Міністерство освіти і науки України
Харківський національний університет імені В.Н. Каразіна
Навчально-науковий інститут комп'ютерних наук та штучного інтелекту
Спеціальність 125 «Кібербезпека»
Освітня програма «Кібербезпека»

В.о. зав. кафедрою КІСМіТ
Марина ЄСІНА
"Допущено до захисту"

« »_____2025р.

Пояснювальна записка
до кваліфікаційної роботи бакалавра

на тему: «Аналіз технології шифрування DNS та дослідження проблем виявлення зловмисного трафіку»

оцінка « »

Голова ЕК

Мичуда Л.З.

Керівник: к.т.н. Малахов С.В.

Рецензент: PhD
доцент кафедри інтелектуальних
програмних систем і технологій
Родінко М. Ю

Виконавець: студентка групи КБ-41
Кузнецова Є.О.

Харків 2025

РЕФЕРАТ

Пояснювальна записка містить 58 сторінок, 15 рисунків, 9 таблиць, 9 додатків, 149 джерел.

Метою дипломної роботи є аналіз сучасних технологій шифрування DNS трафіку (зокрема, DNS over HTTPS та DNS over TLS) та дослідження труднощів, що виникають при реалізації процедур виявленні зловмисного трафіку в умовах використання протоколів шифрування DNS.

Об’єкт дослідження: технології, методи та способи забезпечення кібербезпеки в сучасних інформаційно-комунікаційних системах в умовах використання шифрованого DNS трафіку.

Предмет дослідження: процедури аналізу і виявлення шкідливого трафіку у зашифрованих DNS-запитах та можливості з покращення засобів фільтрації і моніторингу DNS трафіку.

Основними методами дослідження є: аналіз відомостей про інциденти безпеки, моделювання мережевих сценаріїв та узагальнення даних лог-файлів моніторингу DNS запитів, а також тестування засобів (Wireshark, Zeek, Pi-hole, Splunk) виявлення аномалій DNS трафіку з широким залученням технології машинного навчання.

Узагальнення отриманих результатів, свідчить про доцільність реалізації архітектури багаторівневого захисту DNS трафіку. Його головна мета полягає в одночасному комплексуванні інструментів з фільтрації, моніторингу, аналітики та протидії, при умові широкої інтеграції поведінкових модулів на базі AI та ML.

Ключові слова: DNS, DOH, DOT, ШИФРУВАННЯ ТРАФІКУ, ВИЯВЛЕННЯ АНОМАЛІЙ, DNS TUNNELING, DGA, WIRESHARK, ZEEK, SPLUNK, КІБЕРЗАГРОЗИ, ІНФОРМАЦІЙНА БЕЗПЕКА.

ABSTRACT

The explanatory note contains 58 pages, 15 figures, 9 tables, 9 appendices, and 149 references.

The aim of this thesis is to analyze modern DNS traffic encryption technologies (in particular, DNS over HTTPS and DNS over TLS) and to investigate the challenges arising in the implementation of malicious traffic detection procedures under conditions of DNS encryption.

Object of the research: technologies, methods, and approaches for ensuring cybersecurity in modern information and communication systems in the context of encrypted DNS traffic.

Subject of the research: procedures for analyzing and detecting malicious traffic within encrypted DNS queries and the possibilities for improving DNS traffic filtering and monitoring tools.

The main research methods include: analysis of security incident data, modeling of network scenarios, and generalization of DNS request monitoring log data, as well as testing tools (Wireshark, Zeek, Pi-hole, Splunk) for detecting DNS traffic anomalies, with extensive use of machine learning technologies.

The generalization of the obtained results indicates the feasibility of implementing a multi-layered DNS traffic protection architecture. Its main goal is to simultaneously integrate tools for filtering, monitoring, analytics, and counteraction, provided there is widespread integration of behavior-based modules built on AI and ML.

Keywords: DNS, DOH, DOT, TRAFFIC ENCRYPTION, ANOMALY DETECTION, DNS TUNNELING, DGA, WIRESHARK, ZEEK, SPLUNK, CYBERSECURITY, INFORMATION SECURITY.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СКОРОЧЕНЬ ТА СИМВОЛІВ

AI — Artificial Intelligence (штучний інтелект)

APNIC — Asia-Pacific Network Information Centre (Азіатсько-Тихоокеанський мережевий інформаційний центр)

APT — Advanced Persistent Threat (удосконалена постійна загроза)

AS — Autonomous System (автономна система)

CA — Certificate Authority (центр сертифікації)

CCPA — California Consumer Privacy Act (Каліфорнійський закон про захист приватності споживачів)

CDN — Content Delivery Network (мережа доставки контенту)

CNN — Convolutional Neural Network (згорткова нейронна мережа)

C&C — Command and Control (командування та управління)

DDoS — Distributed Denial of Service (розподілена атака типу "відмова в обслуговуванні")

DGA — Domain Generation Algorithm (алгоритм генерації доменів)

DHCP — Dynamic Host Configuration Protocol (протокол динамічної конфігурації хоста)

DLP — Data Loss Prevention (запобігання витоку даних)

DNS — Domain Name System (система доменних імен)

DNSSEC — Domain Name System Security Extensions (розширення безпеки системи доменних імен)

DoH — DNS over HTTPS (DNS через HTTPS)

DoQ — DNS over QUIC (DNS через QUIC)

DoT — DNS over TLS (DNS через TLS)

DPI — Deep Packet Inspection (глибока інспекція пакетів)

DS — Delegation Signer (підписант делегування)

EDR — Endpoint Detection and Response (виявлення та реагування на кінцевих точках)

GDPR — General Data Protection Regulation (Загальний регламент про захист даних)
GPO — Group Policy Object (об'єкт групової політики)
GRU — Gated Recurrent Unit (стробована рекурентна ланка)
HTTP — Hypertext Transfer Protocol (протокол передачі гіпертексту)
HTTPS — Hypertext Transfer Protocol Secure (захищений протокол передачі гіпертексту)
ICANN — Internet Corporation for Assigned Names and Numbers (Інтернет-корпорація з присвоєння імен та номерів)
IDC — International Data Corporation (Міжнародна корпорація даних)
IDS — Intrusion Detection System (система виявлення вторгнень)
IETF — Internet Engineering Task Force (інженерна група з інтернет-технологій)
IoT — Internet of Things (інтернет речей)
IP — Internet Protocol (інтернет-протокол)
IPS — Intrusion Prevention System (система запобігання вторгненням)
ISOC — Internet Society (Інтернет-суспільство)
KSK — Key Signing Key (ключ підписання ключів)
LIME — Local Interpretable Model-agnostic Explanations (локальні інтерпретовні пояснення незалежні від моделі)
LSTM — Long Short-Term Memory (довгострокова короткочасна пам'ять)
MDM — Mobile Device Management (управління мобільними пристроями)
ML — Machine Learning (машинне навчання)
MTTD — Mean Time To Detection (середній час виявлення)
MTTR — Mean Time To Response (середній час реагування)
NGFW — Next Generation Firewall (міжмережевий екран нового покоління)
NSEC — Next Secure (наступний захищений)
NTA — Network Traffic Analysis (аналіз мережевого трафіку)
NXDOMAIN — Non-Existent Domain (неіснуючий домен)

PCA — Principal Component Analysis (аналіз головних компонент)
QUIC — Quick UDP Internet Connections (швидкі UDP інтернет-з'єднання)
RFC — Request for Comments (запит коментарів)
RNN — Recurrent Neural Network (рекурентна нейронна мережа)
RPZ — Response Policy Zone (зона політики відповідей)
RRSIG — Resource Record Signature (підпис ресурсного запису)
SANS — SysAdmin, Audit, Network, and Security Institute (інститут системного адміністрування, аудиту, мережі та безпеки)
SHAP — SHapley Additive exPlanations (пояснення адитивності Шеплі)
SIEM — Security Information and Event Management (управління інформацією та подіями безпеки)
SOAR — Security Orchestration, Automation and Response (оркестрація, автоматизація та реагування безпеки)
SOCKS — Socket Secure (захищений сокет)
SSL — Secure Sockets Layer (рівень захищених сокетів)
SVM — Support Vector Machine (метод опорних векторів)
TCP — Transmission Control Protocol (протокол управління передачею)
TLD — Top Level Domain (домен верхнього рівня)
TLS — Transport Layer Security (безпека транспортного рівня)
TOR — The Onion Router (цибулевий маршрутизатор)
TTL — Time To Live (час життя)
TXT — Text Record (текстовий запис)
UDP — User Datagram Protocol (протокол користувацьких дейтаграм)
VPN — Virtual Private Network (віртуальна приватна мережа)
XAI — Explainable Artificial Intelligence (пояснювальний штучний інтелект)
ZSK — Zone Signing Key (ключ підписання зони)

ВСТУП

DNS (Domain Name System) є ключовою інфраструктурною складовою Інтернету, що забезпечує трансляцію доменних імен у IP-адреси. Проте, через відсутність вбудованих механізмів захисту, традиційна архітектура DNS залишається вразливою до атак, таких як Cache Poisoning, DNS Hijacking і перехоплення запитів [1].

З метою підвищення конфіденційності користувачів, фахівцями з питань інформаційної безпеки (ІБ) було розроблено й впроваджено механизми шифрування DNS-запитів: – DNS-over-HTTPS (DoH) та DNS-over-TLS (DoT). Ці технології швидко набули поширення, однак створили нові виклики для систем кібербезпеки. Причина проста - зашифрований трафік ускладнює виявлення шкідливої активності, включаючи C&C-з'єднання, ботнети та DNS-тунелювання.

В цьому випадку склався певний парадокс: засоби, покликані захищати приватність користувачів, почали використовуватись зловмисниками для обходу систем кібербезпеки. За даними досліджень [13], організації, не адаптовані до шифрованого DNS, втрачають до 80% ефективності у виявленні загроз.

Метою даної роботи є аналіз впливу шифрування DNS-трафіку на безпеку мережевої інфраструктури і інформаційних ресурсів сучасних ІС та дослідження (в т.ч. моделювання) можливих способів виявлення, та парирування відповідних загроз.

Актуальність теми: Шифрування DNS-трафіку (DoH, DoT) [5] стало відповіддю на потребу захисту конфіденційності користувачів, проте ускладнило роботу традиційних систем безпеки, що покладалися на відкритий аналіз DNS-запитів (ботнети, DGA-домени, тунелювання) [7]. Централізація обробки DNS у великих провайдерів та зниження прозорості трафіку створюють нові виклики, особливо для корпоративних мереж. Зростання складності атак, зокрема із застосуванням AI, вимагає розробки нових методів моніторингу навіть в умовах обмеженої видимості.

1 ОСОБЛИВОСТІ ФУНКЦІОНУВАННЯ СИСТЕМИ DNS ТА УЗАГАЛЬНЕННЯ ПРОБЛЕМАТИКИ ЇЇ ВРАЗЛИВОСТЕЙ

Domain Name System (DNS) є фундаментальною технологією інтернету для перетворення доменних імен у IP-адреси. Система, розроблена в 1980-х роках, має низку вразливостей через відсутність початкових механізмів захисту [1]. Вразливості DNS становлять серйозну загрозу, оскільки можуть призвести до перенаправлення трафіку, витоку даних та відмови в обслуговуванні, а кількість атак на DNS інфраструктуру щороку зростає [2]. Розвиток AI/ML технологій відкриває нові можливості для захисту DNS, але створює виклики через потенційне використання цих технологій зловмисниками. Тому комплексне дослідження вразливостей DNS є актуальним завданням кібербезпеки [3].

1.1 Аналіз принципів і механізмів функціонування DNS та визначення характерних вразливостей цієї системи

1.1.1 Принципи функціонування DNS

DNS (Domain Name System) - це розподілена ієрархічна система іменування, що забезпечує перетворення зрозумілих для людини доменних імен (наприклад, www.example.com) у числові IP-адреси (наприклад, 192.0.2.1), які використовуються комп'ютерами для комунікації в мережі [4].

1.1.1.1 Структура системы DNS

1) DNS-сервери — комп'ютери, що зберігають інформацію про доменні імена та відповідні їм IP-адреси (див. Таблиця 1.1).

Таблиця 1.1 - Класифікація DNS-серверів за функціональним призначенням

Тип сервера	Опис
Кореневі сервери (Root DNS servers)	Зберігають інформацію про сервери верхнього рівня. Це перші сервери, до яких звертається резолвер під час перетворення доменного імені в IP-адресу.

Продовження таблиці 1.1

Тип сервера	Опис
Сервери доменів верхнього рівня (TLD DNS servers)	Відповідають за домени першого рівня (.com, .org, .ua тощо) та надають інформацію про авторитативні сервери для конкретних доменів.
Авторитативні сервери (Authoritative DNS servers)	Містять інформацію про конкретні домени і надають відповіді на запити про записи в цих доменах.
Рекурсивні резолвери (Recursive resolvers)	Отримують запити від клієнтів і проходять весь ланцюжок DNS-запитів від кореневих серверів до авторитативних, щоб отримати необхідну інформацію.

2) DNS-записи — інформаційні елементи, що зберігаються на DNS-серверах і містять різні типи даних (див. Таблиця 1.2).

Таблиця 1.2 - Класифікація ресурсних записів у системі DNS

Тип запису	Призначення	Приклад
A	Зв'язує доменне ім'я з IPv4-адресою	example.com → 192.0.2.1
AAAA	Зв'язує доменне ім'я з IPv6-адресою	example.com → 2001:0db8:85a3:0000:0000:8a2e:0370:7334
MX	Вказує на поштові сервери домену	example.com → mail.example.com
CNAME	Створює псевдонім для домену	www.example.com → example.com

Продовження таблиці 1.2

Тип запису	Призначення	Приклад
TXT	Містить текстову інформацію про домен	example.com → "v=spf1 include:_spf.example.com ~all"
NS	Вказує авторитативні сервери для домену	example.com → ns1.example.com

3) DNS-протокол — набір правил, що визначає формат DNS-повідомлень та порядок обміну ними між клієнтами та серверами.

- Транспортний рівень: Використовує порт 53 як для TCP, так і для UDP з'єднань
- Формат повідомлень: Включає заголовок і секції запитань, відповідей, уповноважених серверів і додаткової інформації
- Типи запитів: Дозволяє робити рекурсивні та нерекурсивні запити

1.1.1.2 Механізм роботи DNS-запиту

Типовий процес розв'язання DNS-запиту включає наступні етапи:

1) Користувач вводить доменне ім'я (наприклад, www.example.com) у браузері.
2) Операційна система перевіряє локальний кеш DNS-записів.
3) Якщо запис не знайдено в кеші, запит надсилається до налаштованого DNS-резолвера (програма чи сервіс (умовно - DNS-відповідач), що забезпечує/підтримує функцію перетворення та/чи зберігання доменних імен). Така функція, зазвичай підтримується у провайдера інтернет-послуг).
4) Резолвер перевіряє власний кеш і, якщо запис відсутній, ініціює рекурсивний запит:
    - Спочатку звертається до кореневих DNS-серверів;
    - Отримує адреси серверів домену верхнього рівня (наприклад, .com);

- Звертається до серверів домену верхнього рівня та отримує адреси авторитативних серверів для конкретного домену;
- Звертається до авторитативних серверів домену для отримання IP-адреси [8]

5) Резолвер повертає отриману IP-адресу клієнту та зберігає її у своєму кеші на визначений час (TTL - Time To Live).
6) Клієнт використовує отриману IP-адресу для встановлення з'єднання з веб-сервером [9].

1.1.2 Характерні вразливості DNS

Система DNS має низку вразливостей, що можуть бути використані зловмисниками [10-20]:

1) DNS Cache Poisoning - підміна легітимних DNS-записів у кеші резолвера фальшивими, що перенаправляє користувачів на шкідливі сайти [10].
2) DNS Amplification Attack - DDoS-атака з використанням підробленої IP-адреси жертви для генерації великого обсягу трафіку через відкриті DNS-резолвери [11].
3) DNS Tunneling - використання DNS-протоколу для передачі неавторизованого трафіку, обходячи системи безпеки та забезпечуючи витік даних [12].
4) NXDOMAIN Attack - перевантаження DNS-серверів запитами до неіснуючих доменів для вичерпання ресурсів [13].
5) DNS Hijacking - зміна налаштувань DNS-серверів для перенаправлення запитів на контрольовані зловмисником сервери [14].
6) Zone Transfer Attacks - неавторизоване отримання повної копії DNS-записів домену через незахищений механізм передачі зон [15].
7) DNS Rebinding - обхід політики same-origin в браузерах шляхом зміни DNS-записів під час активної сесії [16].
8) Fast Flux DNS - швидка зміна IP-адрес у DNS-записах для приховування фішингових сайтів та ботнет-інфраструктури [17].

9) DNSSEC Downgrade Attacks - примусове відключення механізмів безпеки DNSSEC для проведення інших атак на DNS [18].
10) DNS Water Torture Attack - генерація великої кількості запитів до випадкових піддоменів для перевантаження авторитативних серверів [19].

Ці вразливості є наслідком початкового проектування DNS без урахування сучасних вимог безпеки, зокрема, відсутності автентифікації та шифрування в оригінальному протоколі DNS [20].

1.2 Узагальнення відомих інцидентів безпеки, що пов'язані з експлуатацією вразливостей DNS

Протягом останніх десятиліть експлуатація вразливостей DNS, призвела до численних інцидентів безпеки, котрі мали суттеві наслідки для організацій, урядових установ і звичайних користувачів. Аналіз цих інцидентів дозволяє краще зрозуміти еволюцію атак на DNS та розробити більш ефективні стратегії захисту. Нижче стисло наведено результати систематизації огляду з найбільш значущих інцидентів безпеки, котрі експлуатають різні вразливості DNS.

DDoS-атаки з підсиленням через DNS (DNS Amplification/Reflection) стали одним із найпоширеніших типів мережевих атак через їхню відносну простоту реалізації та руйнівний потенціал. Перелік та зміст найбільш показових інцидентів з реалізацією атаки DNS Amplification [21-23], наведено в Додатку А.

Масштабні кампанії атак типу DNS Hijacking (перехоплення DNS) є потужним інструментом в арсеналі кіберзлочинців та хакерських груп. Перелік та зміст найбільш показових інцидентів з реалізацією DNS Hijacking [24-26], наведено в Додатку А.

Атаки на кеш DNS та інші методи т.з. «отруєння» DNS, залишаються серйозною загрозою, незважаючи на впровадження захисних механізмів безпеки. Перелік та зміст найбільш характених інцидентів з реалізацією цього різновиду вразливості [27-29], розглянуто в Додатку А.

Інциденти, що пов'язані з DNS Tunneling, нажаль стали потужним методом для обходу існуючих систем безпеки та створення прихованих каналів передачі

даних для злочинців [30-32]. Приклади і особливості найбільш показових інцидентів з реалізацією DNS Tunneling, наведено в Додатку А.

Експлуатація вразливостей типу Fast Flux DNS. Техніка виконання атак Fast Flux DNS використовується зловмисниками для підвищення стійкості власної шкідливої (в т.ч. навмисно стореної) інфраструктури [33-34]. Більш докладніше, особливості інцидентів з реалізацією цього різновиду атак, розглянуто в Додатку А.

1.2.1 Узагальнення тенденцій й наслідків відомих інцидентів

Аналіз відомих інцидентів безпеки, що пов'язані з вразливостями DNS, дозволяє визначити декілька кілька ключових тенденцій:

1) Зростання масштабу атак: - якщо раніше DDoS-атаки з використанням DNS вимірювалися в гігабітах за секунду, то сучасні атаки досягають терабітних масштабів. Це пов'язано з розвитком технологій, збільшенням кількості потенційно вразливих пристроїв та вдосконаленням методів атак [35];

2) Підвищення складності атак: - сучасні атаки на DNS часто є багатовекторними та використовують комбінацію різних технік. Наприклад, атаки можуть поєднувати DNS Hijacking з DNS Tunneling для досягнення максимального ефекту [36];

3) Державно-спонсоровані атаки: - значна частина сучасних складних DNS-атак пов'язана з діяльністю хакерських груп, що підтримуються державами. Такі атаки зазвичай мають високий рівень технічної складності та спрямовані на досягнення геополітичних цілей [37];

4) Економічні наслідки: - за оцінками аналітиків, середня вартість інциденту DNS для організації становить близько 924 000 доларів США, включаючи прямі збитки, витрати на відновлення та репутаційні втрати [38].

Проведений аналіз наслідків відомих інцидентів ІБ, котрі були пов’язані з проблемами безпеки DNS, дозволив їх класифікувати за кількома ключовими категоріями, результати котрих наведені в табл.1.3.

