КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (25), 2024
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2024.25.304317
УДК 004.72

Нємкова Олена Анатоліївна
д.т.н., професор, професор кафедри безпеки інформаційних технологій
Національний університет «Львівська політехніка», Львів, Україна
ORCID ID: 0000-0003-0690-2657
olena.a.niemkova@lpnu.ua

Павлюк Олександр-Юрій Святославович
аспірант кафедри безпеки інформаційних технологій
Національний університет «Львівська політехніка», Львів, Україна
ORCID ID: 0009-0008-6985-203X
oleksandr-iurii.s.pavliuk@lpnu.ua

ДОЦІЛЬНІСТЬ ВИКОРИСТАННЯ ДОМЕНІВ ТИПУ HANDSHAKE У ПОРІВНЯННІ З КЛАСИЧНИМ DNS

Анотація. Однією з ключових структур в сучасній мережі Інтернет є Система Доменних Імен (DNS). Її роль полягає у перетворенні машинних IP-адрес в зручний для людей формат доменів. Оскільки початково система не була спроектованою для глобального використання, у ході її популяризації з'явився ряд недоліків, пов'язаних зокрема з кібербезпекою: доступністю та конфіденційністю. Публічність та ієрархічність системи часто використовується для обмежень цензурою. У цій статті розглянуто доцільність використання альтернативного децентралізованого протоколу під назвою Handshake. За рахунок використання технології розподіленого реєстру Блокчейн він відходить від традиційної ієрархічної DNS в контексті реєстрацій, власності та контролю над доменними іменами. Ця зміна робить структуру децентралізованою, проте водночас виникає ряд недоліків. Handshake домени вимагають спеціального підходу для їх використання пересічними користувачами та започатковують репутаційні та технологічні ризики. В статті аналізуються технічні відмінності між Handshake та DNS, включаючи структуру, реєстрацію доменів та механізм резолвінгу. Розглядається вплив цих відмінностей на користувацький досвід, безпеку, цензуру, доступність та володіння доменами. Досліджуються тренди реєстрацій Handshake та традиційних доменних імен, що демонструє швидкий ріст популярності перших. Окремо виділено потенціал Handshake для корпоративного використання, зокрема для зниження ризику витоку внутрішніх доменних імен, а також посилення кібербезпеки за рахунок використання внутрішніх центрів сертифікації. Визначено обмеження протоколу Handshake та окреслено напрямки для подальших досліджень. Порівняльне дослідження виявило, що переваги протоколу Handshake пов'язані з анонімністю власників відповідних доменних імен, складністю їх блокування, а також з забезпеченим простором для інновацій. З іншого боку, DNS значно переважає у зручності користування, надійності, зрілості, підтримці існуючим програмним забезпеченням, та зменшеними репутаційними ризиками.

Ключові слова: Система Доменних Імен; DNS; Handshake; Блокчейн; децентралізація; кібербезпека; конфіденційність; анонімність; цензура.

ВСТУП

DNS (Domain Name System), або Система Доменних Імен — це одна з найнеобхідніших структур Інтернету, суть якої полягає у перекладенні читабельного для людини доменного імені (наприклад — Wikipedia.org) у «машинну» IP-адресу (91.198.174.192), яка використовується для безпосереднього з'єднання хоста з сервером [1]. Система DNS була створена науковцями в Університеті Каліфорнії в Берклі ще у 1983-му році під час розробки ARPANET — однієї з перших версій Інтернету. До

винайдення DNS зв'язок з IP-адресами маршрутизувався за допомогою файлу Hosts, що зберігався на серверах та містив відповідності доменів та IP-адрес. На той час система DNS використовувалась тільки в вузьких колах, в яких не існувало сторін, що були зацікавлені в отруєнні мережі, тож на початку свого існування протокол не передбачав механізмів захисту чи шифрування. Втім, попри свою очевидну незахищеність, система набула глобальної популярності і глибоко проникла в інфраструктуру Інтернету, оскільки суттєво спрощувала користування мережею.

Постановка проблеми. На сьогоднішній день DNS є централізованою системою, яку ніхто не контролює безпосередньо, що ідеально підходить для глобальних масштабів об'єднаних мереж. За рахунок цього система DNS стала критично важливою, проте водночас її дуже важко модифікувати та захистити. Хоч система і не має центрального органу управління, контроль над нею розподілений нерівномірно, з невеликою кількістю ключових сторін, що володіють значною владою. Ці недоліки часто призводять до:

- Цензури;
- Монополії на ціни та доступність доменних імен;
- Вразливості до кібератак;
- Недостатньої прозорості та підзвітності.

Еволюцією системи DNS можна вважати протокол Handshake — децентралізовану систему доменних імен нового покоління, мета якої — усунути недоліки традиційної DNS за рахунок розподіленого реєстру [2]. Теоретично це робить систему більш стійкою до цензури, більш відкритою до інновацій та більш демократичною і прозорою альтернативою традиційній DNS. Handshake все ще перебуває на ранніх стадіях розробки, тож далі будуть розглянуті переваги та недоліки даного протоколу, а також його потенціал як для пересічних користувачів, так і для великих організацій.

Важливо відмітити, що існує декілька типів хендшейк-доменів: HNS (Handshake), ENS (Ethereum Name Service), Unstoppable Domains [3]. Ці технології пропонують різні підходи до реєстрацій та вектори застосування, проте в контексті цього дослідження ми фокусуємось на спільних рисах технологій, а саме: використання Blockchain як основи розподіленого реєстру та неможливість застосування протоколу DNS в його ієрархічному розумінні. Надалі в дослідженні всі типи об'єднані єдиним терміном «Handshake» або «хендшейк».

Мета статті. Провести порівняльний аналіз переваг та недоліків системи DNS та протоколу Handhshake з точки зору різних аспектів їх використання.

Для досягнення мети вирішено наступні завдання:

- розглянуто основні технічні відмінності DNS та Handshaike та зручність у використанні;
- проаналізовано переваги та недоліки з точки зору кібербезпеки та цензури;
- досліджено доступність ринку доменних імен;
- розглянуто можливості підвищення кібербезпеки для корпоративного досвіду при застосуванні протоколу Handhshake.

