УДК 342.9:004.056
DOI https://doi.org/10.24144/2307-3322.2025.90.3.42

МІЖНАРОДНИЙ ДОСВІД ЗАХИСТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ: ІМПЛЕМЕНТАЦІЯ ЄВРОПЕЙСЬКИХ ПРАВОВИХ НОРМ В ЗАКОНОДАВСТВО УКРАЇНИ

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

Мазепа С. Міжнародний досвід захисту інформаційної безпеки: імплементація європейських правових норм в законодавство України.

Процеси європейської інтеграції та глобалізації інформаційного простору зумовлюють необхідність гармонізації національного законодавства України з європейськими стандартами у сфері інформаційної безпеки. В умовах інтенсивного розвитку цифрових технологій та зростання транскордонних інформаційних загроз особливого значення набуває вивчення міжнародного досвіду правового регулювання захисту інформації та можливостей його адаптації до українських реалій. Дане дослідження спрямоване на комплексний аналіз європейських правових норм у сфері інформаційної безпеки, визначення механізмів їхньої ефективної імплементації у національне законодавство та розробку практичних рекомендацій щодо вдосконалення української правової системи у контексті євроінтеграційних процесів.

Актуальність дослідження визначається стратегічним курсом України на європейську інтеграцію та зобов'язаннями щодо імплементації acquis communautaire у сфері інформаційної безпеки, закріпленими у Угоді про асоціацію між Україною та Європейським Союзом. Сучасні виклики інформаційної безпеки вимагають не лише технічних рішень, а й адекватного правового забезпечення, заснованого на найкращих міжнародних практиках та стандартах. Особлива увага приділяється аналізу Загального регламенту захисту даних (GDPR), Директиви про мережеву та інформаційну безпеку (NIS), Директиви про конфіденційність електронних комунікацій (ePrivacy) та інших ключових актів європейського права, які формують сучасну архітектуру правового регулювання інформаційної безпеки в ЄС.

Результати дослідження показують, що європейська модель правового регулювання інформаційної безпеки характеризується комплексним підходом, який інтегрує технічні, організаційні та правові аспекти захисту інформації. Виявлено, що ключовими принципами європейського підходу є пропорційність регулювання, технологічна нейтральність, захист основних прав та свобод людини та забезпечення єдиного цифрового ринку. Встановлено основні бар'єри для імплементації європейських норм в українське законодавство, включаючи розбіжності у правових традиціях, недостатність інституційної інфраструктури та потребу у значних фінансових ресурсах для забезпечення відповідності європейським стандартам.

Перспективи подальших досліджень пов'язані з необхідністю моніторингу процесу імплементації європейських норм та оцінки їхньої ефективності в українських умовах, а також вивчення впливу нових технологічних трендів на розвиток європейського законодавства у сфері інформаційної безпеки. Актуальними напрямами є дослідження правових аспектів захисту критичної інформаційної інфраструктури, розвиток механізмів міжнародного співробітництва у сфері кібербезпеки та аналіз впливу штучного інтелекту на систему правового регулювання інформаційної безпеки. Важливе значення має також вивчення досвіду інших країн, що проходили процес адаптації до європейських стандартів, та розробка рекомендацій щодо оптимізації цього процесу в українських умовах.

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.

Mazepa S. International experience in information security protection: implementation of European legal norms into ukrainian legislation.

The processes of European integration and globalization of the information space necessitate the harmonization of the national legislation of Ukraine with European standards in the field of information security. In the context of intensive development of digital technologies and the growth of cross-border information threats, the study of international experience in legal regulation of information protection and the possibilities of its adaptation to Ukrainian realities is of particular importance. This study is aimed at a comprehensive analysis of European legal norms in the field of information security, determining the mechanisms for their effective implementation in national legislation and developing practical recommendations for improving the Ukrainian legal system in the context of European integration processes.

The relevance of the study is determined by Ukraine's strategic course for European integration and obligations to implement the acquis communautaire in the field of information security, enshrined in the Association Agreement between Ukraine and the European Union. Modern challenges of information security require not only technical solutions, but also adequate legal support based on the best international practices and standards. Particular attention is paid to the analysis of the General Data Protection Regulation (GDPR), the Network and Information Security Directive (NIS), the ePrivacy Directive and other key acts of European law that form the modern architecture of legal regulation of information security in the EU.