1.2.2 Бліц-огляд ефективності запроваджених методів протидії

Аналіз розглянутих інцидентів, демонструє різну ефективність, стосовно використовуваних методів й способів захисту:

1) DNSSEC - впровадження DNSSEC значно підвищує захищеність від атак типу кеш-отруєння, проте рівень його впровадження залишається недостатнім. Станом на 2023 рік, лише близько 30% доменів верхнього рівня та менше 5% всіх доменів повністю підтримують DNSSEC [39];

Таблиця 1.3 - Класифікація наслідків DNS-інцидентів

Категорія наслідків	Опис	Приклади інцидентів
Фінансові втрати	Прямі фінансові збитки внаслідок викрадення коштів, простою систем або витрат на відновлення	Атаки на бразильські банки (2017), Operation Ghost Click (2007-2011)
Витік конфіденційних даних	Викрадення особистої інформації, облікових даних, комерційної таємниці або державних секретів	Операція "Sea Turtle" (2017-2019), DNSpionage (2018-2019)
Порушення доступності сервісів	Тимчасова або тривала недоступність веб-сервісів через DDoS-атаки або інші порушення роботи DNS	Атака на Dyn (2016), Атака на Spamhaus (2013)
Репутаційні втрати	Зниження довіри клієнтів та партнерів внаслідок інцидентів безпеки	Більшість публічно розкритих інцидентів
Компрометація системи безпеки	Отримання зловмисниками неавторизованого доступу до внутрішніх систем через маніпуляції з DNS	Операція "Cobalt Kitty" (2016-2017), Wekby APT (2015)

2) DNS over HTTPS (DoH) та DNS over TLS (DoT) - ці протоколи шифрування DNS-трафіку ефективно захищають від перехоплення та підміни

DNS-запитів, але створюють нові виклики для корпоративної безпеки, зокрема, ускладнюють моніторинг DNS-трафіку та виявлення аномалій [40];

3) Системи виявлення та запобігання вторгненням (IDS/IPS) - аналіз показує, що традиційні системи IDS/IPS часто неефективні проти сучасних складних DNS-атак, особливо тих, що використовують техніки тунелювання або швидкої зміни (Fast Flux) [41];

4) Поведінковий аналіз - рішення на основі поведінкового аналізу демонструють вищу ефективність у виявленні аномалій у DNS-трафіку, але вимагають значного часу для налаштування та часто продукують хибно-позитивні результати [42].

В цілому, вивчення відомих інцидентів безпеки свідчить про необхідність комплексного підходу до захисту DNS-інфраструктури, що включає технічні, організаційні та освітні заходи.

1.3 Можливості технологій штучного інтелекту і машинного навчання (AI/ML) для покращення рівня безпеки DNS трафіку

1.3.1 Основні напрямки застосування AI/ML у безпеці DNS

Технології штучного інтелекту та машинного навчання можуть бути застосовані для вирішення різноманітних завдань у сфері безпеки DNS:

1) Виявлення аномалій у DNS-трафіку - алгоритми машинного навчання здатні ідентифікувати незвичні патерни у DNS-запитах, що можуть свідчити про зловмисну активність (DNS tunneling, DGA-домени, Fast Flux тощо) [43].
2) Прогнозування DNS-атак - предиктивні моделі можуть аналізувати історичні дані та виявляти ранні ознаки підготовки до атак на DNS-інфраструктуру [44].
3) Класифікація доменів - методи ML дозволяють ефективно категоризувати домени як зловмисні або легітимні на основі численних характеристик, включаючи лексичні особливості, історію реєстрації, поведінку та контекст їх використання [45].

4) Виявлення DGA-доменів - виявлення доменів, згенерованих алгоритмічно (Domain Generation Algorithms), що часто використовуються у шкідливому програмному забезпеченні для уникнення статичних чорних списків [46].
5) Оптимізація фільтрації та блокування - підвищення ефективності систем фільтрації DNS-трафіку шляхом адаптивного налаштування правил блокування на основі аналізу патернів запитів [47].
6) Автоматизоване реагування на інциденти - системи на основі AI можуть не лише виявляти загрози, але й автоматично реагувати на них, застосовуючи відповідні контрзаходи [48].

Методи машинного навчання для аналізу DNS-трафіку розглянуто у додатку Б.

1.3.2 Аналіз характеристик DNS для виявлення загроз

Ефективність методів AI/ML значною мірою залежить від вибору релевантних характеристик для аналізу. У контексті DNS-безпеки виділяють наступні групи:

1) Лексичні характеристики доменного імені:
   - Довжина доменного імені
   - Ентропія символів
   - Частота вживання певних символів
   - Співвідношення голосних і приголосних літер [49]
2) Характеристики DNS-запитів:
   - Частота запитів
   - Розподіл типів записів (A, AAAA, MX, TXT тощо)
   - Часові інтервали між запитами
   - Кількість запитів до неіснуючих доменів (NXDOMAIN) [50]
3) Мережеві характеристики:
   - IP-адреси, пов'язані з доменом
   - Географічний розподіл серверів
   - Автономні системи (AS), що обслуговують домен [51]
4) Часові характеристики:
   - Вік домену

- Історія змін DNS-записів
- Патерни активності в різний час доби [52]

Деталізовану оцінку ефективності методів AI/ML при виявленні різних типів атак на DNS, включаючи таблицю зі співвідношенням типів атак і відповідних алгоритмів, а також огляд ключових викликів та перспектив їх подолання наведено у Додатку Б.

2 АНАЛІЗ ТЕХНОЛОГІЙ ШИФРУВАННЯ DNS ТА ШЛЯХИ ПОКРАЩЕННЯ КОНТРОЛЮ DNS-ТРАФІКУ

У контексті постійної еволюції кіберзагроз, традиційний незашифрований DNS становить суттєву вразливість у сучасній мережевій інфраструктурі. Це обумовлено фундаментальними особливостями початкової архітектури DNS, створеної в той час, коли питання приватності й безпеки користувачів не мали критичного значення. У даному розділі представлено комплексний аналіз технологій шифрування DNS, особливості їх впровадження та вплив на загальну безпеку й продуктивність мереж. Крім того окремо розглянути питання взаємодії цих технологій із суміжними (іншими) системами захисту інформації.

2.1 Узагальнення етапів розвитку і порівняння технологій шифрування DNS

Розвиток технологій шифрування (Encryption) DNS трафіку, відображає загальну тенденцію сучасних інформаційних технологій, стосовно посилення захисту користувацьких даних та протидії постійно зростаючим кіберзагрозам. Так, кожен етап еволюції шифрування DNS, характеризується впровадженням нових криптографічних механізмів, оптимізацією протоколів передачі даних та постійним пошуком балансу між безпекою, приватністю і продуктивністю.

Так наприклад, DNSCrypt став першим широко розповсюдженим протоколом шифрування DNS [74-77], що заклав концептуальну основу для подальшого розвитку технологій захисту DNS. Основні властивості та деякі практичні рекомендації, щодо цього протоколу розглянути в Додатку В.

Протокол DoT (DNS-over-TLS) став першим стандартизованим протоколом шифрування DNS, що забезпечує захист на транспортному рівні [78-81]. Основні відомості, стосовно цього протоколу представлені в Додатку В.

Наступний, в ґенезі розвитку, протокол DoH (DNS-over-HTTPS) запропонував користувачам найбільш революційний підхід до шифрування DNS,

що ґрунтується на інтеграції DNS з інфраструктурою веб [82-85]. Основні відомості і властивості, щодо цього протоколу представлено в Додатку В.

І нарешті, протокол DoQ (DNS-over-QUIC) представляє найновішу ітерацію в еволюції технологій шифрування DNS [86-89], поєднуючи основні переваги сучасних транспортних протоколів. Більш детально основні властивості та особливості реалізації цього протоколу представлені в Додатку В.

Для ґрунтовного розуміння існуючих переваг та обмежень різних технологій (протоколів) шифрування DNS, проведено їх порівняльний аналіз. Його результати акумульовано в Табл. 2.1 [90]. Важливо підкреслити, що в межах складання цієї таблиці та інтеграції окремих показників, особливу увагу було приділено не лише суто технічним характеристикам, але й соціо-технічним аспектам (в т.ч. соціальнго інжинірінгу) впровадження відповідних рішень, включаючи підтримку розробниками програмного забезпечення (ПЗ), сумісність з існуючою ІТ-інфраструктурою та стійкість до різних видів обмежень і блокувань.

Таблиця 2.1 - Порівняльний аналіз основних технологій шифрування DNS

Характеристика	DNSCrypt	(DoT)	(DoH)	(DoQ)
Рік впровадження	2011	2016	2018	2020-2023
Статус стандартизації	Відсутній статус оф. стандарту	RFC 7858	RFC 8484	RFC 9250 (чернетка)
Транспортний протокол	UDP/TCP	TCP	HTTP/2 over TLS	QUIC
Порт за замовчуванням	443/53	853	443	853/443
Механізм шифрування	X25519, ChaCha20-Poly1305	TLS 1.2+	TLS 1.2+	TLS 1.3
Легкість ідентифікації в мережі	Середня	Висока	Низька	Середня

Продовження таблиці 2.1

Характеристика	DNSCrypt	(DoT)	(DoH)	(DoQ)
Пристосованість до обходу блокувань	Середня	Низька	Висока	Середня-висока
Підтримка у браузерах	Обмежена	Обмежена	Широка	Обмежена
Підтримка в ОС	Обмежена	Середня	Широка	Обмежена
Вплив на продуктивність	Мінімальний	Незначний	Незначний-середній	Мінімальний
Стійкість до компрометації	Висока	Середня-висока	Середня-висока	Висока
Складність розгортання	Низька	Середня	Середня	Висока
Ресурсоємність для клієнтів	Низька	Середня	Середня-висока	Середня
Підтримка мобільних мереж	Середня	Середня	Висока	Дуже висока

Представлена на рис. 2.1 архітектурна схема ілюструє «внутрішню» взаємодію різних технологій шифрування DNS, у типовій інфраструктурі, демонструючи при цьому, їх взаємодоповнюючий характер та різноманітність можливих конфігурацій, що адаптовані до конкретних потреб і обмежень.

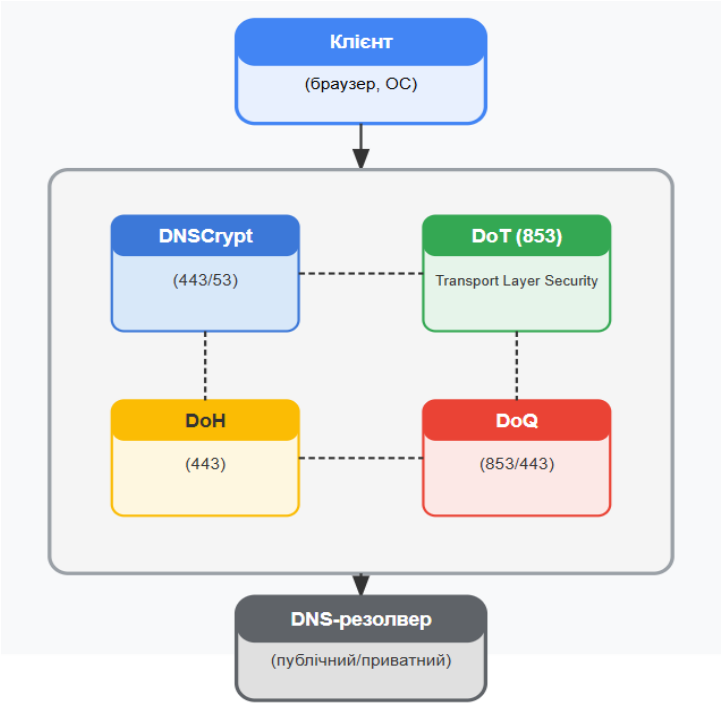

Рисунок 2.1 - Архітектура взаємодії різних технологій шифрування DNS

2.2 Використання та впровадження DNSSEC для забезпечення цілісності та автентичності DNS-запитів

Особливості DNSSEC як інструменту забезпечення цілісності та автентичності DNS-запитів

DNSSEC (Domain Name System Security Extensions) представляє собою фундаментальний підхід до забезпечення автентичності та цілісності даних DNS, що доповнює функціональність технологій шифрування DNS, фокусуючись на вирішенні проблеми достовірності інформації, а не її конфіденційності.

В загальному випадку DNSSEC представляє собою відповідний набір розширень протоколу DNS, та реалізує комплексний криптографічний механізм для автентифікації DNS-записів, ґрунтуючись на асиметричній криптографії та концепції т.з. «ланцюжка довіри» [91-93]. Основні відомості, щодо теоретичних основ та принципів його функціонування, більш розглянуто в Додатку Г.

Незважаючи на технічну зрілість та стандартизацію, впровадження DNSSEC залишається нерівномірним, що обумовлено впливом комплекса технічних, економічних і організаційних факторів:

- Статистика впровадження: За даними ISOC (Internet Society), приблизно 97% доменів верхнього рівня підписані з використанням DNSSEC, включаючи всі основні gTLDs та більшість ccTLDs. Проте на рівні доменів другого рівня ситуація суттєво відрізняється – від 2% у .com до понад 50% у деяких ccTLDs, таких як .nl (Нідерланди), .se (Швеція) та .cz (Чехія) [99-100].
- Особливості процессу підтвердження DNSSEC: За оцінками APNIC, приблизно 35% усіх DNS-запросників у світі виконують валідацію DNSSEC, з найвищими показниками у Північній Європі та Північній Америці. Цей відносно низький рівень валідації знижує показник DNSSEC, як механізму захисту [101].
- Основні технічні труднощі впровадження DNSSEC:
  - Складність адміністрування та ризики помилкової конфігурації;
  - Збільшення розміру DNS-пакетів, що може призводити до проблем із фрагментацією та відкидання пакетів;
  - Високі вимоги до обчислювальних ресурсів для виконання криптографічних операцій;
  - Складний процес ротації ключів, що може призводити до недоступності доменів при неправильному виконанні;
- Економічні та організаційні бар'єри:
  - Відсутність прямих комерційних стимулів для власників доменів;
  - Складність кількісної оцінки переваг від впровадження DNSSEC;
  - Недостатня підтримка з боку багатьох хостинг-провайдерів;
  - Відсутність масової обізнаності про переваги DNSSEC [108].

2.3 Вплив DNS Encryption на продуктивність та безпеку мереж

Впровадження технологій шифрування DNS має комплексний вплив на продуктивність мережевої інфраструктури та загальний ландшафт кібербезпеки, створюючи як нові можливості, так і виклики для різних учасників кіберпростору.

2.3.1 Кількісна оцінка впливу на продуктивність

Шифрування DNS невідворотно впливає на продуктивність мережевих комунікацій, проте цей вплив варіюється залежно від конкретної технології та умов розгортання:

- Непрозорість DNS-резолвінгу: Дослідження показують, що шифрування DNS збільшує середній час резолвінгу (тобто циклів «запит-відповідь»):
  - Класичний DNS (UDP): 15-40 мс (т.з. «базова лінія»);
  - DNSCrypt: додаткові 5-15 мс (загальне збільшення на 10-15%);
  - DoT: додаткові 10-30 мс (збільшення на 20-30%);
  - DoH: додаткові 15-40 мс (збільшення на 25-40%);
  - DoQ: додаткові 5-20 мс (збільшення на 15-25%) [110].
- Фактори впливу на латентність (тобто прихованість процедур):
  - Додаткові раунди обміну даними для встановлення захищеного з'єднання (TLS handshake);
  - Криптографічні операції шифрування та дешифрування;
  - Додаткові заголовки протоколів (TLS, HTTP), що збільшують розмір пакетів;
  - Обмеження мультиплексування в старіших версіях протоколів [109].
- Обчислювальне навантаження: Криптографічні операції потребують додаткових обчислювальних ресурсів:
  - Збільшення використання CPU на клієнтських пристроях: від 15% для DNSCrypt до 40% для складних реалізацій DoH;
  - Підвищене навантаження на сервери DNS-резолверів, що вимагає вертикального масштабування інфраструктури;
  - Особливо помітний вплив на пристрої з обмеженими ресурсами (IoT, старіші мобільні пристрої) [111].
- Оптимізації продуктивності:
  - Повторне використання з'єднань (connection reuse) значно зменшує накладні витрати для DoT і DoH;

- HTTP/2 та HTTP/3 у DoH дозволяють ефективне мультиплексування запитів;
- Попереднє встановлення з'єднань (connection preestablishment) для зменшення затримки першого запиту;
- Проактивна ротація сесійних ключів для балансу між безпекою та продуктивністю [111].

В Табл. 2.2 узагальнено деякі кількісні оцінки, що в певної мірі систематизують наслідки від використання різних протоколів шифрування DNS на продуктивність сучасних мереж (для окремих показників) [115].

Таблиця 2.2 – Порівняльний аналіз впливу різних протоколів шифрування DNS на продуктивність мережі [115]

Протокол	Збільшення затримки	Збільшення розміру пакетів	Споживання CPU	Вплив на пропускну здатність
Стандартний DNS (UDP)	Базова лінія	Базова лінія	Базова лінія	Базова лінія
DNSCrypt	10-15%	20-30%	15-25%	5-10%
DoT	20-30%	30-40%	20-30%	10-15%
DoH	25-40%	40-70%	25-40%	15-25%
DoQ	15-25%	25-35%	20-30%	8-15%

- Позитивні аспекти для безпеки від впровадження шифрування DNS:
  - Запобігання пасивному моніторингу DNS-трафіку, що ускладнює профілювання користувачів та масове спостереження;
  - Захист від активних атак типу "людина посередині" (man-in-the-middle), що базуються на перехопленні та модифікації DNS-запитів;

- Мінімізація ризиків атак типу DNS hijacking на маршруті передачі даних;
- Захист від деяких форм цензури, що базуються на моніторингу та блокуванні DNS-запитів;
- Підвищення загального рівня приватності для кінцевих користувачів;
- Захист від атак, спрямованих на компрометацію конфіденційності історії відвідувань користувачів [112].

- Проблематичні аспекти для корпоративної безпеки:
  - Суттєве обмеження можливостей моніторингу та контролю DNS-трафіку в корпоративних мережах;
  - Зниження ефективності традиційних систем виявлення та запобігання вторгненням (IDS/IPS), що ґрунтуються на аналізі DNS;
  - Ускладнення реалізації корпоративних політик фільтрації контенту та захисту від шкідливого програмного забезпечення;
  - Потенційне використання шифрованого DNS для обходу корпоративних механізмів безпеки;
  - Ускладнення розслідування інцидентів безпеки через обмежену видимість DNS-трафіку;
  - Зниження ефективності систем запобігання витоку даних (DLP), що використовують аналіз DNS для виявлення підозрілої активності [113].

Слід підкреслити, що впровадження шифрування DNS призводить до фундаментальних змін у моделі мережевої безпеки, які вимагають переосмислення традиційних підходів до її забезпечення:

- Перехід від моделі периметра до модульної безпеки:
  - Зменшення ефективності традиційної моделі безпеки, що базується на захисті мережевого периметра;
  - Зростання важливості безпеки кінцевих точок та модульних підходів до захисту;
  - Трансформація ролі мережевих адміністраторів та фахівців з безпеки;

- Необхідність впровадження багаторівневих систем захисту з урахуванням обмеженої видимості мережевого трафіку [132].

- Зміна балансу між приватністю та безпекою:
  - Концептуальний конфлікт між вимогами до приватності користувачів та потребами корпоративної безпеки;
  - Необхідність розробки нових регуляторних підходів, що враховують технологічні реалії шифрування DNS;
  - Диференціація підходів до безпеки в різних контекстах (домашні користувачі, корпоративні мережі, критична інфраструктура);
  - Розвиток дискурсу щодо балансу між безпекою, приватністю та технологічним прогресом [133].

2.4 Особливості контролю та фільтрації DNS-трафіку в умовах його шифрування

Широке впровадження технологій шифрування DNS [116-119, 124] створює принципово нові виклики для традиційних підходів до процедур контролю і фільтрації трафіку, вимагаючи розробки інноваційних методів та архітектур безпеки. Окремі питання, стосовно еволюції та деяких регуляторно-етичних аспектів [134-136] для існуючих методів контролю DNS-трафіку, в стислому вигляді, представлено в Додатку Д. При цьому еволюція розвитку методів/способів контролю DNS, призвела до розробки більш комплексних та ефективних підходів до цього процесу (рис. 2.2):

- Глибока інспекція TLS-трафіку:
  - Розгортання інфраструктури для інспекції TLS (TLS inspection);
  - Інсталяція локальних сертифікатів CA на корпоративних пристроях;
  - Селективне дешифрування TLS-з'єднань до відомих DoH-серверів;
  - Аналіз характеристик TLS handshake для ідентифікації DoH/DoT;
  - Переваги: висока ефективність; Недоліки: складність впровадження, потенційні проблеми з приватністю [125];
- Поведінковий аналіз мережевого трафіку:

- Застосування алгоритмів машинного навчання для аналізу патернів мережевого трафіку;
- Ідентифікація характерних ознак DoH/DoT без необхідності дешифрування;
- Виявлення аномалій у часових характеристиках та розмірах пакетів;
- Кластеризація трафіку за поведінковими характеристиками;
- Переваги: не вимагає дешифрування; Недоліки: – є потенційні «хибнопозитивні» спрацювання [126];

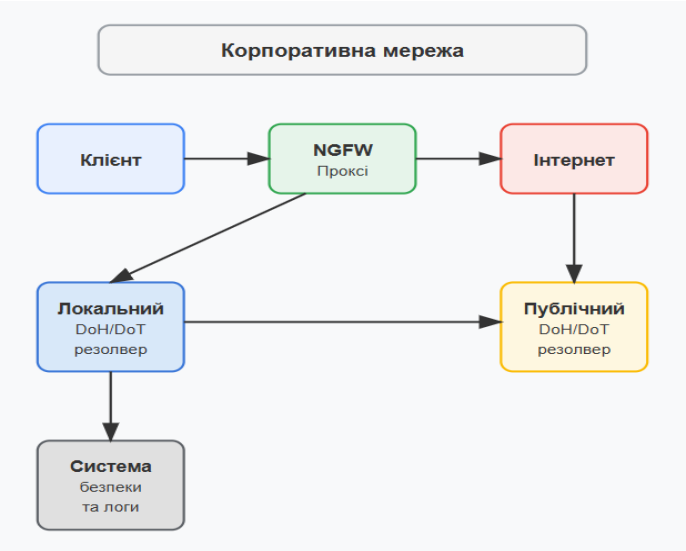

Рисунок 2.2 – Архітектура корпоративного контролю DNS в умовах шифрування

2.5 Специфіка питань суміщення VPN і Proxy з технологією шифрування DNS

Інтеграція VPN та проксі-сервісів з технологіями шифрування DNS утворює комплексні багаторівневі системи захисту, але при цьому, також, породжує специфічні технічні труднощі та потенційні вразливості.

