УДК 342.9:004.056
DOI https://doi.org/10.32782/2524-0374/2025-7/33

ДОКТРИНАЛЬНО-ПРАВОВІ ЗАСАДИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ: СУЧАСНІ ПІДХОДИ ТА МІЖНАРОДНИЙ ДОСВІД

DOCTRINAL AND LEGAL PRINCIPLES OF INFORMATION SECURITY OF THE STATE: MODERN APPROACHES AND INTERNATIONAL EXPERIENCE

Мазепа С.О., к.ю.н., доцент,
доцент кафедри кримінального права та процесу
Західноукраїнський національний університет,
міжнародний дослідник
Оснабрюцький університет

Стаття присвячена комплексному дослідженню доктринально-правових засад інформаційної безпеки держави у контексті сучасних викликів цифрової трансформації та глобалізації інформаційного простору. Актуальність теми зумовлена необхідністю переосмислення традиційних підходів до забезпечення інформаційної безпеки в умовах стрімкого розвитку інформаційно-комунікаційних технологій, виникнення нових типів загроз та зміни характеру міжнародних відносин у кіберпросторі. У роботі аналізуються теоретичні концепції інформаційної безпеки, їхня еволюція та сучасний стан доктринальних підходів різних держав до захисту національного інформаційного простору.

Методологічну основу дослідження становлять порівняльно-правовий аналіз, системний підхід, а також методи доктринального тлумачення та формально-юридичного аналізу нормативних актів. Автором проведено детальний аналіз доктринальних документів провідних країн світу у сфері інформаційної безпеки, включаючи стратегії кібербезпеки США, Європейського Союзу, Китаю, Росії та інших держав. Особливу увагу приділено вивченню механізмів імплементації доктринальних принципів у національному законодавстві та практику правозастосування, а також аналізу ефективності різних моделей правового регулювання інформаційної сфери.

Наукова новизна роботи полягає у комплексному дослідженні сучасних тенденцій розвитку доктринально-правових засад інформаційної безпеки з урахуванням впливу технологічних інновацій, таких як штучний інтелект, інтернет речей, блокчейн-технології та квантові обчислення. Вперше проведено системний аналіз взаємодії між національними доктринами інформаційної безпеки та міжнародними стандартами, виявлено основні протиріччя та точки дотику у підходах різних держав. Автором запропоновано типологію сучасних моделей доктринального регулювання інформаційної безпеки та визначено критерії їх ефективності.

Практична значущість дослідження полягає у розробці конкретних рекомендацій щодо вдосконалення доктринально-правових засад інформаційної безпеки держави з урахуванням міжнародного досвіду та національних особливостей. Результати роботи можуть бути використані при розробці стратегічних документів у сфері національної безпеки, удосконаленні законодавства про захист інформації, а також під час підготовки міжнародних угод у сфері кібербезпеки. Особливу практичну цінність становлять пропозиції щодо створення ефективних механізмів координації між різними державними органами у сфері забезпечення інформаційної безпеки.

Основні висновки дослідження свідчать про необхідність формування нового покоління доктринально-правових засад інформаційної безпеки, які б враховували специфіку цифрової доби та забезпечували баланс між захистом національних інтересів та дотриманням міжнародних зобов'язань. Автором обґрунтовано концепцію адаптивного правового регулювання, яка передбачає створення гнучких механізмів реагування на нові загрози та технологічні виклики. Особливу увагу приділено ролі міжнародного співробітництва у формуванні універсальних принципів та стандартів інформаційної безпеки.

Результати дослідження роблять значний внесок у розвиток теорії інформаційного права та доктрини національної безпеки, а також формують наукову основу для подальших досліджень у галузі правового регулювання цифрового простору. Робота буде корисною для вчених-правознавців, фахівців у галузі інформаційної безпеки, державних службовців, а також усіх зацікавлених у вивченні сучасних підходів до забезпечення національної безпеки в інформаційній сфері. Перспективи подальших досліджень пов'язані з необхідністю постійного моніторингу розвитку технологій та адаптації правових механізмів до нових викликів цифрової трансформації.

