Различают два типа протокола передачи данных HTTP и HTTPS

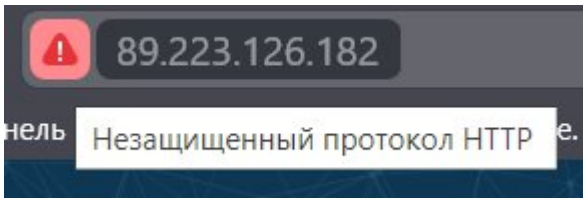
HTTP (от англ. HyperText Transfer Protocol)

Это первый протокол передачи данных, который создали для работы в интернете. У него простой алгоритм работы и основан на соединении (клиент-сервер). Обмен информацией происходит в текстовом формате, в открытом виде. Браузер запрашивает информацию у сервера и показывает контент пользователю.

протокол HTTP не обеспечивает защиту передаваемых данных — любая личная информация может быть перехвачена злоумышленниками;

HTTP работает по порту 80, а HTTPS — по порту 443;

сайты с этими протоколами по-разному отображаются в поисковых системах: так как HTTP не шифрует данные, то поисковые системы считают этот протокол небезопасным и оповещают об этом пользователя — в поисковой строке высвечивается сообщение "Не защищено" или появляется восклицательный знак в красном треугольнике.



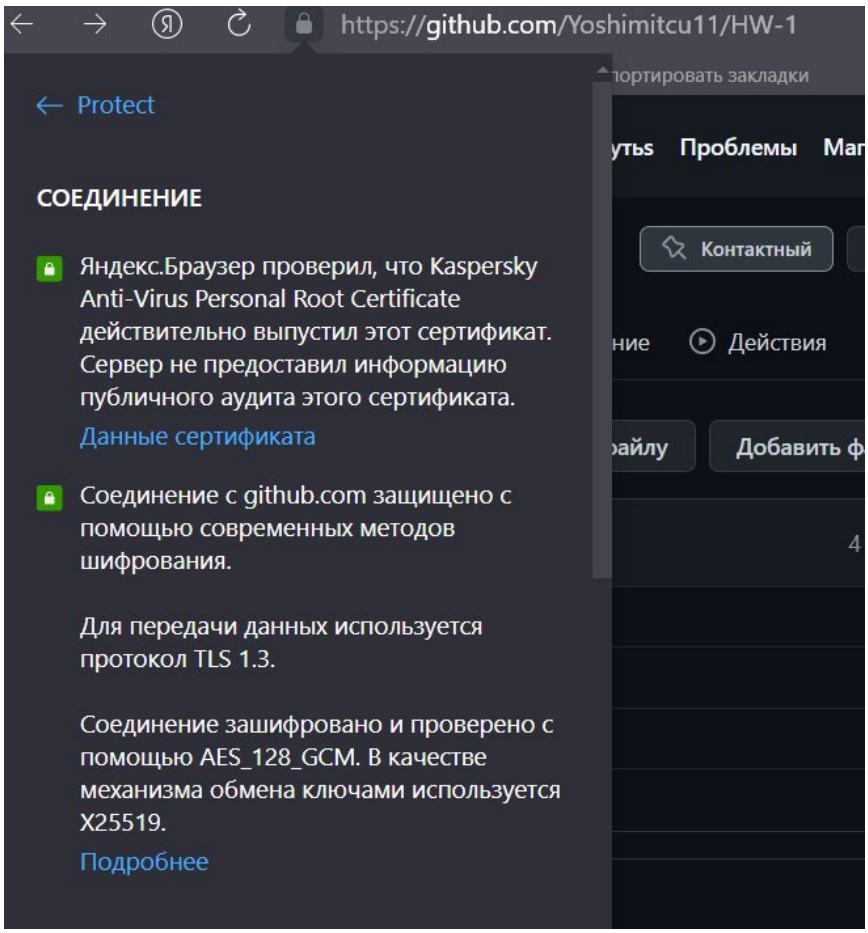
HTTPS (от англ. HyperText Transfer Protocol Secure)

Тот же самый протокол передачи данных в интернете, но уже имеющий защиту SSL – сертификатом.

