ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА СИСТЕМ ТА ТЕХНОЛОГІЙ КІБЕРБЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Технологія запобігання DDOS атакам на основі рішення ENS»

зі спеціальності *125* Кібербезпека та захист інформації
(код, найменування спеціальності)

освітньо-професійної програми *Інформаційна та кібернетична безпека*
(назва програми)

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ Когут Дмитро
(підпис)

Виконав: здобувач вищої освіти групи БСДМ-63
Когут Дмитро
(прізвище, ім'я)

Керівник д.ф., доцент Собчук А.В.
(науковий ступінь, вчене звання, прізвище, ім'я)

Рецензент _____
(науковий ступінь, вчене звання, прізвище, ім'я)

Київ 2025

ВСТУП

Актуальність дослідження. Традиційний підхід до забезпечення кібербезпеки, який передбачав розміщення інфраструктури, сервісів та даних у межах контрольованого корпоративного периметра, перестає відповідати реаліям сучасного Інтернету. Цифрова трансформація, масове використання хмарних платформ, впровадження розподілених сервісів та зростання залежності від онлайн-комунікацій суттєво змінили архітектуру мережевої взаємодії. Одночасно загострюються кіберзагрози, зокрема DDoS-атаки, які стають дедалі складнішими й масштабнішими завдяки появі ботнетів на базі IoT, використанню вразливих серверів та хмарних інструментів для генерації шкідливого трафіку.

У цих умовах централізовані інфраструктурні рішення, зокрема система доменних імен DNS, демонструють суттєві обмеження. DNS залишається критичною точкою відмови, що може бути легко атакована зловмисниками. Атаки на резолюцію імен здатні повністю вивести вебресурс із ладу незалежно від його продуктивності чи захищеності. Саме тому традиційна «точкова» модель захисту — брандмауери, системи запобігання вторгнень, CDN, Anycast-маршрутизація чи хмарні scrubbing-центри — вже не забезпечує належного рівня стійкості до DDoS-атак, оскільки не усуває фундаментальної проблеми централізації.

На цьому тлі все більшого значення набувають децентралізовані мережеві технології, зокрема ENS (Ethereum Name Service) та IPFS (InterPlanetary File System). ENS пропонує альтернативний підхід до доменної резолюції, у якому записи зберігаються не на серверах, а у блокчейні, що гарантує їх незмінність і відсутність централізованих точок відмови. IPFS забезпечує розподілене зберігання вебконтенту, усуваючи необхідність у традиційному хостингу. Разом ENS+IPFS формують архітектуру, стійку до DDoS не за рахунок зміцнення периметра, а за рахунок усунення периметра як такого.

Вищезазначене визначає актуальність теми даної магістерської роботи, основний зміст якої присвячено дослідженню можливостей децентралізованих технологій як

сучасних засобів протидії DDoS-атакам та підвищення доступності мережевих сервісів.

Об'єкт дослідження - забезпечення стійкості та доступності вебресурсів в умовах DDoS-атак.

Предмет дослідження - технології децентралізованої адресації та розподіленого зберігання (ENS і IPFS) як засіб протидії DDoS-атакам.

Мета роботи - розробити та обґрунтувати порядок застосування технологій ENS+IPFS для підвищення стійкості вебресурсів до DDoS-атак та сформувати практичні рекомендації щодо їх впровадження.

Наукові завдання роботи:

дослідити сутність, природу та класифікацію DDoS-атак;

проаналізувати традиційні підходи до захисту та визначити їхні структурні обмеження;

дослідити механізми роботи ENS і IPFS та особливості їх інтеграції;

провести порівняльний аналіз централізованої моделі DNS та децентралізованої ENS+IPFS;

здійснити моделювання поведінки обох архітектур під час DDoS-навантаження;

визначити ефективність ENS+IPFS як засобу підвищення доступності вебресурсів;

сформувати практичні рекомендації для впровадження децентралізованих технологій у корпоративних системах.

Методи дослідження - Методологічну основу роботи становить комплекс підходів, що забезпечують всебічне вивчення проблеми стійкості вебресурсів до DDoS-атак та оцінку потенціалу децентралізованих технологій ENS і IPFS. У дослідженні застосовано метод опрацювання наукової літератури та технічної документації, що дозволило систематизувати сучасні теоретичні підходи до захисту інформаційних систем і проаналізувати архітектурні особливості DNS, ENS та IPFS. Системний аналіз використовувався для дослідження взаємозв'язків між компонентами централізованих і децентралізованих мережевих інфраструктур та

для виявлення структурних вразливостей, які можуть бути використані під час DDoS-атак. Контент-аналіз специфікацій ENS і IPFS дав змогу визначити їхні функціональні можливості, механізми взаємодії та особливості реалізації в реальних умовах. Застосування експериментального методу передбачало моделювання DDoS-навантаження на традиційну DNS-інфраструктуру та децентралізовану модель ENS+IPFS, що дозволило отримати порівняльні практичні результати. Порівняльний аналіз використовувався для оцінки ефективності кожної архітектури на основі показників стійкості, доступності, відмовостійкості та можливості протидії зовнішньому навантаженню.

Практичне значення одержаних результатів - Практичне значення проведеного дослідження полягає у формуванні обґрунтованого підходу до впровадження технологій ENS та IPFS у корпоративних та державних інформаційних системах з метою підвищення їхньої стійкості до DDoS-атак. Результати роботи демонструють, що використання децентралізованої моделі адресації та розподіленого зберігання контенту дозволяє усунути ключові структурні вразливості, характерні для DNS, і забезпечити доступність вебресурсів навіть у разі інтенсивного шкідливого трафіку. У роботі розроблено практичні рекомендації щодо налаштування ENS-доменів, інтеграції IPFS, публікації вебресурсів у децентралізованому середовищі та організації інфраструктури для підвищення відмовостійкості. Отримані результати можуть бути використані фахівцями з кібербезпеки, адміністраторами мережевих систем і розробниками Web3-рішень для створення стійких до DDoS інтернет-сервісів, захисту критичних електронних платформ та впровадження сучасних децентралізованих технологій в організаціях різного масштабу.

Результати кваліфікаційної роботи апробовані на Всеукраїнській науковій конференції «Актуальні проблеми кібербезпеки», яка відбулася 29 жовтня 2025 року в Державному університеті інформаційно-комунікаційних технологій, м. Київ.

1 ДОСЛІДЖЕННЯ ПРОБЛЕМИ ЗАХИСТУ ВІД АТАК З ВИКОРИСТАННЯМ ЦЕНТРАЛІЗОВАНИХ І ДЕЦЕНТРАЛІЗОВАНИХ МЕРЕЖЕВИХ ТЕХНОЛОГІЙ

1.1. Сутність, історія розвитку та класифікація DDoS-атак

Distributed Denial of Service (DDoS) є одним із найпоширеніших і водночас найнебезпечніших типів кібератак, основною метою яких є порушення доступності мережевих ресурсів, сервісів або цілих інформаційних інфраструктур. На відміну від атак, спрямованих на порушення конфіденційності або цілісності даних, DDoS-атаки орієнтовані на компонент доступності (availability), який є критичним для безперервного функціонування сучасних цифрових сервісів. Атака реалізується шляхом створення надмірного навантаження на мережеві канали, обчислювальні ресурси або програмні компоненти цільової системи, а також шляхом експлуатації особливостей і вразливостей мережевих протоколів.

Ключовою відмінністю DDoS-атак від класичних локальних DoS-атак є їх розподілений характер. Джерелами шкідливого трафіку виступає велика кількість географічно та логічно розподілених вузлів, які можуть включати скомпрометовані персональні комп’ютери, сервери, хмарні інстанси, проксі-сервери, а також різноманітні IoT-пристрої з низьким рівнем захисту. Така архітектура атаки значно ускладнює ідентифікацію справжнього ініціатора, обмежує можливості фільтрації трафіку за джерелами та знижує ефективність традиційних засобів блокування. Унаслідок цього DDoS-атаки залишаються однією з найскладніших загроз для сучасних мережевих систем.

Історичний розвиток DDoS-атак тісно пов’язаний з еволюцією Інтернету та зростанням доступності обчислювальних і мережевих ресурсів. Перші масові DDoS-інциденти, зафіксовані наприкінці 1990-х років, використовували відносно прості ботнети, сформовані зі зламаних робочих станцій і серверів. Ці атаки були

обмежені за масштабами, однак уже тоді продемонстрували високу ефективність проти централізованих вебресурсів. Упродовж 2000-х років DDoS-атаки почали активно застосовуватися як інструмент політичного тиску, конкурентної боротьби та саботажу комерційних сервісів. Саме в цей період відбулися перші резонансні атаки на великі пошукові системи, платформи електронної комерції та платіжні сервіси.

Подальший розвиток широкосмугового доступу до Інтернету, поява високошвидкісних каналів зв'язку та стрімке зростання кількості підключених пристроїв призвели до якісного стрибка в еволюції DDoS-загроз. Зловмисники отримали можливість формувати масштабні ботнети, керовані через централізовані або розподілені канали командного управління. Окремим етапом стала поява атак з використанням механізмів відбиття та ампліфікації, які дозволяють багаторазово збільшувати обсяг трафіку, спрямованого на жертву, без пропорційного зростання ресурсів атакуючої сторони. Критичний вплив на еволюцію DDoS-атак мав розвиток ринку IoT-пристроїв, які часто постачаються з типовими обліковими даними та мінімальними засобами захисту. Атаки ботнету Mirai у 2016 році продемонстрували, що мільйони побутових пристроїв можуть бути використані для виведення з ладу ключових елементів глобальної інтернет-інфраструктури.

Упродовж останнього десятиліття чітко простежується тенденція до багатовекторності DDoS-атак. Зловмисники все рідше обмежуються одним типом навантаження, натомість комбінують атаки на пропускну здатність, протокольний рівень і рівень застосунків. Такий підхід ускладнює виявлення та реагування, оскільки кожен клас атак потребує окремих механізмів захисту та аналізу. Мотивація проведення DDoS-кампаній також суттєво розширилася і включає фінансове вимагання, політичні та ідеологічні акції, конкурентну боротьбу, прикриття інших кібератак, а також тестування можливостей ботнетів. Поява моделей DDoS-as-a-Service знизила поріг входу для організації атак і зробила їх доступними навіть для осіб без глибоких технічних знань.

Класифікація DDoS-атак зазвичай ґрунтується на рівнях моделі OSI та механізмах впливу на цільову систему. Атаки на пропускну здатність спрямовані на

перевантаження мережевих каналів або мережевого обладнання шляхом генерації великих обсягів трафіку. До цього класу належать UDP-флуди, ICMP-флуди, а також атаки відбиття та ампліфікації з використанням відкритих сервісів, таких як DNS, NTP або Memcached. Протокольні атаки зосереджені на виснаженні ресурсів мережевих стеків і механізмів керування з'єднаннями, зокрема через масові SYN-запити або маніпуляції з TCP-пакетами. Атаки на рівні застосунків є найбільш складними для виявлення, оскільки імітують легітимну поведінку користувачів і спрямовані на ресурсоємні операції, такі як обробка HTTP-запитів, робота з базами даних або встановлення захищених з'єднань.

Таблиця 1.1

Класифікація DDoS-атак за рівнем реалізації та механізмом впливу

Клас DDoS-атак	Рівень моделі OSI	Основний механізм впливу	Типові приклади атак	Основні наслідки для цільової системи
Атаки на пропускну здатність (Volumetric attacks)	Мережевий рівень (L3–L4)	Генерація надмірного обсягу трафіку з метою перевантаження каналів зв'язку або мережевого обладнання	UDP flood, ICMP flood, DNS amplification, NTP amplification, Memcached amplification	Вичерпання пропускної здатності каналу, недоступність сервісу для легітимних користувачів, повна відмова в обслуговуванні
Протокольні атаки (Protocol attacks)	Транспортний рівень (L4)	Виснаження ресурсів мережевих стеків шляхом зловживання механізмами встановлення та обробки з'єднань	SYN flood, ACK flood, TCP state exhaustion, fragmented packet attacks	Перевантаження мережевого обладнання або ОС, неможливість обробки нових з'єднань
Атаки на рівні застосунків (Application layer attacks)	Прикладний рівень (L7)	Імітація легітимних запитів для навантаження серверної логіки	HTTP GET/POST flood, Slowloris, Slow HTTP	Значне зростання часу відповіді, помилки сервера

Продовження таблиці 1.1

Класифікація DDoS-атак за рівнем реалізації та механізмом впливу

Клас DDoS-атак	Рівень моделі OSI	Основний механізм впливу	Типові приклади атак	Основні наслідки для цільової системи
Атаки відбиття та ампліфікації	Мережевий рівень (L3–L4)	Використання сторонніх серверів для відбиття та багаторазового збільшення трафіку на жертву	DNS reflection, NTP reflection, SSDP reflection	Масштабні перевантаження інфраструктури без значних витрат ресурсів з боку атакуючого
Багатовекторні DDoS-атаки	Кілька рівнів OSI	Одночасне поєднання volumetric, протокольних і прикладних атак	Комбіновані атаки UDP flood + HTTP flood	Ускладнення виявлення та реагування, швидка деградація систем захисту
Багатовекторні DDoS-атаки	Кілька рівнів OSI	Одночасне поєднання volumetric, протокольних і прикладних атак	Комбіновані атаки UDP flood + HTTP flood	Ускладнення виявлення та реагування, швидка деградація систем захисту
Атаки з використанням ботнетів IoT	Мережевий і транспортний рівні	Залучення великої кількості слабко захищених IoT-пристроїв	Mirai, Mozi, Bashlite	Надзвичайно високий обсяг трафіку, складність блокування через розподіленість джерел

Наслідки DDoS-атак проявляються у зниженні доступності сервісів, зростанні латентності, збільшенні кількості помилок, прямих фінансових втратах і суттєвих репутаційних ризиках для організацій. У багатьох випадках DDoS-атаки використовуються як відволікаючий маневр для проведення інших злочинних дій, зокрема проникнення в систему або викрадення конфіденційної інформації.

