

ISSN 1996-1588

Міністерство освіти і науки України



НАУКОВІ ПРАЦІ
ДОНЕЦЬКОГО НАЦІОНАЛЬНОГО
ТЕХНІЧНОГО УНІВЕРСИТЕТУ

Серія: Інформатика, кібернетика
та обчислювальна техніка

№2(43) 2026



Дрогобич 2026

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Наукові праці
Донецького національного технічного
університету

**Серія: “Інформатика, кібернетика
та обчислювальна техніка”**

Всеукраїнський науковий збірник

Заснований у травні 1996 року

Виходить 2 рази на рік

№ 2 (43) ’ 2026

Дрогобич – 2026

Публікується згідно з рішенням Вченої ради ДВНЗ «Донецький національний технічний університет» (протокол № 9 від 17.09.2026).

Збірник містить наукові статті, що висвітлюють результати наукових досліджень і розробок в таких напрямках, як інформатика, кібербезпека, захист інформації, чисельні методи, паралельні обчислення, програмування, розробка засобів обчислювальної техніки, дослідження комп'ютерних мереж, машинна графіка і обробка зображень, автоматизація, робототехніка, математичне моделювання в різних галузях. Матеріали збірника призначені для наукових співробітників, викладачів, інженерно-технічних працівників, аспірантів та студентів.

Засновник та видавець – Донецький національний технічний університет (ДонНТУ)

РЕДАКЦІЙНА КОЛЕГІЯ:

Д-р наук, проф. Я. Ю. Дорогий (головний редактор); д-р наук, проф. Є.О. Башков, (заступник головного редактора); д-р наук, проф. О.А. Дмитрієва, д-р наук, проф. І.М. Журавська; д-р наук, проф. Л.В. Ковальчук; д-р наук, проф. С.Д. Погорілий; д-р наук, проф. В.В. Лукашенко; д-р наук, проф. В.А. Святний; д-р наук, проф. Г.Г. Швачич; д-р наук, проф. І.С. Лактіонов; д-р наук, проф. Ю.С. Ямненко; д-р наук, проф. Гайнрих Штефан; д-р наук, проф. Кінле Йоахим; д-р наук, проф. Реш Міхаель; д-р філософії (канд. наук), доцент В.В. Воропаєва; д-р філософії (канд. наук), доцент Н.В. Дженюк; д-р філософії (канд. наук), доцент А.А. Єфіменко; д-р філософії (канд. наук), доцент І.Я. Зеленьова; д-р філософії (канд. наук), доцент С.В. Марценко; д-р філософії (канд. наук), доцент Н.О. Маслоva; д-р філософії (канд. наук), доцент А.В. Писаренко; д-р філософії (канд. наук), доцент В.П. Полтораk; д-р філософії (канд. наук), доцент М.Ю. Толкачов; д-р філософії (канд. наук), доцент В.В. Цуркан; д-р філософії (канд. наук), доцент І.А. Назарова (відп. секретар випуску), Є.О. Єжова (технічний редактор).

Адреса редакції:

Юридична адреса: пл. Шибанкова, 2, м. Покровськ, Донецька область, 85300

Фактична адреса: вул. Самбірська, 76, м. Дрогобич, Львівська обл., 82111

Адреса для листування: вул. Шевченка, 9, м. Дрогобич, Львівська обл., 82100

E-mail: ikot@donntu.edu.ua

Збірник зареєстровано в Державному комітеті інформаційної політики, телебачення та радіомовлення України. Свідоцтво: серія KB, №7374 від 03.06.2003.

Збірник включено до переліку наукових фахових видань України, в яких можуть публікуватися результати дисертаційних робіт на здобуття наукових ступенів доктора наук, кандидата наук та ступеня доктора філософії за спеціальностями:

- F2 Інженерія програмного забезпечення;
- F3 Комп'ютерні науки;
- F5 Кібербезпека та захист інформації;
- F6 Інформаційні системи і технології;
- F7 Комп'ютерна інженерія;
- G7 Автоматизація, комп'ютерно-інтегровані технології та робототехніка.

(наказ Міністерства освіти і науки України №928 від 11 червня 2026 р.)

Збірник "Наукові праці ДонНТУ, серія "Інформатика, кібернетика та обчислювальна техніка" за наказом № 928 МОНУ від 11.06.2026 отримав категорію Б.

Д. О. Світличний

Підвищення ефективності багатокласової класифікації кібератак у мережах критичної інфраструктури на основі алгоритму GS-GBDT 145

А. М. Ткачов, А. А. Гаврилова, Н. О. Бринза

Забезпечення проактивної кіберстійкості інформаційних систем шляхом синтезу архітектур нульової довіри в умовах багаторівневих загроз 153

І. В. Букатич, М. Ю. Толкачов, Н. В. Дженюк

Модель інтегрованої перевірки цілісності та відновлення персональних даних у міжблокейнових мостах на основі UMAC і криптокодових конструкцій 165

В. І. Ящук, О. І. Полотай, В. С. Балацька

Проектування систем безпеки об'єктів критичної інфраструктури 173

В. М. Шутенко, Б. Ю. Жураковський

Задача узгодженого управління кешуванням та індексацією даних у високонавантажених інформаційних системах 187

О. В. Вовна, А. С. Марина, М. М. Джебженяк

Семантично орієнтований метод багаторівневого контролю та локалізації змін структурованих персональних даних 198

Н. Е. Кунанець, В. В. Пасічник, В. І. Кут, М. В. Орлов, А. А. Веремєєнко

Процедура формування компонентної конфігурації інформаційно-технологічної платформи 212

Д. М. Загорулько, А. О. Фесенко

Референсна архітектура та методика метричного оцінювання інформаційної технології автоматизації бізнес-процесів через API 228

М. О. Слабінога, Т. В. Бойчук

Розробка інформаційної системи моніторингу стану забезпеченості комп'ютерною технікою 236

D. S. Kotelevskiy, I. Y. Zelenova, T. V. Holub, S. S. Hrushko, T. S. Diachuk

Advisory AI-based VHDL code verification system for IT students 244

А. А. Таборовський, Ю. Й. Стрілецький

Засоби апаратної ідентифікації вузлів в розподілених комп'ютерних мережах на основі фізично неклонованих функцій 252

Д. В. Грицюк, С. Ю. Скрупський, В. В. Шкарупило

Дослідження мобільних засобів діагностування автомобільних дизельних сажових фільтрів з використанням нейромережових моделей 264

О. Л. Заміховська

Розробка адаптивної BPMN-моделі управління інцидентами кібербезпеки з використанням Camunda на основі IDEF3-сценаріїв 276

О. К. Карнаухов, С. В. Марценко

Інформаційна технологія оцінювання цифрової зрілості університету 284

УДК 004.056:004.7:519.8

А. М. Ткачов, к.т.н., доцент

А. А. Гаврилова, PhD, доцент

Н. О. Бринза, к.т.н., доцент

^{1,2}НТУ "ХПІ", Харків, Україна³ХНЕУ ім. С. Кузнеця, Харків, Україна¹Andrii.Tkachov@khpi.edu.ua, ²Alla.Navrylova@khpi.edu.ua³Natalia.Brynza@hneu.net

ЗАБЕЗПЕЧЕННЯ ПРОАКТИВНОЇ КІБЕРСТІЙКОСТІ ІНФОРМАЦІЙНИХ СИСТЕМ ШЛЯХОМ СИНТЕЗУ АРХІТЕКТУР НУЛЬОВОЇ ДОВІРИ В УМОВАХ БАГАТОРІВНЕВИХ ЗАГРОЗ

У статті досліджено проблему підвищення проактивної кіберстійкості інформаційно-комунікаційних систем в умовах багаторівневих кібератак. Проаналізовано обмеження периметрової моделі безпеки та обґрунтовано застосування архітектури нульової довіри. Запропоновано математичну модель аналізу мережевого трафіку на основі показника Херста та неекстенсивної ентропії Цалліса. Сформовано комплексний критерій довіри для динамічної оцінки стану вузлів і адаптивного управління доступом. Розроблено механізми безперервної багатofакторної верифікації та мікросегментації. Експериментальні дослідження підтвердили ефективність підходу у виявленні аномалій, скороченні часу реагування та локалізації компрометації.

