DOI: https://doi.org/10.26565/2304-6201-2026-69-09

УДК (UDC) 004.056.5

Чепель Данило Олександрович
аспірант
кафедри кібербезпеки інформаційних систем, мереж і технологій, Харківський національний університет імені В. Н. Каразіна, майдан Свободи, 4, Харків, Україна, 61022;
e-mail: dan4epel@gmail.com
https://orcid.org/0009-0009-7449-8095

Малахов Сергій Віталійович
кандидат технічних наук, доцент
кафедри кібербезпеки інформаційних систем, мереж і технологій, Харківський національний університет імені В. Н. Каразіна, майдан Свободи, 4, Харків, Україна, 61022;
e-mail: malakhov@karazin.ua
https://orcid.org/0000-0001-8826-1616

Гончаров Микита Олександрович
аспірант
кафедри кібербезпеки інформаційних систем, мереж і технологій, Харківський національний університет імені В. Н. Каразіна, майдан Свободи, 4, Харків, Україна, 61022;
e-mail: m.honcharov@student.karazin.ua
https://orcid.org/0000-0002-9790-7260

Застосування парадигми прецедентного аналізу для цілей мультибазового хмарного моніторингу DNS-трафіку

Актуальність. Зростання складності DNS-інфраструктури та підвищення рівня загроз у мережевому середовищі зумовлюють необхідність розроблення інтелектуальних засобів моніторингу DNS-трафіку, здатних забезпечувати прозоре, адаптивне та обґрунтоване виявлення поведінкових аномалій. Особливої актуальності набуває впровадження підходів, що підвищують простежуваність логіки прийняття рішень системами штучного інтелекту.
Мета. Метою роботи є експериментальне дослідження прототипу програмного засобу для моніторингу поточного стану DNS-трафіку з широкою імплементацією можливостей ШІ, в основу логіки якого покладено концепцію прецедентного аналізу (CBR) поведінкових аномалій DNS-трафіку.
Методи дослідження. У роботі використано методи імітаційного моделювання, мультибазові вимірювання часу обробки DNS-запитів із застосуванням системи розподілених хмарних датчиків-тестерів, а також алгоритми прецедентного аналізу для інтелектуальної постобробки даних. Прототип реалізовано у вигляді Python-клієнта, інтегрованого з Gemini API, що функціонує на основі набору даних, сформованого за результатами попередніх досліджень [1-2]. У процесі роботи система автономно модифікує реєстр аномалій шляхом додавання нових прецедентів на основі результатів аналітичної обробки.
Результати. Отримані результати демонструють, що розглянутий підхід для моніторингу DNS-трафіку забезпечує виявлення як уже відомих аномалій, так і локалізацію ще невідомих колізій. Підтверджено перспективність застосування прецедентного підходу для покращення оперативності корегувань параметрів діючої зони політики реагування (RPZ) [3] та підвищення рівня поінформованості персоналу з питань безпеки DNS-трафіку. Водночас експерименти виявили ефект т. зв. «кластеризації», що може призводити до хибнопозитивних результатів оцінки подій та, як наслідок, суперечливих трактувань отриманих відомостей щодо спостережуваних мережевих подій.
Висновки. Перегляд діючих обмежень та завдань аналізу для модулів ШІ і подальше моделювання підтвердили, що внесені зміни суттєвим чином зменшили виявлений ефект «кластеризації» та підвищили надійність інтерпретацій аномалій, які спостерігаються за визначеною системою непрямих (опосередкованих) ознак. Отримані результати підтверджують доцільність подальшого розвитку підходу прецедентного аналізу в системах інтелектуального моніторингу DNS-трафіку.

Ключові слова: *інформаційна безпека, штучний інтелект, фільтрація трафіку, DNS, RPZ, CBR, мережеві аномалії, хмарні обчислення, розподілена мережа, протоколи DNS.*

Як цитувати: Чепель Д. О., Малахов С. В., Гончаров М. О. Застосування парадигми прецедентного аналізу для цілеймультибазового хмарного моніторингу DNS-трафіку. *Вісник Харківського національного університету імені В. Н. Каразіна, серія Математичне моделювання. Інформаційні технології. Автоматизовані системи управління*. 2026. вип. 69. С.111-121. https://doi.org/10.26565/2304-6201-2026-69-09
How to quote: D. Chepel, S. Malakhov and M. Honcharov, "Application of a preceden tanalysis paradigm for the purposes of multibase cloud monitoring of DNS traffic", *Bulletin of V. N. Karazin Kharkiv National University, series Mathematical modelling. Information technology. Automated control systems*, vol. 69, pp. 111-121, 2026. https://doi.org/10.26565/2304-6201-2026-69-09 [in Ukrainian]

1. Вступ

Науково-технічний прогрес у галузі інформаційних технологій сприяє безперервний розробці та впровадженню нових інформаційно-комунікаційних систем (ІКС) і технологій, але водночас, породжує й нові загрози безпеки, зокрема ті, що базуються на використанні DNS-орієнтованих векторів кібератак, такі як атаки DNS-ампліфікації, отруєння кешу резолверів та інші. За таких умов традиційні підходи до аналізу властивостей DNS-трафіку, виявляють досить серйозні функціональні обмеження. До таких умовно «сірих зон» можна віднести: – моніторинг зашифрованого чи обфускованого DNS трафіку; – спорадична динамічна зміна доменів (з боку зловмисників); – нерівномірність мережевих потоків; – робота в умовах впливу атак типу DNS Amplification тощо. Представлена робота є логічним продовженням цілої низки досліджень [1-3], спрямованих на вдосконалення можливостей (*перш за все, швидкість та інформативність*) хмарної мультибазової системи моніторингу поточного стану DNS-трафіку в заданих мережевих локаціях (доменних зонах). Основна увага зосереджена, насамперед, на оцінці застосовності парадигми прецедентного аналізу структури й властивостей поточного DNS трафіку з широким залученням можливостей ШІ. Попередньо, було зроблено припущення, що використання цього підходу може самим суттєвим чином підвищити обґрунтованість і оперативність коригування поточних параметрів зон політики реагування (*Response Policy Zones, RPZ*) та забезпечити своєчасне виявлення аномалій DNS-трафіку, що пов'язані з першими проявами загроз безпеки [1–4], котрі експлуатують вектор DNS. Під терміном «обґрунтованість», слід розуміти покращення ступеню поінформованості персоналу з питань ІБ про актуальний стан мережевих інцидентів, що експлуатують вектор DNS атак, через комплексність результатів аналізу даних моніторингу, в заданих мережевих сегментах (локаціях). Як вказано у роботах [1-2], цей процес відбувається, перш за все, шляхом глибокої інтеграції системи розгалужених програмних датчиків-сенсорів (див. Рис.1 в роботі [1]) й можливостей технології ШІ.

