УДК 342.9:004.056
DOI https://doi.org/10.32782/1813-338X-2025.3.6

С. О. Мазепа
кандидат юридичних наук, доцент,
доцент кафедри кримінального права та процесу
Західноукраїнського національного університету,
міжнародний дослідник
Оснабрюцького університету
https://orcid.org/0000-0003-1282-9089

ІМПЛЕМЕНТАЦІЯ ЄВРОПЕЙСЬКИХ СТАНДАРТІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В НАЦІОНАЛЬНЕ ЗАКОНОДАВСТВО: ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ

Ця стаття присвячена дослідженню процесу імплементації європейських стандартів інформаційної безпеки до національного законодавства України. В умовах активної європейської інтеграції та цифрової трансформації українського суспільства питання гармонізації національного законодавства з вимогами ЄС у сфері кібербезпеки набувають особливої актуальності. Дослідження спрямоване на виявлення ключових проблем та визначення перспективних напрямів удосконалення правового регулювання інформаційної безпеки в Україні.

У роботі проводиться комплексний аналіз основних директив та регламентів Європейського Союзу в галузі інформаційної безпеки, включаючи Директиву NIS2, Акт про цифрові послуги (DSA), Акт про цифрові ринки (DMA) та Загальний регламент із захисту даних (GDPR). Особлива увага приділяється вивченню механізмів транспозиції європейських норм у національні правові системи держав-членів ЄС та можливості адаптації цього досвіду для українських реалій.

Методологічну основу дослідження становлять порівняльно-правовий аналіз, системний підхід та метод експертної оцінки нормативно-правових актів. Автором проаналізовано чинні українські закони у сфері кібербезпеки, захисту персональних даних та цифрового розвитку, а також виявлено прогалини у правовому регулюванні, що перешкоджають ефективній імплементації європейських стандартів. Дослідження базується на вивченні наукових публікацій, офіційних документів ЄС та національного законодавства.

Основними проблемами імплементації визначено: невідповідність термінологічного апарату українського законодавства до європейських стандартів, недостатня розвиненість інституційної інфраструктури кібербезпеки, обмежені фінансові та технічні ресурси для впровадження нових вимог, а також необхідність підвищення кваліфікації фахівців у галузі інформаційної безпеки. Виявлено також процедурні складності координації між різними державними органами, відповідальними за забезпечення кібербезпеки.

Перспективними напрямками вдосконалення правового регулювання визначено: створення єдиної концептуальної бази термінів та визначень відповідно до європейських стандартів, формування ефективної системи міжвідомчої взаємодії, розвиток державно-приватного партнерства у сфері кібербезпеки та створення спеціалізованих освітніх програм. Особлива роль відводиться розвитку цифрової грамотності населення та формуванню культури інформаційної безпеки у суспільстві.

Результати дослідження можуть бути використані для розробки нових нормативно-правових актів України у сфері інформаційної безпеки, а також для підготовки рекомендацій щодо вдосконалення існуючого законодавства. Практична значимість роботи полягає у можливості застосування запропонованих підходів до імплементації європейських стандартів для прискорення процесу євроінтеграції України та підвищення рівня національної кібербезпеки у контексті сучасних викликів та загроз.

Ключові слова: *інформаційна безпека, правоохоронна сфера, кібербезпека, правове забезпечення, адміністративно-правовий аспект, кримінальна відповідальність,*

адміністративна відповідальність, євроінтеграція, гармонізація законодавства, міжнародні стандарти, НАТО, Європейський Союз (ЄС), державна інформаційна політика, загрози інформаційній безпеці, імплементація права, суб'єкти інформаційної безпеки, юридична відповідальність, інформаційні правопорушення, пропаганда, штучний інтелект.

Постановка проблеми. В умовах стрімкого розвитку цифрових технологій та зростаючих кіберзагроз питання забезпечення інформаційної безпеки набувають критичного значення для національної безпеки держав. Україна, перебуваючи на шляху до європейської інтеграції та переживаючи період активної цифрової трансформації, стикається з необхідністю кардинального перегляду існуючих підходів до правового регулювання інформаційної безпеки. Асоціаційна угода між Україною та Європейським Союзом встановлює чіткі зобов'язання щодо гармонізації національного законодавства з європейськими стандартами, що робить дослідження проблем та перспектив імплементації європейських норм у сфері інформаційної безпеки особливо актуальним у сучасних геополітичних умовах.