Ключові слова: кібербезпека, проактивна кіберстійкість, архітектура нульової довіри, фрактальний аналіз, мікросегментація, виявлення аномалій, горизонтальне переміщення.

DOI: 10.31474/1996-1588-2026-2-43-153-164

Вступ

Стрімкий розвиток інформаційно-комунікаційних технологій та масштабні процеси цифровізації державного і приватного секторів зумовлюють безперервне зростання складності архітектури інформаційних систем. Зазначені тенденції неминуче супроводжуються пропорційним збільшенням кількості та витонченості кібернетичних загроз. Сучасний ландшафт кібернетичної небезпеки характеризується домінуванням багаторівневих цілеспрямованих атак, які здатні тривалий час залишатися непоміченими всередині скомпрометованої інфраструктури, поступово розширюючи зону контролю. Класичні підходи до організації інформаційної безпеки, які базуються на захисті виключно зовнішнього мережевого периметра, демонструють критичну неефективність в умовах розмиття меж корпоративних мереж, масового переходу до технологій віртуалізації та поширення віддалених режимів роботи. Традиційна модель довіреної внутрішньої мережі дозволяє зловмисникам, які успішно подолали зовнішній рубіж захисту, безперешкодно здійснювати горизонтальне переміщення між внутрішніми вузлами, підвищувати привілеї та отримувати

несанкціонований доступ до критично важливих інформаційних ресурсів.

Вказані обставини вимагають концептуального перегляду парадигми кіберзахисту та обґрунтованого переходу від реактивних методів реагування на інциденти до забезпечення проактивної кіберстійкості. Проактивна кіберстійкість передбачає здатність інформаційної системи не лише пасивно протистояти деструктивним впливам, але й функціонувати в умовах часткової компрометації з мінімальними втратами продуктивності, постійно та автономно адаптуючись до нових векторів атак. Найбільш дієвим механізмом реалізації такої здатності є впровадження концепції архітектури нульової довіри. Зазначений підхід фундаментально виключає поняття безумовної довіри до будь-якого суб'єкта чи об'єкта мережі незалежно від його фізичного або логічного розташування. Побудова систем захисту за принципом нульової довіри вимагає безперервної багатofакторної верифікації кожного запиту на доступ, динамічного обчислення рівня ризику та впровадження суворої мікросегментації мережі.

Водночас існуючі практичні реалізації таких архітектур часто покладаються на статичні правила та не враховують нелінійну динаміку мережевого трафіку, що суттєво знижує точність виявлення прихованих поточкових аномалій на

ранніх етапах розвитку атаки. Звичайний аналіз сигнатур та пороговий моніторинг не здатні виявити складні аномалії, які маскуються під легітимну поведінку користувачів. Тому надзвичайно актуальним науковим і практичним завданням є розробка новітніх методів математичного моделювання динаміки трафіку для своєчасного виявлення аномальних відхилень та глибока інтеграція цих методів у загальну архітектуру проактивного захисту задля забезпечення безперервної верифікації довіри.

Об'єктом дослідження є процес забезпечення інформаційної безпеки та проактивної кіберстійкості сучасних інформаційно-комунікаційних систем за умов впливу багаторівневих цілеспрямованих загроз.

Предметом дослідження виступають математичні моделі, аналітичні методи та структурні рішення архітектури нульової довіри, спрямовані на виявлення потокових аномалій і динамічне управління доступом до критичних ресурсів.

Метою дослідження є підвищення рівня проактивної кіберстійкості інформаційних систем шляхом розроблення та впровадження комплексної архітектури нульової довіри, яка базується на математичному моделюванні динаміки мережевого трафіку з використанням сучасного апарату нелінійної динаміки.

Для досягнення поставленої мети сформовано та послідовно вирішено наступні **науково-практичні завдання**. По-перше, необхідно здійснити критичний аналіз існуючих підходів до захисту інформаційного периметра, концепцій нульової довіри та визначити ключові обмеження сучасних методів виявлення мережевих аномалій. По-друге, потрібно формалізувати базові параметри мережевого потоку, застосувати апарат фрактального аналізу і нелінійної ентропії та синтезувати комплексний математичний критерій для динамічної оцінки рівня довіри до вузлів мережі. По-третє, необхідно розробити концептуальну структурну схему архітектури нульової довіри, яка використовує отримані математичні залежності для механізмів безперервної верифікації суб'єктів і блокування несанкціонованого горизонтального переміщення. По-четверте, провести експериментальні дослідження запропонованої архітектури в умовах імітаційного моделювання багаторівневих кібератак для оцінювання часу реакції системи та підтвердження ефективності розроблених теоретичних рішень.

1. Аналіз останніх досліджень і публікацій

Протягом останніх кількох десятиліть концептуальним базисом для розробки та практичної реалізації систем забезпечення

інформаційної безпеки виступала традиційна модель захисту мережевого периметра [1, 2]. Зазначена модель ґрунтується на застосуванні чіткого фізичного та логічного розмежування між внутрішнім довіреним середовищем корпоративної мережі та зовнішнім неохопленим середовищем, що за замовчуванням вважається ворожим та потенційно небезпечним [3]. Основний комплекс засобів захисту в межах такої архітектури зосереджений безпосередньо на рубежах перетину мережевого кордону. До ключових технічних компонентів традиційного периметрового захисту належать міжмережеві екрани різних рівнів фільтрації, системи виявлення та запобігання вторгненням, а також засоби побудови віртуальних приватних мереж для забезпечення зашифрованих каналів зв'язку віддалених користувачів [3, 4].

Головним системним і концептуальним недоліком традиційної периметрової моделі є надання неявної або безумовної довіри всім суб'єктам, пристроям, додаткам та інформаційним потокам, які знаходяться всередині контрольованого мережевого сегмента [4]. Зазначений підхід передбачає, що проходження успішної первинної перевірки автентичності та авторизації на зовнішньому рубежі є достатньою умовою для надання розширеного спектра привілеїв усередині інфраструктури [5]. Однак сучасні тенденції розвитку інформаційно-комунікаційних систем, зокрема масовий перехід на хмарні обчислення, активне впровадження технологій віртуалізації, концепція використання власних пристроїв працівників та поширення режимів віддаленої та гібридної роботи, призвели до того, що фізичні та логічні межі мережевого периметра остаточно розмилися [1, 5].

У сучасних умовах класичні засоби захисту периметра демонструють критичну неефективність перед внутрішніми загрозами, компрометацією облікових даних авторизованого персоналу та цілеспрямованими багаторівневими кібератаками [2, 10]. Компрометація хоча б одного облікового запису або кінцевого пристрою всередині периметра надає зловмиснику можливість здійснювати безперешкодне горизонтальне переміщення всередині інфраструктури, підвищувати привілеї та отримувати несанкціонований доступ до критично важливих інформаційних ресурсів [1, 4].

Необхідність подолання системних обмежень периметрової моделі та протидії складним багаторівневим загрозам зумовила розробку та активне впровадження концепцій архітектури нульової довіри [1–3]. У сучасних наукових працях доведено, що забезпечення високого рівня кіберстійкості складних розподілених систем вимагає фундаментального переходу від концепції пасивного захисту

зовнішнього кордону до концептуального принципу «нікому не довіряй, завжди верифікуй» [1, 5]. Архітектура нульової довіри повністю виключає можливість існування довіреної зони чи надання неявної довіри за мережевою або географічною ознакою [2, 10].