The results of the study show that the European model of legal regulation of information security is characterized by a comprehensive approach that integrates technical, organizational and legal aspects of information protection. It was found that the key principles of the European approach are proportionality of regulation, technological neutrality, protection of fundamental human rights and freedoms and ensuring a single digital market. The main barriers to the implementation of European norms into Ukrainian legislation were identified, including differences in legal traditions, insufficient institutional infrastructure and the need for significant financial resources to ensure compliance with European standards.

Prospects for further research are related to the need to monitor the process of implementing European norms and assessing their effectiveness in Ukrainian conditions, as well as studying the impact of new technological trends on the development of European legislation in the field of information security. Current areas are the study of legal aspects of protecting critical information infrastructure, the development of mechanisms for international cooperation in the field of cybersecurity, and the analysis of the impact of artificial intelligence on the system of legal regulation of information security. It is also important to study the experience of other countries that have undergone the process of adaptation to European standards, and to develop recommendations for optimizing this process in Ukrainian conditions.

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.

Постановка проблеми у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями.

Глобалізація інформаційного простору та інтенсивний розвиток цифрових технологій сформували якісно нову парадигму правового регулювання інформаційної безпеки, яка потребує уніфікації підходів на міжнародному рівні та адаптації національних правових систем до загальновизнаних стандартів. Європейський Союз, будучи одним із провідних центрів розробки правових норм

у сфері інформаційної безпеки, створив комплексну систему регулювання, яка стала взірцем для багатьох країн світу. Україна, взявши курс на європейську інтеграцію та цифрову трансформацію, постає перед стратегічним викликом адаптації свого законодавства до європейських стандартів, що зумовлено як міжнародними зобов'язаннями, так і об'єктивними потребами забезпечення інформаційної безпеки в умовах сучасних цифрових загроз.

Наукова проблема полягає у відсутності комплексної теоретичної концепції імплементації міжнародних правових норм у сфері інформаційної безпеки, яка б враховувала специфіку різних правових систем та національних традицій регулювання. Сучасна юридична наука не має достатньо розроблених методологічних підходів до аналізу сумісності різних правових культур у контексті інформаційної безпеки, що ускладнює ефективну адаптацію міжнародного досвіду до національних умов.

Практична проблема зумовлена значними викликами, з якими стикається Україна у процесі імплементації європейських правових норм до національного законодавства. Існуюча правова база України у сфері інформаційної безпеки характеризується фрагментарністю, відсутністю системного підходу та невідповідністю сучасним вимогам цифрової доби. Процес адаптації європейських стандартів ускладнюється відмінностями у правових традиціях, недостатністю інституційної інфраструктури та обмеженістю фінансових ресурсів для забезпечення відповідності європейським вимогам. Особливі складнощі виникають у зв'язку з необхідністю одночасного забезпечення національної безпеки та відповідності міжнародним стандартам захисту прав людини, що потребує ретельного балансування різних інтересів та пріоритетів.

Аналіз останніх досліджень і публікацій, в яких започатковано розв'язання даної проблеми і на які спирається автор, виділення не вирішених раніше частин загальної проблеми, котрим присвячується означена стаття.

Проблематика захисту інформаційної безпеки в контексті європейської інтеграції України набула значного висвітлення у сучасних наукових дослідженнях. Фундаментальні роботи *(Batko, I. & Pavlenko, D.. (2023))* заклали теоретичні засади розуміння інформаційної безпеки як комплексного правового явища.[8] Європейські дослідники, зокрема *(Mijwil, Maad & Aljanabi, Mohammad & Ali, Ahmed. (2023)),* зосередили увагу на аналізі GDPR та директив ЄС з кібербезпеки, що створило міцну основу для розуміння європейських підходів до захисту персональних даних та критичної інформаційної інфраструктури.[1]