Сучасні тенденції розвитку загроз включають подальше зростання інтенсивності атак, активне використання зашифрованого трафіку та ускладнення фільтрації через поширення HTTPS і QUIC.

Підсумовуючи, DDoS-атаки є динамічною та еволюційною загрозою, що змінюється разом із розвитком мережевих технологій і моделей розміщення обчислювальних ресурсів. Усвідомлення їх сутності, історії розвитку та класифікації є необхідною передумовою для формування ефективних стратегій захисту. Саме обмеження традиційних централізованих підходів до забезпечення доступності зумовлюють потребу в дослідженні альтернативних архітектур, зокрема децентралізованих рішень на основі ENS та IPFS, які розглядаються в наступних розділах цієї роботи.

1.2. Понятійно-категоріальний апарат та методи дослідження мережевих атак

Для ґрунтовного дослідження проблематики DDoS-атак і розроблення ефективних підходів до їх запобігання принципово важливим є формування чіткого та узгодженого понятійно-категоріального апарату. Використання коректної термінології забезпечує логічну цілісність дослідження, точність наукових формулювань і можливість однозначного трактування результатів. У сфері кібербезпеки навіть незначні термінологічні неточності можуть призводити до помилкового розуміння механізмів атак, неправильного вибору методів аналізу та неефективних рішень щодо побудови систем захисту мережевої інфраструктури.

Одним із фундаментальних понять мережевих технологій є мережевий протокол, який визначається як формалізований набір правил і процедур, що регламентують формат, порядок і спосіб обміну даними між вузлами мережі. Протоколи транспортного та прикладного рівнів, зокрема TCP, UDP, ICMP, HTTP і DNS, формують основу функціонування Інтернету. Їхні архітектурні особливості безпосередньо впливають на характер DDoS-атак, оскільки саме на рівні протоколів

реалізуються механізми перевантаження мережевих ресурсів, маніпуляції з'єднаннями та відбиття трафіку. Аналіз логіки роботи протоколів дозволяє виявити слабкі місця, які можуть бути використані зловмисниками для масового генерування шкідливих запитів.

Важливим поняттям у контексті кібербезпеки є цілісність даних, що характеризує здатність інформації зберігатися та передаватися без несанкціонованих змін. Порушення цілісності може виникати не лише внаслідок прямого втручання в дані, але й у результаті складних багатовекторних атак, коли DDoS використовується як відволікаючий інструмент для здійснення інших кіберзлочинних дій, зокрема підміни контенту або компрометації систем. Забезпечення цілісності є критично важливим елементом комплексного підходу до захисту інформаційних ресурсів.

Автентифікація відіграє ключову роль у забезпеченні безпеки мережевих сервісів і полягає у перевірці достовірності джерела запиту або суб'єкта доступу. Відсутність або обмеженість механізмів автентифікації на рівні окремих мережевих протоколів, зокрема UDP та традиційної DNS-інфраструктури, створює передумови для підроблення запитів, спуфінгу та реалізації відбивних атак. Саме ці особливості активно використовуються під час організації масштабних DDoS-кампаній, що спрямовані на перевантаження серверів та порушення доступності сервісів.

З точки зору архітектури мереж принципове значення має розмежування між централізованими та розподіленими системами. Централізовані системи характеризуються концентрацією управління або ключових сервісів на обмеженій кількості вузлів, що формує критичні точки відмови. Класична система доменних імен DNS є типовим прикладом такої архітектури, оскільки процес резолюції доменних імен залежить від конкретних серверів і провайдерів. Натомість розподілені системи передбачають виконання функцій і зберігання даних на великій кількості незалежних вузлів, які взаємодіють між собою без єдиного центру управління. Відсутність централізованої точки відмови робить такі системи значно більш стійкими до DDoS-атак.

Окрему роль у дослідженні відіграє поняття адресації в мережі, яке визначає спосіб ідентифікації ресурсів і сервісів. Традиційна DNS-адресація базується на

ієрархічній моделі з авторитетними серверами, тоді як децентралізовані підходи, зокрема Ethereum Name Service, використовують криптографічно захищені записи, що зберігаються у блокчейні. У такій моделі адресація не залежить від фізичного розташування сервера і не може бути змінена або вилучена без участі власника приватного ключа, що суттєво підвищує стійкість до атак на рівні інфраструктури доступності.

У межах Web3-технологій важливого значення набувають поняття децентралізації, смарт-контракту, contenthash, CID, блокчейну та peer-to-peer архітектури. Децентралізація передбачає відсутність центрального органу управління та прийняття рішень мережею на основі механізмів консенсусу. Смарт-контракти реалізують програмну логіку роботи ENS і автоматично виконують задані правила без втручання третіх сторін. Contenthash використовується для зберігання посилань на IPFS-ресурси, тоді як CID є унікальним криптографічним ідентифікатором контенту, що дозволяє адресувати дані за їхнім вмістом, а не за місцем розташування. Блокчейн у цій моделі виконує роль розподіленого реєстру, який гарантує незмінність і достовірність записів, а peer-to-peer архітектура забезпечує відсутність централізованих серверів і підвищену стійкість до DDoS-атак.

Для дослідження мережевих атак і методів їх запобігання застосовується комплекс взаємодоповнювальних наукових методів. Системний аналіз дозволяє розглядати мережеву інфраструктуру як сукупність взаємопов’язаних компонентів і визначати критичні елементи, від яких залежить доступність сервісів. Контент-аналіз мережевих журналів і логів використовується для виявлення аномалій трафіку та характерних ознак DDoS-атак. Математичне моделювання дає змогу оцінити поведінку системи за умов пікових навантажень, прогнозувати деградацію ресурсів і визначати ефективність заходів захисту. Порівняльний аналіз інфраструктур, зокрема DNS і ENS, дозволяє виявити архітектурні відмінності, наявність або відсутність точок відмови та поведінку систем під час атак. Експериментальний метод, заснований на практичному моделюванні атак, забезпечує перевірку теоретичних висновків у наближених до реальності умовах.

Таким чином, формування чіткого понятійно-категоріального апарату та застосування комплексного набору методів дослідження створюють наукову основу для глибокого аналізу DDoS-атак і дозволяють обґрунтовано оцінити ефективність децентралізованих рішень на основі ENS та IPFS як перспективного напряму розвитку сучасних систем кіберзахисту.

1.3. Традиційні технології протидії DDoS-атакам та їх обмеження

На сучасному етапі розвитку кібербезпеки для протидії DDoS-атакам застосовується широкий спектр традиційних технологій, які історично сформувалися в межах централізованих мережевих архітектур. Основна ідея таких підходів полягає у виявленні, фільтрації або перенаправленні шкідливого трафіку, а також у підтриманні доступності сервісів шляхом балансування навантаження між окремими вузлами інфраструктури. Ці механізми широко використовуються у корпоративних і хмарних середовищах та вважаються стандартними засобами базового захисту. Водночас, незважаючи на їх значне поширення та ефективність у боротьбі з окремими типами загроз, традиційні технології мають низку системних обмежень, зумовлених самою природою централізованих систем, передусім наявністю єдиної або обмеженої кількості критичних точок відмови.

Одним із найбільш поширених підходів до протидії DDoS-атакам є фільтрація трафіку на рівні мережевого обладнання. Вона реалізується за допомогою списків контролю доступу, механізмів обмеження швидкості запитів, систем виявлення та запобігання вторгненням, а також міжмережевих екранів. Зазначені засоби дозволяють аналізувати пакети даних за заданими правилами, сигнатурами або поведінковими характеристиками і блокувати трафік, який визначається як підозрілий. Такий підхід є ефективним проти атак низької та середньої інтенсивності, однак у разі масованих volumetric-атак, коли обсяг шкідливого трафіку перевищує пропускну здатність каналів зв’язку, мережеве обладнання виявляється нездатним забезпечити належний рівень захисту. Крім того, агресивні

правила фільтрації нерідко призводять до блокування легітимних користувачів, що негативно впливає на доступність сервісу та знижує якість обслуговування.

Суттєвим обмеженням мережевих засобів захисту є їх безпосередня залежність від фізичних ресурсів обладнання. Маршрутизатори, комутатори та міжмережеві екрани мають обмежену обчислювальну потужність, фіксований обсяг оперативної пам’яті та кінцеву швидкість обробки мережевих пакетів. За умов інтенсивного потоку запитів ці ресурси швидко вичерпуються, що призводить до деградації продуктивності або повної відмови пристроїв. Додатковою проблемою є необхідність оперативного оновлення та адаптації правил фільтрації під час атаки, що в реальних умовах не завжди можливо забезпечити автоматизованими засобами без втручання адміністратора.

Окрему групу становлять заходи протидії DDoS-атакам на рівні інтернет-провайдерів. Провайдери можуть застосовувати очищення трафіку в спеціалізованих центрах, перенаправлення потоків у так звану «чорну діру», механізми формування та пріоритизації трафіку, а також фільтрацію маршрутів між автономними системами. Такі рішення здатні істотно зменшити навантаження на інфраструктуру клієнта у випадку надпотужних атак, однак вони також мають низку суттєвих недоліків. Застосування blackholing фактично означає повне відключення ресурсу від мережі, що робить його недоступним не лише для зловмисників, але й для легітимних користувачів. Використання центрів очищення трафіку потребує значних фінансових витрат і зазвичай є доступним лише для великих організацій, тоді як залучення сторонніх сервісів призводить до збільшення затримок у мережі та створює додаткові точки відмови.

Важливо також зазначити, що заходи захисту на рівні провайдера не забезпечують комплексної безпеки доменної інфраструктури. DNS-сервери, які відповідають за резолюцію імен, залишаються вразливими до окремих типів атак і можуть бути виведені з ладу незалежно від стану вебсервера або каналу зв’язку. У такій ситуації навіть успішне очищення трафіку не гарантує доступності вебресурсу для кінцевих користувачів, оскільки порушення роботи DNS призводить до неможливості встановлення з’єднання із сервісом.

Широке застосування отримали інфраструктурні рішення, зокрема мережі доставки контенту та технологія Anycast. CDN дозволяють кешувати контент на великій кількості серверів, розташованих у різних географічних регіонах, що сприяє розподілу навантаження та зменшенню ризику перевантаження окремих вузлів. Однак такі рішення не усувають проблеми централізованої резолюції доменних імен, оскільки доступ до кешованого контенту все одно залежить від працездатності DNS. Крім того, у разі компрометації або перевантаження початкового сервера CDN може поширювати некоректні або застарілі дані на всі вузли мережі, а сама інфраструктура CDN, будучи публічно ідентифікованою, може стати окремою ціллю масштабних DDoS-атак.

На рівні прикладних сервісів для захисту часто застосовуються Web Application Firewall, які аналізують HTTP-трафік і блокують атаки прикладного рівня. Такі засоби ефективні проти логічних і поведінкових атак, однак за умов високого навантаження WAF сам може перетворитися на критичний компонент системи. Необхідність аналізу кожного запиту створює додаткове навантаження, що підвищує ризик перевантаження та зниження продуктивності. При цьому потужні volumetric-атаки на мережевому рівні практично не піддаються нейтралізації засобами прикладного захисту.

Усі розглянуті традиційні технології протидії DDoS-атакам мають спільну фундаментальну проблему — залежність від централізованої архітектури. Незалежно від конкретного набору засобів захисту, критичні компоненти системи зосереджені на визначених фізичних або логічних вузлах, відмова або перевантаження яких призводить до недоступності сервісу. DNS-сервери залишаються прив’язаними до обмеженого кола операторів, CDN та Anycast лише перерозподіляють навантаження, не усуваючи сам факт централізації, а мережеві фаєрволи, проксі та WAF формують додаткові точки ризику.