Основна ідея парадигми прецедентного аналізу полягає у формуванні і підтриманні в актуальному стані масиву формалізованих даних (*т.з. поведінкових шаблонів*) про типову активність DNS трафіку, котрі використовуються для інтерпретації поточних станів DNS трафіку у відповідності до інформації наявної бази знань (прецедентів). Впровадження такого механізму дій потребує перегляду структури раніше запропонованого тестового алгоритму [1-2], а також модифікації модулів збору та попередньої обробки даних. Реалізація вказаних змін забезпечує потрібні умови для коректного формування, зберігання та подальшого використання отриманих відомостей про прецеденти (колізії, аномалії, інциденти тощо). Проведене комп'ютерне моделювання підтвердило доцільність інтеграції механізмів прецедентного аналізу до структури хмарної системи моніторингу DNS трафіку та підтвердило її здатність фіксувати та обробляти широкий спектр поведінкових аномалій DNS-трафіку.

Мета роботи полягає в розгляді й узагальнені результатів тестового моделювання оновленого механізму прецедентного аналізу поточних даних DNS-трафіку, з застосуванням системи хмарних мультибазових вимірів. Оновлена концепція моніторингу DNS трафіку (доопрацьований алгоритм + нові елементи): - забезпечує комплексний характер відомостей, стосовно поточних мережевих подій (*в частині DNS трафіку*); - зменшує час реагування на інциденти безпеки, які експлуатують вектор DNS атак; - покращує валідність результатів аналізу поведінкових аномалій DNS-трафіку у визначених сегментах глобальної мережі.

2. Аналіз останніх досліджень і публікацій

Моніторинг DNS-трафіку є важливою складовою в загальної системі забезпечення безпеки сучасних ІКС. Своєчасне та точне виявлення аномалій DNS-трафіку дає змогу зменшити потенційну шкоду від загроз, що базуються на експлуатації DNS векторів атак, а також підвищити загальну адекватність адміністрування діючими RPZ [1-3]. Особливості питань аналізу каналів розвідки загроз (*Threat Intelligence Feeds*), механізмів корегування *RPZ* та методів протидії ботнет активності й шифрування DNS-трафіку, коротко розглянуті в [1]. Спираючись на результати аналізу останніх тенденцій, які пов'язані з застосуванням ШІ для цілей моніторингу і фільтрації DNS-трафіку, слід виділити кілька напрямів досліджень, що є релевантними для умов та завдань цієї роботи [5-12]:

2.1 Штучний інтелект в проблематиці аналізу даних

Інтелектуальні системи дають змогу автоматизовано отримувати структуровані знання з великих за обсягами та різнорідних джерел даних, перевершуючи традиційні - статистичні підходи за критеріями масштабованості й адаптивністю цих процесів. Помітною рисою сучасних профільних публікацій є, тренд на інтеграцію методів машинного навчання (ML), логіко-орієнтованих підходів та оптимізаційних методів/способів, як ключових елементів сучасних технологій аналізу даних (*в широкому сенсі цієї проблематики*). В цьому контексті, глибинне навчання визначається, як домінуюча аналітична парадигма. У літературі також, відзначаються певні успіхи в детектуванні й розпізнаванні зображень, стеганографії, обробці сигналів та виявленні мережевих аномалій, досягнуті нейронними мережами [6]. Водночас, попри високу точність прогнозування, глибинне навчання пов’язане з низкою обмежень, зокрема: – значними вимогами до обсягів даних, високою обчислювальною вартістю та низьким рівнем «прозорості» (*тобто, очевидності існуючих та/чи врахованих взаємозв'язків*). Це стимулює розвиток підходів, що поєднують доменно-орієнтовані знання, символічні методи та механізми переносу навчання з метою підвищення їх прикладної застосовності і прозорості систем ШІ. Крім того підкреслюється необхідність перевірки (валідації) відомостей, що згенеровано с залученням ШІ [6]. Загалом результати сучасних досліджень свідчать, що ШІ не лише підвищує ефективність та точність результатів аналізу різнорідних даних, але й трансформує самі підходи до механізмів реалізації та змісту процесів аналітики. В першу чергу це стосується зміщення уваги в бік синтезу інтегрованих інтелектуальних систем, котрі здатні оперативно обробляти складні мультимодальні дані в реальному масштабі часу. Попри швидкий прогрес, залишаються актуальними виклики, пов’язані з прозорістю моделей, необхідністю перевірки результатів та обчислювальними витратами [5-7].

2.2 Штучний інтелект в реаліях умов аналізу DNS-трафіку.

