# Hypertext transfer protocol secure
**Cherkasov D.[1], Ivanov V.[2], Lubova E.[3] (Russian Federation)**

# Безопасный протокол передачи гипертекста
**Черкасов Д. Ю.[1], Иванов В. В.[2], Лубова Е. С.[3] (Российская Федерация)**

*[1]Черкасов Денис Юрьевич / Cherkasov Denis - студент;*
*[2]Иванов Вадим Вадимович / Ivanov Vadim – студент;*
*[3]Лубова Елена Сергеевна / Lubova Elena – студент,*
*кафедра компьютерной и информационной безопасности,*
*Институт кибернетики*
*Московский институт радиотехники электроники и автоматики*
*Федеральное государственное бюджетное образовательное учреждение высшего образования*
*Московский технологический университет, г. Москва*

***Аннотация:*** *https – это протокол, позволяющий добиться обеспечения конфиденциального и безопасного обмена информацией между сайтом и клиентом. Таким образом, он защищает данные, указанные пользователем для того, чтобы совершить покупку или подписаться на обновления. HTTPS нужен, чтобы предотвратить попадание подобной информации в руки мошенников.*
***Abstract:*** *https is a protocol which allows you to achieve the privacy and security of information exchange between the site and the client. Thus, it protects the data specified by the user to make a purchase or sign up for updates. HTTPS is needed to prevent the obtaining of such information in the hands of criminals.*

***Ключевые слова:*** *https, протокол, шифрование, безопасный, данные.*
***Keywords:*** *https, protocol, encryption, secure, data.*

HTTP (HyperText Transfer Protocol) расшифровывается как протокол передачи гипертекста. Также можно сказать, что HTTP является протоколом клиент-сервера, с помощью которого две машины взаимодействуют друг с другом, используя надежный ориентированный на установление соединений транспортный сервис. HTTP может быть реализован поверх любого другого протокола в Интернете или других сетях и предполагает использование только надежной транспортировки. Может быть использован любой протокол, который предоставляет такие гарантии.

HTTP не фиксирует данные. Время соединения меняется в зависимости от того, как быстро приходит ответ на запрос. Сервер обрабатывает каждый запрос заново, поскольку не сохраняет данные о предыдущих заявках. Страницы HTTP хранятся на Вашем компьютере или в кэше. Они загружаются достаточно быстро, однако нужно понимать, что они хранятся в системах, которые Вы не можете контролировать. HTTP использует такие сервера как Apache HTTP, Microsoft IIS, Jigsaw, Zope и т. д.

**Преимущество HTTP.**

Самым главным достоинством данного протокола является независимая платформа, с помощью которой можно осуществить прямой кросс-платформенный перенос. Нет необходимости в том, чтобы контролировать работу HTTP, что позволяет Брандмауэрам его использовать. Глобальные приложения не ориентированы на соединение, поэтому нет никакой необходимости в том, чтобы создавать и поддерживать сеанс для обмена информацией.

**Недостатки HTTP.**

Возникают некоторые проблемы с осуществлением безопасности. В HTTP отсутствует понятие конфиденциальности как таковой – каждый может увидеть ваш контент. Не менее важен тот факт, что в представленную информацию можно с легкостью внести изменения. HTTP ненадежен, поскольку для него отсутствуют какие-либо методы шифрования. Таким образом, может получиться так, что третий человек получит доступ к конфиденциальной информации. Нет никакой аутентификации, поэтому у Вас не будет четкого представления о том, с кем Вы общаетесь. Можно сказать, что аутентификация представлена открытым текстом (в незашифрованном виде), поэтому практически любой человек может перехватить запрос и узнать, какой логин и пароль использует пользователь.

**HTTPS или Безопасный HTTP.**

HTTPS – это комбинация Протокола передачи гипертекста (HTTP) с протоколом SSL/TLS. Теперь все, что Вы передаете по HTTPS, будет отправлено и получено в зашифрованном виде, который добавит элемент безопасности. Когда клиент выполняет запрос, сервер отвечает, предлагая список методов шифрования. В процессе соединения с веб-сайтом посредством HTTPS, веб-сайт шифрует сеанс цифровым сертификатом. Уровень защищенных сокетов или SSL использует криптографическую систему, шифрующую данные двумя ключами, которые являются уникальными кодами, которыми обмениваются браузер и сервер.

HTTPS используется достаточно часто в таких ситуациях, как: вход в банковскую систему, заполнение документов, корпоративных входов в систему и других приложений, в которых данные должны быть защищены. Рекомендуется никогда не вводить данные кредитной карты на веб-сайтах, которые используют HTTP.

