кращою придатністю до використання у сучасних хмарних і розподілених інформаційних середовищах. Класичні моделі DAC і MAC отримали нижчі показники ефективності через обмежену гнучкість і складність масштабування.

Таблиця 1

Багатокритеріальне оцінювання моделей контролю доступу за методом AHP

Модель	Безпека	Масштабованість	Гнучкість	Складність адміністрування	Хмарна придатність	Інтегральний AHP-пріоритет
DAC	0,10	0,08	0,12	0,18	0,07	0,08
MAC	0,22	0,12	0,09	0,10	0,11	0,16
RBAC	0,20	0,21	0,18	0,19	0,17	0,22
ABAC	0,24	0,26	0,29	0,21	0,30	0,26
ZTA	0,24	0,33	0,32	0,32	0,35	0,28

Наукова новизна роботи полягає у застосуванні методу аналізу ієрархій для багатокритеріального оцінювання та вибору моделей контролю доступу в системах управління інформаційною безпекою з урахуванням технічних, організаційних та експлуатаційних критеріїв.

Отримані результати підтверджують доцільність застосування методу AHP для підтримки прийняття рішень у системах управління інформаційною безпекою. Метод аналізу ієрархій може використовуватися для оцінювання ефективності механізмів захисту інформації, вибору моделей контролю доступу та підтримки процесів управління ризиками в сучасних інформаційних системах.

1. Любименко О. М., Штепа О. А., Маслова Н. О., Стаценко О. А. Оцінювання якості web-застосунків управління проєктами на IT-ринку з використанням методу аналізу ієрархій // Науковий вісник Донецького національного технічного університету. 2026. с.99-106, https://doi.org/10.31474/2415-7902-2026-2-17-99-106
2. Saaty T. L. Decision Making with the Analytic Hierarchy Process // International Journal of Services Sciences. 2008. Vol. 1. No. 1. P. 83–98.
3. Sandhu R., Coyne E., Feinstein H., Youman C. Role-Based Access Control Models // IEEE Computer. 1996. Vol. 29. No. 2. P. 38–47.

Використання автоенкодерів для виявлення кібербезпекових аномалій в інформаційно-телекомунікаційних мережах

УДК 004.056:004.8

Євгенія Іванченко[1], Микола Рижаков[2],
Євген Кихтенко[3], Артем Роженко[4]

Державний університет інформаційно-комунікаційних технологій,
[1]e.ivanchenko@duikt.edu.ua, [2]m.ryzhakov@duikt.edu.ua,
[3]e.kykhtenko@stud.duikt.edu.ua, [4]a.rozhenko@stud.duikt.edu.ua

Об'єкти критичної інфраструктури держави — енергетика, транспорт, водопостачання, фінансовий сектор, телекомунікації, охорона здоров'я та

органи публічної влади — у своїй роботі повністю залежать від інформаційно-комунікаційних технологій. Згідно зі звітом Європейського агентства з кібербезпеки ENISA Threat Landscape 2024, кількість інцидентів, спрямованих проти секторів критичної інфраструктури в Європі, продовжує зростати, причому в умовах гібридних загроз спостерігається перехід від точкових атак до тривалих, розосереджених у часі кампаній типу Advanced Persistent Threat (APT) [1]. Особливо вразливим компонентом залишаються телекомунікаційні мережі, що об'єднують промислові SCADA-системи, корпоративні IT-сервіси та сервіси віддаленого керування.

В Україні правові засади функціонування таких об'єктів визначені Законом України «Про критичну інфраструктуру» [2], що нормативно закріплює необхідність побудови ефективних систем моніторингу й кіберзахисту. Однак практика свідчить про обмежену ефективність традиційних сигнатурних і правил-орієнтованих засобів виявлення інцидентів за наявності великого обсягу трафіку, високої швидкості його зміни та активного використання атак нульового дня. Тому одним з найбільш активно досліджуваних напрямів є застосування методів штучного інтелекту, зокрема глибокого навчання, для побудови інтелектуальних компонентів виявлення кіберінцидентів [3; 4; 5].