Отже, головний недолік традиційних технологій захисту від DDoS-атак полягає в їх нездатності усунути корінну архітектурну причину вразливості — існування централізованого елемента, який може бути ціллю атаки. Такі підходи дозволяють лише пом’якшувати наслідки окремих векторів загроз, але не

забезпечують повної стійкості системи в умовах сучасного кіберсередовища. Саме ці обмеження зумовлюють об’єктивну потребу в пошуку альтернативних архітектурних рішень, зокрема децентралізованих підходів на основі ENS та IPFS, які здатні принципово змінити модель забезпечення доступності та захисту вебресурсів.

1.4. Централізована архітектура DNS і її вразливість до DDoS-атак

Система доменних імен (Domain Name System, DNS) є невід’ємною складовою функціонування сучасного Інтернету, оскільки забезпечує перетворення символьних доменних імен у числові IP-адреси, необхідні для встановлення мережевих з’єднань між клієнтами та серверами. Саме DNS виступає першою ланкою доступу до будь-якого вебресурсу, а отже, її стабільність безпосередньо визначає доступність усіх сервісів, що працюють у глобальній мережі. Незважаючи на фундаментальну роль DNS у мережевій інфраструктурі, її архітектура має низку вбудованих обмежень, які зумовлені централізованою ієрархічною моделлю та історичними особливостями проєктування протоколу.

Архітектура DNS базується на багаторівневій ієрархії, що включає кореневі сервери, сервери доменів верхнього рівня та авторитативні сервери конкретних доменів. Резолюція доменного імені відбувається послідовно через ці рівні, а отже, доступність вебресурсу безпосередньо залежить від стабільної роботи кожного з них. Хоча кореневі DNS-сервери фізично розподілені по всьому світу та використовують технології Anycast, їх кількість є обмеженою, а логічна структура залишається централізованою. Це створює системні ризики, оскільки перевантаження або порушення роботи навіть окремих елементів ієрархії може спричинити ланцюгову реакцію, що призводить до недоступності значної кількості доменів.

У контексті DDoS-атак ці обмеження проявляються особливо гостро. Масована атака може бути спрямована як безпосередньо на авторитативний DNS-

сервер конкретного домену, так і на інші рівні ієрархії, порушуючи процес резолюції імен. Перевантаження авторитативного сервера призводить до ситуації, за якої вебресурс стає недоступним для користувачів навіть за умови коректної роботи вебсервера та прикладних сервісів. Таким чином, DNS фактично перетворюється на критичну точку відмови, від якої залежить працездатність усієї інфраструктури доступу.

Додатковим чинником уразливості є те, що DNS-записи зберігаються та адмініструються конкретними DNS-провайдерами або реєстраторами доменів. Це означає, що доступність і коректність доменних записів залежить від зовнішніх організацій, які можуть зазнавати технічних збоїв, помилок конфігурації або цілеспрямованих атак. У разі компрометації DNS-провайдера або внутрішньої помилки адміністрування домен може стати недоступним незалежно від стану інших компонентів системи. Крім того, централізоване управління створює технічну можливість модифікації DNS-записів без безпосередньої участі власника домену, що суперечить принципам довіри та автономності адресації.

Історично DNS-протокол проєктувався в умовах обмеженого та відносно довіреного мережевого середовища, що зумовило відсутність вбудованих механізмів автентифікації та контролю джерела запитів. У сучасних умовах це перетворює DNS на зручний інструмент для зловмисників. Зокрема, DNS широко використовується для реалізації відбивних і ампліфікаційних DDoS-атак, за яких сервер відповідає на підроблений запит, спрямовуючи значно більший за обсягом трафік на IP-адресу жертви. Такі атаки здатні досягати надзвичайно високих потужностей, що перевищують можливості більшості мережевих інфраструктур і роблять DNS не лише об’єктом атак, але й ефективним засобом ураження інших систем.

Окрему проблему становить відсутність у DNS базових механізмів захисту від маніпуляцій на рівні провайдерів і проміжних вузлів. Це дозволяє здійснювати блокування доменів на вимогу державних або корпоративних структур, перенаправляти запити на фішингові чи шкідливі ресурси, впроваджувати фільтрацію контенту або модифікувати DNS-записи без відома користувачів.

Технологія DNSSEC частково вирішує проблему цілісності відповідей шляхом використання криптографічних підписів, однак її впровадження залишається фрагментарним, вона не захищає DNS-інфраструктуру від DDoS-атак і потребує складної конфігурації, що створює додаткове навантаження на систему.

Через відсутність обов'язкового криптографічного підтвердження цілісності в базовому протоколі DNS можливі атаки, спрямовані на підміну відповідей. Атаки типу DNS cache poisoning дозволяють впроваджувати фальшиві записи у кеш провайдера, spoofing-атаки змушують користувача встановлювати з'єднання з підконтрольними зловмиснику серверами, а атаки класу man-in-the-middle створюють умови для перехоплення або модифікації трафіку. У сукупності це формує загрозу не лише доступності сервісів, але й конфіденційності та цілісності даних.

Технічні обмеження DNS-серверів також відіграють суттєву роль у їхній вразливості до DDoS-атак. Кількість оброблюваних запитів, пропускна здатність мережевих інтерфейсів, обсяг кешу та продуктивність процесора мають кінцеві значення. Під час масованих атак DNS часто стає першим компонентом інфраструктури, який виходить з ладу через перевантаження. Це проявляється у зростанні латентності, збільшенні кількості помилок резолюції та повній відсутності відповідей у критичних ситуаціях, коли вебресурс є технічно працездатним, але фактично недоступним для користувачів.

Таким чином, DNS як централізована система має фундаментальні архітектурні обмеження, які не можуть бути повністю усунуті жодними традиційними засобами безпеки. Навіть найефективніші механізми фільтрації, масштабування та оптимізації лише зменшують наслідки атак або відтерміновують відмову, але не усувають її першопричину. Централізація управління, залежність від провайдерів, наявність критичних точок відмови, обмежені криптографічні механізми та можливість використання DNS як інструменту атак формують системну вразливість сучасної доменної інфраструктури. Саме ці структурні недоліки обґрунтовують необхідність дослідження та впровадження децентралізованих систем адресації, зокрема Ethereum Name Service у поєднанні з

IPFS, які здатні забезпечити рівень стійкості та доступності, принципово недосяжний для традиційних DNS-рішень.

2 АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ ЗАХИСТУ НА ОСНОВІ ENS ТА ДЕЦЕНТРАЛІЗОВАНИХ ТЕХНОЛОГІЙ

2.1. Призначення ENS та концепція децентралізованої адресації

Ethereum Name Service (ENS) є однією з ключових інфраструктурних технологій екосистеми Web3, спрямованою на подолання фундаментальних обмежень традиційної моделі адресації в Інтернеті. За своєю суттю ENS являє собою децентралізовану систему доменних імен, побудовану на базі блокчейну Ethereum, яка забезпечує перетворення складних криптографічних ідентифікаторів, зокрема адрес гаманців, хешів децентралізованого контенту, ідентифікаторів смарт-контрактів і інших блокчейн-об’єктів, у короткі, семантично зрозумілі символьні імена формату example.eth. Такий підхід істотно спрощує взаємодію користувачів і програмних систем із децентралізованими середовищами, усуваючи необхідність безпосередньої роботи з довгими та важко сприйнятними публічними ключами.

Традиційна система доменних імен DNS була спроєктована в умовах раннього розвитку Інтернету, коли питання децентралізації, криптографічної довіри, стійкості до цензури та масових атак на доступність не розглядалися як критичні. У моделі Web2 доменне ім’я виконує роль зручного для людини представлення IP-адреси сервера, який фізично розміщений у певному дата-центрі та контролюється конкретним провайдером або організацією. У Web3-середовищі така модель виявляється недостатньою, оскільки взаємодія відбувається не лише з серверами, а й із децентралізованими протоколами, смарт-контрактами та розподіленими сховищами даних. ENS у цьому контексті виступає аналогом DNS для Web3, приховуючи складні блокчейн-адреси та забезпечуючи інтуїтивно зрозумілий механізм доступу до децентралізованих сервісів.

Створення ENS стало відповіддю на низку системних архітектурних проблем традиційної інтернет-інфраструктури. Однією з ключових таких проблем є централізація DNS, яка формує критичні точки відмови у вигляді кореневих і

авторитативних серверів, реєстраторів доменів та DNS-провайдерів. Доступність значної кількості вебресурсів залежить від працездатності обмеженої кількості таких вузлів, а їх перевантаження або компрометація, зокрема внаслідок DDoS-атак, може призводити до масштабних збоїв. Крім того, у централізованій DNS-моделі існує ризик маніпуляції доменними записами, оскільки вони можуть бути змінені на стороні провайдера, підмінені внаслідок атак типу spoofing або cache poisoning, а також модифіковані під впливом адміністративних чи регуляторних рішень. У цій моделі кінцевий користувач не має криптографічних гарантій автентичності відповіді, яку він отримує під час резолюції доменного імені.

ENS реалізує принципово інший підхід до адресації, у якому зазначені проблеми усуваються не шляхом накладання додаткових захисних механізмів на існуючу інфраструктуру, а через зміну самої архітектурної логіки. На відміну від DNS, де записи зберігаються на серверах провайдерів або реєстраторів, ENS використовує смарт-контракти, розгорнуті безпосередньо в мережі Ethereum. Усі доменні записи зберігаються в блокчейні, що забезпечує їхню криптографічну незмінність, прозорість і відсутність єдиного адміністративного центру управління. Будь-які зміни записів можливі виключно за наявності приватного ключа власника домену, а всі операції є публічно перевірюваними, що виключає несанкціоноване втручання або приховану модифікацію даних.

Оскільки блокчейн Ethereum реплікується на тисячах повноцінних вузлів, дані ENS одночасно зберігаються у великій кількості географічно та логічно розподілених копій. Це забезпечує високу відмовостійкість системи та її працездатність навіть у разі виходу з ладу значної частини мережевої інфраструктури. Принциповою відмінністю ENS є відсутність традиційних DNS-серверів як окремих цілей для атак, що унеможливлює класичні DDoS-атаки на процес резолюції імен у звичному розумінні.

Функціональні можливості ENS не обмежуються лише зручним іменуванням криптовалютних адрес. ENS виступає універсальною системою ідентифікації та маршрутизації в децентралізованому середовищі. Один ENS-домен може містити посилання на адреси різних блокчейнів, IPFS-хеші вебресурсів і файлів, текстові

метадані, записи для взаємодії зі смарт-контрактами, а також DNS-сумісні дані, що забезпечують інтеграцію з традиційною Web2-інфраструктурою. Завдяки цьому ENS-домен фактично перетворюється на універсальний цифровий ідентифікатор користувача, сервісу або організації у Web3-просторі.

Ключова концепція ENS полягає у переході від адресації, заснованої на централізованих серверах і довірі до провайдерів, до адресації через незмінний розподілений реєстр. Такий підхід має безпосередній вплив на стійкість системи до DDoS-атак, оскільки усуває сервери резолюції як потенційні точки ураження, зменшує залежність від IP-адрес конкретних вузлів і унеможливлює централізоване блокування або цензуру доменів без участі їх власників. Прозорість і криптографічна перевірюваність усіх операцій з ENS додатково підвищують рівень довіри до системи та виключають приховані маніпуляції з доменними записами.

У контексті протидії DDoS-атакам ENS виступає важливою інфраструктурною основою для побудови децентралізованих вебресурсів у поєднанні з IPFS, систем ідентифікації користувачів, каналів доступу до смарт-контрактів і корпоративних сервісів, критично чутливих до блокувань і порушень доступності. Таким чином, Ethereum Name Service є не лише зручним механізмом прив’язки символьних імен до криптографічних ідентифікаторів, а й стратегічним елементом нової архітектури Інтернету, здатної усунути фундаментальні вразливості традиційного DNS і забезпечити підвищену стійкість до DDoS-атак та інших інфраструктурних загроз.

2.2. Архітектура ENS: Registry, Resolver, Registrar

Архітектура Ethereum Name Service (ENS) спроєктована таким чином, щоб поєднати гнучкість і розширюваність сучасних інтернет-сервісів із принципами децентралізації, криптографічної незмінності та відсутності єдиної точки відмови. На відміну від традиційної системи доменних імен DNS, у якій ключові функції зосереджені на централізованих серверах і контрольовані провайдерами або

реєстраторами, ENS функціонує як децентралізований протокол на базі блокчейна Ethereum. Такий підхід дозволяє зменшити залежність від окремих операторів інфраструктури, підвищити прозорість управління доменними іменами та забезпечити структурну стійкість системи до атак на доступність, зокрема DDoS.

