УДК 004.72
DOI: 10.31673/2409-7292.2025.019877

Павлюк О. Ю., Нємкова О. А.

СИНЕРГІЯ БЕЗПЕКИ ТА ПРОДУКТИВНОСТІ: ОПТИМІЗАЦІЯ DNS-РЕЗОЛВІНГУ ЗА ДОПОМОГОЮ HTTPS-DNS, DNS-OVER-HTTPS, ECH ТА HTTP/3

У статті розглянуто оптимізацію DNS-резолвінгу в умовах зростання кіберзагроз та підвищених вимог до швидкодії інтернет-з'єднань. Проаналізовано вразливості традиційного DNS, зокрема ризики перехоплення, маніпуляцій запитами та їхню залежність від нешифрованих каналів зв'язку, що створює загрозу компрометації даних. Представлено сучасні підходи до підвищення безпеки та ефективності DNS-резолвінгу, зокрема використання новітніх технологій, таких як DNS-over-HTTPS (DoH), HTTPS DNS записів (тип 65), Encrypted Client Hello (ECH), QUIC та HTTP/3. Оскільки ці технології не є взаємозамінними, то для досягнення значної оптимізації DNS-резолвінгу варто застосовувати їх у комплексі, коли вони доповнюють одна одну: DoH забезпечує захищену передачу DNS-запитів, HTTPS DNS записи прискорюють резолвінг, ECH приховує метадані про підключення, а QUIC і HTTP/3 значно зменшують затримки та покращують ефективність передачі даних. У статті описано їхню синергію, що забезпечує шифрування запитів, мінімізацію затримок, підвищення приватності користувачів та обходження обмежень, накладених інтернет-провайдерами. Особливу увагу приділено впливу цих технологій на продуктивність веб-ресурсів, зниження навантаження на DNS-сервери та забезпечення надійного з'єднання навіть у мережах із високими затримками. Наведено приклади клієнтських запитів у вигляді діаграм, що порівнюють традиційний та оптимізований DNS-резолвінг, демонструючи переваги впровадження новітніх протоколів. Окреслено перспективи подальшого розвитку цих технологій та їхній потенційний вплив на створення безпечнішого, швидшого та ефективнішого інтернет-середовища.

Ключові слова: DNS-резолвінг, DNS-over-HTTPS, QUIC, HTTP/3, Server Name Indication, шифрування, приватність, безпека.

Вступ

Традиційна система доменних імен (DNS), що базується на архітектурі запитів та відповідей [1], демонструє ряд архітектурних та протокольних вразливостей, які суттєво обмежують продуктивність та безпеку. Зокрема, незахищені запити DNS, використовуючи протоколи транспортного рівня UDP/TCP на порту 53, є вразливими до перехоплення, атак типу "man-in-the-middle" та спуфінгу, що компрометує цілісність DNS-резолвінгу та може призвести до перенаправлення клієнтів на шкідливі ресурси [2]. Крім того, відсутність інтегрованого механізму шифрування та автентифікації на рівні DNS створює додаткові ризики для конфіденційності користувацьких даних.

Одним із ключових обмежень традиційного DNS є його залежність від централізованих резолверів, що не лише підвищує ризик цензурування та маніпуляцій з боку провайдерів або зловмисників, а й створює єдину точку відмови. До того ж, використання кешування DNS може призводити до затримок у поширенні оновлених записів, а відкритість протоколу до DDoS-атак, зокрема через DNS-ампліфікацію, ще більше загострює проблему його безпеки. Відсутність механізмів верифікації автентичності відповідей також робить систему вразливою до атак, таких як отруєння кешу (cache poisoning), що може спричинити масові збої у роботі веб-ресурсів.

Постановка проблеми

Традиційний процес DNS-резолвінгу передбачає передачу DNS-запитів у відкритому вигляді, що робить їх вразливими до перехоплення та маніпуляцій. Зловмисники можуть перехопити DNS-запити та перенаправити користувача на шкідливі сайти, викрасти конфіденційні дані або змінити вміст веб-сторінок [2].

Крім того, традиційний DNS-резолвінг може бути повільним. Це пов'язано з тим, що DNS-запити можуть проходити через кілька проміжних серверів, перш ніж досягнуть кінцевого пункту призначення. Кожен з цих серверів додає затримку до загального часу резолвінгу. Затримки, пов'язані з передачею DNS-запитів, негативно впливають на швидкість завантаження веб-сторінок, особливо для користувачів, які знаходяться географічно віддалено від DNS-серверів або веб-сайтів [3].