Далі наведено результати досліджень, у тому числі аналіз останніх досліджень і публікацій інших авторів, у висновках визначено переваги та обмеження протоколу Handshake та окреслено напрямки для подальших досліджень.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

DNS проти Handshake: ключові технічні відмінності

Система Доменних Імен (Domain Name System, DNS) має ієрархічну і централізовану структуру, яка ґрунтується на розподілі повноважень між доменами різних рівнів (табл. 1) [4].

Таблиця 1

Ієрархічна структура Системи Доменних Імен

	Опис повноважень
ICANN, IANA	ICANN (Інтернет-корпорація з присвоєння імен і номерів) — некомерційна організація, що відповідає за регулювання технічних аспектів та стандартів DNS, та за коректною роботою Реєстраторів та Реджістрі. IANA (Адміністрація адресного простору Інтернет) — підрозділ ICANN, що зокрема відповідає за менеджмент кореневих серверів.
Кореневі неймсервери (root)	13 кореневих неймсерверів розташовані в різних точках світу. Вони містять інформацію про домени верхнього рівня (TLD), такі як .com, .net, .org та інші. Адреси цих серверів є статичними та використовуються рекурсивними резолверами.
Оператори доменів верхнього рівня (TLD Registries, Реджістрі)	Доменні імена верхнього рівня (TLD, Top-Level Domains) адмініструються різними організаціями, приватними чи державними. Наприклад, TLD .com адмініструється компанією Verisign, .net — компанією Neustar, а .org — некомерційною організацією Public Interest Registry. Також в якості Реджістрі можуть виступати країни (.ua, .de, тощо). Реджістрі надають засоби для створення доменних імен Реєстраторам та містять інформацію про місцезнаходження їх DNS-зон. Реджістрі мають абсолютний контроль над іменами.
Оператори доменів другого рівня (Regisrars, Реєстратори)	Домени другого рівня (SLD, Second-Level Domains) реєструються користувачами у Реєстраторів доменів. Реєстратори — це компанії, акредитовані ICANN які продають домени від імені Реджістрі, ведуть записи про їх власників, та містять інформацію про авторитативні неймсервери. Реєстратори мають обмежений (проте високий) контроль над доменами.
Оператори авторитативних неймсверверів	Авторитативні неймсервери містять безпосередні DNS-зони доменних імен з відповідними DNS-записами. Авторитативні неймсервери можуть бути надані як Реєстратором доменного імені, так і сторонніми компаніями чи особами. Найвідомішими надавачами таких послуг є Cloudflare, UltraDNS, Amazon Route 53.
Постачальники послуги Інтернет (ISP, Internet Service Providers)	Локальні організації, що надають доступ до Інтернету користувачам. На рівні ISP зазвичай знаходяться рекурсивні резолвери, що використовуються більшістю користувачів для доступу до мережі DNS. ISP не мають безпосереднього контролю над доменними іменами, проте можуть збирати, аналізувати та модифікувати DNS-трафік.

Завдяки чітко визначеній структурі та ієрархії, DNS є відносно стабільною та надійною системою. DNS також легко масштабується та може обслуговувати мільйони доменних імен по всьому світу.

При необхідності знайдення IP-адреси, яка відповідає доменному імені, пристрій (браузер, поштовий клієнт, клієнт відеогри, тощо) надсилає DNS-запит. Цей запит проходить через кілька етапів (рис. 1) [5]:

0. Локальний кеш: пристрій перевіряє локальний кеш на наявність відповідного ресурсного запису;
1. Рекурсивний резолвер: у разі відсутності запису в локальному кеші, запит надсилається на рекурсивний резолвер (зазвичай знаходиться на рівні

інтернет-провайдера), який є DNS-сервером, що може відповісти на запит напряму або перенаправити його на інший сервер *(крок 1)*;

2. Кореневі неймсервери: Рекурсивний резолвер перевіряє свій локальний кеш, і у разі відсутності інформації, звертається до кореневих неймсерверів, які є найвищим рівнем DNS-ієрархії *(крок 2)*;
3. TLD неймсервери: Кореневі неймсервери повертають інформацію про знаходження DNS-зони TLD неймсерверів *(крок 3),* рекурсивний резолвер напрямляє запит до них *(крок 4)*;
4. TLD неймсервери повертають інформацію про авторитативні неймсервери, які містять інформацію про кінцеву DNS-зону доменного імені *(крок 5)*;
5. Авторитативні неймсервери отримують запит на конкретний тип ресурсного запису *(крок 6)* та повертають цей запис рекурсивному резолверу *(крок 7)*;
6. Рекурсивний резолвер повертає запитуваний тип запису комп'ютеру *(крок 8),* який ініціює з'єднання з кінцевим веб-сервером *(кроки 9, 10)*.

