УДК 004.056.53:004.942:621.39 DOI: 10.31673/2786-8362.2025.024906

Флоров С.В., к.т.н.; **Черкаський О.В.;**
Черкаський Д.О.; Переметчик Д.О.;
Білан М.В.

ВИЯВЛЕННЯ ГІБРИДНИХ КІБЕРАТАК У МЕРЕЖАХ ЕЛЕКТРОННИХ КОМУНІКАЦІЙ ЗАСОБАМИ ГЛИБОКОГО НАВЧАННЯ ТА ІНТЕГРОВАНИХ СИСТЕМ БЕЗПЕКИ

Florov S.V., Cherkaskyi O.V., Cherkaskyi D.O., Peremetchyk D.O., Bilan M.V. Detection of hybrid cyber attacks in electronic communication networks using Deep Learning and Integrated Security Systems. The article presents a comprehensive approach to modeling electronic communication networks under hybrid cyber attacks using Zero Trust principles and modern data analysis methods. The proposed integration of rapid state-change detection and statistical thresholds with multi-level learning based on convolutional and recurrent neural networks, autoencoders, and visual telemetry fingerprints is discussed. It has been proven that combining sensor data, network traffic, event logs, and firmware artifacts into a unified pipeline increases anomaly detection accuracy and reduces response latency in critical scenarios. The study was conducted considering international standards and framework documents: the Zero Trust Architecture by the U.S. National Institute of Standards and Technology (NIST SP 800-207), ISO/IEC 27001 requirements for information security management systems, NIST SP 800-218 (SSDF) secure software development recommendations, TLS 1.3 and SNMPv3 protocols, as well as the MITRE ATT&CK methodology for describing and analyzing adversary behavior. The article shows that combining statistical filtering methods, deep learning, and standardized security policies contributes to the creation of new tools for security operations and event management centers. From the perspective of the digital economy, the results support the development of resilient communication infrastructures integrated into ecosystems of e-services, cloud platforms, and mobile applications. The proposed solutions form a practical foundation for improving intrusion detection and risk management systems, meet the current requirements of global markets and cyber resilience strategies, and create conditions for long-term trust in digital technologies.

Keywords: hybrid cyber attacks, modeling of electronic communication networks, protocol vulnerabilities, digital economy, international standards, risk management, deep learning

Флоров С.В., Черкаський О.В., Черкаський Д.О., Переметчик Д.О., Білан М.В. Виявлення гібридних кібератак у мережах електронних комунікацій засобами глибокого навчання та інтегрованих систем безпеки. У статті представлено комплексний підхід до моделювання мереж електронних комунікацій в умовах гібридних кібератак із використанням принципів довіри нульового рівня та сучасних методів аналізу даних. Запропоновано інтеграцію швидкої перевірки змін стану й статистичних порогів із багаторівневим навчанням на основі згорткових і рекурентних нейронних мереж, автоенкодерів та візуальних відбитків телеметрії. Доведено, що поєднання сенсорних рядів, мережевого трафіку, журналів подій і артефактів прошивок у єдиний конвеєр підвищує точність виявлення аномалій та знижує затримку реагування у критичних сценаріях. Дослідження виконано з урахуванням міжнародних стандартів і рамкових документів: архітектури довіри нульового рівня за Національним інститутом стандартів і технологій США (NIST SP 800-207), вимог ISO/IEC 27001 щодо систем управління інформаційною безпекою, рекомендацій із безпечної розробки програмного забезпечення NIST SP 800-218 (SSDF), протоколів TLS 1.3 і SNMPv3, а також методології MITRE ATT&CK для опису та аналізу поведінки зловмисників. У статті показано, що поєднання методів статистичної фільтрації, глибинного навчання та стандартизованих політик безпеки сприяє формуванню нових інструментів для центрів операцій безпеки та управління подіями. З позицій цифрової економіки результати підтримують розвиток стійких комунікаційних інфраструктур, які інтегруються в екосистеми електронних послуг, хмарних сервісів і мобільних застосунків. Запропоновані рішення становлять практичну основу для удосконалення систем виявлення вторгнень і управління ризиками, відповідають сучасним вимогам глобальних ринків та стратегіям кіберстійкості, а також створюють умови для довгострокового зростання довіри до цифрових технологій.

Ключові слова: гібридні кібератаки, моделювання мереж електронних комунікацій, вразливості протоколів, цифрова економіка, міжнародні стандарти, управління ризиками, глибинне навчання

Вступ

Електронні комунікаційні мережі сьогодні є критичною інфраструктурою, що забезпечує функціонування цифрової економіки, державних сервісів та фінансових платформ. Водночас саме вони стають головною ціллю гібридних кібератак, які поєднують у собі мережеві, прошивкові та соціотехнічні вектори впливу. Такі атаки відрізняються багатоступеневістю, використанням прихованих методів проникнення та експлуатацією вразливостей протоколів і firmware-компонентів, що робить їх надзвичайно складними для виявлення стандартними засобами захисту.

Традиційні системи виявлення вторгнень (IDS) та платформи управління інформацією і подіями безпеки (SIEM) демонструють обмежену ефективність у роботі з мультимодальними потоками даних, які включають мережевий трафік, журнали автентифікації, сенсорні ряди та артефакти прошивок. Це призводить до високого рівня хибнопозитивних спрацьовувань, затримки реагування та неможливості адекватно протидіяти складним атакам у реальному часі. Проблема ускладнюється тим, що сучасні атаки дедалі частіше спрямовані на критичні протоколи управління (зокрема TLS і SNMP), а також на ланцюги постачання й firmware-рівень, де класичні інструменти моніторингу практично безсилі. Наявність відомих інцидентів, як-от SSL stripping або Heartbleed, підкреслює системний характер цих вразливостей і потребу у створенні нових підходів до безпеки [18; 19; 20].

Отже, у сучасних умовах виникає науково-практична задача: розробити комплексний метод виявлення гібридних кібератак, який би поєднував статистичні алгоритми, глибинне навчання, мультимодальний аналіз та стандартизовані політики Zero Trust. Такий підхід має забезпечити підвищену точність і швидкість реагування, зниження кількості хибних спрацьовувань і відповідність вимогам міжнародних стандартів інформаційної безпеки (ISO/IEC 27001, NIST SP 800-207, NIST SP 800-218) [2; 15; 21].

Аналіз останніх досліджень. У сфері виявлення кіберзагроз протягом останніх років спостерігається стрімкий розвиток підходів, що ґрунтуються на глибинному навчанні та мультимодальній обробці даних. Значний внесок у формування сучасних методів зробила робота Mirsky та співавт., у якій запропоновано ансамблі автоенкодерів для онлайн-аналізу мережевих аномалій (Kitsune) [4]. Подальші дослідження Shone та колег [5] підтвердили ефективність поєднання згорткових і рекурентних нейронних мереж (CNN+LSTM) для задач класифікації мережевого трафіку.