Ще однією проблемою є вразливість SNI (Server Name Indication). SNI передається у незашифрованому вигляді, навіть при використанні HTTPS. SNI є розширенням протоколу TLS, яке дозволяє серверу ідентифікувати, до якого домену клієнт намагається підключитися (це необхідно для серверів, які розміщують кілька доменів на одній IP-адресі). Однак, оскільки SNI передається у відкритому вигляді, інформація може бути перехопленою і домен бути видимим, навіть якщо решта з'єднання зашифрована [4]. Це створює загрозу для приватності користувачів, особливо в країнах з обмеженою свободою інтернету, цензури або стеженням.

Існуючі проблеми з резолвінгом DNS, зокрема вразливість до атак, відсутність шифрування та затримки при обробці запитів, вимагають впровадження сучасних рішень для підвищення безпеки, продуктивності та конфіденційності інтернет-з'єднань. Рішення зазначених проблем полягає у впровадженні новітніх технологій, таких як DNS-over-HTTPS (DoH), HTTPS DNS записи (тип 65), Encrypted Client Hello (ECH), QUIC та HTTP/3, які покращують безпеку, конфіденційність та швидкодію DNS-резолвінгу. Однак ці технології не є взаємозамінними, тому необхідно дослідити можливі способи їхнього поєднання для досягнення оптимальних результатів і забезпечення ефективного функціонування інтернет-з'єднань.

Аналіз останніх публікацій

Новітні протоколи DNS-over-HTTPS (DoH), HTTPS-DNS, Encrypted Client Hello (ECH), QUIC та HTTP/3 становлять інтерес для дослідників, оскільки існує питання, чи повністю вони реалізують заявлені переваги. Наприклад, протокол DNS-over-HTTPS має на меті зашифрувати трафік DNS, щоб зловмисник не зміг відрізнити його від трафіку HTTPS. Автори дослідження [5] застосували машинне навчання для класифікації зашифрованого трафіку, поділяючи його на DNS-over-HTTPS трафік та HTTPS трафік. Вони довели, що без спеціальних вдосконалень, лише за метаданими, ці трафіки можна відрізняти з високою точністю. Це може призвести до блокування DNS-over-HTTPS трафіку агресивним провайдером, щоб змусити користувачів перейти на звичайні DNS-запити. Водночас автори запропонували метод, який ефективно знижує точність класифікації, що дає підстави сподіватися на ефективність протоколу DNS-over-HTTPS.

У документі [6] Робоча група з розробки Інтернету (IETF) надала трек стандартів Інтернету щодо прив’язки послуг і специфікації параметрів через DNS для полегшення пошуку інформації, необхідної для підключення до мережевих служб. Ці стандарти надають більше інформації клієнту перед його спробами встановити з’єднання, що забезпечує потенційні переваги як для продуктивності, так і для конфіденційності. Також передбачена можливість розширення для підтримки майбутніх застосувань, наприклад, ключів для шифрування TLS ClientHello.

У роботі [7] автори здійснили розгортання DNS-сервера з підтримкою HTTPS з метою дослідження клієнтської сумісності з DNS через HTTPS. Результати дослідження висвітлили проблеми, пов’язані зі складністю належної підтримки HTTPS-записів та збоями з’єднання в браузерах у разі неправильного налаштування HTTPS-запису. Автори дійшли висновку, що існують проблеми, пов’язані з IP-підказками та конфігурацією ECH, які необхідно подолати для повноцінного впровадження HTTPS.

У блозі Cloudflare автор [8] обговорює фундаментальні проблеми, що виникають під час впровадження нових протоколів. Це вимагає співпраці між кількома сторонами – постачальники DNS-послуг, взаємодіючи з різними браузерами та клієнтами, мають збільшити підтримку та впровадження HTTPS-записів. Наприклад, Encrypted SNI (розширення TLS, призначене для покращення конфіденційності користувачів в Інтернеті) використовує спеціальний DNS-запис для оголошення відкритого ключа сервера, який клієнти можуть використовувати для отримання секретного ключа, необхідного для шифрування SNI. Без відповідного налаштування всі переваги нових протоколів у швидкодії зводяться нанівець.