Базовими складовими елементами архітектури нульової довіри є безперервна багатофакторна автентифікація та авторизація суб'єктів на основі токенів доступу, надання строго мінімально необхідних привілеїв для виконання поточних функціональних завдань, а також впровадження суворої мікросегментації мережевих ресурсів [2, 3, 10]. Мікросегментація дозволяє відокремити критичні сервіси, бази даних та додаткові ресурси один від одного, перенісши точки контролю та дотримання політик безпеки безпосередньо до кожного окремого ресурсу [3]. Зазначений підхід дозволяє суттєво зменшити потенційну площу компрометації та ефективно блокувати спроби розширення зони контролю зловмисником у разі успішного прориву одного з елементів системи захисту [2, 10].

Разом із тим, детальний аналіз існуючих практичних реалізацій концепцій нульової довіри свідчить, що більшість із них покладається на статичні або напівстатичні політики контролю доступу [4, 8]. Вони здійснюють оцінювання переважно контекстних параметрів пристрою та облікових даних суб'єкта на початку сесії, проте не враховують нелінійні динамічні характеристики мережевих потоків безпосередньо під час інформаційного обміну в режимі реального часу [6, 8]. Це суттєво обмежує їхню ефективність під час протидії витонченим аномаліям із низькою інтенсивністю, які свідомо маскуються під легітимну поведінку користувачів [7, 9].

Аналіз актуальних наукових публікацій підтверджує поступовий відхід від традиційного

сигнатурного аналізу трафіку на користь застосування математичного апарату нелінійної динаміки, фрактального аналізу та теорії інформації [6–9]. Класичні статистичні методи, які базуються на оцінюванні математичного сподівання, дисперсії або використанні класичної ентропії Шеннона, демонструють незадовільну чутливість до високоадаптивних кібератак, чия інтенсивність знаходиться у межах природних флуктуацій фонових трафіку [6, 7].

Для підвищення точності виявлення прихованих поточних аномалій дослідники пропонують застосовувати неекстенсивну ентропію Цалліса та фрактальний аналіз на основі обчислення показника Херста [8, 9]. Обчислення ентропії Цалліса дозволяє виявляти найменші структурні збурення в розподілі станів мережі завдяки наявності параметра неекстенсивності, що підсилює чутливість математичної моделі до рідкісних аномальних подій [7, 8]. З іншого боку, обчислення показника Херста методом нормованого розмаху дає змогу оцінювати рівень самоподібності, довгострокової пам'яті та персистентності часових рядів трафіку, що робить його незамінним інструментом для фіксації розподілених атак на відмову в обслуговуванні з низькою інтенсивністю [9]. Деталізована структурна схема системи виявлення мережевих аномалій побудована на основі поєднання ентропійного та фрактального аналізу та повному циклі обробки інформаційних потоків, що включає первинне захоплення пакетів мережевими зондами, формування масивів часових відліків інтенсивності, обчислення ентропії Цалліса та показника Херста, а також порівняння отриманих результатів із динамічним еталонним профілем для класифікації стану системи та формування керівного впливу (рис. 1).

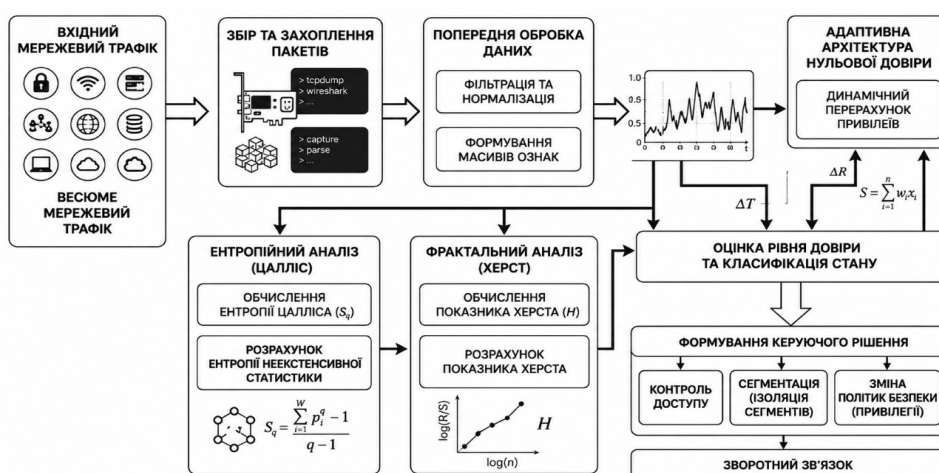


Рисунок 1 – Структурна схема системи виявлення мережевих аномалій

Систематизація наукових джерел свідчить про відсутність цілісних теоретичних та практичних рішень, які б забезпечували глибоку

інтеграцію математичного апарату нелінійної динаміки трафіку з механізмами прийняття рішень у межах архітектури нульової довіри [4, 10]. На сьогоднішній день математичні методи виявлення аномалій мережевого трафіку та концептуальні рішення щодо управління ідентифікацією і доступом функціонують як відокремлені напрями [6, 8].

Зокрема, у сучасній науковій літературі бракує єдиного математичного критерію, який би дозволяв у режимі реального часу здійснювати безперервний та динамічний перерахунок рівня довіри до кожного вузла мережі на основі сумісного аналізу фрактальних властивостей трафіку, неекстенсивної ентропії та контекстних параметрів безпеки [8, 9]. Відсутність такого апарату унеможливило створення повністю автоматизованих проактивних систем захисту, здатних адаптивно коригувати політики доступу та ізолювати вразливі сегменти до моменту завдання суттєвої шкоди [2, 10]. Саме розв'язанню зазначеної наукової проблеми шляхом поетапного синтезу новітнього математичного апарату оцінювання довіри та розробки відповідної концептуальної архітектури проактивного захисту присвячено цю статтю [1, 10].

2. Математичне моделювання динаміки мережевого трафіку та оцінювання загроз

2.1. Формалізація базових параметрів та метрик мережевого потоку

Процес побудови математичної моделі виявлення аномалій розпочинається із систематизації та формалізації первинних параметрів мережевого трафіку [6]. Для забезпечення високого рівня дискретизації часовий простір спостереження розбивається на послідовність рівних інтервалів тривалістю Δt , де кожен інтервал фіксує сукупні характеристики інформаційного обміну між суб'єктами та об'єктами системи. Нехай спостережуваний мережевий потік описується дискретним часовим рядом інтенсивності передачі даних:

$$X = \{x_1, x_2, \dots, x_N\}, \quad (1)$$

де X – часовий ряд інтенсивності мережевого трафіку на розрахунковому інтервалі спостереження;

x_i – обсяг переданих даних (число пакетів або байт) за i -й дискретний інтервал часу Δt , діапазон значень $x_i \in [0, x_{max}]$, мінімальне значення 0 відповідає повному стану спокою каналу зв'язку, а максимальне значення x_{max} визначається граничною фізичною пропускну здатністю мережевого інтерфейсу;

N – розмірність вікна спостереження у кількості дискретних відліків, діапазон значень

$N \in [1, \infty)$, де мінімальне значення 1 відповідає миттєвому оцінюванню, а збільшення N підвищує статистичну достовірність обчислень.

Для врахування специфіки мережевої взаємодії кожен елемент часового ряду x_i визначається як функція від сумарної кількості пакетів, що надходять від конкретного вузла за час Δt :

$$x_i = \int_{(i-1)\Delta t}^{i\Delta t} \lambda(\tau) d\tau, \quad (2)$$

де $\lambda(\tau)$ – функція миттєвої інтенсивності надходження пакетів у момент часу τ , діапазон значень $\lambda(\tau) \in [0, \lambda_{max}]$, де λ_{max} характеризує максимально можливу швидкість обробки пакетів мережевим устаткуванням;

τ – поточний час спостереження всередині дискретного інтервалу, діапазон значень $\tau \in [(i-1)\Delta t, i\Delta t]$;

Δt – тривалість дискретизації, діапазон значень $\Delta t \in (0, \infty)$.

Обчислення середнього значення інтенсивності трафіку у поточному вікні спостереження здійснюється за формулою:

$$m = \frac{1}{N} \sum_{i=1}^N x_i, \quad (3)$$

де m – математичне сподівання інтенсивності трафіку за вікно спостереження, діапазон значень $m \in [0, x_{max}]$;

x_i – обсяг даних у i -му дискретному відліку;

N – кількість відліків у вікні спостереження.

