виступає як центральна консоль SOC-аналітика [2]. Suricata аналізує трафік та формує події у форматі eve.json, після чого Wazuh Agent передає їх на Wazuh Manager для обробки декодерами та правилами кореляції. Отримана інформація відображається на Wazuh Dashboard із зазначенням IP-адреси джерела атаки, типу загрози, часу та статусу реагування. Для ефективного реагування у Wazuh налаштовані спеціалізовані панелі моніторингу (Dashboards), які дозволяють швидко ідентифікувати найбільш атаковані сервіси, географічне розташування джерел атак (GeoIP) та динаміку спрацювань правил Suricata за рівнем критичності. Це забезпечує повну видимість мережевих інцидентів та дозволяє проводити цифрову криміналістику (Digital Forensics) після автоматичного блокування загроз [4].

Поєднання Suricata IPS та SIEM Wazuh створює багаторівневу систему захисту мережі. Suricata забезпечує швидку автоматичну реакцію на рівні мережевого трафіку, а Wazuh надає аналітичний інструментарій для моніторингу та розслідування інцидентів.

1. OISF. Suricata User Guide – Intrusion Detection and Prevention. [Електронний ресурс]. – Режим доступу: https://docs.suricata.io/en/latest/ips/index.html.
2. Wazuh Inc. Integration of Suricata with Wazuh for Network Threat Detection. [Електронний ресурс]. – Режим доступу: https://documentation.wazuh.com/current/proof-of-concept-guide/integrate-network-ids-suricata.html.
3. ENISA Threat Landscape Report 2025. [Електронний ресурс]. – Режим доступу: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025.
4. MITRE Corporation. ATT&CK Framework – Command and Control, Initial Access and Web Attacks Techniques. [Електронний ресурс]. – Режим доступу: https://attack.mitre.org/
5. Scarfone K., Mell P. Guide to Intrusion Detection and Prevention Systems (IDPS). National Institute of Standards and Technology (NIST SP 800-94). – Gaithersburg: NIST, 2007. – 127 p. [Електронний ресурс]. – Режим доступу: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-94.pdf.

Нормативно-правове регулювання кіберзахисту систем штучного інтелекту в Україні

УДК 004.8:342 (043.2)

Артем Жилін[1], Олександра Ценцеря[2]

Київський політехнічний інститут імені Ігоря Сікорського,
[1]zhylinartem@gmail.com, [2]o.tsentseria.s01@kpi.ua

Метою роботи є аналіз нормативно-правової бази кіберзахисту систем штучного інтелекту (далі – ШІ) в Україні та визначення напрямів її удосконалення.

Станом на 2026 рік нормативно-правове регулювання кіберзахисту систем ШІ в Україні перебуває на етапі формування та характеризується фрагментарністю, переважанням документів публічної політики над обов'язковими нормативно-правовими актами.

Таблиця 1

Нормативно-правове регулювання штучного інтелекту в Україні

1. Нормативно-правові акти (НПА)	
Суб'єкт правотворчості	Повна назва
КМУ	Постанова Кабінету Міністрів України (далі – КМУ) від 29.10.2024 № 1238 «Про реалізацію експериментального проекту щодо організації проведення досліджень високотехнологічних засобів методом "Sandbox"»
ДССЗЗІ	Наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України (далі – ДССЗЗІ) від 23.02.2026 № 154 «Про затвердження Рекомендацій з кіберзахисту інформаційно-комунікаційних систем, які використовують технології штучного інтелекту»
2. Документи публічної політики (ДПП)	
КМУ	Розпорядження КМУ від 02.12.2020 № 1556-р «Про схвалення Концепції розвитку штучного інтелекту в Україні»
КМУ	Розпорядження КМУ від 12.05.2021 № 438-р «Про затвердження плану заходів з реалізації Концепції розвитку штучного інтелекту в Україні на 2021–2024 роки»
КМУ	Розпорядження КМУ від 09.05.2025 № 457-р «Про затвердження плану заходів з реалізації Концепції розвитку штучного інтелекту в Україні на 2025–2026 роки»
Мінцифри	Дорожня карта з регулювання штучного інтелекту в Україні: Bottom-Up Підхід
Мінцифри	Біла книга з регулювання ШІ в Україні: бачення Мінцифри

Чинна нормативна база охоплює або кіберзахист інформаційно-комунікаційних систем загалом, без урахування специфіки ШІ-компонентів, або розвиток і впровадження ШІ без акцентованих вимог до кіберзахисту. Перетин цих двох сфер у єдиній обов'язковій нормі фактично відсутній, що й визначає мету досліджень.