© Павлюк О. Ю., Нємкова О. А. (2025). Синергія безпеки та продуктивності: оптимізація DNS-резолвінгу за допомогою HTTPS-DNS, DNS-over-HTTPS, ECH та HTTP/3. Сучасний захист інформації, 1(61), 241–248. https://doi.org/10.31673/2409-7292.2025.019877.

Автори [9] провели дослідження управління ECH в організаційному середовищі, а також запропонували рішення щодо регулювання доступу до веб-сайтів із підтримкою ECH. Було перевірено сумісність нового протоколу з веб-браузерами, які не підтримують ECH. Це важливо, оскільки сучасний IT-ландшафт є різноманітним, і браузери можуть бути застарілими або просто не підтримувати ECH. Під час тестування веб-браузера без підтримки ECH рішення функціонувало без проблем. Автори зазначили, що для клієнтів потрібно обмежити можливості зміни налаштувань проксі-серверів, VPN та браузерів.

Дослідження [10] присвячене вивченню інтеграції протоколу HTTP/3 із QUIC, заснованим на UDP, як альтернативи традиційним версіям HTTP, що працюють на основі TCP. Незважаючи на свої переваги, HTTP/3 стикається з кількома проблемами, зокрема з підтримкою трафіку UDP операційними системами та можливою вразливістю до атак DDoS. Автори відповіли на такі важливі питання: як відбувається інтеграція HTTP/3 та QUIC; які функції та вдосконалення в HTTP/3 вирішують проблеми продуктивності та безпеки, виявлені у попередніх версіях HTTP; як HTTP/3 можна розгорнути у хмарних середовищах для вирішення проблем IoT та веб-додатків.

Автори роботи [11] провели поглиблене дослідження протоколу QUIC щодо його впровадження та застосування. Також вони виконали тестову реалізацію на базі сервісів Amazon AWS для оцінки продуктивності QUIC порівняно з TCP і UDP. Автори обговорюють можливі рішення проблем QUIC, зокрема відновлення втрати даних та механізми виправлення помилок. Крім того, вони провели аналіз безпеки протоколу QUIC.

Отже, розглянуті публікації демонструють значний інтерес дослідників до питань практичної реалізації, застосування, а також проблем безпеки, конфіденційності та продуктивності протоколів DNS-over-HTTPS (DoH), HTTPS DNS-записів (тип 65), Encrypted Client Hello (ECH), QUIC та HTTP/3. Тому актуальним є завдання визначення можливостей оптимізації DNS-резолвінгу на основі цих протоколів.

Метою і задачами роботи є демонстрація синергії сучасних протоколів, таких як DNS-over-HTTPS (DoH), HTTPS-DNS, Encrypted Client Hello (ECH), QUIC та HTTP/3, для оптимізації процесу DNS-резолвінгу, а також дослідження взаємодії технологій для забезпечення швидкого, безпечного та приватного інтернет-з'єднання.

Виклад основного матеріалу

Традиційний DNS-резолвінг: проблеми та обмеження

Для розуміння вразливості та недоліків певних елементів з’єднання, розглянемо спрощений традиційний метод підключення до HTTPS веб-сторінки:

1. Запит клієнта (HTTP): Браузер користувача намагається з'єднатися з веб-сайтом, використовуючи протокол HTTP (наприклад, http://www.example.com).

2. DNS-запит (традиційний): Браузер надсилає DNS-запит до локального DNS-резолвера (зазвичай надається інтернет-провайдером, ISP). Цей запит, як правило, не шифрується (використовуючи UDP або TCP порт 53).

3. DNS-відповідь: DNS-резолвер відповідає IP-адресою сервера веб-сайту. Ця комунікація вразлива до перехоплення та маніпуляцій. Зловмисник може перехопити DNS-запит і надати підроблену IP-адресу.

4. HTTP-з'єднання: Браузер з'єднується з сервером, використовуючи протокол HTTP. Це з'єднання не шифрується. Вся комунікація, включаючи початковий запит, видима для будь-кого, хто моніторить мережу.

5. HTTP-перенаправлення: Сервер відповідає HTTP-перенаправленням (301 або 302) на HTTPS-версію веб-сайту (наприклад, https://www.example.com).

6. DNS-запит (повторний): Браузеру тепер потрібно виконати ще один DNS-пошук для HTTPS-версії сайту. Цей запит також вразливий, як і в кроці 4.