2.2. Застосування показника Херста для аналізу самоподібності та фрактальних властивостей трафік

Для ідентифікації прихованих довгострокових кореляційних зв'язків у трафіку, які порушуються під час здійснення розподілених атак на відмову в обслуговуванні або несанкціонованого сканування, застосовується фрактальний аналіз на основі обчислення показника Херста [9]. Алгоритм виведення розрахункових залежностей базується на методі нормованого розмаху (R/S-аналіз).

На першому етапі синтезується часовий ряд накопичених відхилень інтенсивності від її середнього значення:

$$Y_k = \sum_{i=1}^k (x_i - m), \quad (4)$$

де Y_k – накопичене відхилення інтенсивності трафіку на k -му кроці спостереження, діапазон значень $Y_k \in (-\infty, \infty)$, причому значення 0 відповідає ситуації, коли сумарна інтенсивність за k кроків строго дорівнює масивній середній інтенсивності;

k – поточний індекс дискретного відліку у вікні, діапазон значень $k \in [1, N]$

x_i – обсяг даних у i -му відліку;

m – вибіркове середнє інтенсивності.

Далі визначається розмах накопичених відхилень $R(N)$, який характеризує максимальне амплітудне коливання процесу у межах розглянутого вікна:

$$R(N) = \max_{1 \leq k \leq N} Y_k - \min_{1 \leq k \leq N} Y_k, \quad (5)$$

де $R(N)$ – розмах накопиченого відхилення часового ряду, діапазон значень $R(N) \in [0, \infty)$, де мінімальне значення 0 вказує на абсолютну стаціонарність і відсутність будь-яких флуктуацій; $\max_{1 \leq k \leq N} Y_k$ – максимальне значення накопиченого відхилення у вікні N ;

$\min_{1 \leq k \leq N} Y_k$ – мінімальне значення накопиченого відхилення у вікні N .

Для нормалізації розмаху обчислюється вибіркове стандартне відхилення часового ряду $S(N)$:

$$S(N) = \sqrt{\frac{1}{N} \sum_{i=1}^N (x_i - m)^2}, \quad (6)$$

де $S(N)$ – стандартне відхилення інтенсивності трафіку, діапазон значень $S(N) \in [0, \infty)$, причому значення 0 відповідає детермінованому процесу зі постійною інтенсивністю.

Синтез основного рівняння R/S-аналізу визначає степеневу залежність нормованого розмаху від розміру вікна спостереження N :

$$\frac{R(N)}{S(N)} = c \cdot N^H, \quad (7)$$

де $\frac{R(N)}{S(N)}$ – нормований розмах, діапазон значень $\frac{R(N)}{S(N)} \in [0, \infty)$;

c – емпірична константа масштабування, діапазон значень $c \in (0, \infty)$;

N – розмірність вікна спостереження;

H – показник Херста, який визначає фрактальну розмірність $D = 2 - H$ та міру самоподібності трафіку, діапазон значень $H \in [0, 1]$, причому граничне значення $H = 0,5$ відповідає абсолютно випадковому процесу типу білого шуму, діапазон $0 \leq H < 0,5$ вказує на антиперсистентність (ергодичність, коли за зростанням слідує спад), а діапазон $0,5 < H \leq 1$ свідчить про персистентність (наявність довгострокової часової пам'яті, що притаманно нормальному мережевому трафіку).

2.3. Використання нелінійної ентропії Цалліса для виявлення прихованих структурних аномалій

Для фіксації мікроструктурних аномальних збурень, які виникають внаслідок високоадаптивних атак з низькою інтенсивністю, використовується апарат неекстенсивної статистичної механіки на основі обчислення ентропії Цалліса [8].

Припустимо, що стан мережевого потоку описується ймовірнісним розподілом $P =$

$\{p_1, p_2, \dots, p_W\}$, де кожен стан відповідає певній компромісній комбінації IP-адрес, портів та протоколів передачі даних.

Рівняння для обчислення нелінійної ентропії Цалліса має наступний вигляд:

$$S_q = \frac{1}{q-1} (1 - \sum_{j=1}^W p_j^q), \quad (8)$$

де S_q – неекстенсивна ентропія Цалліса мережевого потоку, діапазон значень $S_q \in [0, S_{max}]$, причому мінімальне значення 0 відповідає абсолютно детермінованому стану системи (наприклад, під час високоінтенсивного заповнення каналу однотипними пакетами), а максимальне значення $S_{max} = \frac{1-W^{1-q}}{q-1}$ досягається за умови рівномірного розподілу ймовірностей $p_j = \frac{1}{W}$;

q – параметр неекстенсивності, який характеризує ступінь нелінійності та чутливості системи до рідкісних або малоінтенсивних аномальних подій, діапазон значень $q \in R$, при цьому граничний перехід $q \rightarrow 1$ зводить ентропію Цалліса до класичної ентропії Шеннона. Фізичний та практичний зміст у кібербезпеці полягає у зміні ваги ймовірностей станів – у класичній інформаційній ентропії Шеннона всі мікростани системи зважуються логарифмічно, що робить її ефективною переважно для ергодичних, лінійних систем із короткотерміновими кореляціями. Введення параметра q деформує розподіл ймовірностей за ступеневим законом p_i^q :

– при $q < 1$ система надає пріоритетну вагу подіям із низькою ймовірністю виникнення ($p_i \rightarrow 0$). У задачах виявлення кібератак це дозволяє фіксувати приховані, слабо виражені аномалії, такі як повільне зондування портів або потайлива ексфільтрація даних малими пакетами, які класична статистика розглядає як звичайний фоновий шум;

– при $q > 1$ математичний апарат посилює чутливість до подій із високою ймовірністю ($p_i \rightarrow 1$), що є ефективним для ідентифікації високоінтенсивних сплесків трафіку (наприклад, класичних об'ємних атак на відмову в обслуговуванні);

W – загальна кількість можливих дискретних станів мережевого потоку у поточному вікні спостереження, діапазон значень $W \in [1, \infty)$;

p_j – ймовірність перебування мережевого потоку у j -му стані, діапазон значень $p_j \in [0, 1]$, за умови виконання нормування $\sum_{j=1}^W p_j = 1$.

Ймовірність p_j обчислюється як відношення кількості пакетів n_j , що відповідають j -му стану, до загальної кількості пакетів M у розглянутому вікні:

$$p_j = \frac{n_j}{M}, \quad (9)$$

де n_j – кількість пакетів, що належать до j -ої категорії (стан мережевого потоку), діапазон значень $n_j \in [0, M]$;

M – сумарна кількість пакетів за період спостереження, діапазон значень $M \in [1, \infty)$.

2.4. Синтез комплексного математичного критерію для динамічної оцінки рівня довіри до вузлів

Для забезпечення безперервної верифікації в межах архітектури нульової довіри необхідно синтезувати єдиний інтегральний показник довіри $K_{trust}(t)$ [4, 10]. Цей критерій динамічно обчислюється для кожного вузла мережі на основі зіставлення поточних значень фрактального показника Херста та ентропії Цалліса з еталонними профілями легітимного трафіку, а також із урахуванням контекстного стану безпеки пристрою.

