навіть неявні зв'язки між різними джерелами даних, що робить їх особливо цінними для виявлення багатоетапних атак (Advanced Persistent Threats, APT). Оглядові праці [1, 2] та емпіричне дослідження [3] наголошують, що в реальних SOC доцільно застосовувати LLM, як інструмент підтримки аналітика, залишаючи остаточне рішення за людиною. При цьому ключовою вимогою є забезпечення пояснюваності (explainability) – аналітик має розуміти, на яких підставах модель робить той чи інший висновок.

Аналіз журналів є центральним напрямом для семантично орієнтованих систем. У роботі LogParser-LLM [4] показано, що врахування семантики повідомлення, а не лише його синтаксичної форми, підвищує якість парсингу динамічних журналів; модель викликається не для кожного запису, а в контрольованих точках, що забезпечує масштабованість. LogPrecis [5] переходить від окремих команд оболонки до послідовності намірів зловмисника та формує відбиток атаки, наближаючи аналіз до методології ATT&CK. Підхід LogPrompt [6] демонструє інтерпретований аналіз журналів із застосуванням стратегій формування запитів (zero-shot, few-shot, chain-of-thought) і одночасним генеруванням текстових пояснень, що зменшує когнітивне навантаження на аналітика. Окремої уваги заслуговує можливість використання LLM для збагачення журналів додатковими метаданими, зокрема геолокацією, типами активності користувачів або історією їхніх дій, що дозволяє будувати більш повну картину інциденту.

Другу групу становлять завдання виявлення вразливостей і атак. APPATCH [7] використовує адаптивне формування запитів і врахування семантики під час аналізу коду; Rondanini та співавтори [8] досліджують виявлення шкідливого програмного забезпечення на периферії за допомогою полегшених (lightweight) LLM; Alnahdi та Narain [9] зосереджуються на узгодженості пояснень IDS із доменними знаннями; AECR [10] автоматично вилучає відомості про техніки атак із звітів кіберрозвідки (Cyber Threat Intelligence, CTI) на основі донавченої моделі. Спільним висновком є те, що LLM працюють краще, коли отримують структурований контекст і керований процес міркування, а не весь інформаційний шум. Це підтверджує доцільність побудови гібридних систем, де LLM взаємодіє з класичними детекторами, отримуючи від них попередньо відфільтровані дані та зосереджуючись на найбільш складних або неоднозначних випадках.

Ключовим механізмом підвищення надійності є генерація з доповненням через пошук (RAG). Система RAGIntel [11] поєднує генеративні можливості LLM із пошуком у структурованих джерелах MITRE ATT&CK, що зменшує ризик галюцинацій і дає відповіді, підкріплені доказами. Для розроблення правил виявлення важливим є підхід Rule-ATT&CK Mapper (RAM) [12], що автоматично зіставляє правила SIEM із техніками ATT&CK за допомогою багатоетапного конвеєра та ланцюжка запитів без додаткового донавчання моделі. Це дає змогу оцінювати покриття технік і визначати прогалини у контенті виявлення.

На основі проаналізованих джерел запропоновано концепцію контрольованого семантичного шару для SOC. Він приймає нормалізовані події або групи сповіщень, використовує RAG для отримання релевантного контексту з бази знань (MITRE ATT&CK, сценарії реагування, історія інцидентів) і формує пояснювальну картку інциденту зі структурованим виходом: короткий опис, докази, підозрілі ознаки, ймовірні техніки ATT&CK, рівень упевненості, альтернативні пояснення та рекомендовані кроки перевірки. Такий шар не замінює SIEM, а доповнює його, скорочуючи час первинного сортування та підвищуючи якість розуміння складних атак. Провідним напрямом дисертаційного дослідження обрано поєднання семантичного збагачення сповіщень із RAG-інтеграцією кіберрозвідки за принципом human-in-the-loop.

Практичне впровадження потребує врахування обмежень LLM. Основними ризиками є галюцинації, ін'єкція інструкцій у запит (prompt injection), конфіденційність журналів, вартість і продуктивність, а також складність оцінювання пояснень. Це формує вимоги до методу: розділення даних та інструкцій, маскування чутливих полів, обмеження відповіді доказами, структурований вихід, аудит запитів і багаторівневе оцінювання якості (технічна правильність, корисність для аналітика, стійкість до маніпуляцій).