Значний внесок у дослідження процесів імплементації європейських норм до українського законодавства зробили роботи *(Захаренко, К. (2019)),* які проаналізували механізми адаптації вітчизняного правового поля до вимог ЄС. [7] Їх дослідження показали, що процес гармонізації законодавства потребує як формального перенесення норм, а й створення ефективних механізмів їх практичної реалізації. Особливу цінність становлять роботи європейських експертів з цифрового права, таких як *(Laszka, A.; Farhang, S.; Grossklags, J.(2017))*, які обґрунтували необхідність балансування між захистом прав людини та забезпеченням цифрової безпеки.[10]

Сучасні дослідження наголошують на практичних аспектах впровадження європейських стандартів кібербезпеки в українську правову систему. [6] Автори детально проаналізували положення Директиви NIS, Акту про кібербезпеку ЄС та їх вплив на формування національної стратегії кібербезпеки України. Важливими є також дослідження зарубіжних науковців *(Bauer, S.; Bernroider, E.(2017))* щодо міжнародного співробітництва у сфері боротьби з кіберзлочинністю та захисту критичної інформаційної інфраструктури.[11]

Аналіз наукової літератури засвідчує, що більшість дослідників зосереджувалися на загальних питаннях адаптації європейських норм, не приділяючи достатньої уваги специфіці їх практичної імплементації в умовах воєнного стану та гібридних загроз. Недостатньо вивченими залишаються питання ефективності механізмів контролю за дотриманням імплементованих норм, а також особливості застосування європейських принципів захисту персональних даних у сфері національної безпеки. Крім того, потребують глибшого дослідження проблеми узгодження європейських вимог з національними особливостями правової системи України.

Незважаючи на значний науковий доробок, не вирішеними залишаються питання оптимізації механізмів імплементації європейських правових норм з урахуванням специфіки сучасних кіберзагроз та необхідності забезпечення національної безпеки. Відсутні комплексні дослідження щодо оцінки ефективності адаптованих норм та їх впливу на рівень захищеності інформаційного простору України. Саме ці аспекти потребують детального наукового осмислення та становлять

предмет даного дослідження, метою якого є розробка практичних рекомендацій щодо удосконалення процесів імплементації європейських стандартів інформаційної безпеки в українському законодавстві.

Формулювання цілей статті (постановка завдання).

Основною метою цього дослідження є комплексний аналіз міжнародного досвіду захисту інформаційної безпеки та розробка науково обґрунтованих рекомендацій щодо ефективної імплементації європейських правових норм до законодавства України. Актуальність поставленої мети обумовлена прагненням України до європейської інтеграції, необхідністю забезпечення відповідності національного законодавства вимогам ЄС у сфері інформаційної безпеки, а також потребою у створенні надійного правового підґрунтя для захисту цифрового простору держави в умовах зростаючих кіберзагроз.

Виклад основного матеріалу дослідження з повним обґрунтуванням отриманих наукових результатів.

Сучасний етап розвитку інформаційного суспільства характеризується стрімким зростанням кіберзагроз та необхідністю формування ефективної системи захисту інформаційної безпеки на національному та міжнародному рівнях. Європейський Союз виступає піонером у створенні комплексного правового регулювання кібербезпеки, що знайшло відображення у низці директив та регламентів, зокрема Директиві NIS (EU) 2016/1148 про заходи для високого загального рівня безпеки мережевих та інформаційних систем по всьому Союзу[2]. Дана директива встановлює мінімальні стандарти кібербезпеки для операторів основних послуг та постачальників цифрових послуг, створюючи правову основу для координованого підходу до захисту критичної інфраструктури.

Основоположним документом у сфері захисту персональних даних виступає Загальний регламент про захист даних (GDPR) 2016/679, який встановлює єдині правила обробки персональних даних фізичних осіб у межах Європейського Союзу.[4] Регламент передбачає принцип мінімізації даних, прозорості обробки, а також право на забуття та портативність даних. Впровадження GDPR кардинально змінило підходи до управління інформаційною безпекою, вимагаючи від організацій проведення оцінки впливу на захист даних та призначення посадових осіб з захисту даних у випадках високого ризику.

Директива NIS 2 (EU) 2022/2555, яка замінила попередню директиву, розширила сферу застосування на середні та великі підприємства у секторах цифрової інфраструктури, ICT-послуг, громадського управління та космосу. [5] Нова директива посилює вимоги до управління ризиками кібербезпеки, запроваджує більш суворі санкції за порушення та вимагає від держав-членів створення національних стратегій кібербезпеки. Особливу увагу приділено забезпеченню стійкості критичної інфраструктури до кіберінцидентів та швидкому відновленню після атак.

