УДК 004.056.5

HTTPS ПРОТИ HTTP: ЧОМУ ВАЖЛИВА БЕЗПЕКА ПЕРЕДАЧІ ДАНИХ

К. Горбенко, група КН-23
Науковий керівник: ***В. Резніченко,*** викладач
Центральноукраїнський національний технічний університет

В сучасному цифровому світі безпека передачі даних є критично важливою. Зростання кіберзагроз робить необхідним перехід від HTTP до HTTPS. Метою даного дослідження є аналіз переваг HTTPS над HTTP у контексті захисту даних користувачів в Інтернеті. Дослідження демонструє, що HTTPS забезпечує шифрування даних, автентифікацію сайту та цілісність передачі інформації, що значно підвищує безпеку.

HTTP (HyperText Transfer Protocol) є протоколом прикладного рівня, розробленим для передачі гіпертекстових документів, таких як HTML, між клієнтом (наприклад, веб-браузером) і сервером [1]. Основний принцип його роботи полягає у взаємодії за схемою запит-відповідь: клієнт надсилає запит до сервера, а сервер повертає відповідь з потрібним ресурсом або повідомленням про стан. HTTP є безстанним протоколом, тобто кожен запит опрацьовується самостійно, без збереження інформації про попередні сесії. Це спрощує архітектуру HTTP, проте для реалізації сесій або збереження стану користувача можуть бути потрібні додаткові механізми.

Протокол HTTP підтримує різноманітні методи запитів: GET – для отримання ресурсів, POST – для передачі даних на сервер, PUT – для оновлення ресурсів і DELETE – для їх вилучення [2]. Кожен HTTP-запит містить набір заголовків, які надають важливу додаткову інформацію, зокрема визначають тип вмісту, який передається, а також механізм кодування чи стиснення, що використовуються для ефективної передачі даних. У відповідях серверів, у свою чергу, також присутні заголовки, які інформують про стан запиту, включаючи статус код, час відповіді, тип переданого вмісту і додаткові параметри, що стосуються конфігурації з’єднання.

HTTPS (HyperText Transfer Protocol Secure) є розширенням протоколу HTTP, яке забезпечує безпечну передачу даних між клієнтом (наприклад, веб-браузером) і сервером. Подібно до HTTP, HTTPS діє за принципом запит-відповідь, але доповнює його рівнем шифрування, що захищає інформацію від перехоплення та маніпуляцій. Оскільки HTTPS працює через порт 443, він обов'язково вимагає наявність SSL/TLS-сертифіката, який є критичним елементом для підтвердження автентичності веб-сайту [1]. Цей сертифікат підтверджує, що сайт дійсно є тим, за кого він себе видає, і забезпечує довіру користувачів до його безпеки [5].

Процес встановлення HTTPS-з'єднання складається з кількох етапів. Спочатку клієнт надсилає запит на сервер для встановлення безпечного з'єднання. У відповідь сервер надсилає свій SSL/TLS-сертифікат, що містить відкритий ключ та інформацію про сервер [2]. Клієнт перевіряє дійсність сертифіката, переконуючись у його надійності та відповідності доменному імені сервера. По успішній перевірці клієнт і сервер узгоджують сеансовий ключ через асиметричне шифрування. Клієнт генерує симетричний ключ, шифрує його відкритим ключем сервера та надсилає назад, а сервер розшифровує його своїм приватним ключем. Після обміну ключами сторони використовують сеансовий ключ для шифрування та дешифрування даних протягом сеансу, забезпечуючи конфіденційність і цілісність переданої інформації [1].

Поглиблене розуміння принципів роботи HTTPS та HTTP дозволяє більш точно оцінити їхні переваги та недоліки, особливо в контексті сучасних вимог до безпеки в Інтернеті.