Висновки. Аналіз літератури 2024–2025 років свідчить, що великі мовні моделі доцільно застосовувати в SOC не як автономний засіб прийняття рішень, а як семантичний шар підтримки аналітика. Найперспективнішими напрямами є аналіз журналів на основі LLM та інтеграція знань через RAG із зіставленням поведінки з MITRE ATT&CK. Встановлено, що ключовою умовою успішного впровадження є поєднання трьох факторів: перше – керованої взаємодії з моделлю через структуровані запити, друге – зовнішнього контексту з перевірених джерел (RAG), третє – обов'язкової участі людини на етапі прийняття рішень. Науковою новизною подальшого дослідження є метод побудови контрольованого семантичного шару, що поєднує нормалізацію подій, пошук релевантних знань, структурований вихід, оцінювання достовірності та участь людини в контурі прийняття рішень. На відміну від існуючих підходів, запропонований метод забезпечує не лише пояснюваність і відтворюваність, але й адаптивність до змін у ландшафті загроз за рахунок інтеграції з актуальними базами знань і зворотним зв'язком від аналітиків. Такий підхід забезпечує пояснюваність, відтворюваність та інтеграцію з наявними засобами SOC. Перспективи подальших досліджень включають експериментальну верифікацію запропонованої архітектури на реальних даних SOC, порівняльний аналіз з класичними методами виявлення, а також дослідження впливу різних стратегій формування запитів на якість виявлення багатоетапних атак.

Література

1. Habibzadeh A., Feyzi F., Atani R. E. Large Language Models for Security Operations Centers: A Comprehensive Survey. arXiv:2509.10858. 2025.

2. Srinivas S., Kirk B., Zendejas J. et al. AI-Augmented SOC: A Survey of LLMs and Agents for Security Automation. Journal of Cybersecurity and Privacy. 2025. Vol. 5(4). 95.

3. Singh R., Tariq S., Chhetri M. B. et al. LLMs in the SOC: An Empirical Study of Human-AI Collaboration in Security Operations Centres. arXiv:2508.18947. 2025.

4. Zhong A., Mo D., Liu G. et al. LogParser-LLM: Advancing Efficient Log Parsing with Large Language Models. Proc. of the 30th ACM SIGKDD Conf. (KDD '24). 2024. DOI: 10.1145/3637528.3671810.

5. Boffa M., Drago I., Mellia M. et al. LogPrécis: Unleashing language models for automated malicious log analysis. Computers & Security. 2024. Vol. 141. 103805.

6. Liu Y., Tao S., Meng W. et al. Interpretable Online Log Analysis Using Large Language Models with Prompt Strategies. Proc. of ICPC 2024. arXiv:2308.07610.

7. Nong K., Yang K., Chen Z. et al. APPATCH: Automated Adaptive Prompting LLMs for Real-World Software Vulnerability Patching. USENIX Security. 2025.

8. Rondanini C., Carminati B., Ferrari E. et al. Malware Detection at the Edge with Lightweight LLMs: A Performance Evaluation. arXiv:2503.04302. 2025.

9. Alnahdi A., Narain S. Towards Transparent Intrusion Detection: A Coherence-Based Framework in Explainable AI Integrating LLMs. IEEE TPS-ISA. 2024.

10. Chen M., Wang J., Xue F., Wu Z. AECR: Automatic Attack Technique Intelligence Extraction Based on Fine-Tuned LLM. Computers & Security. 2025. Vol. 150. 104213.

11. Alhuzali A. LLM-powered threat intelligence: a retrieval-augmented generation approach for cyber attack investigation. PeerJ Computer Science. 2025. Vol. 11. e3371.

12. Wudali P. N., Malul E., Gandhi P. A. et al. Rule-ATT&CK Mapper (RAM): Mapping SIEM Rules to TTPs Using LLMs. arXiv:2502.02337. 2025.

УДК 621.396.2:004.85

Сідень С.В., Кутовий М.Г.