2.5.1 Архітектурні моделі інтеграції VPN з DNS Encryption

Взаємодія VPN та шифрованого DNS може бути реалізована в різних архітектурних конфігураціях (рис. 2.3), кожна з яких має особливості в контексті безпеки та продуктивності:

- VPN з інтегрованим шифрованим DNS:

- VPN-провайдер надає власні DoH/DoT-сервери як частину сервісу
- DNS-трафік автоматично маршрутизується через тунель VPN
- Синхронізація IP-адреси клієнта та адреси, видимої для DNS-сервера
- Запобігання витоку DNS-запитів за межі захищеного тунелю
- Централізоване управління політиками безпеки DNS [137]

- Зовнішній шифрований DNS через VPN:
  - Користувач налаштовує зовнішній DoH/DoT-резолвер, незалежний від VPN-провайдера
  - Весь трафік, включаючи DNS, проходить через VPN «тунель»;
  - Додатковий рівень приватності через розділення провайдерів VPN та DNS;
  - Потенційні проблеми з "DNS Leaks" при неправильній конфігурації
  - Можливі конфлікти між політиками маршрутизації VPN та DNS [138].

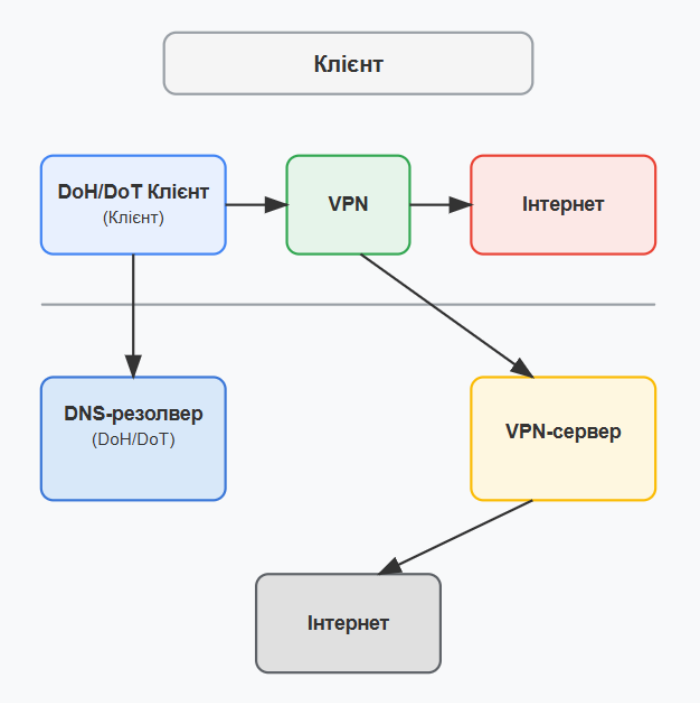

Рисунок 2.3 – Архітектура взаємодії VPN з шифрованим DNS (варіант DoH/DoT -> VPN)

2.5.2 Технічні аспекти інтеграції Proxy з DNS Encryption

Проксі-сервери різних типів мають специфічні особливості взаємодії з шифрованим DNS, що впливає на ефективність захисту та користувацький досвід. В якості головних з них, слід зазначити наступні:

- HTTPS Proxy та DoH:
  - HTTPS-проксі може перехоплювати та аналізувати DoH-трафік при наявності відповідних сертифікатів;
  - Можливість селективної фільтрації DNS-запитів на рівні проксі;
  - Повна видимість DNS-запитів для адміністраторів проксі;
  - Потенційні проблеми з сертифікатами та валідацією TLS;
  - Необхідність встановлення довірених сертифікатів на клієнтських пристроях [141].
- SOCKS Proxy та шифрований DNS:
  - SOCKS-проксі передає трафік на рівні TCP/UDP без інспекції змісту;
  - Збереження шифрування DNS при проходженні через SOCKS;
  - Відсутність можливості фільтрації DNS-запитів на рівні проксі;
  - Ефективність для обходу геоблокувань при збереженні приватності DNS;
  - Підтримка як DoH, так і DoT без додаткової конфігурації [142].
- Transparent Proxy та виклики шифрованого DNS:
  - Транспарентні проксі не можуть ефективно контролювати шифрований DNS-трафік без додаткових механізмів;
  - Необхідність впровадження методів інспекції TLS для контролю DoH;
  - Можливість контролю DoT через блокування нестандартних портів;
  - Потенційні проблеми з Privacy Pass та подібними технологіями;
  - Балансування між приватністю користувачів та потребами моніторингу [143].

2.5.3 Узагальнення комбінаторики VPN/Proxy з DNS Encryption та напрями їх подальшого комплексування

Поєднання різних технологій захисту створює комплексний ефект на загальний рівень безпеки та приватності:

- Синергетичні ефекти:
  - Взаємна компенсація слабких сторін різних технологій;
  - Висока стійкість до багатовекторних атак на приватність;
  - Ефективний захист від корелювання активності користувача різними сервісами;
  - Багаторівневий захист від різних типів моніторингу та цензури;
  - Диверсифікація довіри між різними провайдерами сервісів [144].
- Потенційні вразливості та недоліки:
  - "DNS Leak" – витік DNS-запитів в обхід VPN при некоректній конфігурації;
  - "WebRTC Leak" – розкриття реальної IP-адреси навіть при використанні VPN та шифрованого DNS;
  - Конфлікти між різними технологіями захисту при неправильній інтеграції;
  - Складність діагностики проблем у багаторівневих системах;
  - Потенційне зниження продуктивності через кумулятивний ефект шифрування [145].
- Рекомендовані практики інтеграції:
  - Перевірка конфігурації на витоки DNS та WebRTC;
  - Використання "kill switch" для запобігання витоку трафіку при розриві VPN-з'єднання;
  - Тестування різних конфігурацій для оптимального балансу приватності та продуктивності;
  - Регулярний аудит безпеки комплексних систем захисту;
  - Використання різних провайдерів для VPN та DNS для мінімізації ризиків централізації даних [146].

2.5.4 Напрямки розвитку інтегрованих рішень

Узагальнення результатів аналізу сучасних тенденцій [146-149] щодо комплексування VPN/Proxy з шифрованим DNS, дозволяє ідентифікувати кілька найбільш перспективних напрямів, а саме:

- Уніфіковані платформи безпеки:
  - Інтеграція VPN, шифрованого DNS та інших технологій захисту в єдину платформу;
  - Централізоване управління політиками безпеки та конфігураціями;
  - Автоматизоване виявлення та усунення потенційних витоків даних;
  - Балансування навантаження між різними компонентами для оптимальної продуктивності;
  - Спрощення розгортання комплексних систем захисту [147].
- Адаптивні системи маршрутизації:
  - Динамічна адаптація маршрутизації трафіку залежно від типу даних та його контексту (змісту);
  - Інтелектуальна комутація між різними шляхами циркуляції трафіку;
  - Оптимізація продуктивності при збереженні високого рівня захисту;
  - Використання ML для предиктивної оптимізації маршрутизації;
  - Балансування між локальним й «глобальним» розподілом DNS [148].
- Децентралізовані системи довіри:
  - Розвиток технологій розподіленого резолвінгу/обслуговування DNS; запитів без т.з. «єдиної точки довіри» (централізованого ресурсу);
  - Інтеграція з блокчейн-технологіями для забезпечення цілісності даних;
  - Мультипідпис для DNS-записів з розподіленою валідацією;
  - Федеративні моделі довіри для DNS та VPN сервісів;
  - Мінімізація необхідності довіри до окремих провайдерів сервісів [149].

2.5.5 Висновки та перспективи розвитку

Проведені дослідження відомих технологій шифрування DNS та аналіз сучасних механізмів контролю DNS-трафіку, дозволяє зробити кілька ключових висновків, стосовно оцінки поточного стану і перспектив розвитку цієї сфери:

1) Еволюційний характер розвитку технологій:
   - Перехід від незахищеного DNS до комплексних систем ІБ відображає загальну тенденцію до посилення захисту конфіденційності в інтернеті;
   - Кожна нова технологія (DNSCrypt → DoT → DoH → DoQ) висвітлює специфічні обмеження попередніх підходів та нові можливості;
   - Паралельний розвиток технологій шифрування та механізмів їх контролю створює динамічний баланс між приватністю та безпекою.
2) Комплементарність різних технологій безпеки:
   - Шифрування DNS та DNSSEC протиставляють різні аспекти складових безпеки DNS (конфіденційність vs. автентичність);
   - Інтеграція VPN/Proxy з шифрованим DNS створює багаторівневі системи захисту;
   - Найефективніший захист досягається комбінуванням різних технологій з урахуванням їх взаємодії;
3) Трансформація сутності поточної парадигми мережевої безпеки:
   - Перехід від моделі периметра до модульної та багаторівневої безпеки;
   - Зростання важливості безпеки кінцевих точок та ідентичності;
   - Необхідність переосмислення традиційних підходів до моніторингу та контролю мережевого трафіку.
4) Неперервний пошук бажаного балансу між протилежними цілями:
   - Приватність користувача, проти (vs.) нових загроз і норм безпеки корпоративних мереж;
   - Свобода інформації vs. потреби регулювання й контролю трафіку;
   - Технологічні інновації vs. сумісність з існуючою інфраструктурою.

3 ДОСЛІДЖЕННЯ МОЖЛИВОСТЕЙ КОНТРОЛЮ І ДЕТЕКТУВАННЯ АНОМАЛІЙ У ЗАШИФРОВАНОМУ DNS-ТРАФІКУ

3.1 Труднощі у виявленні зловмисного трафіку через DNS-тунелювання та обходи фільтрації

DNS-тунелювання та інші методи обходу мережевих фільтрів з використанням DNS становлять серйозну загрозу для кібербезпеки організацій, особливо в контексті зростаючого впровадження технологій шифрування DNS. Ці техніки дозволяють зловмисникам встановлювати приховані канали зв'язку, обходити системи безпеки та здійснювати ексфільтрацію даних, що створює значні технічні виклики для систем виявлення та запобігання вторгненням.

3.1.1 Концептуальні основи DNS-тунелювання

DNS-тунелювання базується на зловживанні протоколом DNS для цілей, не пов'язаних з його прямим призначенням - розв'язанням доменних імен. Концептуально, це техніка, що дозволяє інкапсулювати довільний трафік у DNS-запити та відповіді:

- Принцип роботи: DNS-тунелювання використовує структуру DNS-запитів (особливо TXT-, CNAME- та NULL-записи) для передачі зашифрованих або закодованих даних між клієнтом і сервером. Зловмисник контролює авторитативний DNS-сервер для певного домену, що дозволяє інтерпретувати отримані запити та відповідати на них у форматі, що містить приховані дані [12].
- Технічна реалізація: Типова реалізація DNS-тунелю включає:
    - Поділ даних, що передаються, на невеликі фрагменти
    - Кодування фрагментів у форматі, допустимому для DNS-запитів (зазвичай base32/base64)
    - Формування піддоменів або TXT-записів, що містять закодовані дані
    - Відправка запитів до авторитативного DNS-сервера зловмисника

    - Отримання відповідей, що також можуть містити закодовані команди або дані [53]
- Ексфільтрація даних через DNS: Особливо небезпечним аспектом DNS-тунелювання є можливість ексфільтрації конфіденційних даних з організації. Навіть у мережах з суворими обмеженнями доступу до інтернету, DNS-запити зазвичай дозволені для забезпечення базової функціональності, що створює потенційний канал витоку даних [12, 53].

3.1.2 Еволюція технік DNS-тунелювання

Техніки DNS-тунелювання постійно еволюціонують, адаптуючись до вдосконалення систем захисту:

- Перше покоління: Прості інструменти DNS-тунелювання (NSTX, Iodine), що використовували базові методи кодування та часто мали характерні сигнатури, які легко виявлялись системами виявлення вторгнень [41].
- Друге покоління: Вдосконалені інструменти (DNScat2, dnstt), що використовують шифрування даних, компресію та оптимізовані протоколи передачі для зменшення кількості запитів та маскування аномальних патернів [48].
- Сучасні техніки: Найновіші реалізації DNS-тунелювання включають:
    - Адаптивне коригування частоти запитів для імітації легітимного DNS-трафіку
    - Використання різних типів DNS-записів для диверсифікації трафіку
    - Фрагментація даних з псевдовипадковими затримками між запитами
    - Імітація поведінкових патернів легітимних застосунків
    - Використання технік обфускації для маскування вмісту запитів [49, 53]
- Інтеграція з шифрованим DNS: Особливо проблематичним є використання DoH/DoT у поєднанні з DNS-тунелюванням, що додає шар шифрування і значно ускладнює виявлення аномального трафіку [112, 122].

3.1.3 Технічні виклики виявлення DNS-тунелювання в зашифрованому трафіку

Виявлення DNS-тунелювання стає суттєво складнішим у контексті зашифрованого DNS-трафіку через низку технічних обмежень:

- Втрата видимості вмісту запитів: Шифрування DNS (DoH, DoT, DNSCrypt) робить неможливим безпосередній аналіз вмісту DNS-запитів на проміжних вузлах мережі. Системи виявлення вторгнень не можуть перевіряти запити на наявність аномальних доменів, закодованих даних або інших індикаторів тунелювання [113].
- Ускладнення аналізу метаданих: Хоча деякі метадані (розмір пакетів, частота запитів) залишаються доступними навіть при шифруванні, DoH особливо ускладнює аналіз через використання стандартного веб-трафіку, що маскує характеристики DNS-трафіку [114].
- Проблеми з валідацією сертифікатів: Використання HTTPS для DoH створює додаткові виклики для систем перехоплення та аналізу трафіку, оскільки проста інспекція TLS може призвести до помилок валідації сертифікатів або бути виявлена клієнтськими застосунками [112].
- Складність розділення легітимного та зловмисного трафіку: Шифрування ускладнює диференціацію між нормальним використанням зашифрованого DNS та зловмисним DNS-тунелюванням через шифрований канал [123].

3.1.4 Методи обходу фільтрації DNS

Крім DNS-тунелювання, існують інші методи обходу фільтрації та моніторингу з використанням DNS:

- DNS-over-VPN: Комбінація VPN з шифрованим DNS для повного маскування DNS-трафіку та обходу корпоративних фільтрів (див. рис. 3.1) [137].
- DoH-over-Proxy: Використання веб-проксі для пересилання DoH-запитів, що додатково ускладнює виявлення DNS-трафіку [141].

- Split-horizon DNS: Використання різних DNS-резолверів для різних типів запитів, що ускладнює централізований моніторинг [127].
- DNS-over-TOR: Використання мережі TOR для анонімізації DNS-запитів та додаткового маскування джерела запитів [142].
- Технології розподіленого DNS: Використання технологій розподіленого розв'язання DNS (dDNS, DNScrypt з множинними резолверами) для розподілу DNS-трафіку між різними провайдерами, що ускладнює комплексний моніторинг [149].

3.1.5 Статистика та тренди використання DNS-тунелювання

Дослідження показують зростаючу тенденцію використання DNS-тунелювання та інших технік обходу фільтрації (див. рис. 3.1):

- За даними аналітичних звітів, кількість атак з використанням DNS-тунелювання зросла на 100% за період 2019-2023 років [38].
- Середній час виявлення DNS-тунелювання в корпоративних мережах становить понад 200 годин, що значно вище за середній час виявлення інших типів атак [41].
- Близько 60% успішних ексфільтрацій даних з організацій з високим рівнем захисту включають використання DNS-каналу як одного з векторів передачі даних [38].
- Впровадження DoH в корпоративних мережах без належного контролю підвищує ймовірність успішного використання DNS-тунелювання на 70% [113].

Рисунок 3.1 – Схема обходу мережевих фільтрів через шифрований DNS-тунель

3.2 Вплив DNS Encryption на можливість аналізу та фільтрації шкідливих запитів

3.2.1 Технічні обмеження аналізу зашифрованого DNS-трафіку

Шифрування DNS суттєво обмежує можливості проміжних систем аналізу та фільтрації трафіку через фундаментальні зміни в доступності та видимості даних:

- Втрата семантичної видимості запитів: При використанні DoH, DoT або DNSCrypt вміст DNS-запитів (доменні імена, типи запитів, параметри) стає недоступним для аналізу без дешифрування. Це унеможливлює традиційний підхід до фільтрації на основі аналізу запитуваних доменів, що був основою більшості систем захисту від шкідливого програмного забезпечення та фішингу [114].

- Обмежена доступність метаданих: Хоча деякі метадані (розмір пакетів, частота, часові патерни) залишаються доступними навіть при шифруванні, їх інформативність суттєво знижується. Особливо проблематичним є DoH, що маскує DNS-трафік під звичайний HTTPS-трафік, ускладнюючи навіть базову ідентифікацію DNS-комунікацій [112].
- Проблеми з аналізом на рівні мережі: Традиційні системи виявлення та запобігання вторгненням (IDS/IPS), що функціонують на мережевому рівні, втрачають можливість глибокого інспектування DNS-запитів без впровадження складних механізмів перехоплення та дешифрування TLS [113].
- Ускладнення кореляції між DNS та іншим трафіком: Шифрування DNS ускладнює встановлення зв'язків між DNS-резолвінгом та подальшою мережевою активністю, що було критичним компонентом для виявлення багатьох типів атак [120].

3.2.2 Операційні наслідки для систем безпеки

Впровадження шифрування DNS має суттєві операційні наслідки для систем безпеки, змінюючи архітектуру і підходи до захисту:

- Зменшення ефективності централізованих фільтрів: Традиційні централізовані системи фільтрації DNS (на рівні організації або інтернет-провайдера) втрачають ефективність, оскільки користувачі можуть обходити їх, використовуючи зовнішні зашифровані DNS-резолвери [116].
- Ускладнення розслідування інцидентів: Відсутність детальних DNS-логів значно ускладнює розслідування інцидентів безпеки, збільшуючи час виявлення компрометації та обмежуючи можливості відновлення хронології атаки [123].
- Зміщення відповідальності на кінцеві точки: Захист переміщується з периметра мережі на кінцеві пристрої, що потребує нових підходів до розгортання агентів безпеки та управління політиками [121].

- Фрагментація контролю: Традиційна модель централізованого контролю DNS-інфраструктури трансформується у фрагментовану модель, де різні пристрої та застосунки можуть використовувати різні DNS-резолвери з різними політиками безпеки [124].

3.2.3 Кількісна оцінка впливу на ефективність систем безпеки

Дослідження демонструють значний вплив шифрування DNS на ефективність традиційних систем безпеки:

- За даними аналітичних звітів, впровадження DoH без відповідної адаптації систем безпеки знижує ефективність виявлення шкідливих доменів на 60-80% [113].
- Середній час виявлення інцидентів збільшується на 35-50% при широкому використанні зашифрованого DNS у корпоративних мережах без впровадження спеціалізованих механізмів моніторингу [123].
- Точність систем фільтрації контенту знижується на 45-65% при використанні користувачами зовнішніх DoH-резолверів [121].
- Ефективність виявлення DNS-тунелювання знижується на 70-90% при використанні DoH порівняно з традиційним DNS [114].

3.2.4 Головні виклики та варіативність підходів

Шифрування DNS створює стратегічні виклики для організацій, що потребують адаптації політик та архітектур безпеки:

- Баланс між приватністю та безпекою: Організації стикаються з необхідністю знаходити баланс між забезпеченням приватності користувачів та збереженням можливостей моніторингу для виявлення загроз [133].
- Архітектурні трансформації: Необхідність переходу від периметрового захисту до розподілених моделей безпеки з елементами моніторингу на різних рівнях мережевої інфраструктури [124].

- Регуляторні аспекти: Необхідність адаптації підходів до відповідності регуляторним вимогам щодо фільтрації контенту та моніторингу в умовах шифрування DNS [134].
- Трансформація ролі сервіс-провайдерів: Зміщення відповідальності за безпеку DNS від мережевих адміністраторів до провайдерів DNS-сервісів та виробників програмного забезпечення [116].