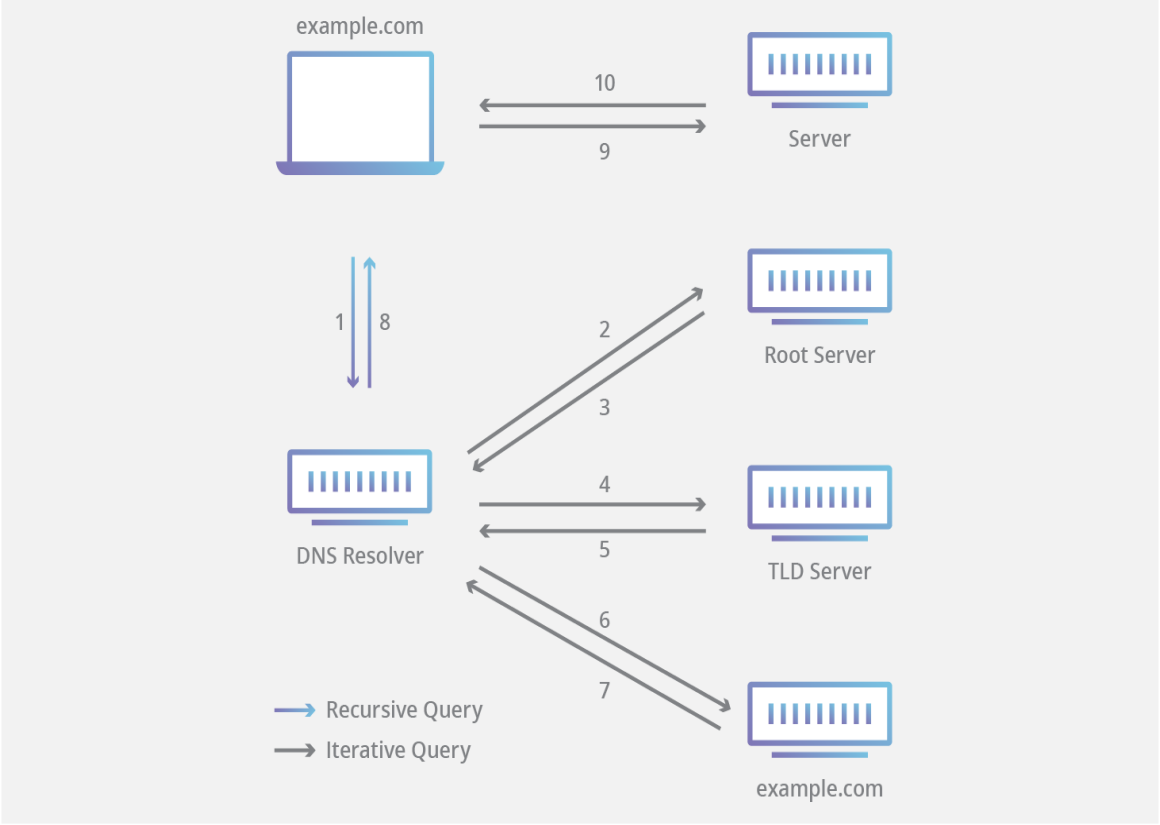

Рис. 1. Схема DNS-запиту, Cloudflare [5]

На відміну від DNS, Handshake — це децентралізована система доменних імен, де реєстрація побудована у розподіленому реєстрі з використанням технології Блокчейн. Це означає, що немає центрального органу, який контролює або управляє всім Handshake-протоколом. Натомість, система Handshake керується мережею розподілених вузлів (нодів), де кожен учасник відповідальний за перевірку і управління кореневою DNS зоною. Через відсутність ієрархічної структури, подібної до DNS, Handshake домени не можуть використовувати стандартні DNS-запити. Це означає, що веб-браузери та інші програми, які покладаються на стандартні DNS-протоколи, не розпізнають Handshake домени.

Досвід користування DNS проти Handshake для пересічних користувачів

Для більшості користувачів DNS працює «невидимо». DNS-інфраструктура добре налагоджена і інтегрована з веб-браузерами та операційними системами. Користувачам не потрібно встановлювати додаткове програмне забезпечення або змінювати налаштування, щоб отримати доступ до класичних доменів.

На відміну від DNS, доступ до ресурсів Handshake вимагає спеціального програмного забезпечення [6]. Цей недолік ускладнює широке впровадження протоколу, оскільки значна частина користувачів все ще покладається на традиційні веб-браузери [7], які не розпізнають Handshake домени як частину ієрархії. Існує кілька браузерних розширень та резолверів, які підтримують Handshake, наприклад, HNS.link, NCDNS, HNS.TO.

Одним із можливих рішень є браузерне розширення, здатне спрощувати процес розпізнавання доменів Handshake. Розширення ігнорує ієрархічну структуру класичного DNS-запиту і натомість використовує RDAP-сервери регістраторів для отримання інформації про авторитативні неймсервери. RDAP є сучасним протоколом, який замінює застарілий WHOIS, забезпечуючи стандартизований та зручніший формат для роботи з реєстраційними даними доменів (рис. 2) [8].

Важливо відмітити, що таке розширення працюватиме лише в контексті браузеру, і не буде покривати сценарії, де браузер не бере участі в DNS-запиті, наприклад: надсилання пошти зовнішнім поштовим клієнтом, пошук серверів клієнтами відеоігор, тощо. Втім, розвиток екосистеми Handshake прогресує, і з часом можуть з’явитись більше рішень, які дозволять «невидимо» працювати з Handshake-доменами на рівні цілої операційної системи.

Кібербезпека

Система DNS має ряд вразливостей внаслідок її ієрархічної структури, а також критичного значення. Виведення з ладу навіть одного DNS-сервера може призвести до довготривалих проблем з доступом до сервісів для мільйонів користувачів [9]. Деякі з найпоширеніших типів атак на DNS включають (перелік атак не є вичерпним):

- *Атаки типу «відмова в обслуговуванні» (DDoS):* Ці атаки спрямовані на перевантаження DNS-серверів трафіком, що робить їх недоступними для користувачів;
- *Атаки типу «DNS cache poisoning»:* Ці атаки спрямовані на підміну DNS-записів у кеші DNS-серверів, що може призвести до того, що користувачі будуть переспрямовані на шкідливі веб-сайти;
- *Атаки типу «DNS spoofing»:* Ці атаки спрямовані на захоплення контролю над DNS-серверами, що може призвести до того, що користувачі будуть переспрямовані на шкідливі веб-сайти або їм буде заблоковано доступ до певних веб-сайтів.