7. HTTPS-з'єднання (вразливий SNI): Браузер з'єднується з сервером через HTTPS. Однак індикація імені сервера (Server Name Indication, SNI) надсилається у відкритому вигляді під час встановлення TLS-з'єднання. Моніторинг мережі все ще може виявити, який домен відвідується, попри те, що з'єднання зашифроване.

Графічно, традиційний сценарій відкриття веб-сайту з передуючим DNS-запитом можна зобразити у вигляді Діаграми 1 наступним чином (рис. 1):

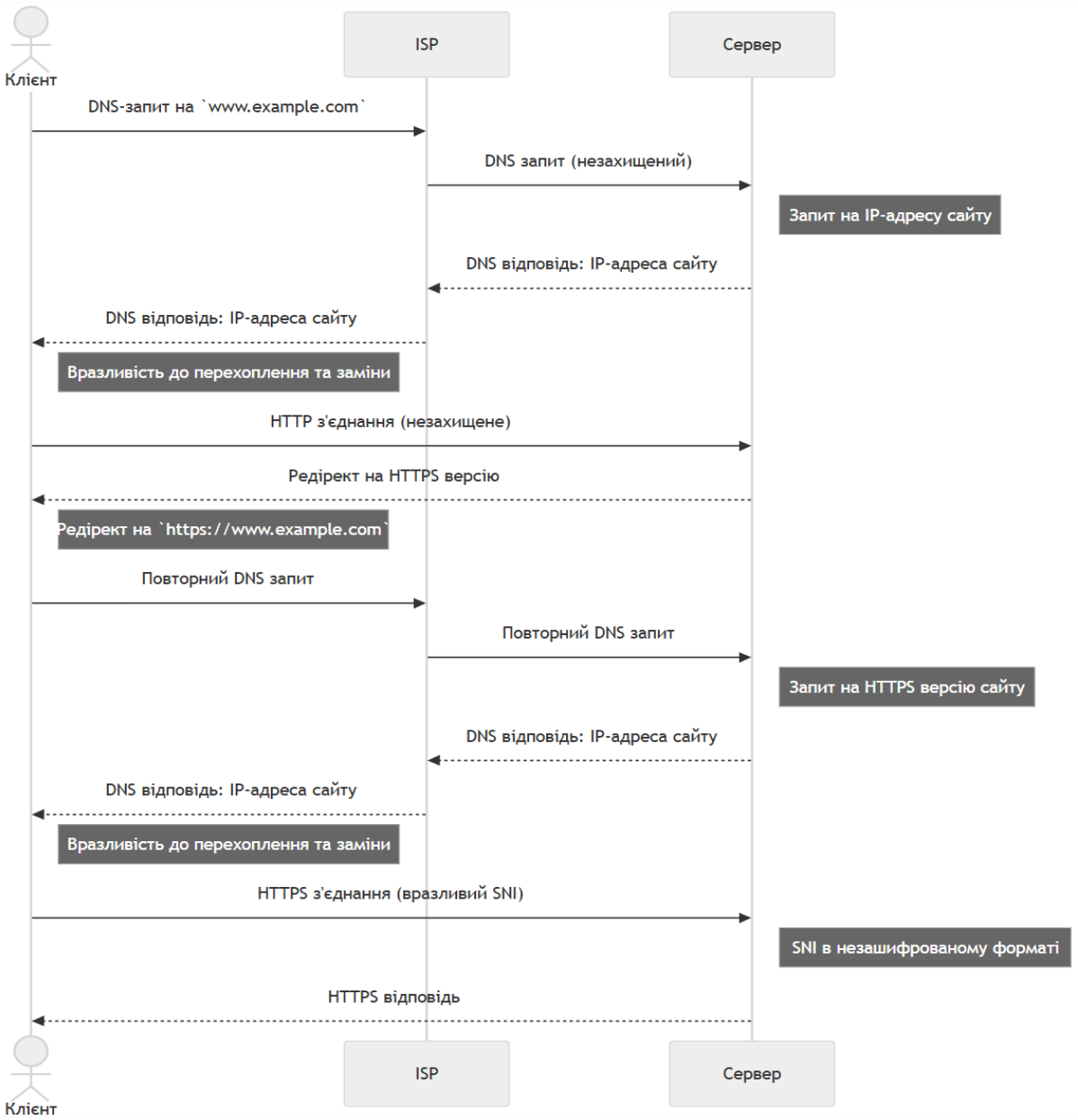

Рис. 1. Діаграма1 – традиційний сценарій відкриття HTTPS-сторінки

Еволюція DNS-безпеки: DoH, HTTPS-DNS (Type 65), SVCB, ECH

З метою вирішення проблем традиційного DNS-резолвінгу було розроблено ряд нових протоколів та технологій, які значно покращують безпеку та конфіденційність користувачів.