АНАЛІЗ МОЖЛИВОСТЕЙ ЗАСТОСУВАННЯ МАШИННОГО НАВЧАННЯ В МЕРЕЖАХ МОБІЛЬНОГО ЗВ'ЯЗКУ 5G/6G

Державний університет інтелектуальних технологій і зв'язку
ssiden@suitt.edu.ua, mishakutovoy@ukr.net

Анотація. *Проаналізовано можливості застосування методів машинного навчання у задачах планування та керування мобільними мережами сучасних та майбутніх поколінь з врахуванням міжсистемних завад. Розглянуті архітектурні особливості мереж 5G New Radio та 6G. Проведено порівняння детермінованих, статистичних та методів машинного навчання для врахування завад, при цьому методи глибокого навчання з підкріпленням та графові нейронні мережі визначено як перспективні підходи для узгодженого керування ресурсами. Розроблено імітаційну модель міжсистемних завад у смузі 3,5 ГГц та наведено кількісні оцінки впливу завад на SINR, захисних відстаней і точності різних підходів до прогнозування завад.*

Ключові слова*: машинне навчання, 5G/6G, мережеве планування, міжсистемні перешкоди, глибоке навчання з підкріпленням, O-RAN, імітаційне моделювання, SINR.*

Розвиток мережі 5G NR та формування концепції мереж 6-го покоління в рамках програми IMT-2030 забезпечують складне завдання планування та управління безпроводовими мережами. Використання міліметрових хвиль, технології Massive MIMO, методів спільного використання спектру створює комплексне електромагнітне середовище, в якому традиційні методи планування мають низьку ефективність. Особливо актуальною є проблема міжсистемних завад, наприклад 5G NR, Wi-Fi, супутниковими та радіолокаційними системами. Згідно з рекомендаціями ITU-R M.2160-0, мережі 6G повинні реалізовувати концепцію AI-native, що враховує глобальну інтеграцію методів штучного інтелекту в структуру мережі. Цей фактор зумовлює необхідність глибшого вивчення методів машинного навчання для таких задач планування та керування мережею.

Впровадження мереж 5G супроводжується рядом невирішених задач, що пов'язані з забезпеченням стабільної якості зв'язку в складних умовах міської забудови. На ефективність мереж впливають завади, затухання сигналу, багатопроменеве поширення та зростання кількості підключених пристроїв. Тому задача систематизації методів машинного навчання саме у контексті задач планування мереж 5G/6G з урахуванням міжсистемних завад є актуальною.

Архітектура мереж 5G NR, базується на дезагрегації базової станції gNB на центральний (CU), розподілений (DU) та радіоблок (RU). Радіоінтерфейс використовує гнучку нумерологію OFDM:

$$\Delta f = 2^{\mu} \cdot 15\text{кГц}, \qquad T_{sym} = \frac{1}{\Delta f}, \qquad \mu \in \{0,1,2,3,4\}, \tag{1}$$

Δf – відстань між піднесучими, μ – індекс нумерології, T_{sym} – тривалість OFDM-символу. Це дозволяє адаптувати мережу до вимог пропускної здатності, затримки та стійкості до доплерівських зсувів. У 5G підтримуються сценарії eMBB, URLLC та mMTC, які відрізняються вимогами до швидкості передачі, надійності та затримки. Концепція 6G розвиває принципи 5G у напрямках AI-native, ISAC, RIS, XL-MIMO та субтерагерцового зв'язку. На відміну від 5G, де алгоритми машинного навчання працюють поверх існуючої архітектури, у 6G штучний інтелект інтегрується безпосередньо у фізичний рівень та механізми керування мережею.

Методи машинного навчання поділяються на навчання з учителем, без учителя, напівкероване та навчання з підкріпленням. Задача навчання з учителем формулюється як мінімізація емпіричного ризику:

(2)

$L(\cdot)$ – функція втрат, $\Omega(\theta)$ – регуляризаційний параметр, λ – коефіцієнт регуляризації. N – кількість тренувальних вибірок.

Навчання з підкріпленням ґрунтується на марковських процесах прийняття рішень, а оптимальна функція визначається рівнянням Беллмана. Для складних задач керування мережами застосовується Deep Reinforcement Learning (DRL). Графові нейронні мережі (GNN) описують мережу як граф та виконують оновлення вузлів за схемою message-passing.:

$$H_v^{(k+1)} = \sigma\Big(W^{(k)} h_v^{(k)} + \sum_{u \in N(v)} W_N^{(k)} h_u^{(k)}\Big), \tag{3}$$

$h_v^{(k)}$ – вектор представлення вузла v на k-му шарі, $N(v)$ – множина сусідів, $\sigma(\cdot)$ – нелінійна функція активації [6].

