УДК 004.056.55

ПРОТОКОЛ HTTPS

Андрей Алексеевич Хохлов
студент
garlic142@gmail.com
Лариса Ивановна Никонорова
кандидат сельскохозяйственных наук, доцент
lenaniknrva@rambler.ru
Мичуринский государственный аграрный университет
г. Мичуринск, Россия

Аннотация. В статье проведен сравнительный анализ протоколов шифрования HTTP и HTTPS, дана характеристика протоколов, а также рассмотрены сертификаты шифрования SSL и TLS.

Ключевые слова: протокол, конфиденциальность, защита, шифрование, сертификат, безопасность, браузер.

Современный мир сложно представить без интернета. Любая передаваемая информация несет в себе определенную ценность и конфиденциальность. Протокол шифрования HyperTextTransferProtocolSecure (сокращенно HTTP) использовался в качестве передачи информации, гипертекста (текста с перекрестными ссылками). В основном протокол использовался для передачи данных, по типу картинок, фотографий и прочего, от клиентского браузера к серверу по принципу «запрос-ответ». При такой работе злоумышленник мог вмешаться в передачу информации, перехватить ее и перенаправить пользователя на другой сайт, либо изменить информацию [1]. Эта уязвимость поставила миллионы людей перед риском потери конфиденциальных данных.

Основными опасностями, связанными с протоколом HTTP являются:

Уязвимость для MITM-атак (Man in the Middle - «человек посередине») атака посредника. В условиях этой атаки третье лицо может вмешаться в подключение, получить доступ к паролям, личным данных, конфиденциальной информации и банковским счетам, совершать кражу информации и заражать устройство сторонним программным обеспечением и прочими вирусами.

Отсутствие шифрования. Протокол HTTP не использует шифрование данных, а значит, что любая информация может попасть в руки злоумышленников. Особенно это касается бесплатных открытых Wi-Fi сетей, где риск незащищённости данных крайне высок.

На данный момент большинство браузеров используют протокол HTTPS, но при использовании его менее защищенной версии HTTP браузеры будут предупреждать пользователя, что подключение не защищено и дальнейшие действия пользователь совершает на своих страх и риск.

Браузеры используют рейтинг SEO, чтобы исключать из поиска или показывать результаты сайтов в самый последний момент, если они используют протокол HTTP.

Все это показывает, что протокол HTTP имеет низкую репутацию, среди современных браузеров и ведет к неоправданному риску потери личной информации [1].

Новая версия протокол HTTP\2 стала этапом эволюции протокола HTTP. Протокол HTTP\2 был разработан в 2015 году и основными улучшениями его стали увеличение скорости загрузки веб-страниц и улучшении общей эффективности. Протокол HTTP\2 не получил обширного распространения.

Сравнительный анализ двух протоколов (таблица 1).

Таблица 1

Сравнение протоколов HTTP и HTTP\2.

Показатель	**HTTP**	**HTTP\2**
Вид передачи данных	Основа это текст, который более понятен человеку, чем машине.	Он построен на принципе двоичной системы (бинарный код). Это позволяет увеличить эффективность и защищать протокол от ошибок.
Сжатие заголовков	Заголовки передаются без сжатия. Объём данных увеличен.	Заголовки сжимаются, используя алгоритм HPACK. Данные занимают меньше объема и быстрее передаются.
Push сервер	Не поддерживается. Ответы на запросы пользователя без интуитивного угадывания предпочтений пользователя.	Поддерживает. Не только отвечает на запросы клиента, но и сам предлагает ресурсы на основе его потребности.
Сертификаты	Работает только поверх HTTPS. Не обязательно использовать сертификаты SSL и TLS	Работает на основе HTTPS. Требования к безопасности выше.
Запросы по приоритету	Не поддерживает. Все	Поддерживает. Запросы

	запросы обрабатываются по порядку.	могут быть расположены в порядке приоритета, если того требует клиент.
Затраты интернет ресурсов	Малоэффективен, так как задействует множество параллельных запросов.	Более эффективная модель. Использует метод мультиплексирования и сжатия заголовков.

Новой версией HTTP стал протокол HTTPS. На сегодняшний день он используется большинством сайтов.