(*Цей список не є вичерпним, однак дослідження різних векторів атак виходить за рамки цієї статті.*)

ISSN 2663 - 4023

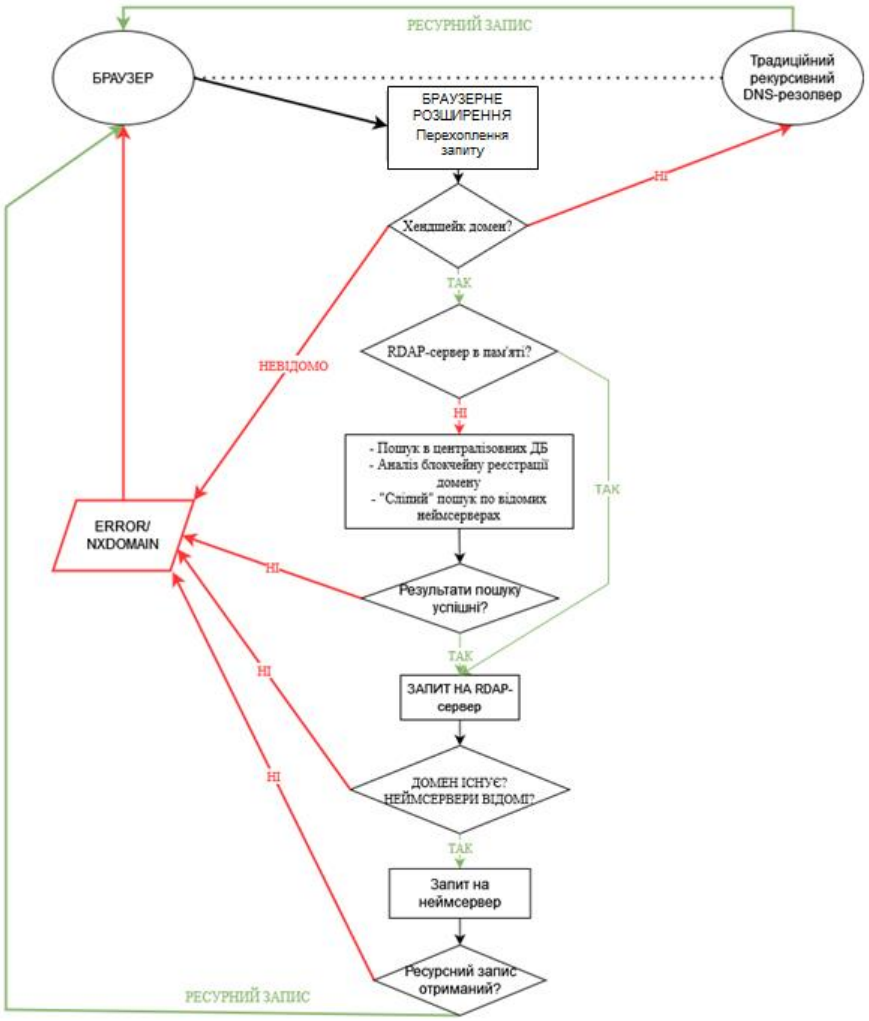

Рис. 2. Спрощена схема роботи браузерного розширення

Важливо зазначити, що DNS постійно вдосконалюється, і розробляються нові методи боротьби з його вразливостями, такі як протоколи DNSSEC, DoT/DoH/DoQ, тощо [10]. Однак DNS — це система з дуже обмеженим простором для інновацій. Нові функції та протоколи безпеки зазвичай розробляються на клієнтській стороні, та потребують ретельного дослідження та аналізу перед імплементацією. Цей процес повільний і складний, що гальмує розвиток DNS. Наслідком вразливостей DNS є зростання кількості та складності кібератак, підвищення ризику втрати даних та конфіденційності, зниження доступності Інтернету для користувачів.

В свою чергу, децентралізований характер Handshake може запропонувати альтернативний підхід до кібербезпеки за рахунок стрімкого розвитку і простору для інновацій. Сам по собі протокол не вирішує проблем, що пов'язані з вразливостями резолверів чи неймсерверів. Проте, за рахунок гнучкості імплементації, Handshake може мати нативне наскрізне шифрування, яке не підтримується класичним DNS.

Цензура та збір даних

Окрім вразливості до кібератак, традиційна система DNS має ще одну суттєву проблему: вона може використовуватися для цензури та збору персональних даних.

Цензура: Уряди або потужні організації можуть технічно цензурувати або блокувати доступ до певних доменів в мережі DNS. Це може здійснюватися шляхом видалення/перенаправлення DNS-записів або блокування доменів. Наприклад, у деяких країнах блокуються доступи до соціальних мереж, новинних сайтів або інших ресурсів, які вважаються небажаними владою [11].

Збір даних: На рівні інтернет-провайдера (ISP) може відбуватися збір, аналіз та продаж персональних даних користувачів, пов'язаних з їх DNS-запитами. Ці дані можуть включати інформацію про те, які веб-сайти відвідують користувачі, коли вони це роблять та з яких пристроїв вони отримують доступ до Інтернету. Ця інформація може використовуватися як для цілей таргетованої реклами, так і для відстеження онлайн-активності користувачів або навіть для урядового контролю [12], [13]. Хоч ця проблема частково вирішується протоколами шифрування DNS (DoQ/DoT/DoH) або використанням VPN, пересічні користувачі все ж ризикують своєю конфіденційністю.

Закони, що визначають дії та повноваження ISP варіюються між країнами та регіонами. В таких країнах, як В'єтнам, Білорусь, Туреччина та Мексика за допомогою ISP влада вводить інтернет-цензуру [14]. В гірших випадках, як от в Індонезії, Китаї, Єгипті, провайдери можуть повністю блокувати доступ до Інтернету з тих чи інших причин. Такі обмеження можуть бути екстремальними, проте не набагато менш важливими є приватність та конфіденційність клієнтських даних у країнах, де немає таких жорстких правил.

З іншого боку, децентралізована природа Handshake робить його значно стійкішим до цензури, порівняно з традиційною системою DNS. Ця стійкість ґрунтується на трьох основних принципах:

- *Відсутність єдиного суб'єкта управління:* У Handshake немає централізованого органу, який може контролювати або блокувати домени. Це робить цензуру контенту значно складнішою для урядів та інших організацій;
- *Захист Блокчейном:* Записи в Handshake зберігаються на блокчейні, що робить їх стійкими до несанкціонованих змін. Це практично унеможливлює модифікацію доменних імен як наслідок рішень тих чи інших інстанцій;
- *Обхід DNS ієрархії в запитах:* Оскільки на відміну від DNS Handshake не використовує ієрархічну структуру запитів, виявлення та відфільтровування цих запитів значно ускладнюється. Іншими словами, оскільки Handshake домени не використовують рекурсивні резолвери, ті не можуть впливати на процес.

