DOI 10.36074/logos-24.01.2025.049

МУЛЬТИПРОТОКОЛЬНИЙ МОНІТОРИНГ ТРАФІКУ DNS, ЯК ОСНОВА ДЛЯ КОРИГУВАННЯ ПОТОЧНИХ ПАРАМЕТРІВ RPZ

Чепель Данило Олександрович[1], Малахов Сергій Віталійович[2]

1. студент навчально-наукового інституту комп'ютерних наук
та штучного інтелекту(*магістратура*)
Харківський національний університет імені В.Н. Каразіна, УКРАЇНА
ORCID ID: 0009-0009-7449-8095

2. канд. техн. наук, ст. науковий співробітник, доцент кафедри
Харківський національний університет імені В.Н. Каразіна, УКРАЇНА
ORCID ID: 0000-0001-8826-1616

Вступ. Представлений матеріал є частиною загального циклу досліджень, що сфокусовані на покращенні параметрів захисту сучасних інформаційних систем за рахунок вдосконалення підсистеми моніторингу та аналізу DNS (*Domain Name System*) запитів для оперативної корекції поточних параметрів зон політик реагування (*RPZ, Response Policy Zone*) та завчасного виявлення аномалій DNS трафіку, що можуть становити серйозну загрозу безпеки [1-3].

Головною метою роботи є стисле ознайомлення з результатами тестових вимірів прототипу програмного засобу моніторингу і оцінки доступності визначеної хмари DNS серверів, як засобу виявлення можливих аномалій DNS трафіку для різних типів відповідних протоколів *(*зокрема *DNS-over-TLS (DoT)* та *DNS-over-HTTPS (DoH))*. Діючий прототип додатку дозволяє проводити децентралізований (*Multi Base*) і монорежимний (*Single Base*) збір, обробку, зберігання і відображення відомостей, стосовно поточних параметрів часових затримок DNS-запитів в умовах використання різних типів протоколів для визначеного (контрольованого) переліку доменних зон.

Основна частина. Головна парадигма проведеного моделювання мала на меті створення зручного й гнучкого програмного інструменту тестування і аналізу поточного стану визначеної хмари *DNS* серверів для вирішення декількох завдань інформаційної безпеки (ІБ), зокрема: – моніторинг доступності визначеного пулу DNS серверів; – оцінка часу реакції серверів для

різних типів протоколів шифрування DNS запитів; – парирування певних наслідків шифрування DNS трафіку (насамперед для *DoT* та *DoH*); – завчасне виявлення ознак роботи алгоритмів генерації доменів (*DGA, Domain Generation Algorithm*) [2-3]. В якості зворотних реакцій проведених тестових вимірювань виступає процес корегування поточних параметрів зон політик реагування – *RPZ* [1]. Діюча модель тестового прототипу додатку поєднує локальні обчислення та розподілені хмарні функції, що, в цілому, забезпечує потрібну точність вимірювань (часу реакції) і широку локацію охоплення, як з точки зору безпосереднього розміщення хмарних програмних датчиків вимірювань, так і з точки зору вибору об'єктів спостереження, тобто контрольованого пулу *DNS* серверів. Спрощена схема (*Single Base Release*) загальної концепції проведеного моделювання, представлена на рис. 1.

