



DOI 10.28925/2663-4023.2026.35.1416

УДК 004.056.53:004.8:004.75

Костюк Юлія Володимирівна

PhD in Computer Science, доцент

доцент кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка

Київський столичний університет імені Бориса Грінченка, м. Київ, Україна

ORCID: 0000-0001-5423-0985

y.kostiuk@kubg.edu.ua

Складанний Павло Миколайович

кандидат технічних наук, доцент

завідувач кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка

Київський столичний університет імені Бориса Грінченка, м. Київ, Україна

ORCID: 0000-0002-7775-6039

p.skladannyi@kubg.edu.ua

**ІНТЕЛЕКТУАЛЬНА СИСТЕМА АДАПТИВНОГО ВИЯВЛЕННЯ КІБЕРЗАГРОЗ НА
ОСНОВІ ГІБРИДНОГО АНАЛІЗУ, НЕЧІТКОЇ ЛОГІКИ ТА НЕЙРОННИХ МЕРЕЖ**

Анотація. У статті досліджено проблему підвищення ефективності виявлення кіберзагроз у сучасних інформаційно-інтелектуальних системах в умовах зростання складності мережових атак, динамічності мережевого середовища та збільшення обсягів мережевого трафіку. Обґрунтовано актуальність використання інтелектуальних методів аналізу кіберподій для забезпечення адаптивного реагування на сучасні кіберзагрози, зокрема атаки нульового дня, DDoS-атаки, мережеві аномалії та модифіковані типи вторгнень. Проведено аналіз сучасних сигнатурних, аномальних і гібридних систем виявлення вторгнень та визначено їх основні недоліки, серед яких високий рівень хибнопозитивних спрацювань, недостатня адаптивність і обмежені можливості виявлення нових типів атак. У роботі запропоновано архітектуру інтелектуальної системи адаптивного виявлення кіберзагроз, яка поєднує сигнатурний та аномальний аналіз із механізмами нечіткої логіки та нейромережевого аналізу в межах єдиної моделі прийняття рішень. Архітектура системи включає модулі збору та попередньої обробки мережевого трафіку, формування вектора ознак, сигнатурного й аномального аналізу, нечіткого оцінювання рівня ризику, нейромережевого аналізу, інтеграції результатів і адаптивного прийняття рішень. Розроблено математичну модель інтегрального оцінювання рівня кіберзагрози на основі адаптивного вагового поєднання результатів різних підсистем аналізу. Запропоновано механізм динамічного налаштування вагових коефіцієнтів залежно від характеристик мережевого трафіку, рівня ризику та типу кіберзагроз. Практичне значення отриманих результатів полягає у можливості використання запропонованої системи для забезпечення кібербезпеки корпоративних мереж, хмарних платформ, автоматизованих систем керування та IoT-середовищ.

Ключові слова: кіберзагрози; система виявлення вторгнень; гібридний аналіз; нечітка логіка; нейронні мережі; інформаційна безпека; адаптивне прийняття рішень; машинне навчання; мережевий трафік; інтелектуальна система.

ВСТУП

В умовах цифрової трансформації та розвитку інформаційно-інтелектуальних систем зростання кількості й складності кіберзагроз підвищує вимоги до захисту комп'ютерних мереж [1, 4, 13, 14, 17]. Особливу небезпеку становлять атаки нульового дня, DDoS-атаки, багатовекторні вторгнення та приховані мережеві аномалії [2, 3, 18]. Сигнатурні IDS ефективні для відомих атак, але обмежені щодо нових і модифікованих загроз, тоді як аномальні підходи здатні їх виявляти, проте характеризуються підвищеним рівнем хибнопозитивних спрацювань [2, 18, 22].

Перспективним напрямом є інтеграція сигнатурного, аномального, нечіткого та нейромережевого аналізу в єдиній адаптивній моделі прийняття рішень [6, 7]. Нечітка логіка забезпечує оцінювання ризику за умов невизначеності [7, 29], а нейронні мережі — виявлення прихованих закономірностей мережевого трафіку [24]. Поєднання цих методів з адаптивним керуванням сприяє підвищенню точності виявлення



атак, зниженню рівня хибнопозитивних спрацювань та оперативному реагуванню на зміни мережевого середовища [10, 12].

Наукова новизна полягає у розробці інтелектуальної системи адаптивного виявлення кіберзагроз, що інтегрує зазначені методи та передбачає динамічне налаштування вагових коефіцієнтів підсистем відповідно до характеристик мережевого трафіку, рівня ризику й типу кіберзагрози. Запропонований підхід орієнтований на корпоративні мережі, хмарні платформи, IoT-середовища, автоматизовані системи керування та критичну інфраструктуру [8, 14, 31].

Постановка проблеми. Стрімкий розвиток інформаційно-комунікаційних технологій, хмарних сервісів, IoT та інформаційно-інтелектуальних систем супроводжується ускладненням кіберзагроз, зокрема атак нульового дня, багатовекторних вторгнень, DDoS-атак і прихованих мережевих аномалій [4, 6, 13, 19, 22]. Традиційні IDS мають обмеження: сигнатурні системи ефективні проти відомих атак, але недостатньо результативні щодо нових загроз, тоді як аномальні здатні їх виявляти, проте характеризуються підвищеним рівнем хибнопозитивних спрацювань [5, 21, 30].

Зростання обсягів і складності мережевого трафіку зумовлює потребу в інтелектуальних методах виявлення прихованих закономірностей, оцінювання ризику та адаптації параметрів системи в реальному часі [24, 25]. Тому актуальним завданням є розробка інтелектуальної системи адаптивного виявлення кіберзагроз на основі гібридного аналізу, нечіткої логіки та нейронних мереж, спрямованої на підвищення точності виявлення атак і зниження рівня хибнопозитивних спрацювань у динамічному мережевому середовищі [6, 24].

Аналіз останніх досліджень і публікацій. Сучасні дослідження інтелектуального виявлення кіберзагроз зосереджені на інтеграції гібридного аналізу, машинного й глибинного навчання та нечіткої логіки для підвищення точності IDS і зменшення кількості хибнопозитивних спрацювань.

M. Ishaque та співавтори запропонували гібридну IDS, що поєднує нечітку логіку для врахування невизначеності, нейронні мережі для прогнозування й класифікації атак та генетичний алгоритм для оптимізації параметрів системи [1]. E. U. H. Qazi, M. H. Faheem та T. Zia розробили модель HDLNIDS на основі згорткових і рекурентних нейронних мереж, яка забезпечує автоматичне виділення ознак мережевого трафіку та класифікацію атак [2]. Подібний підхід реалізовано V. Nnamte та J. Hussain у гібридній DCNN-BiLSTM IDS для багатокласового виявлення мережевих атак [3].