Для більш чіткого розуміння, чому HTTPS є надійнішим вибором для безпеки в Інтернеті, доцільно порівняти ключові характеристики цього протоколу з HTTP. HTTPS значно перевершує HTTP у плані безпеки, оскільки використовує криптографічні протоколи SSL/TLS, що забезпечують як шифрування, так і цілісність переданої інформації, запобігаючи

зчитуванню або підробці даних зловмисниками [3]. HTTP, у свою чергу, передає дані відкрито, що робить їх вразливими до атак. Крім того, HTTPS гарантує автентичність сайту завдяки сертифікатам, підписаним довіреними центрами сертифікації, тоді як HTTP не має механізму перевірки справжності ресурсу. З точки зору правового регулювання, використання HTTPS є важливою умовою відповідності сучасним вимогам щодо захисту персональних даних, зокрема в межах регламенту GDPR в Європейському Союзі. Користувачі також більше довіряють сайтам з HTTPS, що підтверджується візуальними індикаторами в браузері – такими як значок замка – та відсутністю попереджень [4]. Технічно, хоча HTTP може бути трохи швидшим за рахунок відсутності шифрування, лише HTTPS дозволяє використовувати новітні веб-технології, такі як HTTP/2, які компенсують початкові втрати продуктивності та покращують загальну швидкість і ефективність взаємодії. Крім того, провідні браузери все частіше обмежують підтримку HTTP, стимулюючи повний перехід на безпечний протокол.

Порівняймо протоколи HTTP та HTTPS, визначимо ключові відмінності між ними та чітко розкриємо їх вплив на безпеку та ефективність веб-ресурсів.

Таблиця 1. Порівняння ключових характеристик HTTP та HTTPS

Характеристика	HTTP	HTTPS
Безпека передачі даних	Дані передаються у відкритому вигляді, можуть бути перехоплені третіми особами.	Дані шифруються за допомогою SSL/TLS, що унеможливлює перехоплення або зміну інформації.
Автентифікація	Відсутня. Немає способу перевірити справжність сервера, що створює ризик атак MITM.	Сертифікат SSL/TLS підтверджує, що сайт є справжнім, зменшуючи ризик підробки.
Довіра користувачів	Браузери можуть попереджати про небезпеку, знижуючи довіру до ресурсу.	Значок замка в адресному рядку підвищує довіру, користувачі більш охоче взаємодіють із сайтом.
Пошукова оптимізація (SEO)	Сайти на HTTP можуть мати нижчі позиції в пошуковій видачі.	HTTPS сайти отримують перевагу в ранжуванні від Google та інших пошукових систем.
Використовуваний порт	Порт 80, стандартний для незахищеного HTTP-з'єднання.	Порт 443, спеціально зарезервований для зашифрованого HTTPS-трафіку.
Продуктивність	Швидше, оскільки не виконується шифрування.	Незначне зниження швидкості через шифрування, однак сучасні сервери це компенсують.

Отже, порівняльний аналіз дозволяє чітко визначити ключові переваги HTTPS над HTTP. HTTPS забезпечує не лише шифрування даних і автентифікацію, а й сприяє підвищенню довіри користувачів та кращій видимості веб-ресурсу в пошукових системах. У сучасному цифровому середовищі, де питання захисту інформації є першочерговими, використання HTTPS перетворюється з рекомендації на необхідність. Таким чином, впровадження HTTPS є важливим кроком до створення безпечного, надійного та конкурентоспроможного веб-простору.

Список літератури

1. Rud A. Що таке HTTPs: у чому відмінність від http, навіщо потрібний? | Блог HyperHost.UA. HyperHost. URL: https://hyperhost.ua/info/uk/shho-take-https-u-comu-vidminnist-vid-http-navishho-potribnii (дата звернення: 14.05.2025).
2. HTTP и HTTPS – разница между протоколами передачи – AWS. Amazon Web Services, Inc. URL: https://aws.amazon.com/ru/compare/the-difference-between-https-and-http/ (дата звернення: 14.05.2025).
3. Why is HTTP not secure? | HTTP vs. HTTPS. Cloudflare. URL: https://www.cloudflare.com/learning/ssl/why-is-http-not-secure/ (дата звернення: 14.05.2025).
4. Difference between HTTP and HTTPS. Gist. URL: https://gist.github.com/git2thehub/0275a71942590c98a34a85b8664960ce (дата звернення: 14.05.2025).
5. The importance of HTTPS protocol | Dominio. GAL. Dominio .GAL | Portal Oficial do Dominio .GAL. URL: https://dominio.gal/en/the-importance-of-https-protocol/ (дата звернення: 14.05.2025).