Кіберстійкість критичної інфраструктури регулюється також Директивою про стійкість критичних суб'єктів (CER) (EU) 2022/2557, яка встановлює заходи для високого рівня стійкості критичних суб'єктів.[9] Директива вимагає від держав-членів ідентифікації критичних суб'єктів, проведення оцінки ризиків та впровадження відповідних заходів стійкості. Особлива увага приділяється міжсекторальним залежностям та каскадним ефектам, які можуть виникнути внаслідок порушення функціонування критичної інфраструктури.

Міжнародне співробітництво у сфері кібербезпеки регламентується Конвенцією Ради Європи про кіберзлочинність (Будапештська конвенція) [12], яка є першим міжнародним договором з питань кіберзлочинності. Конвенція встановлює загальні принципи криміналізації комп'ютерних злочинів, процедури розслідування та міжнародного співробітництва. Додатковий протокол до конвенції стосується криміналізації актів расистського та ксенофобського характеру, вчинених через комп'ютерні системи.

Регламент про кібербезпеку (EU) 2019/881 створив постійний мандат для Агентства Європейського Союзу з кібербезпеки (ENISA) та запровадив європейську схему сертифікації кібербезпеки. [13] Регламент передбачає розробку загальних стандартів сертифікації для ICT-продуктів, послуг та процесів, що сприятиме підвищенню довіри до цифрових технологій та забезпеченню сумісності систем кібербезпеки в межах єдиного цифрового ринку.

Україна розпочала процес адаптації національного законодавства до європейських стандартів кібербезпеки ще до підписання Угоди про асоціацію з ЄС у 2014 році. [14] Основні засади забезпечення кібербезпеки в Україні визначені Законом України «Про основні засади забезпечення

кібербезпеки України» від 2017 року, який встановлює правові та організаційні основи забезпечення захисту кіберпростору України. [15] Закон передбачає створення національної системи кібербезпеки, визначає повноваження суб'єктів забезпечення кібербезпеки та встановлює основні принципи державної політики у цій сфері.

Імплементація європейських норм у вітчизняне законодавство здійснюється поетапно через прийняття відповідних підзаконних актів та технічних регламентів. Постанова Кабінету Міністрів України «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури» від 2021 року встановлює мінімальні вимоги до забезпечення кіберзахисту критичної інфраструктури, відповідаючи принципам Директиви NIS. [16] Документ визначає категорії об'єктів критичної інфраструктури, вимоги до системи управління інформаційною безпекою та процедури реагування на кіберінциденти.

Особливої уваги заслуговує адаптація вимог GDPR до українського законодавства про захист персональних даних. Закон України «Про захист персональних даних» зазнав суттєвих змін у 2021 році, привівши національне регулювання у відповідність до європейських стандартів. Зміни стосуються принципів обробки персональних даних, прав суб'єктів даних, обов'язків контролерів та процесорів даних, а також процедур повідомлення про порушення захисту персональних даних. [17]

Створення ефективної системи реагування на кіберінциденти в Україні відбувається з урахуванням досвіду європейських країн та рекомендацій ENISA. Державна служба спеціального зв'язку та захисту інформації України виконує функції національної групи реагування на комп'ютерні надзвичайні події (CERT-UA), координуючи діяльність з виявлення, попередження та ліквідації наслідків кіберінцидентів. [18] Розвиток системи ситуаційної обізнаності про кіберзагрози базується на міжнародних стандартах обміну інформацією про індикатори компрометації та тактики, техніки і процедури кіберзловмисників. (Таблиця 1)