Для розподіленого навчання використовується федеративний алгоритм FedAvg.:

$$\theta_{t+1}^{global} = \sum_{k=1}^{K} \frac{n_k}{n} \theta_{t+1}^{(k)}, n = \sum_{k=1}^{K} n_k \tag{4}$$

K – кількість локальних вузлів, n_k – розмір локальної вибірки. Такий підхід забезпечує приватність даних та зменшує навантаження на транспортну мережу.

Задача планування мережі 5G з урахуванням міжсистемних завад можна представити як нелінійну змішано-цілочисельну оптимізацію, в якій потрібно максимізувати пропускну здатність мережі при врахуванні обмежень на допустимі рівні завад для інших систем радіозв'язку. Через надзвичайно великий простір рішень таких задач, класичні методи оптимізації є малоефективними. Саме через це доцільним є використання методів машинного навчання. Оцінювання міжсистемних завад виконується через показник SINR:

$$SINR = \frac{P_S G_S L_S^{-1}}{N_0 + \sum_{k=1}^{K} P_k G_k L_k^{-1}}. \tag{5}$$

P_S – потужність корисного сигналу, G_S – коефіцієнт підсилення антени, L_S – втрати при поширенні сигналу. Потужність теплового шуму у смузі B визначається наступним чином:

$$N_0 = k_B T B F, \tag{6}$$

– постійна Больцмана, $T = 290\text{K}$ – температура у Кельвінах, F – коефіцієнт шуму приймача. Зазвичай критерій прийнятності завад встановлюється на рівні $I/N \leq -6$ дБ.

Існують чотири базові підходи до моделювання рівня міжсистемних завад: детермінований, статистичний, на основі методів машинного навчання та гібридний [7]. Детерміновані методи (такі як метод трасування променів) забезпечують високу точність, але потребують значних обчислювальних ресурсів. Статистичні моделі 3GPP та ITU-R простіші, однак не враховують локальних особливостей середовища. Методи машинного навчання демонструють високу адаптивність, а фізично обґрунтовані підходи поєднують переваги фізичних моделей і нейронних мереж.

В архітектурі мереж O-RAN ключовим компонентом є RAN Intelligent Controller (RIC), представлений рівнями Near-RT RIC та Non-RT RIC. Моделі машинного навчання реалізуються у вигляді xApp і rApp. Для керування мікромірковими завадами застосовуються DRL-агенти, функція винагороди яких враховує пропускну здатність мережі та штраф за інтерференцію:

$$r_t = \sum_{n=1}^{N} R_n(t) - \lambda_I \sum_{\substack{n,n'=1 \\ n' \neq n}}^{N} I_{n,n'}(t), \tag{7}$$

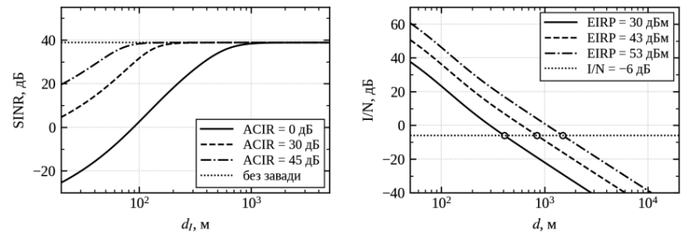
де $R_n(t)$– агрегована пропускна здатність n-ї комірки, $I_{n,n'}(t)$ – міжкоміркова інтерференція, λ_I – ваговий коефіцієнт штрафу.

Для кількісної перевірки сформульованих залежностей розроблено імітаційну модель низхідної лінії 5G NR мовою Python. Параметри сценарію: несійна частота f_c = 3,5 ГГц (смуга n78), ширина смуги $B = 100$ МГц, рівень шуму приймача $F = 5$ дБ, відповідно за формулою (6) – $N_0 = -89$ дБм, потужність БС – 46 дБм, підсилення антени – 15 дБі, відстань абонента до неї – 200 м. У якості моделі поширення радіохвиль було обрано модель 3GPP TR 38.901 для сценарію макро середовища.