Інший перспективний напрям представлено у роботах Ruff і співавт. [6], де розроблено підхід Deep SVDD для однокласової класифікації, що дозволяє виявляти аномалії без необхідності великого обсягу розмічених даних. Додатково активно досліджуються контрастивні моделі без учителя (SimCLR, MoCo), які демонструють високий потенціал у створенні стійких ембеддингів для багатомодальних задач [7; 8]. Ймовірнісні методи також посідають важливе місце у сучасних підходах. Так, алгоритм Bayesian Online Change Point Detection [9] застосовується для фіксації структурних змін у потоках даних у реальному часі. Для побудови адаптивних порогів використовуються квантильні ескізи t-digest [10] та KLL [11], що забезпечують високу точність навіть у великих потоках телеметрії. Ефективність таких рішень підсилюється за рахунок методів екстремальної теорії значень (EVT), які забезпечують робастність калібрування порогів [12].

Окремої уваги заслуговують стандартизовані підходи та міжнародні рекомендації. Парадигма Zero Trust, детально описана у NIST SP 800-207 [2] і концептуально сформульована Forrester Research [17], активно інтегрується з методологіями ISO/IEC 27001 [15] та MITRE ATT&CK [14]. Важливим орієнтиром у забезпеченні безпеки процесів розробки залишається Secure Software Development Framework (SSDF) [21], який визначає вимоги до стійкості ланцюгів постачання та контролю firmware-компонентів.

Підсумовуючи, можна зазначити, що сучасний стан наукових досліджень свідчить про формування багатокомпонентного підходу: поєднання глибинних моделей, ймовірнісних алгоритмів та міжнародних стандартів створює фундамент для побудови систем виявлення гібридних кібератак нового покоління [1–21].

Постановка завдання. Попри значні досягнення у сфері застосування глибинного навчання, ймовірнісних методів та політик Zero Trust у виявленні кібератак, низка фундаментальних питань залишається відкритою. По-перше, недостатньо дослідженою є інтеграція різнорідних потоків телеметрії – мережевого трафіку, сенсорних рядів, журналів автентифікації та артефактів прошивок – у єдиний конвеєр аналізу. Сучасні системи здебільшого фокусуються на одному домені даних, що обмежує їхню ефективність у гібридних сценаріях [4–6].

По-друге, відкритим залишається питання зниження кількості хибнопозитивних спрацьовувань у мультимодальних архітектурах. Використання ансамблів автоенкодерів або CNN+LSTM покращує точність [5], проте не гарантує стабільності роботи у виробничих середовищах. Додатково потребують дослідження методи калібрування ризику, зокрема на основі екстремальної теорії значень (EVT), які поки що обмежено інтегруються в індустріальні рішення [12].

По-третє, залишається невирішеним завдання адаптації підходів машинного навчання до атак firmware-рівня та сценаріїв, що пов’язані з маніпуляціями протоколів TLS і SNMP. Відомі інциденти на зразок SSL-downgrade чи Heartbleed [18; 19] показують, що уразливості можуть існувати на рівні реалізації протоколів, і їх ефективне виявлення потребує нових поєднань методів статистичного й глибинного аналізу.

По-четверте, інтеграція досліджень у практику SOC і SIEM вимагає створення універсальних схем взаємодії з міжнародними стандартами, зокрема ISO/IEC 27001, NIST SP 800-207 та SSDF [2; 15; 21]. Попри наявність методологічної бази, недостатньо розроблено практичні інструменти, які б одночасно відповідали вимогам кіберстійкості та були придатними до масштабного впровадження.

Таким чином, потребує вирішення комплекс завдань: формування єдиного мультимодального конвеєра збору та обробки даних, зниження рівня хибних спрацьовувань, адаптація методів до firmware-сценаріїв, а також інтеграція результатів у стандартизовані процеси управління інформаційною безпекою.

Метою роботи є розробка та верифікація мультимодальної схеми виявлення гібридних кібератак у мережах електронних комунікацій, яка поєднує статистичні методи та моделі глибинного навчання, інтегрується з політикою Zero Trust і відповідає вимогам міжнародних стандартів інформаційної безпеки. У межах цієї мети передбачається побудова конвеєра збору, уніфікації та попередньої обробки телеметрії з різнорідних джерел, створення «вродженого» шару швидкої фільтрації аномалій на основі статистичних алгоритмів, розробка «адаптивного» шару аналізу за допомогою CNN+LSTM, AE+LSTM і самонавчальних моделей, використання методів екстремальної теорії значень для калібрування ризику та зменшення кількості хибнопозитивних спрацьовувань, а також інтеграція розробленої архітектури в інфраструктуру SOC та SIEM з урахуванням міжнародних стандартів і забезпеченням автоматизованого реагування на виявлені загрози.

Виклад основного матеріалу дослідження

Методологія. Методологічна основа дослідження визначається необхідністю інтеграції статистичних алгоритмів, глибинного навчання та політик Zero Trust для забезпечення стійкої роботи систем виявлення вторгнень (IDS) і платформ управління інформацією та подіями безпеки (SIEM) у гібридних середовищах [2, 14, 16]. Розвиток SSL та SNMP-протоколів показав наявність низки критичних уразливостей [18–20], що потребують врахування при проєктуванні методів фільтрації й аналізу. Наукові підходи останніх років, зокрема ансамблі автоенкодерів (Kitsune) [4], CNN+LSTM [5], Deep SVDD [6], а також імовірнісні методи BOCPD [9], t-digest і KLL [10, 11], довели ефективність при роботі з потоковими та мультимодальними даними. Зважаючи на ці виклики, розділ «Методи» спрямований на опис систематизованого підходу: від збору та нормалізації телеметрії до формування двозонної архітектури («вроджений» та «адаптивний» шар), використання CNN+LSTM та AE+LSTM, фузії ризику з EVT-калібруванням і оптимізації розподілу захисних дій [6, 12]. Такий комплекс

дозволяє поєднати швидкі реакції на рівні квантильних імовірнісних моделей із глибоким навчанням, що підвищує ефективність у сценаріях firmware-атак і мультиканальних вторгнень [1, 13, 21].

