https://doi.org/10.31891/2307-5740-2026-356-25
УДК 351.86
JEL classification H11, H12, O38, L86

ДРИГА Дмитро
Відкритого міжнародного університету розвитку людини «Україна»,
https://orcid.org/0000-0003-4426-7551
e-mail: dimadriga6@gmail.com

ЄВРОПЕЙСЬКІ ПІДХОДИ ДО ДЕРЖАВНОГО РЕГУЛЮВАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ: СУЧАСНІ МЕХАНІЗМИ ТА ПЕРСПЕКТИВИ ІМПЛЕМЕНТАЦІЇ В УКРАЇНІ

У статті досліджено сучасні європейські підходи до державного регулювання інформаційної безпеки в умовах цифрової трансформації, розвитку інформаційного суспільства та посилення інформаційних і кібернетичних загроз. Запропоновано практичні напрями імплементації європейського досвіду, серед яких: запровадження ризик-орієнтованого управління інформаційною безпекою, удосконалення механізмів захисту критичної інформаційної інфраструктури, розвиток інтегрованої системи міжвідомчої взаємодії, створення національної системи сертифікації цифрових продуктів і сервісів, регулярне тестування цифрової стійкості державних інформаційних систем, використання технологій штучного інтелекту для моніторингу інформаційного простору та виявлення інформаційних загроз, а також розвиток цифрових компетентностей фахівців органів публічної влади. Доведено, що імплементація сучасних європейських механізмів державного регулювання інформаційної безпеки сприятиме підвищенню ефективності управління інформаційними ризиками, зміцненню інституційної спроможності органів державної влади, розвитку цифрової стійкості, удосконаленню міжвідомчої координації та гармонізації національного законодавства з правом Європейського Союзу.

Ключові слова: державне регулювання, інформаційна безпека, механізми, глобалізація, цифровізація, інформаційні загрози, інформаційна інфраструктура.

DRYHA Dmytro
Open International University of Human Development "Ukraine"

EUROPEAN APPROACHES TO GOVERNMENT REGULATION OF INFORMATION SECURITY: CURRENT MECHANISMS AND PROSPECTS FOR IMPLEMENTATION IN UKRAINE

This article examines contemporary European approaches to government regulation of information security in the context of digital transformation, the development of the information society, and the escalation of information and cyber threats. It analyzes the European Union's key regulatory and institutional mechanisms for ensuring information security. Particular attention is paid to the provisions of the NIS2 Directive, the DORA Regulation, the General Data Protection Regulation (GDPR), the Cybersecurity Act, as well as the activities of the CSIRTs Network, EU-CyCLONe, and the Digital Europe Program. Their role in shaping the modern European model of state regulation of information security is identified; this model is based on the principles of preventive management of information risks, interagency coordination, harmonization of regulatory frameworks, development of digital resilience, and standardization of mechanisms for protecting information resources. This paper summarizes the main mechanisms of state regulation of information security applied in the European Union and identifies opportunities for adapting them to the Ukrainian system of public administration. Practical approaches to implementing European best practices are proposed, including: the introduction of risk-based information security management, the improvement of mechanisms for protecting critical information infrastructure, developing an integrated system of interagency cooperation, establishing a national certification system for digital products and services, regularly testing the digital resilience of government information systems, using artificial intelligence technologies to monitor the information space and detect information threats, and developing the digital competencies of public sector professionals. It has been demonstrated that the implementation of modern European mechanisms for state regulation of information security will contribute to improving the effectiveness of information risk management, strengthening the institutional capacity of government agencies, developing digital resilience, enhancing interagency coordination, and harmonizing national legislation with European Union law. The practical significance of this study lies in the potential to apply its findings in the formulation and implementation of state policy in the field of information security, the improvement of the regulatory framework, the modernization of the system of state regulation of information security, and the development of strategic documents aimed at strengthening Ukraine's information and cyber resilience in the context of digital transformation and European integration.

Keywords: state regulation, information security, mechanisms, globalization, digitalization, information threats, information infrastructure.