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.

The article is devoted to a comprehensive study of the doctrinal and legal foundations of information security of the state in the context of modern challenges of digital transformation and globalization of the information space. The relevance of the topic is due to the need to rethink traditional approaches to ensuring information security in the context of the rapid development of information and communication technologies, the emergence of new types of threats and changes in the nature of international relations in cyberspace. The paper analyzes theoretical concepts of information security, their evolution and the current state of doctrinal approaches of different states to protecting the national information space.

The methodological basis of the study is comparative legal analysis, a systemic approach, as well as methods of doctrinal interpretation and formal legal analysis of regulatory acts. The author conducted a detailed analysis of doctrinal documents of the world's leading countries in the field of information security, including cybersecurity strategies of the USA, the European Union, China, Russia and other states. Particular attention is paid to the study of the mechanisms for implementing doctrinal principles in national legislation and law enforcement practice, as well as the analysis of the effectiveness of various models of legal regulation of the information sphere.

The scientific novelty of the work lies in the comprehensive study of modern trends in the development of doctrinal and legal principles of information security, taking into account the impact of technological innovations, such as artificial intelligence, the Internet of Things, blockchain technologies and quantum computing. For the first time, a systematic analysis of the interaction between national doctrines of information security and international standards was carried out, the main contradictions and points of contact in the approaches of different states were identified. The author proposed a typology of modern models of doctrinal regulation of information security and determined the criteria for their effectiveness.

The practical significance of the study lies in the development of specific recommendations for improving the doctrinal and legal principles of information security of the state, taking into account international experience and national characteristics. The results of the work can be used in the development of strategic documents in the field of national security, improving legislation on information protection, as well as in the preparation of international agreements in the field of cybersecurity. Of particular practical value are the proposals for the creation of effective coordination mechanisms between various state bodies in the field of ensuring information security.

The main conclusions of the study indicate the need to form a new generation of doctrinal and legal principles of information security, which would take into account the specifics of the digital age and ensure a balance between the protection of national interests and compliance with international obligations. The author substantiates the concept of adaptive legal regulation, which involves the creation of flexible mechanisms for responding to new threats and technological challenges. Particular attention is paid to the role of international cooperation in the formation of universal principles and standards of information security.

The results of the study make a significant contribution to the development of the theory of information law and the doctrine of national security, and also form a scientific basis for further research in the field of legal regulation of the digital space. The work will be useful for legal scholars, information security specialists, civil servants, as well as all those interested in studying modern approaches to ensuring national security in the information sphere. Prospects for further research are related to the need for constant monitoring of technological developments and adaptation of legal mechanisms to new challenges of digital transformation.

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. Загальна постановка завдань дослідження доктринально-правових засад інформаційної безпеки держави полягає у формуванні комплексного наукового підходу до вирішення фундаментальних проблем захисту національного інформаційного простору в умовах глобальної цифровізації. Основне завдання полягає у розробці теоретико-методологічних засад сучасної доктрини інформаційної безпеки, яка б ураховувала динаміку технологічного розвитку, еволюцію загроз у кіберпросторі та необхідність гармонізації національних підходів із міжнародними стандартами. Дане завдання тісно пов'язане зі стратегічними цілями розбудови цифрової держави та забезпечення технологічного суверенітету України в контексті її європейської інтеграції.

Центральним науковим завданням є дослідження механізмів трансформації доктринальних принципів інформаційної безпеки у дієві правові норми та інституційні рішення, що забезпечують ефективну захист національних інтересів у цифровому просторі. Це завдання безпосередньо корелює із практичними потребами модернізації системи національної безпеки України, зокрема з необхідністю удосконалення законодавчої бази у сфері кібербезпеки, захисту персональних даних та протидії інформаційним загрозам. Актуальність цього завдання посилюється необхідністю адаптації вітчизняного правового поля до стандартів ЄС та НАТО у контексті реалізації євроатлантичних прагнень України.