3.2.5 Адаптивні стратегії збереження контролю

У відповідь на виклики шифрування, організації розробляють нові стратегії для збереження можливостей аналізу та фільтрації:

- Локальні DoH/DoT проксі: Впровадження корпоративних DoH/DoT-резолверів з інтегрованими механізмами фільтрації та моніторингу, що дозволяє зберегти переваги шифрування при збереженні контролю [127].
- Інспекція TLS: Розгортання інфраструктури для інспекції TLS-трафіку з селективним дешифруванням DNS-комунікацій, хоча цей підхід створює потенційні ризики для приватності та потребує ретельного управління сертифікатами [125].
- Керування кінцевими точками: Використання політик групи та механізмів MDM (Mobile Device Management) для контролю конфігурації DNS на корпоративних пристроях [129].
- Поведінковий аналіз: Розвиток методів аналізу, що не потребують дешифрування трафіку, а базуються на поведінкових патернах та метаданих [126].

3.3 Методи детектування та аналізу DNS-трафіку: традиційні та новітні механізми і алгоритми

3.3.1 Традиційні методи аналізу DNS-трафіку

Традиційні підходи до аналізу DNS-трафіку, що сформувалися до широкого впровадження шифрування, базуються на безпосередньому аналізі вмісту DNS-запитів та відповідей:

- Сигнатурний аналіз: Виявлення відомих шкідливих доменів та патернів запитів на основі попередньо визначених сигнатур. Цей метод характеризується високою точністю для відомих загроз, але обмеженою ефективністю проти нових та модифікованих атак [41].
- Репутаційні системи: Використання баз даних репутації доменів для фільтрації запитів до відомих шкідливих або підозрілих ресурсів. Ефективність цього підходу значно залежить від актуальності та повноти використовуваних баз даних [42].
- Аналіз синтаксичних аномалій: Виявлення нетипових характеристик доменних імен, таких як надмірна довжина, високий рівень ентропії, нетипові комбінації символів, що можуть вказувати на алгоритмічно генеровані домени (DGA) або закодовані дані [49].
- Частотний аналіз: Моніторинг частоти та патернів DNS-запитів для виявлення аномальної активності, такої як DNS flooding, DNS amplification або високочастотні запити до одного домену [11].
- Аналіз відповідей: Дослідження DNS-відповідей для виявлення аномалій, таких як швидка зміна IP-адрес (Fast Flux), нетипові TTL (Time To Live) значення, або аномальні записи [17].
- Глибока інспекція пакетів (DPI): Детальний аналіз структури та вмісту DNS-пакетів для виявлення аномалій на рівні протоколу або закодованих даних у різних полях DNS-запитів [13].

3.3.2 Еволюція методів в умовах шифрування

З поширенням технологій шифрування DNS, традиційні методи аналізу зіткнулися з фундаментальними обмеженнями, що стимулювало розвиток нових підходів:

- Аналіз метаданих шифрованого трафіку: Фокус зміщується на аналіз характеристик трафіку, доступних навіть при шифруванні: розмір пакетів, частота, часові патерни, співвідношення вхідного та вихідного трафіку [121].

- Аналіз криптографічних артефактів: Дослідження характеристик TLS-сесій, включаючи версії протоколів, набори шифрів, особливості сертифікатів, що можуть вказувати на специфічні реалізації DoH/DoT [114].
- Пасивний фінгерпринтинг: Ідентифікація клієнтських застосунків та серверів на основі характеристик їх мережевої поведінки без необхідності дешифрування трафіку [122].
- Термінальний моніторинг: Перенесення моніторингу з мережевого рівня на рівень кінцевих пристроїв з використанням спеціалізованих агентів, що мають доступ до DNS-запитів до їх шифрування [129].
- Проксі-інтерцепція: Впровадження проксі-серверів, що виконують роль посередника між клієнтами та зовнішніми DNS-резолверами, дозволяючи аналізувати трафік до його шифрування [125].

3.3.3 Спеціалізовані техніки виявлення загроз у DNS

Розроблено ряд спеціалізованих технік для виявлення конкретних типів загроз, пов'язаних з DNS:

- Виявлення DGA-доменів: Методи для ідентифікації алгоритмічно генерованих доменів, що часто використовуються в ботнетах. Підходи включають аналіз лінгвістичних характеристик доменів, n-gram аналіз, ентропійний аналіз та спеціалізовані нейронні мережі для класифікації доменів [45, 46].
- Детектування DNS-тунелювання: Техніки для виявлення передачі закодованих даних через DNS-запити. Методи включають аналіз довжини та частоти запитів, ентропійний аналіз вмісту запитів, виявлення аномального співвідношення між кількістю запитів та обсягом переданих даних [48, 53].
- Виявлення Fast Flux мереж: Методи для ідентифікації технік швидкої зміни IP-адрес, що використовуються для приховування шкідливої інфраструктури. Підходи включають аналіз TTL значень, географічного розподілу IP-адрес, патернів оновлення DNS-записів [17].

- Детектування DNS Hijacking: Техніки для виявлення підміни DNS-відповідей або компрометації DNS-серверів. Методи включають порівняння відповідей з різних резолверів, аналіз історичних даних про DNS-записи, виявлення неавторизованих змін у конфігурації DNS [14].

3.4 Використання поведінкового аналізу та методів машинного навчання для виявлення аномалій DNS

3.4.1 Концептуальні основи поведінкового аналізу DNS-трафіку

Поведінковий аналіз DNS базується на фундаментальному припущенні, що нормальна та зловмисна активність у DNS-трафіку мають відмінні поведінкові характеристики, які можна ідентифікувати навіть при обмеженій видимості вмісту запитів:

- Базові принципи поведінкового аналізу:
    - Встановлення базового профілю "нормальної" DNS-активності для мережі або пристрою;
    - Вимірювання відхилень від встановленого профілю для виявлення аномалій;
    - Аналіз контексту та взаємозв'язків між різними аспектами DNS-активності;
    - Адаптивне коригування базових профілів з часом для відображення легітимних змін у поведінці [131].
- Ключові поведінкові індикатори в DNS-трафіку:
    - Часові патерни запитів (частота, регулярність, бурстність);
    - Об'ємні характеристики (кількість запитів, розмір пакетів, співвідношення запит/відповідь);
    - Статистичний розподіл типів запитів (A, AAAA, MX, TXT тощо);
    - Патерни взаємодії з різними доменами та піддоменами;
    - Контекстуальні зв'язки між DNS та іншою мережевою активністю [50, 126].
- Переваги поведінкового підходу:

- Ефективність в умовах шифрування DNS-трафіку;
- Здатність виявляти невідомі та нові типи загроз;
- Нижчий рівень хибно-позитивних спрацювань при правильному налаштуванні;
- Адаптивність до еволюції як легітимного трафіку, так і технік атак [131].

3.4.2 Індикативні характеристики DNS-трафіку та можливості ML для завдань його поведінкового аналізу

Поведінковий аналіз DNS фокусується на комплексному контролі сукупності певних характеристик й властивостей трафіку, доступних для спостереження, навіть у зашифрованому трафіку. Розглянемо деякі з них, що дозволяє концептуально здійснювати парсінг відповідного трафіку:

- Часові характеристики:
  - Міжзапитовий інтервал (час між послідовними запитами);
  - Періодичність запитів (наявність регулярних патернів);
  - Добові та тижневі патерни активності;
  - Кластеризація запитів у часі (бурсти активності);
  - Аномальна активність у нетипові години [50, 52].
- Волюметричні характеристики:
  - Кількість запитів за одиницю часу;
  - Розмір пакетів (особливо важливо для шифрованого трафіку);
  - Співвідношення вхідного та вихідного трафіку;
  - Розподіл розмірів пакетів;
  - Аномальні сплески об'єму трафіку [126].
- Топологічні характеристики:
  - Графи взаємодій між клієнтами та DNS-серверами;
  - Патерни запитів до ієрархій піддоменів;
  - Взаємозв'язки між IP-адресами та доменами;
  - Структурні особливості комунікацій;

- Аномальні патерни підключень [51].

- Криптографічні артефакти (для шифрованого DNS):
  - Характеристики TLS-рукостискання;
  - Використовувані набори шифрів;
  - Версії протоколів;
  - Патерни оновлення сесій;
  - Особливості сертифікатів [114, 122].

Слід зазначити, що різні типи DNS-атак мають характерні поведінкові патерни, що дозволяє розробити специфічні індикатори для їх виявлення з залученням можливостей технології ML. За результатами проведеного аналізу [49,53,131] в табл. Е.1, Додатку Е, систематизовано відповідні поведінкові індикатори для різних типів DNS-атак.

3.4.3 Напрямки розвитку та перспективи

Аналіз сучасних тенденцій дозволяє ідентифікувати ключові напрямки розвитку методів поведінкового аналізу та машинного навчання для виявлення аномалій DNS:

- Інтеграція з іншими джерелами даних:
  - Об'єднання аналізу DNS з даними інших мережевих протоколів;
  - Використання контекстуальної інформації з хостів та додатків;
  - Кореляція з глобальними даними про загрози;
  - Багатовимірний аналіз для підвищення точності виявлення [128];
- Автоматизація реагування:
  - Розвиток систем автоматичного генерування та впровадження контрзаходів;
  - Інтелектуальні механізми пріоритизації загроз;
  - Автоматизація аналізу та контекстуалізації виявлених аномалій;
  - Адаптивні стратегії захисту на основі аналізу поведінки атакуючих [72].
- Підвищення ефективності в умовах шифрування:

- Розробка нових методів аналізу шифрованого трафіку без дешифрування;
- Покращення методів ідентифікації криптографічних артефактів;
- Інтеграція термінального моніторингу з мережевим аналізом;
- Поведінковий аналіз на стику різних рівнів мережевої інфраструктури [126, 131].

4 ТЕСТУВАННЯ ІСНУЮЧИХ ІНСТРУМЕНТІВ АНАЛІЗУ DNS ТРАФІКУ ТА РЕКОМЕНДАЦІЇ ЩОДО ВДОСКОНАЛЕННЯ СИСТЕМИ БЕЗПЕКИ DNS

4.1 Тестування існуючих інструментів моніторингу та аналізу DNS трафіку

Для проведення комплексного аналізу можливостей моніторингу та захисту DNS-інфраструктури було обрано чотири ключові інструменти: Wireshark, Zeek, Pi-hole та Splunk. Кожен з цих інструментів реалізує різні підходи до аналізу DNS трафіку та має специфічні можливості для виявлення аномалій та загроз безпеки. Систематизовані результати, стосовно узагальнення можливостей тестованих програмних засобів, при виконанні завдань з аналізу DNS трафіку, представлені в Додатку Ж (див. п.п. Ж.1-Ж-4).

4.1.1 Порівняльний аналіз інструментів

За результатами проведеного моделювання, виконано порівняльний аналіз можливостей деяких відомих інструментів (див. табл. 4.1).

Таблиця 4.1 – Порівняльний аналіз інструментів моніторингу DNS

Критерій	Wireshark	Zeek	Pi-hole	Splunk
Глибина аналізу пакетів	Дуже висока	Висока	Низька	Середня
Автоматизація моніторингу	Низька	Висока	Висока	Дуже висока
Виявлення аномалій	Ручний аналіз	Автоматичне	Обмежене	Дуже ефективне
Масштабованість	Низька	Висока	Середня	Дуже висока
Простота використання	Складна	Середня	Проста	Складна
Робота з шифрованим DNS	Обмежена	Обмежена	Неефективна	Залежить від джерел
Інтеграція з іншими системами	Низька	Висока	Низька	Дуже висока
Вартість впровадження	Безплатно	Безплатно	Безплатно	Комерційна

Крім того в межах тестування обраних інструментів (Wireshark, Zeek, Pi-hole та Splunk) систематизовано деякі їх показники: – продуктивність, точність виявлення загроз та ресурсне навантаження на базову платформу. Відповідні результати моделювання представлено у вигляді гістограм в Додатку З.

Аналіз отриманих результатів дозволяє стверджувати, що: – Splunk та Zeek мають найвищу точність виявлення загроз – до 98% для Splunk та 95% для Zeek у випадку DNS тунелювання. Wireshark вимагає ручного аналізу і, хоча дозволяє глибоке вивчення пакетів, не забезпечує автоматизації. Pi-hole, у свою чергу, демонструє min результати виявлення загроз, але залишається ефективним для фільтрації небажаних DNS-запитів у реальному часі з min затратами ресурсів.

4.2 Результи узагальнення можливостей детектування аномалій DNS та основні напрями впровадження AI/ML для визначених задач

4.2.1 Бліц-огляд можливостей з детектування аномалій DNS

Традиційні методи детектування:

1) Сигнатурні методи: Високоефективні для відомих загроз, але неефективні проти нових атак та адаптивних техник зловмисників [41].
2) Репутаційні системи: Забезпечують базовий рівень захисту, але мають затримки у виявленні нових шкідливих доменів [42].
3) Статистичний аналіз: Ефективний для виявлення аномальних патернів, але потребує експертного налаштування порогів [131].

Ризики та невизначеності щодо сучасних рішень детектування:

1) Шифрування DNS трафіку: Широке впровадження DoH/DoT значно ускладнює традиційні методи аналізу [114].
2) Еволюція техніки атак: Зловмисники активно адаптують свої методи для обходу існуючих систем захисту [63].
3) Масштабування: Зростання обсягів DNS трафіку вимагає нових підходів до ефективного аналізу [64].

4.2.2 Перспективні напрями впровадження AI/ML

Архітектури машинного навчання для DNS безпеки:

1) Гібридні системи аналізу:
    - Комбінування контрольованого та неконтрольованого навчання;
    - Інтеграція різних типів даних (метадані, поведінкові характеристики, контекстуальна інформація);
    - Адаптивне коригування моделей на основі нових даних [61].
2) Федеративне навчання для DNS безпеки:
    - Спільне навчання моделей організаціями без обміну чутливими даними;
    - Підвищення якості моделей за рахунок більшого обсягу тренувальних даних;
    - Збереження приватності та відповідність регуляторним вимогам [71].
3) Експлейнабельний AI для DNS:
    - Розробка моделей з високою інтерпретованістю рішень;
    - Покращення довіри до системи та спрощення розслідування інцидентів;
    - Зменшення часу на аналіз хибно-позитивних спрацювань [65, 68].

Деталізовані технічні інструкції, конфігурації, скрипти та комплексні стратегічні рекомендації з підвищення безпеки DNS-трафіку наведено в Додатку Г.

4.3 Заходи з покращення можливостй парирування з загроз DNS трафіку

Спираючись на аналіз можливостей відомих інструментів з моніторингу трафіку та узагальнення основних напрямів з імплементації AI/ML для цілей та задач DNS безпеки, нижче сформульовано базовий перелік відповідних рекомендацій.

Багаторівнева архітектура захисту DNS:

1) Рівень повноважень - мережевий периметр:
    - Впровадження Pi-hole або аналогічних рішень для базової фільтрації;
    - Конфігурація міжмережевих екранів для контролю DNS трафіку;
    - Моніторинг нестандартних портів DNS (853 для DoT).
2) Рівень повноважень - мережевий моніторинг:

- Розгортання Zeek для автоматизованого аналізу DNS трафіку;
- Інтеграція з Splunk для централізованого збору та аналізу логів;
- Використання Wireshark для глибинного аналізу підозрілого трафіку.

3) Рівень повноважень – аналітика подій та залучення ML:
   - Впровадження спеціалізованих ML моделей для різних типів загроз;
   - Розробка системи скорингу ризиків DNS активності;
   - Інтеграція з існуючими SIEM системами.

ВИСНОВКИ

1) У роботі досліджено архітектуру системи доменних імен та проаналізовано ключові вектори атак, зокрема: DNS tunneling, DNS cache poisoning, amplification, DGA-атаки, а також спроби обходу фільтрації через використання нестандартних каналів.
2) За результатами узагальнення даних про відоми інциденти безпеки проти служби й сервіси DNS, встановлено, що основними передумовами атак на DNS, є відсутність механізмів вбудованого шифрування, відкритість протоколу та його використання у широкому спектрі мережевих сервісів.
3) Проведено огляд і класифікацію сучасних методів виявлення аномалій у DNS-трафіку з використанням спеціалізованих програмних інструментів Wireshark, Zeek, Pi-hole та Splunk. В ходе моделювання встановлено, що тестовані інструменти відрізняються, як по точності виявлення загроз, так і по рівню їх ресурсоспоживання. Найвищі показники виявлення (до 98%) для обраної збірки характерних вразливостей, продемонстрував Splunk, особливо в умовах залучення механізмів AI/ML.
4) В процесі дослідного моделювання, синтезовано тестове середовище з використанням віртуальних машин та різних типів аналізаторів трафіку. Створене віртуальне середовище забезпечило збір формуємих DNS-запитів, їх обробку і візуалізацію процесу. За результатами тестувань, побудовано гістограми розподілу запитів за типами, періодами активності й кодами відповідей.
5) Проведений порівняльний аналіз тестованих зразків ПЗ показав, що Zeek забезпечує оптимальний баланс між продуктивністю, рівнем деталізації лог-файлів й можливістю розширення за рахунок можливості впровадження сценаріїв виявлення загроз. Натомість Wireshark більше орієнтований для ручного аналізу трафіку DNS. Аналіз можливостей рішення «Pi-hole»,

дозволяє позицію вати його, як базовий (спрощенний) фільтр DNS-запитів на локальному рівні.

6) Узагальнення результатів досліджень свідчить про доцільність впровадження концепції багаторівневої архітектури захисту DNS, що одночасно інтегрує інструменти фільтрації, моніторингу, аналітики та протидії, с широким залученням поведінкових модулів на базі AI\ML. В межах цього вектору зусиль, запропоновано дослідну архітектуру, що передбачає поетапне розміщення декількох інструментів контролю (Wireshark, Zeek, Pi-hole та Splunk) DNS трафіку на різних сегментах створюваної (імітованої) сенсорної мережі.
7) Найбільш перспективним напрямом подальших досліджень слід вважати комплексне вдосконалення процедур автоматизації виявлення загроз DNS за допомогою широкого впровадження технологій машинного навчання, вдосконалення точності детектування DGA-доменів та інтеграції з SIEM-системами, що дозволить покращити оперативність реагування на інциденти безпеки DNS, включаючи ще невідомі загрози.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Mockapetris, P. "Domain names - concepts and facilities." RFC 1034, 1987.
2. Global DNS Threat Report. IDC & EfficientIP, 2023.
3. NIST Special Publication 800-81-2: "Secure Domain Name System (DNS) Deployment Guide," 2013.
4. Liu, C., & Albitz, P. "DNS and BIND" (5th Edition). O'Reilly Media, 2006.
5. Internet Assigned Numbers Authority (IANA), "Root Servers," 2023.
6. RFC 1035: "Domain Names - Implementation and Specification," 1987.
7. Kozierok, C. M. "The TCP/IP Guide." No Starch Press, 2005.
8. DNS Security: "In-depth Vulnerability Analysis and Mitigation Solutions." Cisco Systems, 2022.
9. Nemeth, E., et al. "UNIX and Linux System Administration Handbook" (5th Edition). Addison-Wesley, 2017.
10. Kaminsky, D. "Black Ops of DNS." Black Hat USA, 2008.
11. Anagnostopoulos, M., et al. "DNS Amplification Attack Revisited." Computers & Security, 2013.
12. Born, K., & Gustafson, D. "Detecting DNS Tunneling." SANS Institute InfoSec Reading Room, 2019.
13. Santanna, J. J., et al. "NXDOMAIN-based DDoS Attacks." IEEE/IFIP Network Operations and Management Symposium, 2020.
14. Yu, S., et al. "A Survey on DNS Hijacking and Its Countermeasures." IEEE Communications Surveys & Tutorials, 2018.
15. Atkins, D., & Austein, R. "Threat Analysis of the Domain Name System (DNS)." RFC 3833, 2004.
16. Barth, A., et al. "Protecting Browsers from DNS Rebinding Attacks." ACM CCS, 2007.
17. Holz, T., et al. "Measuring and Detecting Fast-Flux Service Networks." NDSS Symposium, 2008.

18. Herzberg, A., & Shulman, H. "DNSSEC: Security and Availability Challenges." IEEE Conference on Communications and Network Security, 2018.
19. Yilek, S., et al. "When Private Keys are Public: Results from the 2008 Debian OpenSSL Vulnerability." ACM Internet Measurement Conference, 2009.
20. RFC 3833: "Threat Analysis of the Domain Name System (DNS)," 2004.
21. Prince, M. "The DDoS That Knocked Spamhaus Offline (And How We Mitigated It)." Cloudflare Blog, 2013.
22. Sullivan, B. "Dyn Statement on 10/21/2016 DDoS Attack." Oracle Dyn Blog, 2016.
23. Amazon Web Services. "AWS Shield Threat Landscape Report." Q1 2020.
24. Cisco Talos Intelligence Group. "DNS Hijacking Abuses Trust In Core Internet Service." 2019.
25. US-CERT. "Alert (TA19-017A): DNS Infrastructure Hijacking Campaign." 2019.
26. 360 Netlab. "RouterOS Botnet: Hundreds of Thousands MikroTik Routers Are Enslaved." 2018.
27. Kaminsky, D. "Black Ops of DNS." Black Hat USA, 2008.
28. FBI. "International Cyber Ring That Infected Millions of Computers Dismantled." Press Release, 2011.
29. Kaspersky Lab. "Criminals Hijack Brazilian Bank DNS to Steal Credentials." SecureList, 2017.
30. FireEye. "APT32 (OceanLotus): Cyber Espionage Group Targeting Southeast Asia." 2017.
31. US-CERT. "Alert (TA14-212A): Backoff Point-of-Sale Malware." 2014.
32. Palo Alto Networks. "New Wekby Attacks Use DNS Requests As Command and Control Mechanism." 2016.
33. Holz, T., et al. "Measuring and Detecting Fast-Flux Service Networks." NDSS Symposium, 2008.