Стаття надійшла до редакції / Received 22.07.2026
Прийнята до друку / Accepted 10.08.2026
Опубліковано / Published 27.08.2026

ПОСТАНОВКА ПРОБЛЕМИ У ЗАГАЛЬНОМУ ВИГЛЯДІ ТА ЇЇ ЗВ'ЯЗОК ІЗ ВАЖЛИВИМИ НАУКОВИМИ ЧИ ПРАКТИЧНИМИ ЗАВДАННЯМИ

В умовах стрімкої цифрової трансформації суспільства, зростання масштабів кіберзагроз, інформаційних операцій та гібридних форм впливу забезпечення інформаційної безпеки набуває статусу

одного з ключових напрямів державної політики. Для України, яка одночасно протистоїть повномасштабній військовій агресії та реалізує курс на європейську інтеграцію, особливого значення набуває модернізація системи державного регулювання інформаційної безпеки відповідно до сучасних стандартів Європейського Союзу. Європейська модель базується на ризик-орієнтованому управлінні, розвитку цифрової стійкості, захисті критичної інформаційної інфраструктури, міжвідомчій координації та гармонізації нормативно-правового забезпечення. Водночас в Україні триває процес адаптації національного законодавства до права ЄС, що зумовлює необхідність комплексного аналізу європейських механізмів державного регулювання інформаційної безпеки, визначення можливостей їх імплементації та формування практичних напрямів удосконалення національної системи захисту інформаційного простору.

АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ

Дослідження проблем державного регулювання інформаційної безпеки, розвитку інформаційного суспільства, цифрової трансформації публічного управління та забезпечення інформаційної й кібернетичної стійкості держави знайшли широке відображення у працях вітчизняних науковців. Вагомий внесок у розвиток теоретико-методологічних і прикладних засад державного регулювання інформаційної безпеки здійснили Р. В. Бондаренко [1], О. А. Баранов [2], С. Є. Антонова [3], В. Т. Шатун [4], Д. А. Селіхов [5] та ін. У працях сучасних авторів розглянуто питання формування державної інформаційної політики, удосконалення механізмів державного управління у сфері інформаційної безпеки, розвитку цифрового врядування, нормативно-правового забезпечення інформаційних відносин, захисту інформаційних ресурсів, протидії сучасним інформаційним загрозам, а також впровадження цифрових технологій у діяльність органів публічної влади.

Незважаючи на вагомий науковий доробок, недостатньо дослідженими залишаються питання комплексної імплементації європейських нормативно-правових та інституційних механізмів державного регулювання інформаційної безпеки в Україні, адаптації ризик-орієнтованої моделі управління інформаційними ризиками, а також використання сучасних цифрових технологій і технологій штучного інтелекту для моніторингу інформаційного простору та своєчасного реагування на інформаційні й кібернетичні загрози.

ВИДІЛЕННЯ НЕВИРІШЕНИХ РАНІШЕ ЧАСТИН ЗАГАЛЬНОЇ ПРОБЛЕМИ, КОТРИМ ПРИСВЯЧУЄТЬСЯ СТАТТЯ

Незважаючи на вагомий науковий доробок у сфері державного регулювання інформаційної безпеки, недостатньо дослідженими залишаються питання комплексної імплементації європейських нормативно-правових та інституційних механізмів в Україні. Потребують подальшого вивчення практичні аспекти адаптації ризик-орієнтованої моделі управління інформаційними ризиками. Окремої уваги вимагає використання сучасних цифрових технологій і технологій штучного інтелекту для моніторингу інформаційного простору та своєчасного реагування на інформаційні й кібернетичні загрози.

ФОРМУЛЮВАННЯ ЦІЛЕЙ СТАТТІ

Метою статті є дослідження сучасних європейських підходів до державного регулювання інформаційної безпеки, аналіз нормативно-правових та інституційних механізмів забезпечення цифрової стійкості в Європейському Союзі, а також визначення перспектив їх імплементації в систему державного регулювання інформаційної безпеки України в контексті євроінтеграційних процесів та сучасних інформаційних і кібернетичних загроз.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