На рівні нормативно-правових актів єдиним документом, що прямо адресує кіберзахист ШІ-систем, є Наказ ДССЗЗІ від 23.02.2026 № 154 «Про затвердження Рекомендацій з кіберзахисту інформаційно-комунікаційних систем, які використовують технології штучного інтелекту» [1]. Він затверджує рекомендації, а не обов'язкові вимоги, що унеможливлює його застосування як підстави для юридичної відповідальності. Постанова КМУ від 29.10.2024 № 1238 запроваджує механізм регуляторної пісочниці («Sandbox») для тестування високотехнологічних засобів, до яких можуть належати системи ШІ, однак без спеціальних вимог безпеки до таких систем це процедурний механізм,

а не регуляторний стандарт кіберзахисту. Документи публічної політики визначають безпеку та довіру до ШІ як пріоритети державної політики та фіксують напрями, а не норми [2-6]. При цьому орієнтація на поетапну імплементацію EU AI Act [7], зокрема в частині вимог до безпеки ризикових систем, простежується лише у [2] та [6].

З огляду на виявлені прогалини, подолання структурної недостатності регулювання кіберзахисту систем ШІ потребує узгодженої дії на кількох рівнях нормативної ієрархії. На законодавчому рівні – прийняття Верховною Радою України спеціального закону про ШІ із розділом, що встановлює вимоги кіберзахисту ШІ-систем залежно від рівня ризику, до якого вони належать, відповідно до ризик-орієнтованої класифікації EU AI Act [7]. На підзаконному рівні – прийняття окремої постанови КМУ із мінімальними обов'язковими вимогами кіберзахисту для систем ШІ, що спиралися б на NIST AI RMF 1.0 в частині управління ризиками, або на ISO/IEC 42001:2023.

1. «Про затвердження Рекомендацій з кіберзахисту інформаційно-комунікаційних систем, які використовують технології штучного інтелекту». Наказ ДССЗЗІ від 23.02.2026 № 154. URL: https://cip.gov.ua/ua/docs/nakaz-administraciyi-derzhspeczv-yazku-vid-23-02-2026-154-pro-zatverdzhennya-rekomendacii-z-kiberzakhistu-informaciino-komunikaciinikh-sistem-yaki-vikoristovuyut-tekhnologiyi-shtuchnogo-intelektu (дата звернення: 14.05.2026).
2. Про схвалення Концепції розвитку штучного інтелекту в Україні: Розпорядження КМУ від 02.12.2020 № 1556-р. URL: https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80#Text (дата звернення: 15.05.2026).
3. Про затвердження плану заходів з реалізації Концепції розвитку штучного інтелекту в Україні на 2021–2024 роки: Розпорядження КМУ від 12.05.2021 № 438-р. URL: https://zakon.rada.gov.ua/laws/show/438-2021-%D1%80#Text (дата звернення: 15.05.2026).
4. Про затвердження плану заходів з реалізації Концепції розвитку штучного інтелекту в Україні на 2025–2026 роки: Розпорядження КМУ від 09.05.2025 № 457-р. URL: https://zakon.rada.gov.ua/laws/show/457-2025-%D1%80#Text (дата звернення: 15.05.2026).
5. Дорожня карта з регулювання штучного інтелекту в Україні: Bottom-Up Підхід. Мінцифри, 2023. URL: https://storage.thedigital.gov.ua/files/2/22/363bbcaec30bf9d4e598375feca c3227.pdf (дата звернення: 15.05.2026).
6. Біла книга з регулювання ШІ в Україні: бачення Мінцифри. Версія для консультацій. Мінцифри, 2024. URL: https://storage.thedigital.gov.ua/files/a/ba/d5da75c2613e331bb89258f950adcbae.pdf (дата звернення: 15.05.2026).
7. EU Artificial Intelligence Act: up-to-date developments and analyses. URL: https://artificialintelligenceact.eu/ (дата звернення: 16.05.2026).