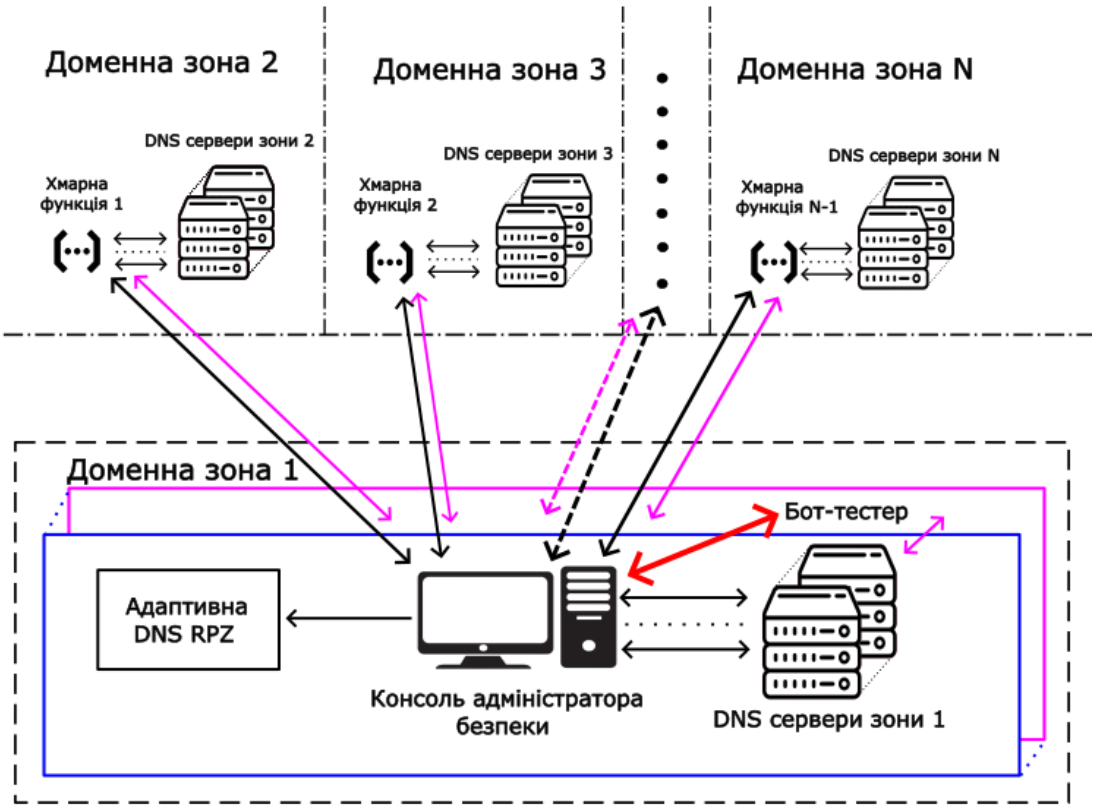

Рис. 1. **Візуалізація моделювання в режимі «*Single Base*»**
(авторська розробка)
(червона стрілка, це канал управління «консоль адміну – бот-тестер»)

В рамках тестового випробування було виконано 10 серій вимірювань протягом п'яти днів. Вимірювання проводилися двічі на добу, орієнтовно о

18:00 та 00:00 (за київським часом). Для тестування було обрано наступні DNS сервери разом із відповідними резервними серверами: – *Google; – Control D; – Cloudflare; – OpenDNS; – Quad9*. Прототип програми реалізований на мові програмування *Java* з використанням технології *Cloud Run functions* від *Google*.

Тестові DNS запити (*структура і зміст запитів не є предметом розгляду даного матеріалу*), включали домени, що розташовані у різних доменних зонах (див. рис.1). В даному разі це: – about.us - США; – globo.com.br - Бразилія; – gov.za - ПАР; – bbc.com.uk – Велика Британія; – work.ua - Україна; – post.japanpost.jp - Японія; – news.com.au - Австралія. Крім того, для спрощення циклів тестових вимірів, були встановлені наступні технологічні затримки: – між серверами однієї пари (*основний-резервний*) – 5 секунд; – між запитами за різними протоколами – 10 хв.

Прототип тестового додатку підтвердив працездатність загальної ідеї моніторингу *DNS* серверів. Наприклад в період вимірів вдалося зафіксувати певні аномалії в роботі серверів *Cloudflare.* Хоча сервери цього сервісу можуть демонструвати дуже малі часи затримок, вони схильні до різких збільшень затримки часу, особливо під час обробки запитів до доменів, які відносяться до умовно «віддалених» (*по відношенню до консолі*) доменних зон (табл. 1).

