УДК 303.7
Марічев Д.О.[1], Зайко Т.А.[2]
[1]студ. гр. КНТ-117 НУ «Запорізька Політехніка»
[2] канд. техн. наук, доц. НУ «Запорізька Політехніка»

ПРИНЦИП РОБОТИ SSL СЕРТИФІКАТУ ШИФРУВАННЯ В HTTPS ПРОТОКОЛІ

При створенні програмного забезпечення (ПЗ), а саме веб-сайтів, розробники стикаються з проблемою незахищеності даних при їх передачі від клієнту до серверу та навпаки. Через це під час передачі є ймовірність перехоплення та змінення цінної інформації шахраями. Обов'язкове шифрування вимагає вся інформація, що стосується проведення платежів в інтернеті: оплата товарів в інтернет-магазинах будь-яким способом, оплата послуг через інтернет-банкінг, виконання платежів в онлайн сервісах і багато іншого [1].

Для вирішення проблеми перехоплення цінної інформації все більше сайтів переходять на захищений протокол HTTPS. У протоколі безпеки HTTPS використовується асиметрична схема шифрування за рахунок використання SSL сертифікату шифрування – завдяки цьому всі дані надійно захищені від перехоплення.

В основі будь-якого методу шифрування лежить ключ. Ключ – це спосіб зашифрувати або розшифрувати повідомлення. В роботі SSL сертифіката беруть участь три ключі: публічний, приватний і сеансовий.

Публічний ключ зашифровує повідомлення. Браузер використовує його,

коли потрібно відправити призначені для користувача дані серверу. Наприклад, після того як було введено дані банківської картки і натиснуто «Оплатити». Цей ключ видно всім, браузер прикріплює його до повідомлення.

Приватний ключ розшифровує повідомлення. Його використовує сервер, коли отримує повідомлення від браузера. Цей ключ зберігається на сервері і ніколи не передається разом з повідомленням.

Сеансовий ключ одночасно зашифровує і розшифровує повідомлення. Браузер генерує його на час, який користувач проводить на сайті. Варто користувачеві закрити вкладку, сеанс закінчиться і ключ перестане працювати.

Шифрування з двома різними ключами називають асиметричним. Використовувати такий метод більш безпечно, але повільно. Тому браузер і сервер використовують його один раз: щоб створити сеансовий ключ.

Шифрування з одним ключем називають симетричним. Цей метод зручний, але не такий безпечний. Тому браузер і робить унікальний ключ для кожного сеансу замість того, щоб зберігати його на сервері.

Браузер і сервер встановлюють SSL з'єднання кожного разу, коли користувач заходить на сайт. Це займає кілька секунд під час завантаження сайту.

Коли вводять адресу сайту в браузері – він запитує у сервера, встановлений для сайту сертифікат. У відповідь сервер відправляє загальну інформацію про SSL сертифікат і публічний ключ. Браузер звіряє інформацію зі списком авторизованих центрів сертифікації. Такий список є у всіх популярних браузерах. Якщо все в порядку, браузер генерує сеансовий ключ, зашифровує його публічним ключем і відправляє на сервер. Сервер розшифровує повідомлення і зберігає сеансовий ключ. Після цього між браузером і сайтом встановлюється безпечне з'єднання через протокол HTTPS [2].

Всі сучасні браузери підтримують захищений протокол HTTPS. І все більше сайтів переходять на його використання – особливо після того, як компанія Google оголосила використання зашифрованого протоколу фактором ранжирування при видачі результатів пошуку.

З січня 2017 року компанія Google почала позначати сайти, які не працюють за HTTPS протоколі як ненадійні. Це означає, що в браузері Google Chrome з’явиться відмітка для сайтів без SSL сертифіката. Якщо на сайті є контактні форми, але немає сертифіката або він встановлений з помилкою – поруч з адресою сторінки з’явиться слово «ненадійних». На усіх сайтах, де встановлений SSL сертифікат, відображається слово «Надійний» [3].

У квітні 2019 року стало відомо про те, що 20% найбільших в світі

сайтів не використовують протокол HTTPS з підтримкою шифрування, незважаючи на обмеження, з якими вони стикаються у зв'язку з цим.

За даними компанії Google, 79 зі 100 найбільш популярних веб-ресурсів, які не пов'язані з компанією, не використовують сертифікат для захищених HTTPS з'єднань. Таку безпеку ігнорують, зокрема, найбільша в світі база даних і інтернет-портал про кінематограф IMDB і газета The New York Times [4].

Таким чином, можна зробити висновок, що використання HTTPS протоколу є майже необхідним у сучасних реаліях, так як він дозволяє захищати персональні дані користувачів від перехоплення та змінення шахраями; допомагає просуванню сайту у ранжуванні в пошуковій видачі.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Що таке HTTPS та для чого його використовувати: [Електрон. ресурс]. – Режим доступу: https://www.kasper.by/blog/chto-takoe-https-i-dlya-chego-ego-ispolzovat/

2. Як працює SSL сертифікат: [Електрон. ресурс]. – Режим доступу: https://ssl.com.ua/info/how-ssl-works/

3. Google: як SSL сертифікат впливає на SEO: [Електрон. ресурс]. – Режим доступу: https://ssl.com.ua/info/ssl-and-google-seo/

4. Переваги HTTPS над HTTP: [Електрон. ресурс]. – Режим доступу: http://www.tadviser.ru/index.php/Статья:HTTP_-_HTTPS