Метою роботи є удосконалення інформаційної технології виявлення кіберінцидентів у телекомунікаційних мережах критичної інфраструктури шляхом застосування глибоких автоенкодерів, що дозволяє підвищити чутливість системи кіберзахисту до раніше невідомих відхилень, скоротити час реакції оператора SOC і зменшити залежність від повністю розмічених навчальних вибірок.

Класифікація методів виявлення аномалій у мережевому трафіку традиційно поділяється на сигнатурні, статистичні, методи класичного машинного навчання та методи глибокого навчання [3; 4]. Сигнатурні засоби (Snort, Suricata) забезпечують високу інтерпретованість для відомих атак, проте не виявляють раніше невідомі загрози й погано пристосовані до роботи з шифрованим трафіком. Статистичні методи (CUSUM, EWMA, аналіз ентропії) фіксують відхилення від типових профілів, але слабко враховують нелінійні залежності між ознаками. Класичні алгоритми (SVM, Isolation Forest, k-NN, Random Forest) демонструють прийнятну точність на розмічених наборах даних, проте їхня ефективність значно знижується у разі несуттєвої кількості позначених прикладів атак та високої розмірності ознакового простору.

Особливістю об'єктів критичної інфраструктури є те, що отримати репрезентативну марковану вибірку аномального трафіку у промисловому середовищі практично неможливо: будь-яка реалізація атаки може мати каскадні наслідки. Тому експерименти проводять переважно у тестових сегментах або на наборах публічних даних (NSL-KDD, CICIDS2017, UNSW-NB15). Актуальним стає підхід частково керованого навчання, у якому модель тренується винятково на прикладах нормального трафіку, а виявлення аномалій ґрунтується на оцінюванні відхилення нового спостереження від засвоєного «еталону». Саме таку поведінку демонструють автоенкодери [4; 6; 8]. Узагальнення зазначених підходів подано у табл. 1.

Таблиця 1

Порівняння методів виявлення аномалій у мережах критичної інфраструктури

Критерій	*Сигнатурні*	*Статистичні*	*Класичне ML*	*Автоенкодер*
Потреба в маркованих даних	Низька	Низька	Висока	Низька
Виявлення 0-day атак	Ні	Частково	Обмежено	Так
Адаптивність до змін трафіку	Низька	Середня	Середня	Висока
Робота з нелінійними ознаками	Ні	Обмежено	Обмежено	Так
Інтерпретованість результату	Висока	Середня	Середня	Середня
Швидкодія в режимі онлайн	Висока	Висока	Середня	Висока
Придатність для критичної інфраструктури	Часткова	Часткова	Часткова	Висока

Формально задача виявлення аномалії формулюється через оцінювання похибки реконструкції вхідного вектора ознак трафіку.

Глибокий автоенкодер є парою симетричних нелінійних відображень — кодувальника $f_\varphi: R^n \to R^k$ і декодувальника $g_\psi: R^k \to R^n$, де $k \ll n$.

Латентне подання $z = f_\varphi(x)$ реалізує стиснений опис нормального трафіку, а реконструкція виконується як $\hat{x} = g_\psi\left(f_\varphi(x)\right)$.

Похибка реконструкції визначається за формулою:

$$E(x) = \|x - \hat{x}\|^2 = \|x - g_\psi\left(f_\varphi(x)\right)\|^2 \quad (1)$$

Модель навчається мінімізацією емпіричного ризику на еталонній вибірці нормального трафіку:

$$L(\varphi, \psi) = \frac{1}{N}\sum_{i=1}^{N} \quad \|x_i - g_\psi\left(f_\varphi(x_i)\right)\|^2 \to min \quad (2)$$

N — обсяг навчальної вибірки. Спостереження визнається аномальним за умови:

$$E(x) > \theta \quad (3)$$

де θ — порогове значення, що визначається як квантиль порядку $0{,}99$ розподілу похибки реконструкції на нормальному трафіку: $\theta = Q_{0.99}(E_{train})$, або адаптивно перераховується відповідно до режиму функціонування мережі: день/ніч, плановий моніторинг, аварійний режим.

Така постановка узгоджується з узагальненою моделлю прогнозування й виявлення кібербезпекових аномалій, запропонованою у попередніх роботах авторів [7; 8].