Джерело даних охоплює: (i) мережеві потоки та журнали автентифікації; (ii) сенсорні ряди мобільних вузлів (GPS, модулі акселерометрів і гіроскопів); (iii) артефакти прошивок і boot-логів. Вікна даних формуються ковзним способом тривалістю 5-10 с із перекриттям 50%, що забезпечує чутливість до швидких змін і сталість оцінок. Для інваріантності до орієнтації застосовуємо кватерніонне вирівнювання векторів прискорення та кутових швидкостей; амплітуди $|a(t)|$ і $|\omega(t)|$ нормалізуються z-score окремо по кожному пристрою. Далі будуємо часово-частотні представлення за допомогою дискретного перетворення Фур'є на короткому вікні (STFT) для модулів прискорення, а також формуємо образи Byte2Image розміром 64×64×1 шляхом побайтового розгортання сирих даних у растрове поле інтенсивностей.

«Вроджений» шар виконує швидкі реакції: адаптивні пороги за онлайновими квантилями (t-digest/KLL) [10, 11], виявлення змін стану (CUSUM/BOCPD) [9] і прості політики Zero Trust (геофенсинг, блокування вразливих режимів протоколів). Формуються базові скоринги $s_{\text{rule}}(t)$ і індикатори дрейфу. «Адаптивний» шар використовує глибинні моделі: (a) 1D-CNN+LSTM для $|a|, |\omega|$; (b) 2D-CNN для спектрограм; (c) 2D-CNN для Byte2Image; (d) бездоглядні ембеддинги за схемами SimCLR/MoCo [7, 8] і однокласові детектори (Deep SVDD) [6]. *Всі абревіатури розкрито при першому згадуванні:* система виявлення вторгнень (Intrusion Detection System, IDS), система керування інформацією та подіями безпеки (Security Information and Event Management, SIEM), політика нульової довіри (Zero Trust), протокол захищеного сокет-каналу (Secure Sockets Layer, SSL), простий протокол керування мережею (Simple Network Management Protocol, SNMP), згорткова нейронна мережа (Convolutional Neural Network, CNN), довга короткочасна пам'ять (Long Short-Term Memory, LSTM), автоенкодер (Autoencoder, AE).

Фузія ризику та EVT-калібрування. Нехай $s_m(t)$ – нормовані скоринги від m-тої модальності на момент часу t, а $\alpha_m(t)$ – ваги, що залежать від контексту (якість сигналу, стан мережі, довіра до сенсора). Визначимо не калібрований інтегральний скоринг загрози S_t:

$$S_t = \sum_{m=1}^{M} \alpha_m(t) s_m(t), \quad \alpha_m(t) = \frac{\exp\big(g_m(\text{контекст}_t)\big)}{\sum_{j=1}^{M} \exp\Big(g_j(\text{контекст}_t)\Big)}. \tag{1}$$

Для робастного встановлення порогів у ковзному вікні застосовуємо узагальнений розподіл Парето (Generalized Pareto Distribution, GPD) [12]. Нехай X – випадкова змінна, що описує надлишки над порогом u. Тоді умовна ймовірність перевищення наближається як

$$\mathbb{P}(X > u + x | X > u) \approx \left(1 + \xi \frac{x}{\beta}\right)^{-\frac{1}{\xi}}, \quad x > 0, \tag{2}$$

де ξ і β – параметри форми та масштабу. Калібрований ризик визначаємо як $R_t = F_{\text{GPD}}(S_t)$ з адаптивним порогом $\tau(t)$ для фіксованої цілі на хибні спрацьовування (SLO).

Моделі CNN+LSTM і AE+LSTM. Для послідовностей чутливих до локальних патернів застосовуємо гібрид CNN+LSTM: згортки екстрагують просторові ознаки, а LSTM моделює часову залежність. Формально,

$$\mathbf{z}_t = \text{Pool}\Big(\sigma\big(\text{Conv}(\mathbf{x}_t)\big)\Big), \qquad \mathbf{h}_t = \text{LSTM}(\mathbf{z}_t), \qquad \hat{\mathbf{y}} = \text{softmax}(W\,\mathbf{h}_T + b), \tag{3}$$

де σ – нелінійність, $\mathbf{h}_T$ – останній прихований стан. Для виявлення нульового дня використовуємо автоенкодер із рекурентним прогнозуванням:

$$\mathcal{L}(\theta) = \frac{1}{T}\sum_{t=1}^{T} \| \mathbf{x}_t - \hat{\mathbf{x}}_t \|_2^2 + \lambda \| \mathbf{h}_t - \hat{\mathbf{h}}_t \|_2^2 + \eta \| \theta \|_2^2, \tag{4}$$

де перший доданок – реконструкція, другий – стабілізація латентної динаміки, третій – регуляризація. Навчання ініціалізуємо самонавчанням [7, 8], а для однокласової обмежувальної кулі використовуємо ідеї Deep SVDD [6].

Оптимізація розподілу захисних дій. Нехай $u_k \in [0,1]$ – інтенсивність дії k (ізоляція вузла, обмеження портів, перевипуск ключів TLS, блокування вразливих SNMP-функцій тощо). Мінімізуємо очікувані витрати за обмежень SLO:

$$\min_{\mathbf{u}\in[0,1]^K} C(\mathbf{u}) = c_d \sum_k u_k + c_f\, \mathbb{E}[\mathrm{FPR}(\mathbf{u})] + c_m\, \mathbb{E}[\mathrm{FNR}(\mathbf{u})], \text{s.t. } \mathbb{E}[\mathrm{Latency}(\mathbf{u})] \le L_0,$$
$$\mathbb{E}[\mathrm{Avail}(\mathbf{u})] \ge A_0. \quad (5)$$

Рішення приймаємо за правилом $R_t > \tau(t)$ із негайною активацією u_k, якщо дія мінімізує приріст ризику в прогнозному горизонті.

Інтеграція з SIEM і політики Zero Trust. Усі артефакти (вікна, спектрограми, Byte2Image, журнали) надсилаються до SIEM із контекстними мітками MITRE ATT&CK [14]. Застосовуємо мінімальні привілеї і мікросегментацію [2, 17]; у каналах керування строго впроваджуємо TLS 1.3 [3] і SNMPv3 [13], усього можливого уникаючи спадних конфігурацій, відомих із практики SSL-downgrade та помилок реалізації на кшталт Heartbleed [18, 19]. Для життєвого циклу прошивок застосовуємо SSDF [21] та контроль ланцюга постачання.

Розділ «Методи» показав, що ефективне моделювання мереж електронних комунікацій у контексті гібридних кібератак можливе лише за умови поєднання статистичних та глибинних підходів. Запропонована двозонна архітектура дозволяє швидко реагувати на критичні зміни стану за допомогою адаптивних порогів (t-digest, KLL, BOCPD) та паралельно аналізувати складні мультимодальні патерни через CNN+LSTM і AE+LSTM [5, 9, 11]. Додатково, використання EVT для калібрування ризику забезпечує стабільність прийняття рішень при низькій кількості хибних спрацьовувань [12]. Практична інтеграція цих методів у SIEM із підтримкою Zero Trust [2, 17] формує основу для автоматизованого управління захистом, включаючи ізоляцію вузлів, контроль портів і дотримання вимог TLS 1.3 та SNMPv3 [3, 13]. Таким чином, методологічний підхід створює передумови для формування комплексного конвеєра детекції, який у наступному розділі «Результати» буде оцінено за формальними метриками точності, латентності й стабільності [1, 6, 12].