Окремий напрям становлять IDS для IoT-середовищ. M. M. Rahman, S. A. Shakil та M. R. Mustakim систематизували методи аналізу трафіку, виділення ознак і машинного навчання для виявлення атак у ресурсно обмежених IoT-мережах [4]. O. Alnasser та співавтори запропонували поєднання сигнатурного й аномального виявлення для захисту IoT і V2G-комунікацій [5].

Перспективним є також використання нечіткої логіки. X. Qiu, L. Shi та P. Fan розробили кооперативну IDS для IoT, що поєднує нечітку логіку з ансамблем згорткових нейронних мереж і враховує масштабованість та різноманітність атак [6]. A. Karakaya запропонував гібридний підхід на основі ансамблевого навчання та нечіткої логіки, спрямований на гнучке оцінювання рівня безпеки й підвищення інтерпретованості результатів [7].

Водночас аналіз досліджень [1–7] виявив недостатню опрацьованість комплексної інтеграції сигнатурного й аномального аналізу, нечіткого оцінювання ризику, нейромережевої класифікації та адаптивного прийняття рішень у межах єдиної системи. Зокрема, потребують подальшого дослідження механізми динамічного налаштування вагових коефіцієнтів підсистем з урахуванням характеристик мережевого трафіку, рівня ризику та типу кіберзагрози. На вирішення цього наукового завдання спрямоване дослідження.

Мета статті. Метою статті є розробка інтелектуальної системи адаптивного виявлення кіберзагроз на основі гібридного аналізу, нечіткої логіки та нейронних мереж для підвищення точності виявлення атак, зменшення кількості хибнопозитивних спрацювань та забезпечення адаптивного реагування на кіберзагрози в умовах динамічного мережевого середовища.

Для досягнення поставленої мети у роботі необхідно вирішити такі завдання:

- провести аналіз сучасних методів та систем виявлення кіберзагроз, визначити їх переваги, недоліки й обмеження в умовах динамічного мережевого середовища;
- дослідити можливості використання гібридного аналізу, нечіткої логіки та нейронних мереж у системах виявлення вторгнень;
- розробити архітектуру інтелектуальної системи адаптивного виявлення кіберзагроз;
- сформулювати математичну модель інтегрального оцінювання рівня кіберзагрози на основі адаптивного поєднання результатів різних підсистем аналізу;
- розробити нечітку модель оцінювання рівня ризику та механізм адаптивного налаштування параметрів системи;



- реалізувати нейромережевий модуль виявлення аномалій у мережевому трафіку;
- розробити механізм адаптивного прийняття рішень щодо виявлення кіберзагроз;
- провести оцінювання ефективності запропонованої системи та визначити перспективи її практичного застосування для забезпечення кібербезпеки інформаційно-інтелектуальних систем.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

У межах дослідження розглянуто проблему підвищення ефективності виявлення кіберзагроз у сучасних інформаційно-інтелектуальних системах шляхом поєднання сигнатурного та аномального аналізу з методами нечіткої логіки й нейромережевого аналізу [1-4]. Запропонований підхід орієнтований на створення адаптивної інтелектуальної системи, здатної забезпечувати підвищення точності виявлення атак, зменшення кількості хибнопозитивних спрацювань та ефективне реагування на кіберзагрози в умовах динамічного мережевого середовища [2, 6, 18]. У даному розділі наведено архітектуру системи, математичні моделі інтегрального оцінювання рівня кіберзагроз, нечітку модель оцінювання ризику, нейромережевий модуль виявлення аномалій та модель адаптивного прийняття рішень.

Архітектура інтелектуальної системи адаптивного виявлення кіберзагроз

У межах дослідження запропоновано інтелектуальну систему адаптивного виявлення кіберзагроз, що інтегрує сигнатурний, аномальний, нечіткий і нейромережевий аналіз у єдиній моделі прийняття рішень [6]. Система має багаторівневу архітектуру та включає модулі збору й попередньої обробки мережевого трафіку, аналізу, оцінювання ризику, інтеграції результатів та адаптивного прийняття рішень [7, 24]. На початковому етапі здійснюються перехоплення мережевого трафіку, фільтрація й нормалізація даних та формування вектора ознак, що характеризує стан мережевого середовища [21, 27].

Для формалізації процесу аналізу мережевого трафіку введемо вектор ознак, який описує поточний стан мережевого середовища та використовується підсистемами сигнатурного, аномального й нейромережевого аналізу. Вектор ознак мережевого трафіку визначається таким чином:

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

де $X(t)$ – вектор ознак мережевого трафіку, $x_i(t)$ – окремі параметри мережевої активності, n – кількість ознак. До вектора ознак входять інтенсивність трафіку, кількість пакетів, тривалість мережевих сесій, частота ТСР/ІР-з'єднань, кількість помилкових запитів та інші параметри мережевого середовища. Їх багатовимірне представлення формує інформаційну основу для виявлення аномальної та потенційно небезпечної активності.

Сформований вектор ознак надходить до модулів сигнатурного, аномального та нейромережевого аналізу. Сигнатурний модуль ідентифікує відомі атаки за базою сигнатур [18], а аномальний – виявляє відхилення від нормальної поведінки мережі. Нейромережевий модуль на основі LSTM-архітектури виявляє приховані залежності та складні багатовекторні атаки [2, 3, 11]. Результати аналізу разом із нечіткою оцінкою ризику інтегруються для визначення рівня кіберзагрози та формування адаптивного рішення.

На рис. 1 наведено архітектуру інтелектуальної системи адаптивного виявлення кіберзагроз, яка включає модулі збору та попередньої обробки мережевого трафіку, сигнатурного та аномального аналізу, нечіткого оцінювання ризику, нейромережевого аналізу й адаптивного прийняття рішень.



Рис. 1. Архітектура інтелектуальної системи адаптивного виявлення кіберзагроз

Запропонована архітектура забезпечує інтеграцію сигнатурного, аномального, нечіткого та нейромережевого аналізу в межах єдиної адаптивної системи прийняття рішень, що створює основу для формалізації математичної моделі інтегрального оцінювання рівня кіберзагроз.