Втім, важливо розуміти, що цензура та фільтрування запитів — не завжди є негативним явищем [15], [16]. Відсутність централізованого контролю в Handshake несе певні недоліки, які можуть мати негативний вплив на безпеку та доступність інформації:

- *Відсутність моніторингу та аудиту:* Через відсутність централізованого контролю стає складніше відстежувати та видаляти шкідливий контент з Handshake. Це може призвести до зростання кількості фішингових сайтів, сайтів з нелегальним або шкідливим контентом, тощо. Цей недолік стосується як зовнішнього виявлення шкідливих доменів (на рівні ISP чи моніторингових компаній як, наприклад, Netcraft) так і локального (антивіруси, фаєрволи);
- *Складність блокування шкідливих доменів:* Користувачам може бути складно самостійно блокувати шкідливі домени в Handshake. Як приклад, при виявлення шкідливого доменного імені в DNS, користувач може знайти

відповідного Регістратора шляхом використання Whois (системи, яка дозволяє отримувати реєстраційні деталі про домен), повідомити про проблему і призвести до блокування ресурсу. Оскільки система Handshake робить сильний нахил на анонімність і відсутність централізації, для пересічних користувачів ускладнюється процес виявлення інстанції, відповідальної за безпеку мережі, у разі необхідності повідомлення про проблему.

Handshake все ще перебуває на стадії розробки, і його довгострокові наслідки для свободи слова, безпеки та інших аспектів Інтернету ще невідомі. Враховуючи загальні тренди підвищення конфіденційності та децентралізації Інтернету як явища, можна очікувати на появу нових методів та інструментів для моніторингу та аудиту контенту в Handshake, а також для блокування шкідливих доменів.

Доступність та володіння

Традиційний ринок доменних імен має ряд проблем, пов'язаних з доступністю та володінням доменами:

- *Обмежена доступність популярних доменів:* Більшість коротких та запам'ятовуваних доменних імен у популярних зонах вже зайняті. Це ускладнює пошук вдалого домену для нових компаній та проектів;
- *«Доменний сквоттинг»:* Деякі користувачі реєструють домени виключно з метою їх подальшого перепродажу за вищою ціною. Це явище хоч і є природним для такого ринку, все ж обмежує пул доступних доменів;
- *Монополізація і високі ціни:* Ціни на популярні домени можуть досягати значних сум, що робить їх недоступними для малих бізнесів та стартапів. Також користувачі не мають можливості отримати доменні імена напряму від TLD-операторів, і натомість вимушені користуватись послугами Реєстраторів, що природньо збільшує ціну.

Станом на Q3 2023 року, існує понад 359.8 мільйонів зареєстрованих доменних імен другого рівня, з яких 172.7 мільйона належать до .COM та .NET [17]. Згідно з публічною статистикою, 10 найпопулярніших Реєстраторів контролюють близько 168 мільйонів доменів. Це зокрема свідчить про те, що більшість коротких та зручних доменних імен вже зайняті. Внаслідок цього, використання доменів як елемента брендингу стає складнішим, а короткі доменні імена виставляються на аукціони за непідйомними для багатьох цінами.

Натомість Handshake використовує систему аукціонів для володіння доменами і пропонує унікальну можливість створювати власні доменні зони верхнього рівня (TLD) [18]. Це вирішує багато проблем традиційного ринку доменних імен: ширший пул потенційних імен, зниження доменного сквоттингу, доступні ціни. Це відкриває нові можливості для брендингу та маркетингу, адже компанії можуть використовувати персоналізовані домени, які краще відображають їх діяльність або бренд.

Для кращого розуміння популярності Handshake доменів, проведемо порівняння загальної кількості реєстрацій в мережі Namebase (один із провайдерів HNS-Handshake доменів) та загальної кількості доменів у портфоліо Namecheap Inc., який є другим за розміром Реєстратором у світі (рис. 3):

