УДК 342.9:004.056
DOI https://doi.org/10.32844/2618-1258.2025.3.35

МАЗЕПА С.О.

ЕВОЛЮЦІЯ КОНЦЕПЦІЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ: ВІД НАЦІОНАЛЬНОЇ БЕЗПЕКИ ДО КІБЕРПРАВОВОГО РЕГУЛЮВАННЯ

EVOLUTION OF THE CONCEPT OF INFORMATION SECURITY: FROM NATIONAL SECURITY TO CYBERLAW REGULATION

У сучасних умовах глобальної цифровізації концепція інформаційної безпеки зазнала кардинальних змін, трансформувавшись із вузькоспеціалізованої галузі військово-технічного захисту в комплексну міждисциплінарну систему правового та технологічного регулювання. Це дослідження аналізує ключові етапи еволюційного розвитку підходів до забезпечення інформаційної безпеки протягом останніх десятиліть.

Історичний аналіз показує, що початкове розуміння інформаційної безпеки формувалося в контексті державної та національної безпеки, коли основний акцент робився на захисті секретної інформації та критично важливих державних систем від зовнішніх загроз. Класична парадигма базувалася на принципах конфіденційності, цілісності та доступності інформації, розглядаючи безпеку переважно через призму технічних засобів захисту та адміністративних заходів контролю.

З розвитком інформаційно-комунікаційних технологій та формуванням глобального кіберпростору відбулося розширення понятійного апарату та методологічних підходів до інформаційної безпеки. Перехід до цифрової економіки зумовив необхідність перегляду традиційних концепцій та формування нової парадигми, яка враховує специфіку віртуального середовища, багаторівневий характер загроз та міжнародний характер інформаційних процесів.

Сучасний етап розвитку характеризується формуванням кіберправового регулювання як самостійної галузі правового знання, що інтегрує елементи інформаційного права, міжнародного права та технічного регулювання. Ця трансформація відбиває об'єктивну потреба у створенні єдиної нормативно-правової бази, здатної забезпечити ефективний захист інформаційних ресурсів за умов транскордонного характеру кіберзагроз і різноманіття суб'єктів інформаційних відносин.

Отримані результати свідчать про формування якісно нової концептуальної моделі інформаційної безпеки, що характеризується інтеграцією технічних, правових та організаційних аспектів захисту в єдину систему кіберправового регулювання. Ця еволюція відбиває об'єктивні закономірності розвитку інформаційного суспільства та визначає перспективні напрями вдосконалення механізмів забезпечення безпеки в цифровому середовищі.

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.*

© МАЗЕПА С.О. – кандидат юридичних наук, доцент, доцент кафедри кримінального права та процесу (Західноукраїнський національний університет), міжнародний дослідник (Оснабрюцький університет) https://orcid.org/0000-0003-1282-9089

In the current context of global digitalisation, the concept of information security has undergone dramatic changes, transforming from a highly specialised area of military and technical defence into a comprehensive interdisciplinary system of legal and technological regulation. This study analyses the key stages of the evolutionary development of approaches to information security over the past decades.

Historical analysis shows that the initial understanding of information security was formed in the context of state and national security, when the main focus was on protecting classified information and critical state systems from external threats. The classical paradigm was based on the principles of confidentiality, integrity and availability of information, viewing security mainly through the prism of technical protection and administrative controls.

With the development of information and communication technologies and the formation of global cyberspace, the conceptual apparatus and methodological approaches to information security have expanded. The transition to the digital economy has necessitated a revision of traditional concepts and the formation of a new paradigm that takes into account the specifics of the virtual environment, the multi-level nature of threats and the international nature of information processes.

The current stage of development is characterised by the formation of cyber law regulation as an independent branch of legal knowledge that integrates elements of information law, international law and technical regulation. This transformation reflects the objective need to create a unified legal framework capable of ensuring effective protection of information resources in the context of cross-border cyber threats and diversity of subjects of information relations.