Особливої гостроти ця проблематика набуває у контексті військової агресії російської федерації проти України, яка супроводжується масштабними кібератаками на критичну інформаційну інфраструктуру держави. У цих умовах забезпечення відповідності українського законодавства сучасним європейським стандартам кібербезпеки стає не лише питанням євроінтеграції, а й імперативом національної оборони. Європейський Союз активно розвиває свою нормативну базу в галузі інформаційної безпеки, приймаючи нові директиви та регламенти, такі як NIS2, Акт про цифрові послуги та Акт про цифрові ринки, що вимагає своєчасної адаптації українського законодавства до європейських вимог, що динамічно змінюються.

Практична актуальність дослідження визначається необхідністю напрацювання конкретних рекомендацій щодо вдосконалення механізмів імплементації європейських стандартів інформаційної безпеки в українське законодавство. Сучасна правова система України характеризується фрагментарністю регулювання у сфері кібербезпеки, відсутністю єдиних термінологічних підходів та недостатньою координацією між різними державними органами, відповідальними за забезпечення інформаційної безпеки. Ці проблеми створюють перешкоди для ефективної протидії кіберзагрозам та гальмують процес інтеграції України в європейський цифровий простір, що зумовлює необхідність проведення комплексного аналізу існуючих викликів та визначення оптимальних шляхів їх подолання.

Наукова **актуальність теми** пов'язана з недостатньою розробленістю теоретичних засад процесу імплементації наднаціональних стандартів інформаційної безпеки у національні правові системи країн, які не є членами Європейського Союзу. Більшість існуючих досліджень зосереджено на аналізі досвіду держав-членів ЄС, тоді як специфіка адаптації європейських норм в умовах перехідних правових систем залишається недостатньо вивченою. Крім того, динамічний розвиток європейського законодавства у галузі цифрових технологій та кібербезпеки потребує постійного моніторингу та аналізу нових тенденцій, що актуалізує необхідність проведення сучасних досліджень, спрямованих на виявлення оптимальних моделей правової рецепції європейських стандартів інформаційної безпеки до національного законодавства України.

Аналіз останніх досліджень і публікацій. Проблематика імплементації європейських стандартів інформаційної безпеки в національне законодавство України привертає увагу багатьох дослідників у контексті євроінтеграційних процесів. вимогам Акту про цифрові послуги ЄС для забезпечення ефективного функціонування цифрового ринку.

Значний внесок у дослідження питань інформаційної безпеки зробили Dunn Cavelty M., Klimburg A. [1; 2]. Дані роботи демонструють еволюцію підходів до забезпечення інформаційної безпеки в умовах цифровізації державних послуг.

Karvatska, Svitlana & Manyk, A. Z. & Labyk, A. R (2025) здійснюють вивчення досвіду України у галузі міжнародного співробітництва у сфері кібербезпеки [5], наголошуючи на практичних механізмах взаємодії з міжнародними партнерами.

Особливу увагу дослідників *Mazepa S., Bratasyuk O. (2023)*, зокрема привертають питання медіарегулювання та протидії інформаційним погрозам. воєнного конфлікту [10].

Gibbons, T., & Humphreys, P. (2012) вніс внесок у розуміння дискурсу розвитку цифрового ринку ЄС [7], що має важливе значення

для розуміння контексту, в якому відбувається імплементація європейських стандартів. європейських стандартів інформаційної безпеки в українському законодавстві в сучасних умовах проведено не було, що зумовлює актуальність цього дослідження.

Мета статті. Метою цієї статті є комплексний аналіз процесу імплементації європейських стандартів інформаційної безпеки в національне законодавство України, виявлення ключових проблем і перешкод, що виникають під час цього процесу, а також визначення перспективних напрямів удосконалення правового регулювання у сфері кібербезпеки задля забезпечення ефективної гармонізації українських правових норм із вимогами європейського законодавства в контексті євроінтеграційних процесів і сучасних викликів цифрового суспільства.

Виклад основного матеріалу. Сучасні процеси глобалізації та цифровізації суспільних відносин актуалізують питання гармонізації національного законодавства з міжнародними стандартами інформаційної безпеки. Особливого значення в цьому контексті набуває імплементація європейських правових норм, які формують базові засади захисту персональних даних та забезпечення кібербезпеки. Директива 2016/1148/ЄС щодо заходів щодо забезпечення високого загального рівня безпеки мережевих та інформаційних систем по всьому Союзу (NIS Directive) встановлює рамкові вимоги до національних систем кібербезпеки, вимагаючи від держав-членів створення відповідних інституційних механізмів та нормативно-правової регламентації [11].