Математична модель інтегрального оцінювання рівня кіберзагрози

Для забезпечення інтеграції результатів сигнатурного, аномального, нечіткого та нейромережевого аналізу розроблено математичну модель інтегрального оцінювання рівня кіберзагрози [1-2, 6]. Інтегральний рівень загрози визначається як адаптивна вагова комбінація результатів окремих підсистем аналізу:

$$R(t) = a(t)S(x) + \beta(t)A(x) + \gamma(t)F(x) + \delta(t)N(x), \quad (2)$$

де $S(x)$ – результат сигнатурного аналізу, $A(x)$ – результат аномального аналізу, $F(x)$ – нечітка локальна оцінка ризику, $N(x)$ – результат нейромережевого аналізу, $a(t), \beta(t), \gamma(t), \delta(t)$ – адаптивні вагові коефіцієнти. Вагові коефіцієнти нормуються за умовою $a(t) + \beta(t) + \gamma(t) + \delta(t) = 1$, $a(t), \beta(t), \gamma(t), \delta(t) \geq 0$, що забезпечує коректність інтегрального оцінювання.

Для забезпечення коректності інтегрального оцінювання рівень кіберзагрози нормалізується в межах інтервалу від 0 до 1. Нормалізований інтегральний рівень кіберзагрози визначається за формулою:

$$R_n(t) = \frac{R(t) - R_{min}}{R_{max} - R_{min}}, \quad (3)$$

де $R_n(t)$ – нормалізований інтегральний рівень кіберзагрози, $R(t)$ – інтегральний рівень кіберзагрози, R_{min}, R_{max} – мінімальне та максимальне значення інтегрального рівня кіберзагрози. Запропонована нормалізація дозволяє забезпечити узгодженість результатів різних підсистем аналізу та підвищити стабільність процесу прийняття рішень.

Запропонована модель дозволяє враховувати внесок кожної підсистеми залежно від поточного стану мережевого середовища та типу кіберзагроз, що узгоджується із сучасними підходами до побудови адаптивних IDS на основі гібридного аналізу та машинного навчання. Використання адаптивних коефіцієнтів забезпечує можливість динамічного налаштування системи та підвищення її стійкості до змін характеристик мережевого трафіку.

Для візуалізації результатів оцінювання на рис. 2 наведено просторове представлення залежності рівня кіберзагрози від інтенсивності мережевого трафіку та ймовірності виникнення загрози. Просторова структура моделі дозволяє виділити зони низького, середнього та критичного рівня ризику, що забезпечує більш ефективне адаптивне прийняття рішень у процесі виявлення кіберзагроз.

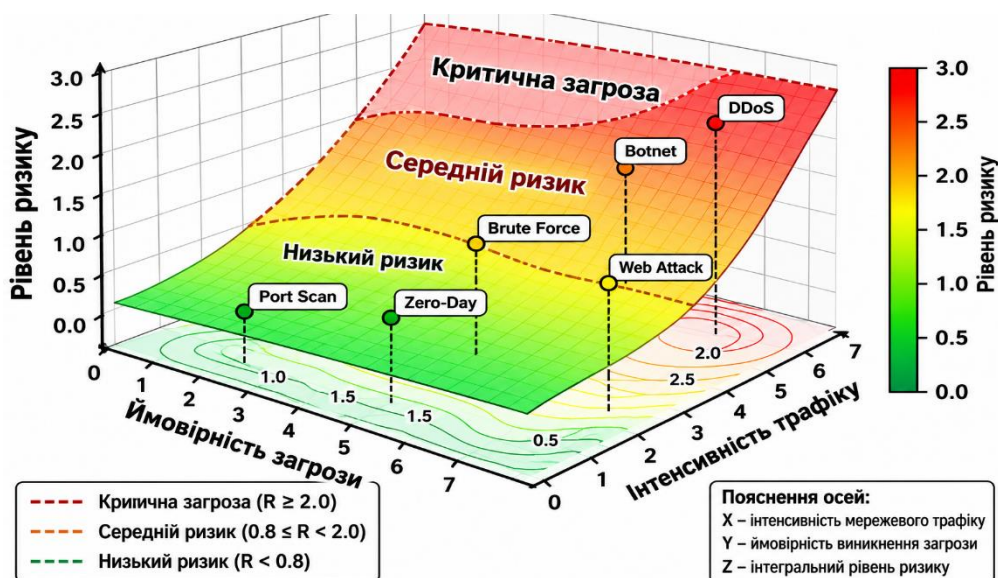


Рис. 2. Просторова адаптивна модель оцінювання кіберзагроз

Для забезпечення адаптивності системи вагові коефіцієнти змінюються залежно від ефективності роботи відповідних підсистем:

$$w_i(t+1) = w_i(t) + \eta(E_i(t) - E_{ref}), \quad (4)$$

де $w_i(t)$ – поточне значення вагового коефіцієнта, η – коефіцієнт адаптації, $E_i(t)$ – поточна ефективність відповідної підсистеми, E_{ref} – еталонне значення точності. Таким чином, система автоматично підвищує



вагу тих підсистем, які забезпечують кращу точність класифікації в поточних умовах функціонування мережі. Після кожного кроку адаптації виконується нормування вагових коефіцієнтів для забезпечення умови $\sum_i w_i(t) = 1$.

Нечітка модель оцінювання рівня ризику

У сучасних мережевих середовищах значна частина параметрів мережевого трафіку характеризується невизначеністю та неповнотою інформації [7, 29]. Для формалізації процесу оцінювання рівня ризику в роботі використано механізм нечіткої логіки.

Нечітка функція належності для оцінювання рівня кіберзагрози має вигляд:

$$\mu_R(x) = \frac{1}{1 + e^{-k(x-c)}}, \quad (5)$$

де x – значення параметра мережевого трафіку, k – коефіцієнт крутизни функції, c – центр функції належності. Нечітка логіка враховує невизначеність параметрів мережевого трафіку та забезпечує гнучкіше оцінювання ризику порівняно з традиційними пороговими методами, що підтверджується дослідженнями інтелектуальних IDS на основі fuzzy-моделей.

Для оцінювання рівня ризику використовуються лінгвістичні змінні: низький ризик; середній ризик; високий ризик; критичний ризик. На основі правил нечіткого висновку формується локальна оцінка ризику $F(x)$, яка використовується під час інтегрального оцінювання рівня кіберзагрози. Для її визначення застосовуються правила нечіткого логічного висновку типу Mamdani.. Приклад правила нечіткої логіки має вигляд:

$$\text{IF Traffic is High AND Anomaly is Critical THEN Threat_Level is Critical}, \quad (6)$$

Використання нечітких правил дозволяє враховувати невизначеність параметрів мережевого середовища та забезпечує більш гнучке оцінювання рівня кіберзагрози порівняно з класичними пороговими методами.

Нейромережевий модуль виявлення аномалій

Для виявлення прихованих атак використано нейромережевий модуль аналізу мережевого трафіку [9, 24], призначений для виявлення складних закономірностей та аномальних залежностей [27]. Глибинна нейронна мережа аналізує вектор ознак, що містить параметри мережевих сесій, інтенсивність трафіку, кількість пакетів, тривалість і частоту з'єднань та характеристики TCP/IP [20–21, 25]. За результатами аналізу визначаються відхилення від нормального профілю активності та оцінюється ймовірність аномальної або несанкціонованої поведінки.