Сучасні фахівці з ІБ відзначають посилення тенденції на використання ШІ для завдань аналізу DNS-трафіку. Основною причиною є зниження ефективності традиційних сигнатурних (реактивних) підходів, які є малорезультативними в умовах інтенсивної обфускації каналів, швидкої зміни доменів та впровадження складних стратегій ухилення від виявлення. Дослідження показують, що моделі машинного навчання здатні виявляти аномалії мережевої поведінки навіть тоді, коли важливі інформативні ознаки приховані технологіями шифрування або навмисно маскуються [13-14]. Наголошується, що методи на основі ШІ забезпечують не лише вищу точність класифікації, але й здатність адаптуватися до нових умов та типів атак. Водночас проблема прозорості загальної логіки дій з боку ШІ, залишається вкрай актуальною. Вочевидь, що інтеграція функцій ШІ у реальні системи ІБ є неможливою без впровадження механізмів формалізованих інтерпретацій (пояснювання), стосовно змісту й логіки штучно синтезованих відомостей. Такий порядок валідації дій ШІ, дозволяє персоналу з безпеки зрозуміти, чому той чи інший запит, потік або процес було кваліфіковано, як підозрілий/аномальний. Ця потреба безпосередньо пов’язана з поняттям «довіри», можливістю аудиту прийнятих рішень і практичною придатністю таких систем у реальних умовах. Інакше кажучи, автоматизація процесів прийняття рішень з боку ШІ має гармонійно поєднуватися з процесом їх контролю. Це особливо важливо, в рамках потенційно неминучого зіткнення можливостей ШІ на боці протиборчих сторін («атака - захист»), де логіка дій та наслідки такої «взаємодії», виходять за рамки традиційних морально-етичних норм й впливу антропогенних

(фізіологічних) обмежень (наприклад, за кількість одночасно спостережуваних подій та/або інтенсивності їх появи та/чи генези тощо). Авторами ряду досліджень зазначається, що сучасні архітектури з залученням елементів ШІ, можуть працювати в режимі реального часу та залишатися стійкими до спроб ухилення з боку зловмисників. Це відкриває хороші перспективи, з точки зору розширення можливостей у сфері моніторингу DNS трафіку [8-9].

2.3 Прецедентний аналіз (Case-Based Reasoning)

Підхід «*Case-Based Reasoning»* (далі - *CBR*) набуває все більшої уваги, як основа для створення більш прозорих, адаптивних і зрозумілих для користувачів систем ШІ. Оскільки сучасні моделі ШІ дедалі все частіше демонструють поведінку у дусі умовної «чорної скриньки»,то саме концепція *CBR* розглядається як адекватний запобіжний механізм. Причина очевидна – така концепція дій апелює на досвід вже відомих випадків (прецедентів), тобто проеціює й масштабує логіку причинно-наслідкових аналогій (в даному контексті - штучного мислення). У дослідженні [10] підкреслюється, що базовий цикл *CBR: «пошук – повторне використання – коригування – збереження»,* забезпечує інтерпретовану структуру в якій результуючі рішення ШІ, ґрунтуються на минулому досвіді, а не на непрозорих статистичних залежностях. Це робить *CBR* особливо привабливим у сферах, де критично важливими є такі категорії й властивості, як: - довіра, переконливість (ґрунтовність дій) та можливість зворотного аудиту. Є думка [10-12], що прецедентні тлумачення підвищують рівень довіри користувачів і покращують розуміння рішень штучної інтелектуальної системи, особливо в експертних галузях, таких як охорона здоров'я чи оцінка поточного стану ІБ сучасних ІКС тощо.

Іншим перспективним напрямом досліджень є інтеграція *CBR* із сучасними моделями ШІ, зокрема з *великими мовними моделями* (*LLM*) [10,12]. В цьому разі *CBR* допомагає функціональним «агентам» на основі *LLM,* зменшувати кількість хибних трактувань, надійніше виконувати доменно-орієнтовані завдання та надавати обґрунтування своїх рішень/дій. Загалом, в якості проміжного висновку, можна стверджувати, що впровадження *CBR,* забезпечує як методологічні, так і концептуальні переваги для ШІ систем. Це підвищує прозорість, послідовність і адаптивність штучно синтезованих рішень, та робить поведінкову логіку систем ШІ, більш узгодженою з логікою мислення людини, наприклад: - психологічну схильність людей шукати підтвердження своїм вже ухваленим рішенням (що, з технічної точки зору, дуже співпадає з загальною концепцією *CBR*).

2. Основна частина

Враховуючи специфіку питань залучення можливостей ШІ до вирішення завдань різноманітних аналітичних систем, слід звернути увагу на той факт (підтверджений отриманими результатами моделювання), що логіка систем ШІ не є чимось унікальною і беззастережно аксіоматичною. У цьому контексті слід мати на увазі принцип (схему дій), що експлуатують кібершахраї при реалізації одного з різновидів атак соціального інжинірингу. Головне у такій схемі - це експлуатація впевненості жертви атаки, у своїй раціональності: - в частині виконуваних дій та/чи думок (логіки рішень). - Така особливість повною мірою збігається з прагненням системи ШІ, самооптимізуватися в процесі вирішення покладених на неї завдань, ігноруючи загальний контекст і взаємозв'язок подій/процесів, що оцінюються. Звідси, більшою мірою, і виникає природа помилково-позитивних спрацьовувань. Для нівелювання зазначених наслідків доводиться обмежувати подібне прагнення ШІ до самооптимізації, шляхом впровадження додаткових інструкцій та прямих заборон. Запорукою належного виконання подібних обмежувально-керуючих дій є можливість реалізації (підтримки) інверсного аудиту логіки прийнятих рішень з боку ШІ.

У межах проведеного циклу моделювань досліджувалися особливості використання парадигми *CBR* для виконання завдань моніторингу поточного стану DNS трафіку із залученням можливостей ШІ. В якості умовного індикатора успішності подібної інтеграції, виступала задача автоматичного доповнення й модифікації таблиці прецедентів про аномалії DNS трафіку. Набір даних, використаний в експерименті, було отримано з попередньої роботи [1]. Такий підхід забезпечив безперервність умов вимірювань й порівнянність результатів. Тестовий програмний стенд реалізований за допомогою *Python*-клієнта, який виконує запити через *Gemini API*. Таким чином, поточний реліз моделюючого алгоритму, в якості вихідних даних використовував заздалегідь підготовлені відомості початкової (стартової) таблиці прецедентів. В загальному

випадку, відповідна таблиця/реєстр містить сукупність базових випадків та відповідні їм інтерпретації. Фрагмент початкової таблиці прецедентів, наведено в Таб. 1.