DNS-over-HTTPS (DoH) – це протокол, який дозволяє передавати DNS-запити через HTTPS-з'єднання. Це означає, що DNS-запити шифруються, що робить їх недоступними для перехоплення та маніпуляцій зловмисниками [5]. Хоча ця технологія є значним кроком уперед у забезпеченні безпеки, вона все ж має певні недоліки, наведені в таблиці 1.

© Павлюк О. Ю., Нємкова О. А. (2025). Синергія безпеки та продуктивності: оптимізація DNS-резолвінгу за допомогою HTTPS-DNS, DNS-over-HTTPS, ECH та HTTP/3. Сучасний захист інформації, 1(61), 241–248. https://doi.org/10.31673/2409-7292.2025.019877.

Таблиця 1

Переваги та недоліки протоколу DNS-over-HTTPS

Переваги DoH:	**Недоліки DoH:**
Шифрування DNS-запитів: Захищає від прослуховування та підміни даних.	**Централізація:** Використання публічних DoH-серверів може призвести до централізації DNS-трафіку, що створює ризики для приватності.
Обхід цензури та підвищення приватності: Дозволяє обходити обмеження на доступ до веб-сайтів, встановлені інтернет-провайдерами або урядами. Ускладнює відстеження активності користувачів в Інтернеті.	**Залежність від HTTPS:** DoH залежить від HTTPS, що може призвести до затримок у разі проблем з HTTPS-з'єднанням.

HTTPS DNS запис (тип 65) дозволяє клієнтам отримувати інформацію, необхідну для встановлення безпечного HTTPS з'єднання, без необхідності робити додаткові запити до сервера. Він стандартизований в RFC 9460 [6]. Цей запис містить такі дані, як IP-адреса, порт та параметри ECH, необхідні для підключення. Клієнт, отримавши цей запис, може одразу використовувати отримані дані для встановлення HTTPS з'єднання. Це прискорює процес підключення, зменшує кількість запитів до сервера та підвищує безпеку [7]. Приклад HTTPS-DNS запису: *example.com. IN HTTPS 1. alpn=h3,h2,http/1.1 port=443 ipv4hint=192.0.2.1, 192.0.2.2.*

Пояснення запису надано у таблиці 2.

Таблиця 2

Пояснення полів HTTPS-DNS запису

Поле	**Опис**
example.com	Доменне ім'я, до якого застосовується запис.
IN	Вказує на клас запису, який майже завжди є "IN" для Інтернету.
HTTPS	Вказує тип запису як HTTPS-запис.
1	Пріоритет запису. Менші числа вказують на вищий пріоритет. Якщо для одного домену існує кілька HTTPS-записів, перевага надається запису з найменшим значенням пріоритету.
.	Крапка представляє кореневий домен, що вказує на те, що цей запис застосовується до вершини домену (example.com), а не до піддомену.
alpn=h3,h2,http/1.1	Визначає протоколи Application-Layer Protocol Negotiation (ALPN), які підтримуються сервером, у порядку переваги. У цьому випадку сервер надає перевагу HTTP/3, потім HTTP/2 і, нарешті, HTTP/1.1.
port	Вказує нестандартний порт для служби HTTPS (за замовчуванням - 443).
ipv4hint/ ipv6hint	Надає список IPv4 або IPv6-адрес як підказки для розташування сервера.
echconfig	Надає інформацію про конфігурацію для Encrypted ClientHello (ECH) для більш безпечного TLS-з'єднання.

SVCB (Service Binding) запис, також визначений в RFC 9460 [6], доповнює HTTPS DNS записи, надаючи більш гнучкі можливості для опису сервісів. Він дозволяє серверам вказувати альтернативні способи підключення, включаючи використання різних портів, протоколів та параметрів ECH. SVCB запис дозволяє оптимізувати процес підключення, вибираючи найбільш підходящий спосіб, і є важливим механізмом для поширення інформації про конфігурацію ECH- надає клієнтам необхідні дані для шифрування SNI [8].

