ПРИВАТНА УСТАНОВА
«НАУКОВО-ДОСЛІДНИЙ ІНСТИТУТ ПУБЛІЧНОГО ПРАВА»

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ ВИЩИЙ НАВЧАЛЬНИЙ ЗАКЛАД
«УЖГОРОДСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ»

Кваліфікаційна наукова
праця на правах рукопису

БІЛОУС ЯРОСЛАВ ВОЛОДИМИРОВИЧ

УДК 342.9

ДИСЕРТАЦІЯ

АДМІНІСТРАТИВНО-ПРАВОВЕ РЕГУЛЮВАННЯ ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В УКРАЇНІ

Подається на здобуття наукового ступеня **кандидата юридичних наук**

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ Я.В. Білоус

Науковий керівник – **Щупаківський Роман Володимирович**,
доктор юридичних наук, старший дослідник

Ужгород – 2025

АНОТАЦІЯ

Білоус Я.В. Адміністративно-правове регулювання використання інформаційних технологій в Україні. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня кандидата юридичних наук зі спеціальності 12.00.07 – адміністративне право і процес; фінансове право; інформаційне право. – ДВНЗ «Ужгородський національний університет», Ужгород, 2025.

У роботі досліджено адміністративно-правове регулювання використання інформаційних технологій в Україні як комплексну проблему, яка потребує системного підходу для забезпечення належного правового регулювання в умовах цифрової трансформації.

Дисертація містить теоретичне обґрунтування адміністративно-правового регулювання у сфері інформаційних технологій, аналізує ґенезу відповідного законодавства в Україні, визначає основні проблеми правового забезпечення використання інформаційних технологій, зокрема у сферах кібербезпеки, електронного урядування, захисту персональних даних.

Особливу увагу приділено аналізу суб’єктів адміністративно-правового регулювання, включаючи органи державної влади, органи місцевого самоврядування та приватних суб’єктів, які виконують делеговані функції. Досліджено адміністративні процедури, що застосовуються у сфері інформаційних технологій, та проблеми правового режиму інформаційної безпеки.

У роботі розглянуто міжнародний досвід регулювання інформаційних технологій, включаючи практики Європейського Союзу, Сполучених Штатів Америки, Естонської Республіки, Республіки Сінгапур, Республіки Корея, Китайської Народної Республіки. Запропоновано шляхи імплементації цих стандартів у національне законодавство України.

Сформульовано перспективи розвитку нормативно-правового

забезпечення використання інформаційних технологій в Україні, включаючи розробку та прийняття Цифрового кодексу України, адаптацію до європейських стандартів, вдосконалення правового регулювання інноваційних технологій (штучний інтелект, блокчейн, IoT), розвиток цифрової інфраструктури та електронного урядування.

Практичне значення одержаних результатів полягає у можливості їх використання для вдосконалення чинного законодавства, підготовки законопроєктів, навчально-методичних матеріалів, а також для підвищення ефективності діяльності органів державної влади та місцевого самоврядування у сфері інформаційних технологій.

Ключові слова: GDPR, адміністративні процедури, адміністративно-правове регулювання, електронне урядування, інформаційна безпека, інформаційні технології, кібербезпека, міжнародні стандарти, цифрова трансформація.

ANNOTATION

Bilous Ya.V. Administrative and legal regulation of the use of information technologies in Ukraine. – Qualification scientific work on the rights of the manuscript.

Thesis for a candidate degree in law sciences by speciality 12.00.07 – administrative law and process; financial law; information law. – Uzhgorod National University, Uzhhorod, 2025.

This dissertation examines the administrative and legal regulation of the use of information technologies in Ukraine as a complex issue requiring a systemic approach to ensure proper legal regulation in the context of digital transformation.

The research provides a theoretical substantiation of administrative and legal regulation in the field of information technologies, analyzes the genesis of relevant legislation in Ukraine, and identifies key issues in the legal framework for the use

of information technologies, particularly in the areas of cybersecurity, e-governance, and personal data protection.

Special attention is devoted to analyzing the subjects of administrative and legal regulation, including government authorities, local self-government bodies, and private entities performing delegated functions. The study explores administrative procedures applied in the field of information technologies and the challenges associated with the legal regime of information security.

The dissertation also examines international practices in regulating information technologies, drawing on the experiences of the European Union, the United States of America, Republic of Estonia. It proposes ways to implement these standards into Ukraine's national legislation.

The study outlines prospects for developing the regulatory framework for the use of information technologies in Ukraine, including the development of a Digital Code of Ukraine, adaptation to European standards, improvement of legal regulation for innovative technologies (artificial intelligence, blockchain, IoT), and the advancement of digital infrastructure and e-governance.

The practical significance of the obtained results lies in their potential application for improving current legislation, drafting bills, preparing educational and methodological materials, and enhancing the efficiency of government and local self-government bodies in the field of information technologies.

Key words: administrative and legal regulation, administrative procedures, cybersecurity, digital transformation, e-governance, GDPR, information security, information technologies, international standards.

СПИСОК ПРАЦЬ, ОПУБЛІКОВАНИХ ЗА ТЕМОЮ ДИСЕРТАЦІЇ:

Статті, в яких опубліковано основні наукові результати дисертації:

1. Білоус Я.В. Основні проблеми нормативно-правового регулювання використання інформаційних технологій в Україні. *Юридичний науковий електронний журнал*. 2023. № 12. С. 650–653. DOI: https://doi.org/10.32782/2524-0374/2023-12/163.

2. Білоус Я.В. Етапи розвитку адміністративно-правового регулювання інформаційних технологій в Україні. *Право та державне управління*. 2024. № 2. С. 357–362. DOI: https://doi.org/10.32782/pdu.2024.2.47.

3. Білоус Я.В. Проблематика правового регулювання інформаційних технологій в Україні в умовах євроінтеграції та цифрової трансформації. *Держава та регіони. Серія: Право*. 2024. № 3. С. 103–107. DOI: https://doi.org/10.32782/1813-338X-2024.3.17.

4. Білоус Я.В. Європейський досвід адміністративно-правового регулювання інформаційних технологій: позитивний досвід для України. *KELM (Knowledge, Education, Law, Management)*. 2024. № 3(63). P. 210–214. DOI: https://doi.org/10.51647/kelm.2024.3.33.

5. Білоус Я.В. Перспективні напрями удосконалення адміністративно-правового регулювання інформаційних технологій в Україні. *Право і суспільство*. 2024. № 2. С. 670–677. DOI: https://doi.org/10.32842/2078-3736/2024.2.96.

Наукові праці, які засвідчують апробацію матеріалів дисертації:

1. Білоус Я.В. Проблеми правового регулювання використання інформаційних технологій в Україні. *Proceedings of the international scientific conference "The latest law developments"*, Wloclawek, Republic of Poland, April 3–4, 2024. Riga : Publishing House "Baltija Publishing", 2024. P. 277–282. DOI: https://doi.org/10.30525/978-9934-26-432-0-66.

2. Білоус Я.В. Перспективні заходи правового регулювання інформаційних технологій в Україні. *Proceedings of the international scientific conference "Scientific innovations in law amidst the impact of the Russian-Ukrainian war on the legal system"*, Riga, the Republic of Latvia, February 7–8, 2024. Riga : Publishing House "Baltija Publishing", 2024. P. 300–304. DOI: https://doi.org/10.30525/978-9934-26-409-2-72.

ЗМІСТ

ВСТУП……..…….9

РОЗДІЛ 1 ЗАГАЛЬНІ ЗАСАДИ АДМІНІСТРАТИВНО-ПРАВОВОГО РЕГУЛЮВАННЯ ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ…….……..……18

1.1 Значення інформаційних технологій у сучасному суспільстві та визначення поняття «адміністративно-правове регулювання інформаційних технологій»……...…..18

1.2 Ґенеза адміністративно-правового регулювання інформаційних технологій в Україні…….……..……...…32

1.3 Нормативно-правові основи регулювання використання інформаційних технологій…….……..……..……...…52

Висновки до розділу 1……...……..76

РОЗДІЛ 2 ОСОБЛИВОСТІ АДМІНІСТРАТИВНО-ПРАВОВОГО РЕГУЛЮВАННЯ ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ…….……..……..79

2.1 Адміністративно-правове забезпечення правового режиму інформаційної безпеки……..……79

2.2 Система суб’єктів адміністративно-правового регулювання в сфері інформаційних технологій……...……..…..…97

2.3 Адміністративні процедури в регулюванні інформаційних технологій…….……...……112

Висновки до розділу 2……...128

РОЗДІЛ 3 ПРОБЛЕМИ ТА ШЛЯХИ ВДОСКОНАЛЕННЯ АДМІНІСТРАТИВНО-ПРАВОВОГО РЕГУЛЮВАННЯ ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В УКРАЇНІ……....…131

3.1 Проблеми правового регулювання інформаційних технологій в умовах цифрової трансформації…….……...……131

3.2 Роль зарубіжного досвіду у вдосконаленні адміністративно-правового регулювання інформаційних технологій……..……146

3.3 Перспективи розвитку нормативно-правового забезпечення використання інформаційних технологій в Україні…….…..……165

Висновки до розділу 3……..182

ВИСНОВКИ…….……186

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ…….……195

ДОДАТКИ……...……..219

ВСТУП

Актуальність теми дослідження. У сучасних умовах інформаційні технології (ІТ) є невід'ємною частиною економічного, соціального та управлінського життя суспільства. Їх застосування не лише сприяє розвитку цифрової економіки, а й кардинально змінює традиційні підходи до організації публічного управління, взаємодії між державою, бізнесом і громадянами. Україна як держава, що активно впроваджує цифрові трансформації, стикається з необхідністю створення ефективної системи адміністративно-правового регулювання у цій сфері.

З одного боку, Україна демонструє прогрес у цифровізації: запуск державного порталу «Дія», розвиток електронного урядування, впровадження електронного документообігу, надання цифрових послуг для громадян. З іншого боку, нормативно-правове регулювання використання інформаційних технологій залишається фрагментарним і не досить узгодженим із міжнародними стандартами. Це призводить до низки проблем, серед яких: недостатній захист персональних даних, відсутність дієвих механізмів забезпечення кібербезпеки, прогалини у правовому забезпеченні інноваційних технологій, таких як блокчейн, штучний інтелект та Інтернет речей.

Особливої актуальності набуває питання інформаційної безпеки в умовах зовнішньої агресії та кіберзагроз, які використовуються для дестабілізації державних інститутів, економіки та громадського порядку. Захист інформаційного простору стає одним із пріоритетів державної політики, що потребує ефективних адміністративно-правових інструментів.

Важливо також враховувати міжнародний досвід країн, які успішно вирішують питання регулювання ІТ-сфери, і адаптувати їхні найкращі практики до українських реалій, що дозволить не лише гармонізувати національне законодавство з європейськими та світовими стандартами, а й

забезпечити конкурентоспроможність України в глобальному цифровому середовищі.

Таким чином, необхідність удосконалення адміністративно-правового регулювання використання інформаційних технологій зумовлена стрімким розвитком цифрових технологій, вимогами інформаційної безпеки, потребою гармонізації з міжнародними стандартами та прагненням створити ефективну систему публічного управління в умовах цифрової трансформації. Все це підкреслює актуальність теми дослідження, орієнтованої на аналіз наявних проблем і розробку рекомендацій для вдосконалення правового регулювання у цій сфері.

Науково-теоретичне підґрунтя для виконання роботи становили праці таких учених, як: В.Б. Авер'янов, В.М. Бевзенко, Д.О. Біленська, А.Л. Борко, А.В. Боровик, О.А. Заярний, Ю.С. Козлова, Д.В. Луценко, І.І. Панова, О.П. Письменна, М.В. Серебро, О.І. Ткачук та інші. На даний момент відсутні комплексні монографічні дослідження, які б детально та всебічно висвітлювали основи адміністративно-правового регулювання застосування інформаційних технологій в Україні. У наявних наукових працях ця проблема розглядалася лише частково або в контексті загальних адміністративно-правових питань, без глибокого та цілісного підходу. Це вказує на необхідність систематизації теоретичних і практичних напрацювань, а також аналізу сучасних тенденцій розвитку адміністративно-правового регулювання використання інформаційних технологій в Україні. Таким чином, питання адміністративно-правового регулювання інформаційних технологій як окремого об'єкта правового впливу потребує детальнішого вивчення та дослідження.

Зв'язок роботи з науковими програмами, планами, темами. Роботу виконано в межах планів науково-дослідної роботи Приватної установи «Науково-дослідний інститут публічного права».

Мета та задачі дослідження. Мета дослідження полягає в тому, щоб на основі наукового аналізу, вивчення й узагальнення теоретичних розробок,

чинного законодавства України та практики його застосування визначити та комплексно дослідити особливості адміністративно-правового регулювання використання інформаційних технологій в Україні, виявити недоліки й протиріччя, характерні для цієї сфери, а також обґрунтувати оптимальні шляхи їх усунення з урахуванням сучасної цифрової трансформації, міжнародних правових стандартів та розвитку інформаційного суспільства, сформувати пропозиції щодо вдосконалення відповідного законодавства.

Для досягнення поставленої мети в дисертації необхідно вирішити такі основні *задачі:*

– визначити поняття та проаналізувати форми адміністративно-правового регулювання використання інформаційних технологій в Україні;

– описати ґенезу адміністративно-правового регулювання інформаційних технологій в Україні та визначити основні етапи розвитку нормативної бази у цій сфері;

– охарактеризувати нормативно-правове забезпечення використання інформаційних технологій в Україні, звертаючи увагу на відповідність сучасним міжнародним стандартам;

– проаналізувати систему суб’єктів адміністративно-правового регулювання у сфері інформаційних технологій та визначити їх правовий статус і взаємодію;

– окреслити особливості адміністративних процедур, що застосовуються в регулюванні інформаційних технологій, і визначити їх ефективність;

– описати проблеми забезпечення правового режиму інформаційної безпеки в Україні, зокрема в умовах зростання кіберзагроз і цифровізації державних послуг;

– виявити основні проблеми адміністративно-правового регулювання використання інформаційних технологій в умовах цифрової трансформації та воєнного стану;

– проаналізувати роль зарубіжного досвіду у вдосконаленні адміністративно-правового регулювання інформаційних технологій і запропонувати можливі напрями його адаптації до українського законодавства;

– сформулювати рекомендації щодо перспектив розвитку нормативно-правового забезпечення використання інформаційних технологій в Україні з урахуванням міжнародних стандартів і потреб цифровізації.

Об'єктом дослідження є суспільні відносини, які виникають у зв'язку з адміністративно-правовим регулюванням використання інформаційних технологій в Україні.

Предметом дослідження є адміністративно-правове регулювання використання інформаційних технологій в Україні.

Методи дослідження. Досягнення поставленої мети та виконання завдань дисертації зумовили використання як методологічної основи роботи сукупність загальнонаукових і спеціальних методів наукового пізнання. Їх застосування дозволило всебічно проаналізувати предмет дослідження, сформулювати відповідні висновки та розробити рекомендації.

Загальнонаукові методи:

– історичний метод застосовано для з'ясування ґенези адміністративно-правового регулювання використання інформаційних технологій в Україні, визначення основних етапів розвитку нормативної бази та встановлення зв'язку між минулим і сучасністю (підрозділ 1.2);

– логічний метод дозволив структурувати та систематизувати матеріал, а також виявити зв'язки між окремими аспектами адміністративно-правового регулювання (підрозділи 1.1, 2.1, 2.3);

– метод узагальнення використовувався для аналізу різних форм адміністративно-правового регулювання, їх впливу на розвиток інформаційних технологій, формулювання висновків і пропозицій (підрозділи 1.1, 2.2);

– системний аналіз дозволив розглянути нормативно-правове забезпечення як цілісну систему, виявити її недоліки та потенційні напрями вдосконалення (розділи 1 і 3).

Спеціальні методи:

– порівняльно-правовий метод використано для аналізу законодавства України та міжнародних правових стандартів, зокрема GDPR, директив ЄС у сфері кібербезпеки, що дозволило виявити можливості для адаптації європейського та світового досвіду в Україні (підрозділи 1.3, 3.2);

– документальний аналіз допоміг дослідити нормативно-правові акти України, міжнародні договори та акти, які визначають правові основи використання інформаційних технологій (підрозділи 1.3, 2.2);

– логіко-семантичний метод застосовано для визначення основних понять і дефініцій, таких як «інформаційні технології», «адміністративно-правове регулювання», «інформаційна безпека», їх уточнення та інтерпретації (підрозділи 1.1, 1.3, 2.3);

– метод моделювання використано для розробки рекомендацій щодо вдосконалення чинного законодавства, формулювання концептуальних пропозицій та прогнозування можливих наслідків їх впровадження (розділ 3).

Інші методи:

– метод аналізу та синтезу дозволив зосередитися на окремих елементах правового регулювання та об’єднати їх у цілісну систему для визначення взаємозв’язків між нормативними актами, суб’єктами регулювання та адміністративними процедурами (підрозділи 2.1, 2.2, 3.1);

– статистичний метод застосовано для аналізу емпіричних даних, зокрема статистики кібератак, впровадження електронних послуг і реалізації цифрових державних програм.

Нормативну основу роботи становлять Конституція України, закони України, укази Президента України, постанови та розпорядження Кабінету Міністрів України, центральних органів виконавчої влади (зокрема, накази Міністерства цифрової трансформації України, Державної служби

спеціального зв'язку та захисту інформації України тощо), органів місцевого самоврядування, міжнародні нормативно-правові акти, згоду на обов'язковість яких надано Верховною Радою України, результати нормопроєктної роботи.

Емпіричну базу дослідження становлять статистичні дані Державної служби статистики України, відомості, розміщені на офіційних вебсайтах суб'єктів публічної адміністрації, правова публіцистика, енциклопедичні, довідникові джерела.

Наукова новизна одержаних результатів полягає в тому, що дисертація є одним із перших у вітчизняній адміністративно-правовій науці цілісних комплексних досліджень, присвячених адміністративно-правовому регулюванню використання інформаційних технологій в Україні. Унаслідок проведеного дослідження сформульовано нові наукові положення та висновки, запропоновані здобувачем, зокрема:

уперше:

– запропоновано авторське визначення поняття «адміністративно-правове регулювання використання інформаційних технологій» як діяльності органів виконавчої влади, інших суб'єктів публічної адміністрації, спрямованої на створення, впровадження та застосування адміністративно-правових норм, що забезпечують ефективне функціонування, розвиток і безпеку інформаційних технологій, а також регулювання відносин між суб'єктами у сфері використання інформаційних технологій із метою забезпечення публічного порядку, захисту прав і свобод людини, підтримки економічної стабільності та національної безпеки;

– обґрунтовано доцільність розгляду інформаційних технологій як об'єкта адміністративно-правового регулювання через їх ключову роль у цифровізації публічного управління, що потребує специфічних підходів до правового забезпечення з урахуванням сучасних викликів, таких як кіберзагрози, приватність та конфіденційність даних;

– визначено основні етапи становлення адміністративно-правового регулювання інформаційних технологій в Україні:

– доінституційний період (радянське правове регулювання до 1991 р.);

– період формування національного законодавства (1991–2010 рр.);

– сучасний період цифрової трансформації (з 2010 р. – дотепер);

удосконалено:

– теоретичні положення щодо системи суб'єктів адміністративно-правового регулювання інформаційних технологій, зокрема, їх класифікацію за рівнем компетенції, сферою діяльності та характером впливу;

– наукові підходи до аналізу адміністративних процедур у сфері використання інформаційних технологій, що дозволило уточнити їх специфіку в умовах цифровізації;

– доктринальні положення щодо правового забезпечення інформаційної безпеки в Україні з огляду на сучасні виклики, пов'язані з кіберзагрозами, гібридною та повномасштабною війнами та забезпеченням стабільності функціонування критичних інформаційних систем;

набули подальшого розвитку:

– положення щодо інтеграції міжнародного досвіду у вдосконалення адміністративно-правового регулювання інформаційних технологій в Україні, зокрема адаптації положень GDPR та директив ЄС щодо кібербезпеки;

– теоретичні основи перспектив нормативно-правового забезпечення цифрової трансформації в Україні, включно з розробкою рекомендацій щодо створення Цифрового кодексу України;

– наукові підходи до формулювання пропозицій стосовно вирішення проблем адміністративно-правового регулювання інформаційних технологій в умовах цифрової трансформації та воєнного стану.

Практичне значення одержаних результатів полягає в тому, що вони можуть бути використані в таких напрямах, як:

– *науково-дослідницька діяльність* – результати дослідження можуть слугувати основою для подальших наукових розробок у сфері адміністративно-правового регулювання інформаційних технологій, зокрема для аналізу нормативного забезпечення цифрової трансформації, дослідження проблем інформаційної безпеки, захисту персональних даних та вдосконалення адміністративних процедур;

– *правотворчість* – сформульовані у роботі висновки та пропозиції можуть бути використані в процесі підготовки законопроєктів та підзаконних актів, спрямованих на вдосконалення правового регулювання інформаційних технологій, кібербезпеки та цифрових державних послуг. Рекомендації щодо адаптації міжнародних стандартів можуть стати основою для імплементації найкращих міжнародних практик у національне законодавство;

– *правозастосовна діяльність* – отримані результати можуть бути використані органами публічної адміністрації для вдосконалення їхньої діяльності у сфері регулювання інформаційних технологій, зокрема в частині забезпечення прозорості адміністративних процедур, захисту прав громадян у цифровому середовищі, а також реагування на кіберзагрози;

– *навчальний процес* – результати дослідження можуть бути використані під час підготовки підручників, посібників, наукових статей, інших навчально-методичних матеріалів із дисциплін, пов’язаних з адміністративним правом, правовим регулюванням цифрових процесів, інформаційною безпекою. Висновки та пропозиції можуть бути впроваджені в навчальні програми спецкурсів із тематики цифрової трансформації публічного управління, адміністративного права та кібербезпеки.

Апробація матеріалів дисертації. Результати дослідження були представлені та обговорені на міжнародних наукових конференціях, зокрема: «The latest law developments» (м. Влоцлавек, Республіка Польща, 3–4 квітня 2024 р.); «Scientific innovations in law amidst the impact of the Russian-Ukrainian war on the legal system» (м. Рига, Латвійська Республіка, 7–8 лютого 2024 р.).

Публікації. Основні положення роботи знайшли відображення в 5 наукових статтях, з них 4 статті опубліковані у виданнях, що визнані як фахові з юридичних наук, та 1 стаття – у зарубіжному науковому виданні, а також у 2 тезах доповідей на науково-практичних конференціях.

Структура та обсяг дисертації. Робота складається зі вступу, трьох розділів, що містять дев’ять підрозділів, висновків, списку використаних джерел і додатків. Загальний обсяг дисертації становить 220 сторінок, у тому числі основного тексту – 186 сторінок. Список використаних джерел налічує 202 найменування.

РОЗДІЛ 1
ЗАГАЛЬНІ ЗАСАДИ АДМІНІСТРАТИВНО-ПРАВОВОГО РЕГУЛЮВАННЯ ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

1.1 Значення інформаційних технологій у сучасному суспільстві та визначення поняття «адміністративно-правове регулювання інформаційних технологій»

Інформаційні технології є невід'ємною складовою сучасного українського суспільства, яке активно переходить до епохи цифровізації. Вони пронизують усі сфери життя — від публічного управління до бізнесу, освіти, медицини та повсякденного життя громадян. Зростаюча роль інформаційних технологій обумовлює необхідність їх ефективного адміністративно-правового регулювання, що сприятиме гармонізації суспільних відносин, забезпеченню національної безпеки, правопорядку та захисту прав громадян.

Цифровізація як процес інтеграції інформаційних технологій у всі аспекти людської діяльності має суттєвий вплив на економіку. Завдяки впровадженню інформаційних технологій, економічні процеси стають більш ефективними, прозорими та динамічними. Загальновідомо, що автоматизація бізнес-процесів дозволила компаніям знижувати витрати, підвищувати продуктивність праці та забезпечувати швидший доступ до ринку. Інтернет-торгівля, яка стала можливою завдяки цифровим платформам, відкрила нові можливості для малого та середнього бізнесу.

Цифровізація економіки також сприяє розвитку фінансових технологій. Застосування блокчейн-технологій, систем електронних платежів і мобільного банкінгу змінюють традиційні фінансові відносини. Інформаційні технології стимулюють появу нових бізнес-моделей, які базуються на цифрових платформах.

Адміністративно-правове регулювання у сфері інформаційних технологій спрямоване на забезпечення безпеки електронних транзакцій, запобігання кіберзлочинності, захист персональних даних та інтелектуальної власності.

У соціальній сфері інформаційні технології сприяють розширенню доступу до освітніх, медичних і культурних послуг. Онлайн-освіта стала особливо популярною в умовах пандемії COVID-19, дозволяючи забезпечити безперервність навчального процесу. У медицині цифрові технології сприяли розвитку «телемедицини», яка дозволила пацієнтам отримувати консультації без необхідності відвідування медичних закладів.

Інформаційні технології також впливають на соціальні комунікації. Соціальні мережі, месенджери та інші платформи стали основними каналами обміну інформацією. Однак, все це також створює й виклики, пов'язані з поширенням дезінформації, маніпуляціями громадською думкою та порушенням приватності.

Адміністративно-правове регулювання інформаційних технологій у соціальній сфері спрямоване на забезпечення балансу між свободою вираження думок і захистом громадських інтересів. Наприклад, у законодавстві Європейського Союзу значна увага приділяється боротьбі з поширенням фейкових новин та ненависницьких висловлювань у мережі Інтернет.

Публічне управління також зазнало суттєвих змін під впливом цифровізації. Електронні послуги, системи електронного документообігу та відкриті дані сприяють підвищенню прозорості, ефективності та доступності адміністративних послуг. Інформаційні технології дозволяють органам публічного адміністрування швидше реагувати на потреби громадян, скорочувати бюрократичні процедури та знижувати витрати на управління.

В Україні впровадження порталу «Дія» стало яскравим прикладом цифровізації публічного управління. Цей портал об'єднує численні послуги,

від реєстрації бізнесу до отримання соціальної допомоги, що значно полегшує доступ громадян до адміністративних послуг.

Таким чином, адміністративно-правове регулювання у сфері інформаційних технологій відіграє ключову роль у забезпеченні стабільного розвитку суспільства в умовах цифрових змін.

Однак для більш точного визначення поняття «адміністративно-правове регулювання інформаційних технологій» необхідно ґрунтовно дослідити його складові, а саме: «адміністративно-правове регулювання» та «інформаційні технології». Аналіз цих категорій надасть можливість визначити ключові напрями їхньої взаємодії.

Варто розпочати з існуючих визначень й трактувань поняття «адміністративно-правове регулювання».

Визначення «адміністративно-правове регулювання» у науковій літературі має глибокі історичні корені. Одним із перших дослідників, які приділили увагу адміністративному праву як механізму регулювання суспільних відносин, був німецький учений Отто Майєр (XIX ст.), який акцентував увагу на регулюванні виконавчої влади та взаємовідносинах між державою і громадянами [1].

У сучасній українській правовій доктрині дослідження адміністративно-правового регулювання набуло розвитку завдяки працям таких вчених, як: В.Б. Авер’янов., В.М. Бевзенко, В.В. Галунько, В.К. Колпаков, І.І. Панова., О.Ф. Скакун. У їхніх роботах адміністративно-правове регулювання здебільшого трактується як діяльність державних органів, спрямована на встановлення, зміну чи припинення правових норм, які регулюють суспільні відносини в публічній сфері.

Зокрема, В. Б. Авер’янов вказував, що адміністративно-правове регулювання в практичній діяльності охоплює три поняття: державне управління, державно-адміністративне регулювання та державні послуги [2].

В. В. Галунько та О. М. Єщук, досліджуючи поняття і зміст адміністративно-правового регулювання, визначають останнє як

цілеспрямований вплив норм адміністративного права на суспільні відносини з метою забезпечення за допомогою адміністративно-правових засобів прав, свобод і публічних законних інтересів фізичних та юридичних осіб, нормального функціонування громадянського суспільства та держави [3].

В.В. Галунько також зазначив, що адміністративно-правове регулювання характеризує спеціально-юридичний механізм впливу адміністративного права на поведінку і діяльність його адресатів; це цілеспрямований вплив норм адміністративного права на суспільні відносини з метою забезпечення за допомогою адміністративно-правових засобів прав, свобод і публічних законних інтересів фізичних та юридичних осіб, нормального функціонування громадянського суспільства і держави. До системи елементів адміністративно-правового регулювання (стадій правозастосування та правоохоронної діяльності) науковець відніс норми адміністративного права; їх зовнішнє вираження - джерела адміністративного права; принципи адміністративного права; тлумачення норм адміністративного права; адміністративно-правові відносини; адміністративно-правовий статус суб'єктів адміністративного права; індивідуальні акти суб'єктів публічної адміністрації; форми діяльності суб'єктів адміністративного права; методи адміністративного права; адміністративно-правові режими; адміністративні процедури; ефективність адміністративно-правового регулювання [3].

В.І. Теремецький вважає, що адміністративно-правове регулювання є цілеспрямованим впливом правових норм, що прийняті державою і є відповідними адміністративними засобами забезпечення прав та законних інтересів фізичних, юридичних осіб і держави у суспільних відносинах із метою підпорядкування їх юридично встановленому правопорядку, а також охорони та розвитку в інтересах суспільства і держави [4].

В теорії адміністративного права поняття адміністративно-правового регулювання базується на загальних теоретичних концепціях. Складність питання зумовлена багатоаспектністю загальнотеоретичних підходів до

правового регулювання. У загальній теорії права найбільш поширеними є два подібні за суттю поняття: правове регулювання та механізм його реалізації.

Так, С. Єсімов зазначає, що поняття правового регулювання використовується в широкому та вузькому значеннях. У широкому розумінні поняття «правове регулювання» вживається для відмінності від інших форм соціального регулювання, істотною та найбільш загальною ознакою якого є використання правових норм для досягнення цілей регулювання. У цьому аспекті правове регулювання є одним із видів родового поняття соціального регулювання. Це загальне визначення не дає сутнісних характеристик правового регулювання [5, с. 74].

Взагалі у правовій науці існують дві концепції співвідношення права і держави. Одна з них стверджує, що саме держава відіграє провідну роль у правотворчості та реалізації норм.

Такі українські правознавці розглядають правове регулювання як цілеспрямовану діяльність держави та її органів, спрямовану на впорядкування суспільних відносин.

Так, наприклад, П. Рабінович визначає правове регулювання як здійснюваний державою за допомогою всіх юридичних засобів владний вплив на суспільні відносини з метою їх упорядкування, закріплення, охорони і розвитку [7, с. 165].

В свою чергу прихильники іншої концепції розглядають право як автономне явище, пов’язане з державою лише як механізмом примусового забезпечення.

С. Єсімов підкреслює, що незалежно від підходу, державне регулювання зберігає ключову роль у сфері адміністративного права, тоді як саморегулювання охоплює організацію внутрішніх відносин соціальних інститутів без втручання держави [5, с. 75].

Саморегульоване право залишається предметом наукових дискусій, оскільки його концепція ґрунтується на ідеї громадянського суспільства як системи недержавних інституцій із власним нормативним забезпеченням. У

будь-якому випадку, правове регулювання є свідомим впливом суб'єкта на суспільні процеси через юридичні механізми [6].

Таким чином, правове регулювання є процесом, що забезпечує упорядкування суспільних відносин за допомогою юридичних засобів. Воно має нормативний, організаційний і цілеспрямований характер та здійснюється державою або громадянським суспільством для гарантування соціальних інтересів.

Правове регулювання вирізняється з-поміж інших форм соціальної регуляції своєю цілеспрямованістю та результативністю, що виявляються в орієнтації правового регулювання на досягнення чітко визначеного в нормах права соціального результату, а також у широкому діапазоні наявних для цього способів дії (починаючи зі стимулювання бажаної поведінки правових суб'єктів через надання певних рекомендацій, встановлення пільг, заохочень і завершуючи можливістю застосування до них засобів державного примусу), що дозволяють ефективно вирішувати поставлені завдання [8].