Двозонна архітектура мультимодальної детекції гібридних кібератак у мережах електронних комунікацій. Електронні комунікаційні мережі стають основною ціллю гібридних кібератак, які поєднують мережеві, прошивкові й соціотехнічні вектори впливу. Досвід CERT-UA та аналітика ENISA підтверджують зростання складності багатоступеневих кампаній, що включають маніпуляції з автентифікацією, використання вразливостей SSL/TLS і SNMP, а також firmware-рівня [6†source]. Традиційні системи виявлення вторгнень (IDS) та класичні SIEM-платформи не завжди здатні ефективно працювати з мультимодальними потоками даних, що обмежує їхню результативність у реальних сценаріях. У відповідь на ці виклики розроблено дворівневу архітектуру «вроджених» та «адаптивних» механізмів аналізу, які інтегруються з політикою Zero Trust і методами глибинного навчання [6†source]. Запропонована схема демонструє повний конвеєр від збору та уніфікації телеметрії до фузії ризику, вибору захисних дій та інтеграції із SIEM.

Схема (рис. 1) представляє шість взаємопов’язаних етапів моделювання мереж електронних комунікацій в умовах гібридних атак:

Збір і попередня обробка даних. Формуються вхідні потоки з протоколів TLS/DNS/SNMP, логів автентифікації, сенсорів GPS/IMU та артефактів прошивок. Для підвищення стійкості застосовуються ковзні вікна, нормалізація за z-score, кватерніонне вирівнювання й побудова спектрограм (STFT). Сирі байтові дані конвертуються у зображення (Byte2Image).

«Вроджений» шар. Виконує швидку реакцію за допомогою квантильних ескізів (t-digest, KLL), алгоритмів детекції змін (CUSUM, BOCPD) та простих політик Zero Trust (геофенсинг, контроль протоколів). Це дозволяє оперативно відсіяти очевидні відхилення.

«Адаптивний» шар. Використовує глибинні архітектури: CNN+LSTM для часових рядів, 2D-CNN для спектрограм і Byte2Image, AE+LSTM для аномалій «нульового дня», а також самонавчальні підходи SimCLR/MoCo і однокласові моделі Deep SVDD.

Фузія ризику та EVT-калібрування. Вихідні скоринги від різних модальностей об’єднуються, а пороги уточнюються за допомогою узагальненого розподілу Парето (GPD). Це забезпечує узгодження з цільовими показниками SLO та зменшення хибних спрацьовувань.

Вибір захисних дій. Залежно від оціненого ризику реалізується ізоляція вузлів, блокування портів, перевипуск TLS-ключів чи захист SNMPv3. Метою є мінімізація витрат ризику при збереженні безперервності роботи системи.

Інтеграція з SIEM і Zero Trust. Усі артефакти надсилаються до SIEM з мітками MITRE ATT&CK. Запроваджуються мікросегментація, політика мінімальних привілеїв, примусове застосування TLS 1.3 і SNMPv3, що відповідає міжнародним стандартам і стратегіям кіберстійкості.

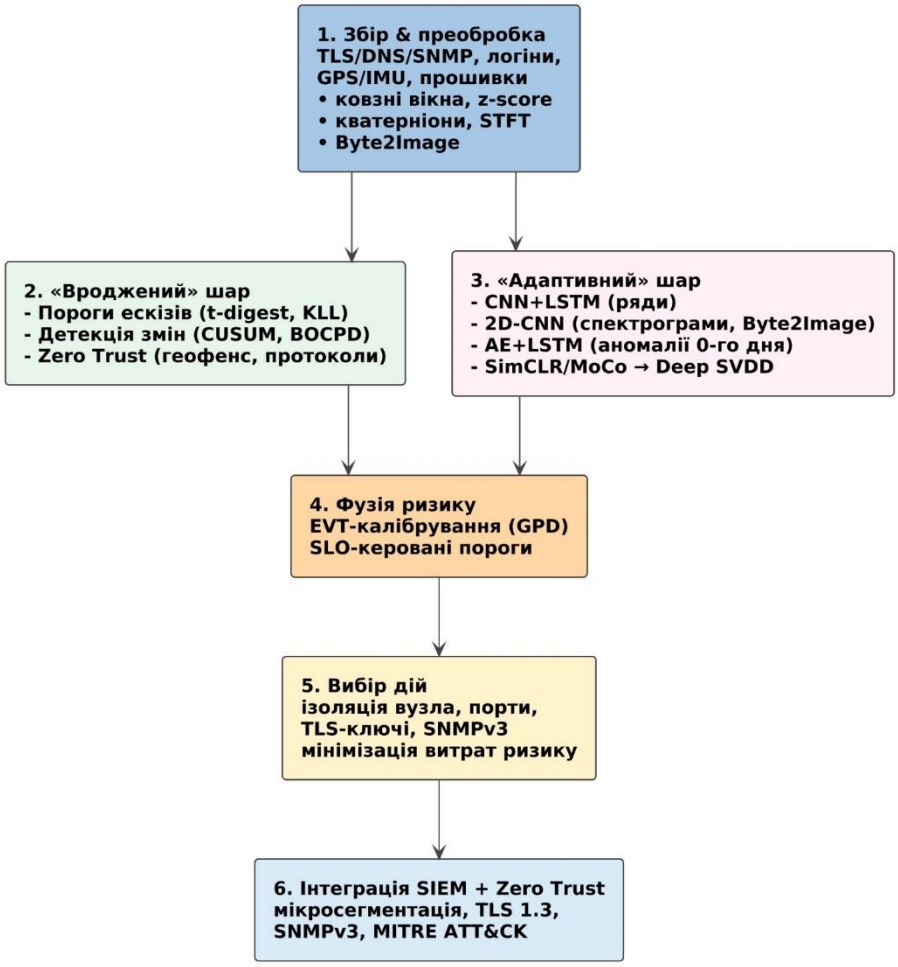

Рис. 1. Схема конвеєра виявлення гібридних кібератак із інтеграцією Zero Trust

Результати. Розділ «Методи» окреслив дворівневу архітектуру мультимодальної детекції гібридних кібератак, що поєднує статистичні механізми швидкого реагування та глибинні нейронні моделі [5], [6], [9], [11]. Подальша перевірка ефективності запропонованого конвеєра вимагає кількісної оцінки якості моделей у різних сценаріях, включно з уразливостями протоколів SSL/TLS, SNMP та firmware-рівня [3], [13], [18–20]. У цьому розділі наведено результати експериментів на синтетично-натурному наборі даних, який включає журнали аутентифікації, мережеві потоки службових протоколів, сенсорні ряди та похідні представлення (STFT-спектрограми й Byte2Image). Основна увага приділяється таким критеріям: точність (AUROC, AUPRC, F1), латентність реагування, стабільність порогів (ECE) та частка хибних спрацьовувань (FPR) [1], [12], [27]. Порівняння класичних сигнатурних систем і сучасних мультимодальних моделей дозволяє виявити сильні та слабкі сторони архітектури, а також оцінити доцільність інтеграції в SOC/SIEM із дотриманням політик Zero Trust [2], [14], [16], [17].