Encrypted Client Hello (ECH) є розширенням протоколу TLS 1.3, яке шифрує частину TLS-рукостискання, відому як "ClientHello", що містить SNI. Це досягається шляхом використання публічних ключів, опублікованих сервером [9]. Для роботи ECH клієнт має отримати конфігурацію ECH до того, як відправить запит на сервер [6]. Ця конфігурація може

© Павлюк О. Ю., Нємкова О. А. (2025). Синергія безпеки та продуктивності: оптимізація DNS-резолвінгу за допомогою HTTPS-DNS, DNS-over-HTTPS, ECH та HTTP/3. Сучасний захист інформації, 1(61), 241–248. https://doi.org/10.31673/2409-7292.2025.019877.

бути отримана з HTTPS DNS або SVCB записів. ECH значно підвищує приватність користувачів, приховуючи інформацію про відвідані веб-сайти.

QUIC та HTTP/3

Для подальшого підвищення швидкості та ефективності інтернет-з'єднань були розроблені протоколи QUIC та HTTP/3. HTTP/3 – це нова версія протоколу HTTP, яка використовує QUIC як транспортний протокол. HTTP/3 був розроблений з метою покращення продуктивності та безпеки веб-додатків. Використання QUIC дозволяє HTTP/3 вирішити проблеми, пов'язані з TCP, такі як блокування черги пакетів (head-of-line blocking) та затримки встановлення з'єднання. HTTP/3 також підтримує шифрування TLS 1.3, що забезпечує захист переданих даних [10]. QUIC (Quick UDP Internet Connections) – це транспортний протокол, розроблений Google, який працює поверх UDP з метою зменшення затримок та підвищення ефективності передачі даних. QUIC використовує шифрування TLS 1.3 для захисту переданих даних та забезпечує гарантію доставки пакетів, як TCP. Проте на відміну від TCP, який використовує послідовну передачу пакетів, QUIC дозволяє передавати декілька потоків даних одночасно, що зменшує затримки та підвищує ефективність. QUIC також дозволяє встановлювати з'єднання швидше, ніж TCP, що зменшує час, необхідний для початку передачі даних [11].

Синергія протоколів: покращення DNS-резолвінгу

При правильному застосуванні технології DoH, HTTPS-DNS, ECH, QUIC та HTTP/3, працюють в синергії, забезпечуючи значне покращення DNS-резолвінгу.

Використання DoH дозволяє шифрувати DNS-запити, що захищає їх від перехоплення та маніпуляцій. HTTPS DNS запис (тип 65) пришвидшує встановлення з'єднання з сайтом, не роблячи додаткових запитів до сервера. ECH шифрує SNI, вирішуючи проблему вразливості та покращуючи приватність користувачів. QUIC та HTTP/3 зменшують затримки та підвищують ефективність передачі даних.

Ця синергія дозволяє:

- Прискорити процес DNS-резолвінгу: HTTPS DNS запис та використання QUIC та HTTP/3 зменшують затримки та підвищують ефективність.
- Прискорити завантаження веб-сторінок: Використання сучасних протоколів зменшує час, необхідний для встановлення з'єднання та передачі даних.
- Покращити анонімність та приватність: DoH та ECH шифрують DNS-запити та SNI, захищаючи інформацію про відвідані веб-сайти.
- Обхід ISP: використання DOH дозволяє обходити DNS резолвер, наданий інтернет-провайдером.

Розглянемо метод підключення до HTTPS веб-сторінки з застосуваннями рекомендацій з безпеки та швидкості, зображений у вигляді Діаграми 2, рис.2:

1. Запит клієнта (HTTPS): Браузер намагається з'єднатися з веб-сайтом, використовуючи HTTPS (наприклад, https://www.example.com).

2. DoH запит: Браузер надсилає DNS-запит через HTTPS (DoH) до DoH резолвера. Цей запит зашифрований, що захищає його від прослуховування та маніпуляцій.

3. DNS відповідь (HTTPS запис): DoH резолвер повертає HTTPS запис. Цей запис містить:

- Цільове ім'я хоста та порт.
- Підтримувані протоколи (наприклад, HTTP/2, HTTP/3).
- Конфігурацію ECH ("echconfig").