Функціональна логіка ENS розділена на три основні компоненти:

• Registry — базовий реєстр доменних імен;

• Resolver — компонент зберігання та надання фактичних записів;

• Registrar — механізм реєстрації та управління доменами.

Такий поділ відповідальності дозволяє зменшити складність окремих елементів системи, забезпечити їх незалежний розвиток і підвищити загальну надійність архітектури.

Registry є центральним елементом ENS і виконує роль децентралізованого довідника доменних імен. Його основним завданням є зберігання мінімального набору метаданих, необхідних для коректної роботи всієї системи. Для кожного доменного імені в Registry фіксується інформація про власника, який має повноваження змінювати налаштування домену, адреса резолвера, що відповідає за зберігання фактичних записів, параметр часу життя результатів резолюції, а також ієрархічні зв’язки між доменами та субдоменами. Важливою особливістю Registry є те, що він не оперує доменними іменами у текстовому вигляді. Кожне ім’я в ENS представлено у формі криптографічного хешу, що забезпечує детерміновану обробку доменної ієрархії та унеможливлює неоднозначність інтерпретації записів. Мінімалістичний дизайн Registry є свідомим архітектурним рішенням, спрямованим на підвищення безпеки та ефективності системи. У цьому компоненті не зберігаються IP-адреси, IPFS-хеші або інші об’ємні дані, а лише посилання на власників і резолвери. Такий підхід дозволяє зменшити витрати на виконання операцій у блокчейні, спростити логіку смарт-контракту та знизити ризик виникнення критичних помилок. Керування записами в Registry здійснюється виключно власником домену. Власником може бути як окрема адреса користувача, так і мультипідписний гаманець, децентралізована автономна організація або

інший смарт-контракт із власною логікою управління, що дозволяє будувати складні моделі контролю доменів без зміни базового протоколу ENS.

Resolver є компонентом ENS, у якому зберігається фактичне значення доменного імені. Саме резолвер відповідає на запит про те, які ресурси або ідентифікатори асоційовані з конкретним доменом. У резолвері можуть зберігатися адреси криптовалютних гаманців, хеші контенту в IPFS, текстові метадані, записи для смарт-контрактів, а також DNS-сумісні записи, що дозволяють інтегрувати ENS із традиційною веб-інфраструктурою. Усі резолвери реалізують стандартний інтерфейс ENS, завдяки чому клієнтські застосунки можуть уніфіковано отримувати дані незалежно від конкретної реалізації резолвера.

Суттєвою перевагою резолверів є їхня гнучкість і незалежність від Registry. Власник домену може використовувати стандартний публічний резолвер або розгорнути власний смарт-контракт із розширеною логікою, наприклад динамічним оновленням записів або інтеграцією з іншими on-chain механізмами. У разі потреби резолвер може бути замінений або оновлений без будь-якого втручання в Registry, що дозволяє адаптувати систему до нових функціональних або безпекових вимог без порушення її цілісності. З точки зору захисту від DDoS-атак принципово важливо, що резолвери не є традиційними мережевими серверами і не приймають DNS або HTTP-запити напряму, оскільки доступ до даних здійснюється через розподілений блокчейн Ethereum.

Компонент Registrar відповідає за процес реєстрації та управління доменними іменами в ENS. Він визначає правила реєстрації, тривалість володіння доменами та механізми їх продовження або звільнення. Для доменів у зоні .eth використовується двофазний механізм commit–reveal, який забезпечує приховування фактичного доменного імені на етапі подання заявки та запобігає атакам типу front-running, за яких зловмисник міг би перехопити заявку на реєстрацію. Такий підхід підвищує безпеку процедури реєстрації та відповідає загальній концепції Web3, де захист реалізується на рівні протоколу.

Взаємодія між Registry, Resolver та Registrar формує повний життєвий цикл доменного імені в ENS, починаючи з його реєстрації та завершуючи резолюцією

імені для кінцевих користувачів і застосунків. Усі ці процеси відбуваються в децентралізованому середовищі без участі централізованих DNS-серверів, кешів провайдерів або адміністративного втручання, що істотно зменшує кількість критичних точок відмови.

У контексті протидії DDoS-атакам архітектура ENS має принципові переваги над традиційною моделлю DNS. Відсутність централізованих серверів резолюції, розподілене виконання логіки смарт-контрактів у мережі Ethereum та неможливість адміністративного відключення домену без участі власника забезпечують високу стійкість системи до атак на доступність. Навіть у разі перевантаження окремих вузлів мережі загальна функціональність ENS зберігається, оскільки кожен вузол містить копію стану реєстру.

Таким чином, архітектура Ethereum Name Service, побудована на взаємодії Registry, Resolver та Registrar, забезпечує чітке розділення відповідальності, гнучкість розвитку, криптографічний контроль і відсутність єдиної точки відмови. Сукупність цих властивостей робить ENS структурно стійким до класичних векторів DDoS-атак і створює надійну основу для побудови децентралізованих вебресурсів у поєднанні з IPFS.

2.3. Механізм резолюції імен ENS та порівняння з традиційним DNS

Механізм резолюції імен у системі Ethereum Name Service є одним із базових елементів її архітектури та визначає спосіб перетворення символьного доменного імені на фактичні цифрові дані, зокрема криптовалютні адреси, ідентифікатори децентралізованого контенту IPFS, текстові записи або параметри взаємодії зі смарт-контрактами. На відміну від традиційної системи DNS, у якій процес резолюції реалізується через багаторівневу ієрархію централізованих серверів, ENS використовує децентралізований підхід, заснований на смарт-контрактах блокчейну Ethereum. Така модель усуває залежність від окремих серверів і провайдерів, що забезпечує високу стійкість

до атак на доступність та інфраструктурних збоїв навіть за умов надвисокого навантаження.

Процес резолюції доменного імені в ENS реалізується як послідовність логічно пов’язаних етапів, кожен з яких відбувається у децентралізованому середовищі без залучення централізованих посередників. На початковому етапі користувач вводить ENS-домен у криптогаманці, Web3-браузері або децентралізованому додатку, що підтримує роботу з ENS. У цьому випадку клієнт не звертається до рекурсивного DNS-сервера інтернет-провайдера, а безпосередньо ініціює зчитування даних зі стану блокчейну Ethereum, використовуючи власний або віддалений вузол мережі.

Наступним етапом є звернення до ENS Registry — центрального смарт-контракту, який виконує роль глобального реєстру доменних імен. Registry зберігає мінімальний набір метаданих, необхідних для функціонування всієї системи, зокрема інформацію про власника домену, адресу резолвера та параметри TTL. Під час резолюції Registry повертає адресу відповідного резолвера, що дозволяє клієнту визначити, де саме зберігаються фактичні записи доменного імені. Оскільки цей реєстр розміщений у блокчейні Ethereum, дані в ньому є криптографічно захищеними та незмінними, що унеможливлює їхню підміну, видалення або модифікацію з боку провайдерів, адміністраторів мережі чи зловмисників.

Після отримання адреси резолвера клієнт звертається до відповідного смарт-контракту Resolver, який містить фактичні записи, асоційовані з доменом. Резолвер може зберігати широкий спектр даних, включно з адресами криптовалютних гаманців, мультивалютними адресами для інших блокчейн-мереж, IPFS-ідентифікаторами вебресурсів, текстовими метаданими, записами ABI для взаємодії зі смарт-контрактами, а також DNS-сумісними записами для гібридної інтеграції з Web2-середовищем. Зчитування цих даних здійснюється шляхом доступу до стану блокчейну або його локальної копії, що виключає можливість перехоплення або підміни відповіді під час резолюції.

На завершальному етапі процесу клієнт інтерпретує отримані дані відповідно до сценарію використання. Якщо результатом є криптовалютна адреса, користувач може безпосередньо ініціювати транзакцію. У разі повернення IPFS-ідентифікатора відбувається завантаження контенту з децентралізованої peer-to-peer мережі. Якщо домен пов'язаний зі смарт-контрактом, клієнт може виконувати виклики його функцій через відповідний інтерфейс. Таким чином, ENS-домен виступає універсальним інструментом ідентифікації та маршрутизації, що поєднує адресацію, доступ до контенту та взаємодію з децентралізованими сервісами.

Принциповою перевагою ENS у контексті протидії DDoS-атакам є відсутність традиційної DNS-інфраструктури як потенційної цілі для атак. У класичній DNS-моделі процес резолюції залежить від доступності кореневих серверів, серверів доменів верхнього рівня, авторитативних серверів і рекурсивних вузлів провайдерів, кожен з яких може бути перевантажений або виведений з ладу внаслідок масованої атаки. ENS не використовує сервери у традиційному розумінні, оскільки виконання смарт-контрактів розподілене між тисячами незалежних вузлів Ethereum, що виключає існування єдиної точки відмови.

Архітектура ENS також усуває вразливості, пов'язані з атаками типу spoofing та cache poisoning. У традиційній DNS-інфраструктурі можливі підміна відповідей, отруєння кешів і атаки типу «людина посередині», що дозволяє зловмисникам маніпулювати трафіком або перенаправляти користувачів на шкідливі ресурси. У ENS відсутні кеші провайдерів, а всі записи зчитуються безпосередньо з криптографічно захищеного реєстру блокчейну. Зміна записів можлива лише за наявності приватного ключа власника домену, що забезпечує високий рівень автентичності та цілісності даних.

Незмінність і довготривала доступність даних у ENS гарантуються самою природою блокчейну Ethereum. Відсутність централізованого адміністратора означає, що жодна окрема організація або держава не може одноосібно змінити

або заблокувати доменний запис. Навіть у разі часткової недоступності мережі або виходу з ладу окремих вузлів процес резолюції продовжує функціонувати, що має критичне значення для забезпечення доступності сервісів у кризових умовах.

Отже, механізм резолюції імен у ENS є не просто альтернативою традиційній DNS-резолюції, а реалізує принципово нову модель адресації, у якій децентралізація, криптографічна довіра та стійкість до DDoS-атак закладені безпосередньо на рівні протоколу. Саме ці архітектурні особливості роблять ENS важливим компонентом сучасних Web3-рішень і перспективною основою для побудови інфраструктур, орієнтованих на високу доступність і безпеку.

Таблиця 2.1.

Порівняльна таблиця DNS та ENS

Параметр	DNS	ENS
Місце зберігання даних	Сервери провайдерів, TLD-сервери	Блокчейн Ethereum
Вразливість до DDoS	Висока (атаки на DNS-сервери)	Низька (немає серверів)
Вразливість до spoofing	Висока	Практично неможлива
Cache poisoning	Поширене	Відсутнє
Централізація	Висока	Низька (децентралізована мережа)
Контроль доступу	Провайдери та реєстратори	Власник приватного ключа
Залежність від інфраструктури	Висока	Мінімальна

Механізм резолюції ENS формує принципово нову модель адресації в мережі Інтернет, яка докорінно відрізняється від традиційних підходів, реалізованих у системі DNS. Він усуває ключові структурні недоліки класичної доменної інфраструктури, зокрема залежність від централізованих серверів, наявність адміністративного контролю з боку провайдерів, можливість підміни або маніпуляції доменними записами, а також високу вразливість до DDoS-атак, спрямованих на інфраструктуру резолюції імен. Завдяки використанню смарт-контрактів і розподіленого реєстру блокчейну Ethereum ENS забезпечує криптографічно гарантовану цілісність даних, відсутність єдиної точки відмови та стабільну доступність сервісів навіть за умов масованих атак або часткових збоїв мережі. У результаті ENS виступає не лише альтернативою DNS, а й одним із найбільш перспективних інструментів для побудови сучасних захищених інформаційних систем, орієнтованих на високу стійкість до атак на інфраструктуру та забезпечення безперервної доступності ресурсів.

2.4. Інтеграція ENS із IPFS: децентралізований веб як засіб протидії DDoS

Однією з ключових проблем традиційної веб-інфраструктури є її залежність від централізованих серверів, які зберігають контент і відповідають на запити користувачів. У класичній Web2-моделі кожен вебресурс має одну або кілька критичних точок відмови, до яких належать вебсервер, вузли CDN або DNS-сервери. У разі масованої DDoS-атаки зловмисники можуть перевантажити ці компоненти, що призводить до повної або часткової недоступності ресурсу незалежно від його обчислювальних можливостей чи використання захисних механізмів. Таким чином, централізована архітектура Web2 залишається вразливою за своєю природою, оскільки атака на обмежену кількість вузлів здатна порушити роботу всієї системи.