Після отримання початкового набору прецедентів, дослідна система автоматично розширює таблицю прецедентів, додаючи нові відомості з коментарями (тлумаченнями явищ й процесів), стосовно причин їх додавання. Така логіка дій дозволяє використовувати раніш отримані знання під час інтерпретації даних нових спостережень (мультибазових вимірів [1]). Це підвищує точність, прозорість (*послідовність й взаємопов'язаність подій*) та відтворюваність результатів аналітики спостережуваного процесу, в даному разі – аномалій DNS трафіку [3].

Аналіз відомостей даних реєстру прецедентів, котрі були згенеровано дослідною системою ШІ (фрагмент реєстру див. в Табл.2), дозволяють констатувати наступне:

1 - діюча модель дій (*логіка ШІ*) поряд з виявленням аномалій, які вже є в реєстрі, фіксує і раніш невідомі випадки, доповнюючи результуючу таблицю новими записами. Наприклад, відсутність відповідей або помилки виконання тестових DNS-запитів [1,3]. Це свідчить про те, що експериментальна ШІ система підтримує не лише сигнатурне виявлення відомих прецедентів, але здатна фіксувати й нові поведінкові аномалії і колізії DNS трафіку;

Таблиця 1. Фрагмент стартової таблиці прецедентів (аномалій)
Table 1. Fragment of the initial table of precedents (anomalies)

Location	Server Name	Test Domain	Plain query time (ms)	DoH query time (ms)	DoT query time (ms)	*Comment*
JAPAN	Google	**nic.ar**	931	241	-	*PQ latency spike*
FINLAND	OpenDNS	**gov.za**	1318	20	214	*PQ latency spike*
FRANCE	Quad9-Reserve	**bbc.co.uk**	444	801	1322	*PQ, DTQ and DHQ latency spike*
ISRAEL	OpenDNS	**paris.fr**	986	1301	1043	*PQ, DTQ and DHQ latency spike*
ISRAEL	Quad9	**bbc.co.uk**	943	362	993	*PQ, DTQ and DHQ latency spike*

***Прим**: - в таблицях 1-2, "PQ"," DTQ" та "DHQ" означають час незашифрованих, DoT та DoH запитів відповідно.*

2 - використання прецедентної парадигми обробки даних, сприяє зменшенню кількості хибних позитивних спрацьовувань. В даному разі аналітик (зворотний аудит) може позначати некоректні чи нерелевантні відомості реєстру, поступово вдосконалюючи (корегуючи) механізми прийняття рішень системою ШІ.

3 - під час тестування першої версії дослідної системи було виявлено явище так званого «***гіперфокусування уваги***» моделі. Це особливо помітно у випадках, коли спостерігалися кластери аномалій одного типу (приклад див. нижче на Рис.1).

Зокрема, така реакція системи фіксувалась у множині записів, що відповідають різним географічним локаціям, із яких було проведено вимірювання та/або DNS-серверам.

Так, поява екстремального значення затримки для одного з DNS протоколів [3-4] у послідовних записах, часто призводила до того, що дослідна система класифікувала всі такі записи, як «*піки затримки для одного протоколу*». При цьому, належним чином не враховувалась динаміка інших параметрів затримки в межах тих самих записів. В інших випадках, система позначала події типу «*Відсутність відповіді*» як аномалії, навіть якщо було достеменно відомо, що запитуваний DNS сервер не підтримує відповідний протокол. Такі реакції спостерігалися в тих випадках, коли ці записи розміщувалися поруч із записами, які дійсно містили збої виконання DNS запитів.

Отримані результати свідчать про те, що *локальна контекстна схожість записів* та *уявна безперервність шаблонів* можуть домінувати над формальними правилами загальної логіки процесу, дозволяючи ШІ формувати власні інтерпретації для «сусідніх» випадків (записів).

Відповідна колізія логіки роботи ШІ фіксувалась, навіть якщо таке узагальнення суперечить явним інструкціям та/або призводить до ігнорування інших важливих атрибутів даних (рис. 1) .

Location	Server Name	Test Domain	Plain	DoH	DoT	*Comment*
ISRAEL	ControlD-Reserve	**bbc.co.uk**	293	-	792	*No support for DHQ protocol*
ISRAEL	ControlD-Reserve	**sina.com.cn**	291	-	775	*No support for DHQ protocol*
ISRAEL	ControlD-Reserve	**nic.ar**	291	-	760	*No support for DHQ protocol*
ISRAEL	ControlD-Reserve	**gov.za**	293	-	785	*No support for DHQ protocol*
ISRAEL	ControlD-Reserve	**terra.com.br**	281	-	744	*No support for DHQ protocol*

Ignoring constraints that define supported protocols

Location	Server Name	Test Domain	Plain	DoH	DoT	*Comment*
FRANCE	Quad9-Reserve	**bbc.co.uk**	296	0	1335	*DHQ is 0*
FRANCE	Quad9-Reserve	**sina.com.cn**	758	0	1279	*DHQ is 0*
FRANCE	Quad9-Reserve	**nic.ar**	501	0	1324	*DHQ is 0*
FRANCE	Quad9-Reserve	**gov.za**	621	0	1282	*DHQ is 0*
FRANCE	Quad9-Reserve	**terra.com.br**	398	0	1330	*DHQ is 0*

Ignoring high plain and DoT latency

Рис.1 Фрагмент записів реєстру з «гіперфокусуванням уваги» ШІ
Fig.1 Fragment of registry entries with AI "hyperfocus of attention"

З метою підвищення репрезентативності даних, тестові вимірювання, з яких був зібраний датасет, здійснювалися з використанням різних комбінацій параметрів: - DNS-сервер (в табл.1-2, це «*Server name*»), географічне розташування точки вимірювання (в табл.1-2, це «*Location*») та доменне ім'я («*Test domain*»). Це дозволило врахувати просторову варіативність в розміщенні DNS-інфраструктури та мінімізувати вплив випадкових чинників на якість вибірки.