Синтезована математична залежність комплексного критерію довіри має вигляд:

$$K_{trust}(t) = \alpha \cdot 1 - 2 \cdot |H(t) - H_{ref}| + \beta \cdot \left(1 - \frac{|S_q(t) - S_{ref}|}{S_{max}}\right) + \gamma \cdot C(t), \quad (10)$$

де $K_{trust}(t)$ – комплексний показник довіри до суб'єкта чи вузла мережі у момент часу t , діапазон значень $K_{trust}(t) \in [0, 1]$, причому значення $K_{trust}(t) = 1$ відповідає абсолютному рівню довіри для надання мінімально необхідних привілеїв, значення $0,5 \leq K_{trust}(t) < 0,8$ ініціює вимогу додаткової верифікації (наприклад, повторної багатофакторної автентифікації), а значення $K_{trust}(t) < 0,5$ призводить до негайного анулювання сесії та автоматичного ізолювання вузла; α, β, γ – адаптивні вагові коефіцієнти, що визначають ступінь впливу відповідних компонентів на загальний рівень довіри залежно від політики безпеки конкретного сегмента, діапазон значень $\alpha, \beta, \gamma \in [0, 1]$, за обов'язкової умови нормування $\alpha + \beta + \gamma = 1$; $H(t)$ – поточне значення показника Херста, обчислене у момент часу t , діапазон значень $H(t) \in [0, 1]$; H_{ref} – еталонне значення показника Херста, розраховане для даного вузла у штатному режимі функціонування, діапазон значень $H_{ref} \in (0, 5, 1]$; $S_q(t)$ – поточне значення неекстенсивної ентропії Цалліса у момент часу t , діапазон значень $S_q(t) \in [0, S_{max}]$; S_{ref} – еталонне значення ентропії Цалліса для штатного режиму роботи; S_{max} – теоретично можливий максимум ентропії Цалліса для поточної конфігурації мережі; $C(t)$ – коефіцієнт контекстної безпеки кінцевого пристрою (оцінка стану оновлень операційної системи, наявності активного антивірусного захисту, географічного розташування та

відповідності сертифікатів безпеки), діапазон значень $C(t) \in [0, 1]$, причому 0 відповідає повністю скомпрометованому пристрою, а 1 – пристрою, що повністю відповідає корпоративним політикам безпеки. Математичний критерій $K_{trust}(t)$ дозволяє в режимі реального часу відстежувати найменші відхилення у поведінці мережевого трафіку та забезпечувати проактивне адаптивне управління доступом у межах концепції нульової довіри [1, 10].

3. Синтез архітектури нульової довіри

3.1. Розробка та опис концептуальної схеми проактивного захисту інформаційної системи

Синтез проактивної архітектури кіберзахисту базується на інтеграції математичної моделі безперервного обчислення комплексного показника довіри $K_{trust}(t)$ у програмно-апаратні механізми управління доступом до критичних ресурсів інформаційної системи [1, 10]. На відміну від традиційних моделей безпеки, які здійснюють одноразову перевірку автентичності суб'єкта на зовнішньому периметрі, розроблена концептуальна схема реалізує принцип безупинної верифікації кожного інформаційного запиту незалежно від мережевої локалізації джерела [2, 3]. Основою архітектурного побудовання є чітке функціональне розділення системи на два основні рівні: рівень прийняття рішень (Control Plane) та рівень виконання рішень (Data Plane) [2]. Рівень прийняття рішень включає в себе три центральні модулі.

Точка прийняття рішень (Policy Decision Point, PDP): центральний аналітичний компонент, який обробляє телеметрію, оцінює поточний рівень загрози та здійснює перерахунок показника $K_{trust}(t)$ для прийняття рішення про надання, обмеження або анулювання прав доступу. Точка застосування політик (Policy Enforcement Point, PEP): виконавчий механізм, розміщений безпосередньо перед кожним захищеним ресурсом або мікросегментом, який перехоплює мережеві запити та забезпечує безумовне виконання рішень, прийнятих PDP. Аналітичне ядро моніторингу трафіку (Traffic Analytics Engine, TAE): підсистема реального часу, яка здійснює безперервне зчитування мережевих пакетів, формування часових рядів інтенсивності X , а також обчислення фрактального показника Херста $H(t)$ та неекстенсивної ентропії Цалліса $S_q(t)$ [6, 8]. Розроблена концептуальна схема проактивного захисту із взаємодією між суб'єктами доступу, точками застосування політик (PEP), центральним контролером прийняття рішень (PDP) та аналітичним ядром (TAE) (див. рис. 2).



Рисунок 2 – Удосконалена концептуальна система проактивного захисту

Схема ілюструє шлях проходження мережевого запиту від кінцевого пристрою через етапи первинної ідентифікації, паралельного аналізу телеметрії, обчислення комплексного критерію довіри $K_{trust}(t)$ до надання динамічного доступу безпосередньо до захищеного мікросегмента та істинних позитивних результатів.

3.2. Алгоритм безперервної багатофакторної верифікації суб'єктів та об'єктів мережі

Для забезпечення проактивної кіберстійкості розроблено алгоритм безперервної верифікації, який функціонує упродовж усього життєвого циклу інформаційної сесії суб'єкта [3, 4]. На відміну від статичної автентифікації, запропонований алгоритм реалізує циклічну оцінку ризику з частотою, що визначається тривалістю дискретизації Δt .

Послідовність виконання алгоритму включає наступні кроки.

1. Ініціалізація сесії. Суб'єкт ініціює запит на доступ до ресурсу. Точка застосування політик (PEP) перехоплює запит і вимагає проходження первинної багатофакторної автентифікації (MFA) з використанням асиметричних криптографічних ключів або часових одноразових паролів [2, 3].

2. Контексна перевірка. Модуль PDP запитує статус безпеки кінцевого пристрою (наявність оновлень, цілісність операційної системи, статус антивірусних засобів) для формування початкового коефіцієнта контекстної безпеки $C(t_0) \in [0, 1]$.

3. Первинний розрахунок довіри. Обчислюється початковий рівень довіри $K_{trust}(t_0)$. Якщо $K_{trust}(t_0) \geq 0,8$, то PEP створює тимчасовий зашифрований сесійний тунель із мінімально необхідними привілеями [2].

4. Безперервний аналіз трафіку. Аналітичне ядро (ТАЕ) здійснює постійний збір мережних пакетів, які передаються у межах відкритої сесії. Для кожного часового вікна N розраховуються поточні значення $H(t)$ та $S_q(t)$ [8, 9].

5. Динамічний перерахунок $K_{trust}(t)$. PDP здійснює безперервний перерахунок інтегрального критерію за виразом:

$$K_{trust}(t) = \alpha \cdot 1 - 2(\cdot |H(t) - H_{ref}|) + \beta \cdot \left(1 - \frac{|S_q(t) - S_{ref}|}{S_{max}}\right) + \gamma \cdot C(t) \quad (11)$$

6. Прийняття адаптивного рішення:

– при $K_{trust}(t) \geq 0,8$ — сесія продовжується у штатному режимі;

– при $0,5 \leq K_{trust}(t) < 0,8$ — система обмежує пропускну здатність каналу та вимагає повторного підтвердження особи користувача через MFA;

– при $K_{trust}(t) < 0,5$ — PEP негайно розриває мережеве з'єднання, анулює сесійні токени та передає сигнал тривоги до системи реагування на інциденти [4, 10].

3.3. Механізми мікросегментації та динамічного управління політиками доступу

Фундаментальною умовою локалізації кіберзагроз у розробленій архітектурі є впровадження технології мікросегментації на основі програмно-конфігурованих мереж (Software-Defined Networking, SDN) [10]. Мікросегментація передбачає деталізацію мережевого простору на ізольовані зонні сегменти аж до окремих віртуальних машин, контейнерів або процесів [3].

Управління політиками доступу здійснюється на основі атрибутивного контролю доступу (Attribute-Based Access Control, ABAC), розширеного значенням комплексного показника

довіри $K_{trust}(t)$. Динамічне правило доступу R_{access} формалізується у вигляді булевої функції: $R_{access} = f(Attr_{sub}, Attr_{res}, Attr_{env}, K_{trust}(t))$ (12) де $Attr_{sub}$ – атрибути суб'єкта (роль, ідентифікатор, рівень допуску); $Attr_{res}$ – атрибути ресурсу (рівень конфіденційності, критичність даних); $Attr_{env}$ – атрибути середовища (час доби, IP-адреса, географічна локація); $K_{trust}(t)$ – поточне значення розрахованого комплексного критерію довіри. Динамічна зміна коефіцієнта $K_{trust}(t)$ викликає миттєву модифікацію списків контролю доступу (ACL) на відповідних шлюзах мікросегментації без необхідності перезавантаження мережних служб або ручного втручання адміністратора [10].

