МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Одеська юридична академія»

СОЦІАЛЬНО-ПОЛІТИЧНА ТА ПРАВОВА СИСТЕМА УКРАЇНИ В ЦИФРОВУ ЕПОХУ: СУЧАСНІ ВИКЛИКИ

МАТЕРІАЛИ
Міжнародної науково-практичної конференції

Одеса, 22 квітня 2026 року

Том 2

Одеса
2026

УДК 34:004:316.4(477)
С 70

Рекомендовано до друку вченою радою
Національного університету «Одеська юридична академія»
(протокол № 8 від 23.04.2026 р.)

За загальною редакцією академіка ***С. В. Ківалова***

С70 **Соціально-політична та правова система України в цифрову епоху**: сучасні виклики : матеріали Міжнар. наук.-практ. конф. (м. Одеса, 22 квітня 2026 р.) / заг. ред. С. Ківалова ; НУ «Одес. юрид. академія». – Одеса : Фенікс, 2026. – Т. 2. – 684 с.

ISBN 978-617-8763-16-9

Матеріали конференції узагальнюють результати наукових досліджень і практичних напрацювань учених, фахівців та представників професійних спільнот, виконаних в умовах воєнного часу та глибоких суспільних трансформацій.

У збірнику представлено широкий спектр наукових розвідок і практико-орієнтованих досліджень, що охоплюють актуальні проблеми публічного та приватного права, функціонування держави, судової та правоохоронної системи, а також трансформації суспільних процесів у цифрову епоху. Значну увагу приділено питанням адміністративного, фінансового, конституційного, міжнародного, морського та митного права, а також сучасним викликам у сфері кримінального права, кримінального процесу, криміналістики та оперативно-розшукової діяльності.

Окремі наукові секції присвячені проблемам удосконалення судоустрою, діяльності прокуратури, адвокатури та інших правоохоронних органів, розвитку трудового права і права соціального забезпечення, а також реформуванню цивільного, господарського, земельного, екологічного та енергетичного права. Збірник відображає також міждисциплінарний характер сучасних досліджень, охоплюючи питання філософії права, світових соціально-політичних процесів, соціології та психології, економіки та підприємництва в умовах війни і повоєнного відновлення. Важливе місце посідають дослідження у сфері інформаційних технологій, кібербезпеки, штучного інтелекту та математичного моделювання як ключових чинників забезпечення національної безпеки.

Крім того, у збірнику висвітлено проблематику педагогіки, лінгвістики права, перекладознавства, журналістики, фізичної та військової підготовки здобувачів вищої освіти.

Збірник розрахований на науковців, викладачів, здобувачів вищої освіти та практиків у галузях права, економіки, соціології, психології, політології, інформаційних технологій і суміжних дисциплін.

УДК 34:004:316.4(477)

Відповідальний за випуск професор ***М. Р. Аракелян***

Матеріали видано в авторській редакції.