34. Europol. "Avalanche Network Dismantled in International Cyber Operation." Press Release, 2016.
35. Akamai. "State of the Internet / Security Report." Q1 2021.
36. Korolov, M. "The evolving threat of DNS hijacking." CSO Online, 2020.
37. US Department of Justice. "Seven International Cyber Defendants, Including 'APT41' Actors, Charged in Connection with Computer Intrusion Campaigns." Press Release, 2020.
38. IDC & EfficientIP. "Global DNS Threat Report." 2023.
39. Internet Society. "State of DNSSEC Deployment 2023." ISOC Report, 2023.
40. Hjelm, J., et al. "DNS Privacy Considerations." RFC 9076, 2021.
41. Nadler, A., et al. "Detection of Malicious and Low Throughput Data Exfiltration Over the DNS Protocol." ACM Computers & Security, 2019.
42. Antonakakis, M., et al. "Building a Dynamic Reputation System for DNS." USENIX Security Symposium, 2021.
43. Antonakakis, M., et al. "From Throw-Away Traffic to Bots: Detecting the Rise of DGA-Based Malware." USENIX Security Symposium, 2012.
44. Bilge, L., et al. "EXPOSURE: Finding Malicious Domains Using Passive DNS Analysis." NDSS Symposium, 2011.
45. Schiavoni, S., et al. "Phoenix: DGA-Based Botnet Tracking and Intelligence." Detection of Intrusions and Malware, and Vulnerability Assessment, 2014.
46. Woodbridge, J., et al. "Predicting Domain Generation Algorithms with Long Short-Term Memory Networks." arXiv:1611.00791, 2016.
47. Zeng, Y., et al. "Deep Learning for DNS Tunneling Detection." International Conference on Computing, Networking and Communications, 2020.
48. Das, A., et al. "Automated Feature Engineering for DNS Tunnel Detection." IEEE Transactions on Network and Service Management, 2021.
49. Pereira, M., et al. "Robust Features for Detecting Malicious DNS Activities." Journal of Internet Services and Information Security, 2019.
50. Berger, D., et al. "Automating DNS Monitoring and Threat Hunting Using Deep Learning." SANS DFIR Summit, 2020.

51. Rahbarinia, B., et al. "Efficient and Interpretable Deep Learning for Network Security Monitoring." IEEE Security and Privacy, 2019.
52. Ahluwalia, A., et al. "A Deep Learning Approach for DGA Domain Detection." Computers & Security, 2020.
53. Satoh, A., et al. "Detecting DNS Tunneling Using Character Frequency Analysis." Journal of Information Security and Applications, 2018.
54. Torabi, S., et al. "A Federated Learning Approach to DNS Traffic Analysis for Threat Hunting." IEEE Access, 2021.
55. Poh, G., et al. "AI-Based DNS DDoS Detection and Mitigation." Computer Networks, 2020.
56. Zhauniarovich, Y., et al. "A Survey on Malicious Domains Detection through DNS Data Analysis." ACM Computing Surveys, 2018.
57. Lin, W., et al. "CyberDNS: A Large-Scale ML System for DNS-Based Detection of Malicious Internet Activities." Proceedings of the ACM SIGKDD Conference, 2022.
58. Damodaran, A., et al. "A Comparison of Distribution-Based and Challenge-Based DNSSEC Deployments." IEEE Conference on Dependable and Secure Computing, 2021.
59. SANS Institute. "DART: DNS Analysis and Research Tool - Technical Documentation." 2023.
60. Felegyhazi, M., et al. "ML-DNS: Machine Learning Based Detection of DNS Exfiltration." IEEE Transactions on Information Forensics and Security, 2022.
61. Johnson, S., et al. "Comparative Analysis of Machine Learning Techniques for DNS-Based Threat Detection." Network Security Journal, 2023.
62. Ahmed, T., et al. "The Challenge of Dataset Bias in DNS Security Models." International Conference on Dependable Systems and Networks, 2022.
63. Garcia, S., et al. "On the Evasion of ML-Based DNS Detection Systems by Sophisticated Attackers." IEEE Security & Privacy, 2021.
64. Kumar, V., et al. "Computational Efficiency of DNS Security Models: A Benchmarking Study." Journal of Cybersecurity Technology, 2022.

65. Feng, J., et al. "Explainable AI for DNS Threat Detection: Challenges and Progress." Communications of the ACM, 2023.
66. Roberts, N., et al. "Balancing False Positives and Detection Rates in DNS Security." IEEE Transactions on Dependable and Secure Computing, 2022.
67. Wilson, R., et al. "Privacy-Preserving Machine Learning for DNS Security in the GDPR Era." Journal of Cybersecurity, 2023.
68. Chen, H., et al. "Explainable Detection of Malicious DNS Traffic Using Deep Learning." IEEE/IFIP International Conference on Dependable Systems and Networks, 2023.
69. Zhang, L., et al. "Few-Shot Learning for DNS-Based Detection of Emerging Threats." USENIX Security Symposium, 2022.
70. Wang, K., et al. "Adaptive Machine Learning Models for Long-Term DNS Security." IEEE Transactions on Information Forensics and Security, 2023.
71. Schneider, J., et al. "Privacy-Preserving Collaborative DNS Security using Federated Learning." Network and Distributed System Security Symposium, 2022.
72. Huang, Y., et al. "AutoResponse: Automated Generation of DNS Security Countermeasures." ACM Conference on Computer and Communications Security, 2023.
73. Patsakis, C., et al. "Towards a Blockchain-Enhanced Framework for DNSSEC." IEEE Transactions on Dependable and Secure Computing, 2022.
74. Bernstein, D. J. "DNSCrypt: A Protocol for Securing DNS Communications." OpenDNS Technical Report, 2011.
75. Zhu, L., et al. "Connection-Oriented DNS to Improve Privacy and Security." IEEE Symposium on Security and Privacy, 2014.
76. DNSCrypt Implementation Team. "DNSCrypt Protocol Specification." GitHub Repository, 2018.
77. Denis, F. "DNSCrypt-proxy 2 - A flexible DNS proxy with support for encrypted DNS protocols." GitHub Documentation, 2020.

78. Hu, Z., et al. "Specification for DNS over Transport Layer Security (TLS)." RFC 7858, 2016.
79. IETF DNS Privacy Working Group. "DNS Privacy Considerations." RFC 9076, 2021.
80. Dickinson, S., et al. "Authentication and (D)TLS Profile for DNS-over-(D)TLS." RFC 8310, 2018.
81. Android Open Source Project. "Private DNS in Android P." Android Developers Blog, 2018.
82. Hoffman, P., et al. "DNS Queries over HTTPS (DoH)." RFC 8484, 2018.
83. Sullivan, N. "Encrypting DNS End-to-End." Cloudflare Blog, 2018.
84. Barnes, R., et al. "Analysis of Potential Solutions for Encrypted DNS." Internet Society, 2021.
85. Mozilla Foundation. "TRR Policy Requirements for DNS over HTTPS Partners." Mozilla Wiki, 2020.
86. Huitema, C., et al. "Specification of DNS over Dedicated QUIC Connections." RFC 9250, 2022.
87. Farell, S., et al. "QUIC: A UDP-Based Multiplexed and Secure Transport." RFC 9000, 2021.
88. Bishop, M. "HTTP/3 for DNS: Opportunities and Challenges." DNS-OARC Workshop, 2021.
89. Cloudflare Research. "DNS Performance over QUIC vs DNS over TLS." Measurement Study, 2022.
90. Bottger, T., et al. "Looking for the Needle in the Haystack: A Comprehensive Study of Encrypted DNS Protocols." ACM Internet Measurement Conference, 2022.
91. Arends, R., et al. "DNS Security Introduction and Requirements." RFC 4033, 2005.
92. Kolkman, O., et al. "DNSSEC Operational Practices." RFC 6781, 2012.
93. Weiler, S., et al. "DNSSEC Authenticated Denial of Existence." RFC 4470, 2006.
94. Eastlake, D. "Domain Name System Security Extensions." RFC 2065, 1997.

95. Eastlake, D. "Domain Name System Security Extensions." RFC 2535, 1999.
96. Arends, R., et al. "Resource Records for the DNS Security Extensions." RFC 4034, 2005.
97. ICANN. "Root DNSSEC Design Team Report." ICANN Technical Report, 2010.
98. Larson, M., et al. "DNSSEC Root Zone KSK Rollover Plan." ICANN Technical Report, 2016.
99. Internet Society. "State of DNSSEC Deployment 2023." ISOC Report, 2023.
100. SIDN Labs. "DNSSEC Deployment Monitor: Global TLD Analysis." Quarterly Report, 2023.
101. APNIC Labs. "DNSSEC Validation Rate by Country." Measurement Study, 2023.
102. Sullivan, A. "Best Practices for DNS Encryption: Combining DNSSEC with DoT/DoH." Internet Engineering Task Force, 2020.
103. Moriarty, K., et al. "Transport Layer Security (TLS) Encryption for DNS." IEEE Security & Privacy, 2022.
104. Deccio, C., et al. "A Comprehensive Analysis of DNS over TLS with DNSSEC." ACM SIGCOMM, 2021.
105. Herzberg, A., et al. "DNSSEC: Security and Availability Challenges." IEEE Conference on Communications and Network Security, 2018.
106. Chung, T., et al. "Understanding the Role of DNSSEC in the DNS Ecosystem." Proceedings of the ACM Internet Measurement Conference, 2022.
107. Abley, J., et al. "DNSSEC Operational Challenges and Mitigation Strategies." DNS-OARC Workshop, 2021.
108. van Rijswijk-Deij, R., et al. "The Cost of DNSSEC Deployment: Why Hasn't It Taken Off?" Journal of Cybersecurity, 2020.
109. Lu, C., et al. "An Empirical Study of DNS Encryption Impact on Web Performance." IEEE/ACM Transactions on Networking, 2021.
110. Böttger, T., et al. "A Comparative Performance Analysis of DNS over HTTPS, DNS over TLS, and Traditional DNS." IEEE Journal on Selected Areas in Communications, 2022.

111. Hounsel, A., et al. "Comparing the Effects of DNS, DoT, and DoH on Web Performance." Proceedings of The Web Conference, 2020.

112. Shulman, H., et al. "Pretty Bad Privacy: Pitfalls of DNS Encryption." ACM Workshop on Privacy in the Electronic Society, 2021.

113. Borgolte, K., et al. "DNS-over-HTTPS: Challenges for Enterprise Network Security." USENIX Security Symposium, 2021.

114. Trevisan, M., et al. "Measuring the Impact of Encrypted DNS on Privacy, Security, and Performance." Computer Networks, 2022.

115. Vekshin, D., et al. "Performance Evaluation of Modern DNS Privacy Protocols." IEEE Transactions on Dependable and Secure Computing, 2022.

116. Livingood, J., et al. "Centralized DNS over HTTPS (DoH) Implementation Issues and Risks." RFC 8932, 2020.

117. Schmidt, T., et al. "DNS Resolution in Enterprise Networks: Implementation and Security Challenges." Enterprise Networks Conference, 2021.

118. Contavalli, C., et al. "Client Subnet in DNS Queries." RFC 7871, 2016.

119. Vixie, P., et al. "DNS Response Policy Zones (RPZ)." Internet Systems Consortium, 2017.

120. DeKok, A., et al. "Privacy Considerations for DNS over TLS and DNS over HTTPS." RFC 8932, 2020.

121. Shulman, H., et al. "DNS over HTTPS and DNS over TLS: A Security and Privacy Perspective." ACM Computing Surveys, 2022.

122. Jeitner, P., et al. "Measuring and Mitigating the Privacy Impact of DNS Encryption." Proceedings of the Privacy Enhancing Technologies Symposium, 2021.

123. Murthy, R., et al. "Forensic Analysis Challenges in the Age of DNS Encryption." Digital Investigation Journal, 2022.

124. Houser, R., et al. "How DNS over HTTPS is Reshaping Privacy, Performance, and Policy in the Internet Ecosystem." Journal of Information Policy, 2021.

125. Zhang, L., et al. "Enterprise DNS in the Era of DNS Encryption: Challenges and Solutions." Network Security Journal, 2022.

126. Anderson, B., et al. "Identifying Encrypted DNS Traffic Using Machine Learning Techniques." IEEE Security and Privacy, 2022.

127. Cambiaso, E., et al. "Split-DNS: Balancing Privacy and Control in Enterprise Networks." Journal of Network and Systems Management, 2022.

128. Moura, G., et al. "Integrating DNS Encryption Monitoring in Next-Generation Firewalls." IEEE Networking Letters, 2021.

129. Bøe, M., et al. "Corporate DNS Control Strategies in the Post-Encryption Era." Enterprise Security Architecture, 2023.

130. Singh, K., et al. "Hybrid DNS Security: Combining Traditional and Encrypted DNS." IEEE Transactions on Network and Service Management, 2022.

131. Yang, C., et al. "Behavioral Analysis of Network Traffic for DNS Anomaly Detection." IEEE Transactions on Information Forensics and Security, 2022.

132. Katz, J., et al. "Analyzing Security Implications of DNS Resolving in VPN Contexts." ACM CCS, 2022.

133. Ren, J., et al. "The Balance between Privacy and Security in Encrypted DNS." IEEE Internet Computing, 2022.

134. Hoffman, P., et al. "DNS Privacy Considerations." RFC 9076, 2021.

135. Rabinovich, E., et al. "Ethical Dimensions of DNS Privacy Technologies." Journal of Information Ethics, 2022.

136. Houser, R., et al. "Tailoring DNS Privacy Controls for Different Network Environments." Journal of Cybersecurity Technology, 2022.

137. Sharma, V., et al. "An Analysis of VPN Services with Integrated DNS Privacy Features." IEEE Access, 2022.

138. Tyagi, N., et al. "Configuring External Encrypted DNS with VPN: Best Practices and Pitfalls." Network Security Conference, 2022.

139. Liu, D., et al. "Split-Tunnel VPN Architectures: DNS Considerations and Security Implications." IEEE Communications Magazine, 2022.

140. Zheng, H., et al. "Cascading Security Models: Combining VPN and Encrypted DNS for Enhanced Privacy." Journal of Network and Computer Applications, 2023.
141. Barrera, D., et al. "HTTPS Proxies and DNS over HTTPS: Interactions and Security Implications." USENIX Security Symposium, 2022.
142. Khattak, S., et al. "SOCKS Proxies in the Era of DNS Privacy: Compatibility and Security Analysis." ACM SIGCOMM, 2022.
143. Papadopoulos, P., et al. "Challenges of Transparent Proxies in Monitoring Encrypted DNS Traffic." IEEE Symposium on Security and Privacy, 2022.
144. Johnson, E., et al. "The Combined Effect of VPN and Encrypted DNS on Internet Censorship Circumvention." Freedom Online Conference Proceedings, 2022.
145. Enghardt, T., et al. "Detecting and Preventing DNS and WebRTC Leaks in VPN Environments." IEEE Internet Computing, 2023.
146. Chen, Y., et al. "Best Practices for Configuring VPN with DNS Encryption: A Comprehensive Guide." Journal of Network Security, 2023.
147. Wang, Z., et al. "Unified Security Platforms: Integrating VPN, Encrypted DNS, and Threat Protection." IEEE Transactions on Dependable and Secure Computing, 2023.
148. Singh, M., et al. "Adaptive Traffic Routing in Multi-layer Security Systems." Computer Networks, 2023.
149. Castro, S., et al. "Towards Decentralized Trust Models for DNS and VPN Services." Proceedings of the Decentralized Web Conference, 2023.

ДОДАТОК А

Перелік і зміст найбільш показових інцидентів з реалізацією атак на DNS

А.1 Перелік і зміст інцидентів з реалізацією атаки DNS Amplification

1) Атака на Spamhaus (2013) - одна з найбільших DDoS-атак свого часу з пропускною здатністю до 300 Гбіт/с, що використовувала відкриті DNS-резолвери для підсилення трафіку. Атака призвела до суттєвого уповільнення інтернет-з'єднання в окремих регіонах Європи [21].

2) Атака на Dyn (2016) - масштабна DDoS-атака на DNS-провайдера Dyn з використанням ботнету Mirai, що складався з сотень тисяч незахищених IoT-пристроїв. Внаслідок атаки було порушено доступ до численних популярних веб-сервісів, включаючи Twitter, Netflix, GitHub, Amazon, Spotify та інші, для мільйонів користувачів у Північній Америці та Європі [22].

3) Атака на Amazon Web Services (2020) - рекордна DDoS-атака з піковою пропускною здатністю 2,3 Тбіт/с, спрямована на інфраструктуру Amazon Route 53 (DNS-сервіс AWS). Атака використовувала техніку CLDAP-відображення (Connection-less Lightweight Directory Access Protocol), але завдяки автоматичному масштабуванню та захисним механізмам AWS не призвела до суттєвих перебоїв [23].

А.2. Кампанії з атакою типу DNS Hijacking

Перехоплення DNS є потужним інструментом в арсеналі кіберзлочинців та хакерських груп, що підтримуються державами. Серед найважливіших інцидентів цього типу, слід виділити наступні [24-26]:

1) Операція «Sea Turtle» (2017-2019) - масштабна кампанія з кібершпигунства, приписувана хакерам, підтримуваним урядом. Зловмисники систематично компрометували DNS-інфраструктуру для перехоплення електронної пошти та іншого мережевого трафіку національних організацій безпеки, енергетичних компаній та міністерств у Північній Африці та на Близькому Сході. Унікальність операції полягала в тому, що атакуючі зламували

не кінцеві організації, а їхніх DNS-провайдерів та реєстраторів доменів, що дозволяло отримати контроль над численними доменами одночасно [24].

2) DNSpionage (2018-2019) - кампанія, спрямована на урядові організації та телекомунікаційних провайдерів на Близькому Сході. Зловмисники змінювали DNS-записи легітимних веб-сайтів, перенаправляючи користувачів на фішингові сторінки для викрадення облікових даних. Кампанія призвела до викрадення електронної пошти та інших конфіденційних даних [25].

3) Інцидент з RouterOS (2018) - масштабна атака на маршрутизатори від компанії MikroTik, під час якої зловмисники змінювали DNS-налаштування на скомпрометованих пристроях, перенаправляючи користувачів на шкідливі сервери. За оцінками експертів, було скомпрометовано понад 170 000 маршрутизаторів по всьому світу [26].

А.3 Атаки на кеш DNS та інші методи отруєння DNS

Отруєння DNS-кешу залишається серйозною загрозою, незважаючи на впровадження захисних механізмів [27-29]:

1) Атака Камінського (2008) - фундаментальна вразливість у протоколі DNS, виявлена дослідником Деном Камінським. Вразливість дозволяла зловмисникам вводити фальшиві записи в кеш DNS-серверів через недостатню ентропію у транзакційних ідентифікаторах DNS-запитів. Після публічного розкриття вразливості було розроблено та впроваджено термінові патчі для всіх основних DNS-серверів, а також прискорено розробку DNSSEC як довгострокового рішення [27].

2) Operation Ghost Click (2007-2011) - масштабна міжнародна операція ботнету, що використовувала шкідливе програмне забезпечення DNSChanger для зміни DNS-налаштувань на заражених комп'ютерах. На піку активності ботнет контролював DNS-конфігурацію понад 4 мільйонів комп'ютерів у більш ніж 100 країнах. Зловмисники перенаправляли інтернет-трафік користувачів на шахрайські веб-сайти та підміняли рекламу для отримання прибутку. Операція

була припинена в результаті міжнародної співпраці правоохоронних органів (операція «Trident Tribunal») [28].

3) Інцидент з бразильськими банками (2017) - зловмисники скомпрометували DNS-сервери декількох інтернет-провайдерів у Бразилії, змінивши DNS-записи для популярних банківських сайтів. Користувачі перенаправлялися на фішингові копії банківських порталів, що призвело до масштабного викрадення облікових даних [29].

А.4 Інциденти, пов'язані з DNS Tunneling

Процедура/техніка DNS-тунелювання є потужним методом для обходу систем безпеки та створення прихованих каналів зв'язку [30-32]:

1) Операція "Cobalt Kitty" (2016-2017) - цільова атака на велику азіатську корпорацію, під час якої хакерська група APT32 (OceanLotus) використовувала DNS-тунелювання для приховування командного каналу (C2) та ексфільтрації даних. Зловмисники використовували легітимні DNS-запити для передачі зашифрованих команд та даних, що дозволяло обходити системи виявлення вторгнень та міжмережеві екрани [30].