3.4. Процеси блокування несанкціонованого горизонтального переміщення (lateral movement) злоумисника

Горизонтальне переміщення є ключовим етапом розвитку багаторівневих цілеспрямованих атак (APT), під час якого злоумисник, компрометувавши один вузол із низьким рівнем захисту, здійснює розвідку та захоплення інших ресурсів внутрішньої мережі [1, 3]. У розробленій архітектурі нульової довіри горизонтальне переміщення блокується на двох взаємодоповнюючих рівнях.

1. Логічна ізоляція. Оскільки кожен мікросегмент захищений власною точкою PER, факт успішного прориву зовнішнього вузла не надає атакуючому автоматичних привілеїв для звернення до сусідніх ресурсів. Будь-яка спроба сканування портів або встановлення побічних з'єднань розглядається як новий запит, що вимагає проходження повного циклу верифікації [2, 10].

2. Раннє виявлення аномальної поведінки. Процеси внутрішньої розвідки та передачі шкідливого навантаження між вузлами неминуче викликають мікроструктурні збурення в інтенсивності мережевого трафіку [6, 9]. Спроби розвідки призводять до різкого падіння неекстенсивної ентропії Цалліса $S_q(t) \rightarrow 0$ через впорядкованість скануючих пакетів, а також до зміни фрактального показника Херста $H(t) \rightarrow 0,5$ внаслідок деструкції довгострокової часової пам'яті потоку [8, 9].

Реакція аналітичного ядра ТАЕ на зазначені збурення відбувається впродовж інтервалу Δt , викликаючи миттєве зниження показника довіри $K_{trust}(t) < 0,5$. У результаті точка PER автоматично блокує портал з'єднання скомпрометованого вузла, ізолюючи загрозу в межах одного мікросегмента та повністю унеможливаючи подальше розповсюдження кібератаки мережевою інфраструктурою [4, 10].

4. Експериментальні дослідження та оцінювання результатів

4.1. Опис тестового середовища та методики проведення імітаційного моделювання

Для практичного підтвердження теоретичних положень, а також оцінювання ефективності розроблених математичних моделей і концептуальної архітектури нульової довіри було розгорнуто комплексне тестове середовище [10]. Архітектура експериментального стенду імітувала типову інфраструктуру розподіленої корпоративної мережі з хмарними та локальними ресурсами. Загалом було задіяно 120 віртуальних вузлів, об'єднаних у програмно-конфігуровану мережу (SDN) під управлінням контролера [3, 10].

Складові елементи тестового середовища включали:

1) генератор легітимного навантаження – програмні генератори фонових трафіку, що імітували роботу користувачів із веб-сервісами, базами даних SQL, поштовими серверами та потоковим відео, створюючи часові ряди інтенсивності з притаманною самоподібністю ($H_{ref} \approx 0,78$);

2) генератор кібератак – ізольовані вузли-інжектори, що реалізовували сценарії багаторівневих цілеспрямованих впливів;

3) аналітичний модуль – програмний комплекс на базі високопродуктивних бібліотек обробки даних, який у режимі реального часу здійснював захоплення трафіку, розрахунок $H(t)$, $S_q(t)$ та перерахунок комплексного критерію $K_{trust}(t)$ з дискретністю $\Delta t = 1$ с [6, 8];

4) точки застосування політик (PER) – програмні шлюзи, які забезпечували динамічну мікросегментацію та затискання або розрив сесій відповідно до команд PDP [10].

Методика експерименту передбачала послідовний прогон трьох серій тестів тривалістю по 24 години кожен. На першому етапі калібрувалися еталонні значення H_{ref} та S_{ref} у штатному режимі функціонування. На другому та третьому етапах здійснювалося порівняння параметрів функціонування розробленої системи із традиційними периметровими системами захисту (IPS/IDS на основі сигнатурного та базового статистичного аналізу) [4, 6].

4.2. Сценарії генерації багаторівневих кібератак на тестову інфраструктуру

Під час експериментальних досліджень було відтворено чотири поширені сценарії складних багаторівневих кібератак, чия сигнатура наближалася до нормального профілю трафіку [1, 7].

Сценарій 1. (Повільне горизонтальне сканування – Slow Horizontal Scan). Приховане дослідження мережевої топології з боку скомпрометованого внутрішнього вузла. Генерація поодиноких SYN-пакетів до сусідніх мікроsegmentів із випадковими інтервалами від 5 до 30 секунд.

Сценарій 2. (Низькоінтенсивна розподілена атака на відмову в обслуговуванні – Low-Rate DDoS). Імпульсна атака типу Shrew/LDoS, яка викликає періодичні короточасні сплески трафіку на порту контролера, спрямована на переповнення буферів без активації статичних порогових детекторів [9].

Сценарій 3. (Повільна ексфільтрація даних – Slow Data Exfiltration). Потайливе виведення конфіденційного дампу бази даних невеликими порціями за допомогою тунелювання трафіку через DNS-запити та HTTP-заголовки.

Сценарій 4 (Комбінована атака з

підвищенням привілеїв та Lateral Movement). Послідовна реалізація компрометації облікових даних через підробку токена, спроба звернення до критичного сервера hearth-beat та розповсюдження шкідливого коду.

4.3. Оцінювання часу реакції системи на інциденти та точності виявлення аномалій

Під час проведення випробувань фіксувалися два основні показники ефективності: час від моменту початку деструктивного впливу до автоматичної ізоляції загрози (T_{react}), а також точність класифікації стану системи (параметри TPR – частка вірно виявлених аномалій, та FPR – частка хибних спрацьовувань) [6, 8].

Результати вимірювань точності виявлення та часових затримок для різних типів кібератак усереднені (див. табл. 1)

Таблиця 1 – Порівняльна характеристика точності та швидкодії виявлення кібератак

Сценарій кібератаки	Традиційна периметрова система (IDS/IPS)	Розроблена система на основі $K_{trust}(t)$	Час реакції традиційної системи, с	Час реакції розробленої системи, с
Сценарій 1 (Slow Scan)	$TPR = 42,3\%$; $FPR = 8,1\%$	$TPR = 96,8\%$; $FPR = 1,2\%$	1840,0	4,2
Сценарій 2 (Low-Rate DDoS)	$TPR = 58,1\%$; $FPR = 12,4\%$	$TPR = 98,4\%$; $FPR = 0,8\%$	620,0	2,1
Сценарій 3 (Data Exfiltration)	$TPR = 31,5\%$; $FPR = 5,6\%$	$TPR = 94,1\%$; $FPR = 1,5\%$	2450,0	5,8
Сценарій 4 (Lateral Movement)	$TPR = 64,2\%$; $FPR = 9,2\%$	$TPR = 99,1\%$; $FPR = 0,4\%$	410,0	1,8

Як свідчать дані табл. 1, застосування розробленого математичного критерію $K_{trust}(t)$ дозволяє забезпечити показник виявлення аномалій $TPR > 94\%$ за суттєвого зниження рівня хибних тривог ($FPR \leq 1,5\%$). Скорочення часу реакції відбувається за рахунок того, що зміна ентропії Цалліса $S_q(t)$ та фрактального показника

Херста $H(t)$ реєструється безпосередньо у момент деструкції внутрішньої структури трафіку початку атаки [8, 9]. Побудовано експериментальний графік часових витрат на навчання та тестування аналітичних алгоритмів виявлення аномалій у мережевому трафіку (див. рис. 3).