**Достоинства и недостатки HTTPS:**

Недостатки:

- сертификат, который нужно оплачивать каждый год (стоимость около $20);
- низкая скорость работы сервера, поскольку часть его ресурсов будет тратиться на шифрование передаваемых данных.

Достоинства:

- пресечение хакерских атак, которые основываются на прослушивании сетевого соединения;
- возрастающее доверие клиентов;
- потенциальное положительное влияние на ранжирование страниц сайта в поисковых системах засчет учета наличия защищенного соединения как фактора ранжирования, а также положительного влияния на поведенческие факторы ранжирования.

**Что такое SSL, TLS и HTTPS?**

SSL расшифровывается как Secure Sockets Layer (уровень защищенных сокетов). Это стандартная технология для обеспечения безопасного интернет-соединения и для защиты любых данных, которыми обмениваются две системы. Это не позволяет преступникам читать и изменять переданную информацию, включая какие-либо персональные данные. Этими двумя системами могут быть сервер и клиент (например, веб-сайт покупок и браузер) или два сервера (например, приложение с персональной идентифицируемой информацией или с информацией о платежной ведомости).

Это делается для того, чтобы данные, переданные между пользователями и сайтами, или между двумя системами, было невозможно прочитать. SSL использует алгоритмы шифрования, чтобы скремблировать данные в пути, что не позволяет хакерам получить доступ к информации, переданной по сети. В этих данных может содержаться личная информация, в том числе включающая в себя номера кредитной карточки и другую финансовую информацию, имена и адреса [1].

Transport Layer Security (TLS) является протоколом, обеспечивающим конфиденциальность и целостность передаваемых данных между двумя взаимодействующими приложениями. Это самый актуальный протокол безопасности на данный момент. Он используется для веб-браузеров и других приложений, которые требуют надежной передачи данных по сети. TLS был основан на SSL и изначально использовался исключительно для повышения безопасности электронной коммерции в Интернете.

Основными различиями между SSL и TLS, которые делают TLS более безопасным и эффективным протоколом аутентификации сообщений, являются новые алгоритмы генерации ключей шифрования. TLS и SSL не совместимы.

Протокол TLS предоставляет три услуги всем приложениям, которые работают над ним:

- шифрование;
- аутентификация;
- целостность.

Могут использоваться не все три сразу, однако для обеспечения безопасности, в основном, используются вместе.

Шифрование – сокрытие информации, передаваемой от одного компьютера к другому;

Аутентификация – проверка авторства передаваемой информации;

Целостность – обнаружение подмены информации подделкой.

HTTPS (Безопасный Протокол передачи гипертекста) появляется в URL, когда веб-сайт защищен сертификатом SSL. Детали сертификата, включая подробности об издании и название компании владельца веб-сайта, можно посмотреть, нажав на символ безопасности в адресной строке браузера.

Для компаний представляющих услуги онлайн или веб-сайтов, принимающих платежи по кредитным или дебетовым картам или включающих передачу персональных данных или личной информации, такой как имена и адреса, сертификат SSL необходим для обеспечения безопасности веб-сайта. Это один из важных способов, позволяющих удостовериться в том, что сайты безопасны и клиенты защищены, но это также кардинально влияет на безопасность сайтов.

Сертификат SSL устанавливается на сервере, но в браузере можно заметить индикаторы, позволяющие пользователям понять, что протокол активирован. Во-первых, если сайт будет защищен SSL, пользователи увидят https://в начале веб-адреса, а не http:// (дополнительная «s» обозначает «безопасный»). Безопасное соединение может быть обозначено значком замка или зеленым сигналом строки поиска.

**Аутентификация уровней.**

В качестве вступления хочется написать о том, что Центры сертификации (CA – Certification authority) могут также аутентифицировать идентификационные данные владельца веб-сайта, добавляя еще один уровень безопасности. Сертификат SSL тогда используется в качестве доказательства идентификационных данных компании. Сертификаты могут быть разделены на три группы аутентификации:

1) Доменные сертификаты SSL. Требуется, чтобы компании доказали свое владение доменным именем. Сертификат содержит доменное имя, предоставленное в Центре сертификации как часть запроса. Поскольку идентификационные данные организации не были проверены здесь, данный уровень является базовым уровнем сертификации SSL. Он подходит только для тестовых серверов и внутренних ссылок.

2) Сертификаты SSL Проверки допустимости организации. Здесь необходимо, чтобы претендент не только доказал, что он владеет доменным именем, которое хочет защитить, но также доказал, что его компания зарегистрирована. Выданный сертификат является доказательством домена и названия компании. Этот уровень аутентификации подходит для сайтов, которые собирают личные данные пользователей сайта. Обратите внимание, что один человек не может получить такие сертификаты. Это доступно только организациям и предприятиям.