У сучасних умовах цифрової трансформації суспільства інформаційна безпека перетворилася на один із ключових елементів забезпечення національної безпеки, сталого функціонування державних інституцій та захисту критичної інформаційної інфраструктури. Глобальна цифровізація, активне впровадження інформаційно-комунікаційних технологій, розвиток штучного інтелекту, хмарних сервісів і платформ цифрової взаємодії суттєво розширюють можливості соціально-економічного розвитку, водночас формуючи нові інформаційні ризики та кібернетичні загрози. Особливої актуальності зазначені виклики набувають в умовах зростання масштабів гібридних конфліктів, коли інформаційний простір стає одним із головних об'єктів деструктивного впливу, а інформаційні та кібероперації використовуються як інструменти досягнення політичних, військових і економічних цілей. За таких умов ефективність державного регулювання інформаційної безпеки визначається не лише спроможністю реагувати на інциденти, а й здатністю формувати комплексну систему превентивного управління інформаційними ризиками та забезпечення цифрової стійкості. Для України, яка реалізує євроінтеграційний курс та здійснює адаптацію національного законодавства до права Європейського Союзу, вивчення й імплементація таких підходів набувають особливої актуальності. Саме тому доцільним є аналіз сучасних європейських механізмів державного регулювання інформаційної безпеки, їх нормативно-правового та інституційного забезпечення, а також визначення перспектив використання цього досвіду в процесі модернізації національної системи забезпечення інформаційної безпеки [6].

Особливу увагу в даному контексті доцільно приділити європейським підходам до забезпечення інформаційної безпеки, які формуються в контексті цифрової трансформації, розвитку цифрового єдиного ринку та посилення стійкості держав-членів Європейського Союзу до інформаційних і кібернетичних загроз. На відміну від традиційних моделей, орієнтованих переважно на реагування на інциденти, сучасна європейська модель базується на превентивному управлінні ризиками, міжвідомчій координації, гармонізації нормативно-правового забезпечення та розвитку цифрової стійкості критичної інформаційної інфраструктури.

Одним із ключових елементів цієї моделі є Директива NIS2 (Directive (EU) 2022/2555), яка суттєво розширила вимоги до забезпечення кібер- та інформаційної безпеки організацій, що функціонують у критично важливих секторах економіки та державного управління. На відміну від попередньої редакції, NIS2 передбачає ризик-орієнтований підхід до управління інформаційною безпекою, запровадження обов'язкових заходів управління кіберризиками, регулярне оцінювання вразливостей, оперативне повідомлення про інциденти, посилення відповідальності керівництва організацій та координацію діяльності національних компетентних органів держав-членів. Практична реалізація положень NIS2 сприяє підвищенню рівня стійкості цифрової інфраструктури та уніфікації механізмів реагування на транскордонні інформаційні загрози. [7].

Важливе значення для забезпечення інформаційної безпеки фінансового сектору має Регламент DORA (Digital Operational Resilience Act), який встановлює єдині вимоги до цифрової операційної стійкості банків, страхових компаній, фінансових установ і постачальників ІКТ-послуг. Регламент передбачає комплексне управління інформаційними та кіберризиками, проведення регулярного тестування цифрової стійкості, контроль діяльності постачальників цифрових сервісів, створення ефективної системи управління інцидентами та безперервний моніторинг інформаційних ризиків. Таким чином, DORA формує єдині стандарти забезпечення безпеки цифрових фінансових екосистем Європейського Союзу [8].

Не менш важливим елементом європейської політики є Загальний регламент про захист даних (GDPR), який визначає сучасні принципи управління персональними даними, встановлює вимоги до їх законної обробки, забезпечує права громадян на захист інформації та покладає на організації обов'язок упроваджувати технічні й організаційні заходи із захисту інформаційних ресурсів. Практика застосування GDPR демонструє, що належний рівень інформаційної безпеки безпосередньо пов'язаний із прозорістю державного управління, цифровою довірою громадян і відповідальністю суб'єктів, які здійснюють обробку інформації [9].

Вагому роль у формуванні сучасної європейської системи інформаційної безпеки відіграє Cybersecurity Act, який посилив повноваження Європейського агентства з кібербезпеки (ENISA) та запровадив європейську систему сертифікації засобів інформаційно-комунікаційних технологій. Завдяки цьому держави-члени отримали уніфіковані підходи до оцінювання рівня безпеки цифрових продуктів, програмного забезпечення, хмарних сервісів і технологічних рішень, що сприяє підвищенню довіри до цифрового середовища та мінімізації потенційних кіберризиків [10].