The results obtained indicate the formation of a qualitatively new conceptual model of information security characterised by the integration of technical, legal and organisational aspects of protection into a single system of cyber legal regulation. This evolution reflects the objective patterns of development of the information society and identifies promising areas for improving the mechanisms of security in the digital environment.

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. Стрімка цифровізація всіх сфер життя у XXI столітті зумовила кардинальну трансформацію традиційних підходів до забезпечення інформаційної безпеки. Сучасне інформаційне суспільство характеризується безпрецедентною інтенсивністю інформаційних потоків, глобальною взаємопов'язаністю цифрових систем та критичною залежністю державних, комерційних та соціальних процесів від функціонування інформаційно-комунікаційних технологій. У цих умовах традиційна парадигма інформаційної безпеки, сформована в епоху автономних обчислювальних систем та локальних інформаційних ресурсів, втрачає свою ефективність та потребує концептуального переосмислення.

Якісні зміни в архітектурі сучасного кіберпростору, включаючи повсюдне впровадження хмарних технологій, розвиток інтернету речей, застосування штучного інтелекту та технологій розподілених реєстрів, генерують нові типи загроз інформаційній безпеці. Гібридні кібератаки, що використовують комбінацію технічних, соціальних та психологічних методів впливу, транскордонний характер кіберзлочинності та зростаючі можливості завдання шкоди критично важливій інфраструктурі через кіберпростір формують якісно нове середовище безпеки. Ця трансформація загрозливого ландшафту потребує адекватного теоретико-методологічного осмислення та розробки відповідних концептуальних підходів до забезпечення захисту інформаційних ресурсів.

Міжнародний характер сучасного кіберпростору обумовлює необхідність гармонізації національних підходів до інформаційної безпеки та формування єдиних стандартів кіберправового регулювання. Відсутність уніфікованої концептуальної бази та узгоджених принципів правового

регулювання у сфері кібербезпеки створює правові лакуни, ускладнює міжнародне співробітництво у протидії кіберзагрозам та знижує ефективність заходів щодо забезпечення інформаційної безпеки. Дослідження еволюційних процесів у розвитку концепції інформаційної безпеки дозволяє виявити закономірності та тенденції, необхідні для формування адекватної сучасним викликам системи кіберправового регулювання.

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. Сучасний стан наукових досліджень у галузі еволюції концепції інформаційної безпеки характеризується інтенсивним розвитком міждисциплінарних підходів та формуванням нової парадигми кіберправового регулювання. Значний внесок у розробку теоретичних основ інформаційної безпеки зробили роботи В.А. Ліпкана [1], О.М. Золотар [2] та М.В. Гуцалюка [3], які досліджували трансформацію національних підходів до забезпечення інформаційної безпеки в контексті глобалізації цифрових процесів. Дані дослідження заклали методологічний фундамент для розуміння еволюційних процесів у сфері захисту інформаційних ресурсів та виявили основні тенденції переходу від традиційних військово-технічних підходів до комплексних систем правового регулювання.

Міжнародні аспекти розвитку концепції інформаційної безпеки отримали відображення в роботах зарубіжних дослідників, серед яких слід виділити дослідження J. Goldsmith [4], T. Rid [5] та M. Libicki [6], присвячені аналізу формування міжнародного кіберправа та механізмів транснаціонального співробітництва у сфері кібербезпеки. Особливу увагу в даних роботах приділено проблемам юрисдикції в кіберпросторі, питанням атрибуції кібератак та розвитку міжнародно-правових норм, що регулюють поведінку держав в інформаційній сфері. Результати цих досліджень свідчать про формування якісно нової системи міжнародних відносин у кіберпросторі, що потребує адекватного правового оформлення.