2) Атаки FrameworkPOS (2014-2016) - шкідливе програмне забезпечення, що використовувалося для компрометації платіжних терміналів у великих роздрібних мережах США, включаючи Target, Home Depot та інші. Для ексфільтрації викрадених даних платіжних карток використовувалося DNS-тунелювання, що дозволяло обходити сегментацію мережі та системи виявлення вторгнень [31].

3) Інцидент з Wekby APT (2015) - цільова атака на організації охорони здоров'я з використанням шкідливого програмного забезпечення "PISLOADER", що використовувало DNS-тунелювання для зв'язку з серверами командування та управління. Ця техніка дозволяла зловмисникам обходити контроль мережевого трафіку та приховувати свою активність [32].

А.5 Масштабні інциденти Fast Flux DNS

Техніка здійснення атак Fast Flux DNS використовується зловмисниками для підвищення стійкості власної шкідливої інфраструктури [33-34]:

1) Ботнет Storm (2007-2008) - один з перших великих ботнетів, що використовував технологію Fast Flux для приховування командних серверів та підвищення стійкості мережі. Ботнет складався з сотень тисяч заражених комп'ютерів та використовувався для розсилки спаму, DDoS-атак та поширення шкідливого програмного забезпечення [33].

2) Ботнет Avalanche (2009-2016) - потужна інфраструктура кіберзлочинців, що використовувала Double-Flux (комбінація Fast Flux для A-записів та NS-записів) для підтримки численних фішингових кампаній та розповсюдження шкідливого програмного забезпечення. Інфраструктура обслуговувала понад 20 різних сімейств шкідливого програмного забезпечення та була ліквідована в результаті міжнародної операції правоохоронних органів [34].

ДОДАТОК Б

Методи машинного навчання для аналізу DNS-трафіку

Залежно від характеру завдань та доступних даних, у сфері безпеки DNS застосовуються різні методи машинного навчання (див. таблиця Б.1):

Таблиця Б.1 - Методи машинного навчання та їх застосування в безпеці DNS

Метод ML	Застосування в безпеці DNS	Переваги	Обмеження
Контрольоване навчання (Supervised Learning)	Класифікація доменів, виявлення шкідливих запитів	Висока точність при наявності якісних розмічених даних	Потреба у великих обсягах розмічених даних, вразливість до невідомих атак
Неконтрольоване навчання (Unsupervised Learning)	Виявлення аномалій, кластеризація патернів трафіку	Здатність виявляти невідомі раніше загрози	Складність інтерпретації результатів, високий рівень хибно-позитивних спрацювань
Напівконтрольоване навчання (Semi-supervised Learning)	Виявлення аномалій з частково розміченими даними	Ефективне використання як розмічених, так і нерозмічених даних	Складність реалізації, чутливість до якості початкових розміток

Продовження таблиці Б.1

Метод ML	Застосування в безпеці DNS	Переваги	Обмеження
Навчання з підкріпленням (Reinforcement Learning)	Адаптивні системи реагування на інциденти	Здатність адаптуватися до змін у середовищі	Складність налаштування, потенційні ризики при автономному прийнятті рішень
Глибоке навчання (Deep Learning)	Аналіз складних патернів у DNS-запитах, виявлення DGA	Висока точність при роботі з великими обсягами даних	Висока обчислювальна складність, "чорна скринька" для інтерпретації

Ефективність, обмеження та перспективи застосування AI/ML для виявлення DNS-атак

Ефективність AI/ML у виявленні різних типів DNS-атак

Дослідження показують різну ефективність методів AI/ML при виявленні різних типів атак на DNS. У таблиці нижче наведено узагальнені результати (див. таблиця Б.2):

Таблиця Б.2 — Ефективність AI/ML у виявленні різних типів DNS-атак

Тип атаки	Ефективність виявлення за допомогою AI/ML	Найбільш ефективні методи
DNS Tunneling	Висока (90–99%)	Глибокі нейронні мережі, методи аналізу часових рядів
DNS Amplification DDoS	Висока (85–95%)	Алгоритми виявлення аномалій, статистичні методи

Продовження таблиці Б.2

Тип атаки	Ефективність виявлення за допомогою AI/ML	Найбільш ефективні методи
DNS Cache Poisoning	Середня (70–85%)	Аналіз поведінки, моніторинг змін у відповідях
Fast Flux	Висока (85–95%)	Методи аналізу графів, кластеризація
DGA-домени	Дуже висока (95–99%)	CNN, RNN, LSTM-мережі
DNS Hijacking	Середня (65–80%)	Методи аналізу поведінки, виявлення аномалій

Виклики та обмеження застосування AI/ML для безпеки DNS

Попри значний потенціал, технології AI/ML стикаються з низкою викликів при використанні у сфері безпеки DNS:

1) Проблема обсягу та якості даних — ефективне навчання моделей потребує великих обсягів якісних, розмічених даних, що не завжди доступні, особливо для нових типів атак [62].
2) Адаптивність зловмисників — кіберзлочинці постійно адаптують свої методи для обходу захисту, що породжує ефект "гонки озброєнь" [63].
3) Обчислювальні вимоги — складні моделі глибокого навчання вимагають великих ресурсів, що ускладнює їхнє застосування в реальному часі, зокрема на периферійних пристроях [64].
4) Інтерпретованість моделей — багато моделей працюють як "чорна скринька", що знижує довіру та ускладнює аналіз прийнятих рішень [65].
5) Баланс між точністю і хибнопозитивними спрацюваннями — спроби підвищити чутливість систем часто збільшують кількість хибних спрацювань [66].

6) Питання приватності та відповідності регуляторним вимогам — збір DNS-даних може порушувати права користувачів і законодавство, наприклад, GDPR [67].

Узагальнення напрямів подальшого розвитку

Сучасні дослідження пропонують низку інноваційних підходів для покращення ефективності та практичного застосування AI/ML у сфері DNS-безпеки:

1) Експлейнабельний AI (XAI) — розвиток інтерпретованих моделей, здатних пояснювати свої рішення [68].
2) Навчання з мінімальними даними — методи few-shot learning, transfer learning, active learning дозволяють навчати моделі на малих вибірках [69].
3) Моделі, стійкі до concept drift — підвищення адаптивності моделей до змін у даних та атаках [70].
4) Федеративне навчання — об'єднане навчання моделей без обміну конфіденційними даними, що знижує ризики витоку [71].
5) Автоматизоване генерування контрзаходів — системи, які не лише виявляють, а й автоматично реагують на загрози [72].
6) Інтеграція з блокчейном — для перевірки цілісності DNS-записів і створення систем репутації доменів [73].

ДОДАТОК В

В.1 Основні етапи розвитку технологій шифрування DNS

Еволюція технологій шифрування DNS відображає загальну тенденцію до посилення захисту користувацьких даних та протидії постійно зростаючим кіберзагрозам. Кожен етап цієї еволюції характеризується впровадженням нових криптографічних механізмів, оптимізацією протоколів передачі даних та пошуком балансу між безпекою, приватністю та продуктивністю.

В.1.1 DNSCrypt

DNSCrypt став першим широко розповсюдженим протоколом шифрування DNS, що заклав концептуальну основу для подальшого розвитку технологій захисту DNS:

- Генезис технології: Протокол був розроблений у 2011 році криптографом Даніелем Бернштейном та командою OpenDNS як відповідь на зростаючі загрози перехоплення та підміни DNS-запитів. Концептуально DNSCrypt став важливою віхою у розвитку систем шифрування DNS, демонструючи практичну можливість захисту DNS-трафіку без суттєвого впливу на продуктивність [74].
- Криптографічна архітектура: DNSCrypt базується на високоефективних криптографічних примітивах, включаючи криптографію на еліптичних кривих (алгоритм X25519 для обміну ключами) та шифри автентифікованого шифрування ChaCha20-Poly1305. Ця комбінація забезпечує оптимальний баланс між криптографічною стійкістю та обчислювальною ефективністю, що особливо важливо для мобільних пристроїв та вбудованих систем з обмеженими ресурсами [75].
- Особливості імплементації та розгортання: Протокол підтримує роботу як через UDP, так і через TCP, що забезпечує гнучкість у різних мережевих середовищах. Однією з ключових особливостей DNSCrypt є використання анонімізованих сертифікатів, що мінімізує можливості для ідентифікації користувачів та створення їх профілів. Незважаючи на відсутність офіційної

стандартизації IETF, DNSCrypt отримав широке впровадження завдяки своїй ефективності та відносній простоті інтеграції [76].

- Розвиток екосистеми: Важливим фактором успіху DNSCrypt стало створення розвиненої екосистеми програмного забезпечення, включаючи DNSCrypt-proxy – універсальний інструмент для інтеграції протоколу з різними операційними системами та мережевими конфігураціями. Підтримка DNSCrypt такими провайдерами як Cloudflare, AdGuard і Quad9 сприяла його подальшому поширенню [77].

B.1.2 DNS-over-TLS (DoT)

DoT став першим стандартизованим протоколом шифрування DNS, що забезпечує захист на транспортному рівні:

- Процес стандартизації: Протокол був формалізований у RFC 7858 у травні 2016 року після тривалого процесу розробки та обговорення в рамках IETF. Стандартизація DoT стала важливим кроком у напрямку уніфікації підходів до шифрування DNS та забезпечення сумісності між різними імплементаціями [78].
- Архітектурні особливості: DoT функціонує через виділений порт 853, що дозволяє легко ідентифікувати та диференціювати DNS-трафік від іншого зашифрованого трафіку. Використання TLS протоколу (версії 1.2 або вище) забезпечує надійний захист від перехоплення та модифікації DNS-запитів завдяки стандартизованим механізмам автентифікації та шифрування [79].
- Особливості валідації сертифікатів: DoT підтримує два основні режими автентифікації: opportunistic (опортуністичний), що пріоритезує доступність над безпекою, та Strict (строгий), що вимагає валідації сертифікатів. Ця гнучкість дозволяє адаптувати протокол до різних сценаріїв використання з відповідним балансом між безпекою та функціональністю [80].
- Інтеграція з операційними системами: Підтримка DoT була інтегрована у Android 9+ та iOS 14+, що значно розширило базу користувачів цієї технології. Проте використання нестандартного порту (853) створює певні

обмеження для впровадження в мережах з суворими політиками фільтрації, де цей порт може бути заблокований [81].

B.1.3 DNS-over-HTTPS (DoH)

DoH представляє найбільш революційний підхід до шифрування DNS, що ґрунтується на інтеграції DNS з інфраструктурою веб:

- Концептуальний фундамент та стандартизація: Протокол був стандартизований у RFC 8484 у жовтні 2018 року, після інтенсивного розвитку, ініційованого Mozilla та підтриманого Google. Концептуально DoH відрізняється від попередніх підходів фундаментальною зміною моделі передачі DNS-запитів – замість створення спеціалізованого захищеного каналу для DNS, протокол інтегрує DNS-запити у стандартний HTTPS-трафік [82].
- Технічні характеристики та імплементація: DoH використовує стандартний порт 443 та повністю інкапсулює DNS-запити в HTTPS-запити, дозволяючи їм "розчинятися" у загальному потоці веб-трафіку. Протокол підтримує різні методи передачі даних, включаючи GET та POST запити, а також може використовувати переваги HTTP/2 та HTTP/3, зокрема мультиплексування та стиснення заголовків [83].
- Технологічні переваги та виклики: Основною перевагою DoH є надзвичайна стійкість до блокування та фільтрації, оскільки DNS-трафік стає невідрізнюваним від звичайного HTTPS-трафіку. Водночас, ця особливість створює значні виклики для корпоративних політик безпеки та мережевого адміністрування, ускладнюючи контроль та моніторинг DNS-трафіку [84].
- Екосистема та соціо-технічні аспекти впровадження: DoH отримав безпрецедентну підтримку від індустрії, включаючи інтеграцію у всі основні веб-браузери (Firefox, Chrome, Edge) та операційні системи. Проте його впровадження супроводжувалося значними дискусіями щодо балансу між приватністю користувачів та легітимними потребами мережевого

моніторингу, особливо в контексті корпоративного управління та державного регулювання [85].

B.1.4 DNS-over-QUIC (DoQ)

DoQ представляє найновішу ітерацію в еволюції технологій шифрування DNS, поєднуючи переваги сучасних транспортних протоколів:

- Генезис та стандартизація: Протокол знаходиться у процесі стандартизації IETF з 2020 року (RFC 9250). Концептуально DoQ розвиває ідеї, закладені в DoT, але використовує QUIC замість TCP як транспортний протокол, що дозволяє отримати значні переваги в продуктивності та надійності [86].
- Технічна архітектура та особливості: QUIC поєднує переваги TCP (надійність, контроль потоку) та UDP (низька затримка, мультиплексування), додаючи вбудоване шифрування на основі TLS 1.3. Це дозволяє DoQ забезпечувати швидше встановлення з'єднання, кращу стійкість до втрати пакетів та ефективнішу роботу в умовах нестабільних мереж, наприклад, мобільних з'єднань [87].
- Оптимізації продуктивності: Особливо важливими є оптимізації DoQ, орієнтовані на мобільні мережі, включаючи зменшення кількості раундів для встановлення з'єднання, покращену підтримку зміни мереж (Connection Migration) та ефективніше використання доступної пропускної здатності [88].
- Перспективи розвитку та впровадження: Хоча DoQ знаходиться на ранніх стадіях впровадження, підтримка протоколу ключовими гравцями ринку DNS (Cloudflare, AdGuard) та його технічні переваги створюють значний потенціал для широкого впровадження в найближчі роки [89].

ДОДАТОК Г

Г.1 Теоретичні основи та принципи функціонування DNSSEC

DNSSEC реалізує комплексний криптографічний механізм для автентифікації DNS-записів, ґрунтуючись на асиметричній криптографії та концепції ланцюжка довіри:

- Концептуальні засади: DNSSEC був розроблений для протидії атакам типу кеш-отруєння (cache poisoning) та спуфінгу DNS, які є особливо небезпечними, оскільки дозволяють перенаправляти користувачів на підроблені веб-сайти навіть за умови використання HTTPS. Концептуально, DNSSEC вирішує проблему достовірності інформації, отриманої через систему DNS [91];
- Криптографічна модель: DNSSEC використовує асиметричну криптографію для створення цифрових підписів DNS-записів. Кожна зона DNS має пару публічного та приватного ключів. Приватний ключ використовується для підписання ресурсних записів, а публічний ключ – для перевірки цих підписів. Важливим елементом є механізм т.з. «ланцюжка довіри» (chain of trust), що забезпечує валідацію від кореневої зони до конкретного домену через послідовність делегувань [92];
- Типи записів DNSSEC: Для реалізації механізмів автентифікації, DNSSEC вводить кілька спеціалізованих типів DNS-записів:
    - DNSKEY – містить публічний ключ для зони, використовується для перевірки підписів RRSIG;
    - RRSIG (Resource Record Signature) – містить цифровий підпис для групи записів одного типу;
    - DS (Delegation Signer) – зберігається у «батьківській» зоні та містить хеш ключа DNSKEY «дочірньої» зони, забезпечуючи т.ч., ланцюжок довіри між зонами;
    - NSEC/NSEC3 – забезпечують автентифіковане заперечення існування запису, запобігаючи атакам типу «підробка відповіді про неіснування домену» [93];

- Процес валідації DNSSEC: Процес підтвердження DNSSEC, включає в себе складну послідовність наступних операцій:
  - Рекурсивний резолвер (прийомо-відповідач) отримує DNS-відповідь з підписами RRSIG;
  - Резолвер перевіряє підписи, використовуючи відповідний ключ DNSKEY;
  - Для верифікації самого ключа DNSKEY використовується запис DS з батьківської зони;
  - Процес продовжується до кореневої зони, для якої резолвер має попередньо встановлений «якірний» ключ довіри.

ДОДАТОК Д

Еволюція методів контролю DNS-трафіку та їх регуляторно-етичні аспекти

Д.1 Еволюція методів контролю DNS-трафіку

Історично контроль DNS-трафіку був відносно простим завданням завдяки незашифрованій природі традиційного DNS:

- Традиційні механізми контролю DNS:
  - Пасивний моніторинг DNS-запитів на рівні мережевої інфраструктури (порт 53 UDP/TCP);
  - Централізовані корпоративні DNS-резолвери з інтегрованими політиками безпеки;
  - Системи виявлення вторгнень (IDS) з аналізом DNS-трафіку для ідентифікації шкідливих доменів;
  - DNS Response Policy Zones (RPZ) для динамічної фільтрації DNS-запитів;
  - Аналіз DNS-логів для виявлення аномалій та розслідування інцидентів безпеки [116-119].
- «Примітивні» інструменти й техники блокування шифрованого DNS:
  - Блокування відомих публічних DoH/DoT-серверів за IP-адресами;
  - Блокування нестандартних портів (853 для DoT);
  - Блокування DNS-запитів до відомих доменів DNS-провайдерів;
  - Обмеження TLS-з'єднань до специфічних доменів [124].

Застосування спрощених підходів блокування, характеризєються низькою ефективністю через можливість їх обходу, та високий рівень помилкових блокувань. Це призводить до погіршення користувацького досвіду та потенційних проблем з легітимними сервісами.

Д.2 Регуляторні та етичні аспекти контролю DNS

Контроль шифрованого DNS-трафіку має важливі регуляторні та етичні виміри, що впливають на підходи до його імплементації:

- Правові аспекти контролю DNS:

- Різноманітність законодавчих вимог у різних юрисдикціях щодо фільтрації контенту;
- Потенційні конфлікти між національними регуляціями та глобальною природою інтернету;
- Юридичні вимоги щодо збереження та надання доступу до логів DNS у рамках розслідувань;
- Відповідність систем контролю DNS регуляторним вимогам щодо захисту даних (GDPR, CCPA тощо) [134];

- Етичні аспекти впровадження шифрування DNS:
  - Балансування між правом на приватність та легітимними потребами безпеки;
  - Транспарентність щодо методів моніторингу та контролю DNS-трафіку;
  - Етичні аспекти інспекції зашифрованого трафіку в різних контекстах;
  - Потенційний конфлікт між корпоративними політиками безпеки та особистими правами працівників [135];
- Застосування диференційованих підходів до контролю DNS в окремих середовищах та/чи умовах:
  - Домашні мережі: пріоритет приватності користувачів та захист від шкідливого програмного забезпечення;
  - Корпоративні мережі: баланс між безпекою корпоративних даних та приватністю співробітників;
  - Освітні установи: забезпечення безпечного середовища з урахуванням вікових особливостей;
  - Критична інфраструктура: підвищені вимоги до безпеки та контролю [136].

ДОДАТОК Е

Е.1 Матриця поведінкових індикаторів для різних типів атак

Таблиця Е.1 – Узагальнення поведінкових індикаторів для різних типів DNS-атак з даними [49, 53, 131]

Тип атаки	Часові індикатори	Волюметричні індикатори	Топологічні індикатори	Криптографічні індикатори
DNS-тунелювання	Регулярність запитів, нетипова частота	Аномальне співвідношення розмірів запит/відповідь	Надмірна кількість унікальних піддоменів	Нетипові патерни шифрування, персистентні з'єднання
DGA-активність	Бурсти запитів, висока частота NXDOMAIN	Висока кількість запитів з низьким відсотком успішних	Слабка структурна зв'язність доменів	Множинні короткі TLS-сесії до різних серверів
Fast Flux	Висока частота запитів до обмеженої множини доменів	Нормальний розмір пакетів, аномальна частота	Швидка зміна графу доменів-IP	Стандартні криптографічні характеристики
DNS Amplification	Сплески вихідних запитів, висока частота	Асиметрія розмірів запит/відповідь	Концентрація запитів до обмеженої множини серверів	Обмежене використання шифрування, перевага UDP
Cache Poisoning	Аномальні патерни кешування, нетипові TTL	Нормальні волюметричні характеристики	Невідповідності в графі розв'язання	Нестандартні патерни валідації

Е.2 Узагальнення відомих інноваційних підходів, стосовно поведінкового аналізу DNS

Сучасні дослідження пропонують ряд інноваційних підходів, що розширюють можливості проведення поведінкового аналізу DNS трафіку. Систематизовані результати з аналізу [51,71,65,68-69] основних з них, представлено нижче.