ISBN 978-617-8763-16-9

Зміст

СЕКЦІЯ 14. ЦИВІЛЬНЕ СУДОЧИНСТВО У СВІТЛІ РЕФОРМУВАННЯ СУДОВОЇ СИСТЕМИ

СЕКЦІЯ 15. АКТУАЛЬНІ ПИТАННЯ ПРАВА ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ ТА ПАТЕНТНОЇ ЮСТИЦІЇ

СЕКЦІЯ 16. АКТУАЛЬНІ ПРОБЛЕМИ ГОСПОДАРСЬКОГО ПРАВА І ПРОЦЕСУ

СЕКЦІЯ 17. ТЕОРЕТИЧНІ ТА ПРАКТИЧНІ ПРОБЛЕМИ ЗЕМЕЛЬНОГО, ЕКОЛОГІЧНОГО ТА ЕНЕРГЕТИЧНОГО ПРАВА

СЕКЦІЯ 18. ФІЛОСОФСЬКІ ОСНОВИ ПРАВА ТА ДЕРЖАВИ

СЕКЦІЯ 19. АКТУАЛЬНІ ПРОБЛЕМИ СВІТОВИХ СОЦІАЛЬНО-ПОЛІТИЧНИХ ПРОЦЕСІВ

СЕКЦІЯ 20. СОЦІОЛОГІЧНИЙ АНАЛІЗ ПРОБЛЕМ СУЧАСНОГО СУСПІЛЬСТВА

СЕКЦІЯ 21. СОЦІАЛЬНО-ПСИХОЛОГІЧНИЙ СТАН ОСОБИСТОСТІ ТА СОЦІУМУ В КРИЗОВИХ СИТУАЦІЯХ

СЕКЦІЯ 22. ЕКОНОМІКА ТА ПІДПРИЄМНИЦТВО В УМОВАХ ЄВРОПЕЙСЬКОГО ВИБОРУ, ВІЙНИ ТА ПІСЛЯВОЄННА ВІДБУДОВА УКРАЇНИ

СЕКЦІЯ 23. ПРОГРАМНА ІНЖЕНЕРІЯ ТА СУЧАСНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

СЕКЦІЯ 24. КІБЕРБЕЗПЕКА ОСОБИ, СУСПІЛЬСТВА ТА ДЕРЖАВИ ЯК ФУНДАМЕНТАЛЬНИЙ ЕЛЕМЕНТ ЗАБЕЗПЕЧЕННЯ ОБОРОНОЗДАТНОСТІ УКРАЇНИ

СЕКЦІЯ 25. ШТУЧНИЙ ІНТЕЛЕКТ І МАТЕМАТИЧНЕ МОДЕЛЮВАННЯ В УМОВАХ ВОЄННИХ ТА БЕЗПЕКОВИХ ВИКЛИКІВ

СЕКЦІЯ 26. КОГНІТИВНО-ПРАГМАТИЧНІ ДОСЛІДЖЕННЯ ДИСКУРСУ, ТЕОРІЯ ТА ПРАКТИКА ПЕРЕКЛАДУ В АСПЕКТІ ВИКЛАДАННЯ ІНОЗЕМНИХ МОВ

СЕКЦІЯ 27. ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ РОЗВИТКУ СУЧАСНОЇ ПЕДАГОГІКИ, ЛІНГВІСТИКИ ПРАВА ТА ЗМІ

СЕКЦІЯ 28. ВИКЛИКИ СУЧАСНОЇ ЖУРНАЛІСТИКИ

СЕКЦІЯ 29. АКТУАЛЬНІ ПРОБЛЕМИ ФІЗИЧНОЇ ТА ВІЙСЬКОВОЇ ПІДГОТОВКИ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ

СЕКЦІЯ 30. ДІЯЛЬНІСТЬ СУЧАСНИХ БІБЛІОТЕК У ЗАКЛАДАХ ВИЩОЇ ОСВІТИ

4. Arisandi D., Nazrul Muhaimin Ahmad N., Subarmaniam A., L Kannan S. The rogue access point identification: a model and classification review. *The Indonesian Journal of Electrical Engineering and Computer Science*. 2021. Vol. 23. No. 3. P. 1527–1537.

5. Sui K., Zhao Y., Pei D., Zimu L. How bad are the rogues' impact on enterprise 802.11 network performance? *2015 IEEE Conference on Computer Communications (INFOCOM)*. 2015. P. 361–369.

Ключові слова: статистичне відхилення, фільтрація трафіку, захоплення пакетів, моніторинг вузлів, запобігання атакам MITM, заголовок IP-пакету, час життя пакета, модель OSI, інкапсуляція трафіку, аналіз часових характеристик, контрольна площина, бездротова безпека, несанкціонована точка доступу, злий двійник, програмна точка доступу, WIDS/WIPS, джиттер, кругова затримка.

Key words: SIEM, Rogue Access Point, Time to Live, Round-Trip Time, Wireless Intrusion Detection System, Man-in-the-Middle, 5G Core Security, Soft AP detection.