У науковій літературі виділяють дві специфічні ознаки правового регулювання: 1) воно має цілеспрямований, організований характер, що забезпечує гарантований результат, а також включає нормативно-організаційний вплив на суспільні відносини, їх державно-владне та ціннісне нормування; 2) реалізується через комплексну систему засобів, спрямованих на досягнення встановлених цілей, при цьому використовується специфічний правовий механізм, який забезпечує виконання поставлених завдань і досягнення результатів, закладених у нормах законодавства.

З іншої сторони, І. Шопіна, досліджуючи поняття «адміністративно-правове регулювання», зазначає, що в адміністративному праві існує дуже важлива для формування векторів його розвитку дилема вибору між приматом держави та концепцією сервісної держави. До початку повномасштабної збройної російської агресії рух адміністративно-правової теорії в бік підтримки примату прав людини та сервісної держави вважався безспірним [10, с. 551].

Закладення у пострадянський період розвитку правової науки у роботах В. Авер'янова базових постулатів щодо публічно-сервісної діяльності та подальшого розвитку адміністративного права відповідно до принципів людиноцентризму справило значний вплив на адміністративно-правову науку [10, с. 552].

Справедливо маємо вказати, що за останні десятиліття утвердилася наукова традиція, в якій пріоритет прав і свобод людини у взаємодії з владними органами став незаперечним. Певною мірою «гуманізація» адміністративного права змінила підхід до його основоположних засад.

Отже, основними характеристиками адміністративно-правового регулювання є його впорядковуючий вплив на суспільні відносини, використання спеціальних адміністративно-правових інструментів, а також орієнтація на стабільне функціонування держави та суспільства.

Дослідники вказують, що адміністративно-правове регулювання спрямоване на: забезпечення ефективної діяльності органів виконавчої влади, підтримання порядку в публічній сфері, врегулювання взаємовідносин між державою та громадянами, а також на гарантування дотримання прав і свобод осіб у сфері публічного управління [11, с. 68].

Адміністративно-правове регулювання характеризується такими особливостями, як нормативна визначеність, спрямованість на підтримання публічного порядку, обов'язковість для всіх учасників правовідносин, наявність механізмів державного контролю і примусу, а також забезпечення правового регулювання інформаційних технологій.

Таким чином, адміністративно-правове регулювання можна охарактеризувати як цілеспрямований вплив норм адміністративного права на суспільні відносини, що має на меті захист прав, свобод і законних інтересів фізичних та юридичних осіб, а також забезпечення належного функціонування громадянського суспільства та держави.

З’ясувавши сутність й значення адміністративно-правового регулювання, необхідно розібратись з поняттям «інформаційні технології» як об'єкта дослідження, враховуючи його історичний та науковий розвиток.

Станом на сьогодні, дефініцію «інформаційні технології» (в однині «інформаційна технологія») містить лише Закон України «Про Національну програму інформатизації» від 04.02.1998 № 74/98-ВР. Так, відповідно до ст.1 вказаного закону, інформаційна технологія – цілеспрямована організована сукупність інформаційних процесів з використанням засобів обчислювальної техніки, що забезпечують високу швидкість обробки даних, швидкий пошук інформації, розосередження даних, доступ до джерел інформації незалежно від місця їх розташування [12].

Нормативне визначення «інформаційні технології» включає терміни, що можуть мати неоднозначне тлумачення та викликати дискусії, що є небажаним для нормативного термінологічного апарату, оскільки може спричинити неточності й суб’єктивність як у подальшій законотворчій діяльності, так і в процесі правозастосування.

Відповідно до ч.8 ст. 1 Угоди про правовий режим інформаційних ресурсів Прикордонних військ держав-учасниць СНД інформаційні технології – сукупність методів, способів, прийомів і засобів обробки документованої інформації і регламентованого порядку її застосування [13].

Тобто, поняття інформаційні технології вже вживаються у множині, і їх визначення ґрунтується не лише на інформаційному процесі, а й на регулюванні порядку подальшого впровадження інформації у суспільні відносини, тобто її практичного використання.

Наприклад, міжнародним стандартом ISO/IEC 38500:2015 «Управління інформаційними технологіями в організаціях» Інформаційні технології визначаються як ресурси, необхідні для збору, обробки, зберігання і розповсюдження інформації [14].

У вітчизняній науковій літературі багато авторів намагаються визначити поняття «інформаційні технології» та «комп’ютерні технології»

шляхом виявлення їхніх подібностей або відмінностей, а інколи при розкритті одного з цих термінів зовсім не згадують про інший, що призводить до довільного трактування. Крім того, недостатньо обґрунтованими є спроби окремих дослідників визначати інформаційні технології через поняття «комп'ютерні технології», що фактично призводить до необґрунтованого звуження їхнього змісту.

Наприклад, Триняк В.Ю. визначає інформаційні технології як конкретні способи й механізми оперування інформацією, які мають безпосередньо культурогенний, гносеогенний та автогенеративний характер [15].

При цьому автор, подібно до деяких інших дослідників, використовує термін «інформаційно-комп'ютерні технології» як синонім «інформаційних технологій», повністю ототожнюючи ці поняття, що ще раз підтверджує існуючу невизначеність та неоднозначність термінологічного апарату в цій сфері.

Також автор пропонує визначення інформаційних технологій як специфічних методів пошуку, зберігання, обробки та поширення інформації, вказуючи при цьому на їхню подвійну природу. З одного боку, інформаційні технології розглядаються як спосіб отримання, обробки та використання інформації, а з іншого – як об'єкт правового регулювання, що вивчається у межах інформаційного права та правової інформатики [16].

Однак таке твердження може бути піддане критиці з двох позицій. По-перше, з точки зору правової науки, об'єктом правового регулювання виступають саме суспільні відносини, а тому інформаційні технології слід розглядати або як предмет правового регулювання, або як об'єкт правовідносин. По-друге, з філософської точки зору, пізнання є процесом, притаманним суб'єкту мислення – людині. Форми пізнання варіюються залежно від його рівнів і можуть включати відчуття, сприйняття, уявлення, поняття, умовиводи, судження, експеримент та досвід. Таким чином,

інформаційні технології, радше, є засобом або інструментом, що сприяє процесу пізнання, а не його формою [16, с.155].

Н. О. Побережна вказує, що інформаційні технології – цілісна технологічна навчальна система, що являє собою інтеграцію технічного, дидактичного, користувального та інформаційно-освітнього середовища, яке забезпечує виконання раніше зумовленої послідовності спільних дій суб'єктів навчання в умовах інформатизації освіти, орієнтованих на досягнення проектованих результатів професійної підготовки робочих кадрів [17].

Окрім того, автор стверджує, що «інформаційні технології є якісним продовженням комп'ютерних технологій». Однак таке твердження не можна вважати логічно обґрунтованим, оскільки комп'ютерні технології є лише однією зі складових інформаційних технологій, а не їхнім безпосереднім продовженням. Це питання буде детальніше розглянуто нижче.

Спостерігається значна варіативність у визначенні понятійного апарату. Безперечно, ключовим критерієм при формулюванні визначень слугує сфера застосування інформаційних технологій. Крім того, більшість авторів схильні ототожнювати інформаційні технології з процесами автоматизованої обробки даних, що ґрунтується на досягненнях сучасності, зокрема використанні високопродуктивних електронно-обчислювальних машин (комп'ютерів).

Згідно з визначенням ЮНЕСКО інформаційна технологія - це комплекс взаємозалежних, наукових, технологічних, інженерних дисциплін, що вивчають методи ефективної організації праці людей, зайнятих обробкою і зберіганням інформації; обчислювальну техніку і методи організації і взаємодії з людьми і виробничим устаткуванням, практичні додатки, а також пов'язані з усім цим соціальні, економічні і культурні проблеми [18, с. 18].

К. Юдкова зазначає, що запропоноване визначення інформаційних технологій охоплює широкий комплекс взаємопов'язаних аспектів, які формують систему відносин у сфері соціально-культурного життя людини, а

також сприяють вирішенню актуальних завдань шляхом використання новітніх знань [18, с. 19].

Крім того, визначення, запропоноване ЮНЕСКО, ґрунтується на підході, який розглядає технологію як науку. Це підтверджується етимологією самого терміна «технологія»: слово technos (з давньогрецької) означає мистецтво або ремесло, а logos – вчення або науку, що в загальному сенсі можна трактувати як «вчення про майстерність», яке передбачає процес трансформації сировини у корисні продукти [18, с. 19].

Справедливо буде зауважити, що існують визначення інформаційних технологій, які не обмежуються лише використанням комп'ютерів, а розглядають їх як сукупність засобів, що забезпечують обробку інформації в різних сферах життєдіяльності людини [21].

Проте всі визначення мають спільний ключовий аспект: інформаційні технології слугують засобом опрацювання інформації.

Отже, можна зробити висновок, що в науковій літературі існують різні підходи до визначення інформаційних технологій: одні акцентують увагу на їх технічних характеристиках, тоді як інші зосереджуються на їх впливі та застосуванні в різних сферах суспільного життя.

Так, К. Юдкова вважає, що всі підходи до спроби визначення поняття інформаційних технологій можна визначити як антропоцентричний та техноцентричний, провівши певну паралель із підходами до визначення інформації, де третім підходом є недетермінований, за яким інформація виступає однією із вихідних первинних загальнонаукових категорії, що відображає структуру матерії та не зводиться до більш простих (вторинних) категорій [23, с. 48].

Антропоцентричний підхід до трактування інформаційних технологій зосереджується на їхньому сприйнятті як сфери людської діяльності, що охоплює соціальні, економічні та виробничі аспекти, де інформація розглядається як сукупність даних і фактів, потенційно здатних перетворюватися на знання. Іншими словами, це область суспільної

активності, пов’язана з реалізацією інформаційних процесів, зокрема збору, обробки, накопичення, збереження, пошуку та поширення інформації, незалежно від галузі застосування.

Таким чином, діяльність у сфері інформаційних технологій є одним із ключових елементів концепції постіндустріального суспільства, що характеризує новий етап розвитку цивілізації – інформаційне суспільство. Основні риси цього етапу включають зростаюче значення інформації та знань, задоволення інформаційних потреб людства, формування глобального інформаційного простору та збільшення частки інформаційних продуктів на світовому ринку. У цьому контексті більш доречним терміном для позначення відповідних процесів є «інформаційна діяльність».

Вдалу дефініцію надав Дорогих С.О., який визначив інформаційну діяльність як сукупність дій, спрямованих на задоволення інформаційних потреб громадян, юридичних осіб та держави, реалізується через інформаційні процеси, що охоплюють створення, збирання, одержання, зберігання, обробку, поширення, пошук, використання інформації та утворюють інформаційні продукти і впорядковані інформаційні ресурси, а також через формування інформаційно-телекомунікаційної інфраструктури, засобів зв’язку та засобів інформаційної безпеки [24].

Техноцентричний підхід розглядає інформаційні технології як процес, головним об'єктом якого є інформація. У межах цього підходу інформаційні технології виступають як інструмент підвищення ефективності інформаційної діяльності завдяки застосуванню сучасних технологічних засобів, стаючи при цьому базисом для процесу інформатизації.

Таке розуміння інформаційних технологій закладене в основу чинного нормативного визначення в Україні, а також саме в такому або близькому за змістом значенні цей термін використовується законодавцем і державними органами. Водночас існуюче визначення має суттєве обмеження: інформаційні технології фактично зводяться до комп’ютерних технологій, що призводить до їх звуженого розуміння як сукупності комп’ютерних засобів

опрацювання інформації. Крім того, як зазначалося раніше, нормативне визначення містить дискусійні терміни, що є недопустимим з точки зору правової визначеності. Враховуючи це, можна дійти висновку, що на сьогодні в Україні відсутнє нормативне визначення інформаційних технологій у їхньому ширшому значенні.

Так, К. Юдкова, досліджуючи поняття інформаційні технології, вважає, що кращим базисним варіантом є саме техноцентричний підхід до визначення цього терміну. Щодо питання використання терміну в множині чи в однині, то варто обрати перший варіант, як такий, який став найбільш вживаним сьогодні. Таким чином, на підставі аналізу як існуючих понять, так і самої суті, природи явища можна надати наступне визначення: інформаційні технології – це цілеспрямована сукупність інформаційних процесів та методів створення, пошуку, отримання, передачі, збору, обробки, накопичення, зберігання, розповсюдження, використання та захисту інформації [23, с. 49].

Отже, термін «інформаційні технології» є багатоаспектним і використовується у різних сферах знань. Проте, через швидкий розвиток цієї галузі, як у законодавстві, так і в науковій літературі, відсутнє єдине загальноприйняте визначення.

Однак з урахуванням аналізу існуючих підходів, інформаційні технології можна розглядати як комплекс технічних, програмних, організаційних інструментів і методів, призначених для створення, обробки, передачі, зберігання та застосування інформації у цифровому форматі, що сприяє ефективному функціонуванню суспільних процесів.

Як зазначає С. Єсімов, використання інформаційних технологій являє собою сполучну ланку, яка об'єднує всю сукупність об'єктів публічного управління в інформаційній сфері, оскільки використання інформаційних технологій у діяльності державних і місцевих органів забезпечує не тільки інформаційну взаємодію органів влади, а й підвищує рівень якості здійснення державних послуг у сфері соціальних відносин [25, с. 27].

Як зазначає Ю. П. Бурило, правовою основою публічного управління в інформаційній сфері є підгалузь адміністративного права, яка являє собою систему однорідних предметно-споріднених правових інститутів, що включають в себе ієрархічно побудовану сукупність первинних і вторинних спеціальних правових норм, які регулюють здійснення галузевого та міжгалузевого управління в різних галузях і сферах, що входять до інформаційної сфери як складного об'єкта публічного управління, шляхом визначення завдань і основних напрямів діяльності держави, системи та адміністративно-правового статусу органів (суб'єктів) публічного управління та керованих ними суб'єктів інформаційних та інформаційно-інфраструктурних відносин, а також регулювання взаємодії між ними [26].

Отже, інформаційні технології мають важливе значення у розвитку публічного управління. Вони сприяють прозорості та відкритості діяльності органів влади, забезпечують доступ громадян до публічних послуг через електронні платформи, дозволяють ефективніше управляти інформаційними потоками в системах електронного урядування.

Враховуючи всі вищенаведені аспекти, адміністративно-правове регулювання інформаційних технологій можна визначити як діяльність органів виконавчої влади, інших суб'єктів публічної адміністрації, яка спрямована на створення, впровадження та застосування адміністративно-правових норм, що забезпечують ефективне функціонування, розвиток і безпеку інформаційних технологій, а також регулювання відносин між суб'єктами у сфері використання інформаційних технологій із метою забезпечення публічного порядку, захисту прав і свобод людини, підтримки економічної стабільності та національної безпеки.

Таке визначення об'єднує основні складові адміністративно-правового регулювання, зокрема: 1) об'єкт регулювання – інформаційні технології, їх розробка, впровадження, використання та вплив на суспільні відносини; 2) суб'єкти регулювання – органи публічної адміністрації, виконавчої влади, суб'єкти господарювання, користувачі інформаційних технологій; 3) мету

регулювання: забезпечення правопорядку у сфері цифрових відносин; захист прав і свобод громадян, що використовують інформаційні технології; створення умов для розвитку економіки, цифрових сервісів і публічних послуг; 4) функції: нормотворча (створення правових норм для сфери інформаційних технологій), контрольна (діяльність органів державної влади з моніторингу і забезпечення дотримання норм), захисна (захист суспільних інтересів, прав громадян і безпеки держави).

Таким чином, відповідне визначення адміністративно-правового регулювання інформаційних технологій враховує сучасний стан цифровізації суспільства, значення інформаційних технологій для публічного управління, економіки та життя громадян, а також специфіку їх правового регулювання в Україні.

1.2 Ґенеза адміністративно-правового регулювання інформаційних технологій в Україні

Розвиток адміністративно-правового регулювання інформаційних технологій в Україні має свою унікальну історію, що охоплює декілька ключових етапів. Кожен з цих періодів характеризується специфічними особливостями правового, організаційного та технологічного характеру.

1. *Доінституційний період (до 1991 р.).* Цей період характеризується початковим використанням інформаційних технологій у сфері публічного управління на території України, яка тоді входила до складу СРСР. На цьому етапі інформаційні технології мали обмежене застосування, переважно у вигляді автоматизованих систем управління для потреб оборонної, космічної та промислової галузей.

Розробка перших електронних обчислювальних машин (ЕОМ) в Україні, таких як МЕОМ у Києві (1948–1951 рр.), заклала основу для подальшого розвитку інформаційних технологій. Проте законодавчого регулювання використання інформаційних технологій у публічному

управлінні в цей період фактично не існувало. Основним джерелом права залишалися акти центральної влади СРСР, що носили директивний характер і регулювали в основному технологічні аспекти використання інформаційних систем [27].

Необхідність переходу в СРСР, до складу якого Україна входила до 1991 р., на комплексну автоматизацію технологічних процесів та управління виробничими підприємствами з використанням досягнень електронної обчислювальної техніки вперше зазначалася в 1959 р. у програмних документах XXI з'їзду КПРС [28].

У директивах наступних з'їздів КПРС спостерігається зростання уваги керівництва СРСР до розвитку обчислювальної техніки, систем зв'язку та автоматизації виробництва. Наприклад, вже на XXIII з'їзді КПРС у 1966 р. Комітету з науки і техніки СРСР було поставлено задачу «створити високоефективну загальнодержавну систему наукової інформації для господарського планування» [29].

Директивами XXIV з'їзду КПРС, який відбувся у 1971 р., було передбачено створення автоматизованих систем управління міністерств, підприємств, обчислювальних центрів Держплану, Держпостачу, Центрального статистичного управління та ряду відомств з подальшим об'єднанням цих систем з єдиною автоматизованою мережею зв'язку країни в загальнодержавну автоматизовану систему збирання та обробки інформації [30].

До основних задач економічного і соціального розвитку Радянського Союзу на 1986-1990 рр., затверджених XXVII з'їздом КПРС у 1986 р., крім автоматизації, входила комп'ютеризація країни, тобто організація масового випуску персональних комп'ютерів та збільшення їх виробництва в 2 - 2,3 рази; нарощування виробництва електронно-обчислювальних машин всіх класів; продовження створення і підвищення ефективності роботи обчислювальних центрів колективного користування, інтегрованих банків

даних, мереж обробки і передачі інформації. Наголошувалось також на необхідності зміцнення зв'язку науки та промисловості [31].

На останньому XXVIII з'їзді КПРС у 1990 році затвердити програму розвитку країни так й не вдалося, оскільки в той час вже посилювалися процеси децентралізації, а в 1991 році Радянський Союз припинив існування, розпавшись на незалежні держави. Проте варто зазначити, що в останні роки існування СРСР у програмних документах наукових установ активно використовувався термін «програма інформатизації республіки» [32].

Подальше правове регулювання процесів інформатизації здійснювалося в межах національних законодавств кожної з новостворених держав. При цьому цей процес супроводжувався розривом міждержавних зв'язків, а також суттєвими змінами в економічній і технологічній сферах.

Так, В. Пилипчук зазначає, що за радянських часів ще у 1975 року відомими українськими вченими Глушковим В.М. і Амосовим М.М. вперше у світі було піднято низку фундаментальних проблем у питанні розбудови складових інформаційного суспільства і правового регулювання інформаційних відносин, використання інформаційних технологій, але надалі до їх практичної розробки справа так і не дійшла. Як наслідок лише в 1990-х роках в умовах входження України у світовий економічний простір на загальнодержавному рівні було задекларовано розвиток інформаційного суспільства та розпочато відповідні наукові дослідження з проблем інформатики, інформатизації та використання інформаційних технологій [33, с. 17].

Таким чином, на даному етапі розвитку адміністративно-правового регулювання інформаційних технологій в Україні основною проблемою була їхня обмежена сфера застосування, що не враховувала потреби державного управління на національному рівні. Відсутність чітких правових механізмів регулювання, а також політична централізація значно уповільнювали процес інтеграції інформаційних технологій у систему державного управління.

2. Період формування національного законодавства (1991–2010 рр.)

З проголошенням незалежності України у 1991 році виникла необхідність створення національної системи правового регулювання в усіх сферах життєдіяльності держави, зокрема й у сфері інформаційних технологій. Цей етап можна охарактеризувати як період формування нормативно-правової бази, що регулює відносини у сфері інформації, комунікацій та інформаційної безпеки.

У нормативно-правових актах різного рівня незалежної України використовувалися терміни «інформатизація» та «інформаційне суспільство». Однак основи правового регулювання процесів інформатизації та побудови сучасного демократичного інформаційного суспільства були закладені в Конституції України, прийнятій 28 червня 1996 р. [34].

Так, в основному законі вказується, що захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього українського народу [34, ст. 17]; гарантується таємниця листування, телефонних розмов, телеграфної та іншої кореспонденції, крім випадків, визначених законом [34, ст. 31]; забороняється збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом; людині надаються права на: ознайомлення в органах державної влади, органах місцевого самоврядування, установах і організаціях з відомостями про себе, які не є державною або іншою захищеною законом таємницею; спростовування недостовірної інформації про себе і членів своєї сім'ї; вимогу вилучення будь-якої інформації та відшкодування матеріальної і моральної шкоди, завданої збиранням, зберіганням, використанням і поширенням такої недостовірної інформації [34, ст. 32]; свободу думки і слова, вільне висловлювання своїх поглядів і переконань [34, ст. 34]; свободу світогляду [34, ст. 35], оскільки плюралізм думок та вільне їх поширення є однією з ознак інформаційного суспільства; свободу об'єднання громадян у політичні партії та громадські

організації для задоволення свої законних інтересів, в тому числі інформаційних [34, ст. 36]; володіння, користування і розпорядження інтелектуальною власністю [34, ст. 41]; підприємницьку діяльність (у тому числі в сфері інформатизації), яка не заборонена законом [34, ст. 42]; вільний доступ до інформації про стан довкілля, якість харчових продуктів і предметів побуту, а також право на її поширення, тобто інформація ніким не може бути засекречена [34, ч. 2, ст. 50]; на освіту [34, ст. 53]; свободу літературної, художньої, наукової і технічної творчості, захист результатів своєї інтелектуальної, творчої діяльності та інтелектуальної власності, авторських прав, моральних і матеріальних інтересів, що виникають у зв'язку з різними видами інтелектуальної діяльності [34, ст. 54].

Вперше у незалежній України слово «інформатизація» законодавчо згадується в Указі Президента України №186/93 від 31.05.1993 р. «Про державну політику інформатизації України» [35], згідно з яким Кібернетичному центру Академії наук України надавався статус головної державної координуючої організації з проблем інформатизації та доручалось до 1 грудня 1993 р. розробити Концепцію державної політики інформатизації України й основні напрями Національної програми інформатизації України.

Цей указ втратив чинність на підставі Указу Президента № 206/95 від 13.03.1995 р. «Про утворення Національного агентства з питань інформатизації" [36]. Основними завданнями агентства були визначені: 1) формування та реалізація державної політики інформатизації, стратегії розвитку інформатизації усіх сфер суспільного життя; 2) координація діяльності центральних органів державної виконавчої влади, підприємств, установ і організацій щодо виконання державних інформатизаційних програм і проектів; 3) розробка проектів нормативних актів з питань інформатизації; 4) організація міжнародного співробітництва, участь у підготовці міжнародних договорів України з цих питань.

Даний центральний орган виконавчої влади з питань інформатизації в Україні часто проходив процедури реорганізації, змінював свою назву,

підпорядкованість та рівень повноважень. Так, з 13.03.1995 р. це було Національне агентство з питань інформатизації при Президентові України [36]; з 16.09.1998 р. — Державне агентство інформатизації України (ДАІНУ), підпорядковане Міністерству інформації України [37]; з 03.06.1999 р. — Державний комітет зв'язку та інформатизації України при Кабінеті Міністрів України [38]; з 08.09.2004 р. — Державний департамент з питань зв'язку та інформатизації при Міністерстві транспорту та зв'язку України [39]; з 26.03.2008 р. — Державний комітет інформатизації України [40]; з 05.07.2010 р. — Державний комітет України з питань науки, інновацій та інформатизації [41]; з 09.12.2011 р. — Державне агентство з питань науки, інновацій та інформації України, яке координується Міністерством освіти і науки, молоді та спорту [43].

Таким чином, сучасний правовий статус цього органу було змінено на агентство, аналогічно до ситуації у 90-х роках XX століття. Крім того, в останні роки в офіційному вжитку все частіше з'являється термін «інновація», тоді як у 90-ті роки XX століття переважало поняття «комерціалізація науки».

Завдання агентства визначені в Положенні [43], головне з яких — участь у формуванні та забезпечення реалізації державної політики у сфері наукової, науково-технічної та інноваційної діяльності, трансферу технологій, інформатизації; формування, використання й захист національних електронних інформаційних ресурсів та створення умов для розвитку інформаційного суспільства.

Базовими для процесів інформатизації адміністративно-правового регулювання інформаційних технологій в Україні в період формування національного законодавства є наступні Закони України: «Про інформацію» [44], Закон України «Про науково-технічну інформацію» [45], Закон України «Про захист інформації в автоматизованих системах» [46], «Про концепцію Національної програми інформатизації» [47], «Про Національну програму інформатизації» [12], «Про Основні засади розвитку інформаційного

суспільства України на 2007—2015 роки» [77], Закон України «Про електронний цифровий підпис» [48].

Закон України «Про інформацію» (1992 р.) є першим законодавчим актом, який заклав правові основи функціонування інформаційної сфери. У ньому визначено поняття інформації, види інформації та принципи її використання [44].

Так, відповідно до ст.1 Закону України «Про інформацію», інформація визначена як будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді.

Стаття 10 Закону України «Про інформацію» визначила види інформації за змістом. Так, за змістом інформація поділяється на такі види: інформація про фізичну особу; інформація довідково-енциклопедичного характеру; інформація про стан довкілля (екологічна інформація); інформація про товар (роботу, послугу); науково-технічна інформація; податкова інформація; правова інформація; статистична інформація; соціологічна інформація; критична технологічна інформація; інші види інформації.

Закон України «Про науково-технічну інформацію» (1993 р.) врегульовував обіг науково-технічної інформації, що мало значення для розвитку інформаційних технологій. Цей Закон визначив основи державної політики в галузі науково-технічної інформації, порядок її формування і реалізації в інтересах науково-технічного, економічного і соціального прогресу країни. Метою Закону було створення в Україні правової бази для одержання та використання науково-технічної інформації. Законом регулюються правові і економічні відносини громадян, юридичних осіб, держави, що виникають при створенні, одержанні, використанні та поширенні науково-технічної інформації, а також визначаються правові форми міжнародного співробітництва в цій галузі. Дія Закону поширюється на підприємства, установи, організації незалежно від форм власності, а також громадян, які мають право на одержання, використання та поширення науково-технічної інформації [45].

Закон України «Про захист інформації в автоматизованих системах» (1994 р.) є одним із перших нормативних актів, спрямованих на забезпечення безпеки інформації. Цей Закон регулює відносини у сфері захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах [46].

Стаття 2 Закону визначає, що об'єктами захисту в системі є інформація, що обробляється в ній, та програмне забезпечення, яке призначено для обробки цієї інформації.

Закон України «Про захист інформації в автоматизованих системах» у 2005 році був перейменований на «Про захист інформації в інформаційно-комунікаційних системах» [49].

Закон України «Про концепцію Національної програми інформатизації» частково розв'язував частину завдань, поставлених Президентом України. Закон містив: характеристику стану інформатизації України на початок 1998 р.; загальні принципи державної політики у сфері інформатизації; ви-значення суті, головної мети та основних завдань Національної програми інформатизації; принципи формування та виконання Національної програми інформатизації; основні напрями інформатизації; очікувані наслідки реалізації програми [12].

У законі загальний стан процесів інформатизації (рівень 2-2,5%) в Україні визнавався незадовільним на фоні кризових явищ в економіці. Вказувалось, що значне технологічне відставання перетворило Україну з виробника сучасних електронних обчислювальних машин на споживача застарілих іноземних моделей засобів обчислювальної техніки; у 1992-1996 рр. порівняно з 1991 р. знизився на 90% рівень промислового виробництва мікроелектроніки; недостатньою є пропускна здатність та низька якість телекомунікаційних систем і мереж передачі даних. Загальні принципи інформатизації України були визначені у розділі III закону, де констатувалося, що державна політика інформатизації є складовою соціально-економічної політики держави в цілому; державне регулювання

процесів інформатизації має проводитися на засадах системності, комплексності й узгодженості; на реалізацію загальнодержавних проектів інформатизації (національна інформаційно-телекомунікаційна система, система національних інформаційних ресурсів, інформатизація економіки, соціальної сфери та оборони) направляються бюджетні кошти; плануються реформування власності, концентрація необхідної кількості державних об'єктів інфраструктури інформатизації та підтримка малих і середніх підприємств; визначаються пріоритетні сфери та напрями концентрації фінансових, матеріальних і трудових ресурсів, причому пріоритети коригуються залежно від ситуації; надається інформаційна підтримка заходам виходу України з кризи, державним органам та пріоритетним галузям економіки; першочерговим вважається створення нормативно-правової бази інформатизації, включаючи систему захисту авторських прав і особистої інформації; розроблення національних стандартів у галузі інформатизації; формування телекомунікаційної інфраструктури, перш за все оптимізація діючої мережі магістралей передачі даних; будівництво нових сучасних каналів, включаючи волоконно-оптичні та супутникові системи зв'язку; формування комп'ютерної мережі освіти, науки та культури як частини загальносвітової мережі Інтернет; здійснення заходів щодо інформаційної безпеки; створення вітчизняної конкурентоздатної виробничої бази засобів обчислювальної техніки; одержання бюджетних інвестицій тільки тими національними виробниками, які можуть забезпечити збільшення обсягів виробництва за рахунок кінцевого продукту, послуг, чистого експорту чи створення продукції, що замінює імпортовану; застосування антимонопольних заходів як на стадії коригування Програми, так і під час її реалізації; всебічна демократизація процесів створення та споживання інформації, загальнодоступність інформаційних ресурсів та послуг, захист прав особи від інформаційного вторгнення.

У законі Програма інформатизації визначається як комплекс взаємопов'язаних окремих завдань (проектів) інформатизації, спрямованих на

реалізацію державної політики та пріоритетних напрямів створення сучасної інформаційної інфраструктури України за рахунок концентрації та раціонального використання фінансових, матеріально-технічних та інших ресурсів, виробничого та науково-технічного потенціалу держави, а також координації діяльності органів державної влади та органів місцевого самоврядування, підприємств, установ, організацій усіх форм власності та громадян у сфері інформатизації. Головною метою Програми є забезпечення громадян та суспільства своєчасною, достовірною та повною інформацією на основі широкого використання інформаційних технологій та забезпечення інформаційної безпеки держави [12].

Закон України «Про Національну програму інформатизації» визначив механізм формування, виконання та корегування Національної програми інформатизації, яка включає Концепцію Національної програми інформатизації; сукупність державних програм з інформатизації; галузеві та регіональні програми та проекти інформатизації; програми та проекти інформатизації органів місцевого самоврядування. Суб'єктами національної програми є замовники та виконавці робіт з інформатизації; організації, що здійснюють експертизу окремих завдань та проектів інформатизації; користувачі автоматизованих та інших інформаційних систем і засобів інформатизації.

Порядок представлення та затвердження Національної програми інформатизації передбачає, що Кабінет Міністрів України щорічно разом з проектом Закону України про Державний бюджет України подає на розгляд Верховної Ради України доповідь про стан інформатизації в Україні; програму завдань з інформатизації на наступний бюджетний рік із визначенням джерел фінансування, завдання Національної програми інформатизації на наступні три роки, зміст та обсяги бюджетного фінансування яких на наступний рік затверджуються Верховною Радою України. Кабінет Міністрів України має у тримісячний термін вжити заходів щодо узгодження національного законодавства згідно з даним законом.

На відміну від вищерозглянутих законів, Закон України «Про Основні засади розвитку інформаційного суспільства на Україні на 2007 — 2015 роки» встановив строки своєї дії [77]. У ньому зазначено, що одним з головних пріоритетів України є прагнення побудувати орієнтоване на інтереси людей, відкрите для всіх і спрямоване на розвиток інформаційне суспільство, в якому кожен міг би створювати і накопичувати інформацію та знання, мати до них вільний доступ, користуватися і обмінюватися ними, мати можливість повною мірою реалізувати свій потенціал, сприяючи суспільному і особистому розвиткові та підвищуючи якість життя.