Фундаментальним документом європейського права у сфері інформаційної безпеки є Загальний регламент захисту даних (GDPR) 2016/679, який кардинально змінив підходи до обробки персональних даних та встановив суворі вимоги до їх захисту. Цей акт передбачає екстериторіальну дію, що зобов'язує держави, які прагнуть інтеграції з європейським правовим простором, адаптувати свої національні законодавчі системи до його вимог. Принципи законності, справедливості, прозорості, обмеження цілей, мінімізації даних, точності, обмеження зберігання, цілісності та конфіденційності, закріплені у статті 5 GDPR, мають знайти відображення у національних нормативних актах [12].

Директива 2002/58/ЕС про конфіденційність та електронні комунікації (ePrivacy Directive), модифікована наступними змінами, встановлює спеціальні правила захисту приватного життя в секторі електронних комунікацій [13]. Цей документ регулює питання обробки даних про трафік, використання cookies, спаму та інших аспектів цифрової приватності. Національне законодавство має забезпечувати баланс між правом на недоторканність приватного життя та необхідністю боротьби з кіберзлочинністю, що потребує ретельного опрацювання правових механізмів.

Конвенція Ради Європи про кіберзлочинність (Будапештська конвенція) 2001 року є першим міжнародним договором, спрямованим на боротьбу з комп'ютерними злочинами та злочинами в Інтернеті [14]. Статті 2–11 Конвенції містять визначення складів кіберзлочинів, які мають бути криміналізовані у національному законодавстві, включаючи незаконний доступ, незаконне перехоплення, втручання у дані та системи, шахрайство та підробку документів з використанням комп'ютерних технологій. Імплементація цих норм потребує комплексного перегляду кримінального законодавства та створення спеціалізованих правоохоронних структур.

Регламент ЄС 2019/881 щодо ENISA (Агентство Європейського Союзу з кібербезпеки) та сертифікації кібербезпеки встановлює загальноєвропейську схему сертифікації продуктів, послуг та процесів у галузі кібербезпеки [15]. Цей документ передбачає створення єдиних стандартів оцінки безпеки ІКТ-продуктів та послуг, що вимагає від національних регуляторів розробки відповідних процедур акредитації та сертифікації. Імплементація цього регламенту сприяє підвищенню довіри споживачів до цифрових технологій та формування єдиного цифрового ринку.

Директива (ЄС) 2022/2555 про заходи щодо забезпечення високого загального рівня кібербезпеки по всьому Союзу (NIS2 Directive) значно розширює сферу застосування вимог кібербезпеки, включаючи нові сектори економіки та встановлюючи суворіші зобов'язання для операторів критично важливих послуг. Національна імплементація цієї директиви вимагає перегляду критеріїв визначення критичної інфраструктури, посилення вимог щодо управління ризиками кібербезпеки та створення ефективних механізмів реагування на інциденти [16].

Однією із ключових проблем імплементації європейських стандартів є невідповідність національних правових традицій та інституційних структур європейським підходам

до регулювання інформаційної безпеки. Відмінності у правових системах, адміністративних процедурах та культурних особливостях створюють перешкоди для прямого запозичення європейських норм. Необхідність адаптації закордонного правового досвіду до національних умов потребує глибокого аналізу сумісності правових інститутів та розробки перехідних механізмів.

Технологічні виклики імплементації пов'язані з необхідністю створення технічної інфраструктури, що відповідає європейським стандартам кібербезпеки. Впровадження вимог щодо захисту персональних даних, повідомлення про порушення безпеки, проведення оцінки впливу на захист даних потребує значних інвестицій у інформаційні системи та підготовку кваліфікованих кадрів. Відсутність достатніх технічних та фінансових ресурсів може суттєво уповільнити процес приведення національних систем у відповідність до європейських вимог.

Інституційні перешкоди включають необхідність створення або реформування національних органів, відповідальних за кібербезпеку та захист персональних даних. Європейські стандарти передбачають існування незалежних регуляторних органів із достатніми повноваженнями та ресурсами для ефективного нагляду за дотриманням вимог інформаційної безпеки. Формування таких інститутів потребує політичної волі, законодавчих змін та виділення відповідного бюджетного фінансування.