Кухаренко Сергій Вікторович
Національний університет «Одеська юридична академія»,
доцент кафедри кібербезпеки, кандидат технічних наук, доцент

РЕГУЛЯТОРНА АРХІТЕКТУРА КІБЕРБЕЗПЕКИ ЄВРОПЕЙСЬКОГО СОЮЗУ: ТРАНСФОРМАЦІЯ НОРМАТИВНОЇ БАЗИ ТА ВИКЛИКИ ІМПЛЕМЕНТАЦІЇ

Упродовж 2024-2026 років Європейський Союз здійснює системну трансформацію підходів до регулювання кібербезпеки, формуючи цілісну нормативну базу, що охоплює як організаційний, так і продуктовий рівні (цикл – від вимог до продуктів до управління кризами). Такий підхід спрямований на забезпечення кіберстійкості у межах єдиного цифрового ринку [5; 10; 19].

Водночас практика застосування нових норм засвідчує наявність розриву між регуляторними вимогами та рівнем готовності держав-членів і суб'єктів господарювання. Додатковим фактором є висока динаміка кіберзагроз, зокрема атак на ланцюги постачання, програм-вимагачів (ransomware) та використання штучного інтелекту в зловмисній діяльності. Це зумовлює необхідність аналізу відповідності чинної нормативної бази реальному стану загроз [6; 7; 15].

У тезах досліджується актуальний стан нормативно-правової бази кібербезпеки Європейського Союзу станом на 2025-2026 роки. Розглянуто ключові регуляторні акти, зокрема Директиву (ЄС) 2022/2555 (NIS2), Регламент (ЄС) 2024/2847 (Cyber Resilience Act), а також ініціативи у сфері кіберсолідарності та уніфікації звітності про інциденти. Визначено проблеми імплементації, зокрема регуляторну фрагментацію, складність комплаєнсу та адаптацію до нових технологічних викликів. Оцінено роль ENISA у формуванні європейської кібербезпекової екосистеми.

Ключові нормативні акти: зміст та строки реалізації

Директива (ЄС) 2022/2555 (NIS2) встановлює базові вимоги до кібербезпеки організацій у критично важливих та інших визначених секторах, запроваджує диференційовані вимоги до «суттєвих» (essential) та «важливих» (important) суб'єктів, обов'язки щодо управління ризиками, встановлює суворі строки звітування про інциденти протягом 24 годин та особисту відповідальність керівництва. Санкції – до 10 млн євро або 2% річного глобального обороту для суттєвих суб'єктів (essential entities); до 7 млн євро або 1,4% – для важливих суб'єктів (important entities) [2; 19].

Регламент (ЄС) 2024/2847 (Cyber Resilience Act, CRA) – Акт про кіберстійкість – встановлює обов'язкові вимоги кібербезпеки для всіх продуктів з цифровими елементами (від смарт-годинників до промислових систем управління) протягом усього життєвого циклу. Запроваджує принцип «безпеки за проєктом» (security by design), підтримку протягом визначеного життєвого циклу продукту, маркування CE та відповідальність виробника за вразливості [1; 11].

Європейська політика кіберсолідарності (**Акт про кіберсолідарність)** набрав чинності 4 лютого 2025 р. Не встановлює регуляторних зобов'язань для приватного сектору, натомість передбачає створення трьох механізмів координації реагування на масштабні кіберінциденти: загальноєвропейська мережа центрів (hubs) обміну інформацією про загрози; Європейський механізм кібербезпеки для підготовки до масштабних інцидентів; Резерв кібербезпеки ЄС – пул довірених постачальників послуг керованої безпеки для реагування на кризові ситуації [3; 14; 16].

Пакет «Цифровий омнібус» Digital Omnibus (ініціатива Єврокомісії щодо уніфікації звітності…) – є найновішим кроком у розвитку нормативної бази. Ініціативи спрямовані на спрощення виконання вимог різних нормативних актів (NIS2, GDPR, DORA, CRA та eIDAS) через єдину точку подачі звітів про інциденти принцип – «report once» («звітуй один раз – поширюй багатьом»). Станом на 2026 рік ці підходи перебувають на стадії політичного узгодження та нормативного формування [4].