Вираз (5) узагальнено на завади по сусідньому каналу введенням коефіцієнта його придушення $ACIR$:

$$SINR(d_I) = \frac{P_S G_S L_S^{-1}}{N_0 + \sum_{k=1}^{K} P_k G_k L_k^{-1} \cdot 10^{-ACIR_k/10}} \tag{11}$$

Результати моделювання наведено на рис. 1. Суміщений за каналом передавач з EIRP 43 дБм знижує відношення SINR абонента нижче порогу демодуляції QPSK (0 дБ) на відстанях до 90 м, а рівень 20 дБ, потрібний для модуляції 64QAM, досягається лише за $d_I > 221$ м (рис. 1, а). Фільтрація сусіднього каналу з ACIR = 30 і 45 дБ скорочує цю відстань до 55 і 21 м відповідно. За критерієм I/N ≤ −6 дБ захисна відстань становить 408, 846 і 1503 м для EIRP 30, 43 і 53 дБм (рис. 1, б), тобто зростає приблизно у 1,8 раза на кожні 10 дБ потужності джерела завади.



а) *б)*

Рисунок 1 - Вплив завади на SINR абонента (а) та визначення захисної відстані за критерієм I/N (б)

Точність оцінювання рівня завад досліджено методом Монте-Карло. Складові похибки кожного підходу задано за узагальненими даними [4, 5], тому порівняння є відносним. Статистичні моделі 3GPP/ITU-R дають RMSE 7,5 дБ і похибку 12,4 дБ на рівні 90-го процентиля, модель машинного навчання – 3,1 і 5,1 дБ, гібридна фізично-обґрунтована модель – 1,9 і 3,1 дБ проти 1,2 і 2,0 дБ у детермінованого розрахунку (рис. 2).

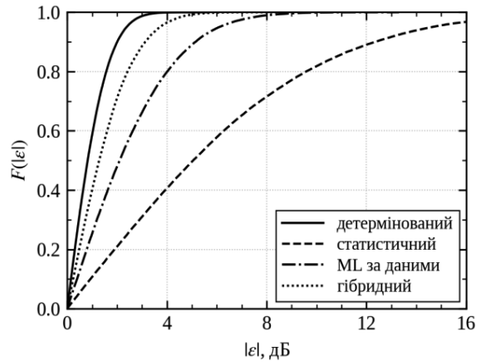


Рисунок 2 - Функції розподілу модуля похибки оцінювання SINR для різних підходів

Висновки. У роботі проаналізовано застосування методів машинного навчання в мережах сучасних та майбутніх поколінь з урахуванням міжсистемних завад та виконано імітаційне моделювання. Визначено, що традиційні методи планування не масштабуються через надзвичайно велику кількість можливих конфігурацій, що зумовлює використання методів машинного навчання для рішення такого типу задач. Систематизовано підходи машинного навчання та визначено найперспективніші, а саме DRL, GNN і FL. Моделювання показало, що завада по суміщеному каналу унеможливлює зв'язок на відстанях до 90 м, тоді як придушення сусіднього каналу на 45 дБ скорочує цю відстань до 21 м, а захисна відстань за критерієм $I/N = -6$ дБ зростає з 408 до 1503 м у разі збільшення потужності джерела завади з 30 до 53 дБм. Гібридні фізично-обґрунтовані моделі зменшують RMSE оцінювання SINR з 7,5 до 1,9 дБ. Подальші дослідження будуть спрямовані на розробку

таких фізично-обгрунтованих моделей прогнозування рівня завад та багатафакторних алгоритмах керування ресурсами мережі.