У парадигмі Web3 підходи до зберігання та доступу до інформації змінюються принципово. Одним із ключових інструментів нового покоління є

InterPlanetary File System — децентралізований протокол зберігання та розповсюдження даних, побудований на основі peer-to-peer архітектури. На відміну від класичних вебсерверів, де кожен файл має фіксоване фізичне розташування, IPFS використовує модель адресації за вмістом. У цій моделі дані ідентифікуються не за адресою сервера, а за їхнім криптографічним хешем, який називається Content Identifier. Такий підхід означає, що користувач запитує не «де знаходиться файл», а «який саме файл потрібен», що має фундаментальні наслідки для безпеки та доступності.

Однією з ключових властивостей IPFS є відсутність єдиного серверного розташування контенту. Замість розміщення даних на конкретному сервері або в дата-центрі контент розподіляється між багатьма учасниками мережі. Будь-який вузол, який має копію файлу, може брати участь у його передачі іншим користувачам. У результаті зникає можливість «вимкнути сайт» шляхом атаки на одного провайдера або хостинг, оскільки дані не прив’язані до конкретної інфраструктури.

Розподіленість IPFS доповнюється механізмом дублювання даних. Контент може одночасно зберігатися на локальних вузлах користувачів, на публічних IPFS-нодах, у приватних інстансах організацій або на IPFS-шлюзах, які кешують дані для підвищення доступності. Чим більше користувачів звертається до певного ресурсу, тим більше копій цього ресурсу автоматично з’являється в мережі. Така поведінка створює ефект самопосилення доступності, коли зростання популярності контенту не збільшує навантаження на систему, а навпаки підвищує її стійкість.

Ще однією фундаментальною властивістю IPFS є криптографічна незмінність контенту. Ідентифікатор CID формується на основі хешу даних, що означає, що будь-яка зміна вмісту автоматично призводить до зміни його ідентифікатора. Це гарантує цілісність даних, унеможливлює приховану підміну контенту та забезпечує захист від атак типу MITM або DNS spoofing, оскільки користувач завжди отримує саме той контент, хеш якого було запитано.

Доступність даних в IPFS забезпечується глобальною peer-to-peer мережею, яка не залежить від працездатності окремих серверів. Навіть у разі відмови значної

частини вузлів дані залишаються доступними з інших учасників мережі. Це створює принципово інший рівень стійкості до атак на доступність у порівнянні з централізованими системами зберігання.

Поєднання Ethereum Name Service та IPFS дозволяє сформувати повністю децентралізовану модель вебресурсу, у якій усунуті традиційні точки відмови. Контент вебсайту, зображення або дані публікуються в IPFS, після чого для них формується криптографічний ідентифікатор CID. Цей ідентифікатор записується у відповідний ENS-домен у полі contenthash. Коли користувач вводить доменне ім’я, наприклад site.eth, ENS через смарт-контракти повертає CID, а IPFS знаходить відповідний контент у мережі та доставляє його користувачеві. Таким чином, ENS виконує функцію децентралізованої адресації, а IPFS — функцію децентралізованого зберігання та доставки даних.

У такій моделі адресація стає незалежною від DNS, зберігання — незалежним від серверів, доступність доменного імені забезпечується блокчейном, а доступність контенту — P2P-мережею. Це принципово змінює підхід до побудови вебресурсів і усуває ключові вразливості Web2-архітектури.

Інтеграція ENS та IPFS має суттєві переваги у контексті протидії DDoS-атакам. У традиційній Web2-моделі зловмисники спрямовують атаки на DNS-сервери, вебсервери, CDN-вузли або API-шлюзи, перевантажуючи їх обчислювальні ресурси чи пропускну здатність. У моделі ENS+IPFS відсутні сервери, які одноосібно відповідають за резолюцію імен або зберігання контенту, що фактично позбавляє атакувальників очевидної цілі.

Навіть у разі атаки на окремі вузли IPFS або Ethereum інші учасники мережі продовжують обслуговувати запити. IPFS динамічно оптимізує маршрути передачі даних, тому перевантаження окремих нод не призводить до деградації всієї системи. Більше того, зі збільшенням кількості користувачів сумарна пропускна здатність мережі зростає, що є протилежністю до поведінки централізованих серверів.

Важливою перевагою є також неможливість централізованого блокування. У системі ENS+IPFS немає провайдера або адміністративного органу, який міг би

видалити сайт, заблокувати домен, змінити контент або примусово перенаправити трафік. Навіть у разі блокування окремих IPFS-шлюзів контент залишається доступним через інші вузли або шляхом прямого підключення до мережі IPFS.

Завдяки розподіленості архітектури атаки на зберігання або резолюцію не здатні вивести з ладу всю систему. Кожен вузол самостійно обслуговує запити, а загальна пропускна здатність мережі зростає разом із кількістю учасників. Це кардинально відрізняє ENS+IPFS від Web2-рішень, де зростання трафіку збільшує навантаження на сервери та підвищує ризик відмови в обслуговуванні.

Незмінність і цілісність контенту забезпечуються криптографічною природою IPFS. Будь-яка спроба маніпуляції даними стає миттєво помітною, оскільки змінюється ідентифікатор CID. Це унеможливлює перехоплення домену, підміну вебресурсу або приховане перенаправлення користувачів.

Таким чином, інтеграція ENS та IPFS формує архітектуру, яка не має централізованих серверів, не потребує традиційної DNS-інфраструктури, захищена від підміни та маніпуляцій, масштабується завдяки peer-to-peer підходу та є структурно і функціонально стійкою до DDoS-атак. За своєю природою ENS+IPFS не лише протидіє атакам на доступність, а й створює нову модель вебу, у якій здійснення таких атак стає технічно складним та економічно недоцільним.

2.5. Порівняльний аналіз ENS і DNS у контексті безпеки та DDoS-стійкості

Традиційна система доменних імен є основою функціонування сучасного Інтернету, однак її архітектура має низку фундаментальних вразливостей. Оскільки DNS побудований на централізованій багаторівневій моделі, зловмисники можуть атакувати як окремі сервери, так і цілі сегменти інфраструктури, що призводить до порушення доступності вебресурсів незалежно від їх реального стану.

На противагу цьому Ethereum Name Service (ENS) реалізує децентралізовану модель, у якій дані зберігаються на блокчейні, а контент — у розподілених P2P-

мережах, таких як IPFS. Така архітектура не лише підвищує безпеку, але й усуває класичні точки відмови, що забезпечує високу стійкість до DDoS-атак.

Для всебічного аналізу наведено порівняння ключових характеристик DNS і ENS.

Таблиця 2.2.

Порівняльна таблиця DNS та ENS у контексті безпеки

Критерій	DNS (централізований)	ENS (децентралізований)
Архітектура	Ієрархічна, багаторівнева структура: кореневі сервери, TLD, авторитативні DNS-сервери	Розподілена система на основі блокчейну Ethereum
Критерій	DNS (централізований)	ENS (децентралізований)
Точки відмови	Кожен рівень DNS може бути атакований або перегружений	Відсутні. Дані зберігаються на тисячах вузлів
Залежність від провайдерів	Висока: резолюція залежить від DNS-провайдера	Відсутня: доступність гарантується блокчейном
Незмінність записів	Відсутня: адміністратор може змінити чи видалити запис	Гарантована. Дані незмінні після запису у блокчейн
Цензура та блокування	Можлива: домен може бути заблокований або відключений	Неможлива без доступу до ключа власника
Масштабованість	Обмежена пропускною здатністю серверів	Дуже висока: масштабування забезпечується мережею
Доступність контенту	Залежить від конкретного серверного розташування	Забезпечується через IPFS — розподілену P2P мережу

Продовження таблиці 2.2.

Порівняльна таблиця DNS та ENS у контексті безпеки

Критерій	DNS (централізований)	ENS (децентралізований)
Тип адресації	URL, залежний від мережевої інфраструктури	IPFS-CID, хеш-контенту, незалежний від місця зберігання
Управління доменами	Централізоване, підконтрольне реєстраторам	Децентралізоване, підконтрольне лише власнику
Витрати на підтримку	Залежні від серверної інфраструктури	Мінімальні, оскільки немає серверів

Традиційна система доменних імен DNS функціонує на основі централізованої ієрархічної архітектури, у якій кожен рівень може стати потенційною ціллю DDoS-атаки. Кореневі сервери, сервери доменів верхнього рівня та авторитативні DNS-сервери мають обмежену пропускну здатність і обчислювальні ресурси. Навіть за умови використання технологій CDN або Anycast базова архітектура DNS залишається вразливою, оскільки зловмисники спрямовують атаки не безпосередньо на вебресурс, а на інфраструктуру, яка забезпечує його доступність. Перевантаження елементів DNS-ієрархії призводить до неможливості резолюції доменних імен і, як наслідок, до повної недоступності сервісу.

Ethereum Name Service реалізує принципово інший підхід до адресації. ENS не використовує традиційних серверів для резолюції імен, а всі записи зберігаються у блокчейні Ethereum, який одночасно реплікується тисячами незалежних вузлів. У результаті конфігурація ENS не містить жодного окремого елемента, який можна було б перевантажити у класичному розумінні. Навіть у разі атаки на окремі вузли мережі загальна доступність системи не порушується, оскільки кожен вузол має повну копію стану реєстру.

Окрім вразливостей до атак на доступність, DNS є сприйнятливим до атак на цілісність даних. У традиційній DNS-інфраструктурі можливі підміна відповідей шляхом DNS spoofing, отруєння кешу рекурсивних серверів, атаки типу «людина посередині» та фальсифікація відповідей авторитативних серверів. Такі методи широко застосовуються для фішингу, викрадення облікових даних, маніпуляції трафіком і перенаправлення користувачів на шкідливі ресурси. Навіть використання додаткових захисних механізмів, таких як DNSSEC, не усуває повністю ризики, а лише зменшує їх і ускладнює реалізацію атак.

ENS запобігає подібним загрозам на рівні протоколу. Зміна будь-якого запису в ENS можлива виключно власником відповідного домену, який володіє приватним криптографічним ключем. Блокчейн Ethereum забезпечує незмінність і повну прозорість історії змін, що унеможливлює приховане втручання або підміну записів. Відсутність серверів і проміжних ланок означає також відсутність можливості перехоплення запиту або підміни відповіді, що принципово усуває класичні DNS-загрози.

Важливим аспектом є також масштабованість і поведінка систем під високим навантаженням. У DNS збільшення кількості запитів безпосередньо впливає на навантаження серверів, що може призводити до деградації продуктивності, утворення черг обробки та зниження доступності ресурсу для легітимних користувачів. У пікові моменти навіть короткочасне перевантаження DNS-інфраструктури може зробити сервіс недоступним.

ENS, у свою чергу, функціонує на інфраструктурі Ethereum, де зберігання і читання даних не залежать від кількості одночасних запитів у традиційному сенсі. Кожен вузол мережі є повноцінною копією блокчейна, що дозволяє системі автоматично усувати вузькі місця. Навіть масовані атаки не здатні порушити роботу механізму резолюції, оскільки запити розподіляються між усіма вузлами мережі, а не концентруються на окремому сервері.

У традиційній DNS DDoS-атаки можуть реалізовуватися на різних рівнях, зокрема шляхом масованого надсилання трафіку, зловживання протоколами або атак прикладного рівня на DNS-сервери. ENS не містить серверів, протоколів або

інфраструктурних точок, які можна було б перевантажити подібними методами. Механізм резолюції ENS працює безпосередньо в блокчейні, а мережа Ethereum є відмовостійкою, географічно розподіленою та здатною функціонувати навіть у разі відмови частини вузлів.

Порівняльний аналіз показує, що ENS структурно усуває фундаментальні вразливості DNS. У той час як традиційну систему доменних імен можливо захищати лише шляхом додавання додаткових рівнів безпеки, таких як CDN, WAF, Anycast або центри очищення трафіку, ENS забезпечує стійкість до DDoS-атак безпосередньо на рівні своєї архітектури. Це означає, що захист не є зовнішнім або допоміжним механізмом, а невід’ємною властивістю системи.

У поєднанні з IPFS ENS формує новий стандарт безпеки та доступності вебресурсів, у межах якого DDoS-атаки втрачають свою ефективність як інструмент впливу. Така модель не лише ускладнює реалізацію атак на доступність, а й робить їх технічно та економічно недоцільними, що підтверджує перспективність використання ENS+IPFS як альтернативи традиційній DNS-інфраструктурі.

3 РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ЗАСТОСУВАННЯ ENS+IPFS ДЛЯ ЗАХИСТУ ВЕБРЕСУРСІВ

3.1. Реєстрація ENS-домену та налаштування резолвера

Для впровадження децентралізованої моделі адресації першим етапом є реєстрація ENS-домену та налаштування його параметрів відповідно до вимог вебресурсу. На відміну від традиційних DNS-доменів, ENS-домен не залежить від реєстраторів або провайдерів — всі операції виконуються безпосередньо через смарт-контракти Ethereum.