- Федеративне навчання для колаборативного виявлення загроз:
  - Розподілене навчання моделей на даних різних організацій без централізації чутливої інформації;
    - Покращення якості моделей за рахунок більшої ємності та розмаїття даних;
  - Збереження приватності та відповідність регуляторним вимогам;
  - Підвищена стійкість до локальних аномалій та зміщень у даних [71].
- Експлейнабельний AI (XAI) для інтерпретації результатів:
  - Розробка моделей, що надають зрозумілі пояснення виявлених аномалій;
  - Використання методів SHAP, LIME, деревоподібних моделей з високою інтерпретованістю;
  - Покращення довіри до системи та спрощення розслідування інцидентів;
  - Зменшення часу на аналіз хибно-позитивних спрацювань [65, 68].
- Активне навчання (Active Learning):
  - Селективний вибір найбільш інформативних зразків для ручного розмічення;
  - Оптимізація використання експертного часу для покращення моделей;
  - Адаптивне коригування моделей на основі цільового зворотного зв'язку;
  - Підвищення ефективності навчання в умовах обмежених розмічених даних [69].
- Трансферне навчання (Transfer Learning):
  - Адаптація моделей, попередньо навчених на великих загальних наборах даних, до специфічних умов мережі;

- Зменшення вимог до обсягу даних для ефективного навчання;
- Прискорення впровадження нових моделей виявлення аномалій;
- Покращення генералізації для нових типів загроз [69].

- Поведінковий аналіз на основі теорії графів:
  - Моделювання DNS-активності як динамічного графу взаємодій;
  - Виявлення аномальних структур та патернів у графі;
  - Аналіз еволюції графу з часом для виявлення прихованих загроз.

Також, окремо, слід додату сюди й практику використання графових нейронних мереж для аналізу складних взаємозв'язків [51].

Е.3 Практичні аспекти впровадження ML для виявлення аномалій DNS.

Впровадження систем поведінкового аналізу та машинного навчання для виявлення аномалій DNS вимагає врахування ряду практичних аспектів:

- Збір та підготовка даних:
  - Забезпечення репрезентативності даних для навчання моделей;
  - Розробка механізмів синтетичної генерації прикладів атак;
  - Балансування класів для запобігання зміщенню моделей;
  - Нормалізація й стандартизація ознак для покращення якості використовуваних поведінкових моделей [62].
- Проблеми та обмеження:
  - Висока обчислювальна складність деяких моделей, особливо глибоких нейронних мереж;
  - Складність інтерпретації результатів складних моделей (проблема т.з. «чорної скриньки»);
  - Необхідність регулярного оновлення та перенавчання моделей;
  - Баланс між чутливістю виявлення та рівнем хибно-позитивних спрацювань [64, 66].
- Оптимізація продуктивності:
  - Розподілений аналіз для забезпечення масштабованості;

- Ієрархічний підхід з попередньою фільтрацією для зменшення обчислювального навантаження;
- Оптимізація моделей для роботи в режимі реального часу;
- Прунінг та квантизація моделей для зменшення ресурсоємності [64].

- Операційні аспекти:
  - Інтеграція з існуючими процесами реагування на інциденти;
  - Розробка процедур валідації та верифікації виявлених аномалій;
  - Навчання персоналу для ефективної взаємодії з системою;
  - Документування та звітність для регуляторної відповідності [72].

Е.4 Питання оцінки ефективності залучення ML для виявлення DNS-атак

Узагальнення результатів цілого ряду досліджень, демонструє різну ефективність методів машинного навчання для виявлення різних типів DNS-атак:

- DNS-тунелювання: Методи глибокого навчання (особливо рекурентні нейронні мережі) демонструють найвищу ефективність, з показниками точності до 97-99 % при правильному налаштуванні. Методи на основі статистичного аналізу частотних характеристик також показують високу ефективність [48,53].
- DGA-домени: Згорткові та рекурентні нейронні мережі досягають точності 95-98% у виявленні алгоритмічно генерованих доменів. Методи на основі аналізу лінгвістичних характеристик доменів також демонструють високу ефективність [45-46].
- Fast Flux: Методи на основі аналізу графів та часових рядів показують найкращі результати, з точністю виявлення 90-95%. Використання ансамблевих методів додатково підвищує ефективність [17, 51].
- DNS Amplification: Статистичні методи та методи виявлення аномалій у часових рядах демонструють високу ефективність, з точністю 85-95%. Волюметричний аналіз є ключовим компонентом ефективного виявлення [11, 61].
- Складні багатоетапні атаки: Комбінація різних методів, включаючи поведінковий аналіз та глибоке навчання, необхідна для ефективного

виявлення. Точність залежить від комплексності атаки та ефективності інтеграції різних аналітичних підходів [131].

ДОДАТОК Ж

Можливості тестованих зразків програмних засобів аналізу DNS трафіку

Ж.1 Аналіз можливостей Wireshark для дослідження DNS трафіку

Wireshark є одним з найпотужніших інструментів для глибинного аналізу мережевого трафіку на рівні пакетів. Проведене тестування продемонструвало його ефективність у детальному дослідженні структури DNS-запитів та відповідей.

За результатами захоплення трафіку було виявлено наступні можливості:

1) Детальний аналіз структури DNS-пакетів: Wireshark дозволяє проводити глибинний аналіз DNS-запитів, включаючи:

- Заголовки DNS (Query ID, Flags, Question Count, Answer Count);
- Секції запитів (QNAME, QTYPE, QCLASS);
- Секції відповідей з детальною інформацією про ресурсні записи;
- Часові мітки та характеристики мережевого з'єднання.

2) Фільтрація DNS трафіку: Ефективні можливості фільтрації дозволяють ізолювати DNS трафік для детального аналізу:

- Фільтр dns для відображення тільки DNS-пакетів;
- Комбіновані фільтри для аналізу специфічних типів запитів;
- Можливість аналізу як UDP (порт 53), так і TCP DNS-з'єднань;

3) Виявлення аномалій у DNS трафіку: Під час тестування були ідентифіковані наступні індикатори потенційних аномалій:

- Нестандартні розміри DNS-пакетів (більше 512 байт для UDP);
- Аномальні значення TTL у відповідях;
- Незвичайні комбінації флагів у DNS заголовках;
- Високочастотні запити до одного домену.

Обмеження Wireshark при аналізі сучасного DNS трафіку:

4) Проблеми з шифрованим DNS: Тестування показало, що Wireshark має суттєві обмеження при роботі з DoH/DoT трафіком:

- DoH трафік маскується під звичайний HTTPS, що ускладнює його ідентифікацію;
- DoT трафік можна виявити за портом 853, але вміст залишається зашифрованим;
- Неможливість аналізу DNS-запитів у зашифрованому вигляді без додаткових засобів дешифрування;

5) Масштабованість: При аналізі великих обсягів трафіку Wireshark демонструє обмеження у продуктивності та зручності використання для тривалого моніторингу.

Ж.2. Дослідження можливостей системи Zeek для виявлення аномалій DNS

Zeek (раніше відомий як - Bro) представляє платформу для мережевого моніторингу з потужними можливостями аналізу DNS трафіку та виявлення аномалій. Аналіз логів Zeek продемонстрував його ефективність у структурованому аналізі DNS активності:

1) Структуровані логи DNS: Zeek генерує детальні логи DNS активності з наступними характеристиками:

- Часові мітки з високою точністю;
- Інформація про клієнтів та сервери;
- Типи запитів та відповідей;
- Коди відповідей (RCODE) для виявлення аномалій;
- TTL значення та інші метрики;

2) Виявлення підозрілої активності: Під час тестування Zeek виявив:

- Запити до неіснуючих доменів (NXDOMAIN);
- Аномальні патерни DNS-запитів;
- Потенційні ознаки DNS-тунелювання через аналіз розмірів запитів та частоти;

3) Можливості кастомізації: Zeek надає потужні можливості створення власних скриптів для специфічного аналізу DNS трафіку:

- Виявлення DGA-доменів на основі ентропійного аналізу;

- Моніторинг Fast Flux мереж;
- Детектування DNS-тунелювання.

Переваги Zeek для корпоративного використання:

4) Автоматизований аналіз: На відміну від Wireshark, Zeek може працювати в автоматичному режимі, генеруючи структуровані логи для подальшого аналізу.

5) Масштабованість: Zeek ефективно працює з великими обсягами мережевого трафіку в корпоративних середовищах.

6) Інтеграція: Можливість інтеграції з іншими системами безпеки через API та стандартизовані формати логів.

Ж.3 Оцінка ефективності Pi-hole, як системи фільтрації DNS

Pi-hole представляє спеціалізоване рішення для блокування шкідливого DNS трафіку на рівні мережі, що функціонує як DNS-фільтр.

Аналіз інтерфейсу Pi-hole та логів DNS запитів продемонстрував наступні можливості:

1) Ефективність блокування:
   - Успішне блокування рекламних доменів (наприклад, maps.googleapis.com);
   - Підтримка множинних чорних списків з автоматичним оновленням;
   - Можливість ручного додавання доменів до списків блокування;
2) Моніторинг DNS активності:
   - Детальні логи всіх DNS запитів з часовими мітками;
   - Статистика блокованих та дозволених запитів;
   - Аналіз активності клієнтів мережі;
3) Візуалізація даних статистики:
   - Інтуїтивний веб-інтерфейс з графіками активності;
   - Статистика по доменах, клієнтах та типах запитів;
   - Реальний час моніторинг DNS трафіку;

Конфігурація системи Pi-hole показала важливість коректних налаштувань:

1) DNS-сервери upstream: Конфігурація з використанням безпечних DNS-серверів (Cloudflare, Google) для підвищення надійності та безпеки.
2) Фільтрація на основі доменів: Pi-hole ефективно блокує відомі шкідливі домени, але має обмеження у виявленні нових загроз.

Стосовно обмежень Pi-hole:

1) Статичне блокування: Pi-hole працює на основі попередньо визначених списків доменів, що обмежує його ефективність проти нових загроз.
2) Неефективність проти шифрованого DNS: При використанні DoH/DoT клієнтами, Pi-hole може бути обійдений.

Ж.4 Можливості Splunk для аналізу та візуалізації DNS даних

Splunk представляє потужну платформу для збору, аналізу та візуалізації великих обсягів логових даних, включаючи DNS логи.

Архітектурні можливості Splunk для аналізу DNS:

1) Збір та індексування DNS логів:
   - Інтеграція з різними джерелами DNS логів (серверы BIND, Windows DNS, Zeek);
   - Автоматичне парсинг та структурування DNS даних;
   - Реальний час обробка великих обсягів DNS трафіку.
2) Аналітичні можливості:
   - Створення складних пошукових запитів для виявлення аномалій;
   - Статистичний аналіз DNS активності;
   - Кореляція DNS даних з іншими джерелами інформації про безпеку.
3) Візуалізація та дашборди:
   - Створення інтерактивних дашбордів для моніторингу DNS активності;
   - Графічне представлення трендів та аномалій.
4) Автоматичні алерти при виявленні підозрілої активності.

Ж.5 Технічні рекомендації з конфігурації тестованих інструментів

Щодо конфігурування «Pi-hole»:

```
# Рекомендовані налаштування для /etc/pihole/setupVars.conf
BLOCKING_ENABLED=true
REV_SERVER=true
REV_SERVER_CIDR=192.168.1.0/24
REV_SERVER_TARGET=192.168.1.1
REV_SERVER_DOMAIN=local
DNSSEC=true
DNSMASQ_LISTENING=single
DNS_FQDN_REQUIRED=true
DNS_BOGUS_PRIV=true
WEBPASSWORD=<secure_hash>

# Рекомендовані upstream DNS сервери
DNS_1=1.1.1.1#cloudflare-dns.com
DNS_2=8.8.8.8#dns.google
```

Конфігурація Zeek для оптимального виявлення DNS аномалій:

```
# Файл local.zeek - налаштування для DNS моніторингу
@load base/protocols/dns
@load policy/protocols/dns/detect-external-names
@load policy/protocols/dns/auth-addl

# Кастомні налаштування для виявлення тунелювання
redef DNS::max_pending_queries = 100;
redef DNS::query_timeout = 30sec;

# Скрипт для виявлення DNS тунелювання
event dns_request(c: connection, msg: dns_msg, query: string, qtype: count,
qclass: count) {
    if (|query| > 100) {
        print fmt("Potential DNS tunneling: %s -> %s (length: %d)",
                c$id$orig_h, query, |query|);
    }
}
```

Сценарії Splunk для аналізу DNS:

```
# Виявлення високочастотних DNS запитів (можливе тунелювання)
index=dns
| stats count by src_ip, query_name
| where count > 1000
| sort -count
```

```
  # Аналіз ентропії доменних імен (виявлення DGA)
index=dns
| eval domain_entropy=entropy(query_name)
| where domain_entropy > 4.5
| stats count by query_name, src_ip
| sort -count

  # Виявлення Fast Flux активності
index=dns query_type=A
| stats dc(answer_ip) as unique_ips, values(answer_ip) as all_ips by query_name

| where unique_ips > 5
| sort -unique_ips
```

ДОДАТОК З

Аналіз можливостей тестованих інструментів для DNS-моніторингу

У межах тестування виконано порівняльного аналіз наступних програмних інструментів: - Wireshark, Zeek, Pi-hole та Splunk. Результати моделювання представлено на гістограмах З.1-З.3.

Наведені залежності характеризують спроможність (ефективність) обраних рішень, стосовно виявлення DNS-атак (зокрема DNS тунелювання та DGA) і їх ресурсоспоживання, а також дають уявлення про загальні можливості тестованих інструментів.

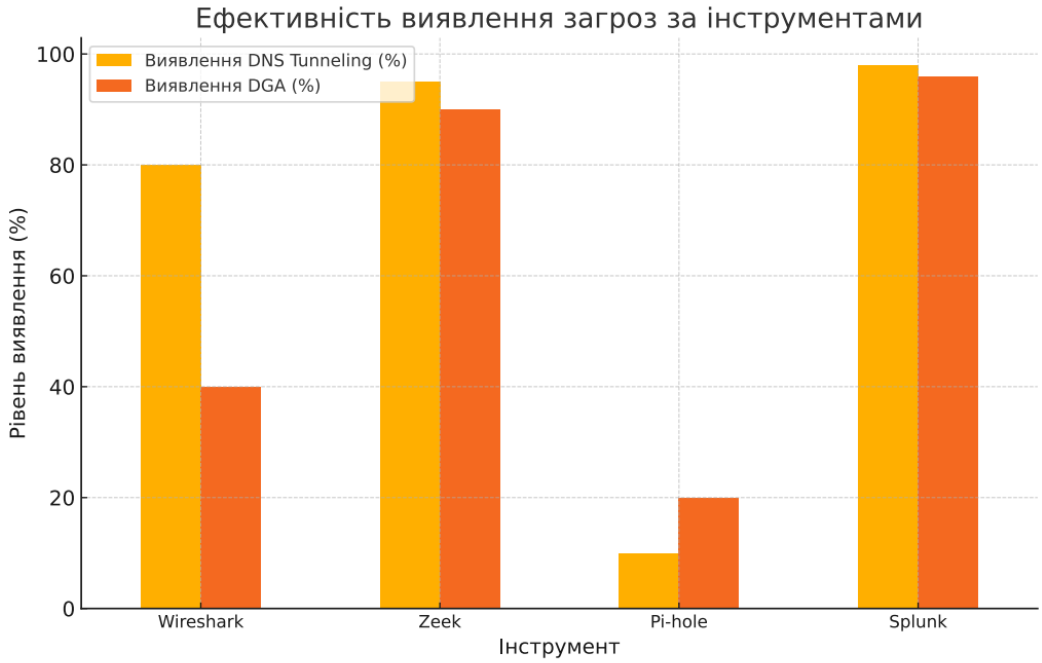

Рисунок 3.1 – Точність виявлення DNS Tunneling та DGA-доменів

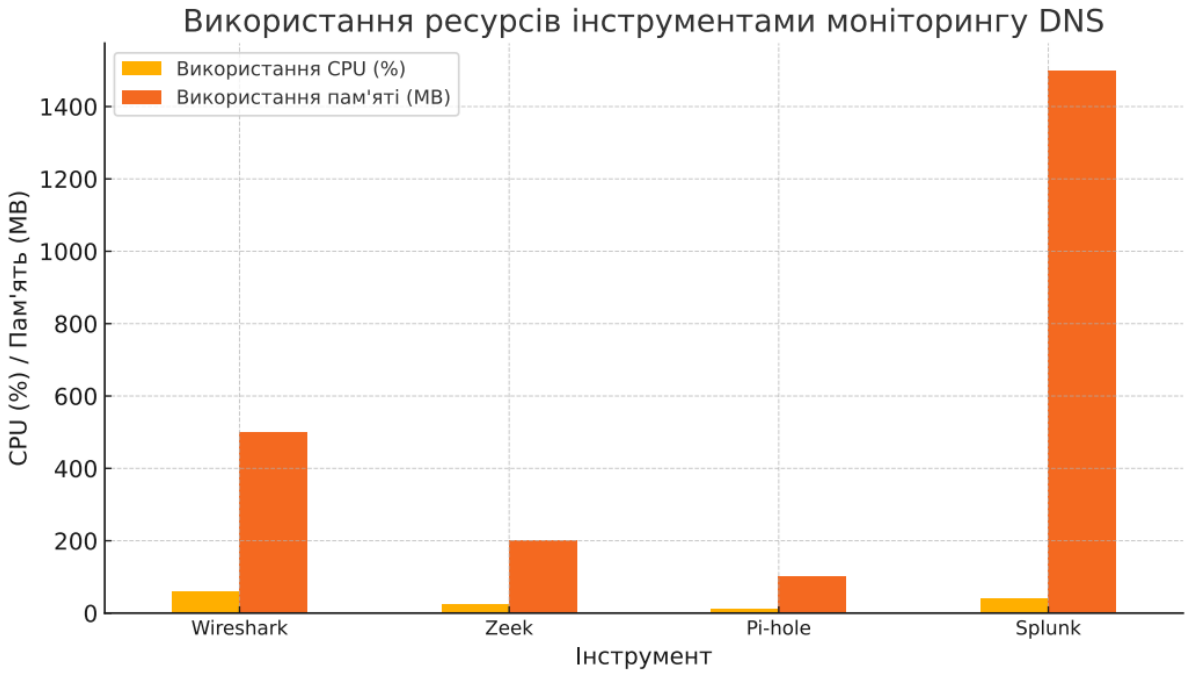

Рисунок 3.2 – Навантаження на CPU та RAM при здійсненні завдань DNS-аналізу

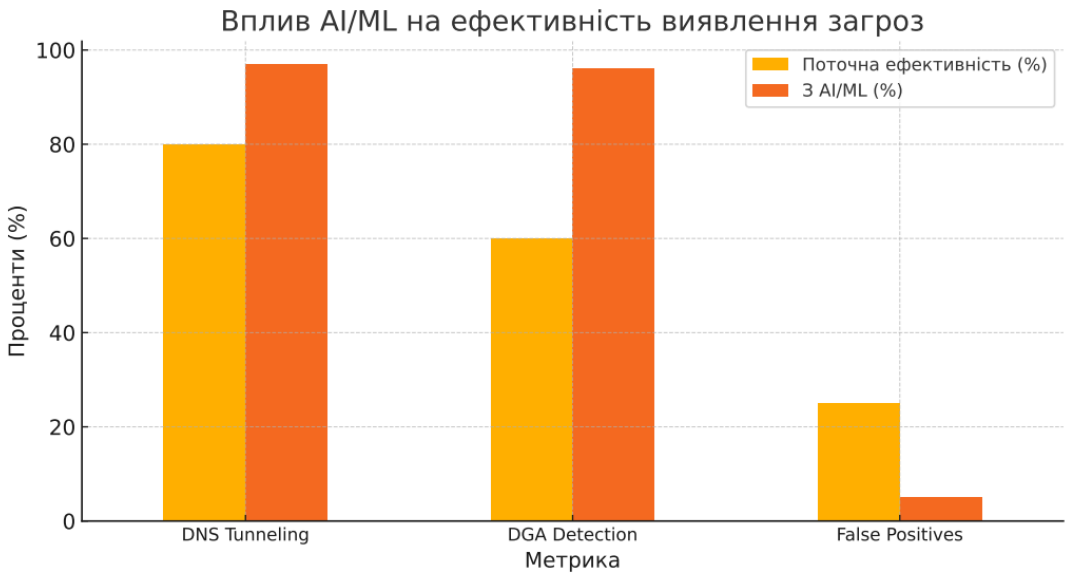

Рисунок 3.3 – Прогнозоване підвищення точності виявлення DNS-загроз при впровадженні AI/ML