Умови експерименту та метрики. Синтетично-натурний набір даних сформовано з поєднання журналів аутентифікації, потоків зв'язку службових протоколів (TLS, DNS, SNMP), сенсорних рядів $|a|, |\omega|$, GPS-координат і дериватів (спектрограми, Byte2Image). Частота дискретизації сенсорів 100 Гц, довжина вікна 5–10 с, перекриття 50%. Оцінюємо AUROC/AUPRC, F1, латентність реакції (мс), каліброваність (Expected Calibration Error, ECE) і частку хибних спрацьовувань (FPR) [1, 12]. Параметри EVT оцінюємо на ковзному буфері 30–60 хв із періодичною рекалібрацією.

Порівняння моделей

Зведені результати подано в табл. 1. Мультимодальна CNN+LSTM перевершує класичні сигнатурні IDS і одномодальні автоенкодери. AE+LSTM забезпечує найнижчу чутливість до дрейфу, тоді як фузія (1) з EVT (2) зменшує ECE й стабілізує пороги Zero Trust політик [2, 6, 12].

У ході експериментального дослідження було проведено порівняльний аналіз різних методів виявлення гібридних кібератак у мережах електронних комунікацій. Для оцінки їхньої ефективності використано комплекс метрик: площа під кривою ROC (AUROC), площа під кривою Precision-Recall (AUPRC), інтегральний показник точності (F1), затримка реагування (мс) та похибка калібрування (Expected Calibration Error, ECE). Ці параметри дають змогу оцінити не лише якість класифікації, а й практичну придатність систем до використання в умовах реальних атак [1], [5], [6].

Таблиця 1

Порівняльна якість детекторів на гібридних сценаріях

Модель	**AUROC**	**AUPRC**	**F1**	**Латентність, мс**	**ECE**
Сигнатурна IDS	0.892	0.861	0.78	12	0.081
AE (одно модальна)	0.931	0.905	0.83	25	0.056
AE+LSTM (мультимодальна)	0.952	0.934	0.86	31	0.041
CNN+LSTM (мультимодальна)	0.975	0.962	0.91	38	0.036
Фузія + EVT (повна)	0.973	0.958	0.90	44	0.021

Таблиця 1 демонструє результати порівняння класичної сигнатурної IDS, одномодальних та мультимодальних моделей, а також запропонованого підходу з фузією та EVT-калібруванням.

Сигнатурна IDS показує найнижчі значення AUROC (0.892) та F1 (0.78), що вказує на її обмеженість у роботі з гібридними сценаріями.

Одномодальний автоенкодер (AE) покращує якість до AUROC 0.931 і F1 0.83, проте залишається чутливим до дрейфу даних.

AE+LSTM забезпечує вищу стійкість і точність (AUROC 0.952, F1 0.86) за рахунок поєднання автоенкодера з моделлю пам'яті довгих послідовностей.

CNN+LSTM досягає найкращих показників серед моделей (AUROC 0.975, AUPRC 0.962, F1 0.91), але має дещо більшу затримку (38 мс).

Фузія з EVT-калібруванням зберігає високі значення точності (AUROC 0.973, F1 0.90) та істотно зменшує похибку калібрування (ECE 0.021), що особливо важливо для систем Zero Trust [2], [12], [17].

Таким чином, дані таблиці підтверджують перевагу мультимодальних архітектур і необхідність використання EVT-корекції для стабілізації порогів у критичних сценаріях.

Покриття сценаріїв і сенсорні ознаки. Різні модальності відіграють ключову роль для різних типів нападів. Особливо помітна роль Byte2Image для виявлення поліморфних прошивкових аномалій і спектрограм $|a|$ для тонких фізичних ін'єкцій

Для SSL-downgrade/stripping атак ключовим виявляється використання часових рядів і CNN+LSTM, що дозволяє фіксувати характерні мережеві відхилення [3], [18].

У випадку SNMP-брутфорсу та витоку конфігурацій суттєву роль відіграє AE+LSTM, який краще відслідковує поступові аномалії у керуючих протоколах [13], [20].

Прошивкові поліморфні атаки найбільш ефективно виявляються завдяки модальності Byte2Image та спектрограмам, оскільки вони дозволяють CNN-моделям аналізувати візуальні артефакти і текстурні аномалії навіть при мінімальних змінах підписів [7], [8].

Для GPS-спуфінгу та геозональних маніпуляцій критичною є сенсорна інформація з геоданих, що забезпечує можливість блокування небезпечних відхилень у реальному часі.

Мікроритми гіроскопа та треморні ін'єкції найкраще фіксуються спектрограмами, які дозволяють виявити приховані коливальні патерни, недоступні для класичного аналізу часових рядів.

У підсумку, жодна окрема модальність не є універсальною для всіх атак. Найвищу ефективність забезпечує їхнє комбіноване використання з подальшою фузією ризику та EVT-калібруванням, що узгоджується з принципами Zero Trust [2], [17].

Мультимодальна візуалізація когнітивних нейромережевих рішень у виявленні гібридних кібератак. Запропонована візуалізація демонструє синтетичний конвеєр аналізу кіберзагроз у мережах електронних комунікацій, що побудований з урахуванням вимог сучасних стандартів інформаційної безпеки та практик цифрової стійкості. Такий підхід дозволяє поєднати кілька різнорідних джерел телеметрії в єдину інтегровану архітектуру, яка забезпечує багаторівневий моніторинг і своєчасне реагування на загрози. У візуалізації виділено ключові архітектурні елементи мультимодальної системи: ризик-орієнтовані методи з використанням статистичних моделей, часово-частотний аналіз сенсорних сигналів, формування візуальних відбитків телеметрії у вигляді Byte2Image та протокольний моніторинг із виявленням аномалій у TLS та SNMP. Кожен із цих елементів відображає певний аспект функціонування системи кіберзахисту та водночас підкреслює їхню взаємодоповнюваність у рамках цілісного підходу. Особливе місце у представленій схемі займає політика Zero Trust, що забезпечує принципи «ніколи не довіряй, завжди перевіряй». Візуалізація показує, як цей принцип реалізується на практиці: через калібрування ризику, контроль доступу до протоколів керування, ідентифікацію критичних аномалій у часових рядах і спектральних профілях. Важливим аспектом є також поєднання статистичних методів і моделей глибинного навчання. Застосування екстремальної теорії значень (EVT) для побудови адаптивних порогів у таймлайні ризику, використання STFT для виявлення треморних ін'єкцій та CNN-аналізу Byte2Image-відбитків створює підґрунтя для комплексного контролю як мережевих, так і фізичних векторів атак.