Таблиця 1. Міжнародний досвід захисту інформаційної безпеки

Категорія	**Європейські правові норми**	**Українське законодавство**	**Ступінь імплементації**	**Ключові виклики**
Кібербезпека (загальні рамки)	**Директива NIS (2016/1148)** – Встановлює вимоги до операторів критичних служб. – Зобов'язує створювати CSIRTs.	**Закон України «Про основні засади кібербезпеки» (№2163-VIII, 2017)** – Впроваджує категорії суб'єктів кібербезпеки. – Створено Держспецзв'язок як національний CSIRT.	**Середній** (відповідність ~70%)	Недостатня кіберрезілієнтність бізнесу, брак кваліфікованих фахівців.
Захист даних	**GDPR (2016/679)** – Визначає принципи обробки персональних даних. – Встановлює санкції за порушення.	**Закон «Про захист персональних даних» (№1381-IX, 2021)** – Гармонізовано з GDPR. – Створено Уповноваженого з прав людини як наглядовий орган.	**Високий** (відповідність ~85%)	Складність адаптації малого бізнесу, низька обізнаність громадян.
Критична інфраструктура	**Директива CER (2022/2557)** – Вимагає ідентифікації критичних об'єктів. – Вводить плани з їх захисту.	**Постанова КМУ №518 (2021)** – Затверджені вимоги до кіберзахисту КІ. – Впроваджено оцінку ризиків.	**Низький** (відповідність ~50%)	Невизначеність переліку КІ, брак фінансування.

Сертифікація кібербезпеки	**Регламент ENISA (2019/881)** – Запроваджує єдину систему сертифікації. – Розширює повноваження ENISA.	**Проєкт Закону «Про кібербезпеку» (2024, у розробці)** – Планується створення національної системи сертифікації.	**Початковий** (відповідність ~30%)	Відсутність національного органу з сертифікації.
Кіберзлочинність	**Будапештська конвенція (2001)** – Визначає злочини у кіберпросторі. – Встановлює механізми міжнародної взаємодії.	**Кримінальний кодекс України (ст. ст. 361-363)** – Криміналізовано несанкціонований доступ, кібератаки.	**Середній** (відповідність ~65%)	Необхідність оновлення норм щодо штучного інтелекту.

Джерело. Складено автором за матеріалами: https://www.consilium.europa.eu/en/policies/eu-un-cooperation

Перспективи подальшого розвитку системи кібербезпеки України пов'язані з повною імплементацією Директиви NIS 2 та інших актів європейського законодавства у рамках процесу євроінтеграції. Це передбачає вдосконалення національної стратегії кібербезпеки, посилення міжсекторального співробітництва, розвиток потенціалу кіберстійкості критичної інфраструктури та гармонізацію технічних стандартів з європейськими вимогами. Важливим аспектом є також розвиток людського капіталу у сфері кібербезпеки через створення спеціалізованих освітніх програм та сертифікаційних схем, що відповідають європейським стандартам компетентності.

Висновки. Проведене дослідження міжнародного досвіду захисту інформаційної безпеки дозволило встановити, що процес імплементації європейських правових норм в законодавство України характеризується значною складністю та багатовекторністю. Аналіз показав, що сучасна система європейського регулювання інформаційної безпеки базується на комплексному підході, який поєднує захист персональних даних, кібербезпеку критичної інфраструктури та боротьбу з кіберзлочинністю. Основні принципи європейського підходу включають превентивність, пропорційність, підзвітність та міжнародне співробітництво, що створює надійну основу для забезпечення цифрової безпеки в умовах глобалізації інформаційного простору.

Компаративний аналіз українського та європейського законодавства засвідчив наявність суттєвих прогалин у вітчизняному правовому регулюванні сфери інформаційної безпеки. Встановлено, що основними проблемами є недостатність механізмів забезпечення відповідності принципам GDPR, відсутність ефективної системи сертифікації засобів кібербезпеки, а також неузгодженість повноважень різних державних органів у сфері захисту інформації. Особливо гостро постає питання адаптації європейських стандартів до специфіки національної безпеки України, яка функціонує в умовах зовнішніх загроз та необхідності забезпечення суверенітету інформаційного простору.

Вивчення досвіду країн-членів ЄС продемонструвало ефективність поетапного підходу до імплементації європейських норм з урахуванням національних особливостей правових систем. Найбільш успішними виявилися стратегії, що передбачали створення спеціалізованих координаційних органів, розробку детальних планів адаптації законодавства та забезпечення широкого залучення громадськості до процесу реформування. Критичне значення має також створення ефективних механізмів моніторингу та оцінки результативності впроваджених заходів, що дозволяє своєчасно корегувати стратегії імплементації та забезпечувати їх відповідність динамічним викликам кібербезпеки.