Таблиця 2. Приклад реєстру прецедентів, синтезованого за допомогою ШІ (фрагмент)
Table 2. Example of a registry of precedents synthesized using AI (fragment)

Location	**Server name**	**Test domain**	**Plain query time (ms)**	**DoH query time (ms)**	**DoT query time (ms)**	***Comment***
ISRAEL	Google-Reserve	**nic.ar**	1030	1018	-	*High PQ and DHQ latency*
USA	OpenDNS-Reserve	**post.japanpost.jp**	833	989	1168	*High latency for all protocols*
FRANCE	Google-Reserve	**nic.ar**	231	911	-	*High DHQ latency with low PQ*
ISRAEL	OpenDNS	**gov.za**	76	345	808	*High DTQ latency compared to PQ and DHQ*
FINLAND	OpenDNS	**xinhuanet.com**	430	1156	1316	*High DHQ and DTQ latency compared to PQ.*
FRANCE	Quad9-Reserve	**bbc.co.uk**	296	0	1335	*Zero DHQ latency, also high DTQ.*
ISRAEL	ControlD	**bbc.co.uk**	852	-	861	*PR is null*

Додатковим підтвердженням зазначеної вище, несподіваної логіки висновків ШІ, є коментарі на кшталт *«DTQ = 0»* у випадках, коли інші показники часу затримки DNS запитів виходили за межі норми (приклад див. рис. 2).

Також, варто зазначити, що значна частина коментарів з блоку ШІ, була сфокусована виключно на одному показнику, попри наявність кількох аномальних ознак у межах одного запису. Це свідчить про надмірне зосередження ШІ на окремих екстремальних (*з його точки зору*) параметрах контрольованого процесу.

Anomalous entry:

Location	Server Name	Test Domain	Plain	DoH	DoT
JAPAN	Quad9	terra.com.br	540	261	0

Рис.2 Різниця коментарів (трактувань) системи на алогічні записи
Fig.2 Difference in system comments (interpretations) on anomalous entries

Для усунення наслідків цієї проблеми було запроваджено новий набір інструкцій, які «заохочують» модель приділяти більше уваги загальному контексту подій й уповільнювати формування власних висновків під час обробки кластерів подібних аномалій. Метою цього вдосконалення є: - спонукати ШІ, враховувати більш ширший контекст показників затримки в межах кожного спостереження поточних подій. Тим самим усуваються передумови концентрації ШІ на одному екстремальному значенні, чим зменшується ризик виникнення явища гіперфокусування на окремому аспекті запису та як наслідок, ігнорування інших релевантних даних або формування хибних позитивних результатів/рекомендацій.

Після корегування відповідних інструкцій для блоку ШІ, спостережено помітні зміни у структурі та змісті коментарів до аномальних записів. Так, замість лаконічних односторонніх класифікацій на кшталт «*пікове значення затримки незашифрованого запиту*» або «*час відповіді DoH дорівнює 0*», модель почала формувати більш комплексні (взаємопов'язані) та порівняльні описи. Наприклад, записи, які раніше позначалися лише як: - «*пікове значення затримки незашифрованого запиту*», тепер описувалися у більш конкретизованій формі, такій як: - «*пікове значення затримки незашифрованого запиту, затримка DoH-запиту перебуває в межах норми*». Аналогічно, випадки з нульовими або аномально низькими чи високими значеннями почали супроводжуватися явними порівняннями з іншими показниками затримки, наприклад: «*нульова затримка DoT-запиту за умов високої затримки незашифрованого запиту*» тощо.

Загалом така зміна характеру коментарів моделі, свідчить про ефективність запроваджених заходів, стосовно зменшення ефекту гіперфокусування. Оновлена парадигма логіки повноважень ШІ, демонструє більш цілісну та взаємопов'язану інтерпретацію аномальних випадків затримки DNS-трафіку. Прийняти заходи зменшили ймовірність упередженості висновків ШІ, відносно ролі та місця будь-якого одного з параметрів в межах спостережуваного процесу, сприяючи більш коректному – контекстно-орієнтованому й аргументованому виявленню реальних аномалій. Це підтверджується через таргетовані коментарі, наявність яких покращує умови для проведення інверсного аудиту логіки ШІ *(«**IA logic IA**» – Inverse Audit of the logic of AI)*. В наслідок проведених змін істотно змінилась точність ідентифікації аномалій DNS трафіку для тих записів, які були внесені до реєстру за участю саме модулю ШІ.

В якості прикладу вказаних процесів, нижче (рис. 3) наведено показові діаграми з характерною різницею аномалій контрольованого параметру (*в даному разі, часу затримки запитів)* для наявного переліку доменів реєстру прецедентів в умовах, «ДО» та «ПІСЛЯ» (світло-сіра, *Modified*) проведених корегувань логіки прийняття рішень дослідної моделі ШІ.