Стан імплементації: проблема регуляторної фрагментації

Станом на початок 2026 року процес імплементації NIS2 у державах-членах залишається нерівномірним: значна частина країн ухвалили відповідне національне законодавство, інша частина перебуває на різних етапах прийняття національного законодавства. Це призводить до: варіативності визначення інцидентів; відмінностей у процедурах звітування; появи додаткових національних вимог. Для транскордонних організацій це означає зростання витрат на комплаєнс та складність дотримання регуляторних вимог у різних юрисдикціях [6; 15; 17].

По-перше, визначення «суттєвого інциденту» варіюється між юрисдикціями: наприклад, деякі держави-члени встановлюють більш жорсткі строки попереднього повідомлення, ніж передбачено NIS2. По-друге, принцип «основного місця перебування» реалізований непослідовно: Угорщина вимагає локальної

реєстрації незалежно від того, де знаходиться штаб-квартира суб'єкта. По-третє, деякі держави встановлюють додаткові вимоги понад мінімальний стандарт директиви [7].

Регуляторне навантаження посилюється необхідністю одночасного дотримання вимог NIS2, GDPR, CRA (для виробників), DORA (фінансовий сектор) та галузевих норм (авіація, енергетика). Пакет «Цифровий омнібус» покликаний усунути дублювання вимог щодо звітності, проте до його набрання чинності організації продовжуватимуть нести подвійне та потрійне навантаження [4; 12].

Роль ENISA у формуванні кібербезпекової екосистеми

ENISA виконує координаційну та методичну функції у сфері кібербезпеки ЄС. Агентство: розробляє рекомендації щодо імплементації NIS2; бере участь у створенні схем сертифікації; координує обмін інформацією між державами-членами.

У червні 2025 р. ENISA опублікувала розширену настанову щодо заходів безпеки відповідно до NIS2. Хоча документ не є юридично обов'язковим, він суттєво конкретизує очікувану імплементацію, наприклад, вимагає багатофакторну автентифікацію на всіх інтернет-орієнтованих системах (VPN, електронна пошта, RDP), а також розробку карт розподілу ролей і навичок для забезпечення комплаєнсу [9].

13 травня 2025 р. ENISA запустила Європейську базу даних вразливостей (EUVD) – централізовану платформу для обміну інформацією, яка спрямована на централізацію інформації про вразливості та функціонує як доповнення до міжнародних систем (CVE/NVD) [18].

Очікується, що в рамках імплементації CRA (орієнтовно з 2026 р.) виробники продуктів з цифровими елементами будуть зобов'язані повідомляти про активно експлуатовані вразливості, зокрема через EUVD або сумісні механізми звітування. Проте стейкхолдери вказують на два системних обмеження: надмірно повільний та непрозорий процес розробки схем сертифікації; суперечки навколо вимог суверенітету в EUCS, що поділяють держав-членів і великих технологічних корпорацій.

Ефективність ENISA значною мірою залежить від координації з національними органами та розвитку механізмів сертифікації [8; 9; 10].

Технологічні виклики та відповідність законодавства новим загрозам

Сучасне кіберзаконодавство ЄС стикається з необхідністю адаптації до нових типів загроз, регулювання яких залишається недостатнім:

- **Атаки на ланцюги постачання (supply chain attacks)** компрометують тисячі організацій через одного постачальника ПЗ або апаратних компонентів. NIS2 і CRA приділяють увагу безпеці ланцюгів постачання, але механізми верифікації (зокрема Software Bill of Materials (SBOM) як один із інструментів забезпечення відповідності CRA) та відповідальності залишаються дискусійними [1; 11].
- **Ransomware (програми-вимагачі)** проти критичної інфраструктури, для яких відсутні спеціалізовані вузькопрофільні регуляторні інструменти.

Попри зростання масштабів атак, EU Cybersecurity Act не встановлює конкретних заборон або превентивних заходів для виробників засобів шифрування даних [8].