Это дает несколько преимуществ
1) Безопасность – Все данные пользователя (личная информация, данные паспорта, номера карты, история браузера) находятся под защитой

2) Положительное влияние на SEO – оптимизацию.
Поисковые системы доверяют сайтам работающим по https протоколу больше, поэтому они находятся выше в списке выдачи поискового запроса.

3) Пользователи выбирают защищенные сайты, потому что не хотят, чтобы их личная информация попала к третьим лицам. Поэтому компания, которая пользуется защищенным протоколом передачи информации на своем сайте – Вызывает доверие у посетителей.



Стоит уделить внимание и самому понятию SSl – сертификата.
SSL — Secure Socket Layer, уровень защищенных сокетов.

SSL является более ранней системой, разработанной компанией Netscape Communications для добавления протокола HTTPS в свой веб-браузер Netscape Navigator.

Протокол SSL обеспечивает защищенный обмен данными за счет двух следующих элементов:

1) Аутентификация
2) Шифрование

SSL использует асимметричную криптографию для аутентификации ключей обмена, симметричный шифр для сохранения конфиденциальности, коды аутентификации сообщений для целостности сообщений.

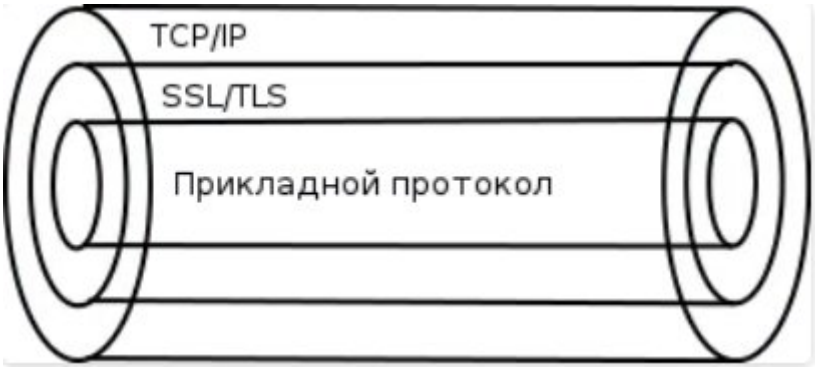
Протокол SSL предоставляет «безопасный канал», который имеет три основных свойства:

1) Канал является частным. Шифрование используется для всех сообщений после простого диалога, который служит для определения секретного ключа.
2) Канал аутентифицирован. Серверная сторона диалога всегда аутентифицируется, а клиентская делает это опционально.
3) Канал надежен. Транспортировка сообщений включает в себя проверку целостности.

Не забудем и про то, что протоколы развивались и дорабатывались и имеют несколько версий.

SSL 1.0 — никогда не публиковался
SSL 2.0 — февраль 1995 года
SSL 3.0 — 1996 год
TLS 1.0 — январь 1999 года
TLS 1.1 — апрель 2006 года
TLS 1.2 — август 2008 года
TLS 1.3 – август 2018 года
Не будем вдаваться в подробности различий версий протоколов, запомним лишь то, что протокол TSL - (Transport Layer Security, безопасность транспортного уровня) был основан на спецификации SSL 3.0 , которая в дальнейшем не получала новых версий.

Схема принципа работы SSL/TSL



Прикладной протокол «заворачивается» в TLS/SSL, а тот в свою очередь в TCP/IP. По сути данные по прикладному протоколу передаются по TCP/IP, но они зашифрованы. И расшифровать передаваемые данные может только та машина, которая установила соединения. Для всех остальных, кто получит передаваемые пакеты, эта информация будет бессмысленной, если они не смогут ее расшифровать.

И вот как происходит соединение Киента с Сервером