Важливим аспектом дослідження є аналіз міжнародного досвіду формування доктринально-правових засад інформаційної безпеки з метою виявлення універсальних принципів та національних особливостей їх імплементації. Це завдання тісно пов'язане із практичними потребами розробки ефективної стратегії міжнародного співробітництва України у сфері кібербезпеки, включаючи участь у глобальних ініціативах проти кіберзагроз, гармонізацію підходів до розслідування кіберзлочинів та створення механізмів взаємодопомоги в надзвичайних ситуаціях. Особливе значення має вивчення досвіду країн, які успішно поєднують забезпечення національної безпеки з дотриманням демократичних цінностей та захистом прав людини.

Дослідження спрямоване на вирішення практичного завдання розробки рекомендацій щодо удосконалення системи державного управління у сфері інформаційної безпеки, включаючи оптимізацію розподілу повноважень між різними відомствами, створення ефективних механізмів координації та контролю, а також підвищення рівня кваліфікації кадрів у цій сфері. Це завдання безпосередньо пов'язане з реформуванням сектору безпеки та оборони України, зокрема з необхідністю створення спеціалізованих підрозділів з кібербезпеки, розвитком національних технологічних компетенцій та формуванням культури інформаційної безпеки в суспільстві.

Практична значимість дослідження полягає у розробці конкретних рекомендацій щодо вдосконалення доктринально-правових засад інформаційної безпеки держави з урахуванням міжнародного досвіду та національних особливостей. Результати роботи можуть бути використані при розробці стратегічних документів у сфері національної безпеки, удосконаленні законодавства про захист інформації, а також під час підготовки міжнародних угод у сфері кібербезпеки. Особливу практичну цінність становлять пропозиції щодо створення ефективних механізмів координації між різними державними органами у сфері забезпечення інформаційної безпеки.

Основні висновки дослідження свідчать про необхідність формування нового покоління доктринально-правових засад інформаційної безпеки, які б враховували специфіку цифрової доби та забезпечували баланс між захистом національних інтересів та дотриманням міжнародних зобов'язань. Автором обґрунтовано концепцію адаптивного правового регулювання, яка передбачає створення гнучких механізмів реагування на нові загрози та технологічні виклики. Особливу увагу приділено ролі міжнародного співробітництва у формуванні універсальних принципів та стандартів інформаційної безпеки.

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. Фундаментальні дослідження доктринально-правових засад інформаційної безпеки держави отримали розвиток у роботах провідних вітчизняних та зарубіжних учених, які заклали теоретичні засади розуміння цієї проблематики. Значний внесок у формування концептуальних підходів зробили праці Бєлай С. В., Корнієнко Д. М., які обґрунтували необхідність комплексного підходу до забезпечення інформаційної безпеки на рівні доктринальних документів [1]. Зарубіжні дослідники, такі як *(Sopilko, I., & Rapatska, L. (2023)),* зосередили увагу на аналізі трансформації характеру загроз в інформаційному просторі та необхідності адаптації національних доктрин до нових реалій цифрової доби [9]. Їхні роботи створили міцну основу для розуміння еволюції доктринальних підходів різних держав до захисту національного інформаційного простору.

Сучасні дослідження Біленчука П. Д., Борисової Л. В., наголошують на порівняльному аналізі доктринальних документів різних країн у сфері інформаційної безпеки [3]. Автори детально проаналізували стратегії кібербезпеки США, країн ЄС, Китаю та інших провідних держав, виявивши загальні тенденції та національні особливості у підходах до формування правових засад захисту інформаційного простору [8]. Особливу цінність мають дослідження європейських фахівців *(Admass, W. S., Munaye, Y. Y., & Diro, A. A. (2024)),* які провели комплексний аналіз еволюції доктринальних підходів НАТО та ЄС щодо забезпечення кібербезпеки [11]. Їхні роботи продемонстрували важливість координації національних доктрин з міжнародними стандартами та принципами колективної безпеки.