Протокол HTTPS (HyperTextTransferProtocolSecure) представляет собой расширенную версию HTTP, он использует шифрование и является приоритетным протоколом в современных браузерах.

Отличительной чертой протокола является использование шифрования, с применением сертификатов SSL и TLS. Это обеспечивает обезопасить клиентов от получения информации третьими лицами. Сайты, которые используют протокол HTTPS, в адресной строке браузера обозначаются началом URL «https://» или значком замка, что является аналогией вышеупомянутой адресной строке. При отсутствии шифрования возникает надпись, что подключение не защищено или перечеркнутый красный замок.

Протокол защищает передаваемую информацию, блокируя перехват, прослушивание или изменение данных в процессе отправки, тем самым предотвращая утечку конфиденциальной информации. Особое место HTTPS занимает при передаче финансовой или кредитной информации, информации связанной с паспортами. Сегодня все официальные сайты используют протокол HTTPS в качестве обеспечения безопасности пользователей и повышения доверии у клиентов [3].

Сравним протоколы HTTP и HTTPS.

Таблица 2

Сравнение протоколов HTTP и HTTPS.

Показатель	HTTP	HTTPS

Безопасность	Шифрование отсутствует. Данные передаются в виде текста. Высокая уязвимость.	Данные шифруются с помощью протоколов. Высокая степень защиты.
Используемые порты	80	443
Скорость соединения	Быстрая	Более медленная, из-за протоколов шифрования
Конфиденциальность	Данные смогут быть перехвачены и прочитаны.	Защита данных от перехвата за счет шифрования
Аутентификация	Отсутствует	Использование сертификатов SSL\TLS для аутентификации сервера
Целостность передаваемых данных	Высокий шанс перехвата данных и их изменений	Шифрование обеспечивает полную защиту от прочтения и изменения данных в процессе передачи
Требования к инфраструктуре	Нет требований	Требования наличия платного сертификата SSL\TLS
SEO-влияние	Плохое отображение в рейтинге сайтов. Предпочтение браузерами более безопасных сайтов	Хорошее отображение в рейтинге сайтов, так как протокол шифрования HTTPS является важным фактором для ранжирования.
Применение	Подходит для сайтов, которые не используют важную информацию	Применим для любых сайтов иособенно для сайтов с обработкой важной информации

Сертификаты SSL (SecureSocketsLayer) и TLS (TransportLayerSecurity) используются для создания зашифрованного канала между пользователем и сервером [3].

Сайты не обязаны иметь сертификат шифрования, но для большего доверия пользователей сети, владельцы сайтов должны приобретать сертификаты шифрования и переходить на защищенную систему HTTPS, несмотря на дополнительные расходы.

Список литературы:

1. Васильева И.Н. Криптографические методы защиты информации. М.: Юрайт. 2024. С. 350.
2. Романьков В. А. Введение в криптографию. М.: Форум. 2023. С. 240.
3. Что такое протокол HTTPS и принципы его работы. / Рег.ру – URL: https://help.reg.ru/support/ssl-sertifikaty/obshchaya-informatsiya-po-ssl/chto-takoye-protokol-https-i-printsipy-yego-raboty#0
4. Бабаш А. В., Баранова Е. К., Ларин Д. А. Информационная безопасность. История защиты информации в России. М.: КДУ. 2017. С. 736.

UDC 004.056.55

HTTPS PROTOCOL

Andrey Al. Khokhlov
student
garlic142@gmail.com
Larisa Iv. Nikonorova
candidate of agricultural sciences, associate professor
lenaniknrva@rambler.ru
Michurinsk State Agrarian University
Michurinsk, Russia

Abstract. The article provides a comparative analysis of HTTP and HTTPS encryption protocols, describes the protocols, and examines SSL and TLS encryption certificates.

Keywords: protocol, confidentiality, protection, encryption, certificate, security, browser.

Статья поступила в редакцию 11.11.2024; одобрена после рецензирования 20.12.2024; принята к публикации 25.12.2024.

The article was submitted 11.11.2024; approved after reviewing 20.12.2024; accepted for publication 25.12.2024.