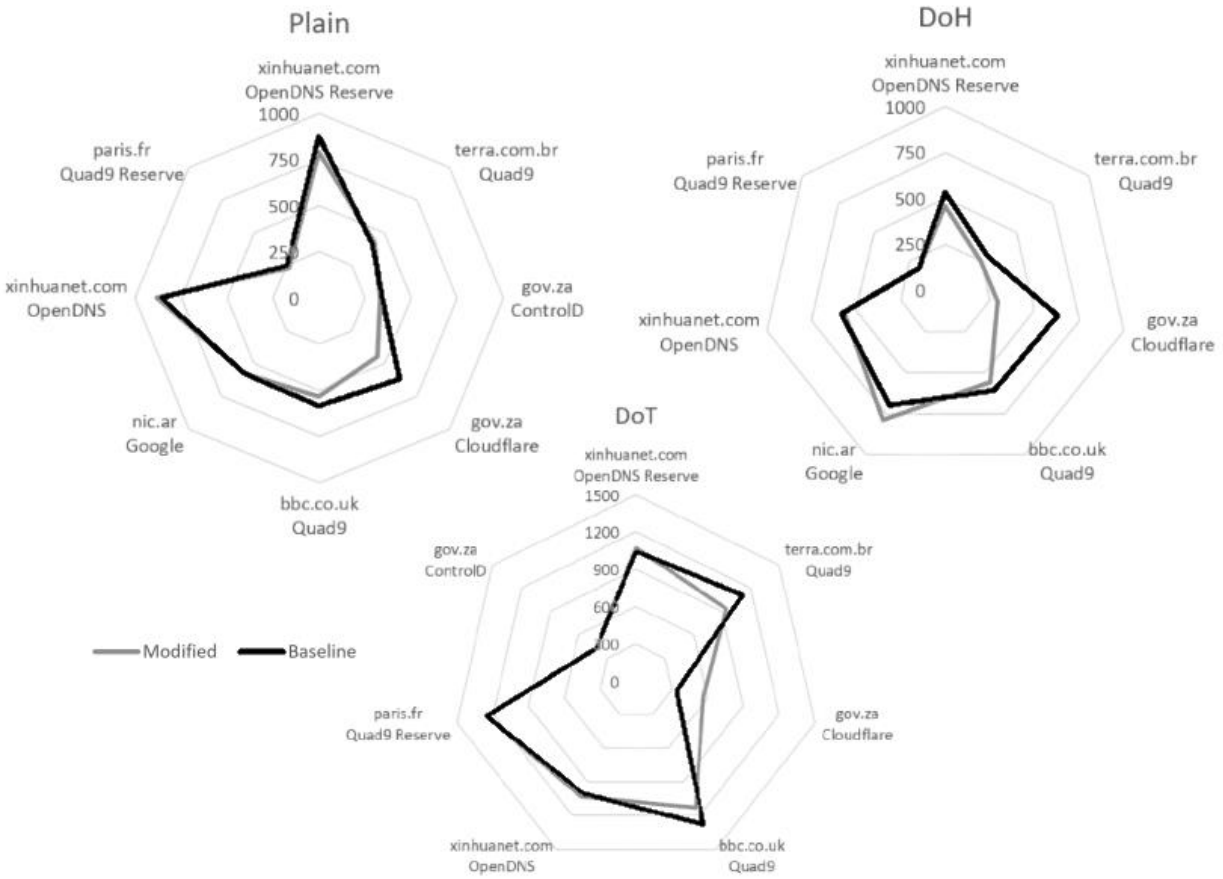

Рис.3 Приклад різниці трактувань аномалій трафіку (шкала часу в [ms])
Fig.3 Example of difference in interpretations of traffic anomalies (time scale in [ms])

Темна/чорна (*Baseline*) лінія на рис. 3 характеризує аномальні показники (середню затримку) «ДО» внесення корегувань. Відповідно, світла лінія характеризує відомості реєстру аномалій, згідно нової парадигмі дій ШІ. Як видно, корегована логіка дій, містить більш ґрунтовний набір даних про виявлені аномалії (за амплітудою часових викидів), що виключає хибні дії/реакції в частині корегування параметрів діючої RPZ. Інше кажучи, результати моніторингу DNS трафіку, стали більш ґрунтовними й виваженими, що відображається через зменшення, як кількості, так й амплітуди «викидів» контрольованого параметра (для умов рис. 3, це часові аномалії DNS запитів). Тобто, чим більш звуженим (чи рівномірним) стає діапазон спостережуваних часових аномалій, тим більш адекватною є реакція системи ШІ на фактичний перебіг контрольованих подій (в т.ч. умов (!) й обставин (!!) процесу, що спостерігається).

4. Висновки

1. Проведено дослідне моделювання програмного інструменту комплексного моніторингу DNS-трафіку із застосуванням концепції прецедентного аналізу (*CBR*), як основи процедурної парадигми ШІ. Підтверджено її придатність для підвищення прозорості виявлення поведінкових аномалій трафіку. Результати моделювання свідчать, що *CBR* підхід, покращує співвіднесення нових спостережень з наявною базою знань, що розширює можливості зворотного аудиту логіки ШІ та підвищує ступінь валідації прийнятих рішень (реакцій ШІ системи).

2. Впровадження *CBR* підвищує прозорість, послідовність і адаптивність штучно синтезованих рішень, та робить поведінкову логіку систем ШІ, більш узгодженою з традиційною логікою мислення людини.

3. Дослідна система успішно доповнила вихідну таблицю прецедентів новими відомостями про аномалії. Підтверджено здатність виявляти, як наперед визначені категорії аномалій, так і додаткові (нові) нерегулярності у даних, що контролюються. Використаний алгоритм обробки

даних забезпечує трактування результатів моніторингу за рамками явно заданих прикладів, водночас зберігаючи/враховуючи логіку причинно-наслідкових зв'язків спостережуваних подій, спираючись на відомості формалізованих шаблонів прецедентів.

4. У ході моделювань визначені обмеження застосованого підходу. Дослідна ШІ система виявила властивість «кластеризації власних трактувань» (ефект т.з. гіперфокусування). Це може призводити до хибної інтерпретації процесів і, як наслідок, до хибних позитивних спрацьовувань. Ефект присутній у випадках, коли подібні відомості розташовані у безпосередній близькості один від одного (кластерах записів). В даному випадку логіка контекстуальній схожості домінує над явними протокольними обмеженнями. В якості компенсаторних заходів, застосовано новий набір обмежень (інструкцій прямої дії). Подальше тестування підтвердило, що ці зміни зменшили прояв виявленого ефекту, підвищивши надійність інтерпретації аномалій.

5. Одержані результати моделювань дозволяють стверджувати, що «логіка роботи систем ШІ не є чимось унікальною і безумовно аксіоматичною». У цьому контексті слід мати на увазі внутрішнє прагнення систем ШІ до самооптимізації в процесі вирішення покладених на них завдань. Це специфічне «прагнення» потребує запровадження додаткових інструкцій та прямих заборон. Запорукою належного виконання подібних обмежувально-керуючих дій є можливість реалізації інверсного аудиту логіки прийнятих ШІ рішень (*«IA logic IA»*).

6. В якості подальших досліджень слід розглядати: - удосконалення механізмів модерації реєстру прецедентів; - масштабування парадигми *CBR* на всі елементи системи хмарного моніторингу DNS трафіку; - розширення можливостей системи, щодо варіативності сценаріїв моніторингу та структури тестових запитів для покращення виявлення нових аномалій.