Таблиця 1

Фрагмент даних тестувань для серверів *Cloudflare*

Назва серверу	Домен	Час (*без шифр.*)	Час *DoH*	Час *DoT*
Cloudflare	*bbc.co.uk*	*20*	*33*	*82*
Cloudflare (*Reserve)*	*bbc.co.uk*	*20*	*40*	*82*
Cloudflare	*work.ua*	*11*	*44*	*80*
Cloudflare (*Reserve)*	*work.ua*	*49*	*43*	*83*
Cloudflare	*post.japanpost.jp*	*945*	*648*	*122*
Cloudflare (*Reserve)*	*post.japanpost.jp*	*137*	*87*	*83*

Через ці збільшення затримок середній час затримки *Cloudflare* є набагато більшим, ніж очікувалося. Наприклад, запит до резервного серверу Cloudflare (*у регіоні США*), щодо домену *globo.com.br,* ввечері 19 листопада, склав 10425 мс. На рис.2-3 приведено середній час затримки основних та резервних серверів *Cloudflare* та *Google,* відповідно (*у регіоні США*).

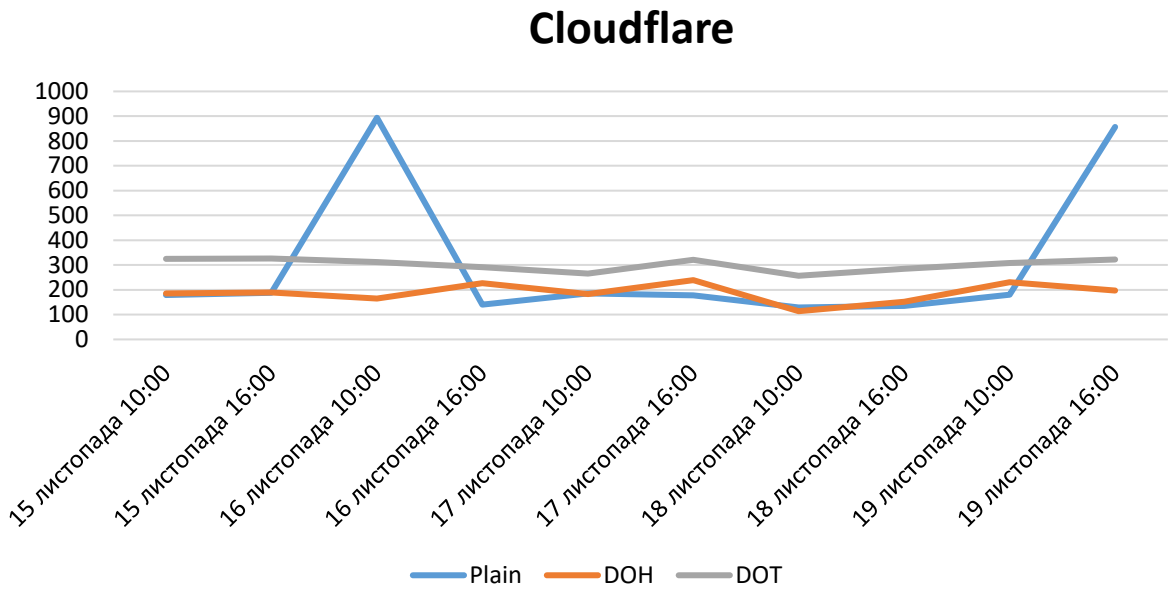

Рис. 2. **Середній час** (ms) **затримки для серверів *Cloudflare*** *(на 19.11.24)*