Процес реєстрації через сервіс ENS Domains включає:

Вибір вільного доменного імені у зоні .eth. Користувач перевіряє доступність імені через офіційний інтерфейс ENS або Web3-додаток.

Рис. 3.1. Реєстрація домену ENS

Підтвердження реєстрації та підпис транзакції. Реєстрація здійснюється шляхом оплати орендної плати за період володіння доменом (зазвичай 1–3 роки) і підпису смарт-контракту через криптогаманець.

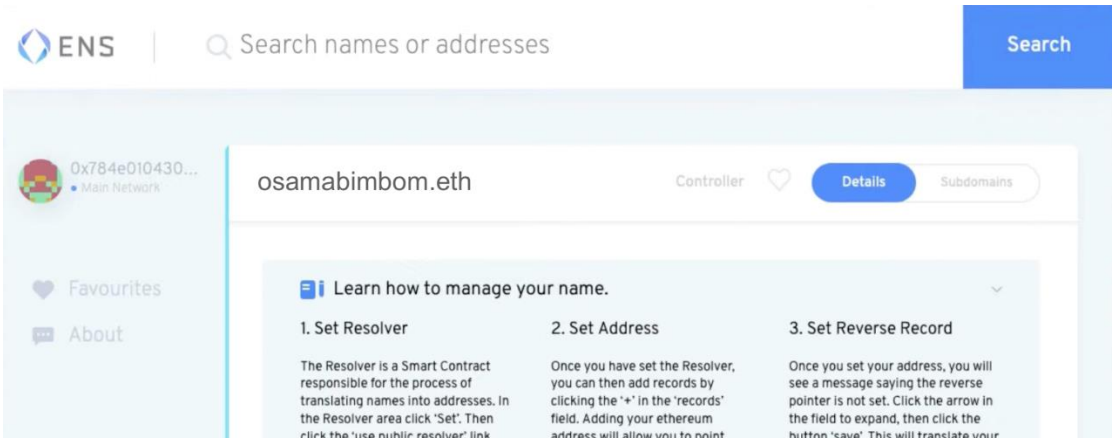

Рис. 3.2 Зареєстрований домен ENS

Призначення резолвера. За замовчуванням використовується Public Resolver, який підтримує:

- – записи адрес,
- – текстові записи,
- – contenthash,
- – multicoin records.

Рис. 3.3 Призначення публічного ресольвера

Рис. 3.4. Призначення публічного ресольвера

Налаштування contenthash. Після отримання IPFS-хешу вебресурсу користувач записує його у поле "Content Hash".

Рис. 3.5. Привязуємо хєш сайту до ENS домену

Перевірка коректності резолюції. Домен можна протестувати через ENS-інструменти або Web3-браузери, переконавшись у правильності маршрутизації до IPFS-контенту.

Завдяки блокчейну Ethereum зміна чи підміна записів стає неможливою без приватного ключа власника домену, що значно підвищує безпеку адресації.

3.2. Публікація вебресурсу в IPFS та методика завантаження односторінкових сайтів

Для розміщення вебресурсу без централізованих серверів використовується IPFS — розподілена peer-to-peer система зберігання контенту. Основна перевага IPFS полягає в тому, що:

- сайт не має фізичного місця розташування;
- контент дублюється на різних вузлах мережі;
- кожна версія сайту має унікальний криптографічний хеш;
- ресурс залишається доступним навіть при недоступності окремих вузлів.

Методика розміщення односторінкового HTML-сайту через IPFS Desktop:

Встановлення IPFS Desktop. Користувач завантажує застосунок з офіційного сайту ipfs.tech і запускає локальний вузол.

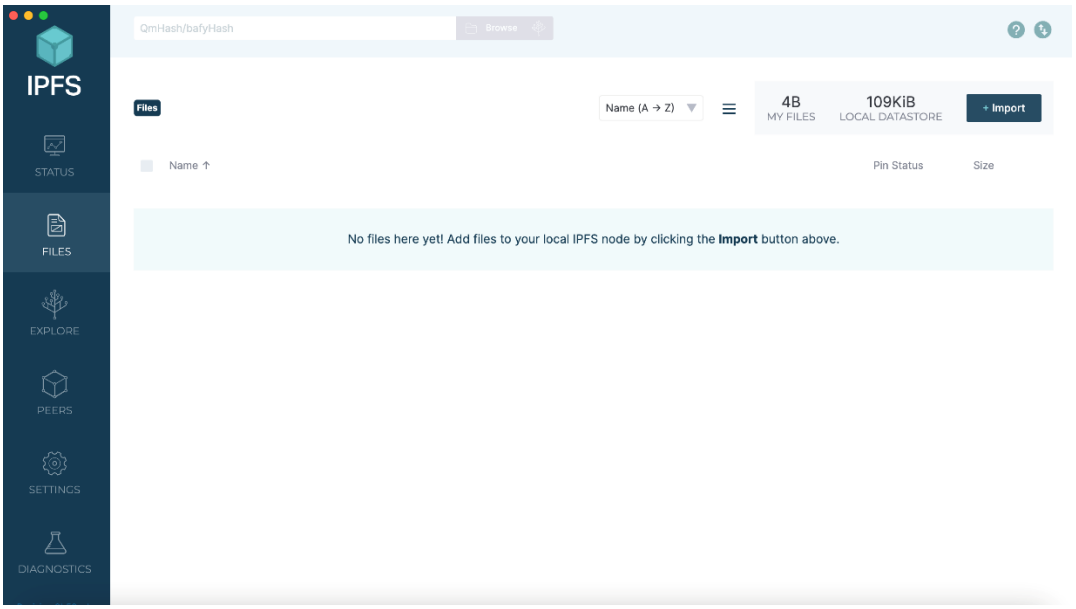

Рис. 3.6 IPSF Desktop

Підготовка файлів. Створюється директорія з HTML-файлом, стилями, зображеннями тощо.

Завантаження в мережу IPFS. Через меню "Import → Add Folder" користувач додає каталог сайту. IPFS автоматично:

- хешує дані,
- генерує кореневий CID,
- зберігає копію у локальному вузлі.

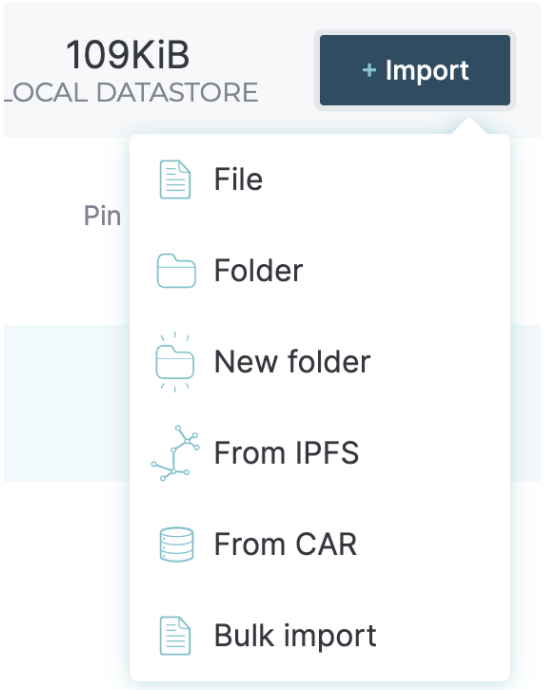

Рис. 3.7 Імпорт потрібного нам файлу

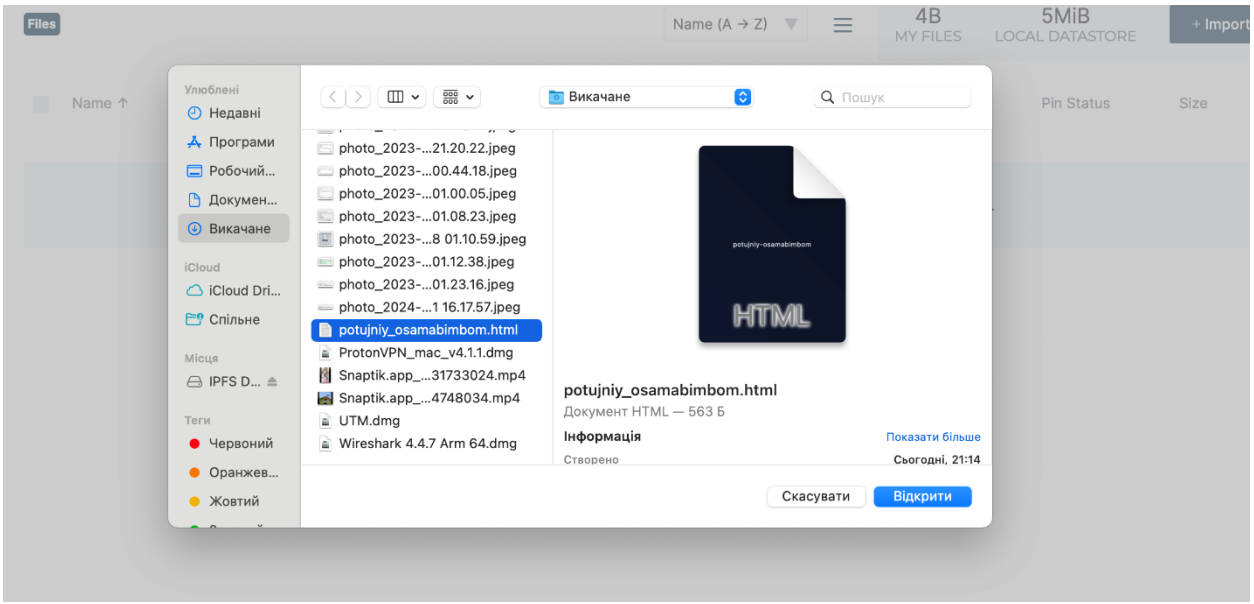

Рис.3.8 Імпорт файлу веб ресурсу

Публікація та закріплення. Щоб стайт гарантовано залишався доступним, виконують *pinning* у локальному вузлі або на сторонніх сервісах.

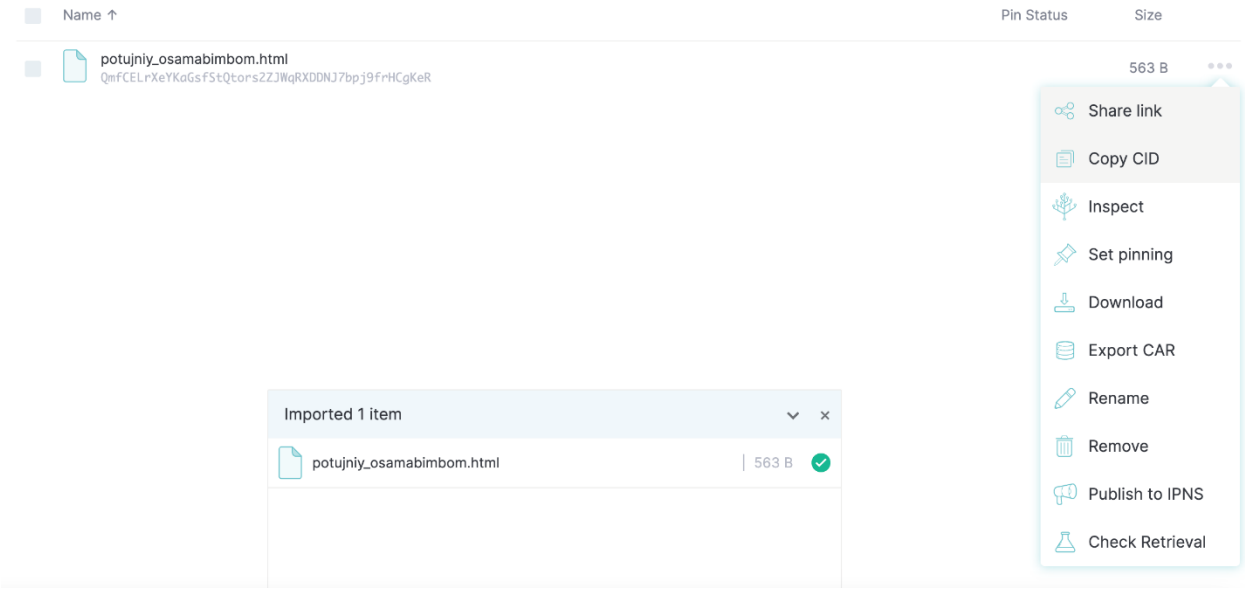

Рис. 3.9. Опублікований ресурс

CID вводиться у ENS-домен: Contenthash → ipfs://CID

Рис. 3.10 Привязуємо CID сайту до ENS домену

Після цього сайт доступний з будь-якого IPFS-шлюзу: https://ipfs.io/ipfs/<CID>; https://cloudflare-ipfs.com/ipfs/<CID>. Або через ENS: myproject.eth.