У законі визначені основні стратегічні цілі інформаційного суспільства в Україні: прискорення розробки та впровадження новітніх конкурентоспроможних інформаційно- комп'ютерних технологій (ІКТ) в усі сфери суспільного життя, зокрема в економіку України і в діяльність органів державної влади та органів місцевого самоврядування; забезпечення комп'ютерної та інформаційної грамотності населення, насамперед шляхом створення системи освіти, орієнтованої на використання новітніх ІКТ у формуванні всебічно розвиненої особистості; розвиток національної інформаційної інфраструктури та її інтеграція зі світовою інфраструктурою; державна підтримка нових «електронних» секторів економіки (торгівлі, надання фінансових і банківських послуг тощо); створення загальнодержавних інформаційних систем, насамперед у сферах охорони здоров'я, освіти, науки, культури, охорони довкілля; збереження культурної спадщини України шляхом її електронного документування; державна підтримка використання новітніх ІКТ засобами масової інформації; використання ІКТ для вдосконалення державного управління, становлення електронних форм взаємодії між органами державної влади і місцевого самоврядування та фізичними й юридичними особами; ефективна участь всіх регіонів у процесах становлення інформаційного суспільства шляхом децентралізації та підтримки регіональних і місцевих ініціатив; за-хист інформаційних прав громадян, насамперед щодо доступності інформації,

захисту інформації про особу, підтримки демократичних інститутів та мінімізації ризику «інформаційної нерівності»; вдосконалення законодавства з регулювання інформаційних відносин (декларується необхідність прийняття інформаційного кодексу); покращення стану інформаційної безпеки в умовах використання новітніх ІКТ. Слід, проте, зазначити, що у тексті даного нормативно-правового акту відсутні офіційне визначення «інформаційного суспільства» та його основні показники [77].

Підсумовуючи, варто зазначити, що законодавство про Національну програму інформатизації носило декларативний характер, оскільки поняття «програма» у науковій, правовій та економічній сферах передбачає не лише визначення загальних принципів, а й чітке формулювання конкретних завдань, призначення відповідальних осіб, виділення необхідних ресурсів, встановлення строків реалізації та механізмів звітності з оцінкою досягнутих результатів.

Вкрай важливе значення для впровадження електронних технологій у всіх сферах суспільного життя України мало прийняття у 2003 році Закону України «Про електронний цифровий підпис» [48], який створив підґрунтя для використання електронних підписів у документообігу та заклав основу для подальшого впровадження електронних технологій у всіх сферах суспільного життя.

Закон визначив, що електронний цифровий підпис має юридичну силу, якщо він відповідає спеціальним встановленим вимогам. Це стало ключовим фактором для впровадження електронного документообігу, оскільки: електронний цифровий підпис (далі - ЕЦП) забезпечив автентичність, цілісність і недоторканність електронних документів. Закон закріпив правовий статус ЕЦП як аналог власноручного підпису в паперових документах.

Прийняття закону дозволило застосовувати електронні підписи у всіх сферах, зокрема в публічному управлінні, бізнесі, банківських операціях, укладенні договорів, податковому обліку тощо. Це сприяло прискоренню

обміну інформацією між державними органами, підприємствами та громадянами, а також оптимізації процесів документообігу, особливо в державному секторі.

Закон закріпив поняття акредитованого центру сертифікації ключів, який відповідає за генерацію, управління ключами електронного підпису та видачу сертифікатів відкритих ключів, що підтверджують автентичність підпису. Це сприяло підвищенню рівня безпеки та довіри до електронних підписів у взаємодії між учасниками цифрового середовища.

Документ також встановив обов'язкове застосування криптографічного захисту для створення та перевірки електронного підпису, що значно знизило ризики несанкціонованого доступу та підробки цифрових підписів, тим самим забезпечивши довіру громадян до електронних документів.

Впровадження цього закону відіграло ключову роль у розвитку електронного документообігу в державному секторі, дозволило зменшити адміністративні витрати, сприяло розбудові електронного врядування, зокрема через можливість подання податкових декларацій в онлайн-режимі, та створило передумови для подальшого впровадження інноваційних інформаційних технологій в Україні.

Загалом можна стверджувати, що цей Закон став каталізатором розвитку цифрової інфраструктури, електронного врядування та електронної комерції. Цей нормативний акт фактично заклав основу для подальшого впровадження електронних технологій у всіх сферах суспільного життя України.

Всі вищерозглянуті нормативно-правові акти визначають інформатизацію як одну зі стратегічних цілей розвитку української держави та побудови інформаційного суспільства, а також деталізують права і свободи людини в інформаційній сфері. Однак їхні положення сформульовані надто узагальнено, а в окремих аспектах навіть дублюються. У документах не визначено конкретних показників, яких слід досягти, не зазначено, скільки фахівців потрібно підготувати та упродовж якого періоду,

які саме обчислювальні засоби та інформаційні технології необхідно використовувати, а також які зміни доцільно внести до чинного законодавства. Визначення цих завдань, які фактично є конкретизованими принципами, покладається на щорічні програми інформатизації.

Водночас процес формування національного законодавства супроводжувався поступовим створенням державних органів, відповідальних за регулювання у сфері інформаційних технологій. Так, у 2000 році була заснована Державна служба спеціального зв'язку та захисту інформації України, яка відіграє ключову роль у забезпеченні кібербезпеки та захисті державної інформаційної інфраструктури.

Незважаючи на революційний розвиток адміністративно-правового регулювання інформаційних технологій в Україні проблемами цього періоду можна виділити: відсутність цілісної стратегії розвитку інформаційних технологій, розгалуженість законодавства та недостатня увага до гармонізації національного законодавства із міжнародними стандартами.

3. Сучасний період цифрової трансформації (з 2010 р.)

Цей етап адміністративно-правового регулювання інформаційних технологій в Україні розпочався зі зростання уваги до цифровізації як ключового напряму розвитку держави. Прийняття низки стратегічних документів та законів заклало основу для розвитку цифрових технологій у публічному управлінні, бізнесі та суспільному житті України.

Сучасний період цифрової трансформації характеризується впровадженням електронного урядування та наданням публічних електронних послуг. Проте на початку цього етапу розбудова інформаційного суспільства в Україні не відповідала потребам та можливостям держави, відбувалося гальмування розвитку інформаційної сфери. З метою усунення вищезгаданих недоліків у 2013 році КМ України видав розпорядження «Про схвалення стратегії розвитку інформаційного суспільства в Україні» [50].

Документ акцентував увагу на необхідності вдосконалення нормативної бази для розвитку інформаційної сфери, впровадження механізмів електронної демократії та цифрового врядування, реалізації заходів для стимулювання електронної економіки, підвищення рівня інформаційної обізнаності громадян, покращення якості адміністративних послуг, а також зміцнення інформаційної безпеки.

У 2014 році утворено Державне агентство з питань електронного урядування. Це орган виконавчої влади, завданнями якого було впровадження політики Уряду країни з метою розвитку інформаційного суспільства, використання електронних інформаційних ресурсів, ширшого впровадження електронних послуг та сервісів, цифровізації центральних та місцевих органів влади [51].

Першочергові завдання та проекти «цифровізації» України до 2020 року викладені у документі «Цифрова адженда України-2020» [52], який розроблений у 2016 році представниками Міністерства економічного розвитку й торгівлі України, Державного агентства з питань електронного урядування, компаній-лідерів світового цифрового ринку, громадських організацій, асоціацій та консалтингових компаній.

Автори виділили стратегічні цілі, підходи до впровадження та інструменти для стимулювання розвитку цифровізації в наступних сферах: економіка, публічне управління, освіта, національна кібербезпека, суспільно-економічна діяльність (охорона здоров’я, наука, соціальна сфера, електронна демократія, електронне урядування, електронна комерція, електронні платежі).

Спираючись на ухвалений у 2016 році проект цифрової трансформації країни, у січні 2018 року Кабінетом Міністрів було затверджено «Концепцію розвитку цифрової економіки та суспільства України на 2018–2020 роки». Вона передбачала вдосконалення цифрової інфраструктури, підвищення рівня цифрової грамотності громадян, впровадження цифрових технологій на робочих місцях, а також масштабні трансформації в сферах громадської

безпеки, охорони довкілля, міського розвитку. Окрему увагу було приділено гармонізації з європейськими та глобальними науковими ініціативами [53].

У серпні 2019 року було утворено Комітет Верховної Ради України з питань цифрової трансформації, до компетенції якого віднесено законодавче забезпечення цифрового розвитку країни, використання мережі Інтернет, реалізацію державних програм інформатизації, участь у європейських цифрових ініціативах, розвиток цифрового підприємництва, телекомунікаційної інфраструктури, кібербезпеки, впровадження системи «відкритих даних» та формування цифрових компетентностей.

У вересні 2019 року на основі реорганізації Державного агентства з питань електронного урядування було утворено Міністерство цифрової трансформації України. Його ключовими завданнями стали формування та реалізація державної політики у сфері цифрового розвитку, електронного врядування, цифрових послуг, інноваційних технологій, а також підтримка ІТ-сектору та сприяння цифровізації економіки [54].

Саме Міністерство цифрової трансформації України (Мінцифра) стало ініціатором і розробником загальновідомого національного цифрового сервісу, який об'єднує електронні державні послуги та цифрові документи.

Системний портал «Дія» (що скорочено від «Держава і я») було офіційно представлено у 2020 році, що стало епохальною подією та значним досягненням України сучасного періоду цифрової трансформації. Ця система складається із інтернет-порталу, мобільного застосунку та цифрових платформ. «Дія» являє собою інформаційно-аналітичну систему та платформу, що була створена українським урядом для поліпшення надання державних послуг та забезпечення взаємодії між державою та громадянами, а також для забезпечення ефективного управління державними ресурсами [121].

Сутність програми «Дія» включає ряд аспектів, що мають невід’ємний вплив на суспільне життя. А саме централізована платформа «Дія» об’єднує в одному місці доступ до різноманітних державних послуг та ресурсів.

Громадяни та бізнес можуть отримати доступ до цих послуг онлайн через веб-сайт або мобільний додаток. «Дія» надає доступ до різних електронних сервісів, таких як замовлення паспорта, реєстрація транспортних засобів, подання декларацій тощо. Це дозволяє спростити та прискорити багато адміністративних процедур [121].

Кожен громадянин має можливість створити свій електронний кабінет на платформі «Дія». Це дає змогу здійснювати онлайн-звернення до органів влади, відслідковувати статуси звернень та виконувати інші адміністративні процедури. Взаємодія з органами влади дозволяє громадянам та бізнесу подавати скарги та пропозиції, слідкувати за відповідями та реагувати на них. Велике значення в інформаційному середовищі має доступ до можливості отримати аналітичні дані та мати до них доступ.

Платформа надає аналітичні дані для покращення управління державними ресурсами та послугами. Дані також робляться відкритими для громадськості з метою забезпечення більшої прозорості та відповідальності [121].

Попри значні досягнення та переваги, ця система зіштовхнулася з низкою викликів. Зокрема, частина населення, особливо у віддалених регіонах, досі не має стабільного доступу до швидкісного інтернету або сучасних мобільних пристроїв, що ускладнює повноцінне користування цифровими послугами. Крім того, зростаючі загрози кібератак на державну цифрову платформу вимагають постійного вдосконалення механізмів кіберзахисту та підвищеної уваги з боку держави.

Ще одним викликом залишається недостатній рівень цифрової грамотності окремих верств населення, зокрема осіб старшого віку, що уповільнює їхню адаптацію до нових цифрових сервісів.

Попри ці труднощі, запуск платформи «Дія» став вагомим кроком у цифровій трансформації публічного управління. Вона заклала основу для створення відкритої, ефективної та доступної системи адміністративних послуг, значно покращивши комунікацію між державою, громадянами та

бізнесом. Окрім того, «Дія» стала символом сучасних змін у сфері публічного адміністрування України та прикладом для інших країн, що прагнуть цифровізувати свої державні сервіси.

Серед головних законодавчих досягнень сучасного періоду цифрової трансформації України необхідно окремо виділити: Закон України «Про основні засади забезпечення кібербезпеки України» (2017 р.) та Закон України «Про електронні довірчі послуги» (2018 р.).

Прийняття Закону України «Про основні засади забезпечення кібербезпеки України» (2017 р.) [80] стало важливим етапом у формуванні національної системи кібербезпеки та адаптації до сучасних викликів у сфері інформаційної безпеки.

Прийнятий закон став фундаментом для формування, функціонування та модернізації національної системи кібербезпеки. Він визначив ключові принципи, серед яких: пріоритетний захист національних інтересів у кіберпросторі, координація взаємодії державних органів, бізнесу та громадян, а також дотримання прав і свобод людини під час здійснення заходів у сфері кібербезпеки.

Документ чітко розподілив повноваження між органами державної влади, відповідальними за кібербезпеку. Так, координацію політики у цій сфері здійснює Рада національної безпеки і оборони України, тоді як Служба безпеки України займається протидією кіберзагрозам, що мають терористичний або шпигунський характер. Державна служба спеціального зв’язку та захисту інформації відповідає за технічну безпеку інформаційних ресурсів та реагування на інциденти, а Національна поліція України – за розслідування кіберзлочинів. Такий розподіл функцій сприяв створенню системного підходу до захисту кіберпростору.

Закон також окреслив перелік загроз, що вимагають негайного реагування, серед яких: атаки на критичну інфраструктуру, несанкціоноване втручання в державні інформаційні системи, поширення дезінформації через

кіберпростір. Це дозволило сфокусувати зусилля держави на пріоритетних напрямах забезпечення кібербезпеки.

Документ зобов'язав державні та приватні суб'єкти, які відповідають за функціонування критично важливої інфраструктури, застосовувати відповідні заходи кіберзахисту. Це сприяло посиленню безпеки у сферах енергетики, фінансів, транспорту, медіа, публічного управління та впровадженню міжнародних стандартів захисту інформації.

Закон став основою для протидії новим загрозам, таким як кібератаки, кібершпигунство, кіберзлочинність і кібертероризм. Він посприяв зміцненню безпеки стратегічно важливих секторів, гармонізації українського законодавства із європейськими та міжнародними стандартами, а також підвищенню загального рівня стійкості країни до сучасних кіберзагроз.

Окрім того, відповідний нормативно-правовий акт визнав важливість міжнародного партнерства в сфері кібербезпеки, включаючи участь України в програмах НАТО з кіберзахисту та співпрацю з ЄС у межах Угоди про асоціацію, зокрема, імплементацію стандартів кібербезпеки ЄС.

Загалом, цей Закон став фундаментом для побудови стійкої національної системи кібербезпеки в умовах зростаючих загроз у цифровому просторі.

Прийняття Закону України «Про електронні довірчі послуги» (2017 р.) [62] мало ключове значення для формування сучасного електронного середовища в Україні. Його вплив був відчутним у багатьох аспектах цифрової трансформації держави, бізнесу та суспільства.

У грудні 2022 року були внесені суттєві зміни до Закону України, які відобразились в тому числі і в оновленій назві Закону — «Про електронну ідентифікацію та електронні довірчі послуги» [62].

Нова назва Закону розширила предмет його регулювання, охоплюючи не лише довірчі послуги, але й процеси електронної ідентифікації.

Цей закон закріпив рівність електронних документів із паперовими, що забезпечує їх використання в адміністративних процедурах, що спростило взаємодію громадян із державними органами та підприємствами.

Крім того, цей законодавчий акт заклав правові засади для функціонування системи електронної ідентифікації. Завдяки впровадженню механізмів електронної ідентифікації стало можливим здійснювати автентифікацію осіб без їхньої фізичної присутності, що значно полегшило автоматизацію адміністративних процесів, таких як реєстрація, подання заяв та отримання послуг.

Документ відіграє ключову роль й у забезпеченні кібербезпеки, оскільки гарантує, що всі процеси електронної ідентифікації та застосування довірчих послуг відповідають стандартам кіберзахисту. Це сприяє мінімізації ризиків несанкціонованого доступу до конфіденційної інформації.

Закон також сприяв підвищенню прозорості та ефективності адміністративних процедур в Україні. Запровадження електронного документообігу та використання цифрових підписів допомагає зменшити корупційні ризики, спрощує процес адміністрування та значно скорочує витрати часу й ресурсів, необхідних для виконання управлінських функцій.

Важливе значення цей нормативний акт має і для підприємницького сектору, оскільки забезпечує зручні інструменти взаємодії бізнесу з державними органами. Зокрема, це стосується подання звітності, укладання договорів та інших юридичних процедур, що сприяє розвитку цифрової економіки та оптимізації ділових процесів.

Таким чином, Закон України «Про електронну ідентифікацію та електронні довірчі послуги» є важливим нормативно-правовим актом, що визначає сучасний етап розвитку адміністративно-правового регулювання інформаційних технологій, так як сприяє цифровій трансформації публічного управління, забезпечує прозорість, ефективність і безпеку адміністративних процесів, а також інтеграцію України в цифровий простір ЄС.

Сучасний період адміністративно-правового регулювання інформаційних технологій в Україні вирізняється активною цифровою трансформацією публічного управління. Разом із тим, цей процес супроводжується низкою викликів, серед яких можна виокремити: необхідність системної протидії кіберзагрозам, особливо в умовах військової агресії з боку РФ; труднощі у фінансуванні цифрових ініціатив; а також потребу в комплексному узгодженні національного законодавства із сучасними тенденціями стрімкого розвитку інформаційних технологій.

Підводячи підсумки, необхідно вказати, що еволюція адміністративно-правового регулювання інформаційних технологій в Україні є прикладом поступового переходу від локальних ініціатив до комплексної системи цифрового управління. У сучасний період Україна демонструє значний прогрес у впровадженні цифрових технологій завдяки стратегічному підходу до реформ у цій сфері. Однак подальший розвиток вимагає посилення законодавчої бази, інтеграції з міжнародними стандартами та подальше впровадження інновацій у публічне управління.

1.3 Нормативно-правові основи регулювання використання інформаційних технологій

Формування ефективної нормативно-правової бази у сфері інформаційних технологій є одним із пріоритетних завдань сучасної правової політики України. Розвиток інформаційного суспільства, цифровізація суспільних процесів та інтеграція України у міжнародний правовий простір зумовлюють необхідність дослідження й удосконалення нормативного регулювання цій сфері.

Стрімкий розвиток суспільних відносин вимагає від держави постійної розробки, вдосконалення та оновлення нормативно-правової бази України, створення спеціальних юридичних норм, правил для регулювання сфери інформаційних відносин.

Наразі в Україні існує значна кількість нормативно-правових актів, які регулюють відносини в сфері інформаційних технологій. Однак багато з них потребують внесення змін та доповнень, оскільки вони не завжди коректно взаємодіють між собою та не можуть ефективно вирішувати виклики сучасного періоду цифрової трансформації України.

Нормативно-правову основу регулювання використання інформаційних технологій в Україні складають наступні напрями державної політики: впровадження електронного документообігу, забезпечення захисту персональних даних та забезпечення кібербезпеки.

Запровадження електронного документообігу в Україні є одним із актуальних й важливих напрямів розвитку інформаційного суспільства. Його інтеграція в управлінські процеси набуває особливого значення в умовах активного впровадження цифрових технологій, що сприяє підвищенню ефективності організацій та їх конкурентоспроможності. Україна нині перебуває на етапі поступового переходу від паперової форми документообігу до цифрової, що обумовлено зростанням обсягів бізнес-операцій, необхідністю забезпечення збереження даних, підвищенням рівня конфіденційності та інформаційної безпеки. Раціональне впровадження та вдосконалення електронного документообігу сприятиме оптимізації робочих процесів, зменшенню витрат і відповідності сучасним нормативним вимогам.

Л. Асанова наголошує, що перевага електронного документообігу виявляється через можливість відправляти вихідні документи, що створюються та підписуються в установі в електронному вигляді через систему електронної взаємодії органів виконавчої влади, що значно прискорює надходження документа до адресата, а також зменшує вартість послуги у разі відправлення службового листа у паперовому вигляді [55, с. 157].

Впровадження систем електронного документообігу є комплексним і багатогранним процесом, що супроводжується численними викликами та перспективами. Успішна реалізація цього процесу потребує детального

аналізу та глибокого розуміння чинної нормативно-правової бази. Важливе значення в дослідженні питань організації електронного документообігу та роботи з цифровими документами має українське законодавство та відповідні нормативно-правові акти.

У 2000 році Президент України підписав Указ «Про заходи щодо розвитку національної складової глобальної інформаційної мережі Інтернет та забезпечення широкого доступу до цієї мережі в Україні». Цей документ визначив розвиток національної складової Інтернету та забезпечення доступу до неї для громадян і юридичних осіб як один із ключових пріоритетів державної політики у сфері інформатизації. Відповідно до положень Указу, основними напрямами роботи стали розбудова інфраструктури інформаційних послуг на базі Інтернету та впровадження передових інформаційних технологій у систему державного управління [56].

Серед інших важливих нормативно-правових актів, що регулюють сферу інформатизації, особливу роль відіграє Постанова Кабінету Міністрів України «Про порядок розміщення інформації про діяльність органів виконавчої влади в мережі Інтернет». Цей документ визначає механізми оприлюднення відомостей про функціонування органів виконавчої влади в онлайн-просторі з метою підвищення прозорості та ефективності їхньої роботи. Впровадження сучасних інформаційних технологій сприяє відкритому доступу громадян до офіційної інформації та державних послуг [57].

Розміщення інформації щодо діяльності державних органів у мережі Інтернет реалізується через: постійне оновлення та підтримку веб-сайтів міністерств, центральних і місцевих органів виконавчої влади відповідно до встановлених вимог; створення та розвиток Єдиного веб-порталу Кабінету Міністрів України, який забезпечує інтеграцію офіційних сайтів державних установ та надає громадянам доступ до актуальних інформаційних ресурсів [57].

Як зазначає В. Петрович, завдяки використанню установами сучасної автоматизованої інформаційної системи документообігу та контролю формується централізована база документів, актів, рішень і окремих доручень та інформації про хід їхнього виконання, яка доступна у будь-який період часу, зменшується час на виконання рутинних операцій, особливо щодо пошуку документів і зв'язаної з ними інформації [58, с. 97].

Також, В. Петрович звертає увагу на те, що ефективна діяльність органів державної влади та місцевого самоврядування в умовах російсько-української війни, коли щоденно неймовірно зростає кількість внутрішньо переміщених осіб, а люди втрачають свої паперові документи і змушені покинути постійне місце проживання, великою мірою залежить від налагодження чіткої системи комунікації, особливо електронної [58, с. 98].

На думку О. Лаби, концепція електронного урядування складається з двох взаємопов'язаних та самостійних частин: внутрішня урядова інформаційна інфраструктура, що подібна до корпоративної мережі, та зовнішня інформаційна інфраструктура, яка взаємодіє з громадянами та організаціями [59, с. 141].

З метою підвищення продуктивності роботи органів державної та місцевої влади в рамках Національної програми інформатизації передбачається об'єднання існуючих і майбутніх інформаційних систем цих органів в один цілісний інформаційно-аналітичний комплекс – Інтегровану інформаційно-аналітичну систему органів державної та місцевої влади України. З урахуванням різноманітності існуючих систем електронного документообігу в органах державної та місцевої влади, передбачається створення єдиної системи електронного документообігу.

Метою цієї системи, як зазначає О. Лаба, є забезпечення швидкості обігу документів (указів, постанов, законів, розпоряджень, повідомлень, звітів, аналітичних довідок тощо), а також зменшення часу, необхідного для прийняття рішень шляхом автоматизації процесів колективного створення та використання документів у державних органах [59, с. 142].

Правовий статус електронного документа та електронного документообігу закріплені у Законах прийнятих Верховною Радою України «Про електронні документи та електронний документообіг» [61], «Про електронні довірчі послуги» [62], «Про електронну комерцію» [63], «Про обов'язковий примірник документів» [64], «Про Національну програму інформатизації» [60], «Про електронні комунікації» [65], «Про Національну систему конфіденційного зв'язку» [66], «Про захист інформації в інформаційно-телекомунікаційних системах» [46], тощо. Проте, на сьогодні відсутній єдиний нормативний акт, який би повноцінно регулював взаємовідносини у сфері систем електронного документообігу.

Закон України «Про електронні документи та електронний документообіг» визначив основні принципи електронного документообігу та використання електронних документів. Згідно з цим законом, електронний документ – це документ, де інформація зберігається у вигляді електронних даних, включаючи всі необхідні реквізити, зокрема, електронний цифровий підпис [61].

Електронний формат документа не може бути підставою для заперечення його юридичної сили. Водночас законодавство передбачає певні обмеження щодо використання електронних документів у якості оригіналів. Зокрема, свідоцтво про право на спадщину не може бути видане виключно в електронному вигляді, так само як і інші документи, що відповідно до норм права мають існувати лише в одному примірнику. Це обмеження діятиме до впровадження централізованої системи зберігання оригіналів електронних документів.

У 2018 році набрав чинності Закон України «Про електронні довірчі послуги» (пізніше назва Закону була змінена на «Про електронну ідентифікацію та електронні довірчі послуги»), який став важливим етапом у формуванні правової основи для використання інформаційних технологій в Україні, спрямованих на підтримку електронного документообігу, розвитку цифрових сервісів та інтеграцію до європейського цифрового простору. Цей

нормативно-правовий акт забезпечує регулювання ключових аспектів використання електронних довірчих послуг та електронної ідентифікації [62].

Закон визначив порядок електронної ідентифікації осіб через різні засоби, такі як електронні підписи, електронні печатки, системи BankID, MobileID тощо. Механізми ідентифікації забезпечують: автентифікацію особи в цифровому середовищі; зручний доступ до електронних державних послуг; інтеграцію з європейськими системами ідентифікації згідно з eIDAS Regulation.

Цей закон регламентує основні види довірчих послуг, зокрема: створення, перевірку та зберігання електронних підписів і печаток; часове позначення електронних документів; реєстрацію та перевірку електронних сертифікатів; забезпечення цілісності даних у цифровому форматі.

Закон встановлює вимоги до постачальників електронних довірчих послуг, зокрема: необхідність сертифікації та акредитації; відповідальність за забезпечення безпеки та надійності послуг; механізми моніторингу та контролю за діяльністю таких суб’єктів.

Відповідний закон закріплює принцип, згідно з яким електронний документ, підписаний кваліфікованим електронним підписом, має таку ж юридичну силу, як і паперовий документ, підписаний власноруч.

Завдяки правовому врегулюванню електронної ідентифікації та довірчих послуг громадяни можуть отримувати державні послуги онлайн, що мінімізує необхідність особистої присутності у державних установах.

Закон України «Про електронну ідентифікацію та електронні довірчі послуги» став фундаментом для розвитку цифрових технологій у правовій та економічній сферах. Його реалізація сприяє зростанню ефективності електронного урядування, підвищенню конкурентоспроможності України на міжнародному ринку та створенню умов для формування цифрового суспільства. Разом із тим, вдосконалення його положень залишається важливим завданням для забезпечення динамічного розвитку ІТ-сфери в Україні.

Для врегулювання питань, пов’язаних із впровадженням електронного урядування в Україні, у 2003 році Кабінет Міністрів України ухвалив Постанову «Про заходи щодо створення електронної інформаційної системи «Електронний уряд». Відповідно до цього документа, передбачалося розроблення необхідних нормативно-правових підстав для функціонування системи «Електронний уряд», а також забезпечення громадян і юридичних осіб швидким та зручним доступом до інформаційних послуг через цю систему. Модель електронного уряду спрямована на підвищення ефективності комунікації між органами виконавчої влади, громадянами та бізнесом шляхом використання сучасних інформаційних технологій. Крім того, система передбачає інтеграцію державних електронних інформаційних ресурсів і платформ у Єдиний веб-портал органів виконавчої влади, що сприяє більшій прозорості та доступності державних послуг. [].

Окрім того, одним із основних документів, якими керуються державні органи є Постанова Кабінету Міністрів України 2018 року «Деякі питання документування управлінської діяльності», якою затверджено «Типову інструкцію із документування управлінської інформації у електронній формі й організації роботи із електронними документами у діловодстві, електронного міжвідомчого обміну», «Типову інструкцію із діловодства у міністерствах, інших центральних й місцевих органах виконавчої влади», «Регламент організації взаємодії органів виконавчої влади у електронній формі». За даними документами визначається: порядок проходження електронного документа із моменту його створення, відправлення чи отримання до моменту передавання до архівного відділу; засади організації документування управлінської інформації у електронній формі для структурних підрозділів, що тимчасово створюють документи в паперовій формі; загальні засади функціонування й застосування системи електронної взаємодії органів виконавчої влади; оперативний інформаційний обмін із застосуванням службової електронної пошти [67].

Як зазначає В. Петрович, процес формування й реалізації державної політики з впровадження системи електронного документообігу вимагає утворення відповідної належної нормативно-правової бази. Із затвердженням удосконалених правил, що регламентуватимуть процеси створення електронних документів та їх обіг в електронних системах, особлива увага має бути зосереджена на їх дієвому застосуванні й забезпеченні якості документів [69, с. 12].

Іншим ключовим напрямом державної політики та складовою нормативно-правової основи регулювання використання інформаційних технологій в Україні є питання забезпечення захисту персональних даних.

У сучасних розвинених країнах стандарти захисту персональних даних знаходяться на високому рівні та постійно вдосконалюються відповідно до динаміки розвитку державних і суспільних процесів. Це є реакцією держави на потребу правового врегулювання відносин, що виникають у сфері обробки та збереження персональної інформації. В українському законодавстві, незважаючи на наявність певних нормативно-правових актів, досі не закріплено створення спеціального органу, відповідального за захист персональних даних, який би забезпечував ефективне функціонування механізму їхнього захисту відповідно до міжнародних стандартів та мав контрольні повноваження у цій сфері. Попри певні законодавчі ініціативи, соціологічні дослідження та аналітичні звіти уповноважених органів демонструють недостатній рівень захисту персональних даних в Україні.

Водночас, попри необхідність подальшого вдосконалення механізмів захисту персональної інформації, вітчизняне законодавство все ж містить діючі організаційно-правові засоби регулювання цієї сфери. Цей механізм охоплює нормативно-правові акти, що регулюють відносини у сфері захисту персональних даних, а також інструменти забезпечення їх ефективного застосування та контроль за дотриманням встановлених вимог. Зокрема, Конституція України (ст. 21, 31, 32) гарантує рівність усіх осіб у правах і гідності, передбачає невідчужуваність і непорушність основних прав і свобод

людини. Вона також містить положення, що забороняють будь-яке втручання у приватне та сімейне життя громадян, крім випадків, передбачених законом. Крім того, збір, зберігання, використання та поширення конфіденційної інформації про особу можливі лише за її згодою, за винятком випадків, визначених законодавством, та лише в інтересах національної безпеки, економічного розвитку та захисту прав людини [34].

Кожному гарантується право на захист від втручання в особисте життя, таємницю листування, телефонних розмов, кореспонденції (також і електронних листів) та іншої інформації, що відноситься до персональних даних. Саме ці конституційні норми є основою для подальшої розробки та вдосконалення вітчизняного законодавства у сфері захисту персональних даних [34].

Основним нормативно-правовим актом, що комплексно регулює правові відносини у сфері захисту персональних даних, є Закон України «Про захист персональних даних» [70].

Дія цього закону охоплює питання правового регулювання збору, обробки та збереження персональних даних і спрямована на гарантування основоположних прав і свобод людини та громадянина, зокрема права на недоторканність приватного життя у зв’язку з обробкою персональної інформації. Цей закон є важливим інструментом правового захисту, що закріплює фундаментальні права людини, передбачені Конституцією України.

Закон визначає, що кожна фізична особа має невід’ємне та непорушне право на захист своїх персональних даних. Кожен громадянин має гарантії щодо захисту від незаконного оброблення, випадкової втрати, знищення чи пошкодження персональних даних, а також від приховування або несвоєчасного надання інформації. Крім того, особа має право на захист від поширення недостовірних відомостей, які можуть завдати шкоди її честі, гідності або діловій репутації.