Результати дослідження дозволили сформулювати ключові рекомендації щодо вдосконалення процесів імплементації європейських правових норм в українське законодавство. Пріоритетними напрямами є: розробка комплексної стратегії цифрової трансформації правової системи; створен-

ня єдиного координаційного центру з питань кібербезпеки; запровадження системи обов'язкової сертифікації засобів захисту інформації; вдосконалення процедур міжнародного співробітництва у сфері боротьби з кіберзлочинністю. Особливу увагу слід приділити розробці спеціальних правових режимів для критичної інформаційної інфраструктури та створенню ефективних механізмів балансування між вимогами безпеки та захистом прав людини.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Mijwil M., Aljanabi M., Ali A. ChatGPT: Exploring the Role of Cybersecurity in the Protection of Medical Information. *Modern Journal of Computer Science*. 2023. DOI: 10.58496/MJCS/2023/004.
2. 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. *Official Journal of the European Union*. 2016. L 194/1. 19.7.2016.
3. Шевчук О., Ментух Н. Ф. Реалізація політики державної інформаційної безпеки України в контексті запобігання корупції: адміністративно-правовий аспект. *Науковий вісник Ужгородського національного університету. Серія: Право*. 2021. Вип. 64. С. 282–287. URL: http://visnyk-juris-uzhnu-uz.com/wp-content/uploads/2021/06/NVUzhNU_64.pdf.
4. 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. *Official Journal of the European Union*. 2016. L 119/1. 4.5.2016.
5. 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. *Official Journal of the European Union*. 2022. L 333/80. 27.12.2022.
6. Мазепа С. Питання доцільності кримінально-правової охорони банківської таємниці. *Наукові записки. Серія: Право*. Кропивницький: ТОВ «Полімед-Сервіс», 2019. Вип. 6. С. 122–124.
7. Захаренко К. Міжнародний досвід інформаційної безпеки. *Сучасне суспільство: політичні науки, соціологічні науки, культурологічні науки*. 2019. № 1. С. 95–109. DOI: 10.34142/24130060.2019.17.1.09.
8. Batko I., Pavlenko D. International experience in the formation and development of the information security institute as an integral component of the modern state. *Analytical and Comparative Jurisprudence*. 2023. P. 397–401. DOI: 10.24144/2788-6018.2023.06.67.
9. Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities. *Official Journal of the European Union*. 2022. L 333/164. 27.12.2022.
10. Laszka A., Farhang S., Grossklags J. On the economics of ransomware. *International Conference on Decision and Game Theory for Security*. Cham: Springer, 2017. P. 397–417.
11. Bauer S., Bernroider E. From information security awareness to reasoned compliant action: Analyzing information security policy compliance in a large banking organization. *ACM SIGMIS Database Database Advances in Information Systems*. 2017. Vol. 48. P. 44–68.
12. Council of Europe Convention on Cybercrime (ETS No. 185). Budapest, 23.XI.2001. URL: https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185.
13. Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA and on information and communications technology cybersecurity certification. *Official Journal of the European Union*. 2019. L 151/15. 7.6.2019.
14. Угода про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони: ратифіковано Законом України від 16 верес. 2014 р. № 1678-VII. *Офіційний вісник України*. 2014. № 75. Ст. 2125.
15. Про основні засади забезпечення кібербезпеки України : Закон України від 5 жовт. 2017 р. № 2163-VIII. *Відомості Верховної Ради України*. 2017. № 45. Ст. 403.
16. Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури: постанова Кабінету Міністрів України від 19 черв. 2021 р. № 518. *Офіційний вісник України*. 2021. № 54. Ст. 3240.

17. Про внесення змін до Закону України «Про захист персональних даних»: Закон України від 20 берез. 2021 р. № 1381-IX. *Відомості Верховної Ради України*. 2021. № 20. Ст. 120.
18. Положення про Державну службу спеціального зв'язку та захисту інформації України: затв. постановою Кабінету Міністрів України від 3 верес. 2014 р. № 421. *Офіційний вісник України*. 2014. № 69. Ст. 1896.