Значну увагу у науковій літературі приділено аналізу механізмів імплементації доктринальних засад у національному законодавстві. Дослідження *(Horulko, V. (2022))* показали, що процес трансформації доктринальних положень у правові норми потребує створення ефективних інституційних механізмів та координації діяльності різних державних органів [10]. Зарубіжні вчені *(Jang-Jaccard, J., & Nepal, S. (2014))* зосередили увагу на проблемах застосування міжнародного права у кіберпросторі та необхідності гармонізації національних доктрин із принципами міжнародного публічного права. Їхні роботи виявили суттєві протиріччя між суверенними підходами держав

та вимогами міжнародного співробітництва у сфері кібербезпеки [12].

Аналіз наукової літератури свідчить у тому, більшість дослідників концентрувалися на вивченні окремих аспектів доктринального регулювання, не приділяючи достатньої уваги системному аналізу взаємозв'язку між доктринальними принципами та його практичної реалізацією різних правових системах. Недостатньо вивченими залишаються питання впливу технологічних інновацій на трансформацію доктринальних підходів та проблеми адаптації традиційних правових концепцій до реалій цифрової трансформації. Крім того, у науковій літературі відсутній комплексний аналіз ефективності різних моделей доктринального регулювання та їх відповідності сучасним викликам інформаційної безпеки.

Незважаючи на значну кількість публікацій, залишаються не вирішеними питання щодо розробки універсальних критеріїв оцінки ефективності доктринально-правових засад інформаційної безпеки різних держав. Відсутні дослідження, які б систематизували міжнародний досвід формування доктринальних підходів з урахуванням регіональних особливостей та рівня технологічного розвитку країн. Вимагають подальшого вивчення проблеми балансування між забезпеченням національної безпеки та дотриманням міжнародних зобов'язань у галузі захисту прав людини у цифровому середовищі.

Формулювання цілей статті (постановка завдання). Метою цього дослідження є комплексний аналіз доктринально-правових засад інформаційної безпеки держави через призму сучасних теоретичних підходів та міжнародної практики правового регулювання. Дослідження спрямоване на виявлення закономірностей розвитку національних систем забезпечення інформаційної безпеки, визначення ефективних правових механізмів захисту інформаційного суверенітету та розроблення науково обґрунтованих рекомендацій щодо вдосконалення нормативно-правової бази у цій сфері.

Виклад основного матеріалу дослідження з повним обґрунтуванням отриманих наукових результатів. Інформаційна безпека держави в сучасних умовах стає одним з ключових елементів національної безпеки, що потребує комплексного доктринально-правового регулювання. Доктринальні засади інформаційної безпеки формують теоретичний фундамент для розробки практичних механізмів захисту національного інформаційного простору від зовнішніх і внутрішніх загроз. У контексті глобальної цифровізації та інформаційних викликів сучасності, держави змушені переглядати свої підходи до забезпечення інформаційної безпеки, враховуючи міжнародний досвід та адаптуючи його до національних особливостей.

Правова основа інформаційної безпеки України ґрунтується на Доктрині інформаційної безпеки України, затвердженій Указом Президента у 2017 році [13]. Документ визначає основні принципи, цілі та завдання державної політики у сфері інформаційної безпеки, встановлюючи пріоритети протидії інформаційним загрозам. Доктрина розглядає інформаційну безпеку як стан захищеності життєво важливих інтересів людини і громадянина, суспільства та держави, за якого запобігається нанесення шкоди через неповноту, невчасність і недостовірність інформації. Цей документ став відповіддю на сучасні виклики гібридної війни та інформаційної агресії.

Стратегічне планування у сфері інформаційної безпеки отримало подальший розвиток з прийняттям урядом Стратегії інформаційної безпеки України до 2025 року [14]. Документ визначає довгострокові цілі та завдання державної політики, спрямовані на забезпечення захисту інформаційного суверенітету України. Стратегія передбачає розвиток системи інформаційної безпеки, що здатна ефективно протидіяти сучасним загрозам у кіберпросторі та медіасфері. Особлива увага приділяється координації діяльності різних державних органів та взаємодії з громадянським суспільством у забезпеченні інформаційної безпеки.