Громадяни мають право звертатися до органів державної влади, місцевого самоврядування та уповноважених установ, відповідальних за захист персональних даних, з метою захисту своїх прав. У разі порушення законодавства про захист персональної інформації особа може використовувати передбачені правові механізми захисту.

Окрім зазначеного закону, питання захисту персональних даних регулюються також кодифікованими нормативно-правовими актами, зокрема положеннями Кримінального кодексу України, Цивільного кодексу України та Кодексу України про адміністративні правопорушення, які містять норми щодо відповідальності за незаконне використання та розповсюдження персональної інформації.

Кримінальний кодекс України [71] містить декілька норм закону щодо захисту персональних даних. Так, статтею 163 передбачено кримінальну відповідальність за порушення таємниці кореспонденції, телефонних розмов, телеграфної чи іншої кореспонденції, що передаються засобами зв'язку або через комп'ютер. Саме цими шляхами люди можуть передавати свої персональні дані конкретній фізичній чи юридичній особі, однак не бажаючи, щоб вони повторно були передані третім особам. Стаття 182 Кодексу визнає злочином незаконне збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди або поширення цієї інформації у публічному виступі, творі, що публічно демонструється, чи в засобах масової інформації. Особі, щодо якої було вчинено дії, визначені у цих статтях, гарантовано право на судовий захист. Володільці баз персональних даних повинні використовувати їх виключно в межах закону.

У Цивільному кодексі України [72] законодавець відніс персональні дані до особистих немайнових прав та визначив спосіб їх захисту від протиправних посягань у судовому порядку. Зміст особистого немайнового права становить можливість фізичної особи вільно, на власний розсуд визначати свою поведінку у сфері свого приватного життя. Звичайно, така

поведінка не повинна нести шкоду іншим членам суспільства, порушувати їх права чи свободи.

Кодекс України про адміністративні правопорушення [73] також містить положення, що стосуються захисту персональних даних. Так, Стаття 188-39 Кодексу визнає порушенням невиконання законних вимог Уповноваженого Верховної Ради України з прав людини щодо усунення порушень у сфері захисту персональних даних. Також у КУпАП містить й загальні статті, які можуть стосуватися порушень у сфері обробки персональних даних, наприклад: стаття 212-2 – «Порушення законодавства про інформацію» (стосується поширення інформації з обмеженим доступом); стаття 212-3 – «Порушення права на інформацію» (може включати неправомірний доступ до персональних даних).

Серед міжнародних нормативно-правових актів у сфері захисту персональних даних Україні слід виділити Регламент Європейського Парламенту і Ради (ЄС) 216/679 від 27.04.2016 р. про захист фізичних осіб при обробці персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних (GDPR) [74].

Цей регламент, який був ратифікований Верховною Радою України та отримав обов’язковий статус для застосування, залишається актуальним й сьогодні, оскільки користувачі мережі інтернет часто заповнюють різноманітні аплікаційні форми для реєстрації на веб-сайтах, залишаючи свої персональні дані. Відповідно, питання захисту персональної інформації від несанкціонованого доступу та можливих негативних наслідків, включаючи юридичні, є одним із ключових аспектів державної політики у сфері захисту прав людини та громадянина. Розробники документа зазначають, що стрімкий розвиток цифрових технологій та глобалізація створюють нові виклики у сфері захисту персональних даних. Обсяги збору та обробки персональної інформації значно збільшилися, а сучасні технологічні рішення дозволяють як приватним компаніям, так і державним органам обробляти

персональні дані в безпрецедентних масштабах. Фізичні особи дедалі частіше надають доступ до своїх персональних даних як на локальному, так і на міжнародному рівні. Технологічний прогрес вплинув не лише на економічні процеси, а й на соціальні взаємодії, що вимагає комплексного підходу до регулювання цього питання. Захист персональної інформації має забезпечувати не лише свободу обміну даними в межах Європейського Союзу та їх передачі до інших держав й міжнародних організацій, а й гарантувати високий рівень безпеки та дотримання прав суб'єктів персональних даних.

Такі трансформації вимагають створення надійних й більш узгоджених правових основ для захисту даних у межах ЄС, а також запровадження ефективного механізму їх реалізації. З огляду на значущість довіри у формуванні цифрової економіки на рівні внутрішнього ринку, необхідно забезпечити фізичним особам контроль над власними персональними даними. Посилення правової та практичної визначеності в цьому питанні є важливим не лише для громадян, а й для бізнесу та органів державної влади [76, с.33].

Запровадження цього нормативного документа в європейському правовому просторі підкреслює його ключову роль у захисті прав людини на міжнародному рівні. Він відображає своєчасну реакцію на сучасні виклики, зумовлені стрімким розвитком інформаційних технологій та їх впливом на суспільство. Зростання цифрової взаємодії між людьми та державою вимагає розробки чітких правових норм, що регулюватимуть правовідносини у сфері захисту персональних даних.

Держава, виступаючи гарантом безпеки персональної інформації, має забезпечувати ефективний організаційно-правовий механізм, який сприятиме захисту прав громадян у цій сфері. Це включає розробку та впровадження превентивних заходів, спрямованих на зменшення ризиків порушення законодавства про захист персональних даних, а також механізмів швидкого відновлення порушених прав.

Водночас важливу роль у збереженні конфіденційності даних відіграють і самі їх власники. Вони повинні усвідомлювати значущість дотримання належних технічних і правових заходів для мінімізації потенційних загроз, що можуть виникнути внаслідок неправомірного доступу чи використання їхньої інформації.

Організаційну складову механізму захисту персональних даних утворюють уповноважені державні органи та посадові особи, відповідальні за виконання функцій у цій сфері. Відповідно до закону, вони мають визначені повноваження, що спрямовані на забезпечення належного рівня захисту персональних даних та здійснення контролю за дотриманням правових норм у цій галузі. У ст. 22 Закону України «Про захист персональних даних» [70] визначено вичерпний перелік органів, які здійснюють контроль за додержанням законодавства про захист персональних даних у межах повноважень, передбачених законом. Сюди належать: Уповноважений Верховної Ради України з прав людини та суди.

До повноважень Уповноваженого ВРУ з прав людини належить: «1) отримувати пропозиції, скарги та інші звернення фізичних і юридичних осіб з питань захисту персональних даних та приймати рішення за результатами їх розгляду; 2) проводити на підставі звернень або за власною ініціативою виїзні та безвиїзні, планові, позапланові перевірки володільців або розпорядників персональних даних в порядку, визначеному Уповноваженим, із забезпеченням відповідно до закону доступу до приміщень, де здійснюється обробка персональних даних; 3) отримувати на свою вимогу та мати доступ до будь-якої інформації (документів) володільців або розпорядників персональних даних, які необхідні для здійснення контролю за забезпеченням захисту персональних даних, у тому числі доступ до персональних даних, відповідних баз даних чи картотек, інформації з обмеженим доступом; 4) затверджувати нормативно-правові акти у сфері захисту персональних даних у випадках, передбачених цим Законом; 5) за підсумками перевірки, розгляду звернення видавати обов’язкові для

виконання вимоги (приписи) про запобігання або усунення порушень законодавства про захист персональних даних, у тому числі щодо зміни, видалення або знищення персональних даних, забезпечення доступу до них, надання чи заборони їх надання третій особі, зупинення або припинення обробки персональних даних; 6) надавати рекомендації щодо практичного застосування законодавства про захист персональних даних, роз'яснювати права і обов'язки відповідних осіб за зверненням суб'єктів персональних даних, володільців або розпорядників персональних даних, структурних підрозділів або відповідальних осіб з організації роботи із захисту персональних даних, інших осіб; 7) взаємодіяти із структурними підрозділами або відповідальними особами, які відповідно до цього Закону організовують роботу, пов'язану із захистом персональних даних при їх обробці; оприлюднювати інформацію про такі структурні підрозділи та відповідальних осіб; 8) звертатися з пропозиціями до Верховної Ради України, Президента України, Кабінету Міністрів України, інших державних органів, органів місцевого самоврядування, їх посадових осіб щодо прийняття або внесення змін до нормативно-правових актів з питань захисту персональних даних; 9) надавати за зверненням професійних, самоврядних та інших громадських об'єднань чи юридичних осіб висновки щодо проектів кодексів поведінки у сфері захисту персональних даних та змін до них; 10) складати протоколи про притягнення до адміністративної відповідальності та направляти їх до суду у випадках, передбачених законом; 11) інформувати про законодавство з питань захисту персональних даних, проблеми його практичного застосування, права і обов'язки суб'єктів відносин, пов'язаних із персональними даними; 12) здійснювати моніторинг нових практик, тенденцій та технологій за-хисту персональних даних; 13) організовувати та забезпечувати взаємодію з іноземними суб'єктами відносин, пов'язаних із персональними даними, у тому числі у зв'язку з виконанням Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних та Додаткового протоколу до неї, інших міжнародних договорів України у сфері

захисту персональних даних; 14) брати участь у роботі міжнародних організацій з питань захисту персональних даних» [70].

Про важливість та актуальність цієї ділянки роботи Уповноваженого ВРУ з прав людини свідчить необхідність включення звіту про стан додержання законодавства у сфері захисту персональних даних до щорічної доповіді про стан додержання та захисту прав і свобод людини і громадянина в Україні.

Суб'єкт персональних даних має право звернутися до суду за відновленням свого порушеного права. Відповідно до листа Уповноваженого ВРУ з прав людини, суд володіє механізмами контролю за додержанням законодавства про захист персональних даних у межах повноважень, передбачених законом. Там зазначено: «Статтею 22 Закону України «Про захист персональних даних», передбачено покладення контролю за додержанням законодавства про захист персональних даних у межах повноважень, передбачених законом, на Уповноваженого та суди. Таким чином, механізм здійснення судами зазначеного контролю має відбуватись на підставі законодавства про судоустрій, тобто в процесі здійснення судами судочинства (цивільного, адміністративного, кримінального та під час розгляду справ про адміністративні правопорушення), а також шляхом надання Пленумом вищого спеціалізованого суду, за результатами узагальнення судової практики, роз'яснень рекомендаційного характеру з питань застосування спеціалізованими судами законодавства при вирішенні справ відповідної судової юрисдикції.

У підсумку, організаційно-правовий механізм захисту персональних даних охоплює державні органи, органи місцевого самоврядування, а також володільців і розпорядників персональних даних, наділяючи їх відповідними правами та покладаючи на них певні обов'язки у цій сфері. Відповідно до положень Закону України «Про захист персональних даних», у державних органах, органах місцевого самоврядування, а також серед володільців і розпорядників персональних даних, що здійснюють їх обробку, яка підлягає

повідомленню відповідно до цього Закону, має бути створений або визначений структурний підрозділ чи відповідальна особа, що забезпечує організацію роботи щодо захисту персональних даних під час їх обробки.

Інформація про зазначений структурний підрозділ або відповідальну особу повідомляється Уповноваженому Верховної Ради України з прав людини, який забезпечує її оприлюднення. До повноважень структурного підрозділу чи особи, відповідальної за захист персональних даних, належать: 1) інформування та консультування володільця або розпорядника персональних даних з питань додержання законодавства про захист персональних даних; 2) взаємодія з Уповноваженим Верховної Ради України з прав людини та визначеними ним посадовими особами його секретаріату з питань запобігання та усунення порушень законодавства про захист персональних даних. Відповідно до вимог Закону України «Про захист персональних даних» особисто забезпечують захист персональних даних, якими вони володіють, фізичні особи-підприємці, у тому числі лікарі, які мають відповідну ліцензію, адвокати, нотаріуси.

Як вказує М. Бліхар, організаційно-правовий механізм захисту персональних даних структурно складається з двох елементів – організаційного і правового. Організаційним елементом механізму захисту персональних даних є діяльність органів, служб, посадових осіб, які наділені законом правом вчиняти певні дії для обробки, зберігання та забезпечення захисту персональних даних. Правовий елемент є структурним компонентом організаційно-правового механізму, який за допомогою наявних у певній національній правовій системі засобів та способів регулює суспільні відносини у певній сфері з метою забезпечення правопорядку. А правовим елементом механізму захисту персональних даних є наявність ефективної нормативно-правової основи (законодавчої бази) [76, с.34].

Варто також вказати, що попри часткову гармонізацію національного законодавства про захист персональних даних з Регламентом Європейського Парламенту і Ради (ЄС) 216/679 від 27.04.2016 р., Закон України «Про

захист персональних даних» має ряд недоліків й потребує подальшого оновлення з урахуванням сучасних європейських стандартів.

Серед очевидних недоліків закону можна виділити наступні: 1) недостатній рівень відповідальності (санкції за порушення законодавства значно менші порівняно з Регламентом ЄС, що знижує рівень захисту персональних даних); 2) фрагментарність регулювання (закон не охоплює всі аспекти обробки даних, зокрема автоматизовані рішення, які впливають на права суб'єктів персональних даних); 3) відсутність інституційної незалежності органу контролю (у ЄС, на відміну від України, передбачено незалежні органи із захисту персональних даних, що сприяє більш ефективному контролю).

Національне законодавство про захист персональних даних забезпечує правову базу для розвитку цифрових послуг, таких як електронний документообіг, електронна комерція, онлайн-платежі та цифрова ідентифікація. Оновлення цього закону сприятиме не лише підвищенню рівня захисту приватності, але й збільшенню довіри громадян до інформаційних технологій, що є важливим чинником цифрової трансформації держави.

Таким чином, Закон України «Про захист персональних даних» є важливим елементом нормативно-правових основ регулювання інформаційних технологій. Його модернізація в умовах інтеграції до європейського правового простору є необхідною передумовою для забезпечення ефективного функціонування інформаційних технологій та захисту прав громадян у цифровому середовищі.

Іншим важливим напрямом державної політики та складовою нормативно-правової основи регулювання використання інформаційних технологій в Україні є питання забезпечення кібербезпеки.

В сучасному технологічному середовищі, де цифрові рішення дедалі більше інтегруються у всі сфери життя суспільства, питання кібербезпеки набувають особливої актуальності. Україна також стикається з цими

викликами, що зумовлює необхідність приділяти особливу увагу кібербезпеці як на державному рівні, так і серед громадянського суспільства.

Нормативно-правове регулювання у сфері кібербезпеки в Україні ґрунтується на положеннях Конституції України, низці законів, які стосуються основ національної безпеки, внутрішньої та зовнішньої політики, захисту державних інформаційних ресурсів та інформації. До цієї правової бази також входять міжнародні угоди, ратифіковані Україною, укази Президента України, постанови Кабінету Міністрів, а також інші нормативно-правові акти, ухвалені для імплементації положень національного законодавства.

Хоча Конституція України не містить прямого згадування про кібербезпеку, оскільки її основні положення були розроблені ще до масового поширення інтернету та цифрових технологій, тии не менш вона закладає фундаментальні принципи захисту прав і свобод громадян (ст.ст. 3, 31, 32, 34, 40, 92) [34]. Ці принципи можуть застосовуватися й у сфері забезпечення кібербезпеки, формуючи правову основу для подальшого розвитку відповідних механізмів захисту.

Вперше поняття інформаційної безпеки в Україні було визначено в Законі України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки» від 09.01.2007 р. № 537-V, в якому інформаційна безпека визначено як стан захищеності життєво важливих інтересів людини, суспільства і держави, за якого запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації [77].

У стандарті ICO/IEC 27032 надається визначення «кібербезпеки» через призму безпеки кіберпростору, а саме як збереження конфіденційності, цілісності та доступності інформації в кіберпросторі. При цьому кіберпростором у вже згаданому стандарті визначається середовище, що

виникає внаслідок функціонування на основі єдиних принципів і за загальними правилами інформаційних, телекомунікаційних та інформаційно-комунікаційних систем [78].

В свою чергу відповідно до ДСТ України ISO/IEC 27032:2016 п. 4.21 кіберпростором вважається складне середовище, що виникає в процесі взаємодії людей, програмного забезпечення і послуг Інтернет-послуг Інтернету, за допомогою технологічних пристроїв або об'єднаних мереж, яка не існує в будь- якій фізичній формі [79].

На сьогоднішній день одним із ключових нормативних актів в сфері кібербезпеки в Україні є Закон України «Про основні засади забезпечення кібербезпеки України» № 2163-VIII, що був прийнятий 05 жовтня 2017 р., та який визначає стратегічні завдання, принципи та механізми регулювання в сфері кібербезпеки в Україні, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, а також встановлює основні принципи та засади захисту інформації та інформаційних систем. Основна мета закону - забезпечити національну безпеку, суверенітет, територіальну цілісність та інтереси України у кіберпросторі [80].

Закон визначає стратегічні завдання забезпечення кібербезпеки, зокрема, захист інформації, інформаційних систем та критично важливих об'єктів від кіберзагроз.

Також закон встановлює визначення основних термінів, що використовуються у сфері кібербезпеки, таких як кіберзагроза, кіберзлочин, кібербезпека тощо.

Закон визначає основні принципи, на яких ґрунтується діяльність забезпечення кібербезпеки, зокрема принципи законності, поваги до прав людини і основоположних свобод, відкритості, доступності, стабільності та захищеності кіберпростору, розвитку мережі Інтернет та відповідальних дій у кіберпросторі, невідворотності покарання за вчинення кіберзлочинів, відкритості, прозорості, відповідальності, забезпечення національних інтересів України та міжнародного співробітництва з ціллю зміцнення

взаємної довіри у галузі кібербезпеки та узгодження спільних підходів щодо протидії кіберзагрозам, об`єднання зусиль у розслідуванні та запобіганні кіберзлочинності, а також недопущення використання кіберпростору в терористичних, воєнних, інших протиправних цілях.

Законом визначається перелік основних суб'єктів національної системи кібербезпеки, якими в свою чергу є Державна служба спеціального зв'язку та захисту інформації України, Міністерство оборони України та Генеральний штаб Збройних Сил України, Національна поліція України, Служба безпеки України, розвідувальні органи, Національний банк України, а також містить перелік основних завдань, що покладені на ці органи.

Закон встановлює відповідальність за порушення вимог законодавства у сфері кібербезпеки, включаючи встановлення адміністративної, цивільно-правової та кримінальної відповідальності.

Окрім вищезгаданого, закон регулює основні завдання урядової команди реагування на комп'ютерні надзвичайні події України CERT-UA, порядок державно-приватної взаємодії у сфері кібербезпеки, контроль за законністю заходів із забезпечення кібербезпеки України а також міжнародне співробітництво у сфері кібербезпеки.

Прийняття цього закону безумовно стало важливим кроком для розвитку ефективної системи захисту інформації та інформаційних систем в Україні, а також для забезпечення національної безпеки в кіберпросторі.

Не менш важливим в питанні забезпечення інформаційної безпеки є Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 05.07.1994 №80/94-ВР, прийнятий з метою забезпечення захисту інформації в інформаційно-телекомунікаційних системах та визначає порядок доступу до інформації в інформаційно-телекомунікаційній системі, умови обробки інформації в системі, забезпечення захисту інформації в інформаційно-телекомунікаційній системі, права та обов`язки забезпечення захисту інформації в інформаційно-телекомунікаційних системах, повноваження державних органів у сфері захисту інформації в інформаційно-

телекомунікаційних системах, а також відповідальність за порушення законодавства про захист інформації в інформаційно- телекомунікаційних системах. Окрім цього цим законом встановлюються вимоги і правила щодо захисту інформації в автоматизованих системах та передбачається можливість створення у державних установах та організаціях підрозділів, служб, які організують роботу, пов'язану із захистом інформації в автоматизованих системах [46].

Що стосується міжнародної діяльності в галузі захисту інформації в автоматизованих (інформаційно-телекомунікаційних) системах, то цей закон дозволяє іноземним державам, іноземним фізичним та юридичним особам: бути власниками автоматизованих систем в Україні; бути власниками інформації, що розповсюджується та обробляється в автоматизованих системах України; засновувати спільні підприємства для створення автоматизованих систем, постачання інформації до автоматизованих систем України, обміну інформацією між автоматизованими системами України та автоматизованими системами інших держав.

Важливість прийняття цього закону полягає в першу чергу в тому, що забезпечення безпеки інформації у інформаційно-телекомунікаційних системах є ключовим аспектом забезпечення національної безпеки, оскільки різного роду інформаційні атаки можуть бути використані для спроб втручання в політичні процеси держави, здійснення економічного шпигунства, а також можуть мати наслідком інші загрози для країни. Окрім цього, забезпечення високого рівня захисту інформації стимулює розвиток електронного урядування та електронної комерції, оскільки воно підвищує довіру до цих систем серед громадян та бізнесу.

Також доречно було б виділити Закон України «Про Національну поліцію» від 02.07.2015 № 580-VIII. Цей закон визначає загальні положення щодо структури та функцій Національної поліції, включаючи кіберполіцію як один із її підрозділів [81], яка в свою чергу була утворена як міжрегіональний територіальний орган Національної поліції Постановою Кабінету Міністрів

України від 13 жовтня 2015 р. № 831 «Про утворення територіального органу Національної поліції» [82].

Кіберполіція здійснює розслідування правопорушень у сфері інформаційних технологій, зокрема несанкціонованого доступу до персональних даних, шахрайських схем в інтернеті, актів кібертероризму та інших злочинів у кіберпросторі. Крім того, її діяльність спрямована на впровадження превентивних заходів, які допомагають запобігати кіберзлочинності, а також підвищувати рівень цифрової безпеки серед громадян та бізнесу.

У 2016 році Україна прийняла національну стратегію кібербезпеки, введену в дію рішенням Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України», затверджену указом Президента України № 96/2016, яка визначала стратегічні цілі та завдання у сфері захисту кіберпростору. Основні напрямки цієї стратегії включали:

- створення правової бази: розвиток та удосконалення законодавства у сфері кібербезпеки для забезпечення ефективного захисту критично важливих інформаційних інфраструктур та особистої інформації громадян;
- інституційну підтримку: створення спеціалізованих організацій та структур для координації дій у сфері кібербезпеки, включаючи Національний координаційний центр кібербезпеки;
- розвиток технічних засобів захисту: підвищення рівня технічного захисту інформаційних систем та мереж шляхом розвитку сучасних технологій та засобів кіберзахисту;
- забезпечення освіти та підвищення обізнаності: збільшення рівня обізнаності населення та фахівців у сфері кібербезпеки через навчальні програми, тренінги та інші освітні заходи;
- міжнародне співробітництво: розширення співпраці з міжнародними партнерами у сфері кібербезпеки для обміну досвідом, інформацією та ресурсами [83].

Ця стратегія стала важливим кроком для України у зміцненні захисту кіберпростору в умовах зростаючих кіберзагроз. Однак в контексті швидкого розвитку кіберзлочинності та постійного появлення нових загроз, стратегія кібербезпеки потребує постійного оновлення та адаптації до сучасних викликів.

У зв`язку з метою адаптації стратегії до сучасних реалій сьогодення, указом Президента України від 26 серпня 2021 року № 447/2021 визнано такою, що втратила чинність, статтю 2 Указу Президента України від 15 березня 2016 року № 96 «Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України», та введено в дію рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України», тобто по суті затверджено нову стратегію кібербезпеки в Україні.

Відповідним стратегічним документом визначено основні засади побудови національної системи кібербезпеки, зокрема у ньому вказується, що окрім основних суб’єктів національної системи кібербезпеки, Україна буде залучати до розв’язання завдань у даній сфері ширше коло учасників, зокрема суб’єктів господарювання, громадські об’єднання та окремих громадян. Ключову об’єднувальну та координаційну роль у цьому процесі згідно даної стратегії повинні відігравати Національний координаційний центр кібербезпеки, а також урядова команда реагування на комп'ютерні надзвичайні події України CERT-UA.

Також даний документ містить перелік основних пріоритетів забезпечення кібербезпеки України, а саме: убезпечення кіберпростору задля захисту суверенітету держави та розвитку суспільства; захист прав, свобод і законних інтересів громадян України у кіберпросторі; європейська і євроатлантична інтеграція у сфері кібербезпеки.

Формування нової якості національної системи кібербезпеки потребує чіткого та зрозумілого визначення стратегічних цілей, що мають бути досягнуті протягом періоду реалізації цієї Стратегії, у зв’язку з чим стратегію

передбачені стретегічні цілі для формування потенціалу стримування, набуття кіберстійкості, а також вдосконалення взаємодії.

У Стратегії також визначено основні напрями зовнішньополітичної діяльності України у сфері кібербезпеки, зокрема передбачається, що Україна у сфері кібербезпеки повинна забезпечити поглиблення євроінтеграційних процесів, здійснивши уніфікацію підходів, методів і засобів забезпечення кібербезпеки з усталеними практиками Європейського союзу і НАТО [83].

Так, Л. Веселова зазначає, що Україна безумовно зацікавлена у впровадженні міжнародного досвіду у сфері адміністративно-правового та організаційного забезпечення кібербезпеки, який їй потрібен у якості вдалого прикладу у формуванні відповідної політики і побудови власної системи правового та організаційного забезпечення кібербезпеки. Успіх та ефективність адміністративно-правового забезпечення кібербезпеки забезпечується синхронними заходами, спрямованими як у напрямі співпраці з фаховими міжнародними інституціями в сфері забезпечення кібербезпеки, так і у напрямі формування адекватного викликам гібридної війни національного законодавства у цій сфері [84].

Ю. Третяк в свою чергу вказує, що забезпечення безпеки в кіберпросторі не вичерпується лише заходами державного регулювання і контролю, а натомість в багатьох випадках прямо залежить від свідомої і відповідальної поведінки учасників правовідносин, зокрема, але не виключно, суб’єктів господарювання. Є очевидним той факт, шо на даний час високий інтерес у кіберзлочинців викликає ринок віртуальних активів (криптовалют) та електронної комерції. Використовуючи різні способи здійснення атак, хакери здійснюють крадіжки електронних грошей безпосередньо у їх власників, або ж використовують для цього підручні ресурси - гаманці, біржі та інше. Кібератаки на суб’єктів господарювання та їх діяльність можуть набувати абсолютно різних форм. Це може бути зокрема фішинг, який здійснюється, наприклад, за допомогою розсилки

електронних повідомлень співробітникам або використання вірусного програмного забезпечення [85].

Внаслідок недоліків правового регулювання в національному кібернетичному просторі України спостерігається ряд негативних явищ, що створюють реальні, а також потенційні загрози кібербезпеці. Яскравим прикладом таких загроз є інформаційно-психологічний тиск на населення України з боку засобів масової інформації Російської Федерації у 2014 році на території Автономної Республіки Крим та південно-східних регіонах України, що в свою чергу мало наслідком російську інформаційну експансію в національний інформаційний простір України, а також захоплення стратегічних об'єктів української телекомунікаційної інфраструктури [85].

Поділяємо думку І. Діордіци про те, що чинна нормативно-правова база України у сфері інформаційних технологій є надзвичайно важливим інструментом їх регулювання та забезпечення цифровізації держави й суспільства, однак вона однозначно потребує удосконалення [86].

Підсумовуючи вищевикладене, зазначимо, що гармонізація із міжнародними стандартами, усунення фрагментарності та систематизація національного законодавства у сфері інформаційних технологій не лише сприятиме інтеграції України у світовий цифровий простір, а й підвищить ефективність адміністративно-правового регулювання у цій сфері.

Висновки до розділу 1

1. Дослідження значення інформаційних технологій у сучасному суспільстві вчергове підтверджує, що цифровізація є невід'ємною частиною сучасного світу та охоплює всі сфери життєдіяльності – від побутової сфери до економіки, публічного управління та соціальної комунікації. Їхня інтеграція в суспільні процеси суттєво змінює традиційні механізми взаємодії між державою, бізнесом та громадянами, вимагаючи належного адміністративно-правового регулювання.

На основі існуючих наукових визначень й трактувань проаналізовано поняття «адміністративно-правове регулювання» та «інформаційні технології» з метою визначення основних напрямів їхньої взаємодії.

Здійснено концептуальне визначення поняття «адміністративно-правове регулювання інформаційних технологій» як діяльності органів виконавчої влади, інших суб'єктів публічної адміністрації, яка спрямована на створення, впровадження та застосування адміністративно-правових норм, що забезпечують ефективне функціонування, розвиток і безпеку інформаційних технологій, а також регулювання відносин між суб'єктами у сфері використання інформаційних технологій із метою забезпечення публічного порядку, захисту прав і свобод людини, підтримки економічної стабільності та національної безпеки.

2. Дослідження розвитку становлення адміністративно-правового регулювання використання інформаційних технологій в Україні з метою виокремлення відповідного позитивного історичного досвіду дозволило виявити кілька важливих етапів, що відображають зміни в суспільних відносинах, технічному прогресі та законодавчій базі.

Перший етап – доінституційний період (до 1991 р.) – характеризувався відсутністю власного національного правового регулювання та використанням інформаційних технологій переважно у військових, промислових і наукових сферах у межах централізованої політики СРСР. На цьому етапі закладалися лише технологічні основи, а правове регулювання було обмежене директивами радянського уряду.

Другий етап – період формування національного законодавства (1991–2010 рр.) – розпочався з проголошення незалежності України та необхідності розробки правової бази для регулювання інформаційних технологій. Було прийнято основоположні закони, що заклали правовий фундамент для подальшого розвитку сфери інформаційних технологій.

Третій етап – сучасний період цифрової трансформації (з 2010 р.) – ознаменувався активним впровадженням цифрових технологій в публічному

управлінні, економіці та суспільному житті. Було ухвалено стратегічні законодавчі акти та запущено інноваційні електронні платформи, що стало потужним стимулом для цифрової трансформації України. Було створено фундамент для прозорої, ефективної та доступної системи адміністративних послуг, який сприяє покращенню взаємодії між державою, громадянами та бізнесом.

Незважаючи на значний прогрес у правовому регулюванні інформаційних технологій, подальший розвиток цієї сфери потребує комплексного підходу, що включає ефективне правове регулювання, інституційну підтримку та впровадження інноваційних технологій.

3. Розвиток інформаційного суспільства та цифрових технологій в Україні зумовив необхідність створення ефективної нормативно-правової бази, що регулює використання інформаційних технологій. В Україні діє значна кількість законодавчих та підзаконних актів, які регулюють цифровізацію суспільства, проте їхня фрагментарність і недостатня узгодженість створюють певні виклики у сфері правозастосування.

З’ясовано, що нормативно-правову основу регулювання використання інформаційних технологій в Україні складають наступні напрями державної політики: впровадження електронного документообігу, забезпечення захисту персональних даних та забезпечення кібербезпеки.

Нормативно-правове регулювання використання інформаційних технологій в Україні продовжує активно розвиватися, проте для ефективної цифровізації держави необхідно усунути прогалини в законодавстві, гармонізувати його з міжнародними стандартами та забезпечити належний рівень правозастосування.

РОЗДІЛ 2
ОСОБЛИВОСТІ АДМІНІСТРАТИВНО-ПРАВОВОГО РЕГУЛЮВАННЯ ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

2.1 Адміністративно-правове забезпечення правового режиму інформаційної безпеки

Інформаційна безпека є однією з основних складових національної безпеки будь-якої держави в умовах глобалізації та цифрової трансформації. У сучасному світі інформаційні ресурси стали ключовим елементом суспільного розвитку, що робить їх захист першочерговим завданням для державної політики. Адміністративно-правове забезпечення правового режиму інформаційної безпеки є важливим інструментом регулювання та управління цією сферою, що спрямоване на забезпечення захисту суспільних інтересів, прав громадян і національної безпеки.

Згідно із визначенням, яке наведене у Великому енциклопедичному юридичному словнику, термін «правовий режим» (від лат. regimen – «управління, керівництво») означає певну сукупність юридичних засобів, способів, що застосовуються в певній сфері суспільних відносин та забезпечують дію механізму правового регулювання.

Правовому режиму притаманні наступні особливості:

1) він встановлюється законодавством та забезпечується примусовою силою держави;

2) він є специфічним порядком правового регулювання, що складається із сукупності юридичних засобів, спрямованих на досягнення певної мети, й характеризується певним їх співвідношенням;

3) правовий режим особливим чином регламентує певні сфери суспільних відносин, виділяючи суб’єктів та об’єкти права;

4) в основу правового режиму покладено той чи інший спосіб правового регулювання – заборону, дозвіл чи позитивне зобов’язання [87].