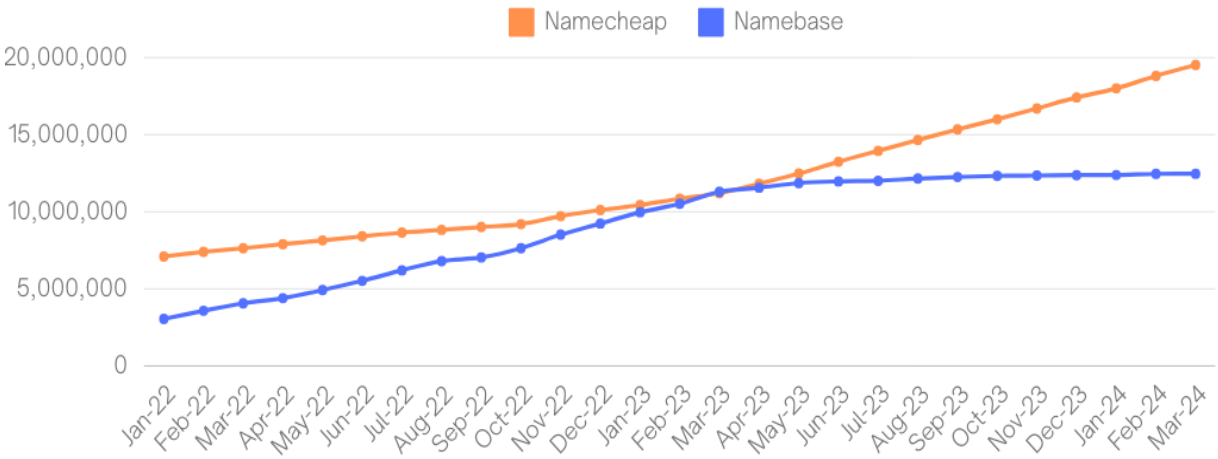

Рис. 3. Порівняння кількості реєстрацій між Namecheap та Namebase

Згідно зі статистикою, наведеною на веб-сторінці Namebase [19], а також інформацією з ресурсу Domain Name Stat [20], тренд на Handshake-домени почав стрімко зростати, сягаючи 12.5 млн доменів у квітні 2024 року у порівняні з 3 млн доменів у січні 2022 року, в той час як приріст в портфоліо Namecheap відбувся з 7 млн доменів у січні 2022 року до 19.5 млн в квітні 2024 року. Іншими словами, за період в два роки, кількість доменів в мережі HNS збільшилась на ~316.6%, в той час як в компанії Namecheap — на ~178.57%. Безперечно, на загальну кількість реєстрації впливає багато різних факторів: ціни, маркетинг, глобальні тренди, тощо. Скажімо, важливим фактором, який прослідковується на графіку, став тренд на децентралізацію та Web3 в період 2022–2023, які тісно пов'язані з природою Handshake-доменів. Втім, враховуючи загальні тренди реєстрацій, можна підсумувати, що мережа Handshake продовжує набирає значної популярності серед користувачів.

Корпоративний досвід

Handshake пропонує унікальну можливість для корпоративного використання доменів: створення доменів, які використовуються лише в межах корпоративної мережі. Це має ряд переваг:

- *Зменшення поверхні атаки:* Внутрішні домени Handshake не доступні ззовні, що значно зменшує ризик кібератак;
- *Захист конфіденційності:* Випадкові витоки конфіденційних внутрішніх доменів ускладнюється;
- *Цінність для компаній у регіонах з суворим регулюванням:* Handshake домени можуть використовуватися для створення безпечних та захищених від цензури веб-сайтів, що актуально для компаній, які працюють в таких умовах;
- *Внутрішні комунікаційні інструменти:* Handshake домени можуть використовуватися для створення прихованих внутрішніх комунікаційних інструментів.

Використання Handshake доменів разом з внутрішніми центрами сертифікації (CA) значно підвищує рівень безпеки для корпоративних мереж. Це ускладнює для зловмисників імітацію внутрішніх сайтів, використовуючи фальшиві сертифікати, оскільки Handshake домени можуть бути сертифіковані лише авторизованими внутрішніми CA. Такий підхід підвищує довіру користувачів, які можуть бути впевнені в автентичності внутрішніх сайтів, захищених надійними сертифікатами. Ця комбінація

технологій також захищає від атак типу «людина посередині», оскільки сертифікати підтверджують зв'язок між доменом та внутрішнім CA, унеможливлюючи перехоплення трафіку зловмисниками. В цілому, поєднання Handshake доменів з внутрішніми CA створює багаторівневу систему захисту, яка робить корпоративні мережі значно стійкішими до кібератак.

Втім, наразі Handshake домени мають певні недоліки, які можуть обмежувати їх широке корпоративне впровадження. Екосистема Handshake все ще перебуває на стадії розвитку і не має достатнього поширення та зрілості, що може бути неприйнятним ризиком для великих корпорацій. Використання Handshake доменів може призвести до залежності від менш розвиненої екосистеми, що може не відповідати потребам та очікуванням великих підприємств. Також, зв'язок Handshake з децентралізованими мережами може мати негативний або позитивний вплив на імідж компанії, залежно від її галузі. Децентралізовані технології можуть асоціюватися з інноваціями, безпекою та конфіденційністю, що може бути вигідним для деяких компаній. З іншого боку, децентралізовані мережі також можуть асоціюватися з анонімністю, незаконною діяльністю та кіберзлочинністю, що може зашкодити іміджу деяких компаній.

Правові та податкові наслідки використання Handshake доменів для певних видів діяльності також все ще нечіткі. Компаніям важливо ретельно вивчити всі аспекти регулювання перед прийняттям рішення про використання Handshake. Чітке розуміння правових та податкових наслідків використання Handshake доменів має вирішальне значення для забезпечення законності та безпеки діяльності компанії.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Дослідження виявило, що Handshake, як децентралізована система доменних імен, пропонує ряд переваг порівняно з традиційною DNS. Зокрема, це підвищена безпека за рахунок потенціалу до інновацій, стійкість до цензури та більш гнучка система реєстрації та володіння доменами. Також перспективним є використання Handshake для корпоративних мереж, забезпечуючи захист від витоків конфіденційних даних та підвищуючи рівень безпеки за рахунок використання внутрішніх доменів та центрів сертифікації.

Однак Handshake, як порівняно нова технологія, має свої обмеження. Обмежене поширення та необхідність спеціального програмного забезпечення можуть стримувати його широке впровадження, особливо серед корпоративних користувачів. Крім того, відсутність централізованого контролю може створювати певні ризики, пов'язані з можливістю зловживань та поширенням шкідливого контенту. Обмежений обсяг даних та відсутність довгострокових досліджень впливу протоколу Handshake ускладнюють остаточні твердження щодо його переваг та недоліків. У табл. 2 відображено переваги та недоліки DNS та Handshake в залежності від вимог користувачів до даних сервісів.

Таблиця 2

Порівняння переваг і недоліків DNS та Handshake

Підхід до сервісу	DNS		Handshake	
	Переваги	**Недоліки**	**Переваги**	**Недоліки**
Кібербезпека	Розвиток протоколів DNSSEC, DoT/DoH/DoQ Налагоджені аналітичні засоби; прозорість протоколу	Обмежений потенціал для інновацій; відсутність вбудованого шифрування; вразливість до кібератак (DDoS, DNS cache poisoning, DNS spoofing)	Можливість наскрізного шифрування; високий потенціал для інновацій; можливість використання альтернативних протоколів передачі даних	Вразливість до атак, притаманних Блокчейн-системам; відсутність довгострокових досліджень протоколу
Цензура	Прозорість ієрархії полегшує блокування шкідливих доменів	Можливість блокування доступу до соціально значимої інформації	Анонімність власників доменних імен; ускладнене блокування імен з метою цензури	Ускладнені моніторинг та аудит мереж; складність блокування шкідливих доменів
Доступність доменних імен	Простий та прозорий процес реєстрації; ціни стабілізовані контролюючими органами	Обмежений пул доступних доменів; простір для доменного сквотингу; монополізація цін	Можливість створювати домени верхнього рівня; практично необмежений пул імен	Немає на даному етапі розвитку протоколу
Корпоративний досвід	Зменшені репутаційні ризики; зрілість інфраструктури	Великий вектор атак за рахунок вразливостей протоколу	Створення імен що існують лише локально; обхід блокувань місцевих влад	Збільшені репутаційні та технічні ризики за рахунок іноваційності протоколу
Технічні аспекти для звичайних користувачів	Невидимість роботи протоколу; нативна інтеграція в більшості пристроїв	Немає на даному етапі розвитку протоколу	Немає на даному етапі розвитку протоколу	Вимагає спеціального програмного забезпечення