Перспективи успішної імплементації європейських стандартів інформаційної безпеки пов'язані з поетапним підходом до гармонізації законодавства, що враховує національні особливості та можливості. Створення національних стратегій кібербезпеки, що ґрунтуються на європейських принципах, але адаптованих до місцевих умов, може забезпечити ефективне впровадження міжнародних стандартів. Важливим елементом є розвиток міжнародного співробітництва в галузі обміну інформацією про кіберзагрози та координацію заходів у відповідь.

Довгострокові вигоди від імплементації європейських стандартів інформаційної безпеки включають підвищення рівня захисту прав громадян у цифровому середовищі, зміцнення довіри до національної цифрової економіки та інтеграцію до європейського цифрового простору. Відповідність міжнародним стандартам сприяє залученню іноземних інвестицій у ІКТ-сектор, розвитку експорту цифрових послуг та зміцненню національної конкурентоспроможності. Створення сучасної правової бази інформаційної безпеки є необхідною умовою для побудови цифрового суспільства та держави, що відповідає викликам XXI століття.

Заключно слід зазначити, що успішна імплементація європейських стандартів інформаційної безпеки потребує комплексного підходу, який включає не лише зміну законодавства, а й створення ефективних інституцій, розвиток технічної інфраструктури та підготовку кваліфікованих кадрів. Тільки системна робота з усіх напрямків може забезпечити досягнення цілей гармонізації національного законодавства з європейськими вимогами та створення надійної системи захисту інформації у цифрову епоху.

Висновки і пропозиції. Проведене дослідження дозволяє констатувати, що процес імплементації європейських стандартів інформаційної безпеки до національного законодавства України характеризується системними проблемами, що перешкоджають ефективній гармонізації правових норм. Основними перешкодами є концептуальні відмінності у підходах до правового регулювання інформаційної безпеки, невідповідність термінологічного апарату українського законодавства до європейських стандартів, а також недостатня інституційна готовність державних органів до впровадження комплексних заходів кібербезпеки. Виявлені проблеми свідчать про необхідність кардинального перегляду існуючих механізмів правової рецепції європейських норм та створення системного підходу до процесу імплементації.

Аналіз європейського законодавства у сфері інформаційної безпеки демонструє динамічний розвиток правових стандартів, які потребують постійної адаптації національних законодавчих систем до нових викликів цифрової доби. Особливо важливими для України є вимоги Директиви NIS2, Акту про цифрові послуги, Акту про цифрові ринки та GDPR, які встановлюють високі стандарти захисту персональних даних, кібербезпеки критичної інфраструктури та регулювання цифрових платформ. Українське законодавство демонструє часткову відповідність цим стандартам, проте існуючі прогалини у правовому регулюванні створюють ризики для національної інформаційної безпеки та гальмують процес європейської інтеграції.

Перспективними напрямками вдосконалення правового регулювання інформаційної безпеки в Україні визначено: розробку єдиної

концептуальної основи термінології кібербезпеки відповідно до європейських стандартів; створення ефективної системи міжвідомчої координації та розмежування повноважень між державними органами; формування інституційної інфраструктури, здатної забезпечити повноцінну імплементацію європейських вимог; розвиток механізмів державно-приватного партнерства у сфері кібербезпеки. Реалізація цих напрямів потребує не лише законодавчих змін, а й суттєвих інвестицій у технічне оснащення, підготовку кваліфікованих кадрів та створення культури інформаційної безпеки у суспільстві.

Список використаної літератури:

1. Dunn Cavelty M. Cyber-Security and Threat Politics: US Efforts to Secure the Information Age. London : Routledge. 2008. 224 p.
2. Klimburg A. The Darkening Web: The War for Cyberspace. New York : Penguin Press. 2017. 352 p.
3. Mazepa S. Criminal Law Provisions Countering Propaganda on Social Media in Connection with the Russo-Ukrainian War. *OER Osteuropa Recht.* 2023. Vol. 68. № 4. P. 443–456.
4. Tietievin M. Experience of Ukraine in the field of international cooperation in the field of Cyber Security. *Uzhhorod National University Herald*. Series: Law. 2024. № 3. P. 263–266. DOI: 10.24144/2307-3322.2024.82.3.41
5. Karvatska S., Manyk A. Z., Labyk A. R. The right to cybersecurity: cooperation on countering cyber threats in Ukraine and the EU. *Juridical scientific and electronic journal.* 2025. P. 381–383. DOI: 10.32782/2524-0374/2025-2/89
6. Марущак А. І. Стратегія кібербезпеки України: правові засади та механізми реалізації. *Вісник Національного університету «Львівська політехніка».* Серія: Юридичні науки. 2024. № 2 (38). С. 112–119.
7. Gibbons T., Humphreys P. Audiovisual Regulation under Pressure: Comparative Cases from North America and Europe. 1st ed. Routledge, 2012. DOI: 10.4324/9780203144091
8. Мазепа С. Небезпечне поєднання пропаганди та інтернету в умовах російсько-української війни. *Право України.* 2024. № 1. С. 129–140.
9. Karpenko V. L. Institutional design of cybersecurity agencies: comparative study of EU member states. *Comparative Public Administration Review.* 2024. Vol. 13. № 2. P. 67–84.
10. Mazepa S., Bratasyuk O. Die Gewährleistung der Informationssicherheit in der Ukraine–Verwaltungs- und strafrechtliche Maßnahmen. OER Osteuropa Recht. 2023. Vol. 68. № 4. P. 421–442.
11. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive). *Official Journal of the European Union.* L 194, 19.7.2016. P. 1–30.
12. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). *Official Journal of the European Union.* L 119, 4.5.2016. P. 1–88.
13. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in electronic communications sector (ePrivacy Directive). *Official Journal of the European Communities.* L 201, 31.7.2002. P. 37–47.
14. Council of Europe Convention on Cybercrime (Budapest Convention), CETS No. 185, Budapest, 23.XI.2001. URL: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185
15. Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification. *Official Journal of the European Union.* L 151, 7.6.2019. P. 15–69.
16. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS2 Directive). *Official Journal of the European Union.* L 333, 27.12.2022. P. 80–152.

Mazepa S. O. Implementation of European information security standards into national legislation: problems and prospects

This article is devoted to the study of the process of implementation of European information security standards into the national legislation of Ukraine. In the context of active European integration and digital transformation of Ukrainian society, the issues of harmonisation of national legislation with EU requirements in the field of cybersecurity are becoming particularly relevant. The study is aimed at identifying key issues and determining promising areas for improving the legal regulation of information security in Ukraine.

The paper provides a comprehensive analysis of the main EU directives and regulations in the field of information security, including the NIS2 Directive, the Digital Services Act (DSA), the Digital Markets Act (DMA) and the General Data Protection Regulation (GDPR). Particular attention is paid to the study of the mechanisms of transposition of European norms into the national legal systems of EU member states and the possibility of adapting this experience to Ukrainian realities.

The methodological basis of the study is a comparative legal analysis, a systematic approach and the method of expert assessment of legal acts. The author analyses the current Ukrainian laws in the field of cybersecurity, personal data protection and digital development, and identifies gaps in legal regulation that impede the effective implementation of European standards. The research is based on the study of scientific publications, official EU documents and national legislation.

The main problems of implementation are identified as follows: inconsistency of the terminology of Ukrainian legislation with European standards, insufficient development of the institutional cybersecurity infrastructure, limited financial and technical resources for the implementation of new requirements, and the need to improve the skills of information security professionals. Procedural difficulties in coordination between various government agencies responsible for ensuring cybersecurity have also been identified.

Promising areas for improving legal regulation include the creation of a unified conceptual framework of terms and definitions in accordance with European standards, the formation of an effective system of interagency cooperation, the development of public-private partnerships in the field of cybersecurity, and the creation of specialised educational programmes. A special role is given to the development of digital literacy and the formation of a culture of information security in society.

The results of the study can be used to develop new legal acts of Ukraine in the field of information security, as well as to prepare recommendations for improving existing legislation. The practical significance of the work lies in the possibility of applying the proposed approaches to the implementation of European standards to accelerate Ukraine's European integration and improve the level of national cybersecurity in the context of current challenges and threats.

Key words: *information security, law enforcement, cybersecurity, legal support, administrative-legal aspect, criminal liability, administrative liability, European integration, harmonization of legislation, international standards, NATO, European Union (EU), state information policy, information security threats, implementation of law, subjects of information security, legal liability, information offenses, propaganda, artificial intelligence.*

Дата першого надходження рукопису до видання: 21.07.2025
Дата прийнятого до друку рукопису після рецензування: 25.08.2025
Дата публікації: 30.09.2025