Література

1. Letaief K. B., Chen W., Shi Y., Zhang J., Zhang Y.-J. A. The Roadmap to 6G: AI Empowered Wireless Networks. IEEE Communications Magazine. 2019. Vol. 57, No. 8. P. 84–90. DOI: 10.1109/MCOM.2019.1900271.
2. 3GPP TS 38.300 V18.2.0. NR; NR and NG-RAN Overall description; Stage 2 (Release 18). Sophia Antipolis : 3GPP, p. 167. (2024).
3. ITU-R Recommendation M.2160-0. Framework and overall objectives of the future development of IMT for 2030 and beyond. Geneva : International Telecommunication Union, p. 25. (2023).
4. Alhammadi A., Shayea I., El-Saleh A. A., Azmi M. H., Daradkeh Y. I., Mohamad H. Artificial Intelligence in 6G Wireless Networks: Opportunities, Applications, and Challenges. International Journal of Intelligent Systems. 2024. Vol. 2024. Article ID 8845070. DOI: 10.1155/2024/8845070.
5. Lohan P., Kantarcı B., Ferrag M. A., Tihanyi N., Shi Y. From 5G to 6G Networks: A Survey on AI-Based Jamming and Interference Detection and Mitigation. IEEE Open Journal of the Communications Society. 2024. Vol. 5. P. 3920–3974. DOI: 10.1109/OJCOMS.2024.3416808.
6. Shen Y., Shi Y., Zhang J., Letaief K. B. Graph Neural Networks for Scalable Radio Resource Management: Architecture Design and Theoretical Analysis. IEEE Journal on Selected Areas in Communications. 2021. Vol. 39, No. 1. P. 101–115. DOI: 10.1109/JSAC.2020.3036965
7. Siden S., Tsarov R., Stepanov D., Shulakova K., Pavlov A. Hybrid AI-Based Path Loss Prediction Model for 5G/6G Networks. *Proceedings of International Conference on Applied Innovation in IT*. 2026. Vol. 14, Issue 2. P. 21–27. DOI: https://doi.org/10.25673/123804

УДК 342.922:004.056.5

Большакова О.В.

АДМІНІСТРАТИВНО-ПРАВОВІ ІНСТРУМЕНТИ ЗАХИСТУ ІНФОРМАЦІЇ В УКРАЇНІ: ПРАВОВІ КОЛІЗІЇ ТА НАПРЯМИ РЕФОРМУВАННЯ

ВСП «Фаховий коледж вимірювань Державного університету інтелектуальних технологій і зв'язку»
z0634280810@gmail.com

Анотація. *Тези доповіді присвячено комплексному аналізу сучасного стану, проблем та перспектив розвитку адміністративно-правових методів забезпечення інформаційної безпеки в Україні в умовах євроінтеграції. У роботі виявлено ключові матеріальні колізії чинного законодавства. Зокрема, досліджено кризу санкцій Кодексу України про адміністративні правопорушення (КУпАП) за делікти у сфері захисту персональних даних. Особливу увагу приділено нормативному розриву перехідного періоду після прийняття Закону України № 4336-IX та правовому вакууму в регулюванні використання генеративного штучного інтелекту персоналом. На основі аналізу доктрини інформаційного права та європейських стандартів запропоновано конкретні напрями реформування вітчизняного законодавства, включаючи перехід до системи диференційованих оборотних штрафів та автоматизованого комплаєнсу.*

Ключові слова: *інформаційне право, адміністративна відповідальність, захист інформації, штучний інтелект, кібербезпека, персональні дані, правова колізія.*

Стрімкий розвиток цифрових технологій, масштабне впровадження хмарних обчислень та систем штучного інтелекту, а також перманентні кіберзагрози в умовах воєнного стану вимагають радикального переосмислення системи забезпечення інформаційної безпеки України. Адміністративно-правові інструменти захисту інформації (інститути ліцензування, сертифікації, державного нагляду та адміністративної відповідальності) є базисом, що визначає легітимні межі та правила поведінки суб'єктів інформаційних правовідносин. Проте діюче законодавство України наразі демонструє системний розрив між технологічними реаліями та правовим інструментарієм його регулювання, що актуалізує необхідність виявлення наявних колізій та обґрунтування векторів реформування.

Так, першою проблемою, яку хотілося б відзначити, є певна диспропорція між реальним характером кіберзагроз і заходами адміністративного примусу, закріпленими у КУпАП. Зокрема, санкції за ст. 188-31

(невиконання законних вимог посадових осіб органів Державної служби спеціального зв'язку та захисту інформації України) та ст. 188-39 (порушення законодавства у сфері захисту персональних даних) передбачають максимальні штрафи на рівні від 100 до 2000 неоподатковуваних мінімумів доходів громадян (що еквівалентно кільком тисячам або десяткам тисяч гривень) [4]. У наукових працях вітчизняних адміністративістів (зокрема, у дослідженнях І. Ковбаса, А. Стрельникова та ін.) наголошується, що за таких умов адміністративне стягнення повністю втрачає свою превентивну (запобіжну) та правовідновлювальну функції, перетворюючись на суто номінальний «податок на правопорушення». Науковці підкреслюють, що чинний каральний інструментарій КУпАП моделювався за радянським зразком і розрахований на індивідуальних суб'єктів або дрібні посадові провини, а тому є абсолютно неадаптованим до деліктів у цифровому середовищі.