Подальші дослідження Handshake мають зосередитися на кількох ключових напрямках:

- *Handshake та Інтернет речей (IoT):* Вивчення можливостей використання Handshake доменів для покращення безпеки та управління великою кількістю пристроїв IoT;
- *Нові методи шифрування:* Дослідження потенціалу Handshake для підтримки нових, більш безпечних та стійких до стеження методів шифрування;
- *Вплив на ринок доменних імен:* Аналіз довгострокового впливу Handshake на ринок доменних імен, включаючи ціни, доступність та конкуренцію.

- *Соціальні та економічні наслідки:* Вивчення соціальних та економічних наслідків впровадження Handshake, включаючи питання свободи слова, доступу до інформації та економічного розвитку.

Загалом, Handshake представляє собою перспективну альтернативу традиційній DNS, яка має потенціал змінити підхід до управління доменними іменами та підвищити безпеку та стійкість Інтернету. Проте, для повного розкриття його потенціалу необхідні подальші дослідження та розробки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Dooley, M., & Rooney, T. (2017). Introduction to the Domain Name System (DNS). *Cryptography and Network Security (7th ed.),* 29–55. https://doi.org/10.1002/9781119328292.ch2
2. Namebase Learning Center. Seattle: Namebase. (2023). *About Handshake*. https://learn.namebase.io/about-handshake/about-handshake
3. Ahmad, K. (2022). *What's the Difference Between HNS, ENS, & Unstoppable Domains?* MakeUseOf. https://www.makeuseof.com/whats-the-difference-between-hns-ens-unstoppable-domains/
4. Postel, J. (1994). *Domain Name System Structure and Delegation*. https://www.rfc-editor.org/rfc/rfc1591.html
5. Cloudflare. (n. d.). What is DNS? https://www.cloudflare.com/learning/dns/what-is-dns/
6. Rajendran, B., & Palaniappan, D. A. (2022). Universal Domain Name Resolution Service – Need and Challenges - Study on Blockchain Based Naming Services. *IEEE Region 10 Symposium (TENSYMP).* https://doi.org/10.1109/TENSYMP54529.2022.9864361
7. Nemkova, O. A., & Pavlyuk, O. Yu. O. YU. (2024). Browser Extension Based on QUIC and RDAP: Fast and Convenient Access to Decentralized Handshake Domains. *Issue 86: Proceedings of the International Scientific Conference*, 40-43.
8. Gañán, C. H. (2021). WHOIS sunset? A primer in Registration Data Access Protocol (RDAP) performance. *14th IFIP*, 72–87. https://doi.org/78-3-903176-40-9
9. Graham-Cumming, J. (2020). *Cloudflare outage on July 17, 2020.* Cloudflare Blog. https://blog.cloudflare.com/cloudflare-outage-on-july-17-2020
10. Hounsel, A., Borgolte, K., Schmitt, P., Holland, J., & Feamster, N. (2019). Analyzing the costs (and benefits) of DNS, DoT, and DoH for the modern web. *Proceedings of the Applied Networking Research Workshop (ANRW '19),* 20–22. https://doi.org/10.1145/3340301.3341129
11. Lowe, G., Winters, P., & Marcus, M. L. (2007). *The Great DNS Wall of China.* https://censorbib.nymity.ch/pdf/Lowe2007a.pdf
12. Li, J., et al. (2018). Can We Learn what People are Doing from Raw DNS Queries? *IEEE INFOCOM 2018 - IEEE Conference on Computer Communications,* 2240–2248. https://doi.org/10.1109/INFOCOM.2018.8486210
13. *FCC Settles Verizon "Supercookie" Probe, Requires Consumer Opt-In for Third Parties. Federal Communications Commission.* (n. d.). https://www.fcc.gov/document/fcc-settles-verizon-supercookie-probe
14. Koch, R. (2018). *State censorship is on the rise.* https://protonvpn.com/blog/global-censorship
15. Afonso, J., & Veiga, P. (2008). Protecting the DNS infrastructure of a top level domain: Real-time monitoring with network sensors. *5th IEEE International Conference on Mobile Ad Hoc and Sensor Systems*, 873–879. https://doi.org/10.1109/MAHSS.2008.4660136
16. Yan, G., Li, Q., Guo, D., & Meng, X. (2020). Discovering Suspicious APT Behaviors by Analyzing DNS Activities. *Sensors, 20,* 731. https://doi.org/10.3390/s20030731
17. *The Domain Name Industry Brief Quarterly Report*. (n. d.). https://dnib.com/articles/the-domain-name-industry-brief-q4-2023
18. *Name minting auction. Namebase Learning Center.* (n. d.). https://learn.namebase.io/about-handshake/handshake-auction
19. Namebase. (n. d.). *Handshake Usage Statistics.* https://www.namebase.io/stats/#usage
20. *Namecheap, Inc. Domain Name Stat.* (n. d.). https://domainnamestat.com/statistics/registrar/NameCheap_Inc_-IANA_ID-1068

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (25), 2024
ISSN 2663 - 4023

Olena Niemkova
Doctor of Sciences, Professor, Professor of the Department of Information Technology Security department
Lviv Polytechnic National University, Lviv, Ukraine
ORCID ID: 0000-0003-0690-2657
olena.a.niemkova@lpnu.ua