Результатом роботи нейромережевого модуля є оцінка ймовірності аномальної активності:

$$P_{an}(t) = \frac{1}{1 + e^{-z(t)}}, \quad (7)$$

де $P_{an}(t)$ – ймовірність аномалії, $z(t)$ – вихід нейронної мережі. Використання нейромережевого аналізу забезпечує можливість виявлення прихованих та раніше невідомих атак у режимі реального часу.

Для оцінювання ефективності роботи нейромережевого модуля використовується функція середньоквадратичної похибки:

$$E = \frac{1}{n} \sum_{i=1}^n (y_i - \hat{y}_i)^2, \quad (8)$$

де E – середньоквадратична похибка, y_i – реальне значення, $\hat{y}_i$ – прогнозоване значення нейронної мережі, n – кількість спостережень. Мінімізація значення похибки дозволяє підвищити точність класифікації мережевих подій та покращити ефективність виявлення прихованих кіберзагроз.

Навчання та тестування нейромережевого модуля здійснювалися на відкритих наборах CICIDS2017, UNSW-NB15 та CSE-CIC-IDS2018, що містять нормальний трафік і різні типи атак, зокрема DDoS, DoS, Brute Force, Botnet та Web Attacks [13, 30]. Оптимізація ваг нейронної мережі виконується методами зворотного поширення помилки та градієнтного спуску [2–3, 24]. Для аналізу часових залежностей у межах експериментальної реалізації застосовано LSTM-архітектуру. Transformer-моделі з механізмом self-attention розглядаються як перспективний напрям розширення нейромережевого модуля для аналізу складних взаємозв'язків у мережевому трафіку.

Модель адаптивного прийняття рішень

На завершальному етапі функціонування системи формується адаптивне рішення щодо наявності кіберзагрози та необхідної реакції системи. Для цього використовується інтегральна модель прийняття рішень:

$$U(t) = f(R(t), P_{an}(t), C(t)), \quad (9)$$

де $U(t)$ – керувальна дія, $R(t)$ – інтегральний рівень кіберзагрози, $P_{an}(t)$ – ймовірність аномалії, $C(t)$ – критичність інформаційного ресурсу. Залежно від отриманого значення система може: здійснювати пасивний моніторинг; генерувати попередження; блокувати мережеві з'єднання; ізолювати сегменти мережі; ініціювати процедури реагування на кіберінциденти.

Залежно від рівня ризику система адаптивно змінює параметри підсистем, пороги виявлення аномалій і чутливість нейромережевого модуля. За зростання кіберзагрози активується посилений режим моніторингу та реагування, що підвищує ефективність виявлення атак і стабільність системи в динамічному мережевому середовищі [12, 31]. Запропонований підхід поєднує гібридний аналіз, нечітку логіку та нейромережеві технології, забезпечуючи адаптивність системи, зниження хибнопозитивних спрацювань і підвищення точності виявлення відомих та невідомих атак [14, 17, 22]. Це створює основу для інтелектуального адаптивного кіберзахисту корпоративних мереж, хмарних середовищ і автоматизованих систем керування.

На рис. 3 представлено алгоритм функціонування інтелектуальної системи адаптивного виявлення кіберзагроз. Алгоритм відображає послідовність обробки мережевого трафіку, що включає етапи попередньої обробки даних, сигнатурного та аномального виявлення, нечіткого оцінювання ризику й нейромережевого аналізу. На основі інтеграції результатів аналізу система визначає рівень кіберзагрози та приймає адаптивне рішення щодо реагування або подальшого моніторингу мережевого середовища



Рис. 3. Алгоритм функціонування інтелектуальної системи адаптивного виявлення кіберзагроз

Ключовою особливістю алгоритму є адаптивне налаштування вагових коефіцієнтів підсистем відповідно до їх поточної ефективності, що забезпечує динамічне коригування інтегральної оцінки кіберзагрози.

Оцінювання ефективності запропонованої системи

Для оцінювання ефективності запропонованої системи використано основні метрики якості класифікації кіберзагроз, зокрема Precision, Recall та F1-score. Використання зазначених метрик дозволяє комплексно оцінити точність виявлення атак і рівень хибнопозитивних спрацювань.

Точність класифікації визначається за формулою:

$$Precision = \frac{TP}{TP + FP}, \quad (10)$$

де TP – кількість правильно виявлених атак, FP – кількість хибнопозитивних спрацювань.

Повнота виявлення атак визначається таким чином:

$$Recall = \frac{TP}{TP + FN}, \quad (11)$$

де FN – кількість пропущених атак.

Для інтегрального оцінювання ефективності використовується F1-міра:

$$F1 = 2 \cdot \frac{Precision \cdot Recall}{Precision + Recall}, \quad (12)$$

де F1 – інтегральний показник ефективності класифікації, що враховує збалансованість між точністю виявлення атак та повнотою їх класифікації. Використання наведених метрик дозволяє оцінити ефективність функціонування системи в умовах динамічного мережевого середовища та порівняти її з традиційними IDS.

Розрахунок метрик здійснювався для сценаріїв S1–S4: нормального функціонування мережі, аномальної активності, DDoS-атак і багатовекторних вторгнень та динамічної зміни рівня кіберзагроз [13]. Для навчання й тестування нейромережевого модуля використано набори CICIDS2017, UNSW-NB15 і



CSE-CIC-IDS2018, що містять нормальний трафік та різні типи атак [2–3, 30]. Попередня обробка передбачала нормалізацію параметрів, формування вектора ознак і балансування класів.

Моделювання виконано в середовищі Linux із використанням Python, TensorFlow, Scikit-learn і NumPy [24, 30], а для аналізу та обробки трафіку застосовано Wireshark і Pandas. Нейромережевий модуль реалізовано на основі TensorFlow та LSTM-архітектури [3, 11, 25] із використанням CPU і GPU-прискорення.

Сценарний підхід забезпечив оцінювання системи за різних рівнів мережевого навантаження та кіберзагроз. Результати наведено в табл. 1 та порівняно з традиційними сигнатурними й аномальними IDS для оцінювання впливу гібридного аналізу, нечіткої логіки та нейромережевих технологій на точність виявлення атак і рівень хибнопозитивних спрацювань.