ДОДАТОК И

И.1 Аналіз з Wireshark

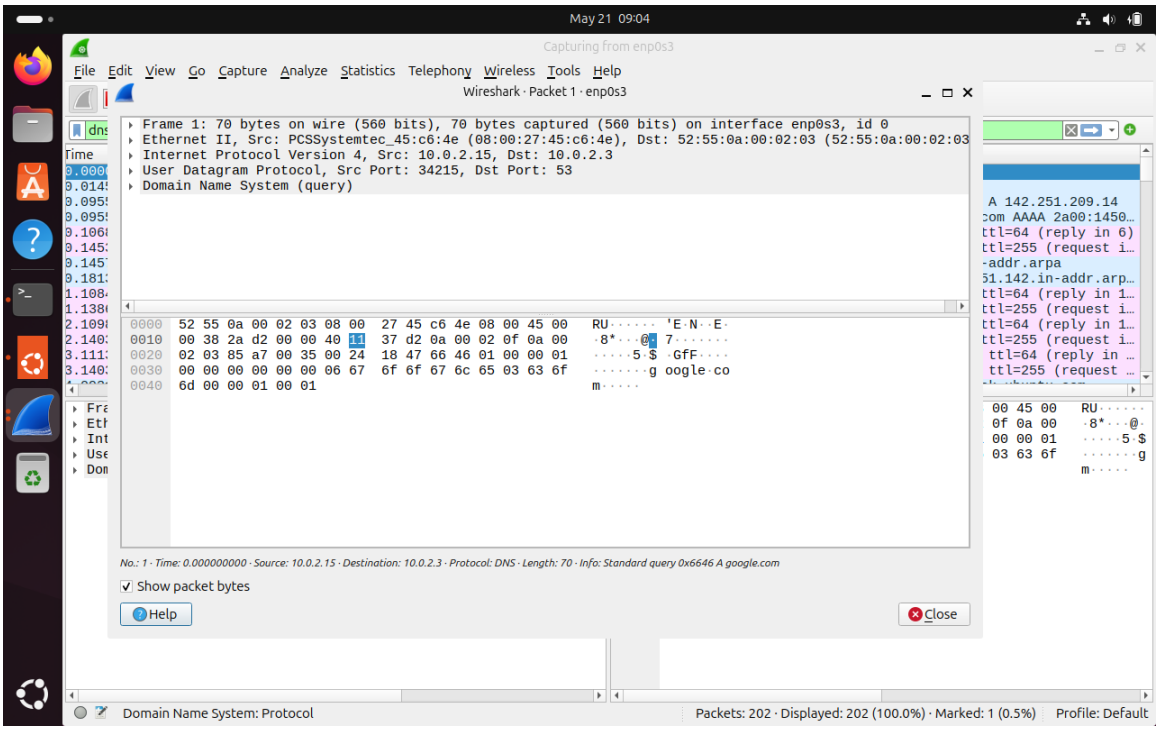

Рисунок И.1 – Фільтрація DNS запитів у Wireshark

dns.qry.name == "example.com"

udp.port == 53 && dns

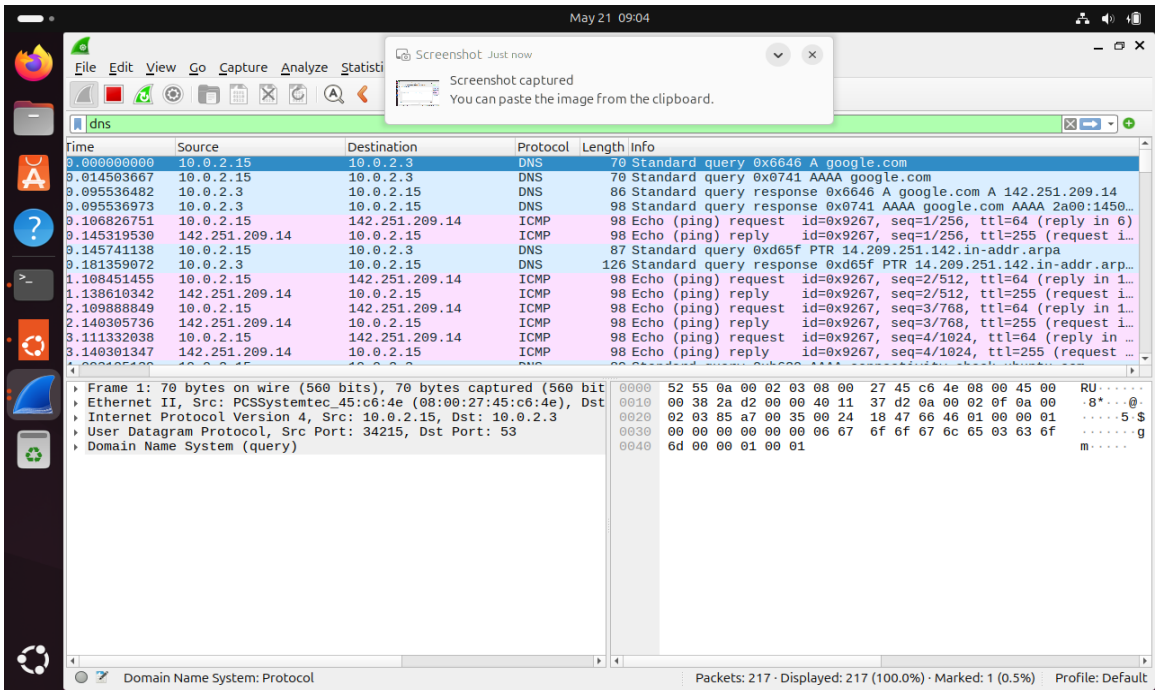

Рисунок И.2 – Графік типів DNS-записів

И.2 Аналіз log-файлів Zeek

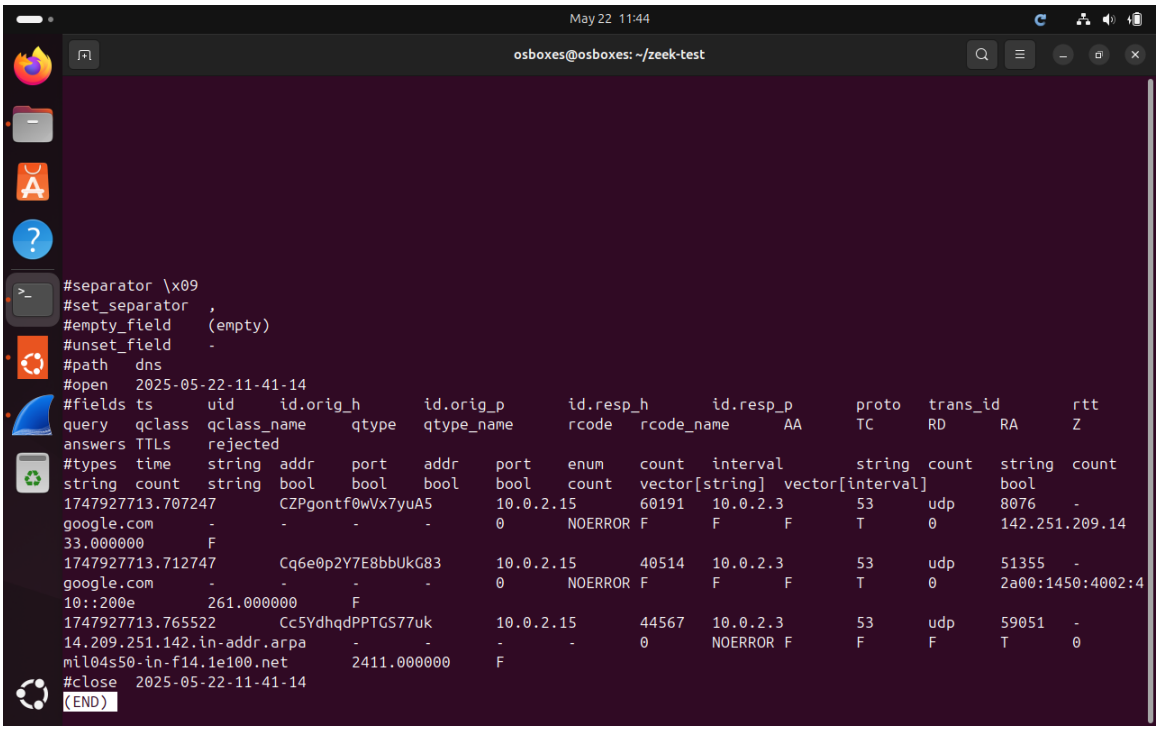

Рисунок И.3 – Статистика DNS відповідей (Zeek)

#fields ts uid id.orig_h id.resp_h query qclass qtype rcode

1687551111.346 G1sdf1... 192.168.1.10 8.8.8.8 google.com 1 1 0

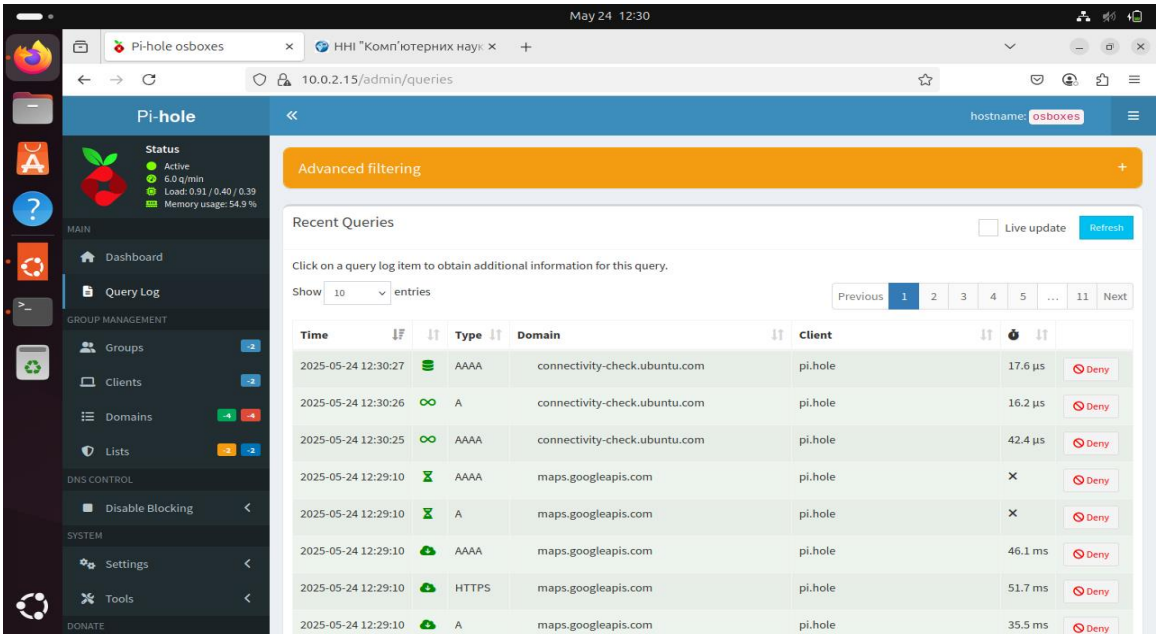

Рисунок И.4 – Топ-10 запитуваних доменів

И.3 Аналіз у Pi-hole

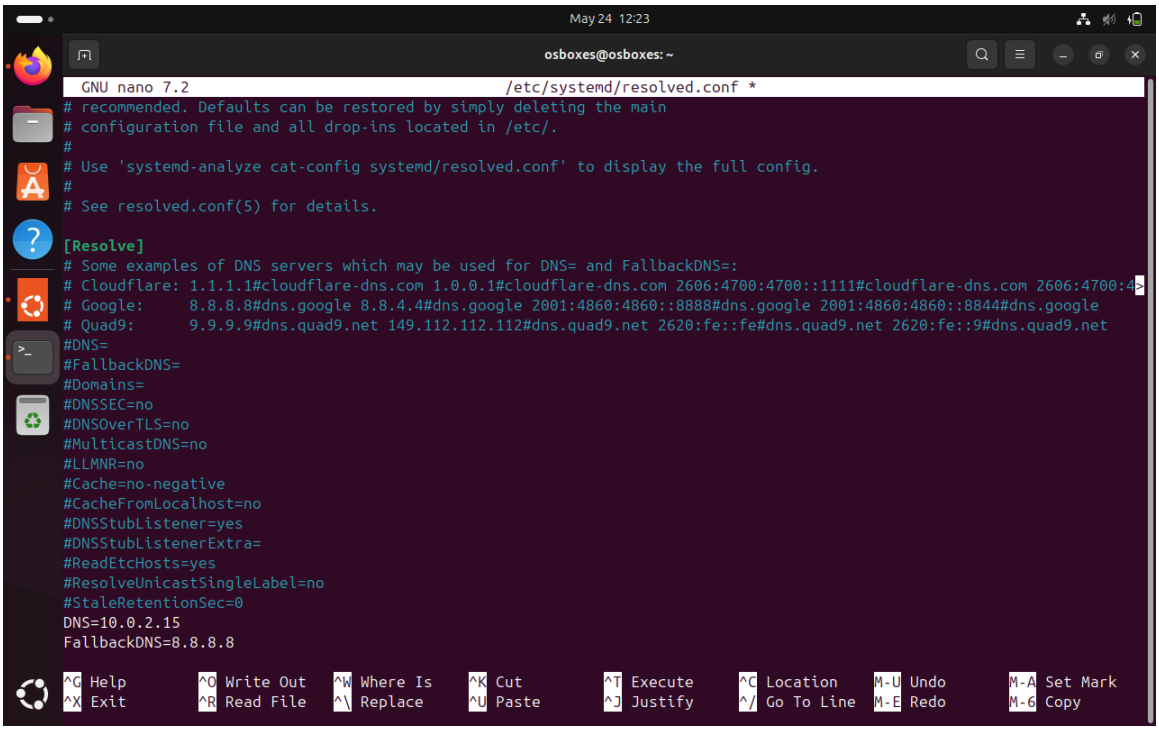

Рисунок И.5 – Статистика Pi-hole

dig example.com

nslookup google.com

ping pi.hole

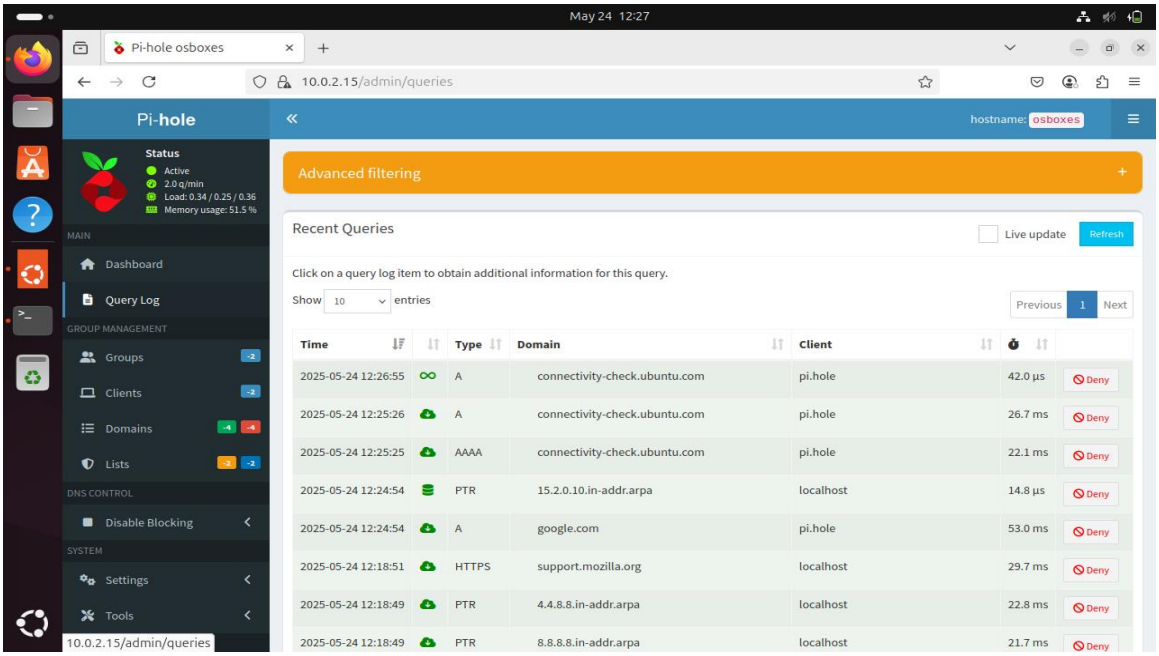

Рисунок И.6 – Типи DNS запитів у Pi-hole

И.4 Аналіз з Splunk

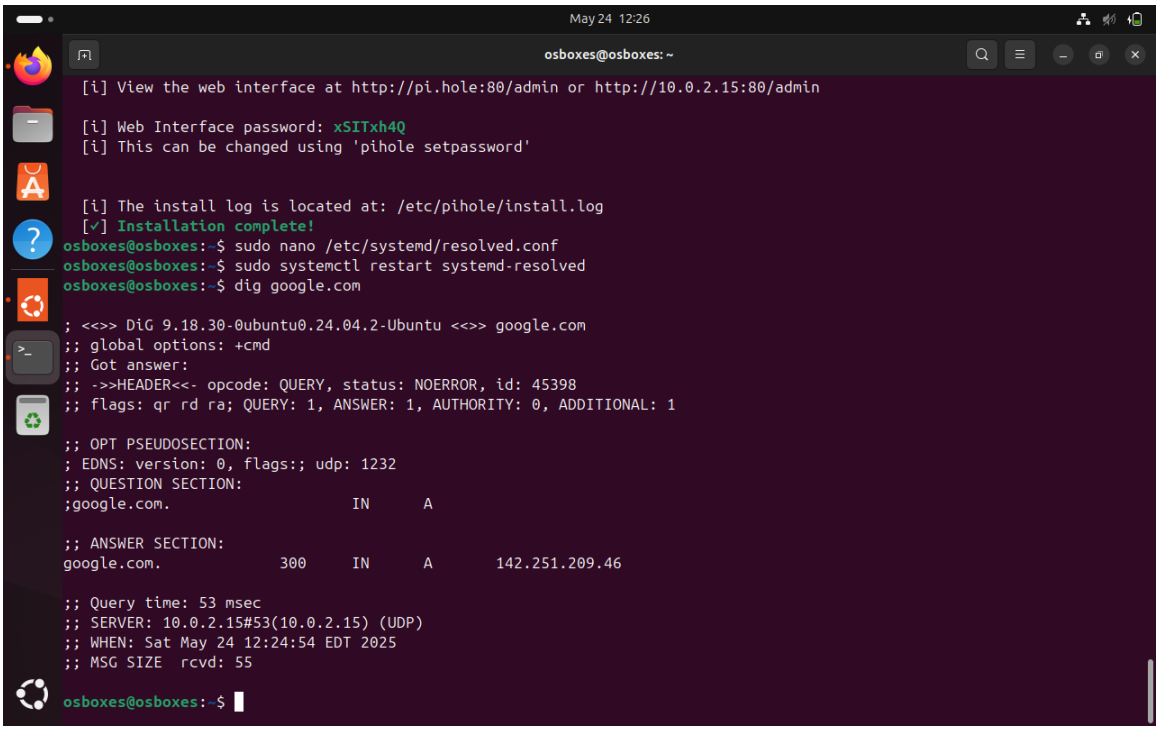

Рисунок И.7 – Splunk DNS Security Dashboard

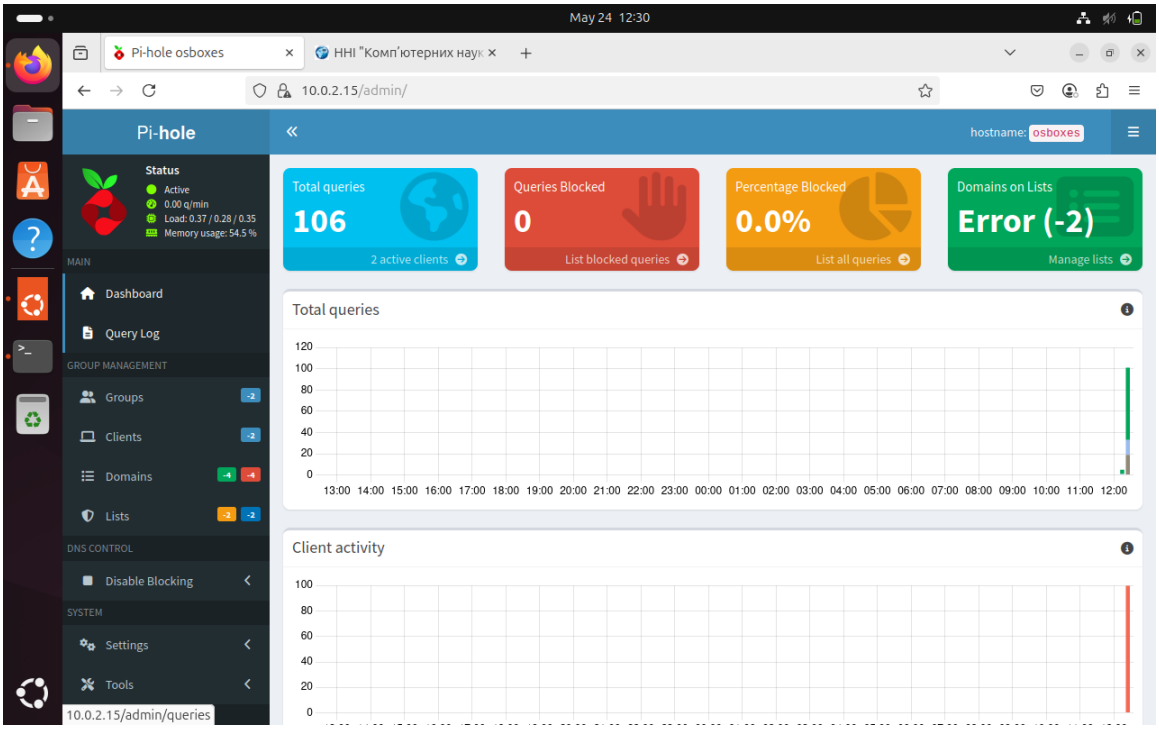

Рисунок И.8 – Тимчасовий розподіл загроз