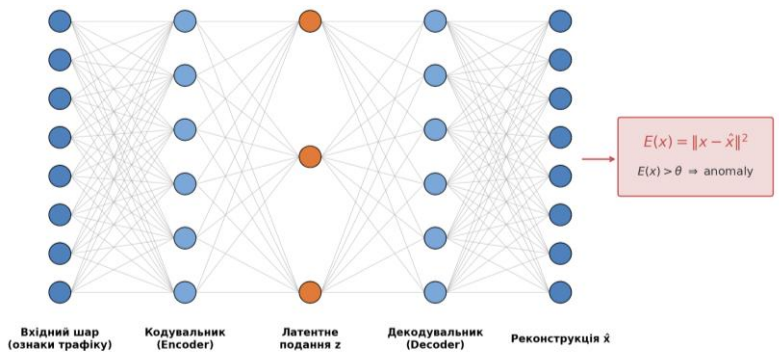

Рис. 1. Архітектура глибокого автоенкодера для виявлення кіберінцидентів у мережі

Удосконалена інформаційна технологія виявлення кіберінцидентів реалізована як п'ятиетапний процес обробки трафіку (рис. 2) і охоплює: збір мережевого трафіку (NetFlow/IPFIX, pcap-файли або агенти на мережевих пристроях), попередню обробку (очистка, нормалізація z-score, кодування категоріальних ознак, формування часових вікон), застосування навченого автоенкодера для отримання реконструкції, обчислення похибки та її порівняння з адаптивним порогом, формування рішення про класифікацію спостереження як нормального або аномального і його передачу до системи реагування Security Operations Center (SOC).

Рис. 2. Узагальнена схема інформаційної технології виявлення кіберінцидентів

Архітектура автоенкодера реалізована як симетрична повнозв'язна мережа з функцією активації ReLU у прихованих шарах і лінійною — у вихідному, регуляризацією шарами Dropout та оптимізатором Adam. Орієнтовні значення гіперпараметрів моделі, отримані за результатами попередніх експериментів на наборі CICIDS2017, наведено у табл. 2.

Таблиця 2

Орієнтовні гіперпараметри глибокого автоенкодера

Параметр	*Значення / діапазон*	*Коментар*
Розмірність входу n	40–80	Обсяг ознак трафіку після обробки
Розмірність латенту k	8–16	Стиснення у 4–8 разів
Кількість прихованих шарів	3 + 3 (симетрично)	Глибокий автоенкодер

Активація / Dropout	ReLU / 0,1–0,2	Регуляризація для стійкості
Оптимізатор / Learning rate	Adam / $1 \cdot 10^{-3}$	Стандартні значення
Розмір батча / епохи	256 / 50–100	Контроль за раннього зупинкою
Поріг θ	$Q_{0,99}$(E_train)	Адаптивний за режимом мережі

Запропонована технологія дозволяє формувати рішення про наявність кіберінциденту в режимі, наближеному до реального часу. За результатами попередніх досліджень авторів [7; 8] та інших робіт у відкритих джерелах [3; 4], для подібних архітектур на наборах CICIDS2017 і NSL-KDD досягається значення F1-міри у діапазоні 0,92–0,97 за умови ретельного підбору ознак та порогу. У межах поточної роботи увагу акцентовано не на максимізації одного показника, а на структурній сумісності рішення з вимогами до систем кіберзахисту критичної інфраструктури: робота за умов частково розмічених даних, виявлення раніше невідомих відхилень, можливість інтеграції з SIEM/SOAR, керованість поточним режимом експлуатації.

До переваг підходу варто віднести виявлення поведінкових відхилень незалежно від наявності сигнатури, гнучке масштабування (модель легко перенавчається на нову топологію або режим роботи об'єкта) та сумісність з вимогами Закону України «Про критичну інфраструктуру» [2] і підходами ENISA [1]. Серед обмежень — необхідність регулярного оновлення моделі, ризик дрейфу концепції (concept drift) та потреба у механізмах інтерпретації для оператора SOC, зокрема через техніки SHAP, LIME або модулі контекстуалізації подій [9].