СПИСОК ЛІТЕРАТУРИ

1. Chepel D., Malakhov S. Multibased cloud monitoring of DNS traffic for operative correction of current RPZ parameters. *Modern information security*. 2025. Т. 63, № 3. С. 176–187. URL: https://doi.org/10.31673/2409-7292.2025.031949 (дата звернення: 23.02.2026).
2. Chepel D., Malakhov S. Summary of DNS traffic filtering trends as a component of modern information systems security. *Computer science and cybersecurity*. 2024. № 1. С. 6–21. URL: https://doi.org/10.26565/2519-2310-2024-1-01 (дата звернення: 23.02.2026).
3. Чепель Д., Малахов С. Мультипротокольний моніторинг трафіку DNS, як основа для коригування поточних параметрів RPZ. *Theoretical and practical aspects of modern scientific research*. 2025. URL: https://doi.org/10.36074/logos-24.01.2025.049 (дата звернення: 23.02.2026).
4. Коробейнікова Т., Федчук Т. Огляд протоколів DNS, DoH та DoT. *Débats scientifiques et orientations prospectives du développement scientifique*. 2024. URL: https://doi.org/10.36074/logos-01.03.2024.056 (дата звернення: 23.02.2026).
5. Advancements in artificial intelligence and data science: models, applications, and challenges / M. F. Safitra et al. *Procedia computer science*. 2024. Т. 234. С. 381–388. URL: https://doi.org/10.1016/j.procs.2024.03.018 (дата звернення: 23.02.2026).
6. Data analysis in the era of generative AI / J. P. Inala et al. 2024. (Препринт). URL: https://doi.org/10.48550/arXiv.2409.18475 (дата звернення: 23.02.2026).
7. Artificial intelligence approaches and mechanisms for big data analytics: a systematic study / A. M. Rahmani et al. *PeerJ computer science*. 2021. Т. 7. e488. URL: https://doi.org/10.7717/peerj-cs.488 (дата звернення: 23.02.2026).
8. Zebin T., Rezvy S., Luo Y. An explainable AI-based intrusion detection system for DNS over HTTPS (DoH) attacks. *IEEE transactions on information forensics and security*. 2022. С. 1. URL: https://doi.org/10.1109/tifs.2022.3183390 (дата звернення: 23.02.2026).
9. Ali B., Chen G. Next-generation AI for advanced threat detection and security enhancement in DNS over HTTPS. *Journal of network and computer applications*. 2025. Т. 244. 104326. URL: https://doi.org/10.1016/j.jnca.2025.104326 (дата звернення: 23.02.2026).
10. Pradeep P., Caro-Martínez M., Wijekoon A. Empowering explainable artificial intelligence through case-based reasoning: a comprehensive exploration. *IEEE transactions on knowledge and data engineering*. 2025. С. 1–20. URL: https://doi.org/10.1109/tkde.2025.3609825 (дата звернення: 23.02.2026).

11. Pradeep P., Caro-Martínez M., Wijekoon A. A practical exploration of the convergence of Case-Based Reasoning and Explainable Artificial Intelligence. *Expert systems with applications*. 2024. 124733. URL: https://doi.org/10.1016/j.eswa.2024.124733 (дата звернення: 23.02.2026).
12. Hatalis K., Christou D., Kondapalli V. Review of case-based reasoning for LLM agents: theoretical foundations, architectural components, and cognitive integration. 2025. (Препринт). URL: https://doi.org/10.48550/arXiv.2504.06943 (дата звернення: 23.02.2026).
13. Гончаров М., Чепель Д., Малахов С. Оцінка обчислювальної складності етапу попередньої обробки вхідних даних при реалізації процедур стегановставки зображень. *Наука і техніка сьогодні*. 2025. № 8(49). URL: https://doi.org/10.52058/2786-6025-2025-8(49)-1228-1245 (дата звернення: 23.02.2026).
14. Горелько М., Малахов С. Аналіз метаданих шифрованого трафіку як чинник нівелювання «сліпих зон» безпеки в сучасних IT - системах. *Інтелектуальні технології у міждисциплінарних дослідженнях: Збірник наукових праць XI МНТК*. Харків: ХНУ ім. В.Н. Каразіна, Україна, 2025. С. 89–92.

REFERENCES

1. D. Chepel and S. Malakhov, “Multibased cloud monitoring of DNS traffic for operative correction of current RPZ parameters,” *Modern Information Security*, vol. 63, no. 3, pp. 176–187, 2025. Accessed: Feb. 23, 2026. [Online]. Available: https://doi.org/10.31673/2409-7292.2025.031949
2. D. Chepel and S. Malakhov, “Summary of DNS traffic filtering trends as a component of modern information systems security,” *Computer Science and Cybersecurity*, no. 1, pp. 6–21, Sep. 2024. Accessed: Feb. 23, 2026. [Online]. Available: https://doi.org/10.26565/2519-2310-2024-1-01 [in Ukrainian]
3. D. Chepel and S. Malakhov, “Мультипротокольний моніторинг трафіку DNS, як основа для коригування поточних параметрів RPZ [Multi-protocol DNS traffic monitoring as a basis for adjusting current RPZ parameters],” in *Theoretical and Practical Aspects of Modern Scientific Research*. Eur. Scientific Platform, 2025. Accessed: Feb. 23, 2026. [Online]. Available: https://doi.org/10.36074/logos-24.01.2025.049 [in Ukrainian]
4. T. Korobeinikova and T. Fedchuk, “Огляд протоколів DNS, DoH та DoT [Overview of DNS, DoH, and DoT protocols],” in *Débats scientifiques et orientations prospectives du développement scientifique*. Eur. Scientific Platform, 2024. Accessed: Feb. 23, 2026. [Online]. Available: https://doi.org/10.36074/logos-01.03.2024.056 [in Ukrainian]
5. M. F. Safitra, M. Lubis, T. F. Kusumasari, and D. P. Putri, “Advancements in artificial intelligence and data science: Models, applications, and challenges,” *Procedia Computer Science*, vol. 234, pp. 381–388, 2024. Accessed: Feb. 23, 2026. [Online]. Available: https://doi.org/10.1016/j.procs.2024.03.018
6. J. P. Inala *et al.*, *Data Analysis in the Era of Generative AI*. To be published. Accessed: Feb. 23, 2026. [Online]. Available: https://doi.org/10.48550/arXiv.2409.18475
7. A. M. Rahmani *et al.*, “Artificial intelligence approaches and mechanisms for big data analytics: A systematic study,” *PeerJ Computer Science*, vol. 7, Apr. 2021, Art. no. e488. Accessed: Feb. 23, 2026. [Online]. Available: https://doi.org/10.7717/peerj-cs.488
8. T. Zebin, S. Rezvy, and Y. Luo, “An explainable AI-based intrusion detection system for DNS over HTTPS (DoH) attacks,” *IEEE Transactions on Information Forensics and Security*, p. 1, 2022. Accessed: Feb. 23, 2026. [Online]. Available: https://doi.org/10.1109/tifs.2022.3183390
9. B. Ali and G. Chen, “Next-generation AI for advanced threat detection and security enhancement in DNS over HTTPS,” *Journal of Network and Computer Applications*, vol. 244, p. 104326, Dec. 2025. Accessed: Feb. 23, 2026. [Online]. Available: https://doi.org/10.1016/j.jnca.2025.104326
10. P. Pradeep, M. Caro-Martínez, and A. Wijekoon, “Empowering explainable artificial intelligence through case-based reasoning: A comprehensive exploration,” *IEEE Transactions on Knowledge and Data Engineering*, pp. 1–20, 2025. Accessed: Feb. 23, 2026. [Online]. Available: https://doi.org/10.1109/tkde.2025.3609825
11. P. Pradeep, M. Caro-Martínez, and A. Wijekoon, “A practical exploration of the convergence of Case-Based Reasoning and Explainable Artificial Intelligence,” *Expert Systems With Applications*, p. 124733, Jul. 2024. Accessed: Feb. 23, 2026. [Online]. Available: https://doi.org/10.1016/j.eswa.2024.124733