Таким чином вебресурс стає повністю децентралізованим та стійким до атак на інфраструктурні компоненти.

3.3. Моделювання DDoS-атак на традиційний DNS і ENS+IPFS

Для обґрунтування доцільності переходу від традиційної архітектури DNS до децентралізованої моделі ENS+IPFS було проведено моделювання умовної DDoS-атаки на два різні варіанти розміщення одного й того самого вебресурсу. Метою моделювання не було відтворення конкретного інциденту кібернападу або використання реальних шкідливих інструментів, а порівняльний аналіз поведінки двох інфраструктурних підходів в умовах різкого зростання кількості запитів, характерного для атак типу «відмова в обслуговуванні».

У межах дослідження розглядалися два сценарії. У першому сценарії застосовувалася традиційна Web2-модель, за якої вебсайт розміщувався на одному VPS-сервері з фіксованими обчислювальними ресурсами, а доступ до нього здійснювався через стандартну DNS-інфраструктуру з використанням A-запису, що пов’язував доменне ім’я з IP-адресою сервера. У другому сценарії використовувалася децентралізована Web3-модель, у якій той самий вебресурс публікувався в мережі IPFS, а доступ до нього здійснювався через ENS-домен, у полі contenthash якого зберігався відповідний IPFS-CID.

Під час моделювання аналізувалися ключові показники, які мають критичне значення з погляду протидії DDoS-атакам. Зокрема оцінювалася доступність ресурсу для кінцевого користувача під час і після зростання навантаження, стабільність механізму резолюції імен, поведінка інфраструктури при збільшенні обсягу трафіку, а також можливість повної втрати функціональності сервісу. Обрання саме цих показників зумовлене тим, що DDoS-атаки спрямовані насамперед на порушення доступності, а не на компрометацію конфіденційності або цілісності даних.

У моделі з використанням традиційної DNS-інфраструктури при поступовому збільшенні умовного DDoS-навантаження було зафіксовано характерні негативні ефекти. На початкових етапах різкого зростання кількості запитів спостерігалося порушення стабільності резолюції доменних імен. Рекурсивні DNS-сервери провайдерів почали працювати нестабільно, час відповіді

на DNS-запити зростав у кілька разів, а також періодично виникали тайм-аути та помилки резолюції. Для кінцевого користувача це проявлялося у вигляді значного збільшення часу завантаження вебресурсу або повідомлень про неможливість знайти домен, навіть за умови того, що сам вебсервер ще не був повністю перевантажений.

На наступному етапі, за умов подальшого збільшення обсягу запитів, почалося перевантаження вебсервера. Сервер поступово вичерпував пул доступних з'єднань, з'являлися помилки класу 5xx, а легітимні запити користувачів починали конкурувати зі шкідливими запитами. Фактично сервіс переставав коректно виконувати свої функції, оскільки обчислювальні ресурси сервера використовувалися неефективно і були зайняті обробкою надмірного трафіку.

У разі подальшого зростання інтенсивності атаки система переходила у стан повної втрати функціональності. Вебсервер переставав відповідати на більшість запитів, DNS-сервери дедалі частіше повертали помилки або взагалі не відповідали, а для користувачів ресурс ставав повністю недоступним. Такий стан можна охарактеризувати як повну відмову сервісу, за якої інфраструктура більше не здатна виконувати свої основні завдання.

Окрему увагу було приділено аналізу наслідків після зменшення інтенсивності атаки. Було встановлено, що навіть після спаду навантаження частина DNS-записів залишалася у некоректному або нестабільному стані, вебсервер потребував додаткового часу для відновлення нормальної роботи, а легітимні користувачі ще певний період стикалися з помилками або деградацією продуктивності. Це свідчить про те, що DNS і серверна інфраструктура є критичними точками відмови, а атака на рівні адресації або обслуговування запитів здатна вивести сервіс з ладу навіть після завершення активної фази атаки.

У децентралізованій моделі ENS+IPFS вебресурс був опублікований у мережі IPFS, а його криптографічний ідентифікатор CID був записаний у ENS-домен у полі contenthash. У такій конфігурації адресація здійснювалася через блокчейн Ethereum, а зберігання і доставка контенту — через розподілену peer-to-peer мережу IPFS.

Важливою особливістю цієї моделі є відсутність єдиного вебсервера або DNS-сервера, який міг би стати ціллю атаки.

Під час моделювання було встановлено, що механізм резолюції ENS зберігає стабільність навіть при значному зростанні кількості запитів. Оскільки ENS працює на базі блокчейна Ethereum і використовує читання даних зі смарт-контрактів, резолюція імен не залежить від конкретних провайдерів або географічно локалізованих вузлів. Навіть у разі недоступності частини вузлів мережі загальний процес резолюції залишався стабільним, без зростання затримок, тайм-аутів або помилок.

Стійкість IPFS до навантаження пояснюється його розподіленою природою. Контент зберігається одночасно на багатьох вузлах, а кожен користувач, який завантажує ресурс, потенційно стає додатковим джерелом даних. Мережа IPFS автоматично обирає найближчі або найефективніші вузли для доставки контенту. Під час моделювання навіть за умов перевантаження окремих вузлів інші учасники мережі продовжували обслуговувати запити, що унеможливлювало повну втрату доступу до ресурсу.

На відміну від DNS-сценарію, у моделі ENS+IPFS не спостерігалося різкого зростання затримок, деградації швидкодії або ситуацій, коли ресурс ставав повністю недоступним. Інфраструктура не демонструвала різких «провалів» у роботі навіть за змодельованих екстремальних умов навантаження. Це пояснюється відсутністю єдиного фронту атаки, оскільки ні механізм адресації, ні система зберігання не залежать від окремого сервера або вузла.

Ключовою відмінністю ENS+IPFS від традиційної DNS-моделі є неможливість сформувати ефективну централізовану точку атаки. Доменне ім’я не залежить від DNS-провайдера, контент не прив’язаний до одного вебсервера, а сама DDoS-атака не може бути спрямована на один конкретний об’єкт інфраструктури. У результаті ENS+IPFS виявляються структурно несприйнятливими до більшості класичних сценаріїв DDoS-атак, у яких зловмисник обирає конкретну інфраструктурну ціль для перевантаження.

Узагальнення результатів моделювання показало, що традиційна модель DNS у поєднанні з централізованим вебсервером є чутливою до зростання шкідливого трафіку, швидко демонструє деградацію продуктивності та може повністю втратити функціональність. Натомість модель ENS+IPFS характеризується стабільною резолюцією імен, відсутністю єдиних точок відмови та збереженням доступності вебресурсу навіть за умов високого навантаження. Отримані результати підтверджують доцільність використання ENS+IPFS як структурно стійкої архітектури до DDoS-атак і демонструють, що децентралізований підхід здатний суттєво підвищити загальний рівень кіберзахисту вебресурсів.

3.4. Порівняльний аналіз поведінки DNS і ENS+IPFS під час атак

Аналіз результатів проведеного моделювання виявив суттєві відмінності між поведінкою традиційної централізованої DNS-архітектури та децентралізованої моделі ENS+IPFS в умовах інтенсивного навантаження. Хоча обидві системи виконують однакову базову функцію адресації вебресурсів, їх реакція на DDoS-атаки принципово різниться через відмінну архітектурну природу та механізми обробки запитів.

Під час моделювання традиційний DNS-сценарій продемонстрував характерну для централізованих систем деградацію продуктивності. Із зростанням кількості запитів DNS-сервери починали працювати з помітними затримками, а процес резолюції доменних імен вимагав дедалі більше часу. У низці випадків запити не завершувалися в межах допустимого тайм-ауту, доменні імена тимчасово вважалися недоступними, а провайдери кешували помилкові відповіді, що негативно впливало на доступність ресурсу навіть після зменшення інтенсивності атаки. Це свідчить про те, що DNS-система має обмежену та фіксовану пропускну здатність, яка швидко вичерпується під час масованої шкідливої активності.

Окрім збільшення затримок, для DNS були характерні переривання процесу резолюції доменних імен. Під час атаки виникали ситуації, коли домен тимчасово

не знаходився через перевантаження авторитативного сервера, сервер не міг обробити запит або повністю відмовлявся відповідати через перевищення внутрішніх лімітів. Такі помилки виникали нерегулярно та непередбачувано, що унеможливлювало стабільне прогнозування доступності ресурсу. Для кінцевих користувачів це проявлялося у вигляді хаотичної роботи вебсайту, коли сторінка могла відкриватися в один момент і ставати недоступною в наступний.

Паралельно з деградацією DNS-інфраструктури спостерігалося перевантаження вебсерверної частини системи. Вебсервер починав вичерпувати пул доступних з'єднань, зростало споживання оперативної пам'яті та процесорного часу, а також формувалася черга запитів, які не могли бути своєчасно оброблені. У підсумку вебсервер переставав ефективно виконувати функцію обслуговування контенту, навіть якщо формально продовжував працювати.

За умов інтенсивного навантаження традиційний DNS-сценарій переходив у стан повної втрати доступності ресурсу. Це проявлялося у повній відсутності відповідей, неможливості отримати коректний DNS-запис, недоступності IP-адреси, а також у тривалому періоді відновлення після завершення атаки. Отримані результати підтверджують, що DNS є критичною точкою відмови, а DDoS-атака на рівні адресації або вебсерверної інфраструктури здатна повністю зупинити сервіс, навіть якщо сам вебресурс технічно не знищений.

На відміну від традиційної DNS-моделі, децентралізована архітектура ENS+IPFS продемонструвала стабільну та передбачувану поведінку навіть за умов значного навантаження. ENS зберігає всі записи у блокчейні Ethereum, який складається з тисяч незалежних вузлів, що одночасно підтримують актуальний стан реєстру. Унаслідок цього жодна атака типу DDoS не здатна вивести з ладу механізм резолюції імен, оскільки система не використовує DNS-серверів, транзитних мережевих вузлів або централізованих обчислювальних елементів. Навіть за масових запитів дані домену зчитувалися без збоїв і затримок, що робить ENS принципово стійким до атак на інфраструктурному рівні.

IPFS, у свою чергу, забезпечив відмовостійку та розподілену доставку контенту. Під час збільшення трафіку мережа IPFS поводилася стабільно та

передбачувано, оскільки кожен вузол, що має копію контенту, міг брати участь у його розповсюдженні. Система автоматично спрямовувала запити до найближчих або найменш завантажених вузлів, а часткова недоступність окремих шлюзів або нод не впливала на загальну доступність ресурсу. У результаті не виникало «вузьких місць», характерних для класичних вебсерверів.

Навіть у випадку умовної атаки, спрямованої на окремий IPFS-шлюз, інші вузли мережі продовжували обслуговувати запити без порушення доступності ресурсу. Це означає, що в ENS+IPFS неможливо атакувати один сервер для повного виведення сайту з ладу, а сама система природно балансується за рахунок peer-to-peer архітектури. Для досягнення ефекту, аналогічного DDoS у Web2-системах, зловмиснику необхідно було б одночасно впливати на сотні або тисячі незалежних вузлів, що є практично недосяжним з технічної та економічної точок зору.

Результати моделювання показали, що поєднання ENS+IPFS не демонструє деградації продуктивності, не втрачає працездатності та не створює відчутних для користувача затримок навіть під час інтенсивного навантаження. Доступність ресурсу зберігалася протягом усього періоду моделювання, що кардинально відрізняє цю архітектуру від традиційної DNS-моделі. Відсутність централізованої інфраструктури усуває класичні точки прикладення DDoS-атак і забезпечує принципово вищий рівень стійкості до загроз доступності.

Таблиця 3.1

Підсумкова таблиця порівняння

Показник	DNS	ENS+IPFS
Доступність під час атаки	Низька	Висока
Стійкість резолюції	Порушується, значні затримки	Залишається стабільною
Ризик повного відключення	Високий	Практично відсутній
Архітектура	Централізована	Децентралізована

Продовження таблиці 3.1

Підсумкова таблиця порівняння

Показник	DNS	ENS+IPFS
Вплив DDoS на функціональність	Критичний, можливе повне падіння	Мінімальний, ресурс продовжує працювати

Моделювання чітко демонструє, що ENS+IPFS принципово перевершують традиційний DNS з точки зору стійкості до DDoS-атак. Тоді як DNS-архітектура характеризується високою вразливістю через централізовану природу та залежність від окремих серверів, ENS+IPFS забезпечують природну відмовостійкість завдяки блокчейн-технологіям і розподіленому зберіганню контенту.

3.5. Практичні рекомендації щодо впровадження ENS+IPFS у корпоративні системи

На основі проведених теоретичних і практичних досліджень можна сформулювати низку практичних рекомендацій, спрямованих на підвищення стійкості корпоративних вебресурсів до DDoS-атак шляхом впровадження децентралізованої архітектури ENS+IPFS. Запропоновані рекомендації орієнтовані на реальні корпоративні інформаційні системи та можуть бути адаптовані залежно від масштабу інфраструктури, типу сервісів і вимог до доступності.