3) Расширенные сертификаты SSL Проверки допустимости. Эти сертификаты помогают защитить пользователей от предоставления их личной информации на поддельных веб-сайтах, которые могут быть использованы преступниками. Расширенные сертификаты SSL проверки допустимости требует двух вышеуказанных проверок для домена и компании, а также необходимости выполнить несколько дополнительных этапов проверки, которые связаны с доказательством того, что сертификат SSL принадлежит зарегистрированной компании. Эта дополнительная информация о компании затем представляется в выданном сертификате в адресной строке и может быть доступна для просмотра из многих веб-браузеров, если Вы нажмете на значок замка. При посещении сайта с расширенным сертификатом SSL многие браузеры высвечивают зеленую адресную строку в качестве высшего знака доверия к веб-сайту. Этот тип сертификатов также доступен только организациям и предприятиям.

**Как работает сертификат SSL?**

Основной принцип заключается в том, что когда Вы устанавливаете сертификат SSL на своем сервере, и браузер подключается к нему, наличие сертификата SSL инициирует SSL (или TLS) протокол, который будет шифровать информацию.

SSL работает непосредственно поверх протокола управления передачей (TCP), эффективно выполняя роль слоя безопасности. Это позволяет более высоким протокольным уровням оставаться неизменными, при том, что они все еще будут обеспечивать безопасное соединение. Таким образом, под уровнем SSL, другие протокольные уровни в состоянии функционировать без изменений.

Если сертификат SSL используется правильно, злоумышленник сможет увидеть, какие IP-адреса и порты подключены, также – примерное количество отправленных данных. Хакер может разорвать соединение, но и сервер, и пользователь узнают, что это было сделано третьей стороной. Тем не менее, он не сможет перехватить какую-либо информацию [2].

Хакер может выяснить, к какому хосту подключается пользователь, но не сможет вычислить остальную часть URL. Поскольку соединение зашифровано, важная информация остается в безопасности.

1. SSL начинает работать после того, как соединение по протоколу TCP установлено, инициируя то, что называют квитированием (подтверждение приёма-передачи структурной единицы информации) SSL.

2. Сервер отправляет свой сертификат пользователю вместе со многими уточнениями (включая подробности о версии SSL/TLS и методах шифрования).

3. После этого пользователь проверяет сертификат и выбирает высший уровень шифрования, который может поддерживаться обеими сторонами, и запускает безопасный сеанс. Существует большое количество различных методов – шифров – которые применяются в зависимости от ситуации.

4. Чтобы гарантировать целостность и подлинность всех переданных сообщений, протоколы SSL и TLS также включают процесс аутентификации, используя коды аутентификации сообщений (MAC).

**Серверы.**

Благодаря способу работы SSL, серверам не нужно иметь встроенные корневые сертификаты, но необходимо установить соответствующий промежуточный сертификат(ы). До тех пор, пока сертификат установлен правильно, он может поддерживаться любым сервером.

Приборы и операционные системы

Операционные системы для компьютеров, планшетов и мобильных телефонов поддерживаются. Тем не менее, в случае мобильных телефонов может получиться так, что некоторые старые устройства не будут поддерживать новую версию SSL или TLS протоколов, так что стоит изучить этот вопрос, прежде, чем устанавливать сертификаты.

**Как реализовать сертификат SSL на сайте.**

В зависимости от того, как и где был размещен сайт, существуют различные способы добавления сертификата SSL. Если на сайте присутствует элемент электронной коммерции, необходимо будет получить сертификат. Крупные хостинг провайдеры часто предлагают хостинг пакеты, включающие SSL сертификаты.

Также возможно перенести существующий SSL протокол с другого хоста (экспортируя его из исходного сервера и импортируя на новый). Для этого нужно будет следовать инструкциям на интересующем Вас сайте. Обратите внимание на тот факт, что некоторые Центры сертификации требуют получить лицензию на каждый сервер, где будет размещен сертификат.

Поскольку с использованием HTTPS весь трафик становится зашифрованным, то у злоумышленников уменьшается возможность перехватить данные пользователя (украсть идентификационные cookie; узнать, чем вы занимаетесь; видеть, что вы набираете на клавиатуре).

### *Литература*


1. *Walls Colin.* Embedded Software: The Works. United States of America: Elsevier, 2005. 391 c.
2. *Joris Claessens.* Computer Security and Industrial Cryptography. Belgium: Leuven - Heverlee, 2002. 287 c.