4. Зашифрований ClientHello (ECH): Браузер використовує конфігурацію ECH з HTTPS запису для шифрування повідомлення ClientHello в TLS рукостисканні. Це приховує SNI, запобігаючи можливості для сторонніх осіб бачити, який веб-сайт відвідується.

5. HTTPS з'єднання: Браузер встановлює безпечне HTTPS з'єднання з сервером. Вся комунікація зашифрована та захищена. З'єднання відбувається швидше, оскільки браузер має всю необхідну інформацію з HTTPS запису.

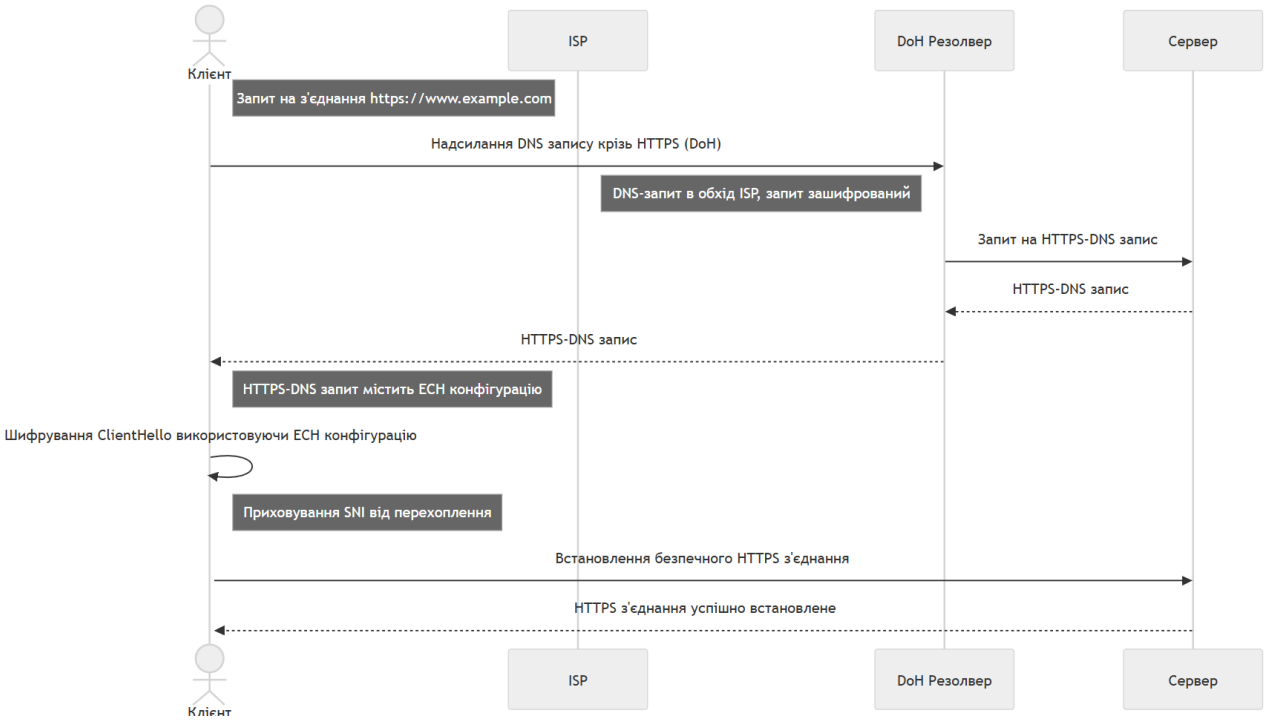

Рис. 2. Діаграма 2 – Сценарій відкриття HTTPS-сторінки із застосуванням рекомендованих протоколів

Ключові відмінності, виділені на діаграмах:

• Безпека DNS: Діаграма 1 показує вразливий, незашифрований DNS, тоді як Діаграма 2 показує безпечний, зашифрований DoH.

• Безпека з'єднання: Діаграма 1 показує початкове незашифроване HTTP-з'єднання та вразливе HTTPS-з'єднання (SNI відкритий). Діаграма 2 показує пряме, безпечне HTTPS-з'єднання з ECH, що захищає SNI.

• Продуктивність: Діаграма 2 демонструє більш швидке з'єднання завдяки HTTPS запису, який надає всі необхідні деталі з'єднання в одному DNS запиті. Діаграма 1 вимагає кількох DNS запитів та перенаправлення.