Oleksand-Iurii Pavliuk
Postgraduate student of Information Technology Security department
Lviv Polytechnic National University, Lviv, Ukraine
ORCID ID: 0009-0008-6985-203X
oleksandr-iurii.s.pavliuk@lpnu.ua

FEASIBILITY OF USING HANDSHAKE DOMAIN NAMES IN COMPARISON WITH THE CLASSIC DNS

Abstract. One of the key structures in the modern Internet is the Domain Name System (DNS). Its role is to convert machine IP addresses into a human-friendly domain format. Since the system was not originally designed for global use, a number of shortcomings appeared during its popularization, particularly related to cyber security: accessibility and privacy. System publicity and hierarchy are often misused with censorship purposes. This article discusses the feasibility of using an alternative decentralized protocol called Handshake. It departs from the traditional hierarchical DNS in the context of registrations, ownership and control of domain names through the use of Blockchain distributed ledger technology. This change makes the structure decentralized, however, a number of disadvantages arise at the same time. Handshake domains require a special approach for their use by ordinary users and introduce reputational and technology risks. The article analyzes the technical differences between Handshake and DNS, including the structure, domain registration, and resolution mechanism. The impact of these differences on user experience, security, censorship, availability, and domain ownership is discussed. The trends of Handshake and traditional domain name registrations are studied, which demonstrates the rapid growth of the former's popularity. Handshake's potential for corporate use is highlighted separately, in particular for reducing the risk of leakage of internal domain names, as well as strengthening cyber security through the use of internal certification centers. Limitations of the Handshake protocol are identified and directions for further research are outlined. A comparative study revealed that the advantages of the Handshake protocol are related to the anonymity of the owners of the respective domain names, the difficulty of blocking them, as well as the provided space for innovation. On the other hand, DNS is significantly superior in ease of use, reliability, maturity, support by existing software, and reduced reputational risks.

Keywords: Domain Name System; DNS; Handshake; Blockchain; decentralization; cyber security; confidentiality; anonymity; censorship.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Dooley, M., & Rooney, T. (2017). Introduction to the Domain Name System (DNS). *Cryptography and Network Security (7th ed.),* 29–55. https://doi.org/10.1002/9781119328292.ch2
2. Namebase Learning Center. Seattle: Namebase. (2023). *About Handshake*. https://learn.namebase.io/about-handshake/about-handshake
3. Ahmad, K. (2022). *What's the Difference Between HNS, ENS, & Unstoppable Domains?* MakeUseOf. https://www.makeuseof.com/whats-the-difference-between-hns-ens-unstoppable-domains/
4. Postel, J. (1994). *Domain Name System Structure and Delegation*. https://www.rfc-editor.org/rfc/rfc1591.html
5. Cloudflare. (n. d.). What is DNS? https://www.cloudflare.com/learning/dns/what-is-dns/
6. Rajendran, B., & Palaniappan, D. A. (2022). Universal Domain Name Resolution Service – Need and Challenges - Study on Blockchain Based Naming Services. *IEEE Region 10 Symposium (TENSYMP).* https://doi.org/10.1109/TENSYMP54529.2022.9864361

7. Nemkova, O. A., & Pavlyuk, O. Yu. O. YU. (2024). Browser Extension Based on QUIC and RDAP: Fast and Convenient Access to Decentralized Handshake Domains. *Issue 86: Proceedings of the International Scientific Conference*, 40-43.
8. Gañán, C. H. (2021). WHOIS sunset? A primer in Registration Data Access Protocol (RDAP) performance. *14th IFIP*, 72–87. https://doi.org/78-3-903176-40-9
9. Graham-Cumming, J. (2020). *Cloudflare outage on July 17, 2020.* Cloudflare Blog. https://blog.cloudflare.com/cloudflare-outage-on-july-17-2020
10. Hounsel, A., Borgolte, K., Schmitt, P., Holland, J., & Feamster, N. (2019). Analyzing the costs (and benefits) of DNS, DoT, and DoH for the modern web. *Proceedings of the Applied Networking Research Workshop (ANRW '19),* 20–22. https://doi.org/10.1145/3340301.3341129
11. Lowe, G., Winters, P., & Marcus, M. L. (2007). *The Great DNS Wall of China.* https://censorbib.nymity.ch/pdf/Lowe2007a.pdf
12. Li, J., et al. (2018). Can We Learn what People are Doing from Raw DNS Queries? *IEEE INFOCOM 2018 - IEEE Conference on Computer Communications,* 2240–2248. https://doi.org/10.1109/INFOCOM.2018.8486210
13. *FCC Settles Verizon "Supercookie" Probe, Requires Consumer Opt-In for Third Parties. Federal Communications Commission.* (n. d.). https://www.fcc.gov/document/fcc-settles-verizon-supercookie-probe
14. Koch, R. (2018). *State censorship is on the rise.* https://protonvpn.com/blog/global-censorship
15. Afonso, J., & Veiga, P. (2008). Protecting the DNS infrastructure of a top level domain: Real-time monitoring with network sensors. *5th IEEE International Conference on Mobile Ad Hoc and Sensor Systems,* 873–879. https://doi.org/10.1109/MAHSS.2008.4660136
16. Yan, G., Li, Q., Guo, D., & Meng, X. (2020). Discovering Suspicious APT Behaviors by Analyzing DNS Activities. *Sensors, 20,* 731. https://doi.org/10.3390/s20030731
17. *The Domain Name Industry Brief Quarterly Report*. (n. d.). https://dnib.com/articles/the-domain-name-industry-brief-q4-2023
18. *Name minting auction. Namebase Learning Center.* (n. d.). https://learn.namebase.io/about-handshake/handshake-auction
19. Namebase. (n. d.). *Handshake Usage Statistics.* https://www.namebase.io/stats/#usage
20. *Namecheap, Inc. Domain Name Stat.* (n. d.). https://domainnamestat.com/statistics/registrar/NameCheap_Inc_-IANA_ID-1068