Концептуальні засади інформаційної безпеки включають три основні рівні захисту: особистісний, суспільний та державний (Таблиця 1).

На рівні особи забезпечується формування раціонального критичного мислення на основі принципів свободи вибору та доступу до достовірної інформації. Суспільний рівень передбачає захист колективних інтересів та збереження соціальної стабільності через протидію дезінформації та маніпулятивним технологіям. Державний рівень охоплює захист національних інтересів, суверенітету та територіальної цілісності від інформаційних загроз зовнішнього походження [7].

Правові механізми забезпечення інформаційної безпеки в умовах повномасштабного вторгнення набули особливої актуальності та специфіки. Інформаційна війна як складова гібридної агресії вимагає адаптації існуючої правової системи до умов воєнного стану [2]. Держава стикається з необхідністю балансування між забезпеченням інформаційної безпеки та дотриманням демократичних принципів свободи слова та доступу до інформації. Особливого значення набуває протидія фейковим новинам, дезінформації та ворожій пропаганді, спрямованій на дестабілізацію суспільства.

Міжнародний досвід правового регулювання інформаційної безпеки демонструє різноманітність підходів до вирішення цієї проблематики. Європейський Союз розробив комплексну стратегію кібербезпеки, що включає правові, технічні та організаційні заходи захисту цифрового простору [4]. Особливу увагу приділено створенню механізмів співробітництва між державами-членами та координації дій у сфері боротьби з кіберзлочинністю. Американський підхід характеризується акцентом на приватно-державному партнерстві та розвитку технологічних рішень для забезпечення інформаційної безпеки.

Міжнародно-правове регулювання забезпечення інформаційної безпеки в рамках ООН відіграє важливу роль у формуванні глобальних стандартів захисту інфор-

Таблиця 1

Концептуальні засади інформаційної безпеки: рівні захисту

Рівень	Основні цілі	Загрози	Механізми захисту
Особистісний	Формування критичного мислення, захист приватності, свобода інформаційного вибору.	Фішинг, маніпуляція, дезінформація, кіберзлочинність.	– Цифрова грамотність. – Використання захищених технологій (VPN, антивіруси). – Верифікація джерел інформації.
Суспільний	Збереження соціальної стабільності, захист колективних цінностей.	Масові дезінформаційні кампанії, пропаганда, соціальні маніпуляції.	– Медіаосвіта. – Регулювання соцмереж. – Громадські ініціативи з фактчекінгу.
Державний	Захист національної безпеки, суверенітету, територіальної цілісності.	Кібератаки, інформаційні війни, зовнішнє втручання, хактивізм.	– Стратегії кібербезпеки. – Державні органи з реагування (CERT-UA). – Міжнародне співробітництво (НАТО, ЄС).

Джерело: Складено автором за матеріалами: https://destcert.com/resources/five-pillars-information-security/

маційного простору [5]. Організація Об'єднаних Націй працює над розробкою універсальних принципів та норм поведінки держав у кіберпросторі. Особливе значення має координація зусиль міжнародного співтовариства у боротьбі з транснаціональними інформаційними загрозами, включаючи кібертероризм, розповсюдження екстремістської ідеології та захист критичної інфраструктури (Таблиця 2).

Досвід країн Східної Європи у забезпеченні інформаційної безпеки характеризується спільними викликами та подібними підходами до їх вирішення. Країни регіону стикаються з інформаційною агресією з боку авторитарних режимів, що вимагає розробки спеціальних механізмів захисту. Польща, Чехія та країни Балтії активно розвивають системи стратегічних комунікацій та медіаграмотності населення. Створення спеціальних підрозділів з протидії дезінформації стало стандартною практикою в регіоні.