Висновки та перспективи подальших досліджень

Традиційний DNS-резолвінг має ряд вразливостей, таких як незахищені DNS-запити та вразливість SNI, які негативно впливають на користувацький досвід. Використання DoH дозволяє шифрувати DNS-запити, захищаючи їх від перехоплення та маніпуляцій. HTTPS DNS запис (тип 65) пришвидшує встановлення з'єднання з сайтом, надаючи необхідну інформацію в одному DNS-запиті. ECH шифрує SNI, що вирішує проблему вразливості та покращує приватність користувачів. QUIC та HTTP/3 зменшують затримки та підвищують ефективність передачі даних, це забезпечує швидке завантаження веб-сторінок. Синергія цих протоколів дозволяє досягти значних покращень у процесі DNS-резолвінгу. Користувачі отримують швидший, безпечніший та конфіденційніший доступ до веб-ресурсів.

Перспективи подальшого розвитку та впровадження цих технологій є багатообіцяючими. З подальшим розвитком інтернету та зростанням вимог до безпеки та приватності, ці протоколи стануть ще важливішими. Важливо, щоб інтернет-провайдери, розробники браузерів та веб-серверів активно впроваджували ці технології, щоб забезпечити користувачам найкращий можливий досвід.

Перелік посилань

1. Dooley M., Rooney T. Introduction to the Domain Name System (DNS) / M. Dooley // DNS SECURITY MANAGEMENT (7th ed.). – Hoboken, NJ: Wiley-IEEE Press. – 2017. – P. 17–30.

2. A survey of domain name system vulnerabilities and attacks / Kim T. H., Reeves D. // Journal of Surveillance, Security and Safety, – 2020, 1: 34–60.

3. Comparing DNS resolvers in the wild / Ager B., et al. // In: Proceedings of the 10th ACM SIGCOMM conference on Internet measurement. – 2010. – P. 15–21. https://doi.org/10.1145/1879141.18791.

4. Privacy Leaks Via SNI and Certificate Parsing / Koshy A. M., et al. // In: *2023* International Conference on Quantum Technologies, Communications, Computing, Hardware and Embedded Systems Security (iQ-CCHESS). IEEE. – 2023. – P. 1–5. https://doi.org/10.1109/iQ-CCHESS56596.2023.10391827.

5. Privacy of DNS-over-HTTPS: Requiem for a Dream? / Csikor L., et al. // In: 2021 IEEE European Symposium on Security and Privacy (EuroS&P). IEEE. – 2021. – P. 252–271. https://doi.org/10.1109/EuroSP51992.2021.00026.

6. Service Binding and Parameter Specification via the DNS (SVCB and HTTPS Resource Records) [Electronic resource] / Schwartz B. M., Bishop M., and Nygren E. // *Request for Comments* 9460. RFC Editor, November, – 2023. Web page: https://www.rfc-editor.org/rfc/rfc9460.html (2025).

7. Exploring the Ecosystem of DNS HTTPS Resource Records: An End-to-End Perspective / Dong H., et al. // In: Proceedings of the 2024 ACM on Internet Measurement Conference. – 2024. – P. 423–440. https://doi.org/10.48550/arXiv.2403.15672.

8. Speeding up HTTPS and HTTP/3 negotiation with... DNS [Electronic resource] / Ghedini A. // Cloudflare Blog, September 30, – 2020. Web page: https://blog.cloudflare.com/speeding-up-https-and-http-3-negotiation-with-dns/ (2025).

9. Encrypted Client Hello, balancing privacy enhancements with security implications [Electronic resource] / Kartavcevas P., Maksimovic L. // University of Skövde, School of Informatics. – 2024. Web page: https://his.diva-portal.org/smash/record.jsf?pid=diva2%3A1882070&dswid=-8911 (2025).

10. What We Know About HTTP/3 and Its Implementation: A Literature Review / Koch J., Falowo O., Elrod N. // In: 2024 IEEE 3rd International Conference on Computing and Machine Intelligence (ICMI). IEEE. – 2024. – P. 1–7. https://doi.org/10.1109/ICMI60790.2024.10585883.

11. Security and performance evaluations of QUIC protocol / Soni M., Rajput B. S. // In: Data Science and Intelligent Applications: Proceedings of ICDSIA 2020. Springer Singapore. – 2021. – P. 457–462.

Надійшла 20.02.2025