Юристи-практики (зокрема, експерти з Digital Law та комплаєнсу) констатують, що для IT-компаній або операторів критичної інфраструктури сплата мінімального штрафу є економічно вигіднішою, ніж фінансування високовартісних організаційно-технічних заходів із кіберзахисту. В умовах, коли масштабний витік інформації здатний завдати матеріальних збитків на мільйони гривень, призвести до компрометації військовослужбовців або підірвати національну безпеку держави, такий правовий лібералізм є недопустимим [5].

Додатково виникає гостра правова колізія із євроінтеграційними зобов'язаннями України. Генеральний регламент про захист даних ЄС (GDPR) та нова європейська Директива з кібербезпеки NIS2 оперують концепцією «ефективних, пропорційних та стримувальних» санкцій, встановлюючи штрафи до 10–20 мільйонів євро або до 2–4% від загального світового річного обороту компанії за аналогічні правопорушення. Відтак, подолання кризи матеріальних санкцій КУпАП вимагає не просто механічного підвищення фіксованих штрафів, а концептуального переходу до диференційованих оборотних фінансово-адміністративних санкцій для юридичних осіб [2]. Вважаємо, що необхідно здійснити перехід від фіксованих мізерних штрафів до європейської практики оборотних штрафів - стягнення відсотків від загального річного обороту компанії-порушника.

Істотним деструктивним чинником у системі адміністративно-правових методів є інституційна криза перехідного періоду, викликана прийняттям Закону України № 4336-IX «Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури» [6]. Цей нормативно-правовий акт ознаменував довгоочікувану відмову від архаїчної та надмірно бюрократизованої моделі Комплексних систем захисту інформації (КСЗІ) на користь сучасного ризикоорієнтованого підходу та впровадження інституту CISO (офіцерів з кібербезпеки). Проте імплементація закону натрапила на класичну юридичну проблему - системне відставання підзаконного нормативно-правового регулювання.

У сучасних дослідженнях Інституту держави і права імені В. М. Корецького НАН України та роботах фахівців з інформаційного права (зокрема, К. Бєлякова, Р. Гринюка та ін.) зазначається, що заміна застарілого закону без миттєвого оновлення масиву відомчих інструкцій породжує так звану «правову асиметрію». Прийнятий закон вимагає гнучкого управління ризиками, побудови профілів безпеки та оцінки реальної технологічної стійкості IT-інфраструктури. Водночас посадові особи контролюючих та наглядових органів під час проведення реальних перевірок керуються чинними підзаконними актами (наказами відомств, положеннями, методичними рекомендаціями НД ТЗІ), які де-юре залишаються орієнтованими на застарілу методологію КСЗІ [3].

Як свідчить сучасна правозастосовча практика та експертні звіти Держспецзв'язку щодо готовності суб'єктів до нових вимог, ці колізії змушують суб'єктів господарювання та державні установи функціонувати в умовах подвійних стандартів. Замість спрямування фінансових та інтелектуальних ресурсів на реальний кіберзахист і протидію актуальним загрозам, організації змушені утримувати «паперовий комплаєнс» - дублювати стоси застарілої звітності та журналів обліку, щоб формально уникнути адміністративних претензій регуляторів. Як зазначається в офіційних роз'ясненнях Держспецзв'язку України щодо розбудови оновленої нормативної бази на виконання Закону № 4336-IX, практична реалізація реформи потребує скасування або системного перегляду значного масиву підзаконних актів. Наукова спільнота та експерти з кіберкомплаєнсу наголошують, що збереження чинності застарілих інструкцій створює правову асиметрію і штучно утримує «паперовий» характер захисту інформації замість оцінки реальних ризиків за європейськими стандартами [1]

І на останок, хотілося б відзначити відсутність національного адміністративно-правового регулювання використання генеративного штучного інтелекту (аналога європейського AI Act), що унеможливлює притягнення працівників до відповідальності за передачу конфіденційної інформації чи комерційної таємниці на публічні сервери ШІ-платформ, оскільки юридичний статус таких дій у трудовому та адміністративному