Удосконалена інформаційна технологія виявлення кіберінцидентів у телекомунікаційних мережах критичної інфраструктури, побудована на основі глибоких автоенкодерів та адаптивного порогового аналізу, дозволяє підвищити точність і своєчасність виявлення відхилень, у тому числі раніше невідомих, та зменшити залежність від повністю розмічених наборів даних. Запропонована п'ятиетапна архітектура (збір трафіку → попередня обробка → автоенкодер → оцінка похибки → адаптивний поріг → класифікація) узгоджується з вимогами національного законодавства й рекомендаціями ENISA та може бути інтегрована до існуючих систем моніторингу й реагування. Подальші дослідження будуть спрямовані на інтеграцію автоенкодерів з механізмами оцінювання критичності інцидентів, прогнозування навантаження на мережу та семантичної інтерпретації подій у складі комплексних інформаційних технологій кіберзахисту.

1. ENISA Threat Landscape 2024. European Union Agency for Cybersecurity, 2024. 142 p. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024 (дата звернення: 28.04.2026).
2. Про критичну інфраструктуру : Закон України від 16.11.2021 № 1882-IX. URL: https://zakon.rada.gov.ua/laws/show/1882-20 (дата звернення: 28.04.2026).
3. Kwon D., Kim H., Kim J., Suh S. C., Kim I., Kim K. A survey of deep

learning-based network anomaly detection. Cluster Computing. 2019. Vol. 22. P. 949–961. DOI: 10.1007/s10586-017-1117-8.
4. Chalapathy R., Chawla S. Deep learning for anomaly detection: A survey. arXiv preprint arXiv:1901.03407. 2019. 50 p.
5. Goodfellow I., Bengio Y., Courville A. Deep Learning. Cambridge : MIT Press, 2016. 800 p.
6. Hinton G. E., Salakhutdinov R. R. Reducing the dimensionality of data with neural networks. Science. 2006. Vol. 313, № 5786. P. 504–507.
7. Іванченко Є. І., Рижаков М. М. Узагальнена модель прогнозування та виявлення кібербезпекових аномалій на основі штучного інтелекту. Кібербезпека: освіта, наука, техніка. 2025. URL: https://csecurity.kubg.edu.ua/index.php/journal/article/view/823.
8. Рижаков М. М. Моделі та методи виявлення кіберінцидентів у телекомунікаційних мережах критичної інфраструктури : дис. … д-ра філософії : 125 / Держ. ун-т інформ.-комунікац. технологій. Київ, 2025. URL: https://duikt.edu.ua/uploads/p_2958_82196938.pdf.
9. Pang G., Shen C., Cao L., Hengel A. v. d. Deep learning for anomaly detection: A review. ACM Computing Surveys. 2021. Vol. 54, № 2. P. 1–38. DOI: 10.1145/3439950.

Програмний засіб для шифрування у системі залишкових класів

УДК 004.424

Олег Момотюк[1], Михайло Голембйовський[2], Михайло Касянчук[3]

Західноукраїнський національний університет,
[1]momotjuk98@gmail.com, [2]mykhailo.2097@gmail.com, [3]kasyanchuk@ukr.net

У сучасних інформаційних системах зростає потреба у криптографічних алгоритмах, які поєднують достатній рівень захисту даних із високою швидкодією та можливістю ефективної реалізації в умовах обмежених обчислювальних ресурсів [1]. Одним із перспективних підходів до підвищення продуктивності криптографічних операцій є використання системи залишкових класів (СЗК) [2, 3]. Її перевага полягає в тому, що велике число може бути подане як набір залишків за декількома попарно взаємно простими модулями. У такому представленні арифметичні операції виконуються незалежно для кожного модуля, що створює природні передумови для паралельної обробки даних. Це дає змогу зменшити складність обчислень над великими числами та підвищити швидкодію алгоритмів, які використовують модульну арифметику.

Дана робота присвячена розробці програмного засобу для шифрування в СЗК. Запропонований підхід змінює логіку обробки повідомлення: криптографічне перетворення застосовується не до окремих символів, а до числового блоку відкритого тексту. Такий блок розкладається на залишки за системою модулів, після чого для кожного залишку виконується окреме криптографічне перетворення. Отримані змінені залишки об’єднуються у зашифроване число за допомогою китайської теореми про залишки (КТЗ).