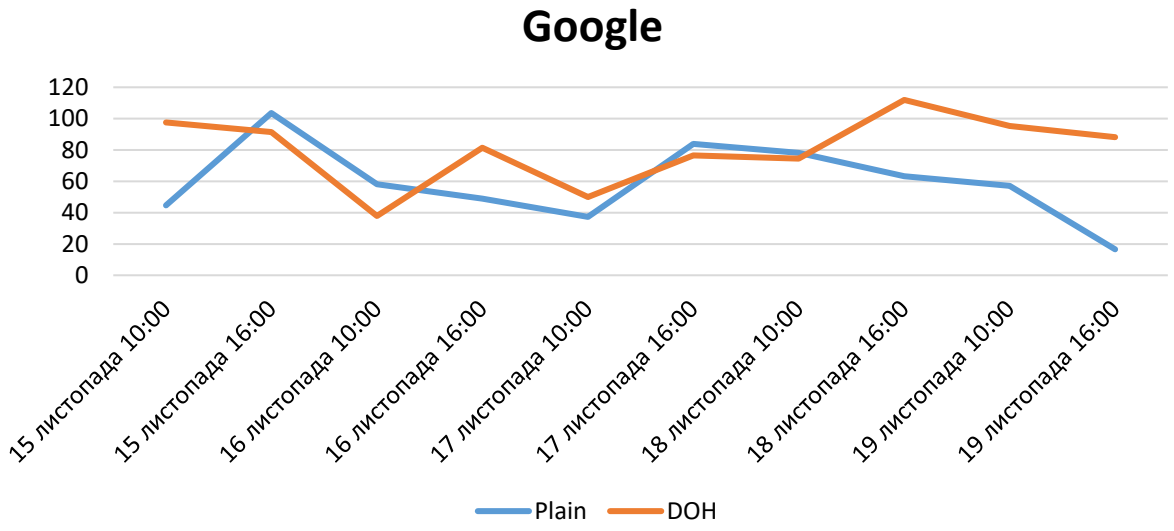

Рис. 3. **Середній час** (ms) **затримки для визначеної пари серверів *Google*** *(на 19.11.24)*

Висновки.

1. Досліджено прототип дослідної програми, яка дозволяє здійснювати поточний моніторинг доступності заданої хмари DNS серверів і часові затримки для трьох типів протоколів (незашифровані, DoH, DoT). Тестовий

додаток забезпечує обробку, збереження і візуалізацію результатів, що полегшує задачу аналізу стану DNS у різних доменних зонах.

2. Розглянуті результати тестових випробувань надані у версії вимірів «*Single Base Release*». Повна реалізація розподіленої структури вимірювань та можливість автоматизації процесу формування і порядку застосування різних тестових сигнатур, значно посилить інформативність процесу, що моделюється.

3. Результати досліджень мають на меті процес оптимізації налаштувань корпоративної DNS інфраструктури *(в частині адміністрування діючих політик RPZ*), вибору оптимальних за часом і локацією серверів та сприяння виконання завдань, стосовно виявлення аномалій і збоїв у роботі DNS сервісів.

4. Перспективами подальших досліджень є: - удосконалення користувацького інтерфейсу тестового додатку; - впровадження режиму мультибазових (*Multi Base*) хмарних вимірювань; - створення інструментів для автоматичного синтезу вимірювальних сигнатур і узагальнення отриманих даних за рахунок залучення можливостей технології штучного інтелекту.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

[1] Чепель, Д., Малахов, С., & Колованова, Є. (2024). Огляд можливостей фільтрації DNS, як інструмента безпеки сучасних інформаційних систем. *Grail of Science*, (42), 395–398. https://doi.org/10.36074/grail-of-science.02.08.2024.055

[2] Данило Чепель, & Сергій Малахов. (2024). Узагальнення напрямів фільтрації DNS трафіку як складової безпеки сучасних інформаційних систем. *Комп'ютерні науки та кібербезпека*, (1), 6-21. https://doi.org/10.26565/2519-2310-2024-1-01

[3] Коробейнікова, Т., & Федчук, Т. (2024). Огляд протоколів DNS, DOH та DOT. Збірник наукових праць «ΛΌГОΣ», (March 1, 2024; Paris, France), 253–256. https://doi.org/10.36074/logos-01.03.2024.056