– **Застосування штучного інтелекту в кібератаках**, що створює перетин між різними нормативними режимами. Автоматизація фішингу, генерація DeepFake для Соціальної інженерії, оптимізація експлойтів [7; 10].
– **Квантові загрози криптографії** – прямі вимоги щодо постквантової криптографії наразі відсутні у CRA попри розуміння невідворотності загрози для довгострокової безпеки комунікацій [1; 8].

Регулювання відкритого програмного забезпечення (open source) було уточнене у CRA шляхом виключення некомерційного програмного забезпечення та введення поняття «open source steward» відповідального суб'єкта за підтримку проекту [11].

Секторальні та міжнародні аспекти

ЄС активно розвиває секторальні ініціативи, зокрема у сфері охорони здоров'я, де створюються спеціалізовані механізми підтримки кібербезпеки. Особливість полягає у створенні під егідою ENISA Центру підтримки кібербезпеки для лікарень, що надаватиме спеціалізовані рекомендації, інструменти та навчання. Заходи впроваджуються поетапно протягом 2025-2026 рр.

Оновлений план управління кіберкризами ЄС (EU Cyber Blueprint, червень 2025 р.) запровадив узгоджені процедури, єдину таксономію та інструменти ситуаційної обізнаності під керівництвом ENISA та мережі CSIRT. Перше міжнародне навчання нового формату операційного рівня з кібербезпеки BlueOLEx, спрямоване на тестування готовності Європейського Союзу до масштабних кіберкриз відбулося 4 листопада 2025 р [5; 9].

Міжнародний вимір кібербезпеки ЄС реалізується через системні кібердіалоги: з Великою Британією (грудень 2025 р.), Україною (жовтень 2025 р.), Індією (березень 2025 р.) та Республікою Корея (травень 2025 р.). Ці формати охоплюють обмін інформацією про загрози, розвиток безпеки ланцюгів постачання та координацію політики щодо нових технологій. Для України ці процеси мають значення у контексті гармонізації законодавства з правом ЄС [13].

Актуальність розглянутого питання зростає на тлі ескалації гібридних загроз та зближення кібербезпеки з питаннями стратегічної автономії ЄС. Досвід формування регуляторної архітектури Союзу є безпосередньо релевантним для України в контексті євроінтеграції адаптації національної системи кібербезпеки до європейських стандартів.

За результатами аналізу можна сформулювати такі висновки:

1. Європейський Союз сформував комплексну багаторівневу систему регулювання кібербезпеки, яка охоплює як організаційні, так і продуктові аспекти, проте її ефективність критично залежить від якості її імплементації на національному рівні.

2. Регуляторна фрагментація залишається ключовим викликом, що впливає на однаковість застосування норм та створює додаткове навантаження на суб'єктів транскордонних організацій.

3. Перетин між новими технологіями (ШІ, квантові обчислення) та чинним кіберзаконодавством залишається частково нормативно невизначеним.

4. ENISA набуває дедалі більшого стратегічного значення, однак її ефективність обмежена нестачею ресурсів, повільним процесом сертифікації та суперечками навколо вимог технологічного суверенітету.

Подальший розвиток нормативної бази має бути спрямований на: уніфікацію вимог; врахування нових технологічних ризиків; підвищення ефективності координаційних механізмів [2; 4; 10; 19].

Список використаних джерел:

1. Regulation (EU) 2024/2847 – Cyber Resilience Act. *Official Journal of the EU*. L 2024/2847, 20.11.2024.

2. Directive (EU) 2022/2555 – NIS 2 Directive. *Official Journal of the EU*. L 333, 27.12.2022.

3. Cyber Solidarity Act. Council of the EU, 02.12.2024, in force 04.02.2025.

4. Digital Omnibus Package. *European Commission*. 19.11.2025.

5. EU cybersecurity: strategy and key policies. Council of the EU. URL: https://www.consilium.europa.eu/en/policies/cybersecurity/