Поряд із нормативно-правовими механізмами Європейський Союз активно розвиває інституційне співробітництво у сфері інформаційної безпеки. Зокрема, функціонують мережі CSIRTs Network, EU-CyCLONe, діяльність яких спрямована на координацію реагування на масштабні кіберінциденти, обмін інформацією про загрози, проведення спільних навчань і формування механізмів оперативної взаємодії між державами-членами. Додатковим інструментом забезпечення цифрової безпеки є реалізація програм Digital Europe Programme, які передбачають розвиток цифрових компетентностей, підтримку центрів кібербезпеки, упровадження технологій штучного інтелекту та зміцнення цифрової інфраструктури Європейського Союзу [11].

Для України європейський досвід має особливу практичну цінність у контексті виконання євроінтеграційних зобов'язань та наближення національного законодавства до права Європейського Союзу. З метою систематизації основних складових сучасної європейської моделі державного регулювання інформаційної безпеки доцільно узагальнити ключові нормативно-правові та інституційні механізми, які формують єдину систему забезпечення цифрової стійкості держав-членів Європейського Союзу. Такий підхід дозволяє визначити функціональне призначення кожного механізму, оцінити його внесок у формування сучасної системи управління інформаційною безпекою та окреслити напрями адаптації європейського досвіду до національної системи державного регулювання.

Проведений аналіз свідчить, що сучасна європейська модель державного регулювання інформаційної безпеки характеризується комплексністю, системністю та превентивною спрямованістю. На відміну від традиційних підходів, які орієнтувалися переважно на реагування на інформаційні інциденти, сучасна практика Європейського Союзу ґрунтується на інтеграції нормативно-правових, організаційних, технологічних та інституційних механізмів, що забезпечують безперервне управління інформаційними ризиками та розвиток цифрової стійкості. Для України така модель становить не лише приклад успішної реалізації державної політики у сфері інформаційної безпеки, а й практичний орієнтир для подальшого вдосконалення національного законодавства, розвитку інституційної взаємодії, модернізації механізмів захисту критичної інформаційної інфраструктури та формування сучасної системи державного регулювання

інформаційної безпеки відповідно до європейських стандартів. Саме тому адаптація зазначених механізмів має розглядатися як один із пріоритетних напрямів зміцнення інформаційної стійкості України в умовах сучасних інформаційних і кібернетичних загроз.

Таблиця 1

Ключові механізми державного регулювання інформаційної безпеки в Європейському Союзі та можливості їх імплементації в Україні

Європейський механізм	Основний зміст	Практичне значення для України
NIS2 (Directive (EU) 2022/2555)	Ризик-орієнтоване управління інформаційною та кібербезпекою, захист критичної інфраструктури, управління інцидентами, відповідальність керівництва	Запровадження комплексної системи управління інформаційними ризиками, удосконалення механізмів захисту критичної інформаційної інфраструктури, розвиток міжвідомчої координації
DORA (Digital Operational Resilience Act)	Забезпечення цифрової операційної стійкості фінансового сектору, тестування стійкості, моніторинг ІКТ-ризиків	Посилення безпеки цифрових фінансових сервісів, створення єдиної системи управління цифровими ризиками у фінансовій сфері
GDPR	Захист персональних даних, принципи законної обробки інформації, забезпечення прав громадян	Гармонізація законодавства щодо захисту персональних даних, підвищення цифрової довіри, удосконалення механізмів інформаційної безпеки органів влади
Cybersecurity Act	Сертифікація ІКТ-продуктів, посилення ролі ENISA, уніфікація вимог до безпеки цифрових технологій	Запровадження національної системи сертифікації цифрових рішень, підвищення рівня захисту інформаційно-комунікаційних технологій
CSIRTs Network та EU-CyCLONe	Координація реагування на масштабні кіберінциденти, обмін інформацією, спільні навчання	Формування ефективної системи міжвідомчого інформаційного обміну та координації реагування на інформаційні й кібернетичні загрози
Digital Europe Programme	Розвиток цифрових компетентностей, підтримка кібербезпеки, штучного інтелекту та цифрової інфраструктури	Підвищення цифрової спроможності державних органів, розвиток кадрового потенціалу та впровадження інноваційних цифрових технологій у сферу інформаційної безпеки

Джерело: сформовано автором на основі даних [12]

Водночас адаптація європейських підходів не повинна обмежуватися формальним приведенням національного законодавства у відповідність до вимог Європейського Союзу. Вона має передбачати комплексне впровадження сучасних управлінських практик, спрямованих на підвищення стійкості інформаційного простору, удосконалення механізмів державного регулювання та розвиток інституційної спроможності органів публічної влади. Особливо актуальними для України є практики, що вже довели свою ефективність у країнах ЄС та можуть бути інтегровані з урахуванням сучасних безпекових викликів і процесів цифрової трансформації (табл. 2).