Таблиця 1

Порівняння ефективності методів виявлення кіберзагроз

Метод	Precision	Recall	F1-score
Signature IDS	0.82	0.80	0.81
Anomaly IDS	0.87	0.85	0.86
Proposed System	0.95	0.94	0.945

Запропонована система досягла Precision = 0.95, Recall = 0.94 та F1-score = 0.945, перевищивши сигнатурну IDS за F1-score на 0.135, а аномальну — на 0.085. Результати підтверджують ефективність інтеграції гібридного, нечіткого та нейромережевого аналізу.

На рис. 4 представлено замкнений контур адаптивного керування виявленням кіберзагроз, що охоплює формування вектора ознак, гібридний аналіз мережевого трафіку, інтегральне оцінювання рівня кіберзагрози та адаптивне реагування. Зворотний зв'язок забезпечує оцінювання ефективності підсистем і динамічне коригування їх вагових коефіцієнтів відповідно до поточного стану мережевого середовища.



Рис. 4. Замкнений контур адаптивного керування виявленням кіберзагроз

Для визначення функціональних відмінностей проведено порівняння запропонованої системи із сучасними IDS (табл. 2).

Таблиця 2

Порівняння запропонованої системи з існуючими IDS

Система	Тип аналізу	AI/ML	Fuzzy Logic	Adaptivity
Snort	Сигнатурний	Ні	Ні	Ні
Suricata	Сигнатурний/аномальний	Частково	Ні	Ні
Zeek	Поведінковий	Частково	Ні	Частково
Proposed System	Гібридний	Так	Так	Так



Як видно з табл. 2, запропонована система, на відміну від традиційних IDS, поєднує гібридний і нейромережовий аналіз, нечітку логіку та адаптивне прийняття рішень з урахуванням рівня кіберзагрози й характеристик мережевого трафіку. Це забезпечує динамічне налаштування параметрів системи відповідно до змін мережевого середовища.

Обговорення. Експериментальні результати підтвердили ефективність інтеграції сигнатурного, аномального, нечіткого та нейромережевого аналізу. Водночас дослідження проводилося в модельованому мережевому середовищі без урахування мобільності вузлів, розподілених edge-середовищ і повномасштабних high-load сценаріїв, що визначає межі узагальнення отриманих результатів.

Отримані результати підтверджують доцільність використання LSTM для аналізу часових залежностей мережевого трафіку. Перспективним напрямом розвитку нейромережевого модуля є застосування Transformer-архітектур та XAI для аналізу складних залежностей і підвищення інтерпретованості рішень [23, 28]. Використання LSTM- і Transformer-моделей дає змогу враховувати часові залежності мережових подій та аналізувати значні обсяги трафіку, а механізми Explainable Artificial Intelligence (XAI) підвищують інтерпретованість отриманих результатів.

Адаптивні механізми аналізу є актуальними також для захисту критичної інфраструктури, електромобільних [15], безпроводових і високошвидкісних мереж [26], де своєчасне виявлення аномальної активності та реагування на багатовекторні атаки визначають стійкість і кібербезпеку систем [16].

Порівняння зі Snort, Suricata та Zeek показало, що інтеграція інтелектуального аналізу, нечіткої логіки й адаптивного керування підвищує адаптивність системи до сучасних кіберзагроз. На відміну від традиційних IDS, запропонований підхід передбачає не лише виявлення відомих атак, а й аналіз поведінкових характеристик мережевого середовища та виявлення потенційно небезпечної активності.

Водночас ефективність нейромережевого модуля залежить від якості та репрезентативності навчальних даних, а застосування глибоких нейронних мереж і Transformer-моделей може потребувати значних обчислювальних ресурсів. Подальші дослідження доцільно спрямувати на зниження обчислювальної складності, розвиток адаптивного навчання, перевірку підходу в розподілених edge- та high-load середовищах, а також інтеграцію із SIEM-платформами й системами автоматизованого реагування на кіберінциденти.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

У статті вирішено актуальне науково-практичне завдання розробки інтелектуальної системи адаптивного виявлення кіберзагроз на основі гібридного аналізу, нечіткої логіки та нейронних мереж для підвищення ефективності функціонування сучасних систем кіберзахисту. Проведений аналіз сучасних систем виявлення вторгнень показав, що традиційні сигнатурні та аномальні IDS характеризуються недостатньою адаптивністю, високим рівнем хибнопозитивних спрацювань та обмеженими можливостями виявлення нових типів атак у динамічному мережевому середовищі.

У межах дослідження розроблено архітектуру інтелектуальної системи, яка поєднує сигнатурний та аномальний аналіз із механізмами нечіткої логіки, нейромережевого аналізу та адаптивного прийняття рішень. Запропоновано математичну модель інтегрального оцінювання рівня кіберзагрози на основі адаптивного вагового поєднання результатів різних підсистем аналізу. Розроблено нечітку модель оцінювання рівня ризику, нейромережовий модуль виявлення аномалій та механізм адаптивного керування параметрами функціонування системи залежно від поточного рівня кіберзагроз.

Експериментальне оцінювання показало, що запропонована система забезпечує Precision = 0.95, Recall = 0.94 та F1-score = 0.945, перевищуючи сигнатурний і аномальний підходи за F1-score відповідно на 0.135 та 0.085. Отримані результати підтверджують ефективність гібридного аналізу, нечіткої логіки та нейромережових технологій для адаптивного виявлення кіберзагроз у динамічному мережевому середовищі.

Перспективи подальших досліджень пов'язані з удосконаленням механізмів адаптивного навчання нейромережових моделей, інтеграцією технологій Explainable Artificial Intelligence для підвищення інтерпретованості рішень системи, а також використанням методів прогнозування кіберзагроз на основі аналізу часових рядів мережевого трафіку. Подальший розвиток системи доцільно спрямувати на оптимізацію обчислювальної складності алгоритмів, підтримку розподілених хмарних середовищ та інтеграцію із сучасними SIEM- і SOAR-платформами для автоматизованого реагування на кіберінциденти.

Дослідження проведено в рамках реалізації науково-дослідної теми "Методи та моделі забезпечення кібербезпеки інформаційних систем переробки інформації та функціональної безпеки програмно-технічних комплексів управління критичної інфраструктури (реєстраційний номер 0122U200483 від 06.07.2022).



СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Ishaque, M., Md Johar, M. G., Khatibi, A., & Yamin, M. (2023). A novel hybrid technique using fuzzy logic, neural networks and genetic algorithm for intrusion detection system. *Measurement: Sensors*, 30, 100933. <https://doi.org/10.1016/j.measen.2023.100933>
2. Qazi, E. U. H., Faheem, M. H., & Zia, T. (2023). HDLNIDS: Hybrid deep-learning-based network intrusion detection system. *Applied Sciences*, 13(8), 4921. <https://doi.org/10.3390/app13084921>
3. Hnamte, V., & Hussain, J. (2023). DCNNBiLSTM: An efficient hybrid deep learning-based intrusion detection system. *Telematics and Informatics Reports*, 10, 100053. <https://doi.org/10.1016/j.teler.2023.100053>
4. Rahman, M. M., Shakil, S. A., & Mustakim, M. M. (2024). A survey on intrusion detection system in IoT networks. *Cyber Security and Applications*, 3, 100082. <https://doi.org/10.1016/j.csa.2024.100082>
5. Alnasser, O., Al Muhtadi, J., Saleem, K., & Shrestha, S. (2025). Signature and anomaly based intrusion detection system for secure IoTs and V2G communication. *Alexandria Engineering Journal*, 125, 424–440.
6. Qiu, X., Shi, L., & Fan, P. (2025). A cooperative intrusion detection system for internet of things using fuzzy logic and ensemble of convolutional neural networks. *Scientific Reports*, 15, 15934. <https://doi.org/10.1038/s41598-025-99938-1>
7. Karakaya, A. (2025). A hybrid approach for IoT security: Combining ensemble learning with fuzzy logic. *Sensors*, 25(18), 5668. <https://doi.org/10.3390/s25185668>
8. Костюк, Ю. В., Складанний, П. М., & Гнатченко, Д. Д. (2026). Ризик-адаптивна авторизація в Zero Trust із динамічною довірою та токенами. *Проблеми програмування*, 1, 66–81. <https://doi.org/10.15407/pp2026.01.066>
9. Hassan, M. M., Gumaei, A. H., Alsanad, A., Alrubaijan, M., & Fortino, G. (2020). A hybrid deep learning model for efficient intrusion detection in big data environment. *Information Sciences*, 513, 386–396.
10. Костюк, Ю., Рзаєва, С., & Рзаєв, Д. (2026). Інтелектуальний аналіз мережевого трафіку для виявлення інцидентів інформаційної безпеки. *Наука і техніка сьогодні*, 2(56), 1909–1940. [https://doi.org/10.52058/2786-6025-2026-2\(56\)-1909-1928](https://doi.org/10.52058/2786-6025-2026-2(56)-1909-1928)
11. K, M., Renuka, S., K, L., & Y. M., M. (2025). Hybrid deep learning approach for efficient intrusion detection using DCNN and BiLSTM. In *2025 3rd International Conference on Data Science and Network Security (ICDSNS)* (pp. 1–6). IEEE. <https://doi.org/10.1109/ICDSNS65743.2025.11168612>
12. Складанний, П., Костюк, Ю., & Рзаєва, С. (2026). Безперервна оцінка доступу в Zero Trust Access Management на основі подієвих сигналів безпеки та динамічного керування сесіями. *Математичні машини і системи*, 1, 29–46. <https://doi.org/10.34121/1028-9763-2026-1-29-46>
13. Checker, S., Yadav, M., & Katarya, R. (2023). A survey on intrusion detection system for IoT networks based on artificial intelligence. In *2023 International Conference on Electrical, Electronics, Communication and Computers (ELEXCOM)* (pp. 1–6). IEEE. <https://doi.org/10.1109/ELEXCOM58812.2023.10370067>
14. Rzaeva, S., Skladannyi, P., Kostiuk, Y., Abramov, V., & Kravchenko, V. (2025). Adaptive information security management in cloud-oriented intelligent transportation systems. *Ukrainian Scientific Journal of Information Security*, 31(1), 23–36. <https://doi.org/10.18372/2225-5036.31.20634>
15. Pawlik, L., Wilk-Jakubowski, J. L., Grabski, P. T., & Wilk-Jakubowski, G. (2025). Securing the electrified future: A systematic review of cyber attacks, intrusion and anomaly detection, and authentication in electric vehicle charging infrastructure. *Energies*, 18(18), 4847. <https://doi.org/10.3390/en18184847>
16. Складанний, П. М., Гулак, Г. М., & Костюк, Ю. В. (2025). Генератор хаотичних чисел із нечітким керуванням для криптографічних систем із динамічною довірою. *Телекомунікаційні та інформаційні технології*, 4(89), 137–147. <https://doi.org/10.31673/2412-4338.2025.048916>
17. Костюк, Ю., Складанний, П., Рзаєва, С., Самойленко, Ю., & Коршун, Н. (2025). Інтелектуальні системи керування та захисту в кіберфізичних і хмарних середовищах Smart Grid. *Кібербезпека: освіта, наука, техніка*, 2(30), 125–156. <https://doi.org/10.28925/2663-4023.2025.30.956>
18. Kamboj, A., Ravindran, V., & Ojha, S. (2025). A comparative analysis of signature-based and anomaly-based intrusion detection systems. *International Journal of Latest Technology in Engineering Management & Applied Science*, 14, 209–214. <https://doi.org/10.51583/IJLTEMAS.2025.140500026>
19. Li, P., Wang, H., Tian, G., & Fan, Z. (2024). A cooperative intrusion detection system for the Internet of Things using convolutional neural networks and black hole optimization. *Sensors*, 24(15), 4766. <https://doi.org/10.3390/s24154766>
20. Костюк, Ю., Складанний, П., Рзаєва, С., Мазур, Н., Черевик, В., & Аносов, А. (2025). Особливості реалізації мережових атак через TCP/IP-протоколи. *Кібербезпека: освіта, наука, техніка*.



