существует возможность создать такой сертификат, не обращаясь в Центр сертификации. Подписываются такие сертификаты этим же сертификатом и называются самоподписанными (self-signed).

Технически такой сертификат не отличается от версии, подписанной доверенным центром. Разница — в подписи, заверяющей сертификат.