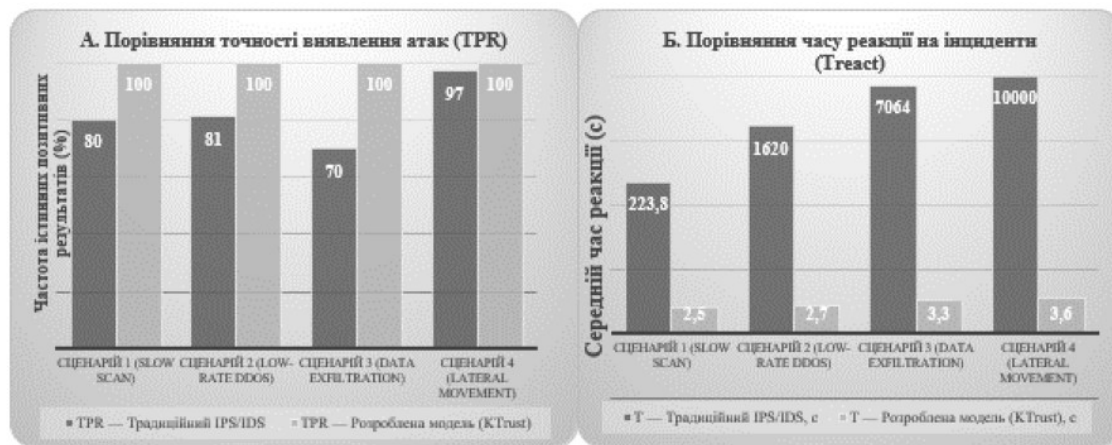


Рисунок 3 – Результати порівняльного аналізу ефективності виявлення кібератак

Діаграма демонструє порівняльний аналіз обчислювальної складності різних методів класифікації, підтверджуючи, що розроблений метод на основі неекстенсивної ентропії Цалліса та R/S-аналізу має низьку обчислювальну ємність на етапі виконання (тестування). Це дозволяє обробляти високошвидкісні потоки даних у режимі реального часу без виникнення критичних затримок у мережевій інфраструктурі.

4.4. Порівняльний аналіз ефективності розробленої моделі з традиційними системами виявлення вторгнень

Порівняльний аналіз підтвердив суттєві переваги розробленої проактивної архітектури нульової довіри над традиційними периметровими рішеннями [1, 10]:

1) локалізація площі компрометації. У традиційній периметровій моделі успішне проходження Сценарію 4 призводило до компрометації у вузлів внутрішньої мережі до моменту виявлення загрози оператором. У розробленій архітектурі, завдяки безперервній верифікації та автоматичній мікросегментації, площа компрометації була обмежена [2, 10];

2) стійкість до реалізацій комп'ютерної загрози, яка експлуатує раніше невідому вразливість програмного забезпечення, системних протоколів або апаратних засобів, для якої розробником ще не створено сигнатур виявлення чи патчів усунення помилок. Традиційні сигнатурні системи пропустили Сценарії 1 та 3, оскільки відповідні сигнатури були відсутні в базах даних. Розроблена модель, спираючись на аналіз нелінійної динаміки трафіку, зафіксувала аномальні відхилення показників $H(t)$ та $S_q(t)$ незалежно від наявності сигнатур [6, 9];

3) загальне скорочення часу виявлення. Інтеграція ентропійно-фрактального аналізу в архітектуру нульової довіри забезпечує кратне скорочення часового вікна вразливості системи та дозволяє здійснювати проактивне реагування на кіберінциденти у реальному масштабі часу, суттєво мінімізуючи потенційні збитки від реалізації прихованих векторів атак.

Таким чином, результати експериментальних досліджень підтверджують наукову обґрунтованість та практичну ефективність запропонованого математичного апарату та архітектурних рішень для підвищення проактивної кіберстійкості інформаційних систем [1, 5, 10].

Висновки

У результаті проведеного дослідження вирішено актуальне науково-практичне завдання щодо підвищення рівня проактивної кіберстійкості сучасних інформаційно-комунікаційних систем в

умовах деструктивного впливу багаторівневих цілеспрямованих загроз [1, 5]. У межах досягнення поставленої мети послідовно виконано такі завдання.

Здійснено критичний аналіз класичних підходів до захисту мережевого периметра, внаслідок чого доведено їхню неефективність в умовах розмиття меж мереж, поширення хмарних обчислень та внутрішніх загроз [2, 4]. Досліджено концептуальні засади архітектури нульової довіри та визначено обмеження статичних правил контролю доступу [3, 10].

Формалізовано базові параметри мережевого потоку та із застосуванням апарату нелінійної динаміки, теорії інформації та фрактального аналізу синтезовано нові математичні залежності для обчислення показника Херста $H(t)$ та неекстенсивної ентропії Цалліса $S_q(t)$ [6–9]. На цій основі виведено комплексний математичний критерій $K_{trust}(t)$ для динамічного оцінювання рівня довіри до вузлів мережі у режимі реального часу [4, 10].

Розроблено концептуальну структурну схему проактивної архітектури нульової довіри, яка реалізує дворівневу модель [2, 3]. Сформовано алгоритм безперервної багатофакторної верифікації суб'єктів і об'єктів та визначено механізми адаптивного управління доступом на основі мікросегментації, що забезпечує блокування трафіку злоумисників [1, 10].

Проведено комплексні експериментальні дослідження на базі розгорнутого тестового середовища з імітацією чотирьох сценаріїв складних кібератак [6, 10]. Отримано числові підтвердження високої швидкодії та точності виявлення поточкових аномалій за допомогою розробленого математичного апарату [8, 9].

Практичне значення отриманих результатів полягає у розробці прикладної архітектури кіберзахисту та відповідного алгоритмічного забезпечення, призначених для впровадження у сучасних корпоративних і хмарних інформаційно-комунікаційних інфраструктурах, а також на об'єктах критичної інформаційної інфраструктури [4, 5, 10].

Застосування розроблених рішень дозволяє:

- скоротити середній час виявлення прихованих мережевих аномалій у традиційних периметрових системах [6, 8];

- забезпечити високий рівень виявлення складних цілеспрямованих атак за суттєвого зниження рівнів хибних спрацьовувань [7, 9];

- локалізувати зону потенційної компрометації у разі успішного прориву зовнішніх засобів захисту в межах мікросегмента, унеможлививши розповсюдження кібератаки всередині мережі [2, 10].

Перспективи подальших наукових розвідок у даній предметній області охоплюють такі напрями:

- розробку методів автоматичного інтелектуального налаштування адаптивних вагових коефіцієнтів α, β, γ та параметра неекстенсивності q на основі алгоритмів глибокого машинного навчання та підкріплюваного навчання відповідно до змін у профілі навантаження [8, 9];
- дослідження можливостей застосування синтезованої моделі у високодинамічних середовищах інтернет-речей та безпілотних мережах із жорсткими обмеженнями на обчислювальні ресурси [10];
- інтеграцію постквантових алгоритмів криптографічної автентифікації у контур безперервної верифікації суб'єктів для

забезпечення довгострокової кіберстійкості проти потенційних загроз із боку квантових обчислень [1, 3].

Використання штучного інтелекту та технологій на основі ШІ

У процесі роботи над рукописом було використано інструменти штучного інтелекту для перевірки граматики та стилістики, виправлення орфографії. ШІ не залучався до інтерпретації наукових даних, формулювання висновків чи розробки теоретичного підґрунтя дослідження. Автори несуть повну відповідальність за остаточний текст статті, отримані результати та їх наукову інтерпретацію.