На основі викладеного можна виділити чотири базові умови, необхідні для ефективного функціонування будь-якого правового режиму:

1) наявність відповідної нормативно-правової бази, яка закріплює відповідний правовий режим, а також ефективних механізмів державного контролю та примусу, що забезпечують його реалізацію;

2) юридичні інструменти, які застосовуються в межах конкретного правового режиму, повинні бути узгоджені між собою та спрямовані на досягнення чітко визначених цілей;

3) чітке виокремлення суб’єктів та об’єктів, чиї відносини регулюються відповідним правовим режимом;

4) коректно обрані й пристосовані до цілей правового режиму способи (засоби) правового регулювання.

Слід зазначити, що перша з наведених умов є визначальною для всіх інших. Зокрема, саме законодавство встановлює мету правового режиму, визначає взаємозв’язок та порядок застосування юридичних механізмів, окреслює коло суб’єктів і об’єктів правового регулювання, а також визначає допустимі способи впливу.

Беручи до уваги зазначене, доцільним вбачається детальний аналіз загальнотеоретичних засад правового режиму інформаційної безпеки.

Правовий режим інформаційної безпеки можна визначити як сукупність правових норм і механізмів, які визначають порядок дій суб'єктів у сфері інформаційної безпеки, їхні обов'язки та відповідальність.

Правовий режим спрямований на забезпечення інформаційної безпеки шляхом: регулювання відносин у сфері захисту інформації, запобігання та протидії інформаційним загрозам, забезпеченню балансу між безпекою та правами людини.

По своїй суті інформаційна безпека є метою, а правовий режим є її засобом.

Інформаційна безпека є стратегічною метою: досягти стану, коли національний інформаційний простір, права громадян та державні інтереси надійно захищені.

Правовий режим є засобом досягнення цієї мети через розробку, прийняття та реалізацію правових норм і процедур.

Інформаційна безпека визначає, які саме проблеми та загрози необхідно вирішувати. Правовий режим забезпечує інструменти та правила, як ці проблеми вирішувати.

Правовий режим має адаптуватися до цих змін, оновлюючи нормативно-правову базу відповідно до нових викликів та загроз.

Таким чином, інформаційна безпека є певним цільовим станом, який характеризується захищеністю інформаційної сфери, а «правовий режим інформаційної безпеки» є комплексом інструментів й правил, за допомогою яких відповідний стан досягається. Ефективність інформаційної безпеки безпосередньо залежить від якості, комплексності та динамічності правового режиму.

Складовими правового режиму інформаційної безпеки є правові норми: Закони та підзаконні акти, що регулюють питання інформаційної безпеки, норми міжнародного права, імплементовані в національне законодавство.

Суб’єктами забезпечення правового режиму інформаційної безпеки є органи державної влади (наприклад, Рада національної безпеки і оборони України, Служба безпеки України, Міністерство цифрової трансформації України, Національна рада з питань телебачення і радіомовлення, Національна поліція України тощо), а також, громадські організації, наукові установи та приватний сектор.

Інструментами реалізації правового режиму інформаційної безпеки є відповідні нормативно-правові акти.

Об'єктами захисту правового режиму інформаційної безпеки є інформаційні ресурси (державні інформаційно-комунікаційні системи, приватні бази даних), національний інформаційний простір (ЗМІ, інтернет-

простір тощо), права громадян на інформацію, приватність та захист персональних даних.

Метою правового режиму інформаційної безпеки є: 1) захист національного інформаційного простору (протидія дезінформації, пропаганді, кіберзлочинності); 2) захист державного суверенітету та територіальної цілісності в умовах гібридної та воєнної агресії; 3) гарантування прав громадян (право на доступ до достовірної інформації, захист персональних даних від несанкціонованого доступу та використання); 4) розвиток інформаційної стійкості (формування суспільного імунітету до дезінформації); 5) забезпечення національної єдності.

Основними принципами правового режиму інформаційної безпеки є: 1) законність (діяльність суб'єктів забезпечення інформаційної безпеки має базуватися виключно на чинному законодавстві); 2) пропорційність (дотримання балансу між захистом інформаційного простору та свободою слова); 3) технологічна нейтральність (застосування правових норм до всіх технологій незалежно від їх типу); 4) прозорість (доступність інформації про дії держави у сфері інформаційної безпеки для громадян і суспільства).

Таким чином, правовий режим інформаційної безпеки можна визначити як встановлений державою комплекс правових норм, принципів та механізмів, спрямованих на забезпечення стану захищеності національного інформаційного простору, прав і свобод громадян, суспільства та держави в інформаційній сфері. Цей режим включає правила поведінки, що регулюють відносини між суб'єктами інформаційної безпеки, передбачають механізми захисту інформації від внутрішніх і зовнішніх загроз.

Зважаючи на фундаментальну роль законодавства у формуванні та функціонуванні будь-якого правового режиму, аналіз правового режиму забезпечення інформаційної безпеки України доцільно розпочати з основоположного нормативно-правового акту України – Конституції України.

Комплексний аналіз положень Конституції України дає підстави стверджувати, що на рівні Основного Закону вже закріплено низку норм, які визначають істотні особливості правового режиму забезпечення інформаційної безпеки України.

Так, стаття 1 Конституції України встановлює: «Україна є суверенна і незалежна, демократична, соціальна, правова держава». Стаття 3 Конституції України встановлює: «Людина, її життя і здоров'я, честь і гідність, недоторканність і безпека визнаються в Україні найвищою соціальною цінністю». Водночас, частина 1 статті 17 Конституції України визначає: «Захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього Українського народу» [34].

Таким чином, відповідно до положень Конституції України, пріоритетним завданням правового регулювання в державі є збереження її суверенітету та незалежності. Водночас реалізація цього завдання повинна здійснюватися не «будь-якою ціною», а з дотриманням принципів і норм демократичної, соціальної та правової держави. Тобто, наявність однієї з ключових функцій держави не виключає необхідності виконання інших її завдань.

Зазначене дозволяє виділити дві ключові особливості правового режиму забезпечення інформаційної безпеки України, визначені на конституційному рівні:

- першочергова пріоритетність розвитку такого правового режиму;
- необхідність збалансованого правового регулювання, яке забезпечить дотримання інших конституційних пріоритетів без їх обмеження.

З огляду на це, оптимальним підходом до виконання вимог Конституції України є формування збалансованого правового режиму інформаційної безпеки, у якому імперативні механізми правового регулювання поєднуються з диспозитивними, рекомендаційними та стимулюючими заходами.

XXI століття ознаменувалося безпрецедентним розвитком технологій у сфері зв'язку та цифровізації. Чимало ключових процесів, що визначають життєдіяльність людини, нині тісно інтегровані з мережею Інтернет, яка продовжує швидко розвиватися разом із її інфраструктурою, суміжними технологіями та ринками послуг.

У результаті ми спостерігаємо небачене раніше розширення доступу до інформації, що ставить під сумнів ефективність суто імперативного підходу в регулюванні інформаційних правовідносин. У сучасних умовах правової держави повна ізоляція людини від шкідливого інформаційного впливу є практично нездійсненною, так само як і забезпечення інформаційної безпеки виключно зусиллями державних органів.

Повертаючись до положень Основного Закону, важливо підкреслити, що ч. 1 статті 17 Конституції України цілком логічно і справедливо зазначено, що забезпечення інформаційної безпеки України є не лише функцією держави, а й справою всього українського народу [34]. Іншими словами, сам законодавець на конституційному рівні визначив, що забезпечення інформаційної безпеки є й завданням усього українського суспільства.

З огляду на те, що Україна опинилася перед викликами масштабної збройної та інформаційної війни, питання забезпечення інформаційної безпеки як складової національної безпеки набули особливої важливості та стратегічного значення.

Окрім Основного Закону України, правові засади національної безпеки України регламентуються Законом України «Про національну безпеку України» від 21 червня 2018 р., в якому визначено понятійний апарат у сфері національної безпеки [88].

До ключових категорій, які становлять зміст національної безпеки України віднесено: «національна безпека України», «національні інтереси України», «державна безпека», «громадська безпека і порядок», «воєнна безпека» тощо. Відповідно до п.9 ч.1 ст.1 Закону України «Про національну

безпеку України» під національною безпекою України розуміється: «захищеність державного суверенітету, територіальної цілісності, демократичного конституційного ладу та інших національних інтересів України від реальних та потенційних загроз» [88].

При цьому в п.6 ч.1 ст.1 даного Закону дається визначення загрозам національної безпеки України, а саме: «явища, тенденції і чинники, що унеможливлюють чи ускладнюють або можуть унеможливити чи ускладнити реалізацію національних інтересів та збереження національних цінностей України» [88].

З огляду на ці положення, до основних об'єктів національної безпеки України варто віднести: 1) людину та громадянина – їхні конституційні права, свободи та обов'язки; 2) суспільство – його духовні, морально-етичні, культурні, історичні, інтелектуальні й матеріальні цінності, інформаційний простір, навколишнє природне середовище та природні ресурси; 3) державу – її конституційний лад, суверенітет, територіальну цілісність і недоторканність.

Зважаючи на комплексний характер національної безпеки, вона включає низку взаємопов'язаних підсистем та елементів. До ключових складових цієї системи можна віднести політичну, економічну, воєнну, соціальну, екологічну, інноваційну, а також науково-технологічну безпеку [89].

Так, А. Войціховський зазначає, що з огляду на стрімкий розвиток інформаційно-комунікаційних технологій, тотальну комп'ютеризацію (цифровізацію), створення глобального інформаційного простору були сформовані принципово нові субстанції – інформаційне суспільство, кіберпростір, що мають безмежний потенціал і значний вплив на політичний, економічний, соціальний і культурний розвиток держави. Саме створення інформаційного суспільства призвело до виникнення багатьох кіберзагроз у важливих сферах життєдіяльності суспільства (банківська, воєнна, критична інфраструктура тощо), тому до національної безпеки держави

цілком виправдано відносять інформаційну безпеку як самостійний елемент національної безпеки [90, с. 283].

Інформаційна безпека визнається правовим поняттям. Під ним розуміється стан захищеності національних інтересів України в інформаційній сфері, що визначається сукупністю збалансованих інтересів особистості, суспільства і держави [91].

Глобалізація сучасного інформаційного простору сприяє послабленню рівня інформаційного суверенітету держави, а рівень його розвитку та безпека безпосередньо впливають на загальний стан національної безпеки. Саме тому одним із ключових напрямів міжнародної діяльності у сфері інформаційної безпеки є розбудова та вдосконалення механізмів міжнародного співробітництва у цій сфері.

З огляду на масштабність глобальних інформаційних викликів та обмеженість можливостей окремих держав самостійно протистояти загрозам, важливим є активний розвиток міжнародної взаємодії для забезпечення інформаційної безпеки. Така співпраця має бути спрямована на комплексне вирішення актуальних проблем із залученням широкого кола учасників, що дозволить максимально враховувати інтереси світової спільноти та формувати ефективні механізми протидії сучасним інформаційним загрозам.

Концепція міжнародної інформаційної безпеки вперше була втілена у Резолюції Генеральної Асамблеї ООН A/RES/53/70 «Досягнення у сфері інформатизації та телекомунікацій у контексті міжнародної безпеки» від 4 грудня 1998 року. Цей документ став відправною точкою для глобального обговорення необхідності створення нового міжнародно-правового порядку, в основі якого лежать інформація, інформаційні технології та способи їх застосування [92].

Резолюція Генеральної Асамблеї ООН A/RES/54/49 «Досягнення у сфері інформатизації і телекомунікацій в контексті міжнародної безпеки» від 1 грудня 1999 р. вперше вказала на об’єктивні загрози міжнародній

безпеці інформаційного простору стосовно не лише до цивільної, а також до військової сфери [93].

На виконання цієї Резолюції в 2000 р. в Секретаріаті ООН були представлені «Принципи, що стосуються міжнародної інформаційної безпеки», які були опубліковані в доповіді Генерального секретаря ООН від 10 червня 2000 р. для їх подальшого спільного обговорення. Принципи визначають правила поведінки держав в інформаційному просторі, створюючи для них відповідні моральні зобов‘язання, а також закладають основу для міжнародних переговорів під егідою ООН та інших міжнародних організацій з проблем інформаційної безпеки. Вперше були наведені такі визначення понятійного апарату системи міжнародної інформаційної безпеки, як: «інформаційний простір», «інформаційний ресурс», «інформаційна війна», «інформаційна зброя», «інформаційна безпека», «загроза інформаційної безпеки», «міжнародна інформаційна безпека», «неправомірне використання інформаційно-телекомунікаційних систем», «несанкціоноване втручання в інформаційно-телекомунікаційні системи та інформаційні ресурси», «критично важливі структури», «міжнародний інформаційний тероризм» і «міжнародна інформаційна злочинність» [94].

Наступні засідання Генеральної Асамблеї ООН продовжували дискусію та пошук ефективних рішень щодо міжнародної інформаційної безпеки, що знайшло відображення в низці ухвалених резолюцій і доповідей. Зокрема, питання, пов’язані з міжнародною інформаційною безпекою, неодноразово розглядалися на різних сесіях Генеральної Асамблеї ООН, що підтверджують такі резолюції: A/RES/55/63 від 4 грудня 2000 року та A/RES/56/121 від 19 грудня 2001 року щодо протидії злочинному використанню інформаційних технологій; A/RES/57/239 від 20 грудня 2002 року про формування глобальної культури кібербезпеки; A/RES/58/199 від 23 грудня 2003 року та A/RES/64/211 від 21 грудня 2009 року, які спрямовані на розбудову глобальної культури кібербезпеки та захист критично важливої

інформаційної інфраструктури; A/RES/62/17 від 5 грудня 2007 року щодо сприяння багатосторонньому розгляду існуючих і потенційних загроз у сфері інформаційної безпеки; A/RES/71/28 від 5 грудня 2016 року, присвячена досягненням у сфері інформатизації та телекомунікацій у контексті міжнародної безпеки та інші [94].

Європейський Союз також активно реалізує політику щодо забезпечення інформаційної безпеки, приділяючи особливу увагу кібербезпеці як її ключовій складовій. Гарантування інформаційної безпеки стало одним із стратегічних напрямів діяльності ЄС. У 2001 році Європейська комісія представила перший концептуальний документ під назвою «Мережева та інформаційна безпека: європейський політичний підхід», у якому окреслено основні напрями вирішення проблеми захисту інформаційного простору. Документ вводить поняття «мережева та інформаційна безпека», під яким розуміється здатність інформаційних мереж і систем протистояти як випадковим інцидентам, так і цілеспрямованим атакам, що можуть загрожувати доступності, автентичності, цілісності та конфіденційності даних, а також стабільному функціонуванню послуг, які надаються через ці мережі та системи [95].

У наступні роки органами ЄС було ухвалено значну кількість нормативно-правових актів, спрямованих на впровадження різних підходів до забезпечення інформаційної безпеки в країнах-членах Європейського Союзу. Серед них можна назвати наступні: Рамкове рішення Ради ЄС 2005/222/JHA щодо нападу на інформаційні системи від 24 лютого 2005 р., яка встановила мінімальні правила визначення кримінальних злочинів та санкцій у сфері неправомірного впливу на інформаційні системи [96]; Повідомлення Комісії ЄС «На шляху до загальної політики в сфері боротьби з кіберзлочинністю» від 22 травня 2007р., в якому даються визначення терміну «кіберзлочинність» та основні напрями політики ЄС щодо інформаційної безпеки [97]; Повідомлення Комісії ЄС «Захист Європи від широкомасштабних кібератак та руйнувань: посилення рівня

підготовленості, безпеки та стійкості» від 30 березня 2009 р., в якому визначено основні заходи для посилення безпеки та здатності європейської критичної інформаційної інфраструктури протистояти зовнішнім впливам [98]; Стратегія кібербезпеки ЄС «Відкритий, надійний та безпечний кіберпростір» від 07 лютого 2013 р., яка рекомендує державам-членам ЄС розвивати міждержавне співробітництво у протидії кіберзагрозам [99]; Директива Європейського парламенту і Ради ЄС щодо заходів по забезпеченню високого загального рівня безпеки мережевих та інформаційних систем у всьому Союзі від 6 липня 2016 р., яка закріпила єдині правила та вимоги в сфері кібербезпеки для всіх держав-членів ЄС (підвищення спроможності системи кібербезпеки на національному рівні, підвищення рівня європейського співробітництва і запровадження управління ризиками та зобов‘язання сповіщати про кіберінциденти операторів базових послуг та провайдерів цифрових послуг тощо)[100]; Повідомлення Комісії ЄС «Стійкість, стримування та захист: створення сильної кібербезпеки для ЄС» від 13 вересня 2017 р., в якому визначається важливість кібербезпеки для процвітання та безпеки держав-членів ЄС і необхідність колективного та широкомасштабного підходу у протидії кіберзагрозам тощо [101].

З метою вдосконалення системи інформаційної безпеки в рамках ЄС було сформовано спеціалізований організаційний механізм. Важливу роль у ньому відіграє Європейське агентство з питань мережевої та інформаційної безпеки (ENISA), яке було утворено 10 березня 2004 р. До завдань ENISA відноситься вдосконалення мережевої та інформаційної безпеки в ЄС, сприяння розвитку культури мережевої та інформаційної безпеки на користь громадян, споживачів, підприємств та громадських організацій ЄС, а також сприяння безперебійному функціонуванню внутрішнього ринку ЄС [102].

Розуміючи, що ефективний захист інформаційної безпеки в європейському кіберпросторі значною мірою залежить від міжнародної

співпраці, у 2013 році в межах Європейського поліцейського офісу (Європолу) було утворено Європейський центр боротьби з кіберзлочинністю. Основними напрямами його діяльності стали розслідування шахрайських дій в інтернеті, а також злочинів, які загрожують безпеці критично важливої інфраструктури та інформаційних систем Європейського Союзу [103].

Варто зазначити, що Європейський Союз активно оновлює свої підходи до кібербезпеки відповідно до сучасних викликів. Цей процес включає впорядкування нормативно-правової бази з метою забезпечення єдності державної політики в цій сфері, розробку загальноєвропейських рекомендацій щодо захисту інформаційного простору, розширення структур, що відповідають за кібербезпеку, посилення моніторингу національного інформаційного середовища, а також зміцнення механізмів захисту критично важливих інформаційних систем ЄС.

Усвідомлюючи значущість інформаційної безпеки як невід'ємної складової національної безпеки, більшість країн світу активно впроваджують комплексні заходи з її забезпечення. До них належать удосконалення національного законодавства в сфері кібербезпеки, а також утворення спеціалізованих державних органів для контролю та координації дій у цій сфері.

На сьогодні інформаційна безпека та кіберзахист є стратегічними питаннями глобального масштабу, що впливають на всі верстви населення. Державна політика з інформаційної безпеки та кібербезпеки спрямована на посилення національної безпеки та підвищення стійкості державних інформаційних систем. Це підтверджується прийняттям національних стратегій з кібербезпеки в таких країнах, як США, Швеція, Естонія, Фінляндія, Чехія, Франція, Німеччина, Литва, Велика Британія, Канада, Японія, Індія, Австралія, Нова Зеландія, Колумбія та інші. Перелік країн наочно показує, що проблема інформаційної безпеки та кібербезпеки визнається актуальною в усьому світі. [104].

Не залишилась осторонь цієї проблеми й Україна, здійснивши внутрішньодержавні комплексні заходи з інформаційної безпеки та кібербезпеки.

Так, станом на сьогодні забезпечення інформаційної безпеки в Україні регламентовано Стратегією інформаційної безпеки, затвердженої Указом Президента України від 28 грудня 2021 року №685/202 [105] та Стратегією кібербезпеки України, затвердженої Указом Президента України від 26 серпня 2021 року №447/2021 [83].

В контексті розгляду питання адміністративно-правового забезпечення правового режиму інформаційної безпеки необхідно звернути увагу саме на Стратегію інформаційної безпеки. Саме у ній представлено визначення «інформаційна безпека України», сформульовані актуальні виклики й загрози національній безпеці України в інформаційній сфері, стратегічні цілі та завдання, спрямовані на протидію таким загрозам, захист прав осіб на інформацію та захист персональних даних.

Метою Стратегії інформаційної безпеки визначено посилення спроможностей щодо забезпечення інформаційної безпеки держави, її інформаційного простору, підтримки інформаційними засобами та заходами соціальної та політичної стабільності, оборони держави, захисту державного суверенітету, територіальної цілісності України, демократичного конституційного ладу, забезпечення прав та свобод кожного громадянина [105].

Досягнення мети здійснюватиметься шляхом вжиття заходів щодо стримування та протидії загрозам інформаційній безпеці України та нейтралізації інформаційної агресії, у тому числі спеціальних інформаційних операцій держави-агресора, спрямованих на підрив державного суверенітету, територіальної цілісності України, забезпечення інформаційної стійкості суспільства та держави, створення ефективної системи взаємодії між органами державної влади, органами місцевого самоврядування та

суспільством, а також розвиток міжнародної співпраці у сфері інформаційної безпеки на засадах партнерства та взаємної підтримки [105].

Правовою основою Стратегії є Конституція України, закони України, Стратегія національної безпеки України, затверджена Указом Президента України від 14 вересня 2020 року № 392 [106], а також міжнародні договори, згода на обов'язковість яких надана Верховною Радою України.

Реалізація Стратегії була розрахована на період до 2025 року. Проте з початком повномасштабного вторгнення Російської Федерації у 2022 році її актуальність набула ще більшого сенсу, а заходи по реалізації її програми здійснюються та вдосконалюються донині.

Саме у Стратегії інформаційної безпеки дається визначення терміну «інформаційна безпека України» як складової частини національної безпеки України, стану захищеності державного суверенітету, територіальної цілісності, демократичного конституційного ладу, інших життєво важливих інтересів людини, суспільства і держави, за якого належним чином забезпечуються конституційні права і свободи людини на збирання, зберігання, використання та поширення інформації, доступ до достовірної та об'єктивної інформації, існує ефективна система захисту і протидії нанесенню шкоди через поширення негативних інформаційних впливів, у тому числі скоординоване поширення недостовірної інформації, деструктивної пропаганди, інших інформаційних операцій, несанкціоноване розповсюдження, використання й порушення цілісності інформації з обмеженим доступом [105].

Відповідно до Стратегії інформаційної безпеки, основними напрямами забезпечення інформаційної безпеки України є стійкість та взаємодія, для досягнення яких необхідним є виконання таких стратегічних цілей та завдань: 1) протидія дезінформації та інформаційним операціям; 2) забезпечення всебічного розвитку української культури та утвердження української громадянської ідентичності; 3) підвищення рівня медіакультури та медіаграмотності суспільства; 4) забезпечення дотримання прав особи на

збирання, зберігання, використання та поширення інформації, свободу вираження своїх поглядів і переконань, захист приватного життя, доступ до об'єктивної та достовірної інформації, а також забезпечення захисту прав журналістів, гарантування їх безпеки під час виконання професійних обов'язків, протидія поширенню незаконного контенту; 5) інформаційна реінтеграція громадян України, які проживають на тимчасово окупованих територіях та на прилеглих до них територіях України, до загальноукраїнського інформаційного простору, а також відновлення їх права на інформацію, що дає їм змогу підтримувати зв'язок з Україною; 6) створення ефективної системи стратегічних комунікацій; 7) розвиток інформаційного суспільства та підвищення рівня культури діалогу.

На даний момент, в умовах повномасштабної війни, підходи до виявлення загроз і реагування на них зазнали змін, що зумовило певне обмеження прав людини з огляду на необхідність протидії потенційним і реальним загрозам для України.

У зв’язку з введенням в країні правового режиму воєнного стану, тимчасово, на період його дії, запроваджуються обмеження щодо прав і законних інтересів юридичних осіб. Ці заходи здійснюються в обсязі, необхідному для реалізації заходів, передбачених частиною першою статті 8 Закону України «Про правовий режим воєнного стану». Такі обмеження спрямовані на забезпечення належного функціонування державних інституцій у кризовий період і протидію загрозам національній безпеці [107].

Серед конституційних норм, щодо яких можливі обмеження їх дії є і ті, що безпосередньо стосуються інформаційних прав. Зокрема:

– стаття 31 («Кожному гарантується таємниця листування, телефонних розмов, телеграфної та іншої кореспонденції»);

– стаття 32 («Ніхто не може зазнавати втручання в його особисте і сімейне життя, крім випадків, передбачених Конституцією України»);

– стаття 34 («Кожному гарантується право на свободу думки і слова, на вільне вираження своїх поглядів і переконань»);

– стаття 41 («Кожен має право володіти, користуватися і розпоряджатися своєю власністю, результатами своєї інтелектуальної, творчої діяльності»).

Ці обмеження зумовлені неможливістю повного захисту осіб, які перебувають на територіях, що постраждали від військової агресії. Україна не може нести відповідальність за порушення прав людини на тимчасово окупованих територіях та в зонах активних бойових дій. Крім того, такі обмеження сприяють ухваленню нормативно-правових актів, спрямованих насамперед на забезпечення інформаційної безпеки держави. Хоча подібні заходи можуть вступати в певну суперечність із загальноприйнятими стандартами гарантій прав людини, у воєнний час пріоритет державних інтересів є ключовим для збереження основоположних прав широкого кола осіб шляхом гарантування функціонування самої держави.

Завершення воєнного стану автоматично відновить дію норм, що були тимчасово обмежені. Від початку його запровадження було внесено низку змін до нормативно-правових актів, враховуючи специфіку воєнного часу. Вони стосуються регулювання певних аспектів інформаційних правовідносин, зокрема обмеження на поширення суспільно небезпечної інформації, визначення процедур технічної фіксації даних у воєнний період, встановлення або посилення відповідальності за розповсюдження певних категорій інформації, а також врегулювання процесуальних дій щодо вилучення та обробки інформаційних даних.

Варто нагадати, що у березні 2022 року Верховна Рада України ухвалила закон, який запроваджує кримінальну відповідальність за несанкціоновану фото- та відеозйомку переміщення Збройних Сил України та міжнародної військової допомоги під час воєнного стану. Цей закон доповнив Кримінальний кодекс статтею 114-2, яка передбачає покарання за розповсюдження інформації про переміщення зброї та військової техніки без офіційного дозволу [108].

Крім того, 22 березня 2022 року набули чинності зміни до Кримінального процесуального кодексу України, які спрощують проведення слідчих дій та тимчасовий доступ до речей і документів. Зокрема, під час дії воєнного стану тимчасовий доступ до певних речей і документів може здійснюватися на підставі постанови прокурора, погодженої з керівником прокуратури, без ухвали слідчого судді [109].

Також, законодавцем було посилено кримінальну відповідальність за виготовлення та поширення забороненої інформаційної продукції, що сприяє захисту інформаційного простору України в умовах воєнного стану [110].

Як зазначає, І. Котерлін, сьогоднішні воєнні реалії чітко демонструють, що інформація є зброєю «масового ураження». Тому необхідно створити ефективний механізм, який би забезпечив державну інформаційну безпеку і дотримання прав людини та водночас дозволив би людям не відчувати ефекту посягань на свободи та демократію. Найбільша цінність українців полягає у їх розумінні та сприйнятті понять свобода і справедливість. Формування інформаційної безпеки, особливо в умовах війни, є комплексною технічною та політико-правовою діяльністю уповноважених органів, спрямованою на захист держави, суспільства і людини. У воєнний час захист інформаційної безпеки держави є пріоритетним оскільки безпосередньо від нього залежить безпека суспільства і людини. У час війни публічно-правовий захист виходить за межі традиційного регулювання і поглинає приватно-правові відносини. Необхідно розуміти, що за умов воєнних дій держава часто об’єктивно неспроможна гарантувати права людини в повному об’ємі. Однак збереження фундаментальних засад на основі політичної та правової взаємодії механізмів забезпечення інформаційної безпеки оберігає підвалини демократії та систему загальних принципів права від руйнування волюнтаристськими рішеннями. Якщо війна валить стіни нашої конституційної оселі – міцний фундамент демократизму дасть змогу їх відновити і відбудувати [111, с. 78].

Підсумовуючи все вищевикладене, зазначимо, що правовий режим інформаційної безпеки є фундаментом для захисту національних інтересів в епоху цифрової трансформації України. Його ефективне функціонування залежить від належної законодавчої бази, координації дій органів влади, технологічної інфраструктури та активної участі суспільства.

У сучасних умовах розвитку інформаційного суспільства захист національного інформаційного простору та гарантування інформаційної безпеки давно стали стратегічними пріоритетними завданнями як для України, так і для інших держав світу. Інформаційна безпека є невід'ємною складовою загальної системи національної безпеки, проте водночас може розглядатися як окремий напрям її забезпечення. Враховуючи глобальний характер загроз у цій сфері, виникає необхідність не лише формування ефективної національної стратегії, а й розробки міжнародних механізмів взаємодії для спільного протистояння викликам, що постають перед країнами.

Для України питання інформаційної безпеки на сучасному етапі набуває особливого значення, зумовленого необхідністю протидії незаконним загрозам та інформаційним атакам, спрямованим на її інформаційний простір. З огляду на те, що європейська інтеграція є визначеним стратегічним вектором зовнішньої політики України, важливим завданням для державних органів є розвиток плідної співпраці з ЄС у сфері інформаційної безпеки. Крім того, доцільним вбачається й дослідження та застосування досвіду зарубіжних країн, які вже сформували ефективну організаційно-правову систему у цій сфері, з метою адаптації найкращих практик до українського законодавства та розробки ефективних заходів у сфері захисту інформаційного простору.

2.2 Система суб'єктів адміністративно-правового регулювання в сфері інформаційних технологій

Ефективне адміністративно-правове регулювання сфери інформаційних технологій можливе лише за умови чіткої взаємодії між різними суб'єктами, які мають чітко визначені законодавством повноваження, функції та відповідальність.

Складність адміністративно-правового регулювання в сфері інформаційних технологій визначається її багатоаспектністю, що зумовлює необхідність участі в цьому процесі великої групи різноманітних суб'єктів.

На думку ряду науковців суб'єктний склад виступає одним із критеріїв поділу правового регулювання на державне та недержавне правове регулювання.

Так, на думку Н.А. П'янова, державне правове регулювання – це регулювання, яке здійснюють органи держави, державні організації та державні посадові особи. Такий вид регулювання є визначальним та основним, оскільки норми позитивного права встановлюються та застосовуються переважно цією категорією суб'єктів. Натомість, недержавне правове регулювання – це регулювання, яке здійснюється безпосередньо народом або недержавними органами та організаціями, або учасниками суспільних відносин. Недержавні органи та організації можуть здійснювати правове регулювання тих чи інших суспільних відносин шляхом участі у прийнятті як нормативних правових актів, так і актів застосування права, в свою чергу учасники суспільних відносин можуть здійснювати правове регулювання шляхом упорядкування власних відносин за допомогою індивідуальних правових договорів [112].

Як справедливо визначає В. Смородинський, держава є головним, але не єдиним, суб'єктом правового регулювання, оскільки встановлює переважну більшість правил у цій сфері на рівнях правотворчості та правозастосування. При цьому специфічною властивістю правового

регулювання є його забезпеченість державою, оскільки держава уповноважує органи публічної влади на створення джерел права, здійснення їх оновлення, однакового застосування, забезпечення примусу тощо [113, с. 18]

Під системою суб'єктів адміністративно-правового регулювання в сфері інформаційних технологій слід розуміти сукупність органів законодавчої, виконавчої та судової влади, державних, громадських та інших організацій і об'єднань, а також громадян, які можуть брати участь в адміністративно-правовому регулюванні використання інформаційних технологій відповідно до законодавства, що регламентує відносини у цій сфері.

Ключовими функціями суб'єктів адміністративно-правового регулювання в сфері інформаційних технологій є розробка та впровадження державної політики у сфері цифрових технологій, регулювання діяльності суб'єктів ринку інформаційних технологій, ліцензування операторів телекомунікацій та інтернет-послуг, координація розвитку електронного урядування, забезпечення належного надання цифрових послуг громадянам, а також, безпосередня взаємодія із структурами, що забезпечують інформаційну безпеку та кібербезпеку в Україні.