6. NIS2 Update: EU Cyber Authority Sets Out Compliance Expectations. Skadden, Arps. August 2025.

7. European Cybersecurity Regulatory Update NIS2 and Beyond. Bird & Bird. December 2025.

8. Cybersecurity Act review: What to expect. European Parliament Research Service. 2025.

9. ENISA. NIS2 Technical Implementation Guidance. 2025. URL: https://www.enisa.europa.eu

10. Navigating the EU Cybersecurity Policy Ecosystem. INTERFACE Policy Brief. 2025.

11. Cyber Resilience Act. *Open Source Security Foundation (OpenSSF)*. URL: https://openssf.org/public-policy/eu-cyber-resilience-act/

12. NIS2 & CRA: New cybersecurity obligations. *SZA*. 2025. URL: https://www.sza.de

13. Cybersecurity. *European External Action Service (EEAS)*. URL: https://www.eeas.europa.eu/eeas/cybersecurity_en

14. Regulation (EU) 2025/38 – Cyber Solidarity Act. *Official Journal of the European Union*. OJ L 38, 15.01.2025. URL: https://eur-lex.europa.eu/eli/reg/2025/38/oj/eng

15. Bernižan M., Martinović I., Schmid S. Identifying and Modeling Barriers to Compliance with the NIS2 Directive: A DEMATEL Approach. *Systems*. 2025. Vol. 5. Iss. 4. Art. 97. URL: https://www.mdpi.com/2624-800X/5/4/97

16. Mazzini, G. The Cyber Solidarity Act: Framework and Perspectives for the New EU-Wide Cybersecurity Solidarity Mechanism Under the EU Legal System. *European Journal of Risk Regulation*. 2025. URL: https://doi.org/10.1017/err.2025.18

17. ECSO White Paper: NIS2 Implementation – Challenges & Priorities. *European Cyber Security Organisation (ECSO)*. January 2025. URL: https://ecs-org.eu/ecso-uploads/2025/01/ECSO-White-Paper-NIS2-Implementation.pdf

18. ENISA. *European Vulnerability Database (EUVD)*. 2025. URL: https://euvd.enisa.europa.eu

19. European Commission. NIS2 Directive: securing network and information systems. *Digital Strategy*. January 2026. URL: https://digital-strategy.ec.europa.eu/en/policies/nis2-directive

Ключові слова: кібербезпека ЄС, NIS2, Cyber Resilience Act, ENISA, кіберстійкість, управління кібербезпекою, організаційне забезпечення, імплементація, регуляторна фрагментація.

Key words: EU cybersecurity, NIS2, Cyber Resilience Act, ENISA, cyber resilience, cybersecurity management, organizational support, implementation, regulatory fragmentation.

Chepurna Olena
National University «Odessa Law Academy»
Associate Professor of the Department of Cybersecurity,
PhD of Physical and Mathematical Sciences, Associate Professor

ANALYTICAL MODELS OF DECISION-MAKING IN STATE CYBERSECURITY SYSTEMS UNDER CONDITIONS OF UNCERTAINTY

The functioning of state-level cybersecurity systems takes place in conditions of uncertainty, which is both objective and informational. On the one hand, cyber threats are formed as random processes with significant variability of parameters, which makes it impossible to accurately predict them. On the other hand, the available data on potential attacks, their probability and the scale of consequences are fragmented, incomplete and often contradictory, which limits the possibilities of their direct use in formalized decision-making procedures. Under such conditions, the cybersecurity management process acquires the features of a task with incomplete information, where not only the assessment of threat parameters, but also the degree of trust in these assessments plays a significant role.

The use of traditional deterministic approaches in this context does not provide an adequate level of adequacy, since such approaches assume the fixity of the input parameters and do not consider their stochastic nature. As a result, the solutions obtained may be optimal only for a separate, often hypothetical scenario, but lose their effectiveness when the conditions for the functioning of the system change. This is especially manifested in the conditions of adaptive behavior of an attacker, who changes attack strategies in response to the implemented protection measures, which leads to a dynamic reformatting of the risk environment.