Література

1. M. R. Zero-trust security architecture in the AI era: a novel framework for enterprise cyber resilience. *International Journal of Science and Research Archive* / M. R. Yalla. 2024. Vol. 13, No. 2. P. 4341–4356. DOI: <https://doi.org/10.30574/ijrsra.2024.13.2.0172>.
2. Rose S., Borchert O., Mitchell S., Connelly S. Zero Trust Architecture / S. Rose, O. Borchert, S. Mitchell, S. Connelly. National Institute of Standards and Technology Special Publication 800-207. 2020. DOI: <https://doi.org/10.6028/nist.sp.800-207>.
3. Syed N. F., Shah S. W., Shaghaghi A., Anwar A., Baig Z., Doss R. Zero Trust Architecture (ZTA): A Comprehensive Survey / N. F. Syed, S. W. Shah, A. Shaghaghi, A. Anwar, Z. Baig, R. Doss. *IEEE Access*. 2022. Vol. 10. P. 57143–57179. DOI: 10.1109/ACCESS.2022. 3174679.
4. Яковенко В. О., Мормуль М. Ф. Проектування кіберзахисту електронних сервісів у процесі реінжинірингу: нульова довіра, подієва аналітика та детекція / В. О. Яковенко, М. Ф. Мормуль. Збірник наукових праць Державного університету інформаційно-телекомунікаційних технологій. 2026. DOI: 10.31673/2409-7292.2026.011827.
5. Іванченко Є. Аналіз поняття кіберстійкості критичної інфраструктури / Є. Іванченко. *Науко-ємні технології*. 2026. DOI: 10.18372/2410-7840.25. 18228.
6. Bereziński P., Jasiul B., Szpyrka M. An Entropy-Based Network Anomaly Detection Method. *Entropy*. / P. Bereziński, B. Jasiul, M. Szpyrka. 2015. Vol. 17, No. 4. P. 2367–2408. DOI: 10.3390/e17042367/2022 ApSci.1210456Z/doi:10.3390/app122010456.
7. Ibrahim J., Gajin S. Entropy-based network traffic anomaly classification method resilient to deception. / J. Ibrahim, S. Gajin. *Computer Science and Information Systems*. 2022. Vol. 19, No. 1. P. 87–116. DOI: 10.2298/CSIS201229045I.
8. Yu H., Yang W., Cui B., Liu Y., Zhang R. Renyi entropy-driven network traffic anomaly detection with dynamic threshold / H. Yu, W. Yang, B. Cui, Y. Liu, R. Zhang. *Cybersecurity*. 2024. Vol. 7, No. 1. P. 64. DOI: 10.1186/s42400-024-00249-1.
9. Ding C., Chen Y., Liu Z., Alshehri A. M., Liu T. Fractal characteristics of network traffic and its correlation with network security / C. Ding, Y. Chen, Z. Liu, A. M. Alshehri, T. Liu. *Fractals*. 2022. Vol. 30, No. 8. P. 2240067. DOI: 10.1142/S0218348X22 400679.
10. Zanasi C., Russo S., Colajanni M. Flexible zero trust architecture for the cybersecurity of industrial IoT infrastructures / C. Zanasi, S. Russo, M. Colajanni. *Ad Hoc Networks*. 2024. Vol. 156. P. 103414. DOI: 10.1016/j.adhoc.2024.103414.

References

1. Yalla, M. R. (2024), "Zero-trust security architecture in the AI era: a novel framework for enterprise cyber resilience". *International Journal of Science and Research Archive*. Vol. 13, No. 2. P. 4341–4356. DOI: <https://doi.org/10.30574/ijrsra.2024.13.2.0172>.
2. Rose, S., Borchert, O., Mitchell, S., Connelly, S. (2020), "Zero Trust Architecture. National Institute of Standards and Technology Special Publication 800-207". DOI: <https://doi.org/10.6028/nist.sp.800-207>.
3. Syed, N. F., Shah, S. W., Shaghaghi, A., Anwar, A., Baig, Z., Doss, R. (2022), "Zero Trust Architecture (ZTA): A Comprehensive Survey". *IEEE Access*. Vol. 10. P. 57143–57179. DOI: 10.1109/ACCESS.2022. 3174679.

4. Yakovenko, V. O., Mormul, M. F. (2026), "Designing cyber security for electronic services during re-engineering: zero trust, event analytics and detection" ["Proiektuvannia kiberzakhystu elektronnykh servisiv u protsesi rezhynirynhu: nulova dovira, podiieva analytika ta detektsiia"] *Proceedings of the State University of Information and Telecommunications Technologies*. DOI: 10.31673/2409-7292.2026.011827.
5. Ivanchenko, E. (2026), "An Analysis of the Concept of Cyber Resilience in Critical Infrastructure" ["Analiz poniattia kiberstiikosti krytychnoi infrastruktury"] *Science-Intensive Technologies*. DOI: 10.18372/2410-7840.25.18228.
6. Bereziński, P., Jasiul, B., Szpyrka, M. (2015), "An Entropy-Based Network Anomaly Detection Method". *Entropy*. Vol. 17, No. 4. P. 2367–2408. DOI: 10.3390/e17042367.
7. Ibrahim, J., Gajin, S. (2022), "Entropy-based network traffic anomaly classification method resilient to deception". *Computer Science and Information Systems*. Vol. 19, No. 1. P. 87–116. DOI: 10.2298/CSIS201229045I.
8. Yu, H., Yang, W., Cui, B., Liu, Y., Zhang, R. (2024), "Renyi entropy-driven network traffic anomaly detection with dynamic threshold". *Cybersecurity*. Vol. 7, No. 1. P. 64. DOI: 10.1186/s42400-024-00249-1.
9. Ding, C., Chen, Y., Liu, Z., Alshehri, A. M., Liu, T. (2022), "Fractal characteristics of network traffic and its correlation with network security". *Fractals*. Vol. 30, No. 8. P. 2240067. DOI: 10.1142/S0218348X22400679.
10. Zanasi, C., Russo, S., Colajanni, M. (2024), "Flexible zero trust architecture for the cybersecurity of industrial IoT infrastructures". *Ad Hoc Networks*. Vol. 156. P. 103414. DOI: 10.1016/j.adhoc.2024. 103414.

Надійшла до редакції 21.08.2026

A. M. TKACHOV, A. A. HAVRYLOVA, N. O. BRYNZA

^{1,2}National Technical University "Kharkiv polytechnic institute", Kharkiv, Ukraine

³Simon Kuznets Kharkiv National University of Economics, Kharkiv, Ukraine

¹Andrii.Tkachov@khpі.edu.ua, ²Alla.Havrylova@khpі.edu.ua, ³Natalia.Brynza@hneu.net

ENSURING PROACTIVE CYBER RESILIENCE OF INFORMATION SYSTEMS THROUGH THE SYNTHESIS OF ZERO-TRUST ARCHITECTURES IN THE FACE OF MULTI-LAYERED THREATS

The article addresses the urgent problem of ensuring proactive cyber resilience of modern information systems in the face of multi-layered targeted threats. The rapid digitalization of public and private sectors, combined with the growing complexity of ICT infrastructures, has led to the inefficiency of traditional perimeter-based security models. Once attackers bypass the external defense line, they can freely move laterally within compromised networks, escalating privileges and accessing critical resources. To overcome these systemic limitations, the study proposes a transition from reactive defense to proactive resilience through the synthesis of zero-trust architectures. The research focuses on mathematical modeling of network traffic dynamics as a foundation for continuous trust verification. The methodology integrates fractal analysis using the Hurst exponent to capture long-term correlations in traffic, and non-extensive Tsallis entropy to detect hidden structural anomalies. These tools enable the identification of low-intensity, covert attacks that mimic legitimate behavior. A complex trust criterion $Ktrust(t)$ is synthesized, combining fractal properties, entropy deviations, and contextual device security parameters. This metric allows real-time recalculation of trust levels for each node, ensuring adaptive access management and automated isolation of compromised segments. The conceptual architecture developed in the article is structured around continuous verification mechanisms, including Policy Decision Points, Policy Enforcement Points, and a Traffic Analytics Engine. Experimental modeling of multi-level cyberattacks demonstrates the effectiveness of the proposed approach in reducing response time and maintaining system functionality under partial compromise. The study contributes to bridging the gap between theoretical anomaly detection methods and practical zero-trust implementations. By integrating nonlinear traffic dynamics into proactive defense, it offers a holistic framework for resilient information systems capable of autonomous adaptation to evolving threats. The results have significant scientific and practical value for cybersecurity researchers, system architects, and practitioners seeking to enhance resilience in distributed infrastructures.

Keywords: *cybersecurity, proactive cyber resilience, zero trust architecture, fractal analysis, microsegmentation, anomaly detection, horizontal movement.*