12. K. Hatalis, D. Christou, and V. Kondapalli, *Review of Case-Based Reasoning for LLM Agents: Theoretical Foundations, Architectural Components, and Cognitive Integration*. To be published. Accessed: Feb. 23, 2026. [Online]. Available: https://doi.org/10.48550/arXiv.2504.06943
13. М. Гончаров, Д. Чепель, and С. Малахов, "Оцінка обчислювальної складності етапу попередньої обробки вхідних даних при реалізації процедур стегановставки зображень," *Наука і техніка сьогодні*, no. 8(49), Sep. 2025. Accessed: Feb. 23, 2026. [Online]. Available: https://doi.org/10.52058/2786-6025-2025-8(49)-1228-1245 [in Ukrainian]
14. M. Horelko and S. Malakhov, "Аналіз метаданих шифрованого трафіку як чинник нівелювання «сліпих зон» безпеки в сучасних IT – системах [Metadata analysis of encrypted traffic as a factor in eliminating security "blind spots" in modern IT systems]," in *Інтелектуальні технології у міждисциплінарних дослідженнях: Збірник наукових праць XI МНТК*. Харків, Україна: ХНУ ім. В.Н. Каразіна, 2025, pp. 89–92. [in Ukrainian]

Chepel Danylo *Ph.D student*
of the Department of Cybersecurity of Information Systems, Networks and Technologies
V.N. Karazin Kharkiv National University, 4 Svobody sq., Kharkiv, Ukraine, 61022
Malakhov Serhii *Ph.D, Associate Professor*
of the Department of Cybersecurity of Information Systems, Networks and Technologies
V.N. Karazin Kharkiv National University, 4 Svobody sq., Kharkiv, Ukraine, 61022
Honcharov Mykyta *Ph.D student*
of the Department of Cybersecurity of Information Systems, Networks and Technologies
V.N. Karazin Kharkiv National University, 4 Svobody sq., Kharkiv, Ukraine, 61022

Application of a precedent analysis paradigm for the purposes of multibase cloud monitoring of DNS traffic

Relevance. The increasing complexity of DNS infrastructure and the growing level of threats in the network environment necessitate the development of intelligent DNS traffic monitoring tools capable of providing transparent, adaptive, and well-grounded detection of behavioral anomalies. Particular relevance is associated with the implementation of approaches that enhance the traceability of decision-making logic in artificial intelligence (AI) systems.
Purpose. The purpose of this study is to experimentally investigate a prototype software tool for monitoring the current state of DNS traffic with extensive implementation of AI capabilities, the logic of which is based on the concept of case-based reasoning (CBR) for behavioral DNS traffic anomaly analysis.
Research Methods. The study employs simulation modeling methods, multi-base measurements of DNS query processing time using a system of distributed cloud-based sensor-testers, as well as case-based reasoning algorithms for intelligent post-processing of data. The prototype was implemented as a Python client integrated with the Gemini API, operating on a dataset formed based on the results of previous studies [1–2]. During operation, the system autonomously modifies the anomaly registry by adding new cases based on analytical processing results.
Results. The obtained results demonstrate that the proposed DNS traffic monitoring approach ensures the detection of both previously known anomalies and the localization of previously unidentified irregularities. The feasibility of applying the case-based approach to improve the efficiency of adjusting the parameters of the active Response Policy Zone (RPZ) [3] and to enhance situational awareness of personnel regarding DNS traffic security has been confirmed. At the same time, the experiments revealed a so-called "clustering" effect that may lead to false positive event assessments and, consequently, contradictory interpretations of the observed network events.
Conclusions. The revision of existing constraints and analytical tasks for AI modules, followed by further modeling, confirmed that the introduced modifications significantly reduced the identified "clustering" effect and improved the reliability of anomaly interpretation based on a defined system of indirect (implicit) indicators. The obtained results confirm the feasibility of further developing the case-based reasoning approach in intelligent DNS traffic monitoring systems.

Keywords: *information security, artificial intelligence, traffic filtering, DNS, RPZ, CBR, network anomalies, cloud computing, distributed network, DNS protocols.*

Надійшла у першій редакції 25.01.2026; рекомендована до друку 01.03.2026; опублікована 03.04.2026.
The first version has been received on 25.01.2026; was recommended for printing on 01.03.2026; published 03.04.2026.