21. Yang, G., Huang, Q., Lv, H., & Lu, X. (2025). A network intrusion detection system based on convolutional neural network. In 2025 IEEE International Conference on High Performance Computing and Communications (HPCC) (pp. 1265–1271).
22. Костюк, Ю., Хорольська, К., Бебешко, Б., Довженко, Н., Коршун, Н., & Пазинін, А. (2025). Інструментальні засоби забезпечення інформаційної безпеки від прихованих загроз в інфраструктурі хмарних обчислень. *Кібербезпека: освіта, наука, техніка*, 4(28), 633–655. <https://doi.org/10.28925/2663-4023.2025.28.857>
23. Zhang, L., & Xu, C. (2022). A intrusion detection model based on convolutional neural network and feature selection. In 2022 5th International Conference on Artificial Intelligence and Big Data (ICAIBD) (pp. 162–167). IEEE. <https://doi.org/10.1109/ICAIBD55127.2022.9820384>
24. Складанний, П., Костюк, Ю., Рзаєва, С., Самойленко, Ю., & Савченко, Т. (2025). Розробка модульних нейронних мереж для виявлення різних класів мережових атак. *Кібербезпека: освіта, наука, техніка*, 3(27), 534–548. <https://doi.org/10.28925/2663-4023.2025.27.772>
25. Farhan, S., Mubashir, J., Haq, Y. U., et al. (2025). Enhancing network security: An intrusion detection system using residual network-based convolutional neural network. *Cluster Computing*, 28, 251. <https://doi.org/10.1007/s10586-025-05156-9>
26. Костюк, Ю., Бебешко, Б., Гулак, Г., Складанний, П., Рзаєва, С., & Хорольська, К. (2024). Забезпечення кібербезпеки та швидкодії передачі даних у безпроводних мережах. *Безпека інформації*, 30(3), 365–375. <https://doi.org/10.18372/2225-5036.30.20357>
27. Mo, Y., Li, H., Wang, D., & Liu, G. (2024). An intrusion detection system based on convolution neural network. *PeerJ Computer Science*, 10, e2152. <https://doi.org/10.7717/peerj-cs.2152>
28. Dang, X., & Li, Z. (2022). Network intrusion detection approach based on convolutional neural network. In 2022 4th International Conference on Communications, Information System and Computer Engineering (CISCE) (pp. 247–251). IEEE. <https://doi.org/10.1109/CISCE55963.2022.9851014>
29. Шевченко, С., Жданова, Ю., Складанний, П., & Петренко, Т. (2024). Нечіткі когнітивні карти як інструмент візуалізації сценаріїв реагування на інциденти в системах безпеки. *Кібербезпека: освіта, наука, техніка*, 2(26), 417–429. <https://doi.org/10.28925/2663-4023.2024.26.707>
30. Mohammadpour, L., Ling, T. C., Liew, C. S., & Aryanfar, A. (2022). A survey of CNN-based network intrusion detection. *Applied Sciences*, 12(16), 8162. <https://doi.org/10.3390/app12168162>
31. Костюк, Ю., Складанний, П., & Рзаєва, С. (2026). Управління якістю сповіщень у SIEM на основі ризик-орієнтованого оцінювання та зворотного зв'язку SOC. *Український науковий журнал інформаційної безпеки*, 31(3), 151–163. <https://doi.org/10.18372/2225-5036.31.21161>

**Yuliia Kostiuk**

PhD in Computer Science

Associate Professor of the Department of Information and
Cyber Security named after Professor Volodymyr Buriachok
Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine
ORCID: 0000-0001-5423-0985
y.kostiuk@kubg.edu.ua

Pavlo Skladannyi

PhD, Associate Professor, Head of the Department of Information and
Cyber Security named after Professor Volodymyr Buriachok
Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine
ORCID: 0000-0002-7775-6039
p.skladannyi@kubg.edu.ua

**INTELLIGENT ADAPTIVE CYBER THREAT DETECTION SYSTEM BASED ON HYBRID
ANALYSIS, FUZZY LOGIC, AND NEURAL NETWORKS**

Abstract. The article investigates the problem of improving the efficiency of cyber threat detection in modern intelligent information systems under conditions of increasing complexity of network attacks, dynamic network environments, and growing volumes of network traffic. The relevance of using intelligent methods for cyber event analysis to ensure adaptive response to modern cyber threats, including zero-day attacks, DDoS attacks, network anomalies, and modified intrusion types, is substantiated. An analysis of modern signature-based, anomaly-based, and hybrid intrusion detection systems is carried out, and their main shortcomings are identified, including a high level of false positives, insufficient adaptability, and limited capabilities for detecting new attack types. The paper proposes the architecture of an intelligent adaptive cyber threat detection system that combines signature-based and anomaly-based analysis with fuzzy logic and neural network mechanisms within a unified decision-making model. The system architecture includes modules for network traffic collection and preprocessing, feature vector generation, signature-based and anomaly-based analysis, fuzzy risk assessment, neural network analysis, result integration, and adaptive decision-making. A mathematical model for integrated cyber threat assessment based on adaptive weighted combination of the results of different analysis subsystems is developed. A mechanism for dynamic adjustment of weighting coefficients depending on network traffic characteristics, risk level, and cyber threat type is proposed. The practical significance of the obtained results lies in the possibility of using the proposed system to ensure cybersecurity of corporate networks, cloud platforms, automated control systems, and IoT environments.

Keywords: cyber threats; intrusion detection system; hybrid analysis; fuzzy logic; neural networks; information security; adaptive decision-making; machine learning; network traffic; intelligent system.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Ishaque, M., Md Johar, M. G., Khatibi, A., & Yamin, M. (2023). A novel hybrid technique using fuzzy logic, neural networks and genetic algorithm for intrusion detection system. *Measurement: Sensors*, 30, 100933. <https://doi.org/10.1016/j.measen.2023.100933>
2. Qazi, E. U. H., Faheem, M. H., & Zia, T. (2023). HDLNIDS: Hybrid deep-learning-based network intrusion detection system. *Applied Sciences*, 13(8), 4921. <https://doi.org/10.3390/app13084921>
3. Hnamte, V., & Hussain, J. (2023). DCNNBiLSTM: An efficient hybrid deep learning-based intrusion detection system. *Telematics and Informatics Reports*, 10, 100053. <https://doi.org/10.1016/j.teler.2023.100053>
4. Rahman, M. M., Shakil, S. A., & Mustakim, M. M. (2024). A survey on intrusion detection system in IoT networks. *Cyber Security and Applications*, 3, 100082. <https://doi.org/10.1016/j.csa.2024.100082>
5. Alnasser, O., Al Muhtadi, J., Saleem, K., & Shrestha, S. (2025). Signature and anomaly based intrusion detection system for secure IoTs and V2G communication. *Alexandria Engineering Journal*, 125, 424–440.