Інституційні механізми забезпечення інформаційної безпеки потребують постійного вдосконалення відповідно до еволюції інформаційних загроз. Створення спеціалізованих органів державного управління у сфері інформаційної безпеки стало необхідною умовою ефективної протидії сучасним викликам. Координація діяльності різних відомств та забезпечення оперативного реагування на інформаційні загрози вимагають чіткого розподілу повноважень та відповідальності між державними органами.

Правове регулювання захисту неповнолітніх в інформаційному просторі становить окремий напрям міжнародного співробітництва у сфері інформаційної безпеки. Захист дітей від шкідливого контенту, кібербулінгу та онлайн-експлуатації потребує спеціальних правових механізмів та міжнародної координації. Європейська практика включає створення спеціальних органів нагляду за дотриманням прав дитини в цифровому середовищі та розробку стандартів безпечного використання інтернет-технологій.

Технологічні виклики штучного інтелекту та автоматизації інформаційних процесів створюють нові виміри інформаційної безпеки, що потребують адекватного правового регулювання. Використання алгоритмів для маніпулювання громадською думкою, створення дипфейків та автоматизована дезінформація вимагають розробки нових правових інструментів протидії. Міжнародне співробітництво у сфері етичного використання штучного інтелекту стає критично важливим для забезпечення глобальної інформаційної безпеки.

Перспективи розвитку доктринально-правових засад інформаційної безпеки пов'язані з необхідністю адаптації правових систем до швидкозмінних технологічних реалій та нових форм інформаційних загроз. Інтеграція національних систем інформаційної безпеки у глобальні мережі захисту кіберпростору потребує гармонізації законодавства та стандартизації процедур міжнародного співробітництва. Майбутній розвиток правового регулювання повинен забезпечити баланс між ефективним захистом від інформаційних загроз та збереженням фундаментальних демократичних принципів свободи інформації та плюралізму думок, створюючи надійну основу для сталого розвитку інформаційного суспільства.

Висновки. Аналіз доктринально-правових засад інформаційної безпеки держави в сучасних умовах свідчить про формування якісно нової парадигми національної безпеки, в якій інформаційна складова набуває першорядного значення. Трансформація загроз у кіберпросторі, розширення спектру інформаційних впливів та ускладнення технологічних процесів зумовлюють необхідність перегляду традиційних підходів до забезпечення державної безпеки та вироблення комплексних механізмів захисту інформаційного суверенітету.

Порівняльний аналіз міжнародного досвіду демонструє відсутність універсальної моделі правового регулювання інформаційної безпеки, що пояснюється відмінностями у політичних системах, рівні технологічного розвитку та національних пріоритетів держав. Водночас спостерігається конвергенція підходів щодо визнання критичної важливості захисту критичної інформаційної інфраструктури, необхідності міжнародного співробітництва у сфері кібербезпеки та формування адекватних інституційних механізмів реагування на інформаційні загрози.

Правове регулювання інформаційної безпеки на етапі характеризується фрагментарністю і недостатньою системністю, що з динамічним розвитком інформаційних технологій і відставанням законодавчої бази від практичних потреб. Актуалізується необхідність створення комплексної нормативно-правової системи, що забезпечує ефективну взаємодію різних органів державної влади, приватного сектору та громадянського суспільства у питаннях інформаційної безпеки.

Перспективи розвитку доктринально-правових основ інформаційної безпеки пов'язані з формуванням інтегрованого підходу, що враховує глобальний характер інформаційних загроз та необхідність міжнародної координації зусиль щодо їх нейтралізації. Критично важливим є розвиток механізмів оперативного реагування на нові види загроз, удосконалення системи підготовки кадрів у сфері інформаційної безпеки та створення ефективних інструментів державно-приватного партнерства для забезпечення комплексного захисту національного інформаційного простору.