Суб'єкти, що беруть участь у процесі застосування інформаційних технологій, діють у визначених межах і відповідно до своєї компетенції. В умовах сучасного розвитку, коли належне регулювання використання інформаційних технологій та забезпечення інформаційної безпеки стають ключовими елементами державної політики та гарантією стабільності країни, активне залучення різних суб'єктів до цього процесу є неминучим і виправданим.

Аналізуючи питання публічного управління у сфері інформаційних технологій, першочерговим завданням вбачається формування чіткої термінологічної та категоріальної бази, що дозволить забезпечити ефективне правове регулювання та координацію дій усіх задіяних суб'єктів.

Так, Законом України «Про інформацію» встановлено поняття інформації як будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді [44].

Відповідно до Закону України «Про Національну програму інформатизації», інформаційна технологія – цілеспрямована організована сукупність інформаційних процесів з використанням засобів обчислювальної техніки, що забезпечують високу швидкість обробки даних, швидкий пошук інформації, розосередження даних, доступ до джерел інформації незалежно від місця їх розташування [12].

З огляду на вищенаведені визначення, можна дійти висновку, що ключовими складовими інформаційних технологій є: інформація (у тому числі дані, що являють собою формалізовану інформацію, придатну для автоматичної або автоматизованої обробки), апаратні засоби обчислювальної техніки, відповідне програмне забезпечення, а також засоби передачі, поширення та доступу до інформації незалежно від її місця зберігання.

Основна увага зосереджується на об’єктах, що безпосередньо стосуються сучасних інформаційних технологій, а саме: інфраструктурі, яка забезпечує процеси збору, обробки, зберігання, розповсюдження, пошуку та передачі інформації; інформаційних відносинах, що виникають у процесі використання зазначених технологій.

В умовах сучасних загроз та викликів, що постають перед національною безпекою України в інформаційній сфері, особливу значущість набуває розробка теоретично обґрунтованої класифікації суб’єктів, які беруть участь в адміністративно-правовому регулюванні інформаційних технологій. Незважаючи на динамічність інформаційного середовища та його різноманітність будь-яка класифікація не може бути вичерпною, тим не менш повинна залишатися практичною та ефективною для правозастосування.

Система суб’єктів адміністративно-правового регулювання у сфері інформаційних технологій включає кілька основних груп:

Перша група (державні суб'єкти) – представлені Президентом України, законодавчими, виконавчими та судовими органами, органами місцевого самоврядування. Вони мають різні компетенції, але спільно виконують ключові завдання та функції в цій сфері.

Друга група (недержавні суб'єкти) – поділяються на дві підгрупи: 1) юридичні особи (комерційні компанії, громадські та освітні організації, науково-дослідні інститути, аналітичні центри тощо); 2) фізичні особи (громадяни), які можуть брати участь у розвитку ІТ-сфери та захисті прав користувачів.

Ці групи формують багаторівневу структуру адміністративно-правового регулювання в галузі інформаційних технологій. Держава відіграє провідну роль у цьому процесі, оскільки має необхідні ресурси для реалізації широкого спектра завдань. Вона відповідає за розробку та впровадження нормативно-правових актів, здійснює контроль за їх виконанням, фінансує освітні програми з підготовки фахівців, забезпечує міжнародну співпрацю для протидії транскордонним інформаційним загрозам і сприяє розвитку технологій у сфері інформаційної безпеки.

Ефективна координація між державними органами та приватним сектором є критично важливою для формування надійної системи захисту національної безпеки в інформаційній сфері. Комплексний державний підхід передбачає створення стійкої інформаційної екосистеми, здатної оперативно реагувати на сучасні виклики та загрози.

Громадянське суспільство та окремі громадяни відіграють важливу роль у доповненні діяльності державних органів, привносячи інновації та спеціалізовані знання, які сприяють вирішенню специфічних завдань і розробці новітніх технологічних рішень. Таким чином, значущість кожної з цих груп є незаперечною, оскільки лише спільні зусилля всіх суб'єктів, що входять до єдиної системи адміністративно-правового регулювання в сфері інформаційних технологій, дозволяють забезпечити належне формування, реалізацію та контроль державної політики у цій сфері.

У цьому контексті ключовими чинниками розвитку цифрової економіки, електронного урядування та ринку інформаційних технологій, а також зміцнення національної безпеки в інформаційній сфері є розбудова міжсекторальної співпраці, активне залучення громадянського суспільства до процесів прийняття рішень та поглиблення взаємодії між усіма зацікавленими сторонами.

Організація спільної діяльності суб'єктів адміністративно-правового регулювання інформаційних технологій може здійснюватися через взаємний обмін інформацією, спільне планування та реалізацію заходів, координацію дій у розв'язанні спільних завдань, проведення спеціального моніторингу тощо.

Взаємодія між цими суб'єктами базується щонайменше на трьох напрямках: правовому, організаційному та функціональному.

Правова основа взаємодії визначається нормами Конституції України, законами та підзаконними нормативно-правовими актами, що регулюють їхні повноваження, права, обов'язки та механізми співпраці.

Так, наприклад, Закон України «Про центральні органи виконавчої влади» визначає порядок співпраці міністерств та інших органів виконавчої влади [118].

Закон України «Про місцеві державні адміністрації» визначає порядок взаємодії місцевих державних адміністрацій з органами місцевого самоврядування, їхні повноваження та обов'язки [119].

Відповідно до статті 5 Закону України «Про Національну поліцію», поліція у процесі своєї діяльності взаємодіє з органами державної влади та органами місцевого самоврядування відповідно до закону та інших нормативно-правових актів [81].

Закон України «Про адміністративну процедуру» встановлює єдині, чіткі та зрозумілі правила взаємодії органів влади з громадянами та бізнесом, забезпечуючи законність, визначеність та передбачуваність усіх дій органів влади, що зачіпають права та свободи громадян та бізнесу [120].

Організаційні основи взаємодії суб'єктів адміністративно-правового регулювання формуються на основі внутрішньої організації органів державної влади та юридичних осіб, що діють у публічній сфері.

Ці основи включають розподіл функцій і завдань між суб'єктами, планування їхньої діяльності, проведення спільних заходів.

В якості прикладу організаційної взаємодії на основі внутрішньої організації органів державної влади можна привести взаємодію між Міністерством цифрової трансформації України (Мінцифри) та іншими центральними органами виконавчої влади під час впровадження та подальшого забезпечення електронної системи «Дія» [121].

Суть їх взаємодії полягає у розподілі функцій та завдань. Мінцифри відповідає за загальне стратегічне керівництво, розробку технічних стандартів, створення інфраструктури платформи «Дія». Міністерство юстиції України, в свою чергу, забезпечує інтеграцію своїх реєстрів (державний реєстр актів цивільного стану громадян, реєстр прав власності тощо) до системи «Дія».

Державна податкова служба України надає доступ до реєстрів платників податків. Міністерство внутрішніх справ України забезпечує обмін інформацією через свої реєстри (наприклад, про наявність транспортних засобів та водійських посвідчень).

Крім того, їх взаємодія полягає й у плануванні діяльності, зокрема, спільній розробці етапів інтеграції даних, узгодженні функціональних вимог і стандартів, які забезпечують єдину архітектуру обміну даними, навчанні співробітників державних органів для використання системи (платформи) «Дія», укладанні міжвідомчих меморандумів про співпрацю та створенні міжвідомчої робочої групи, яка координує технічні та організаційні аспекти.

Функціональні основи взаємодії суб'єктів адміністративно-правового регулювання залежать від специфіки функцій, які виконують ті чи інші суб'єкти.

Наприклад, у сфері інформаційних технологій органи виконавчої влади взаємодіють із приватними операторами, забезпечуючи дотримання норм адміністративного права.

Прикладом функціональної взаємодії у сфері інформаційних технологій може бути співпраця Державної служби спеціального зв'язку та захисту інформації України (ДССЗЗІ) із приватними операторами зв'язку та провайдерами інтернет-послуг.

Так, суть їх взаємодії полягає у контролі виконання адміністративно-правових норм. Зокрема, ДССЗЗІ забезпечує виконання вимог закону щодо захисту інформації, яка передається через телекомунікаційні мережі. А приватні оператори та провайдери зобов'язані дотримуватися нормативно-правових актів щодо безпеки інформації, зокрема, встановлювати засоби захисту та здійснювати моніторинг безпеки передачі даних.

ДССЗЗІ надає методичну допомогу та рекомендації провайдерам щодо побудови захищених каналів зв'язку та протидії кіберзагрозам. Приватні оператори реалізують ці рекомендації на своїй інфраструктурі, забезпечуючи надійність передачі даних. У разі виявлення кіберзагроз (наприклад, атаки на державні чи приватні інформаційні ресурси), оператори зв'язку зобов'язані оперативно інформувати ДССЗЗІ, який в свою чергу координує заходи з ліквідації загрози, залучаючи відповідні підрозділи.

Доцільно вбачається розглянути взаємозв'язок суб'єктів адміністративно-правового регулювання в сфері інформаційних технологій з розвитком електронного урядування як двох взаємопов'язаних елементів забезпечення цифрової трансформації публічного управління України.

Як було вказано вище, систему суб'єктів адміністративно-правового регулювання в сфері інформаційних технологій складають органи державної влади та місцевого самоврядування. Субсидіарно функцію впровадження електронного урядування забезпечують суб'єкти господарювання, які надають послуги зі створення інформаційно-комунікаційних продуктів,

громадські організації шляхом участі у формування державної політики у сфері діджиталізації.

Також, виокремити відповідальні органи державної влади дозволяє аналіз засадничих нормативно-правових актів щодо стратегії впровадження електронного урядування, зокрема, Державної стратегії регіонального розвитку на 2021–2027 роки [115], Стратегії реформування державного управління на період на 2022-2025 роки [116], Концепції розвитку електронного урядування в Україні [117].

Відповідно до Концепції розвитку електронного урядування відповідальними органами є Державне агентство з питань електронного урядування, центральні органи виконавчої влади за відповідними напрямами, органи місцевого самоврядування, підприємства, установи та організації комунальної форми власності. Державною стратегією регіонального розвитку передбачено відповідальні органи: Міністерство цифрової трансформації, Національна комісія, що здійснює державне регулювання у сфері зв'язку та інформатизації.

Систему суб'єктів впровадження електронного урядування доцільно поділити на дві групи: суб'єкти публічного сектору та суб'єкти громадського сектору. У структурі суб'єктів публічного сектору доцільно виокремити органи державної влади загальної компетенції (Верховна Рада України, Президент України, КМУ), центральні органи спеціальної компетенції (Міністерство цифрової трансформації, Національна комісія, що здійснює державне регулювання у сфері зв'язку та інформатизації); центральні органи спеціальної компетенції за сферами управління (Міністерство юстиції України, Міністерство економіки України, Міністерство інфраструктури України, Міністерство освіти і науки України, Міністерство охорони здоров'я України, Міністерство соціальної політики, Міністерство фінансів України, відповідні служби та агентства та інші), органи місцевого самоврядування.

Державні органи загальної компетенції формують та впроваджують політику держави у сфері застосування інформаційних технологій та розвитку електронного урядування.

Зокрема, Верховною Радою України прийнято низку законів: «Про електронні комунікації», «Про електронні довірчі послуги», «Про електронну комерцію», «Про режим спільного транзиту та запровадження національної електронної транзитної системи», «Про стимулювання розвитку цифрової економіки в Україні», «Про основні засади забезпечення кібербезпеки в Україні», «Про адміністративні послуги», «Про національну інфраструктуру геопросторових даних» тощо.

Президент України також відіграє ключову роль у формуванні та реалізації державної політики у сфері інформаційних технологій, зокрема через затвердження стратегій та координацію діяльності виконавчих органів у сфері інформаційних технологій.

В якості прикладу, що підтверджує повноваження Президента України у сфері інформаційних технологій можна навести: Стратегію кібербезпеки України 2021 року (Указ Президента України №447/2021 від 26 серпня 2021 року, яким було затверджено рішення Ради національної безпеки і оборони України про Стратегію кібербезпеки України) [80]. Цей документ визначає пріоритети національних інтересів у сфері кібербезпеки та встановлює цілі й завдання для розбудови національної системи кібербезпеки; Стратегію інформаційної безпеки України 2021 року (Указ Президента України №685/2021 від 28 грудня 2021 року, який ввів у дію рішення Ради національної безпеки і оборони України про Стратегію інформаційної безпеки) [105]. Цей документ визначає актуальні виклики та загрози національній безпеці в інформаційній сфері, а також стратегічні цілі та завдання для протидії таким загрозам; План реалізації Стратегії кібербезпеки України (Указ Президента України №37/2022 від 1 лютого 2022 року вводить у дію рішення Ради національної безпеки і оборони України про План реалізації Стратегії кібербезпеки України) [122]. Цей план деталізує заходи

та механізми впровадження положень Стратегії кібербезпеки, забезпечуючи координацію між різними державними органами та інституціями.

Впровадження державної політики у сфері електронного урядування включає щорічну підготовку та подання Кабінетом Міністрів України на розгляд Верховної Ради України звіту щодо стану інформатизації в державі. Крім того, уряд визначає пріоритети Національної програми інформатизації на три роки вперед, а також розробляє програму завдань та заходів з інформатизації на наступний бюджетний рік. Щорічно Верховна Рада України затверджує завдання Національної програми інформатизації на найближчі три роки, а також обсяги їх фінансування з державного бюджету на наступний рік [122].

Міністерство цифрової трансформації як орган спеціальної компетенції реалізує державну політику у сферах цифровізації, цифрового розвитку, цифрової економіки, цифрових інновацій та технологій; електронного урядування та електронної демократії, розвитку інформаційного суспільства; впровадження електронного документообігу, розвитку цифрових навичок та цифрових прав громадян; відкритих даних, розвитку національних електронних інформаційних ресурсів та інтероперабельності, розвитку інфраструктури широкосмугового доступу до Інтернету та телекомунікацій, електронної комерції та бізнесу; надання електронних та адміністративних послуг; електронних довірчих послуг та електронної ідентифікації та інвестицій в ІТ-індустрію; розвитку ІТ-індустрії [122].

Національна комісія, що здійснює державне регулювання у сфері зв’язку та інформатизації, є органом державного регулювання у сфері телекомунікацій, інформатизації, користування радіочастотним ресурсом та надання послуг поштового зв’язку. У визначеній сфері комісія здійснює повноваження органу ліцензування, дозвільного органу, регуляторного органу та органу державного нагляду (контролю) [122].

Державна служба спеціального зв’язку та захисту інформації України є центральним органом виконавчої влади зі спеціальним статусом, який

забезпечує формування та реалізацію державної політики у сферах спеціального зв'язку, захисту інформації, кіберзахисту та активної протидії агресії у кіберпросторі. Її повноваження та функції у сфері інформаційних технологій підтверджуються наступними нормативно-правовими актами.

Закон України «Про Державну службу спеціального зв'язку та захисту інформації України» встановлює правові основи діяльності служби, визначаючи її як спеціально уповноважений центральний орган виконавчої влади у сфері захисту інформації та спеціального зв'язку [123].

Постанова Кабінету Міністрів України від 3 вересня 2014 р. №411 «Про затвердження Положення про Адміністрацію Державної служби спеціального зв'язку та захисту інформації України» визначає основні завдання та функції Держспецзв'язку, зокрема у сферах криптографічного та технічного захисту інформації, телекомунікацій, користування радіочастотним ресурсом, урядового фельд'єгерського зв'язку та кіберзахисту [124].

Законом України «Про захист інформації в інформаційно-комунікаційних системах» визначено правові та організаційні основи захисту інформації в інформаційно-комунікаційних системах, де Держспецзв'язку виступає як регулятор та контролюючий орган [46].

Центральним органам спеціальної компетенції делегуються повноваження з використання інформаційних технологій та впровадження електронного урядування за певними напрямами.

Міністерство економіки України надає пропозиції щодо формування та реалізації державної політики у сфері надання адміністративних послуг; бере участь у формуванні та реалізації державної політики у сфері інформатизації, розвитку електронного урядування, побудови сучасного інформаційного суспільства в державі; забезпечує в межах повноважень, передбачених законом, впровадження сучасних інформаційно-телекомунікаційних технологій, створення системи національних інформаційних ресурсів.

Міністерство юстиції забезпечує формування та реалізацію державної політики у сфері державної реєстрації актів цивільного стану, державної реєстрації речових прав на нерухоме майно та їх обтяжень, державної реєстрації обтяжень рухомого майна, державної реєстрації юридичних осіб, громадських формувань, що не мають статусу юридичної особи, та фізичних осіб-підприємців, реєстрації статуту територіальної громади м. Києва, реєстрації статутів Національної академії наук та національних галузевих академій наук, державної реєстрації друкованих засобів масової інформації та інформаційних агентств як суб'єктів інформаційної діяльності; формує і веде онлайн-реєстри: Державний реєстр актів цивільного стану громадян; Державний реєстр речових прав на нерухоме майно; Єдиний державний реєстр юридичних осіб, фізичних осіб-підприємців та громадських формувань; Єдиний реєстр громадських формувань; Реєстр громадських об'єднань; Державний реєстр друкованих засобів масової інформації та інформаційних агентств як суб'єктів інформаційної діяльності; Реєстр символіки громадських об'єднань.

Державна архівна служба України забезпечує створення, зберігання та використання архівних електронних документів; розробляє вимоги до оформлення документів, організації електронного документообігу; бере участь у реалізації державної інформаційної політики у сфері створення, використання та оновлення державних інформаційних ресурсів, а також у сфері технічного захисту інформації в інформаційно-телекомунікаційних системах Державної архівної служби України, державних архівних установ, науково-дослідних установ та спеціальних установ страхового фонду документації.

Інші центральні органи виконавчої влади у межах своєї компетенції забезпечують електронний документообіг, надання адміністративних послуг онлайн, виступають розпорядниками електронних реєстрів, баз даних.

Органи місцевого самоврядування як суб'єкти адміністративно-правового регулювання в сфері інформаційних технологій мають дещо

обмежені повноваження у сфері інформаційних технологій, особливо порівнюючи їх з державними органами загальної компетенції, але тим не менш відіграють важливу роль у розвитку локальної інформаційної інфраструктури, організації заходів із підвищення цифрової грамотності населення, взаємодії з центральними органами виконавчої влади у реалізації національних цифрових програм.

До наступної групи суб'єктів адміністративно-правового регулювання в сфері інформаційних технологій та електронного урядування належить громадський сектор.

Громадський сектор відіграє важливу роль у сфері інформаційних технологій в Україні. До цього сектору належать: комерційні компанії, підприємства, організації та фізичні особи-підприємці, які розробляють, впроваджують та використовують ІТ-рішення, цифрову продукцію, а також, громадянське суспільство та громадяни України.

Зазначимо, що приватні компанії є провідними рушіями технологічного прогресу, розробляючи нові продукти та послуги, що сприяють цифровій трансформації суспільства. Окрім того, відповідні компанії часто взаємодіють з органами державної влади у реалізації спільних проектів, таких як розвиток електронного урядування чи надання електронних послуг громадянам. Приватні ІТ-компанії беруть участь у громадських обговореннях та надають експертні висновки щодо регулювання ІТ-сфери. Така взаємодія сприяє створенню сприятливого бізнес-середовища та забезпечує баланс між інтересами держави та громадського сектору.

Система суб'єктів адміністративно-правового регулювання в сфері інформаційних технологій представлена також громадянським суспільством та громадянами України.

Ці суб'єкти відіграють не менш важливу роль у сфері інформаційних технологій в Україні ніж інші вищепредставлені групи. Їхня участь, зокрема, забезпечує демократичний контроль, сприяє розвитку інформаційних технологій та захисту прав користувачів.

Громадські організації здійснюють нагляд за діяльністю державних органів та приватних компаній у сфері інформаційних технологій, забезпечуючи прозорість та підзвітність їхньої роботи.

Інститути громадянського суспільства відстоюють права користувачів, зокрема щодо захисту персональних даних, свободи слова в інтернеті та доступу до інформації. Окрім того, громадяни та їх об'єднання беруть участь у розробці нормативно-правових актів, надаючи експертні пропозиції та зауваження, що враховуються під час ухвалення рішень.

Громадські організації проводять тренінги, семінари та інформаційні кампанії, спрямовані на підвищення цифрової грамотності населення.

Громадяни можуть ініціювати розгляд питань, пов'язаних з інформаційними технологіями, через подання електронних петицій до органів влади, участі в онлайн-голосуванні тощо.

Громадські ініціативи часто стають каталізаторами впровадження нових технологій та рішень у суспільстві.

Організації громадянського суспільства активно працюють над захистом прав користувачів в цифровому середовищі, протидіючи цензурі та незаконному збору даних.

Цікавою та не менш цінною вбачається систематизація суб'єктів в сфері інформаційних технологій та електронного урядування представлена іншими науковцями. Так, зокрема, В. Марченко виокремлює наступні види суб'єктів електронного урядування: 1) Президент України; 2) Верховна Рада України; 3) Кабінет Міністрів України; 4) органи місцевого самоврядування; 5) фізичні особи: громадяни України, іноземці, апатриди, біпатриди, біженці, переміщенні особи; 6) юридичні особи: підприємства, установи, організації; 7) колективні утворення: громадські організації та інші громадські об'єднання, політичні партії; 8) інші специфічні суб'єкти у сфері електронного урядування: робоча група з розробки урядової політики в сфері розвитку електронного урядування при Віце-прем'єр-міністрові України – Міністрові регіонального розвитку, будівництва та житлово-комунального

господарства України, інші робочі та експертні групи, центр надання адміністративних послуг, адміністратор, суб’єкти звернення, підписувачі; користувачі; центр сертифікації ключів; засвідчувальний центр тощо [125].

Взагалі у науковій літературі існують дві протилежні позиції щодо складу суб'єктів електронного урядування. Перша точка зору полягає в тому, що розширене використання інформаційних технологій може зменшити роль державних органів у процесі ухвалення управлінських рішень, оскільки за умов «електронної демократії» забезпечується більш активна участь громадян у процесах публічного управління. Натомість друга концепція стверджує, що цифровізація, навпаки, сприятиме посиленню ролі державних установ, підвищенню ефективності їх роботи та, відповідно, зростанню їх значущості [125].

Проведений нами аналіз підтверджує обґрунтованість другої концепції, оскільки навіть за умови широкого впровадження інформаційно-комунікаційних технологій залишається необхідність ухвалення дискреційних рішень органами влади, а також забезпечення належного функціонування цифрової інфраструктури. Водночас електронне урядування сприяє активній взаємодії держави з інститутами громадянського суспільства, залученню громадян до процесу ухвалення управлінських рішень, що створює умови для підвищення прозорості та ефективності публічного управління.

Таким чином, запропонована класифікація дозволяє чітко окреслити межі правового регулювання та управління у сфері застосування інформаційних технологій, враховуючи рівні відповідальності та повноваження визначених груп. Вона сприяє створенню цілеспрямованих нормативно-правових актів, які можуть охоплювати як окремих суб’єктів, так і їх об’єднання чи всю систему загалом. Такий підхід забезпечує формування стабільної та гнучкої системи адміністративно-правового регулювання в сфері інформаційних технологій, здатної оперативно адаптуватися до змін у внутрішньому та зовнішньому середовищі.

Підводячи підсумки необхідно зазначити, що система суб'єктів адміністративно-правового регулювання у сфері інформаційних технологій охоплює широкий спектр учасників, які діють на різних рівнях та виконують різноманітні функції, спрямовані на формування, впровадження і контроль державної політики в сфері використання інформаційних технологій.

Відповідна взаємодія між суб'єктами регулювання базується на правовій, організаційній та функціональній основах, що гарантує ефективність реалізації завдань у сфері інформаційних технологій. Залучення кожної групи суб'єктів до цього процесу дозволяє забезпечити прозорість, підзвітність і стабільний розвиток інформаційного суспільства в Україні, сприяючи цифровій трансформації та інтеграції новітніх технологій у всі сфери суспільного життя.

2.3 Адміністративні процедури в регулюванні інформаційних технологій

Сучасний стан правового регулювання публічного адміністрування в Україні дає підстави стверджувати, що його реалізація здебільшого здійснюється через процедурні правовідносини. Це стосується як виконання зовнішніх функцій суб'єктів публічної адміністрації у їх правових формах, так й організації внутрішніх процесів у самій публічній адміністрації.

І. Юрійчук справедливо вказує, що категорія адміністративних процедур є відносно новою в адміністративному праві й досі не набула чітко усталеного змістового визначення. На думку автора термін «адміністративна процедура» складається з двох ключових понять. По-перше, «процедура» визначається як упорядкований процес виконання певних дій для досягнення конкретного результату. По-друге, поняття «адміністративний» у правовій науці може означати як управлінський аспект, так і функцію, що має обслуговуючий характер. Така подвійна інтерпретація визначального поняття адміністративного права пояснює існування двох видів правовідносин у

сфері публічного управління. Перший тип охоплює відносини управлінського характеру, що виникають за ініціативою владних суб'єктів та передбачають покладання переважно обов'язків на приватних осіб. Другий тип охоплює взаємодію приватних осіб із публічною адміністрацією, у межах якої реалізується значний обсяг прав приватних осіб. Врегулювання цих двох типів правовідносин вимагає застосування різних принципів та підходів [128, с. 151].

На сучасному етапі розвитку адміністративного права України поняття «адміністративна процедура» не має однозначного визначення у вітчизняній науці та чіткої відмінності від терміна «адміністративний процес». Дискусії щодо співвідношення цих понять тривають, що зумовлює відсутність єдиного підходу до їхнього тлумачення. Однак останнім часом у науковому середовищі все частіше виділяють «адміністративні процедури» як окремий інститут адміністративного права, який виходить за межі адміністративного процесу [128, с. 151].

Варто зазначити, що правове регулювання адміністративних процедур у різний час досліджували такі науковці, як В. Авер'янов, Ю. Басова, В. Бевзенко, С. Братель, О. Буханевич, В. Галунько, Н. Губерська, О. Левченко, А. Луцик та інші [127, с. 57; 129, с. 693; 130, с. 122; 131, с. 100; 132, с. 128; 133; 134, с. 107; 135; 136; 137, с. 12].

Науковці мають різні підходи до розуміння адміністративних процедур. Одні вважають їх частиною адміністративного процесу, інші – окремою правовою категорією. Юрисдикційний підхід визначає адміністративний процес як вирішення спорів, тоді як процедури розглядаються як регламентована діяльність органів влади. Управлінська концепція передбачає поділ на адміністративно-процедурну та адміністративно-юрисдикційну діяльність.

Окрім того, адміністративна процедура визначається як послідовний порядок дій, встановлений адміністративно-правовими нормами для розгляду індивідуальних справ. Науковці трактують її по-різному: одні акцентують на

правозастосуванні, інші – на процедурно-процесуальній формі, нормативному порядку ухвалення рішень чи механізмі реалізації прав.

Необхідно визнати, що адміністративні процедури та адміністративний процес є самостійними правовими категоріями. Так, на нашу думку В. Бевзенко справедливо розмежовує їх, відносячи перше до матеріального адміністративного права, а друге – до адміністративно-процесуального права, яке охоплює судовий захист прав і свобод. Такий підхід підтверджує тезу про те, що адміністративні процедури спрямовані на реалізацію прав, а адміністративний процес – на їх охорону [127; 128, с. 153].

Та попри відмінності в підходах, загальновизнаним фактом є те, що адміністративні процедури впорядковують діяльність органів влади, забезпечують відкритість, ефективність управлінських рішень і запобігають зловживанням, а також, відіграють ключову роль у забезпеченні взаємодії громадян із державою та сприяють балансу між владними повноваженнями та правами особи.

Безумовно адміністративні процедури є важливим інструментом реалізації державної політики й у сфері інформаційних технологій. Вони забезпечують чіткість, прозорість та ефективність регулювання, створюючи умови для взаємодії між державними органами, приватним сектором та громадянським суспільством у цій сфері.

Останніми роками Україна цілеспрямовано рухається в напрямку розвитку цифрових технологій, їх впровадження у всі сфери життєдіяльності. Не обійшла цифровізація й публічне адміністрування України.

З кожним роком все більше зростає обсяг комунікацій між громадянами та органами державної й муніципальної влади за допомогою інформаційно-телекомунікаційних технологій.

Так, І. Бойко зазначає, що пандемія та війна тільки прискорили процеси впровадження інформаційних технологій в усіх сферах життя. Адже люди, які опинилися спочатку в умовах вимушеної ізоляції, а потім мусили рятувати своє життя, покидати домівки, потребували послуг і допомоги від

влади; це підштовхнуло державу шукати шляхи забезпечення ефективної комунікації для задоволення потреб людей через використання цифрових технологій [138, с. 130].

Вже запроваджені в Україні механізми електронного урядування сприяють прозорості державної влади, покращенню доступу до послуг, оперативному вирішенню питань і спрощенню комунікації.

Термін «цифровізація» став невід'ємною частиною як національного правового простору, так і практичної діяльності. Його походження пов'язують із директором медіа-лабораторії Массачусетського технологічного інституту Ніколасом Негропонте, який ще у 90-х роках XX століття у своїй книзі Being Digital («Бути цифровим») описав поступову цифрову трансформацію суспільства. Він передбачав, що в майбутньому все, що можливо оцифрувати, неодмінно буде переведено в цифровий формат. Його ідеї стали основою сучасного розуміння процесу цифровізації [139].

Цифровізація сприяє підвищенню оперативності та гнучкості управлінських процесів, роблячи адміністративні послуги більш доступними для громадян. Це, в свою чергу, дозволяє значно скоротити витрати на утримання апарату державних службовців, оптимізуючи бюджетні ресурси.

Серед істотних переваг цифровізації у сфері публічного адміністрування варто відзначити швидкість ухвалення рішень, ефективний контроль за їх виконанням, а також усунення черг при отриманні адміністративних і публічних послуг. У період дії правового режиму воєнного стану цифрові технології набувають ще більшого значення, оскільки сприяють раціональному використанню обмежених державних ресурсів.

У багатьох країнах світу питання розвитку цифрової економіки та суспільства винесено на рівень державної політики, що підтверджується ухваленими стратегіями та програмами цифрового розвитку. Зокрема, у Данії така стратегія з'явилася у 2000 році, у Сінгапурі — у 2005-му, а в Європейському Союзі, Великій Британії, Австралії, Гонконзі та Новій

Зеландії — у 2009 році. У Канаді стратегія цифрової економіки була прийнята у 2010 році, у Малайзії — у 2012-му, у Південній Кореї — у 2013-му, а в Індії та Казахстані — у 2015 році [140, с. 5].

Концептуальний вираз цифровізації процесів управління Кабінет Міністрів України втілив у Концепції розвитку електронного урядування в Україні та схваленій ним Стратегії здійснення цифрового розвитку, цифрових трансформацій і цифровізації системи управління державними фінансами на період до 2025 року [141].

Україна долучилася до Програми «Цифрова Європа» до 2027 року, що надає фінансування для цифровізації країн Європи за різними напрямами. Мета «Цифрової Європи» – пришвидшення відновлення економіки та цифрова трансформація. Участь у Програмі наблизить Україну до Єдиного цифрового ринку ЄС [142].

В основу української моделі цифровізації закладено концепцію трансформації соціального середовища шляхом адаптації громадян до комфортного отримання цифрових послуг, що спочатку було характерним західним розвиненим національним економікам.

Останніми роками відбулися значні зміни в правовому регулюванні адміністративних процедур, насамперед завдяки ухваленню ключових законодавчих актів, що визначають особливості процедурних правовідносин у сфері публічного адміністрування.

Правове регулювання адміністративних процедур здійснюється з урахуванням процесів їх цифровізації. Оцифрування суспільних відносин охоплює різні аспекти життєдіяльності сучасного суспільства, включаючи механізми реалізації публічної влади через функціонування публічного адміністрування. Це обумовлює необхідність адаптації правових інститутів, у тому числі й адміністративних процедур, до нових суспільних відносин, що формуються в умовах впровадження цифрових технологій. Варто погодитися з думкою, що цифровізація не лише змінює способи взаємодії між сторонами

публічно-владних відносин, а й безпосередньо впливає на зміст адміністративних процедур [143].