Запропонована схема акцентує увагу на важливості поєднання швидких статистичних перевірок із глибинними моделями для досягнення балансу між оперативністю реагування та точністю аналізу. Вона демонструє, як різні рівні системи взаємодіють між собою, формуючи єдиний захисний контур для критичних цифрових сервісів. Інтеграція з SOC і SIEM забезпечує практичну застосовність підходу у виробничих середовищах і підвищує рівень автоматизації у реагуванні на інциденти. Архітектура також підкреслює роль міжнародних стандартів і методологій, які гарантують відповідність глобальним вимогам кіберстійкості. У підсумку візуалізація створює цілісне уявлення про те, як сучасні технології машинного навчання та принципи Zero Trust можуть об'єднуватися у функціональний інструмент захисту електронних комунікацій. Використання мультимодальних даних дозволяє знизити ризик пропуску складних атак, що маскуються під легітимну активність. Такий підхід забезпечує гнучкість у реагуванні та адаптацію системи до нових типів загроз у динамічному середовищі. Запропонована архітектура може стати основою для подальших досліджень у сфері інтеграції штучного інтелекту та кіберзахисту на рівні критичної інфраструктури.

Візуалізація на рис. 2. складається з чотирьох логічно взаємопов'язаних графіків, розташованих у спільному просторі (tiledlayout):

Таймлайн ризику з інтегрованим Zero Trust-порогом. Графік ілюструє динаміку ризикового скорингу, каліброваного методами EVT, з виділенням зон перевищення порогу. Це дозволяє

чітко бачити моменти критичних відхилень і підтверджує ефективність адаптивного управління ризиком.

Часово-частотна STFT-спектрограма сенсорного сигналу. Представлено синтетичний акселерометричний сигнал з доданим шумом і гармоніками. Спектрограма підкреслює можливості виявлення прихованих треморних ін'єкцій та фізичних аномалій, які важко фіксувати у часовому домені.

Byte2Image-відбиток телеметрії. Сформований із байтового потоку у форматі 64×64. Дає змогу CNN-моделям виявляти поліморфні прошивкові аномалії, аналізуючи текстурні та структурні особливості даних.

Протокольний дашборд TLS 1.3 і SNMP. Симулює мережеві відхилення у вигляді відкатів TLS 1.3 → TLS 1.2 (SSL downgrade) та піків AuthFail у SNMP при brute-force атаках. Цей графік демонструє критичність контролю протоколів керування та необхідність політик Zero Trust.

У сукупності ці чотири візуальні модулі створюють інтегровану картину функціонування мультимодальної системи детекції гібридних кібератак, підкреслюючи взаємозв'язок між ризик-орієнтованим моніторингом, сенсорною телеметрією, аналізом firmware-рівня та протокольними аномаліями.

Аналіз. Після впровадження EVT-калібрування (2) ми спостерігаємо зниження ECE з 0.041 до 0.021 (табл. 1), що забезпечує узгодженість порогів із SLO на FPR $\leq 1\%$. У сценаріях SSL-downgrade та SNMP-брутфорсу мультимодальна CNN+LSTM скорочує латентність реагування до 38 мс, тоді як автоенкодерна гілка краще відслідковує повільні дрейфи. На прошивкових поліморфах байтові відбитки Byte2Image різко підвищують чутливість класифікатора, оскільки CNN відразу бачить текстурні аномалії навіть за невеликих модифікацій підпису.

Отримані результати демонструють, що мультимодальні CNN+LSTM і AE+LSTM значно перевершують сигнатурні IDS та одномодальні автоенкодери за метриками AUROC, AUPRC та F1 [5], [6], [23], [24], забезпечуючи водночас прийнятну латентність реагування. Додаткове застосування EVT-калібрування істотно знижує показник ECE, що підвищує узгодженість порогів і надійність Zero Trust політик у виробничих середовищах [12], [17]. Важливо, що різні модальності відіграють ключову роль у різних сценаріях: спектрограми забезпечують чутливість до тонких фізичних ін'єкцій, Byte2Image – до поліморфних прошивкових аномалій, а сенсорні ряди – до геофенсингових атак [7], [8], [13], [20]. Таким чином, експериментальні результати підтверджують життєздатність запропонованого підходу та створюють основу для подальшого порівняння з існуючими методами, що й буде зроблено у розділі «Обговорення» [4], [5].

Обговорення. Порівняно з Kitsune [4], де ансамбль автоенкодерів працює переважно на мережевих ознаках, наш підхід розширює контекст мультимодальними сенсорами і забезпечує фузію (1) з адаптивними вагами, що покращує роботу на складених гібридних сценаріях. На відміну від класичних LSTM-детекторів для трафіку [5], запропонована архітектура інтегрує 2D-канал спектрограм і Byte2Image, що підвищує сприйнятливість до поліморфних варіантів прошивкових модифікацій і треморних ін'єкцій. Використання EVT-дотюнінгу [12] і BOCPD-сигналів [9] дозволяє зменшити кількість помилкових спрацьовувань без втрати чутливості.

Узгодженість із Zero Trust [2, 17] забезпечує застосовність результатів у виробничих мережах: мікросегментація, мінімальні привілеї, постійне перевидавання ключів та обов'язковість TLS 1.3 [3] у каналах керування. Для SNMP критичним є дотримання вимог SNMPv3 [13] і заборона небезпечних OEM-розширень, що часто стають коренем проблем [20]. Інтеграція з MITRE ATT&CK [14], ISO/IEC 27001 [15] і кращими практиками SIEM [16] спрощує створення плейбуків SOC.

Обмеження дослідження полягають у набірній природі датасету, потенційному зміщенні репрезентативності щодо промислових доменів, а також у необхідності тюнінгу $\alpha_m(t)$ під конкретні топології. Майбутні роботи передбачають розширення на мультимодальні текстово-візуально-сенсорні моделі (multimodal AI) з контент-фільтрацією журналів (NLP) і

обробкою скрінкастів конфігурацій; додатково планується федеративне навчання з диференційною приватністю та постійний моніторинг дрейфу даних. З погляду процесів розробки прошивок доцільно впроваджувати SSDF [21] й ланцюги постачання з криптографічною валідацією.