Технічні аспекти еволюції інформаційної безпеки досліджені в роботах І.В. Діордіци [7], В.Л. Бурячка [8] та Н.Ф. Ментух[9], які аналізують вплив сучасних інформаційних технологій на розвиток методів і засобів захисту інформації. Дані дослідження демонструють, що технологічна трансформація цифрового середовища обумовлює необхідність кардинального перегляду традиційних підходів до забезпечення інформаційної безпеки та формування нових концептуальних моделей, що враховують специфіку хмарних обчислень, технологій штучного інтелекту та розподілених систем.

Правові аспекти трансформації концепції інформаційної безпеки розглянуті в роботах О.А. Баранова [10], К.І. Бєлякова [11] та О.Р. Шевчук[12], які досліджують процеси формування кіберправа як самостійної галузі правового регулювання. Особливу увагу в даних дослідженнях приділено аналізу нормативно-правової бази забезпечення інформаційної безпеки, проблемам гармонізації національних законодавств та розвитку інституту правової відповідальності за правопорушення в кіберпросторі.

Незважаючи на значну кількість досліджень, присвячених окремим аспектам інформаційної безпеки, в сучасній науковій літературі недостатньо комплексних робіт, що аналізують еволюцію концепції інформаційної безпеки як цілісний процес трансформації від національно-державної парадигми до системи кіберправового регулювання. Даний пробіл у науковому знанні обумовлює необхідність проведення комплексного дослідження, що інтегрує технічні, правові та організаційні аспекти еволюції концепції інформаційної безпеки в єдину теоретичну модель.

Формулювання цілей статті. Метою дослідження є комплексний аналіз історичних етапів трансформації концепції інформаційної безпеки від початкових підходів, заснованих на принципах національної безпеки та державного контролю над інформаційними ресурсами, до формування сучасної парадигми кіберправового регулювання, що охоплює багаторівневу систему захисту інформаційного простору.

Дослідження спрямовано на виявлення ключових факторів, що обумовили еволюційні зміни в розумінні сутності інформаційної безпеки, аналіз трансформації суб'єктно-об'єктного складу відносин у сфері кібербезпеки, а також систематизацію сучасних тенденцій розвитку правового регулювання кіберпростору з метою прогнозування перспективних напрямів удосконалення концептуальних засад забезпечення інформаційної безпеки в умовах глобальної цифровізації та появи нових технологічних викликів.

Виклад основного матеріалу дослідження з повним обґрунтуванням отриманих наукових результатів. Історичний аналіз розвитку концепції інформаційної безпеки дозволяє виділити декілька якісно відмінних етапів, кожен з яких характеризується специфічними підходами

до розуміння сутності інформаційної безпеки та методів її забезпечення. Перший етап, що охоплює період з 1940-х по 1970-ті роки, характеризувався формуванням класичної парадигми інформаційної безпеки в контексті національної безпеки держави [13]. На даному етапі основна увага приділялася захисту секретної державної інформації від несанкціонованого доступу, при цьому інформаційна безпека розглядалася переважно як технічна проблема забезпечення конфіденційності даних в автономних обчислювальних системах.

Другий етап еволюції концепції інформаційної безпеки, що припадає на 1980-1990-ті роки, пов'язаний з розвитком персональних комп'ютерів та формуванням локальних обчислювальних мереж [14]. Даний період характеризується розширенням розуміння інформаційної безпеки за межі державного сектора та включенням у сферу регулювання комерційних організацій і приватних користувачів. Прийняття в США Закону про комп'ютерне шахрайство та зловживання 1986 року (Computer Fraud and Abuse Act) [15] та аналогічних нормативних актів в інших розвинених країнах ознаменувало початок формування правової бази інформаційної безпеки, що виходить за рамки традиційного адміністративного регулювання у сфері державної таємниці.