Таблиця 2

Перспективні європейські практики державного регулювання інформаційної безпеки для впровадження в Україні

Практика	Зміст	Очікуваний результат для України
Ризик-орієнтоване управління інформаційною безпекою	Постійна ідентифікація, оцінювання та моніторинг інформаційних і кіберризиків відповідно до вимог NIS2	Перехід від реагування на інциденти до їх прогнозування та попередження
Єдина система координації реагування	Створення інтегрованої платформи взаємодії між державними органами, секторальними CSIRT та операторами критичної інфраструктури	Скорочення часу реагування на інформаційні та кіберінциденти, підвищення ефективності міжвідомчої взаємодії
Регулярне тестування цифрової стійкості	Проведення аудиту інформаційної безпеки, навчань, кібернавчань і перевірок захищеності державних інформаційних систем	Своєчасне виявлення вразливостей та підвищення готовності до кризових ситуацій
Сертифікація ІКТ-продуктів і цифрових сервісів	Запровадження національної системи оцінювання безпеки цифрових продуктів за європейськими стандартами	Зменшення ризиків використання незахищених програмних і технічних рішень
Розвиток цифрових компетентностей	Систематичне навчання державних службовців, працівників критичної інфраструктури та фахівців із кібербезпеки	Формування професійного кадрового потенціалу у сфері інформаційної безпеки
Використання штучного інтелекту для моніторингу інформаційного простору	Автоматизований аналіз інформаційних потоків, виявлення дезінформації, прогнозування інформаційних загроз	Підвищення оперативності прийняття управлінських рішень та ефективності інформаційної протидії
Запровадження єдиних стандартів управління інформаційною безпекою	Уніфікація вимог до захисту інформаційних ресурсів органів державної влади та критичної інфраструктури	Забезпечення єдиного рівня захисту державних інформаційних систем та їх сумісності з європейськими вимогами

Джерело: сформовано автором

Упровадження зазначених практик сприятиме формуванню в Україні сучасної моделі державного регулювання інформаційної безпеки, яка відповідатиме європейським принципам управління цифровими ризиками та забезпечення цифрової стійкості. Особливе значення матиме розвиток ризик-орієнтованого

управління, цифрової взаємодії між органами державної влади, постійного моніторингу інформаційного середовища із застосуванням технологій штучного інтелекту, а також системної підготовки кадрів у сфері інформаційної безпеки. Реалізація цих напрямів не лише прискорить виконання Україною євроінтеграційних зобов'язань, а й підвищить спроможність держави ефективно протидіяти сучасним інформаційним і кібернетичним загрозам, забезпечуючи захист національних інтересів в умовах цифрового розвитку та воєнних викликів.

ВИСНОВКИ З ДАНОГО ДОСЛІДЖЕННЯ І ПЕРСПЕКТИВИ ПОДАЛЬШИХ РОЗВІДОК У ДАНОМУ НАПРЯМІ

Отже, проведене дослідження засвідчило, що сучасна європейська модель державного регулювання інформаційної безпеки ґрунтується на комплексному поєднанні нормативно-правових, організаційних, інституційних і технологічних механізмів, спрямованих на забезпечення цифрової стійкості держави, захист критичної інформаційної інфраструктури та ефективне управління інформаційними ризиками. Обґрунтовано, що для України особливої актуальності набуває імплементація європейських підходів до державного регулювання інформаційної безпеки шляхом адаптації ризик-орієнтованої моделі управління, розвитку системи міжвідомчої координації, впровадження сучасних механізмів моніторингу інформаційного простору, сертифікації цифрових продуктів і сервісів, регулярного оцінювання цифрової стійкості критичної інформаційної інфраструктури та системної підготовки фахівців у сфері інформаційної безпеки. Реалізація зазначених напрямів сприятиме гармонізації національного законодавства з правом Європейського Союзу, підвищенню інституційної спроможності органів державної влади, зміцненню інформаційної та кібернетичної стійкості держави, а також формуванню сучасної моделі державного регулювання інформаційної безпеки, здатної ефективно забезпечувати захист національних інтересів України в умовах цифрової трансформації, євроінтеграції та зростання сучасних інформаційних і воєнних викликів.