6. Qiu, X., Shi, L., & Fan, P. (2025). A cooperative intrusion detection system for internet of things using fuzzy logic and ensemble of convolutional neural networks. *Scientific Reports*, 15, 15934. <https://doi.org/10.1038/s41598-025-99938-1>
7. Karakaya, A. (2025). A hybrid approach for IoT security: Combining ensemble learning with fuzzy logic. *Sensors*, 25(18), 5668. <https://doi.org/10.3390/s25185668>
8. Kostiuk, Y. V., Skladannyi, P. M., & Hnatchenko, D. D. (2026). Risk-adaptive authorization in Zero Trust with dynamic trust and tokens. *Problems in Programming*, 1, 66–81. <https://doi.org/10.15407/pp2026.01.066>
9. Hassan, M. M., Gumaei, A. H., Alsanad, A., Alrubaian, M., & Fortino, G. (2020). A hybrid deep learning model for efficient intrusion detection in big data environment. *Information Sciences*, 513, 386–396.
10. Kostiuk, Y., Rzaieva, S., & Rzaiev, D. (2026). Intelligent network traffic analysis for detecting information security incidents. *Science and Technology Today*, 2(56), 1909–1940. [https://doi.org/10.52058/2786-6025-2026-2\(56\)-1909-1928](https://doi.org/10.52058/2786-6025-2026-2(56)-1909-1928)
11. K, M., Renuka, S., K, L., & Y. M., M. (2025). Hybrid deep learning approach for efficient intrusion detection using DCNN and BiLSTM. In 2025 3rd International Conference on Data Science and Network Security (ICDSNS) (pp. 1–6). IEEE. <https://doi.org/10.1109/ICDSNS65743.2025.11168612>
12. Skladannyi, P., Kostiuk, Y., & Rzaieva, S. (2026). Continuous access assessment in Zero Trust Access Management based on security event signals and dynamic session management. *Mathematical Machines and Systems*, 1, 29–46. <https://doi.org/10.34121/1028-9763-2026-1-29-46>
13. Checker, S., Yadav, M., & Katarya, R. (2023). A survey on intrusion detection system for IoT networks based on artificial intelligence. In 2023 International Conference on Electrical, Electronics, Communication and Computers (ELEXCOM) (pp. 1–6). IEEE. <https://doi.org/10.1109/ELEXCOM58812.2023.10370067>
14. Rzaeva, S., Skladannyi, P., Kostiuk, Y., Abramov, V., & Kravchenko, V. (2025). Adaptive information security management in cloud-oriented intelligent transportation systems. *Ukrainian Scientific Journal of Information Security*, 31(1), 23–36. <https://doi.org/10.18372/2225-5036.31.20634>
15. Pawlik, L., Wilk-Jakubowski, J. L., Grabski, P. T., & Wilk-Jakubowski, G. (2025). Securing the electrified future: A systematic review of cyber attacks, intrusion and anomaly detection, and authentication in electric vehicle charging infrastructure. *Energies*, 18(18), 4847. <https://doi.org/10.3390/en18184847>
16. Skladannyi, P. M., Hulak, H. M., & Kostiuk, Y. V. (2025). Chaotic number generator with fuzzy control for cryptographic systems with dynamic trust. *Telecommunication and Information Technologies*, 4(89), 137–147. <https://doi.org/10.31673/2412-4338.2025.048916>
17. Kostiuk, Y., Skladannyi, P., Rzaieva, S., Samoilenko, Y., & Korshun, N. (2025). Intelligent control and protection systems in cyber-physical and cloud-based Smart Grid environments. *Cybersecurity: Education, Science, Technique*, 2(30), 125–156. <https://doi.org/10.28925/2663-4023.2025.30.956>
18. Kamboj, A., Ravindran, V., & Ojha, S. (2025). A comparative analysis of signature-based and anomaly-based intrusion detection systems. *International Journal of Latest Technology in Engineering Management & Applied Science*, 14, 209–214. <https://doi.org/10.51583/IJLTEMAS.2025.140500026>
19. Li, P., Wang, H., Tian, G., & Fan, Z. (2024). A cooperative intrusion detection system for the Internet of Things using convolutional neural networks and black hole optimization. *Sensors*, 24(15), 4766. <https://doi.org/10.3390/s24154766>
20. Kostiuk, Y., Skladannyi, P., Rzaieva, S., Mazur, N., Cherevyk, V., & Anosov, A. (2025). Features of network attack implementation through TCP/IP protocols. *Cybersecurity: Education, Science, Technique*.
21. Yang, G., Huang, Q., Lv, H., & Lu, X. (2025). A network intrusion detection system based on convolutional neural network. In 2025 IEEE International Conference on High Performance Computing and Communications (HPCC) (pp. 1265–1271).
22. Kostiuk, Y., Khorolska, K., Bebesko, B., Dovzhenko, N., Korshun, N., & Pazynin, A. (2025). Tools for ensuring information security against hidden threats in cloud computing infrastructure. *Cybersecurity: Education, Science, Technique*, 4(28), 633–655. <https://doi.org/10.28925/2663-4023.2025.28.857>
23. Zhang, L., & Xu, C. (2022). A intrusion detection model based on convolutional neural network and feature selection. In 2022 5th International Conference on Artificial Intelligence and Big Data (ICAIBD) (pp. 162–167). IEEE. <https://doi.org/10.1109/ICAIBD55127.2022.9820384>
24. Skladannyi, P., Kostiuk, Y., Rzaieva, S., Samoilenko, Y., & Savchenko, T. (2025). Development of modular neural networks for detecting various classes of network attacks. *Cybersecurity: Education, Science, Technique*, 3(27), 534–548. <https://doi.org/10.28925/2663-4023.2025.27.772>
25. Farhan, S., Mubashir, J., Haq, Y. U., et al. (2025). Enhancing network security: An intrusion detection system using residual network-based convolutional neural network. *Cluster Computing*, 28, 251. <https://doi.org/10.1007/s10586-025-05156-9>



26. Kostiuk, Y., Bebeshko, B., Hulak, H., Skladannyi, P., Rzaieva, S., & Khorolska, K. (2024). Ensuring cybersecurity and high-speed data transmission in wireless networks. *Information Security*, 30(3), 365–375. <https://doi.org/10.18372/2225-5036.30.20357>
27. Mo, Y., Li, H., Wang, D., & Liu, G. (2024). An intrusion detection system based on convolution neural network. *PeerJ Computer Science*, 10, e2152. <https://doi.org/10.7717/peerj-cs.2152>
28. Dang, X., & Li, Z. (2022). Network intrusion detection approach based on convolutional neural network. In 2022 4th International Conference on Communications, Information System and Computer Engineering (CISCE) (pp. 247–251). IEEE. <https://doi.org/10.1109/CISCE55963.2022.9851014>
29. Shevchenko, S., Zhdanova, Y., Skladannyi, P., & Petrenko, T. (2024). Fuzzy cognitive maps as a tool for visualizing incident response scenarios in security systems. *Cybersecurity: Education, Science, Technique*, 2(26), 417–429. <https://doi.org/10.28925/2663-4023.2024.26.707>
30. Mohammadpour, L., Ling, T. C., Liew, C. S., & Aryanfar, A. (2022). A survey of CNN-based network intrusion detection. *Applied Sciences*, 12(16), 8162. <https://doi.org/10.3390/app12168162>
31. Kostiuk, Y., Skladany, P., & Rzaieva, S. (2026). SIEM alert quality management based on risk-oriented assessment and SOC feedback. *Ukrainian Scientific Journal of Information Security*, 31(3), 151–163. <https://doi.org/10.18372/2225-5036.31.21161>

Отримано редакцією журналу / Received: 26.05.26

Прорецензовано / Revised: 16.06.26

Схвалено до друку / Accepted: 26.10.26



This work is licensed under Creative Commons Attribution-noncommercial-sharealike 4.0 International License.