Третій етап розвитку концепції інформаційної безпеки, що розпочався в кінці 1990-х років, пов'язаний з формуванням глобальної мережі Інтернет та переходом до мережевої парадигми інформаційних процесів [16]. Глобалізація інформаційного простору обумовила необхідність перегляду традиційних підходів до забезпечення інформаційної безпеки, заснованих на принципах територіальної юрисдикції та національного суверенітету. Прийняття Конвенції Ради Європи про кіберзлочинність (Будапештська конвенція) у 2001 році [17] стало першим міжнародно-правовим актом, спрямованим на гармонізацію національних підходів до боротьби з кіберзлочинністю та створення механізмів міжнародного співробітництва у сфері інформаційної безпеки.

Сучасний етап розвитку концепції інформаційної безпеки, що розпочався в першому десятилітті XXI століття, характеризується формуванням парадигми кібербезпеки та переходом до комплексного кіберправового регулювання [18]. Стратегія національної кібербезпеки США 2003 року [19] та аналогічні документи інших держав закріпили нове розуміння інформаційної безпеки як критично важливого елементу національної безпеки в цифрову епоху. Даний підхід передбачає інтеграцію технічних, правових, організаційних та міжнародно-правових механізмів забезпечення безпеки в єдину систему захисту національного кіберпростору.

Якісні зміни в архітектурі сучасного кіберпростору, пов'язані з розвитком хмарних технологій, інтернету речей та систем штучного інтелекту, обумовили формування нових типів загроз інформаційній безпеці та відповідну трансформацію концептуальних підходів до їх нейтралізації [20]. Доктрина інформаційної безпеки України 2017 року [21] та Стратегія кібербезпеки України 2021 року [22] відображають сучасне розуміння інформаційної безпеки як багаторівневої системи захисту інформаційних ресурсів, що включає технічні, правові, організаційні та міжнародно-правові компоненти.

Міжнародно-правовий вимір сучасної концепції інформаційної безпеки отримав розвиток у рамках діяльності спеціалізованих міжнародних організацій та регіональних інтеграційних об'єднань [23]. Резолюції Генеральної Асамблеї ООН про досягнення у сфері інформатизації та телекомунікацій у контексті міжнародної безпеки [24], документи Групи урядових експертів ООН з досягнень у сфері інформатизації та телекомунікацій у контексті міжнародної безпеки [25] та регіональні угоди про співробітництво у сфері інформаційної безпеки формують правову основу для гармонізації національних підходів та розвитку міжнародного співробітництва в даній галузі.

Особливого значення в сучасній концепції інформаційної безпеки набувають питання захисту персональних даних та забезпечення цифрових прав людини [26]. Прийняття Загального регламенту із захисту даних Європейського Союзу (GDPR) у 2018 році [27] та аналогічних нормативних актів в інших юрисдикціях відображає трансформацію підходів до інформаційної безпеки в напрямку посилення захисту прав і свобод людини в цифровому середовищі. Дана тенденція свідчить про формування людиноцентричної парадигми інформаційної безпеки, в якій захист персональних даних та цифрових прав розглядається як невід'ємний елемент загальної системи кібербезпеки.

Розвиток технологій штучного інтелекту та машинного навчання створює нові виклики для традиційних підходів до забезпечення інформаційної безпеки та потребує формування адекватних правових механізмів регулювання [28]. Проекти регулювання штучного інтелекту в Європейському Союзі, США та інших юрисдикціях демонструють спроби створення правової бази для управління ризиками, пов'язаними з використанням ШІ-технологій у критично важливих галузях. Інтеграція систем штучного інтелекту в інфраструктуру інформаційної безпеки відкриває

нові можливості для автоматизації процесів виявлення та нейтралізації кіберзагроз, але одночасно створює додаткові вектори атак та потребує перегляду традиційних підходів до оцінки та управління ризиками.(Таблиця 1)

Таблиця 1

Еволюція концепції інформаційної безпеки: від національної безпеки до кіберправового регулювання