Література

1. Бондаренко Р. В., Михальчук В. М. Інформаційна безпека держави. Інвестиції: практика та досвід. 2021. № 5. С. 95–101. DOI: https://doi.org/10.32702/2306-6814.2021.5.95
2. Баранов О. А. Правове забезпечення інформаційної сфери: теорія, методологія і практика : монографія. Київ : Видавничий дім «АртЕк», 2014. URL : https://ippi.org.ua/pravove-zabezpechennya-informatsiinoi-sferi-teoriya-metodologiya-i-praktika
3. Антонова С. Є., Мартинюк Г. Ф. Інформаційна безпека. Державне управління: удосконалення та розвиток, 2019. No11.URL: http://www.dy.nayka.com.ua/pdf/11_2019/38.pdf
4. Шатун В. Т., Гладун О. В. Інформаційна безпека – невід'ємна складова національної безпеки України. Наукові праці Чорноморського державного університету імені Петра Могили комплексу "Києво-Могилянська академія". Серія : Державне управління. 2016. Т. 267, Вип. 255. С. 174-180. URL: http://nbuv.gov.ua/UJRN/Npchdu_2016_267_255_29
5. Селіхов Д. А. Інформаційна безпека особистості: теоретико-правовий аспект. Науковий вісник Ужгородського національного університету. Серія: Право, 2026. № 93. Т. 1. https://doi.org/10.24144/2307-3322.2026.93.1.25
6. Калюжний Р. Питання концепції реформування інформаційного законодавства України. Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. 2000. № 1. С. 17-21. URL: https://ela.kpi.ua/handle/123456789/15952
7. Милосердна І. М. Інформаційна безпека як елемент національної безпеки: теоретичний вимір та особливості впровадження. Науковий журнал «Політикус», 2024. № 4. С. 179-185. URL: http://politicus.od.ua/4_2024/28.pdf
8. Подорожна Т. С. Інформаційна безпека людини в системі національної безпеки: виклики та загрози. Аналітично-порівняльне правознавство, 2024. № 2. С. 500-506. DOI: https://doi.org/10.24144/2788-6018.2024.02.85
9. Квіткін П. В., Дятлова І. В., Петрова Л. О. Інформаційна безпека особистості: теоретико-методологічний аналіз. Вісник Національного юридичного університету імені Ярослава Мудрого, 2021. № 4 (51). С. 46-62. DOI: https://doi.org/10.21564/2663-5704.51.241998
10. Смотрич Д., Бріалко Л. Інформаційна безпека в умовах воєнного стану. Науковий вісник Ужгородського національного університету. Серія: Право, 2023. № 77. Ч. 2. С. 121-127. DOI: https://doi.org/10.24144/2307-3322.2023.77.2.20
11. Наливайко О.І. Принципи правового захисту людини: підходи до класифікації. Держава і право. Серія «Юридичні і політичні науки», 2001. Вип. 13. С. 26-33. URL: http://search.nbuv.gov.ua/publ/REF-0000465270
12. Виздрик В.С., Мельник О.М. Інформаційна безпека в Україні: сучасний стан. Grail of Science. 2023. № 24. С. 196-202. DOI: https://doi.org/10.36074/grail-of-science.17.02.2023.034