Ethereum Name Service доцільно розглядати як ефективну альтернативу традиційному DNS для критично важливих корпоративних сервісів. На відміну від класичної системи доменних імен, ENS не містить централізованих вузлів, які можуть стати ціллю DDoS-атаки або об’єктом адміністративного впливу. Використання ENS дозволяє забезпечити стійкість доменних записів до перехоплення чи несанкціонованої модифікації, унеможливити блокування доменів сторонніми організаціями, зменшити залежність від DNS-провайдерів і

регуляторних структур, а також гарантувати доступність доменних записів завдяки зберіганню даних у блокчейні Ethereum. Перехід ключових сервісів на ENS може суттєво знизити ризик простоїв, спричинених атаками на рівні адресації.

Для розміщення корпоративного контенту доцільно використовувати мережу IPFS, особливо у випадках статичних вебсторінок, корпоративних порталів, документації, маркетингових сайтів, каталогів та інших ресурсів з невеликою частотою змін. Розміщення таких матеріалів у IPFS забезпечує розподілене зберігання контенту, що усуває залежність від одного сервера або дата-центру та унеможливлює відмову сервісу внаслідок його перевантаження. Доставка даних здійснюється з найближчих або найменш завантажених вузлів мережі, що підвищує швидкодію та знижує ефективність атак на конкретний хостинг. Додатковою перевагою є криптографічна цілісність контенту, яка гарантує, що користувачі отримують саме той вміст, який було опубліковано, без ризику прихованої підміни. Оскільки IPFS є децентралізованою мережею, для забезпечення постійної доступності корпоративного контенту рекомендується використовувати спеціалізовані сервіси закріплення даних, так звані pinning-сервіси. Такі сервіси забезпечують збереження файлів у мережі IPFS незалежно від активності кінцевих користувачів. Використання хмарних або керованих pinning-рішень дозволяє підтримувати стабільне зберігання критично важливої інформації, забезпечувати дублювання контенту на кількох географічно розподілених вузлах та скорочувати час відновлення доступності у разі локальних збоїв або відмов окремих нод. Це мінімізує ризик втрати доступу до корпоративних ресурсів навіть за умов часткової деградації мережі IPFS.

Для повноцінного впровадження децентралізованої архітектури корпоративні вебсервіси повинні бути технічно підготовлені до інтеграції з ENS та IPFS. Зокрема, необхідно коректно налаштувати параметр contenthash у записах ENS, що забезпечує зв’язок між доменним іменем і відповідним IPFS-контентом. У разі використання розширених функцій або кастомних смарт-контрактів важливо забезпечити можливість оновлення резолвера без порушення доступності сервісу. Корпоративні застосунки також мають підтримувати інтеграцію з Web3-

браузерними API, що дозволяє напряму читати ENS-записи та взаємодіяти з блокчейном. Для забезпечення сумісності з користувачами Web2 доцільно реалізувати дублювання доступу, коли поряд із ENS-доменом надаються посилання через IPFS-шлюзи, що дозволяє поступово переходити до нової моделі адресації без втрати аудиторії.

Важливо розглядати ENS+IPFS не як повну заміну всіх наявних засобів кіберзахисту, а як складову багаторівневої стратегії протидії DDoS-атакам. Децентралізована архітектура усуває критичні точки відмови, властиві централізованим DNS-системам і класичним серверним інфраструктурам, мінімізує ризики спрямованих атак на доступність і забезпечує безперервність роботи сервісів навіть у разі масштабного зовнішнього навантаження. У поєднанні з традиційними механізмами захисту, такими як мережеві фаєрволи, системи моніторингу та аналізу трафіку, ENS+IPFS формують комплексну систему захисту нового покоління, побудовану на принципах децентралізації.

Наведені рекомендації підтверджують, що інтеграція ENS+IPFS має значний потенціал для використання в корпоративних інформаційних системах, які прагнуть мінімізувати ризики простоїв, пов’язаних із DDoS-атаками. За умови правильної технічної реалізації та поетапного впровадження організації можуть створити високодоступні вебресурси, стійкі до інфраструктурних збоїв і кібератак, що повністю відповідає сучасним вимогам безпеки та розвитку Web3-екосистеми.

ВИСНОВКИ

У дипломній роботі було проведено всебічне, комплексне та багаторівневе дослідження проблеми забезпечення стійкості вебресурсів до DDoS-атак, а також ґрунтовно проаналізовано можливість застосування децентралізованих технологій ENS та IPFS як сучасної альтернативи традиційній DNS-інфраструктурі. У ході дослідження встановлено, що проблема протидії DDoS-атакам не обмежується технічними аспектами фільтрації трафіку чи застосуванням окремих засобів захисту. Вона має насамперед архітектурний характер, оскільки значна частина вразливостей випливає безпосередньо з принципів побудови класичної системи доменних імен.

Поглиблений аналіз теоретичних основ роботи DNS показав, що ця система, незважаючи на десятиліття розвитку та численні вдосконалення, залишається централізованою за своєю природою. Її структура включає кореневі DNS-сервери, сервери доменів верхнього рівня та авторитетні сервери, що обслуговують домени другого й наступних рівнів. Кожен із цих компонентів є необхідним елементом загальної інфраструктури, однак водночас становить критичну точку відмови. У разі спрямованої атаки на будь-який із цих елементів ланцюг резолюції доменних імен може бути порушено, що автоматично призводить до недоступності пов’язаних вебресурсів, навіть якщо їхні сервери залишаються повністю працездатними.

Особливо небезпечним є той факт, що кореневі та TLD-сервери мають глобальне значення, а отже стають надзвичайно привабливими цілями для атак масштабного характеру. Досвід реальних інцидентів, таких як DDoS-атака на DNS-провайдера Dyn у 2016 році, демонструє, що компрометація одного з вузлів може спричинити масштабні збої в роботі тисяч популярних сервісів. Таким чином, централізована модель DNS у сучасних умовах високої інтенсивності та доступності інструментів атакуємих технологій перетворюється на системний ризик для всього інтернет-середовища.

У дипломній роботі також було детально проаналізовано традиційні методи протидії DDoS-атакам, зокрема використання CDN-платформ, Anycast-архітектури, систем веб-аплікаційного захисту , а також хмарних scrubbing-центрів, краще відомих як DDoS-миттєвими «чистильними» сервісами. Попри значну ефективність цих рішень у пом'якшенні наслідків атак, вони працюють реактивно, тобто розв'язують проблему вже після початку атаки. Крім того, вони не усувають базову архітектурну вразливість — існування точки, на яку можна спрямувати перевантаження.

Важливо підкреслити, що навіть найпотужніші комерційні CDN-мережі або протидійні сервіси здатні лише розподіляти навантаження та відсікати шкідливий трафік, але не можуть ліквідувати залежність від DNS. Атака на авторитетний сервер домену, через який проходить резолюція, робить недоступним домен незалежно від наскільки ефективно захищено сам вебсайт. Саме тому традиційні підходи забезпечують лише тимчасове підвищення стійкості, а не принципове вирішення проблеми.

Проведений аналіз дозволив сформувати висновок, що для підвищення стійкості вебресурсів до DDoS-атак необхідно переходити від реактивної моделі захисту до архітектурно нового підходу, в основі якого лежить усунення централізованих точок відмови. Саме таку можливість відкриває застосування децентралізованих технологій ENS та IPFS, які дозволяють реалізувати доменну систему нового покоління — без серверів, без одноосібних провайдерів і без централізованих вузлів, чиє падіння може призвести до повної втрати доступності вебресурсу.

У ході роботи було встановлено, що ENS як децентралізована система доменних імен усуває ключові структурні вразливості DNS. ENS зберігає записи у мережі Ethereum, що виключає можливість підміни чи маніпуляції доменом з боку провайдера. Резолюція імен у ENS не покладається на DNS-сервери, а отже — позбавлена тих точок відмови, які традиційно стають цілями для DDoS-атак. У свою чергу IPFS забезпечує розподілену модель зберігання вебконтенту, у якій немає центрального сервера, здатного стати жертвою перевантаження чи знищення.

Поєднання ENS і IPFS створює нову архітектуру доступу до вебресурсів, у якій як адресація, так і передача даних здійснюються децентралізовано, із застосуванням криптографічних гарантій цілісності та автономної роботи мережі.

Практична частина дослідження включала розгортання двох тестових середовищ: вебресурсу, що використовує традиційний DNS, та сайту, опублікованого через ENS і IPFS. Під час моделювання DDoS-атак традиційна DNS-архітектура продемонструвала критичну вразливість. Різко збільшився час відповіді DNS, з'явилися численні помилки резолюції, а робота вебсервера стала нестабільною. У піковий момент атаки ресурс, що працював на основі DNS, став повністю недоступним. У той самий час система ENS+IPFS зберегла цілковиту доступність: домен коректно резольвився через блокчейн, а контент успішно отримувався з різних вузлів IPFS без видимих затримок і без втрати функціональності. Навіть під інтенсивним навантаженням не було зафіксовано ознак деградації резолюції чи порушення доступності даних.

Порівняльний аналіз результатів продемонстрував суттєву перевагу ENS+IPFS у контексті стійкості до DDoS-атак. На відміну від DNS, який залежить від централізованої інфраструктури, ENS+IPFS функціонують у децентралізованому середовищі, де повністю відсутні точки відмови. Це дозволяє забезпечити стабільність роботи вебресурсів навіть у випадку масштабних атак. Записи ENS є незмінними завдяки зберіганню у блокчейні, а модель IPFS гарантує розподілену доступність контенту без можливості його блокування чи видалення централізованим суб'єктом. Таким чином, ENS+IPFS формують нову парадигму побудови стійких інформаційних систем, у яких від самого початку усуваються архітектурні причини, що дозволяють реалізовувати DDoS-атаки на рівні інфраструктури.

Загалом отримані результати підтверджують доцільність впровадження ENS і IPFS у практику захисту критично важливих сервісів, корпоративних мереж та державних ресурсів. Децентралізовані технології здатні істотно підвищити рівень безпеки та доступності вебресурсів, пропонуючи підхід, який не обмежується реакцією на атаки, а передбачає структурне усунення їх основних векторів.

Проведене дослідження демонструє, що ENS+IPFS є перспективним напрямом розвитку сучасної кібербезпеки та можуть стати ключовим компонентом майбутніх інтернет-інфраструктур, орієнтованих на максимальну стійкість і безпеку.

ПЕРЕЛІК ПОСИЛАНЬ

1. Blockchain and interplanetary file system (ipfs)-based data storage system for vehicular networks. *Mdpi*. URL: https://www.mdpi.com/2079-9292/12/7/1545 (дата звернення: 01.12.2025).
2. DDoS attack - HackYourMom. *HackYourMom*. URL: https://hackyourmom.com/en/kibervijna/dosddos/denial-of-service-ddos-ataka/

   (дата звернення: 01.12.2025).
3. ENS: decentralized domain name system of the web3 generation. *Whitebit*. URL: https://blog.whitebit.com/en/ens-decentralized-domain-name-system/ (дата звернення: 01.12.2025).
4. Explained : InterPlanetary File System (IPFS). *Binance Square*. URL: https://www.binance.com/uk-UA/square/post/275467(дата звернення: 10.12.2025).
5. Fleek documentation. *Fleek*. URL: https://resources.fleek.xyz/docs/

   (дата звернення: 10.12.2025) .
6. IPFS documentation | IPFS docs. *IPFS Documentation | IPFS Docs*. URL: https://docs.ipfs.tech (дата звернення: 10.12.2025).
7. The interplanetary file system (IPFS) | Giuliano mega. *Giuliano Mega*. URL: https://www.giulianomega.com/post/2023-08-03-ipfs/

   (дата звернення: 10.12.2025).
8. What is a DDoS attack?. *Cloudflare*. URL: https://developers.cloudflare.com/learning-paths/prevent-ddos-attacks/concepts/ddos-attacks/

   (дата звернення: 18.12.2025)..

9. What is Ethereum name service (ENS)?. *Binance*. URL: https://www.binance.com/en/academy/articles/what-is-ethereum-name-service-ens

(дата звернення: 18.12.2025).

10. What is the Ethereum name service?. *ENS Documentation*. URL: https://docs.ens.domains/learn/protocol/ (дата звернення: 18.12.2025).

11. How to host your dapp with IPFS+ENS and access it via ethdns. *Medium*. URL: https://makoto-inoue.medium.com/how-to-host-your-dapp-with-ipfs-ens-and-access-it-via-ethdns-c96046059d87 (дата звернення: 18.12.2025).