Водночас адміністративні процедури, реалізовані в електронній формі, зберігаючи свою основну функцію впорядкування виконання повноважень суб'єктами публічного адміністрування у встановлених правових межах, забезпечують фактичну взаємодію учасників правовідносин через застосування інформаційно-комунікаційних технологій. У цьому процесі здійснюється реалізація суб’єктивних прав та юридичних обов’язків сторін, що визначає фактичний зміст правовідносин.

Дослідження процедурних аспектів адміністративно-правового забезпечення розвитку інформаційних технологій в Україні можливе лише на підставі аналіз нормативно-правових актів, які безпосередньо регулюють діяльність органів публічного управління у цій сфері. З огляду на значний обсяг джерел адміністративного права, що стосуються цифрової трансформації, питання визначення та характеристика адміністративних процедур у сфері адміністративно-правового регулювання інформаційних технологій набуває особливої актуальності та потребує ґрунтовного наукового дослідження.

На наш погляд, адміністративні процедури у сфері адміністративно-правового регулювання інформаційних технологій в Україні варто класифікувати саме за їх змістовним наповненням на: 1) управлінські; 2) реєстраційні; 3) організаційно-кадрові; 4) дозвільно-ліцензійні; 5) контрольні; 6) процедури інтернаціоналізації.

На думку М. Білей управлінські процедури в частині реалізації організаційної функції публічного управління, стосуються створення, перетворення та ліквідації органів державної влади, державних та комунальних підприємств, установ та організацій; укладення відповідних управлінських договорів про співробітництво між органами державного управління; прийняття рішень, що забезпечують ресурсний потенціал державного управління [144].

Н. Христинченко відзначає, що управлінські адміністративні процедури є одними із найбільш важливих та необхідних у науковій сфері, адже вони виражають волю в тому чи іншому управлінському рішенні, що приймається уповноваженим на те органом влади, який здійснює реалізацію державної політики в зазначеній сфері. Тобто вони вказують на певний порядок управління, яким чином посадо ва особа наукової установи чи інший орган має діяти для того, щоб його діяльність була законною та відповідала встановленим нормативно-правовим приписам [145, с. 166].

Управлінські процедури в сфері адміністративно-правового регулювання інформаційних технологій в Україні включають розробку нормативно-правових актів, які визначають державну політику та стратегічний розвиток галузі, прогнозування та визначення пріоритетів, реалізацію державних програм, моніторинг ефективності політики, а також управління суб'єктами публічного адміністрування.

Загалом, ці процедури є нормативно визначеним процесом ухвалення стратегічних і секторальних рішень у сфері інформаційних технологій, що забезпечують ефективне публічне адміністрування та розвиток галузі в межах законодавчих вимог.

Управлінські процедури у сфері адміністративно-правового регулювання інформаційних технологій спрямовані на формування та реалізацію державної політики у сфері інформаційних технологій. Вони охоплюють: розробку державних програм та стратегій розвитку цифрової економіки, встановлення стандартів і регламентів використання інформаційних технологій у публічному управлінні, впровадження системи електронного урядування, організацію діяльності органів державної влади, відповідальних за цифрову трансформацію (наприклад, Міністерство цифрової трансформації України).

У процесі формування демократичної правової держави особливу значущість мають реєстраційні процедури. Так, К. Куркова зазначає, що під поняттям реєстраційні процедури слід розуміти визначений чинним

законодавством порядок діяльності органів публічного управління, спрямований на документальне підтвердження правового статусу суб’єкта або надання нових правових ознак об'єкту. Основними завданнями реєстраційних процедур є: офіційне закріплення певного права за особою; офіційне підтвердження законності правових актів; засвідчення визначеного статусу фізичних чи юридичних осіб; облік юридично значущих фактів [146, с. 59].

Реєстраційні процедури у сфері адміністративно-правового регулювання інформаційних технологій в Україні охоплюють механізми офіційної фіксації даних, що мають юридичне значення у сфері інформаційних технологій. До них належать: державна реєстрація суб'єктів господарювання у сфері інформаційних технологій, реєстрація доменних імен в українському сегменті інтернету, включення підприємств до реєстру ІТ-індустрії (наприклад, реєстрація в Дія.City), реєстрація об’єктів інтелектуальної власності, зокрема програмного забезпечення, а також, внесення інформації до Єдиного державного реєстру програмних продуктів.

Важливими у сфері адміністративно-правового регулювання інформаційних технологій також є адміністративні процедури, що стосуються кадрового потенціалу інформаційно-технологічної сфери – організаційно-кадрові процедури.

Організаційно-кадрові процедури регламентують питання кадрового забезпечення в державних органах, задіяних у сфері інформаційних технологій, а також діяльність відповідних установ: призначення та звільнення посадових осіб, відповідальних за цифрову трансформацію України, атестацію державних службовців у сфері кібербезпеки та цифровізації, сертифікацію фахівців з кібербезпеки, адміністрування державних баз даних, формування навчальних програм та підготовка кадрів для публічного управління у сфері інформаційних технологій.

Загалом, можна вважати, що організаційно-кадрові процедури у сфері адміністративно-правового регулювання інформаційних технологій – це

внутрішньоорганізаційна процедурна діяльність з призначення, переведення, звільнення, заохочення, стажування, підвищення кваліфікації, атестації суб'єктів інформаційно-технологічної діяльності з метою забезпечення належної кадрової політики у площині інформаційно-технологічного розвитку [146, с. 61].

Ще одним видом адміністративних процедур в означеній сфері є дозвільно-ліцензійні процедури.

Так, Н. Христинченко під дозвільними процедурами розуміє встановлений чинним законодавством порядок діяльності суб'єктів публічного адміністрування, за результатами якої надаються дозволи на провадження певних видів діяльності та здійснення юридично значущих дій. Ключовими цілями дозвільних процедур є: забезпечення безпеки громадян та інтересів держави; надання можливостей для реалізації певних прав особи, передусім у сфері економічної діяльності; унормування контролю за діяльністю, щодо якої суб'єктом публічного адміністрування надано дозвіл [145, с.167; 146, с. 61].

В свою чергу О. Джафарова та К. Куркова вказують, що сутність дозвільних процедур полягає в тому, що ця діяльність урегульована нормами адміністративно-процесуального права, знаходиться у межах повноважень органів публічної влади, визначена чинним законодавством, спрямована на реалізацію норм адміністративно го матеріального права, а також матеріально-правових норм інших галузей права у процесі вирішення конкретних справ щодо забезпечення прав, свобод, законних інтересів фізичних та юридичних осіб тощо. Більшість послуг, що надаються органами публічної адміністрації, має саме дозвільний характер, оскільки їхнім результатом є видача документа, який підтверджує статус суб'єкта чи об'єкта, дозволяє реалізувати конституційні права або засвідчує юридичну чинність певних дій чи послуг [146, с. 62; 147].

Щодо місця дозвільно-ліцензійних процедур в площині інформаційно-технологічної діяльності, слід сказати, що ці процедури пов'язані з видачею

дозволів і ліцензій на певні види діяльності у сфері інформаційних технологій. Вони включають: ліцензування діяльності у сфері надання телекомунікаційних послуг, отримання дозволів на використання криптографічних засобів та електронних цифрових підписів, сертифікацію програмного забезпечення, що використовується в державних структурах.

Важливе місце в системі адміністративних процедур у сфері адміністративно-правового регулювання інформаційних технологій в Україні займають контрольні процедури, спрямовані на забезпечення ефективного функціонування інформаційно-технологічної сфери в цілому.

Під контрольними процедурами вчені розуміють встановлений чинним законодавством порядок втручальної контрольно-наглядової діяльності суб'єктів публічного адміністрування, яка полягає у здійсненні перевірки дотримання законів та інших нормативно-правових актів. Ключовими цілями контрольних процедур є: запобігання вчиненню правопорушень з боку об'єкта перевірки; належне реагування на звернення фізичних та юридичних осіб з приводу ймовірних порушень чинного законодавства в діяльності об'єкта перевірки; самостійне виявлення порушень чинного законодавства в діяльності об'єкта перевірки [146, с. 62].

Контрольні процедури у сфері адміністративно-правового регулювання інформаційних технологій встановлюють механізми державного нагляду та контролю за дотриманням вимог у сфері інформаційних технологій. Вони включають: державний контроль за кібербезпекою та захистом критичної інформаційної інфраструктури, перевірку виконання вимог ліцензійних умов у сфері телекомунікацій, моніторинг виконання нормативних актів щодо захисту персональних даних, контроль за правомірністю використання державних інформаційних ресурсів.

До наведених вище видів адміністративних процедур у сфері адміністративно-правового регулювання інформаційних технологій варто також віднести процедуру інтернаціоналізації.

Процедури інтернаціоналізації інформаційно-технологічного розвитку передбачають діяльність органів публічної адміністрації, спрямовану на міжнародну співпрацю, адаптацію до світових стандартів, залучення інвестицій, підвищення конкурентоспроможності галузі та розвиток освітніх програм. Вони охоплюють гармонізацію законодавства з міжнародними нормами, участь у глобальних проєктах із кібербезпеки, співпрацю з іноземними партнерами та використання міжнародних платформ для обміну цифровими даними.

Поділ адміністративних процедур у сфері інформаційних технологій за змістовним наповненням дозволяє систематизувати діяльність держави, встановити чіткі механізми правового регулювання та сприяти розвитку цифрової інфраструктури України. Кожна група процедур відіграє важливу роль у забезпеченні ефективного функціонування інформаційних технологій в Україні та їх безпечного використання.

Підсумовуючи, можемо зробити висновок, що адміністративні процедури у сфері адміністративно-правового регулювання інформаційних технологій України – це діяльність суб'єктів публічної адміністрації, що має публічний, нормативно визначений, логічний характер, спрямована на впорядкування управлінських, реєстраційних, організаційно-кадрових, дозвільно-ліцензійних, контрольних, інтернаціоналізаційних правовідносин інформаційно-технологічного розвитку для уніфікації адміністративної практики суб'єктів публічної адміністрації, належного публічного адміністрування інформаційно-технологічної сфери та захисту прав суб'єктів інформаційно-технологічної діяльності.

Нормативним підґрунтям процедурних відносин у інформаційно-технологічній (цифровій) сфері виступають як правові акти, що визначають загальні засади правових відносин у цифровій формі, так і спеціальні правові акти, якими регламентовано адміністративні процедури або деякі особливості розгляду адміністративних справ, зокрема у цифровій формі. До першої групи можна віднести Закон України «Про електронні

комунікації» від 16.12.2020 р., яким визначено основи державної політики у сферах передавання та/або приймання інформації незалежно від її виду або типу у вигляді електромагнітних сигналів за допомогою технічних засобів електронних комунікацій та радіочастотного спектра, а також права, обов'язки та відповідальність фізичних і юридичних осіб, які беруть участь у відповідній діяльності або користуються електронними комунікаційними послугами [148].

Правові відносини, які виникають при наданні послуг з надання будь-яких технічних та програмних засобів або інших компонентів інформаційної (автоматизованої) системи, які доступні за допомогою технології хмарних обчислень, такі як процесорний час (обчислювальна потужність), місце в сховищах даних, обчислювальні мережі, бази даних і комп'ютерні програми, а також особливості використання хмарних послуг органами державної влади, органами влади Автономної Республіки Крим, органами місцевого самоврядування, військовими формуваннями, утвореними відповідно до законів України, державними підприємствами, установами та організаціями, суб'єктами владних повноважень та іншими суб'єктами, яким делеговані такі повноваження, врегульовано Законом України «Про хмарні послуги» від 17.02.2022 р. [149].

Принципи створення та функціонування інформаційно-комунікаційних систем, що забезпечують збирання, накопичення, захист, облік, відображення, оброблення електронних даних та надання відповідної інформації визначено Законом України «Про публічні електронні реєстри» від 18.11.2021 р. [150].

Відносини у сферах електронної ідентифікації, як використання ідентифікаційних даних особи в електронній формі, які однозначно визначають фізичну, юридичну особу або уповноваженого представника юридичної особи та надання електронних довірчих послуг, що надаються для забезпечення електронної взаємодії двох або більше суб'єктів, врегульовано

Законом України «Про електронну ідентифікацію та електронні довірчі послуги» від 05.10.2017 р. [62].

Основним законодавчим актом, що встановлює засади електронного документообігу як сукупності процесів створення, оброблення, правлення, передавання, одержання, зберігання, використання та знищення документів, інформацію в яких зафіксовано у вигляді електронних даних, включаючи обов'язкові реквізити документа (електронні документи), які виконуються із застосуванням перевірки цілісності та у разі необхідності з підтвердженням факту одержання таких документів та використання електронних документів, є Закон України «Про електронні документи та електронний документообіг» від 22.05.2003 р. [61].

Відносини у сфері діяльності, що спрямована на запобігання несанкціонованим діям щодо інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах, урегульовано Законом України «Про захист інформації в інформаційно-комунікаційних системах» від 05.07.1994 р. [46].

Законом України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 р. визначено правові та організаційні основи забезпечення захисту життєвоважливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері захищеності життєвоважливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі (кібербезпека) та повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки. [80].

Правові відносини, пов’язані із захистом і обробкою персональних даних, зокрема й відносини з обробки персональних даних, яка здійснюється повністю або частково із застосуванням автоматизованих засобів, урегульовано Законом України «Про захист персональних даних» від 01.06.2010 р. [70].

Положення щодо надання адміністративних послуг в електронній формі містяться також у Законі України «Про адміністративні послуги» від 06.09.2012 р., ст.17 якого передбачено надання адміністративних послуг в електронній формі засобами Єдиного державного вебпорталу електронних послуг, який виступає також офіційним джерелом інформації про надання адміністративних послуг [152].

Основним законодавчим актом, яким регламентовано відносини суб’єктів публічного адміністрування з фізичними та юридичними особами щодо розгляду і вирішення адміністративних справ, є Закон України «Про адміністративну процедуру» від 17.02.2022 р. Відповідний нормативно-правовий акт було розроблено з урахуванням впливу цифровізації, що знайшло вияв у закріпленні можливості використання інформаційно-комунікаційних технологій на будь-якій стадії адміністративного провадження [120].

Законом України «Про адміністративну процедуру» було надане визначення терміну «адміністративна процедура» як визначений законом порядок розгляду та вирішення справи; «процедурній дії» як дії адміністративного органу, що вчиняється під час розгляду справи, але якою справа не вирішується по суті; «функції публічної адміністрації» як надання адміністративних послуг, здійснення інспекційної (контрольної, наглядової) діяльності, вирішення інших справ за заявою особи або за власною ініціативою адміністративного органу [120].

Аналіз положень Закону дає змогу оцінити рівень цифровізації адміністративних процедур в Україні та їхню відповідність сучасним викликам. Закон передбачає механізми застосування інформаційно-

комунікаційних технологій у процесах подання звернень, розгляду справ, ухвалення рішень та адміністративного оскарження.

Так, О. Соловйова зазначає, що норми Закону України «Про адміністративну процедуру», що регламентують застосування цифрових технологій, можна умовно розподілити на кілька категорій відповідно до їхньої ролі та послідовності застосування в межах адміністративного провадження:

1. Подання заяви в електронній формі – через Єдиний вебпортал державних послуг, з використанням електронного підпису або автентифікації.
2. Участь в адміністративному провадженні – можливість подання клопотань і доступу до матеріалів справи онлайн.
3. Використання електронних доказів – інформація з державних реєстрів та електронні копії документів визнаються доказами.
4. Автоматизований розгляд справ – адміністративний акт може прийматися без втручання посадових осіб на основі електронних документів і даних з реєстрів.
5. Оформлення рішень – адміністративні акти можуть бути видані в електронній формі та надіслані засобами електронного зв’язку.
6. Адміністративне оскарження – подання скарг можливе в електронному форматі

Такий підхід дозволяє оцінити рівень цифровізації адміністративних процедур та ефективність їхньої адаптації до сучасних викликів [152].

Безспірним фактом є те, що запровадження цифрових адміністративних процедур сприяє підвищенню прозорості діяльності органів влади, спрощенню взаємодії громадян із державними установами та покращенню якості публічних послуг.

Водночас, справедливо буде вказати, що цифровізація публічно-правової сфери розпочалася ще до ухвалення Закону України «Про адміністративну процедуру», зокрема, можливість електронної комунікації

була передбачена в законах України: «Про звернення громадян», «Про адміністративні послуги».

Проте, на відміну від вищевказаних законодавчих актів, саме Закон України «Про адміністративну процедуру» системно закріпив загальні засади використання цифрових технологій у всіх адміністративних провадженнях, що забезпечує ефективний розгляд справ та захист прав осіб у цифровому середовищі [152].

Підсумовуючи все вищевикладене, варто зазначити, що успішний розвиток інформаційно-технологічного потенціалу держави значною мірою залежить від ефективної діяльності публічної адміністрації у цій сфері. Зокрема, адміністративні процедури мають виконувати роль дієвого інструменту для: а) належного регулювання та управління інформаційно-технологічною сферою на рівні державної політики; б) гарантування конституційних прав фізичних та юридичних осіб, включно із захистом від неправомірних дій органів публічної адміністрації та їх посадових осіб; в) забезпечення належного функціонування органів публічної адміністрації, що дозволить їм ефективно реалізовувати свої завдання та повноваження, діючи в інтересах суспільства та з дотриманням прав і свобод громадян при ухваленні суспільно значущих рішень.

Таким чином, адміністративні процедури у сфері інформаційних технологій є невід'ємним елементом забезпечення прав, свобод і законних інтересів учасників суспільних відносин та основою для ефективного регулювання, забезпечуючи баланс між інтересами держави, бізнесу та громадян України. Їх вдосконалення в умовах цифровізації сприяє підвищенню прозорості, доступності та безпеки публічного управління, створюючи сприятливі умови для розвитку інформаційного суспільства в Україні.

Висновки до розділу 2

1. Адміністративно-правове забезпечення правового режиму інформаційної безпеки є важливим елементом національної безпеки України, особливо в умовах цифрової трансформації та гібридної агресії. Інформаційна безпека охоплює захист інформаційного середовища від загроз, забезпечення прав громадян на доступ до достовірної інформації та захист персональних даних. У цьому контексті правовий режим виступає механізмом забезпечення цілісності, конфіденційності та доступності інформації.

Розглянуті положення свідчать, що правовий режим інформаційної безпеки ґрунтується на нормах Конституції України, Законах «Про національну безпеку України», «Про інформацію», «Про захист персональних даних», а також стратегічних документах, таких як Стратегії інформаційної та кібербезпеки. Це забезпечує ефективність управління інформаційними ризиками, координацію між органами державної влади та приватним сектором, а також інтеграцію України у світовий цифровий простір.

Особливу увагу слід приділяти гармонізації національного законодавства із міжнародними стандартами та розвитку правових механізмів протидії новим загрозам, включаючи кібератаки, дезінформацію та пропаганду.

Таким чином, адміністративно-правове забезпечення інформаційної безпеки є не лише основою для розвитку інформаційного суспільства та зміцнення довіри громадян до цифрових технологій, але й умовою для збереження національного суверенітету. Вдосконалення правового режиму інформаційної безпеки є важливим кроком для забезпечення сталого розвитку України у цифрову епоху.

2. Система суб’єктів адміністративно-правового регулювання у сфері інформаційних технологій є багатогранною та охоплює різноманітних

учасників, які взаємодіють задля забезпечення розвитку інформаційного суспільства, захисту прав і свобод громадян, а також гарантування національної безпеки. До цієї системи належать державні органи, органи місцевого самоврядування, приватний сектор, громадянське суспільство та окремі громадяни.

Державні органи відіграють ключову роль у формуванні, впровадженні та контролі за реалізацією державної політики у сфері інформаційних технологій. Органи місцевого самоврядування забезпечують розвиток локальної інфраструктури та сприяють цифровій трансформації на місцевому рівні. Приватний сектор виступає рушієм технологічного прогресу, забезпечуючи інноваційні рішення, необхідні для цифровізації. Громадянське суспільство та окремі громадяни забезпечують демократичний контроль, прозорість і баланс інтересів між державою, бізнесом і суспільством.

Ефективність адміністративно-правового регулювання у сфері інформаційних технологій забезпечується через чітку взаємодію між суб’єктами на основі правової, організаційної та функціональної основ. Взаємодія спрямована на досягнення прозорості, підзвітності та передбачуваності у процесах регулювання, що відповідає європейським стандартам та сприяє інтеграції України до глобального цифрового простору.

Успішна реалізація адміністративно-правового регулювання у сфері інформаційних технологій залежить від збалансованого залучення всіх суб’єктів, вдосконалення нормативно-правової бази та постійної адаптації до нових викликів цифрової епохи. Це створює передумови для сталого розвитку інформаційного суспільства, захисту прав громадян і забезпечення національної безпеки в умовах глобалізації та цифрової трансформації.

3. Адміністративні процедури відіграють ключову роль у регулюванні інформаційних технологій в Україні, забезпечуючи правову визначеність, ефективність та прозорість процесів публічного адміністрування в цифровій сфері. Вони створюють нормативні механізми, що регулюють діяльність

державних органів, приватного сектору та громадянського суспільства у сфері інформаційних технологій.

Дослідження показало, що адміністративні процедури в цій сфері мають складну структуру та охоплюють управлінські, реєстраційні, організаційно-кадрові, дозвільно-ліцензійні, контрольні та інтернаціоналізаційні аспекти. Цей комплексний підхід дозволяє ефективно впроваджувати державну політику цифрової трансформації, сприяти інноваціям та захисту інформаційного простору.

Цифровізація адміністративних процедур, яка активно розвивається в Україні, сприяє підвищенню ефективності публічного управління, мінімізації бюрократії та корупційних ризиків, покращенню якості надання адміністративних послуг. Впровадження електронного урядування та цифрових платформ демонструє прагнення держави до створення зручного та доступного правового середовища у сфері інформаційних технологій.

Таким чином, адміністративні процедури у сфері інформаційних технологоій є важливим елементом сучасного публічного управління. А їх ефективне впровадження та вдосконалення сприяє розвитку інформаційного суспільства, посиленню демократичних принципів управління та інтеграції України у глобальний цифровий простір.

РОЗДІЛ 3
ПРОБЛЕМИ ТА ШЛЯХИ ВДОСКОНАЛЕННЯ АДМІНІСТРАТИВНО-ПРАВОВОГО РЕГУЛЮВАННЯ ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В УКРАЇНІ

3.1 Проблеми правового регулювання інформаційних технологій в умовах цифрової трансформації

Світова цифрова трансформація стала одним із головних трендів сучасного суспільного розвитку, впливаючи на всі аспекти життя – від економіки до культури. Водночас вона створює безліч викликів у сфері правового регулювання, особливо в контексті використання інформаційних технологій. Стрімкий розвиток технологій часто випереджає законодавче забезпечення, що призводить до правових прогалин, конфліктів інтересів і нових викликів для державних інституцій, бізнесу та суспільства.

Не є секретом, що інформаційні технології розвиваються настільки швидко, що закони, ухвалені кілька років тому, часто втрачають актуальність ще до їх практичного впровадження.

Головною складністю правового регулювання інформаційних технологій в Україні є те, що консервативний характер правової системи часто не дозволяє їй оперативно реагувати на стрімкі технологічні зміни. Процес ухвалення законодавчих актів потребує значного часу, обговорень та узгодження між усіма зацікавленими сторонами, у той час як технології зазнають суттєвих змін ледь не щодня.

Цифрова трансформація ставить перед науковою спільнотою виклик щодо визначення правового статусу нових явищ, таких як: криптовалюти, штучний інтелект, Інтернет речей чи автономні системи. Виникає питання: чи можна розглядати ці явища як об'єкти власності, суб’єкти права, чи вони становлять абсолютно нову категорію, що потребує окремого підходу до їх правового регулювання?

Початок XXI століття відзначився прогресивним розвитком фінансових інститутів. Одним із таких інститутів став ринок криптовалют. Останніми роками використання цифрових активів стрімко зростає в усьому світі, і ця тенденція не обійшла стороною й Україну.

Попри те, що Національний банк України свого часу класифікував криптовалюту, зокрема біткойн, як «грошовий сурогат», зацікавленість у ній серед громадян лише продовжує зростати. Так, ще у середині 2016 року один із найбільших українських банків запровадив можливість купівлі та продажу біткойнів. А майже через рік в Україні відбулася перша у світі угода купівлі-продажу нерухомості за криптовалюту (Ethereum). Власник квартири в Києві, перебуваючи у США, продав її через свого представника. Цей випадок став одним із яскравих прикладів довіри й популярності до криптовалют в Україні [154, с. 174].

Водночас держава стикається з численними викликами в цій сфері, зокрема із відсутністю належного правового регулювання використання криптовалют. Ставлення до цифрових активів залишається неоднозначним: юристи й економісти дають їм часто різні оцінки. У той час як правники наголошують на ризиках й правових невизначеностях, економісти в основному підкреслюють потенційні переваги та перспективи розвитку цього ринку.

Так, науковці-економісти розглядають криптовалюту як альтернативний варіант традиційної валюти, що має низку переваг:

- транзакції з використанням криптовалюти є повністю анонімними та конфіденційними. Всі дані щодо операцій зашифровані у вигляді унікального набору символів, а персональна інформація не прив’язана до криптовалютного гаманця.
- кожна одиниця криптовалюти має унікальний код, що унеможливлює її підробку.
- децентралізований характер криптовалюти виключає наявність

центрального органу контролю, тому засновники цифрових активів чи фінансові установи не можуть впливати на її функціонування. Регулювання обміну та проведення транзакцій здійснюється безпосередньо користувачами електронних гаманців.

- відсутність прив'язки до банківських систем сприяє значному зменшенню комісійних зборів за проведення транзакцій, які зазвичай покривають лише витрати на енергоресурси, необхідні для здійснення операції.
- децентралізована система криптовалют скорочує час проведення транзакцій, оскільки підтвердження операцій відбувається за лічені секунди.
- фінансові операції здійснюються безпосередньо між власниками електронних гаманців, що прискорює обробку платежів та зменшує витрати на комісійні збори.
- випуск більшості криптовалют має встановлений обмежений ліміт, оскільки максимальна кількість одиниць визначається кінцевим числом можливих комбінацій символів, з яких формується кожна нова одиниця цифрових грошей. Це сприяє контролю за обсягом грошової маси в обігу та допомагає знижувати рівень інфляції [155, с. 40].

Очевидно, що такий підхід є логічним і безперечно заслуговує на увагу.

Проте, незважаючи на очевидні переваги, більшість правничої спільноти, а також представники банківського сектора висловлюють критичні зауваження щодо цих цифрових активів.

Зокрема, у листі НБУ № 29-208/72889 від 8 грудня 2014 року зазначено, що випуск біткойнів як «віртуальної валюти» не має внутрішньої вартості та не є зобов'язанням жодної фізичної або юридичної особи [157].

На думку Національного банку України, біткойни слід розглядати як грошовий сурогат, що позбавлений внутрішньої цінності. Крім того, регулятор підкреслює, що операції з купівлі-продажу біткойнів за долари США чи іншу іноземну валюту можуть мати ознаки діяльності фінансових пірамід та потенційно бути пов'язаними з сумнівними операціями, що

підпадають під законодавство про запобігання легалізації доходів, отриманих незаконним шляхом, та фінансування тероризму.

У зазначеному листі також міститься попередження для громадян і підприємств про ризики, пов'язані з обміном віртуальних валют на товари чи готівкові кошти. Такі операції можуть призвести до повної втрати фінансів, а також спричинити залучення учасників до незаконної діяльності, зокрема до відмивання грошей і фінансування тероризму.

З метою захисту прав споживачів і гарантування безпеки фінансових операцій Національний банк України рекомендує використовувати лише ті платіжні та транзакційні системи, які офіційно внесені до Реєстру платіжних систем, їхніх учасників і постачальників фінансових послуг.

Станом на сьогодні в Україні досі тривають дискусії щодо правового статусу криптовалют. Так, прийнятий у 2022 році Закон України «Про віртуальні активи» [158] визначив основні поняття в цій галузі, але його ключові аспекти: оподаткування, захист прав інвесторів і протидія відмиванню коштів, досі залишаються нерозкритими

Верховна Рада України, слідуючи світовим тенденціям, врахувала позицію Міжнародної групи з протидії відмиванню коштів (FATF) [159], яка використовує термін «віртуальні активи», ухвалюючи Закон України «Про віртуальні активи» № 3153-IX від 10.06.2023. Однак закон так і не набув чинності через відсутність затверджених змін у податковому законодавстві та у зв'язку з невпровадженням Державного реєстру постачальників послуг, пов'язаних із віртуальними активами.

Документ містить низку невизначеностей і суперечностей, зокрема щодо поняття «віртуальний актив».

Вперше цей термін було введено у Законі України «Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення» [160], де він визначається як «цифрове вираження вартості, яким

можна торгувати у цифровому форматі або переказувати і яке може використовуватися для платіжних або інвестиційних цілей».

Водночас, відповідно до норм Закону України «Про віртуальні активи», вони розглядаються як нематеріальне благо, що є об’єктом цивільних прав, має вартість і виражене у вигляді сукупності електронних даних. На підставі системного аналізу випливає, що такі активи в Україні не визнаються засобом платежу й не можуть бути об'єктом обміну на товари, роботи або послуги.

Історія ухвалення Закону України «Про віртуальні активи» стала своєрідним символом боротьби за правове визнання криптовалют та інших цифрових активів у правовому полі України. Попри серйозні наміри законодавців упорядкувати цю сферу, закон так і не набув чинності. Цей випадок наочно продемонстрував складність поєднання впровадження інноваційних технологій, забезпечення економічної стабільності та дотримання міжнародних зобов’язань.

Одним із можливих варіантів розв’язання проблем, пов’язаних із цим законом, є адаптація досвіду міжнародного регулювання, зокрема імплементація Регламента (ЄС) 2023/1114, відомого як Markets in Crypto-Assets Regulation (MiCA) [161].

Ця регуляція вводить визначення «криптоактив» і розподіляє криптоактиви на три категорії: токени електронних грошей, токени з прив’язкою до активу та інші криптоактиви, що не підпадають під визначення EMTs і ARTs. Вона також запроваджує правила розкриття інформації, обмеження щодо використання інсайдерської інформації, заборону її неправомірного розголошення та маніпулятивних дій на ринку криптоактивів. Крім того, MiCA встановлює вимоги до провайдерів послуг у цій сфері.

Цей документ є важливим етапом у формуванні єдиної правової бази для регулювання віртуальних активів у Європейському Союзі, що дозволяє

посилити захист користувачів і інвесторів та може стати основою для внесення змін до Закону України «Про віртуальні активи».

Основні положення регламенту MiCA спрямовані на гармонізацію підходів до регулювання криптоактивів у всіх країнах-членах ЄС, а також на встановлення чітких вимог до функціонування цього ринку. Зокрема, документ передбачає: уніфіковану класифікацію криптоактивів (токени електронних грошей, токени з прив'язкою до активу, utility-токени), визначення восьми основних типів послуг, пов'язаних із криптоактивами, встановлення вимог до постачальників послуг із криптоактивами, що включають необхідність отримання ліцензій [162].

Однією з ключових цілей MiCA є створення рівноваги між правами провайдерів криптопослуг та інтересами інвесторів. У зв'язку з цим документ встановлює вимоги до мінімального статутного капіталу, корпоративного управління, страхування та обов'язкового розкриття інформації. Також він вводить заборони та обмеження щодо маніпулювання ринком криптоактивів.

Попри наявність базового законодавства, в Україні залишаються нерозв'язаними питання щодо правового регулювання криптоактивів, зокрема їх ідентифікації, класифікації та механізмів контролю за різними видами віртуальних активів.

Приклад визначення поняття «віртуальний актив» в Законі України «Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом» підтверджує, що у чинному законодавстві існують суперечності, які потребують доопрацювання, зокрема щодо оподаткування операцій із віртуальними активами.

Закон України «Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом» фактично підміняє поняття криптовалюти терміном «віртуальні активи», що створює додаткові труднощі у визначенні їхнього правового статусу.