References

1. Bondarenko R. V., Mykhalchuk V. M. (2021). Informatsiina bezpeka derzhavy [Information Security of the State]. *Investytsii: praktyka ta dosvid – Investments: Practice and Experience,* no. 5, pp. 95–101. DOI: https://doi.org/10.32702/2306-6814.2021.5.95
2. Baranov O. A. (2014). Pravove zabezpechennia informatsiinoi sfery: teoriia, metodolohiia i praktyka [Legal Support of the Information Sphere: Theory, Methodology and Practice]. Kyiv: ArtEk. Available at: https://ippi.org.ua/pravove-zabezpechennya-informatsiinoi-sferi-teoriya-metodologiya-i-praktika
3. Antonova S. Ye., Martyniuk H. F. (2019). Informatsiina bezpeka [Information Security]. *Derzhavne upravlinnia: udoskonalennia ta rozvytok – Public Administration: Improvement and Development,* no. 11. Available at: http://www.dy.nayka.com.ua/pdf/11_2019/38.pdf
4. Shatun V. T., Hladun O. V. (2016). Informatsiina bezpeka – nevidiemna skladova natsionalnoi bezpeky Ukrainy [Information Security as an Integral Component of the National Security of Ukraine]. *Naukovi pratsi Chornomorskoho derzhavnoho universytetu imeni Petra Mohyly. Seriia: Derzhavne upravlinnia – Scientific Works of Petro Mohyla Black Sea State University. Series: Public Administration,* vol. 267, no. 255, pp. 174–180. Available at: http://nbuv.gov.ua/UJRN/Npchdu_2016_267_255_29
5. Selikhov D. A. (2026). Informatsiina bezpeka osobystosti: teoretyko-pravovyi aspekt [Personal Information Security: Theoretical and Legal Aspect]. *Naukovyi visnyk Uzhhorodskoho natsionalnoho universytetu. Seriia: Pravo – Uzhhorod National University Herald. Series: Law*, no. 93, vol. 1. DOI: https://doi.org/10.24144/2307-3322.2026.93.1.25
6. Kaliuzhnyi R. (2000). Pytannia kontseptsii reformuvannia informatsiinoho zakonodavstva Ukrainy [Issues of the Concept of Reforming Information Legislation of Ukraine]. *Pravove, normatyvne ta metrolohichne zabezpechennia systemy zakhystu informatsii v Ukraini – Legal, Regulatory and Metrological Support of Information Protection Systems in Ukraine*, no. 1, pp. 17–21. Available at: https://ela.kpi.ua/handle/123456789/15952
7. Myloserdna I. M. (2024). Informatsiina bezpeka yak element natsionalnoi bezpeky: teoretychnyi vymir ta osoblyvosti vprovadzhennia [Information Security as an Element of National Security: Theoretical Dimension and Implementation Features]. *Politykus – Politicus*, no. 4, pp. 179–185. Available at: http://politicus.od.ua/4_2024/28.pdf
8. Podorozhna T. S. (2024). Informatsiina bezpeka liudyny v systemi natsionalnoi bezpeky: vyklyky ta zahrozy [Human Information Security in the National Security System: Challenges and Threats]. *Analitychno-porivnialne pravoznavstvo – Analytical and Comparative Jurisprudence,* no. 2, pp. 500–506. DOI: https://doi.org/10.24144/2788-6018.2024.02.85
9. Kvitkin P. V., Diatlova I. V., Petrova L. O. (2021). Informatsiina bezpeka osobystosti: teoretyko-metodolohichnyi analiz [Personal Information Security: Theoretical and Methodological Analysis]. *Visnyk Natsionalnoho yurydychnoho universytetu imeni Yaroslava Mudroho – Bulletin of Yaroslav Mudryi National Law University,* no. 4 (51), pp. 46–62. DOI: https://doi.org/10.21564/2663-5704.51.241998
10. Smotrych D., Brialko L. (2023). Informatsiina bezpeka v umovakh voiennoho stanu [Information Security under Martial Law]. *Naukovyi visnyk Uzhhorodskoho natsionalnoho universytetu. Seriia: Pravo – Uzhhorod National University Herald. Series: Law,* no. 77, part 2, pp. 121–127. DOI: https://doi.org/10.24144/2307-3322.2023.77.2.20
11. Nalyvaiko O. I. (2001). Pryntsypy pravovoho zakhystu liudyny: pidkhody do klasyfikatsii [Principles of Legal Protection of Human Rights: Approaches to Classification]. *Derzhava i pravo. Seriia "Yurydychni i politychni nauky" – State and Law. Series "Legal and Political Sciences*", issue 13, pp. 26–33. Available at: http://search.nbuv.gov.ua/publ/REF-0000465270
12. Vyzdryk V. S., Melnyk O. M. (2023). Informatsiina bezpeka v Ukraini: suchasnyi stan [Information Security in Ukraine: Current State]. *Grail of Science,* no. 24, pp. 196–202. DOI: https://doi.org/10.36074/grail-of-science.17.02.2023.034