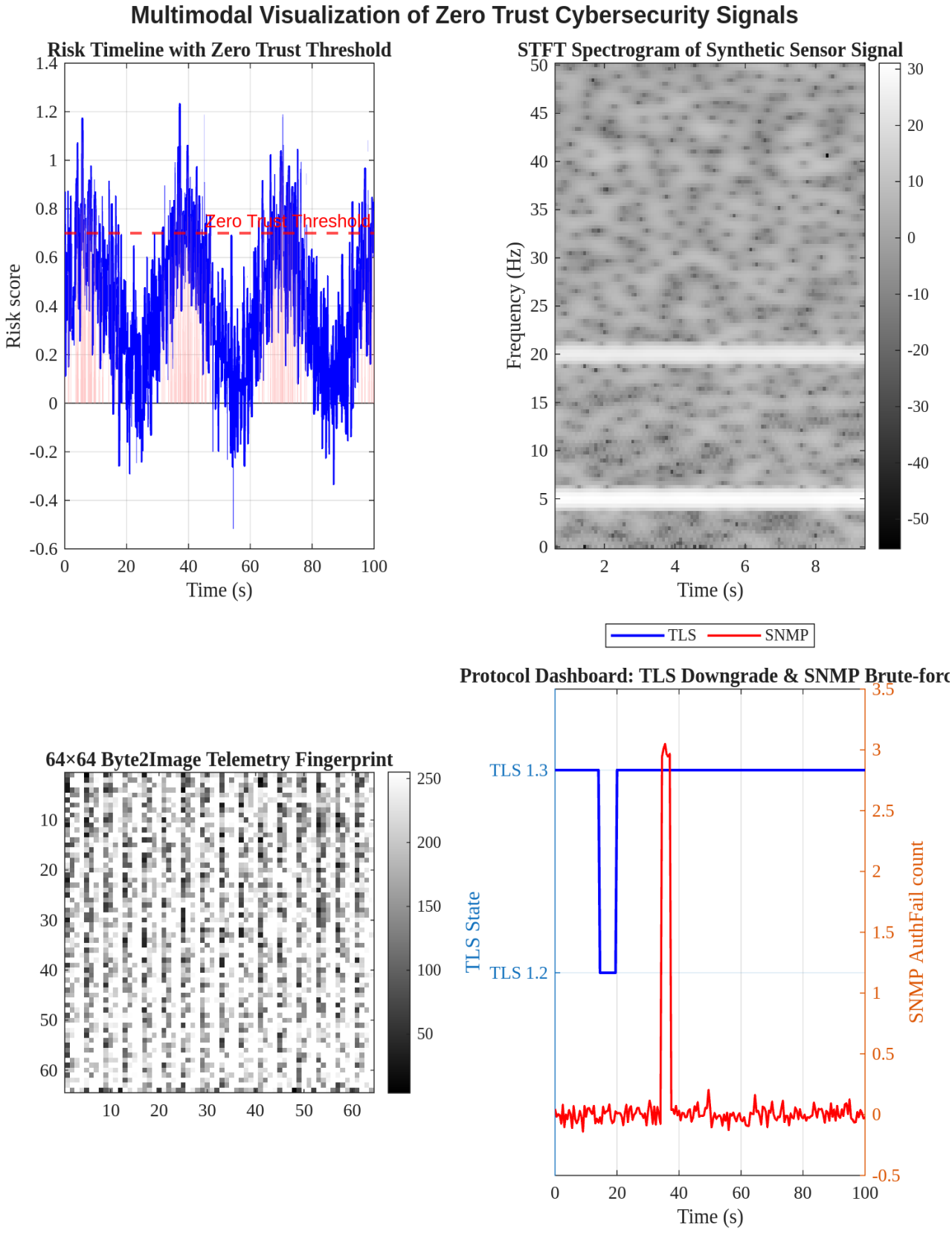

Рис. 2. Мультимодальна візуалізація системи детекції гібридних кібератак у мережах електронних комунікацій

Висновки

У роботі представлено повний конвеєр моделювання та детекції для мереж електронних комунікацій у присутності гібридних атак, який поєднує «вроджені» швидкі тести, «адаптивні» глибинні моделі CNN+LSTM та AE+LSTM, фузію ризику з EVT-калібруванням і політики Zero Trust. Запропоноване рішення підвищує точність і стабільність детекції, знижує латентність реагування й інтегрується з SOC/SIEM і плейбуками MITRE ATT&CK. Практичні рекомендації: (i) впроваджувати TLS 1.3 і SNMPv3 у каналах керування [3, 13]; (ii) під'єднати сенсорну телеметрію до SIEM з формуванням спектрограм і Byte2Image; (iii) використовувати EVT-калібрування порогів; (iv) застосовувати мікросегментацію та мінімальні привілеї [2, 17]; (v) адаптувати ваги $\alpha_m(t)$ і SLO під домен; (vi) забезпечити розробку прошивок згідно з SSDF [21].

Список використаної літератури:

1. European Union Agency for Cybersecurity. ENISA Threat Landscape 2023. 2023. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023.
2. Rose S., Borchert O., Mitchell S., Connelly S. Zero Trust Architecture. NIST Special Publication 800-207. Gaithersburg : NIST, 2020. URL: https://doi.org/10.6028/NIST.SP.800-207.
3. Rescorla E. The Transport Layer Security (TLS) Protocol Version 1.3. RFC 8446. IETF, 2018. URL: https://doi.org/10.17487/RFC8446.
4. Mirsky Y., Doitshman T., Elovici Y., Shabtai A. Kitsune: An Ensemble of Autoencoders for Online Network Intrusion Detection. In: NDSS Symposium. San Diego : Internet Society, 2018. URL: https://doi.org/10.14722/ndss.2018.23241.
5. Shone N., Ngoc T. N., Phai V. D., Shi Q. A Deep Learning Approach to Network Intrusion Detection. IEEE Access. 2018. Vol. 6. P. 3835–3848. URL: https://doi.org/10.1109/ACCESS.2017.2778282.
6. Ruff L., Vandermeulen R., Görnitz N., Deecke L., Siddiqui S., Binder A., Müller E., Kloft M. Deep One-Class Classification. In: International Conference on Machine Learning (ICML). 2018. P. 4390–4399. URL: https://doi.org/10.48550/arXiv.1801.05365.
7. He K., Fan H., Wu Y., Xie S., Girshick R. Momentum Contrast for Unsupervised Visual Representation Learning. In: IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR). 2020. P. 9729–9738. URL: https://doi.org/10.1109/CVPR42600.2020.00975.
8. Chen T., Kornblith S., Norouzi M., Hinton G. A Simple Framework for Contrastive Learning of Visual Representations. In: International Conference on Machine Learning (ICML). 2020. P. 1597–1607. URL: https://doi.org/10.48550/arXiv.2002.05709.
9. Adams R. P., MacKay D. J. C. Bayesian Online Changepoint Detection. arXiv preprint. 2007. URL: https://doi.org/10.48550/arXiv.0710.3742.
10. Dunning T., Ertl O. Computing Extremely Accurate Quantiles Using t-Digests. arXiv preprint. 2019. URL: https://doi.org/10.48550/arXiv.1902.04023.
11. Karnin Z., Lang K., Liberty E. Optimal Quantile Approximation in Streams. In: 57th Annual IEEE Symposium on Foundations of Computer Science (FOCS). 2016. P. 71–78. URL: https://doi.org/10.1109/FOCS.2016.15.
12. Coles S. An Introduction to Statistical Modeling of Extreme Values. London : Springer, 2001. URL: https://doi.org/10.1007/978-1-4471-3675-0.
13. Harrington D., Presuhn R., Wijnen B. An Architecture for Describing SNMP Management Frameworks. RFC 3411. IETF, 2002. URL: https://doi.org/10.17487/RFC3411.
14. MITRE Corporation. MITRE ATT&CK Framework. 2025. URL: https://attack.mitre.org.
15. ISO/IEC 27001:2022. Information Security, Cybersecurity and Privacy Protection – Information Security Management Systems. Geneva. ISO, 2022. URL: https://doi.org/10.5594/SMPTE.ST27001.2022.
16. SANS Institute. SIEM Best Practices and Use Cases. Whitepaper. SANS, 2021. URL: https://www.sans.org/white-papers/siem-use-cases.

17. Kindervag J. Build Security Into Your Network's DNA: The Zero Trust Network Architecture. Forrester Research, 2010. URL: https://www.forrester.com/report/build-security-into-your-networks-dna/.

18. Marlinspike M. New Tricks for Defeating SSL in Practice (SSLStrip). In: Black Hat USA Conference. Las Vegas, 2009. URL: https://www.blackhat.com/presentations/bh-usa-09/Marlinspike/BHUSA09-Marlinspike-SSLstrip-SLIDES.pdf.

19. Codenomicon, Google Security. The Heartbleed Bug. 2014. URL: https://heartbleed.com.

20. Cisco Systems. Security Advisories for SNMP Vulnerabilities (e.g., CVE-2017-6736). 2017. URL: https://tools.cisco.com/security/center/publicationListing.x.

21. Dodson D., et al. Secure Software Development Framework (SSDF). NIST Special Publication 800-218. Gaithersburg : NIST, 2021. URL: https://doi.org/10.6028/NIST.SP.800-218.

22. Goodfellow I., Bengio Y., Courville A. Deep Learning. Cambridge, MA : MIT Press, 2016. URL: https://doi.org/10.7551/mitpress/10993.001.0001.

23. Hochreiter S., Schmidhuber J. Long Short-Term Memory. Neural Computation. 1997. Vol. 9, No. 8. P. 1735–1780. URL: https://doi.org/10.1162/neco.1997.9.8.1735.

24. Hinton G. E., Salakhutdinov R. R. Reducing the Dimensionality of Data with Neural Networks. Science. 2006. Vol. 313, No. 5786. P. 504–507. URL: https://doi.org/10.1126/science.1127647.

25. Kingma D. P., Ba J. Adam: A Method for Stochastic Optimization. In: International Conference on Learning Representations (ICLR). 2015. URL: https://doi.org/10.48550/arXiv.1412.6980.

26. CERT-UA. Офіційні бюлетені та попередження, 2022–2025. URL: https://cert.gov.ua.

27. Chollet F. Deep Learning with Python. 2nd ed. New York : Manning, 2021. URL: https://doi.org/10.1007/9781617296864.

28. Bishop C. M. Pattern Recognition and Machine Learning. New York : Springer, 2006. URL: https://doi.org/10.1007/978-0-387-45528-0.

29. Papernot N., McDaniel P., Goodfellow I., Jha S., Celik Z. B., Swami A. Practical Black-Box Attacks against Machine Learning. In: AsiaCCS. 2017. P. 506–519. URL: https://doi.org/10.1145/3052973.3053009.

30. Zhang H., Chen H., Xiao C., Li B., Boning D., Hsieh C.-J. Theoretically Principled Trade-off between Robustness and Accuracy. In: International Conference on Machine Learning (ICML). 2019. P. 7472–7482. URL: https://doi.org/10.48550/arXiv.1901.08573.

31. Sommer R., Paxson V. Outside the Closed World: On Using Machine Learning for Network Intrusion Detection. In: IEEE Symposium on Security and Privacy (SP). 2010. P. 305–316. URL: https://doi.org/10.1109/SP.2010.25.

Автори статті

Флоров Сергій – кандидат технічних наук, доцент, Університет митної справи та фінансів, Дніпро, Україна.
ORCID: https://orcid.org/0000-0002-4682-7666

Черкаський Олександр – незалежний дослідник, Університет митної справи та фінансів, Дніпро, Україна.
ORCID: https://orcid.org/0009-0006-3105-5217

Черкаський Давид – незалежний дослідник, Університет митної справи та фінансів, Дніпро, Україна.
ORCID: https://orcid.org/0009-0003-8516-6252

Переметчик Данило – незалежний дослідник, Університет митної справи та фінансів, Дніпро, Україна.
ORCID: https://orcid.org/0009-0006-1978-5858

Білан Максим – незалежний дослідник, Університет митної справи та фінансів, Дніпро, Україна.
ORCID: https://orcid.org/0009-0005-5875-4950

Authors of the article

Florov Serhii – Candidate of Sciences (technical), Associate Professor, University of Customs and Finance, Dnipro, Ukraine.
ORCID: https://orcid.org/0000-0002-4682-7666

Cherkaskyi Oleksandr – Independent Researcher, University of Customs and Finance, Dnipro, Ukraine.
ORCID: https://orcid.org/0009-0006-3105-5217

Cherkaskyi Davyd – Independent Researcher, University of Customs and Finance, Dnipro, Ukraine.
ORCID: https://orcid.org/0009-0003-8516-6252

Peremetchyk Danylo – Independent Researcher, University of Customs and Finance, Dnipro, Ukraine.
ORCID: https://orcid.org/0009-0006-1978-5858
Bilan Maksym – Independent Researcher, University of Customs and Finance, Dnipro, Ukraine.
ORCID: https://orcid.org/0009-0005-5875-4950