Період	Основні характеристики	Ключові документи/події	Вплив на розвиток інформаційної безпеки
1950–1980 (Холодна війна)	– Акцент на криптографії та захисті державних комунікацій. – Інформаційна безпека як частина військової стратегії.	– Розвиток ARPANET (попередник Інтернету). – Створення DES (Data Encryption Standard, 1977).	Закладення основ сучасного шифрування та захисту даних. Вплив військових технологій на інформаційну безпеку.
1980–1990 (Початок цифрової ери)	– Зростання кіберзлочинності. – Перші кібератаки на корпорації. – Розвиток антивірусних технологій.	– Перший вірус "Brain" (1986). – Прийняття Закону США про комп'ютерні шахрайства (1986).	Перехід від виключно державного захисту до корпоративної та індивідуальної кібербезпеки.
1990–2000 (Глобалізація Інтернету)	– Масове поширення Інтернету. – Зростання фішингу, DDoS-атак. – Поява перших міжнародних стандартів.	– Директива ЄС про захист даних (95/46/ЕС). – Створення PCI DSS (стандарт безпеки платіжних систем).	Формування міжнародних підходів до захисту даних. Початок регулювання кіберзлочинності.
2000–2010 (Ера кібертероризму)	– Атаки 9/11 та їхній вплив на кібербезпеку. – Розвиток соціальних мереж і нових загроз. – Поява концепції "кібервоєн".	– Конвенція Ради Європи про кіберзлочинність (2001). – Стратегія кібербезпеки США (2003).	Включення кібербезпеки до національної безпеки. Початок міжнародного співробітництва.
2010–2020 (Епоха кіберправового регулювання)	– GDPR та інші регламенти захисту даних. – Зростання штучного інтелекту в кібербезпеці. – Криптовалюти та нові виклики.	– GDPR (2016/679). – Директива NIS (2016/1148). – Закон України "Про кібербезпеку" (2017).	Гармонізація національних законодавств із міжнародними стандартами. Акцент на захисті критичної інфраструктури.
2020–дотепер (Сучасні тенденції)	– Розвиток квантових обчислень. – Штучний інтелект у кіберзахисті. – Гібридні війни та кібератаки під час конфліктів.	– Директива ЄС NIS 2 (2022/2555). – Регулювання AI Act (2024). – Кібератаки під час війни в Україні.	Інтеграція AI у кібербезпеку. Зростання значення міжнародної кіберспівпраці.

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

Корпоративний вимір сучасної концепції інформаційної безпеки характеризується формуванням комплексних систем управління інформаційними ризиками та розвитком стандартів корпоративної кібербезпеки [29]. Міжнародні стандарти серії ISO 27000, стандарт NIST Cybersecurity Framework та інші регулятивні документи формують методологічну основу для

побудови корпоративних систем інформаційної безпеки, інтегрованих у загальну систему корпоративного управління. Розвиток концепцій безперервного моніторингу безпеки, управління інцидентами та забезпечення стійкості бізнесу відображає трансформацію корпоративних підходів до інформаційної безпеки від реактивної моделі захисту до проактивної системи управління ризиками.

Технологічна трансформація сучасного кіберпростору, пов'язана з розвитком технологій блокчейн, квантових обчислень та периферійних обчислень (edge computing), формує якісно нові вимоги до систем інформаційної безпеки [30]. Квантові технології створюють як нові можливості для захисту інформації через квантову криптографію, так і загрози для традиційних криптографічних систем у зв'язку з потенційною можливістю використання квантових комп'ютерів для злому існуючих алгоритмів шифрування. Дана дихотомія потребує перегляду довгострокових стратегій забезпечення інформаційної безпеки та розробки нових концептуальних підходів до криптографічного захисту інформації.

Формування концепції кіберправового регулювання як інтегративної системи правових норм, що регулюють відносини в кіберпросторі, являє собою закономірний результат еволюції концепції інформаційної безпеки від вузькоспеціалізованої галузі військово-технічного захисту до комплексної міждисциплінарної системи забезпечення безпеки в цифровому середовищі [31]. Сучасне кіберправове регулювання характеризується конвергенцією норм інформаційного права, міжнародного права, адміністративного права та кримінального права в єдину систему правового регулювання відносин у кіберпросторі. Дана конвергенція відображає об'єктивну потребу в створенні адекватної правової бази для регулювання складних багатосуб'єктних відносин у цифровому середовищі та забезпечення балансу між вимогами безпеки, економічної ефективності та захисту прав людини.