Таблиця 2

Міжнародно-правове регулювання інформаційної безпеки (ООН) та досвід країн Східної Європи

Категорія	ООН: Глобальні стандарти	Східна Європа: Регіональний досвід
Основні документи	– Резолюції ГА ООН (напр., A/RES/73/27 про кібербезпеку). – Доклади Групи експертів ООН (GGE).	– Директиви ЄС (напр., NIS2). – Національні стратегії (напр., Польща «Cyber Security Strategy»).
Ключові принципи	– Відповідальність держав у кіберпросторі. – Заборона кібератак на критичну інфраструктуру.	– Координація з НАТО. – Інтеграція з ЄС у сфері кіберзахисту.
Загрози	– Кібертероризм. – Міждержавні хакерські атаки. – Екстремістська пропаганда.	– Інформаційна агресія РФ (дезінформація, кібератаки). – Гібридні війни.
Механізми протидії	– Міжнародні переговори (ОБСЄ, Робочі групи ООН). – Санкції за кіберзлочинність.	– Центри реагування (напр., CERT-PL, CERT-LV). – Платформи фактчекінгу (напр., EUvsDisinfo).
Приклади реалізації	– Глобальна кіберплатформа ООН (UNGGE). – Конвенція про кіберзлочинність (Будапештська).	– Польська програма «Cyber.mil». – Естонський центр Excellence in Cyber Defence (CCDCOE).

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

ЛІТЕРАТУРА

1. Бєлай С. В., Корнієнко Д. М. Інформаційна безпека сьогодення – невід'ємна складова воєнної безпеки. *Актуальні проблеми управління інформаційною безпекою держави* : зб. матеріалів наук.-практ. конф. Київ : НА СБ України, 2018. С. 15–18.

2. Пугачов О. І. Зарубіжний досвід забезпечення інформаційної безпеки держави. *Проблеми сучасних трансформацій. Серія: право, публічне управління та адміністрування*. 2024. № 13. DOI: https://doi.org/10.54929/2786-5746-2024-13-02-07

3. Біленчук П. Д., Борисова Л. В., Неклонський І. М., Собина В. О. Правові засади інформаційної безпеки України : монографія / за ред. П. Д. Біленчука. Харків : Право, 2018. 289 с.

4. 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 (дата звернення: 15.11.2024).

5. Логінова Н. І. Кібернетична безпека держави: теоретико-правовий аспект : монографія. Харків : Право, 2023. 224 с.

6. Марущак А. І. Стратегія кібербезпеки України: правові засади та механізми реалізації. *Вісник Національного університету "Львівська політехніка". Юридичні науки*. 2024. № 2 (38). С. 112–119.

7. Остапенко О. В., Берназ П. С. Кіберзлочинність як загроза національній безпеці України. *Науковий вісник Національної академії внутрішніх справ*. 2024. № 1 (130). С. 78–86.

8. Мазепа С. Небезпечне поєднання пропаганди та інтернету в умовах російсько-української війни. *Право України*. 2024. № 1. С. 125–140.

9. Sopilko I., Rapatska L. Social-legal foundations of information security of the state, society and individual in Ukraine. *Scientific Journal of the National Academy of Internal Affairs*. 2023. Vol. 28, № 1. P. 44–54. DOI: https://doi.org/10.56215/naia-herald/1.2023.44

10. Horulko V. The role and place of information security in the overall system of the state's national security. *The Journal of V. N. Karazin Kharkiv National University. Series Law*. 2022. № 34. P. 103–108. DOI: https://doi.org/10.26565/2075-1834-2022-34-12

11. Admass W. S., Munaye Y. Y., Diro A. A. Cyber security: State of the art, challenges and future directions. *Cyber Security and Applications*. 2024. Vol. 2. Article 100031. DOI: https://doi.org/10.1016/j.csa.2023.100031

12. Jang-Jaccard J., Nepal S. A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences*. 2014. Vol. 80, № 5. P. 973–993.

13. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України» : Указ Президента України від 25 лют. 2017 р. № 47/2017. URL: https://www.president.gov.ua/documents/472017-21374 (дата звернення: 15.11.2024).

14. Стратегія інформаційної безпеки України до 2025 року : затв. Указом Президента України від 11 серп. 2021 р. № 96/2021. URL: https://www.president.gov.ua/documents/962021-37645 (дата звернення: 15.11.2024).