Перспективи подальшого розвитку концепції інформаційної безпеки пов'язані з формуванням глобальної системи кіберправового регулювання, заснованої на принципах міжнародного співробітництва, технологічної нейтральності та захисту фундаментальних прав людини в цифровому середовищі [32]. Розвиток механізмів багатостороннього співробітництва у сфері кібербезпеки, гармонізація національних законодавств та створення ефективних інститутів міжнародного кіберправа являють собою ключові напрямки еволюції сучасної концепції інформаційної безпеки в напрямку формування стійкого та безпечного цифрового середовища для сталого розвитку людської цивілізації.

Висновки. Дослідження еволюції концепції інформаційної безпеки демонструє фундаментальну трансформацію підходів до захисту інформаційних активів та кіберпростору. Первинна парадигма, що базувалася на принципах національної безпеки та державоцентричному підході до захисту критичної інформації, поступово еволюціонувала в комплексну систему багаторівневого регулювання. Ця трансформація обумовлена зростаючою цифровізацією суспільних відносин, появою нових типів загроз та необхідністю забезпечення захисту як державних, так і приватних інтересів у кіберпросторі.

Ключовою тенденцією розвитку концепції інформаційної безпеки є розширення суб'єктного складу та об'єкта захисту. Якщо на початковому етапі основний акцент робився на захисті державних інформаційних ресурсів та критичної інфраструктури, то сучасна парадигма охоплює широкий спектр суб'єктів – від індивідуальних користувачів до транснаціональних корпорацій. Відповідно, об'єкт захисту розширився від класифікованої державної інформації до персональних даних, інтелектуальної власності, комерційних секретів та інформаційної інфраструктури в цілому.

Формування кіберправового регулювання як самостійної галузі юридичної науки та практики представляє якісно новий етап розвитку концепції інформаційної безпеки. Цей процес характеризується створенням спеціалізованих правових механізмів, адаптованих до специфіки кіберпростору, включаючи норми кіберкримінального права, регулювання захисту персональних даних, кібербезпеки критичної інфраструктури та міжнародного співробітництва у сфері боротьби з кіберзлочинністю. Особливого значення набуває гармонізація національних правових систем з міжнародними стандартами та принципами кіберправа.

Перспективи подальшого розвитку концепції інформаційної безпеки пов'язані з необхідністю адаптації до викликів штучного інтелекту, квантових технологій та інших інноваційних рішень, що потребують переосмислення традиційних підходів до забезпечення безпеки кіберпростору. Важливим напрямом є розробка превентивних механізмів захисту, заснованих на принципах "безпеки за дизайном" та проактивного управління ризиками, що дозволить забезпечити стійкість інформаційних систем в умовах постійно змінюваного ландшафту загроз.

Список використаних джерел:

1. Ліпкан В.А. Національна безпека України: навчальний посібник / В.А. Ліпкан. – К.: КНТ, 2019. – 552 с.
2. Золотар О.М. Інформаційна безпека людини, суспільства, держави / О.М. Золотар. – К.: Стилос, 2020. – 446 с.
3. Гуцалюк М.В. Правове забезпечення інформаційної безпеки України / М.В. Гуцалюк. – К.: Центр учбової літератури, 2018. – 368 с.
4. Goldsmith J. Cybersecurity Treaties: A Skeptical View / J. Goldsmith // Future Challenges Essay, Hoover Institution. – 2011. – Vol. 14. – P. 1-15.
5. Rid T. Cyber War Will Not Take Place / T. Rid. – London: Hurst & Company, 2013. – 280 p.
6. Libicki M.C. Cyberdeterrence and Cyberwar / M.C. Libicki. – Santa Monica: RAND Corporation, 2009. – 240 p.
7. Діордіца І.В. Кібербезпека: сутність та методологічні підходи до визначення / І.В. Діордіца // Підприємництво, господарство і право. – 2018. – № 9. – С. 178-184.
8. Бурячок В.Л. Інформаційна та кібербезпека: соціотехнічний аспект / В.Л. Бурячок, В.Б. Толубко, В.О. Хорошко, С.В. Толюпа. – К.: ДУТ, 2019. – 288 с.
9. Мазепа С. Концептуальне осмислення правових основ інформаційної безпеки в контексті глобальних міжнародних тенденцій. Юридичний науковий електронний журнал. 2024. № 9. С. 489-492
10. Баранов О.А. Інформаційне право України: стан, проблеми, перспективи / О.А. Баранов. – К.: КВІЦ, 2019. – 368 с.
11.Бєляков К.І. Інформаційне право України / К.І. Бєляков. – К.: Алерта, 2017. – 340 с.
12. Mentukh, N., & Shevchuk, O. (2023). Protection of information in electronic registers: Comparative and legal aspect. Law, Policy and Security, 1(1), 4-17.
13. Закон України "Про основи національної безпеки України" від 19.06.2003 № 964-IV // Відомості Верховної Ради України. – 2003. – № 39. – Ст. 351.
14. Закон України "Про інформацію" від 02.10.1992 № 2657-XII // Відомості Верховної Ради України. – 1992. – № 48. – Ст. 650.
15. Computer Fraud and Abuse Act of 1986, 18 U.S.C. § 1030 // United States Code. – 1986.
16. Закон України "Про телекомунікації" від 18.11.2003 № 1280-IV // Відомості Верховної Ради України. – 2004. – № 12. – Ст. 155.
17. Convention on Cybercrime (Budapest Convention), Council of Europe Treaty Series № 185. – Budapest, 2001.
18. Закон України "Про основні засади забезпечення кібербезпеки України" від 05.10.2017 № 2163-VIII // Відомості Верховної Ради України. – 2017. – № 45. – Ст. 403.
19. The National Strategy to Secure Cyberspace / The White House. – Washington, 2003. – 76 p.
20. Указ Президента України "Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року "Про Доктрину інформаційної безпеки України"" від 25.02.2017 № 47/2017 // Урядовий кур'єр. – 2017. – № 38.
21. Указ Президента України "Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року "Про Доктрину інформаційної безпеки України"" від 25.02.2017 № 47/2017 // Урядовий кур'єр. – 2017. – № 38.
22. Указ Президента України "Про Стратегію кібербезпеки України" від 26.08.2021 № 447/2021 // Урядовий кур'єр. – 2021. – № 165.
23. Угода про співробітництво держав-учасниць СНД у боротьбі зі злочинами у сфері комп'ютерної інформації (укладена у м. Мінську 01.06.2001) // Бюлетень міжнародних договорів України. – 2007. – № 11. – С. 24-31.
24. Резолюція Генеральної Асамблеї ООН A/RES/73/27 "Досягнення у сфері інформатизації та телекомунікацій у контексті міжнародної безпеки" від 05.12.2018 // UN Doc. A/RES/73/27.
25. Доповідь Групи урядових експертів з досягнень у сфері інформатизації та телекомунікацій у контексті міжнародної безпеки A/70/174 від 22.07.2015 // UN Doc. A/70/174.
26. Закон України "Про захист персональних даних" від 01.06.2010 № 2297-VI // Відомості Верховної Ради України. – 2010. – № 34. – Ст. 481.
27. 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. – 2016. – L 119/1.

Дата першого надходження рукопису до видання: 24.07.2025
Дата прийнятого до друку рукопису після рецензування: 28.08.2025
Дата публікації: 29.09.2025.