Підсумовуючи вищевикладене, можна дійти наступних висновків:

– криптовалюта є унікальним феноменом, який має ряд переваг у порівнянні з традиційними валютами. Зокрема, вона не піддається впливу інфляції, а також відкриває можливості для отримання прибутку, хоча це пов’язано з певними ризиками;

– використання криптовалюти тягне за собою значні ризики для її власників. Одним із ключових є майже повна відсутність правового захисту у разі порушення їхніх прав або вчинення шахрайських дій у цій сфері.

З іншої сторони, застосування криптовалют може мати й негативні наслідки для держави, зокрема:

- через анонімність та особливості криптовалютних транзакцій зростає ризик використання цифрових активів для легалізації доходів, отриманих злочинним шляхом;

- існує можливість виведення коштів за кордон без належного контролю з боку державних органів, що сприяє ухиленню від сплати податків та інших обов’язкових платежів;

- система оподаткування доходів, отриманих від операцій з криптовалютами, залишається нерозвиненою, що створює труднощі у контролі та регулюванні цього сектору.

Враховуючи динамічний розвиток віртуальних активів, Україна повинна не лише спиратися на міжнародний досвід, а й створювати власні механізми регулювання, що відповідатимуть реаліям внутрішнього ринку. Постійне оновлення та вдосконалення регулятивних рамок є необхідним для забезпечення економічної стабільності та захисту прав громадян та інвесторів у цій високотехнологічній сфері.

Іншим актуальним питанням в межах теми огляду проблеми адміністративно-правового регулювання інформаційних технологій в умовах цифрової трансформації України є правове регулювання використання Інтернету речей (далі – IoT).

О. Костенко справедливо зазначає, що сьогодні людство живе в епоху Інтернету речей (IoT), який забезпечує інтеграцію будь-яких фізичних

об’єктів, матеріальних та нематеріальних суб’єктів у глобальну цифрову екосистему завдяки використанню електронних пристроїв. Все це зумовлює необхідність проведення наукових досліджень, ідентифікації ключових проблем і викликів у сфері IoT, а також аналізу їхнього впливу на соціальні та технологічні відносини [165, с. 130].

Особливості й проблеми правового регулювання використання Інтернету речей (IoT) в Україні досліджувались такими вітчизняними правниками, як О. Баранов, О. Костенко, Є. Харитонов та О. Харитонова [163, с. 8; 164, с. 172; 165, с. 130; 166, с. 68].

Окрім того, фундаментальні дослідження у питаннях впровадження, використання та правового регулювання Інтернету речей (IoT) здійснювались американськими й китайськими науковцями та правниками: N. Kong, Park Jungsoo, N. Crespi, G. Lee, Ilyoung Chong, Lu Yan, Yan Zhang, Laurence T. Yang, Huansheng Ning [167; 168; 169; 170].

Перспективні напрями правового регулювання Інтернету речей (IoT) та штучного інтелекту охоплюють визначення правового статусу взаємодії «людина – робот», удосконалення механізмів прийняття рішень штучним інтелектом, а також адаптацію правових норм до розвитку IoT у різних сферах (цивільне, адміністративне, інформаційне право тощо). Дослідження також спрямовані на забезпечення конкуренції, захист прав споживачів, кібербезпеки та інтелектуальної власності.

У контексті правового регулювання IoT українські науковці пропонують застосовувати концепцію «ІТ-право», що інтегрує традиційні цивільні правовідносини з цифровими процесами. Однак питання систематизації правових норм залишається досі відкритим, оскільки поняття IoT постійно змінюється. В більшості випадків його визначають як: 1) систему підключених пристроїв, які обмінюються даними; 2) комплекс технічних систем і штучного інтелекту для суспільних відносин; 3) глобальну мережу взаємопов’язаних фізичних і віртуальних об’єктів [171, с. 112].

Науковці підкреслюють необхідність розробки комплексного законодавства, яке охоплюватиме всі аспекти управління ідентифікаційними даними, включаючи їх застосування в технологіях Інтернету речей (IoT). Такий підхід сприятиме ефективному регулюванню суспільних відносин у сфері управління ідентифікаційною інформацією, що використовується для розпізнавання суб'єктів та об'єктів у державних реєстрах, базах даних та інформаційно-комунікаційних системах [165, с. 133].

Іншим не менш важливим питанням у розрізі проблематики адміністративно-правового регулювання інформаційних технологій в умовах цифрової трансформації України є правове регулювання використання штучного інтелекту (далі – ШІ).

Штучний інтелект дедалі більше набуває значення невід'ємного елементу цифрової трансформації в Україні. Його використання охоплює різні галузі — медицину, транспорт, фінанси, публічне управління, водночас створюючи правові, етичні та соціальні дилеми. Одним із найбільш складних викликів залишається визначення відповідальності за рішення, ухвалені алгоритмом, або дії автономних пристроїв, створених на основі штучного інтелекту [172, с. 153].

Правове регулювання штучного інтелекту ускладнюється його здатністю до самонавчання, адаптації до змін та ухвалення рішень без безпосереднього втручання людини. Вирізняють кілька ключових аспектів цієї проблеми: 1) розподіл відповідальності (у разі, якщо рішення, прийняте штучним інтелектом, спричиняє негативні наслідки, виникає питання щодо визначення суб'єкта відповідальності. Чи повинен відповідати власник пристрою, який його експлуатує? Або ж має відповідати розробник чи виробник, що створили алгоритм та саму технологію? Чи відповідальність має нести користувач, який безпосередньо взаємодіє з ШІ?); 2) складність встановлення причинно-наслідкового зв'язку (традиційна юридична практика ґрунтується на необхідності доведення зв'язку між діями суб'єкта та їх наслідками. Проте у випадку з ШІ такий зв'язок часто є нечітким, що

ускладнює правове регулювання); 3) непередбачуваність поведінки ШІ (алгоритми можуть функціонувати у спосіб, який не передбачили їхні розробники, що створює додаткові труднощі у встановленні відповідальної особи).

Ці фактори вимагають від держави розробки нових підходів до правового регулювання штучного інтелекту, які б враховували специфіку його функціонування та можливі ризики.

У прийнятій 2 грудня 2020 року Кабінетом Міністрів України «Концепції розвитку штучного інтелекту в Україні» термін «штучний інтелект» визначено як «організовану сукупність інформаційних технологій, що дозволяють вирішувати складні комплексні завдання, використовуючи систему наукових методів дослідження та алгоритмів обробки інформації, отриманої або самостійно створеної під час функціонування. Крім того, штучний інтелект здатен формувати та використовувати власні бази знань, моделі прийняття рішень, алгоритми роботи з інформацією та обирати способи досягнення поставлених цілей». У документі також наголошується на «відсутності або недосконалості правового регулювання штучного інтелекту, зокрема в таких сферах, як освіта, економіка, публічне управління, кібербезпека, оборона, а також на проблемах у законодавстві щодо захисту персональних даних» [173].

У квітні 2021 року Європейський Союз оприлюднив законопроєкт про штучний інтелект (Artificial Intelligence Act; AI Act) [174], спрямований на створення загальної нормативно-правової бази для регулювання всіх аспектів застосування штучного інтелекту (за винятком військової сфери), який 01 серпня 2024 року набув чинності [175].

Відповідний нормативно-правовий акт покликаний регулювати правила у сфері штучного інтелекту, він став першим у світі комплексним нормативним актом щодо штучного інтелекту. Закон гарантує, що штучний інтелект, який було розроблено для використовування в ЄС, заслуговує довіри, має гарантії захисту основних прав людей. Закон спрямований на

створення гармонізованого внутрішнього ринку штучного інтелекту в ЄС, заохочення впровадження цієї технології та створення сприятливого середовища для інновацій та інвестицій [176].

Європейський закон про штучний інтелект спрямований на впорядкування та регулювання програм штучного інтелекту залежно від рівня ризику, який вони можуть становити. Передбачена класифікація поділяє ШІ-системи на чотири основні рівні ризику: «неприйнятний», «високий», «обмежений» і «мінімальний», а також включає окрему категорію для ШІ загального призначення.

Відповідний закон запровадив:

– єдині правила щодо введення в обіг, експлуатації та використання ШІ-систем на території Європейського Союзу;

– заборону певних практик, пов’язаних зі штучним інтелектом;

– спеціальні вимоги до ШІ-систем із високим рівнем ризику та встановлення відповідальності для операторів таких систем;

– єдині стандарти прозорості для ШІ, що взаємодіє з людьми, зокрема для систем розпізнавання емоцій та біометричної категоризації;

– регулювання ринкового нагляду та контролю за штучним інтелектом [176].

У статті 3 Закону міститься визначення терміну «система штучного інтелекту», під яким розуміється програмне забезпечення, створене з використанням одного або кількох методів і підходів, зазначених у Додатку I до Закону. Таке програмне забезпечення здатне виконувати певні завдання, визначені людиною, і формувати результати у вигляді контенту, прогнозів, рекомендацій або рішень, що впливають на середовище, з яким вони взаємодіють [176].

Не має жодних сумнівів, що прийнятий AI Act матиме безпосередній вплив на правове регулювання штучного інтелекту й в Україні, що лише підкреслює необхідність оперативного розроблення механізмів імплементації

та дотримання міжнародних стандартів у вітчизняних технологічних проєктах.

Необхідно ще додати, що у Європейському Союзі ШІ не визнається суб'єктом права, але розглядаються механізми відповідальності розробників і користувачів. Тому Україні корисно було б адаптувати ці підходи до своїх національних умов.

Крім того, європейські стандарти вимагають й врахування етичних принципів при розробці ШІ. Для України важливо імплементувати ці принципи, зокрема прозорість, об'єктивність та неприпустимість дискримінації, враховуючи при цьому специфіку українського суспільства.

Отже, для ефективного використання ШІ в умовах євроінтеграції та цифрової трансформації України необхідно створити нормативно-правову базу, яка чітко визначатиме сфери застосування ШІ, відповідальність за наслідки його використання, механізми захисту прав осіб, постраждалих від дій ШІ.

З огляду на це, штучний інтелект вбачається потужним інструментом цифрової трансформації, але водночас він створює нові виклики для правової системи України. Вирішення проблеми відповідальності за рішення алгоритмів та дії автономних пристроїв вимагає системного підходу, гармонізації з міжнародними стандартами, врахування етичних аспектів та забезпечення прозорості. Україна має всі можливості стати одним з лідерів у цій сфері, якщо своєчасно забезпечить адаптацію національного законодавства та ефективну імплементацію міжнародного досвіду.

Серед основних проблем правового регулювання інформаційних технологій в умовах цифрової трансформації та повномасштабної війни особливе місце займає проблема належного забезпечення Україною кібербезпеки.

Варто вказати, що з початком повномасштабного вторгнення росії Україна зіткнулася не лише з масованими ракетними обстрілами, а й із широкомасштабними кібератаками в цифровому просторі. Ці атаки різняться

за своїми формами та цілями: від спроб дестабілізувати суспільно-політичну ситуацію до атак на критичну інфраструктуру та несанкціонованого доступу до конфіденційної інформації громадян.

Агресія в кіберпросторі створила серйозні виклики для української кібербезпеки, з огляду на що, її посилення стає одним із ключових завдань для уряду та правоохоронних органів України.

Дослідження проблеми сучасного стану кіберзагроз та заходів захисту в Україні є вкрай важливим для розробки ефективних стратегій протидії. Вивчення цих аспектів дозволяє не лише визначити потенційні ризики та вразливості, а й сформувати практичні рекомендації та інноваційні підходи до зміцнення кібербезпеки держави.

Вважаємо, що станом на сьогодні на законодавчому рівні відсутня чітко визначена система заходів державного регулювання у сфері кіберзахисту, що потребує подальшої роботи над удосконаленням адміністративно-правових механізмів у цій галузі.

Так, Стратегія кібербезпеки України, ухвалена рішенням Ради національної безпеки і оборони України від 14 травня 2021 року та затверджена Указом Президента № 447/2021 [83], хоча й мала на меті адаптацію державної політики у сфері кіберзахисту до сучасних викликів, однак має низку недоліків, що обмежують її ефективність.

Зокрема, Стратегія кібербезпеки України не містить детального алгоритму дій та чітко структурованих механізмів їх реалізації, що ускладнює її практичне застосування. В документі визначені лише загальні принципи, проте відсутня деталізація конкретних інструментів та механізмів, які мають використовуватися для забезпечення ефективного державного регулювання у сфері кіберзахисту. Стратегією не встановлено й чіткого розподілу повноважень між органами державної влади, що може призводити до дублювання функцій або, навпаки, відсутності належного реагування на кіберзагрози. Окрім того, вона потребує більш глибокої гармонізації з

провідними міжнародними стандартами з кібербезпеки, що дозволило б підвищити ефективність захисту кіберпростору України.

В умовах воєнного стану надзвичайно важливим є забезпечення кібербезпеки об'єктів критичної інфраструктури, а також розробка та впровадження стандартів і заходів для ефективного захисту від кіберзагроз, таких як кібератаки чи кібершпигунство. Ці аспекти регулюються Загальними вимогами до кіберзахисту об’єктів критичної інфраструктури, затвердженими постановою Кабінету Міністрів України від 19 червня 2019 року № 518 [177].

Вищезгадані загальні вимоги визначають технічні, організаційно-методологічні, а також технологічні умови кіберзахисту об’єктів критичної інфраструктури, що є обов’язковими до виконання підприємствами, установами та організаціями, які згідно законодавства відносяться до об’єктів критичної інфраструктури, зокрема даними вимогами визначено наступне: порядок формування на об’єктах критичної інфраструктури загальної політики інформаційної безпеки; управління доступом користувачів та адміністраторів до об’єктів захисту об’єктів критичної інформаційної інфраструктури; ідентифікацію та автентифікацію користувачів та адміністраторів об’єктів критичної інформаційної інфраструктури; умови забезпечення мережевого захисту компонентів та інформаційних ресурсів на об’єктах критичної інформаційної інфраструктури, а також умови, необхідні для забезпечення доступності та стабільності компонентів та інформаційних ресурсів об’єктів критичної інфраструктури; визначення умов та правил використання змінних пристроїв і носіїв інформації на об’єктах критичної інформаційної інфраструктури [177].

Крім того, в умовах воєнного стану набуває особливого значення питання цифрової грамотності, й не лише для ІТ-фахівців, а й для всіх громадян України. Важливо забезпечити поширення знань про цифровий етикет, правила кібергігієни та ефективні методи захисту персональних даних у мережі.

Для забезпечення інформаційної безпеки в Україні критично важливо дотримуватися основ кібергігієни, зокрема у протидії фейковим новинам, діпфейкам, підробленим сайтам, фішинговим атакам і несанкціонованому доступу до особистих акаунтів. Слід орієнтуватися виключно на офіційні та перевірені джерела інформації, уникаючи непідтверджених даних у соціальних мережах. Водночас необхідно пам'ятати, що навіть авторитетні медіа та офіційні особи можуть припускатися помилок, особливо в умовах воєнного стану [178, с. 45].

Україна повинна бути готовою забезпечувати власний соціально-економічний розвиток у цифровому середовищі, що потребує здатності ефективно протидіяти деструктивним кіберзагрозам, зміцнювати кіберстійкість на всіх рівнях та налагоджувати співпрацю між усіма суб'єктами кібербезпеки на основі довіри.

Таким чином, сучасний етап розвитку кіберпростору вимагає принципово нових підходів до управління інформаційними ресурсами. Ефективність цих змін значною мірою залежить від того, наскільки гнучко організовані процеси на державному рівні та як швидко впроваджуються нові стратегії й методи боротьби з потенційними загрозами.

Як ми з'ясували, правове регулювання інформаційних технологій в умовах цифрової трансформації є складним, динамічним і багатовимірним процесом. Основними проблемами залишаються розрив між швидкістю розвитку технологій і законодавства, колізії між правом на приватність і технологічними можливостями, недостатня регуляція кібербезпеки, етичні виклики та розбіжності між національними й міжнародними підходами.

Для вирішення цих проблем необхідно адаптувати правову систему до нових реалій, активно впроваджувати цифрові інструменти в публічне управління, забезпечувати гармонізацію законодавства з міжнародними стандартами та посилювати співпрацю між державами-партнерами України. Лише за таких умов інформаційні технології зможуть стати інструментом прогресу, а не джерелом загроз.

3.2 Роль зарубіжного досвіду у вдосконаленні адміністративно-правового регулювання інформаційних технологій

Дослідження перспективних напрямів вдосконалення адміністративно-правового регулювання інформаційних технологій в Україні буде неповним без системного аналізу та узагальнення відповідного досвіду зарубіжних країн.

У сучасному глобалізованому світі інформаційні технології є ключовим фактором розвитку економіки, публічного управління та суспільства в цілому. Ефективне регулювання цієї сфери є надзвичайно складним завданням, оскільки технології змінюються швидше, ніж законодавство встигає адаптуватися. Саме тому вивчення і використання зарубіжного досвіду у цій сфері є важливим елементом формування національної правової системи, особливо в умовах цифрової трансформації України.

Зарубіжний досвід адміністративно-правового регулювання інформаційних технологій досліджувався багатьма науковцями-правниками, проте в основному фрагментарно, в контексті іншої тематики, що актуалізує необхідність проведення окремого дослідження даної тематики.

Розвиток інформаційних технологій у різних країнах відбувається нерівномірно, а підходи до їх регулювання залежать від політичного устрою, економічної ситуації та культурних особливостей. Однак чимало держав вже створили ефективні механізми регулювання сфери інформаційних технологій, які можуть бути корисними для України.

Варто наголосити, що використання зарубіжного досвіду дозволяє Україні уникати типових помилок у регулюванні цієї сфери, переймати найкращі практики організації публічного управління у сфері інформаційних технологій, інтегруватися у міжнародний цифровий простір та забезпечувати відповідність українського законодавства європейським і міжнародним стандартам.

Україна, як держава, що прагне до інтеграції з Європейським Союзом, повинна враховувати перш за все особливості європейських правових підходів до регулювання інформаційних технологій.

Європейський Союз активно формує правове поле для регулювання інформаційних технологій, приділяючи особливу увагу захисту персональних даних, кібербезпеці, розвитку цифрової економіки та електронному врядуванню.

Так, одним із найважливіших досягнень Європейського Союзу (далі – ЄС) у цій сфері є впровадження Загального регламенту про захист даних (далі - GDPR), який набув чинності 25 травня 2018 року [74].

GDPR встановив суворі правила щодо обробки, зберігання та передачі персональних даних, надаючи громадянам контроль над їхньою особистою інформацією. Цей регламент став еталоном для багатьох країн, які адаптували своє законодавство відповідно до його вимог.

Формування цього важливого нормативно-правового акту стало результатом тривалого процесу розвитку правового регулювання захисту персональних даних. У ньому простежуються історичні досягнення та еволюція глобальної правової доктрини.

Важливо зазначити, що Україна не стоїть осторонь цих процесів, а навпаки, активно долучається до них.

Після набуття чинності 25 травня 2018 року Європейського регламенту про захист персональних даних минуло понад шість років, що дозволяє оцінити його ефективність та вплив на правові та суспільні відносини. Варто підкреслити, що дія цього нормативного акту розповсюджується на територію України, хоча й не в повному обсязі.

З огляду на це, питання захисту персональних даних набуло значної уваги серед науковців, правників та громадськості. У сучасних наукових та публіцистичних працях нерідко висловлюється думка, що GDPR є переважно приватно-правовим явищем, нововведенням європейського законодавства у сфері цивільного права. Проте цей регламент є наслідком тривалого розвитку

концепції основоположних прав і свобод людини, витоки якої сягають набагато раніше за 25 травня 2018 року.

Сфера захисту персональних даних охоплює комплекс правових відносин, які включають як публічно-правові, так і приватно-правові аспекти. Водночас, приватно-правові механізми регулювання та захисту персональних даних виконують додаткову (субсидіарну) роль у порівнянні з публічно-правовими нормами. Це пояснюється тим, що історично захист персональних даних розвивався як складова конституційно-правового та адміністративно-правового механізму охорони права на недоторканність приватного життя, що відображено в концепції «прайвесі». Найчіткіше ця ідея реалізована в правових традиціях загального права. В американській правовій системі було сформовано концепцію «прайвесі», яка об'єднала захист приватного життя громадян і свободи особи від неправомірного або надмірного втручання держави, що ґрунтується на принципах індивідуалізму та загальнодемократичних цінностях.

Нормативно-правова база публічного управління у сфері захисту персональних даних в Україні включає спеціальний законодавчий акт, а також окремі норми, які закріплені в інших законах. Основним документом у цій сфері є Закон України «Про захист персональних даних» [70], який фактично імплементує положення Директиви 95/46/ЄС, що вже втратила чинність [179].

З огляду на це, необхідним кроком є приведення положень Закону України «Про захист персональних даних» у відповідність до Загального регламенту про захист даних (GDPR), ухваленого Європейським Парламентом та Радою ЄС і чинного з 25 травня 2018 року. Це є важливим напрямом державної політики у сфері захисту персональних даних, особливо в умовах воєнного стану, оскільки формування національної системи захисту даних потребує врахування актуальних європейських правових стандартів.

Сучасний розвиток суспільства супроводжується зростаючим значенням інформаційної сфери та широким використанням автоматизованих

технологій для обробки та передачі даних. Їх застосування у всіх сферах життя підвищує ризики порушення приватного життя, а також створює загрозу незаконного використання персональних даних.

У сучасному цифровому середовищі уникнути процесу ідентифікації стає все складніше, проте необхідно забезпечити належний контроль за збереженням, обробкою та використанням персональної інформації без згоди її власника. Це підкреслює важливість правового регулювання цього питання та підвищення рівня обізнаності громадян щодо захисту їхніх персональних даних.

Таким чином, Загальний регламент про захист даних (GDPR) є одним із найбільш значущих нормативно-правових актів у сфері захисту персональних даних за останні десятиліття. Він поширюється на всі організації, що здійснюють обробку персональної інформації осіб, які проживають у країнах Європейського Союзу або Європейської економічної зони, незалежно від місця реєстрації такої організації. Це робить регламент одним із наймасштабніших законодавчих документів у сфері захисту даних у світі.

З огляду на зобов'язання України поступово адаптувати свою правову систему до норм та регуляторної бази ЄС у сфері інформаційного суспільства та електронних комунікацій (стаття 394 Глави 14 «Інформаційне суспільство» Угоди про асоціацію між Україною та ЄС), держава має забезпечити відповідність національного законодавства та практик у сфері захисту персональних даних та приватного життя вимогам європейських стандартів, включаючи положення GDPR [180].

З урахуванням зазначеного, гармонізація законодавства України з європейськими стандартами у сфері захисту персональних даних та впровадження положень GDPR є, по-перше, необхідним кроком у процесі євроінтеграції, а по-друге – сприятиме створенню сучасного та ефективного інформаційного середовища, що відповідатиме потребам громадян та

бізнесу, що, у свою чергу, позитивно вплине на економічний розвиток країни та забезпечить високий рівень безпеки персональних даних.

У 2016 році ЄС прийняв Директиву про безпеку мереж та інформаційних систем (NIS Directive) [181], яка встановлює мінімальні вимоги до кібербезпеки для державних і приватних організацій. Директива зобов'язує держави-члени створювати національні стратегії кібербезпеки та спеціальні органи, відповідальні за кіберзахист, забезпечуючи оперативну взаємодію між ними. У 2022 році була прийнята оновлена версія — NIS2, яка розширила сферу дії Директиви та запровадила більш суворі вимоги, зокрема щодо звітності та відповідальності за порушення [182].

Відповідна Директива визначила основні вимоги до національних стандартів з кібербезпеки, встановив механізми зміцнення стратегічної та оперативної співпраці між державами-членами та запровадила низку зобов’язань для організацій, які працюють у секторах, критично важливих для економіки та суспільства. Відповідно до цієї директиви, компанії повинні впроваджувати заходи з кібербезпеки та повідомляти про кіберінциденти компетентним органам [182].

Одним із ключових напрямів політики ЄС у сфері кібербезпеки є сертифікація інформаційно-комунікаційних технологій, яка сприяє підвищенню рівня довіри до цифрових продуктів, послуг та процесів. У законодавстві Європейського Союзу про кібербезпеку наголошується, що для розвитку цифрового ринку, включаючи сферу обробки даних та Інтернету речей, важливо забезпечити належний рівень кіберзахисту. Відповідно до цього нормативного акту, функції з розробки та впровадження системи сертифікації покладено на Агентство Європейського Союзу з кібербезпеки (ENISA), яке взаємодіє з державними органами, представниками бізнесу та організаціями, що займаються стандартизацією. Закон ЄС про кібербезпеку також розширив мандат ENISA, надавши їй більше повноважень та ресурсів для виконання нових завдань [183].

Значний внесок у розробку стандартів кібербезпеки на міжнародному рівні здійснюють Міжнародна організація зі стандартизації (ISO) та Міжнародна електротехнічна комісія (IEC). Вони створили спеціалізовану систему регулювання у сфері кібербезпеки, зокрема розробили стандарт ISO/IEC 27002, який містить рекомендації для організацій щодо розробки, впровадження та вдосконалення системи управління інформаційною безпекою (ISMS). Цей стандарт надає найкращі практики та контрольні заходи для кіберзахисту, охоплюючи такі аспекти, як управління доступом, криптографія, безпека персоналу та реагування на кіберінциденти. Він слугує основою для організацій, які прагнуть забезпечити надійний захист своїх інформаційних активів [184].

Таким чином, Європейський Союз здійснює комплексні правові, організаційні та технічні заходи для забезпечення кібербезпеки організацій. Україні варто переймати цей досвід, зокрема у сфері сертифікації цифрових продуктів, послуг та процесів.

Європейська стратегія «Єдиний цифровий ринок» (Digital Single Market Strategy) є ще одним яскравим прикладом європейських ініціатив покликаних стимулювати розвиток цифрових послуг, електронної комерції та впроваджувати новітні інформаційні технології [185].

Стратегія є однією з найбільш амбітних ініціатив Європейського Союзу у сфері цифровізації. Вона була представлена у травні 2015 року Європейською Комісією і має на меті усунення бар'єрів для цифрових послуг, створення сприятливого середовища для інновацій та забезпечення доступу до цифрових продуктів і послуг для громадян усіх країн-членів ЄС.

Простими словами «Єдиний цифровий ринок» є інтегрованим простором, у якому люди, бізнес і державні органи можуть вільно взаємодіяти в цифровому середовищі. Мета стратегії полягає у тому, щоб зробити ЄС більш конкурентоспроможним на глобальному рівні, стимулюючи розвиток цифрової економіки, впровадження інноваційних технологій та підвищення довіри до цифрових сервісів.

Для України відповідна стратегія ЄС є зразковою, адже використання досвіду «Єдиного цифрового ринку» допоможе не лише розвивати цифрову економіку, але й сприятиме інтеграції у глобальну цифрову екосистему.

Ще одним із пріоритетних напрямків модернізації публічного управління в країнах ЄС є електронне урядування.

Електронне урядування – це сучасний підхід до організації державного (публічного) управління, спрямований на підвищення ефективності, відкритості та прозорості діяльності державних органів та місцевого самоврядування. Використання інформаційних та телекомунікаційних технологій сприяє формуванню нового типу публічного управління, орієнтованого передусім на задоволення потреб громадян.

Європейські країни вже тривалий час активно впроваджують цифрові технології у сфері надання державних послуг через Інтернет. Вони успішно співпрацюють у цьому напрямку, заохочуючи громадян до участі в процесі ухвалення та реалізації політичних рішень. Протягом останнього десятиліття цифровізація публічного управління стала одним із ключових пріоритетів для ЄС, що пов’язано, зокрема, зі зростаючим значенням цифрових державних послуг для розвитку єдиного цифрового ринку. Це відбувається на фоні занепокоєння щодо цифрового суверенітету Європи, оскільки новітні технології, розроблені поза межами ЄС, можуть становити ризики для контролю громадян над їхніми персональними даними.

Окрім цього, компанії, що працюють за межами ЄС, розглядаються як потенційні перешкоди для розвитку європейських технологічних підприємств, оскільки агресивні процеси поглинань можуть обмежувати конкуренцію. У відповідь на це Європейський парламент та інші регуляторні органи ЄС запроваджують нові механізми оцінки таких процесів. Наприклад, у 2023 році був запущений принцип «Єдиного подання» (Once-Only Principle, OOP), який передбачає взаємозв’язок базових державних реєстрів між країнами-членами ЄС. Проте низка держав ще не встигли виконати вимоги щодо впровадження цього принципу [186].

Хоча деякі країни ЄС та Європейської асоціації вільної торгівлі (ЄАВТ), такі як Австрія, Естонія, Ісландія, Чорногорія, Нідерланди та Норвегія, досягли значного прогресу у впровадженні цифрових стратегій та стандартів ЄС, національний і місцевий рівні розвитку все ще залишаються нерівномірними. Впровадження цифрових посвідчень у Європі відбулося майже повсюдно, однак можливість транскордонного доступу до державних послуг за їх допомогою досі є обмеженою.

Таким чином, для повноцінного впровадження цифрового уряду країни ЄС продовжують розвивати свої системи, адаптуючи державні служби до сучасних цифрових реалій. Це, зокрема, стосується підвищення рівня цифрової компетентності серед державних службовців, що є важливим чинником успішної інтеграції цифрових технологій у державне (публічне) управління.

На рівні Європейського Союзу виокремлюються два ключові чинники розвитку цифрового уряду. Перший полягає в тому, що цифрові державні послуги є важливими для формування єдиного цифрового ринку, оскільки вони сприяють зручному та безпечному доступу громадян до послуг, товарів і даних незалежно від кордонів.

Другий фактор стосується посиленої уваги до питань цифрового суверенітету Європи, особливо у сфері новітніх технологій. У межах стратегії «Формування цифрового майбутнього Європи» та ініціативи «Цифровий компас 2030» Європейська комісія визначила цифровізацію державних послуг однією з основних цілей цифрового десятиліття ЄС. Програма політики до 2030 року, ухвалена у вересні 2021 року, вперше визначила цифрові орієнтири для країн-членів ЄС та запровадила механізми управління для їх реалізації [187].

На сьогодні понад 90% державних послуг у 36 європейських країнах вимагають певної форми ідентифікації та автентифікації – онлайн чи офлайн. Хоча національні цифрові посвідчення широко використовуються в ЄС, їх впровадження залишається нерівномірним [188, с. 69-70].

Незважаючи на широке поширення таких посвідчень, лише 64% онлайн-послуг приймають офіційні національні цифрові ідентифікатори. Ще 9% державних сервісів вимагають використання інших форм державної ідентифікації (наприклад, податкового номера), а 1% дозволяє застосовувати цифрові ідентифікатори приватного сектора, зокрема токени електронного банкінгу. При цьому менше ніж 44% цифрових послуг підтримують єдиний вхід, що змушує користувачів повторно проходити автентифікацію у різних державних системах [188, с.71].

Європейська комісія також ініціювала структуру цифрової ідентифікації, яка має законодавчу основу. Вона передбачає, що цифрові гаманці будуть пов'язані з національними цифровими посвідченнями та міститимуть додаткові атрибути особи, наприклад водійські права. Це дозволить громадянам отримувати онлайн-послуги без ризику розголошення зайвих персональних даних.

Ключову роль у цьому процесі відіграє Регламент ЄС про електронну ідентифікацію та довірчі послуги (eIDAS), який визначає механізми забезпечення транскордонного використання цифрових ідентифікаторів та доступу до державних послуг в інших країнах ЄС [189].

Для створення сучасної та ефективної системи електронного врядування необхідно враховувати світовий досвід та адаптувати найкращі міжнародні практики. Як свідчить аналіз розвитку електронного врядування в країнах ЄС, Україні варто орієнтуватися на їхні досягнення та впроваджувати найбільш успішні рішення.

Європейський Союз у листопаді 2022 року запустив проєкт «Цифрова трансформація для України» (DT4UA), який спрямований на підтримку України у впровадженні ефективних, доступних і безпечних державних послуг, а також на швидке реагування на виклики, пов'язані з війною [190]

Фінансова допомога ЄС охоплює чотири основні напрями: 1) розвиток цифрових послуг і вдосконалення застосунку «Дія»; 2) покращення механізмів обміну даними між державними реєстрами та органами влади; 3)

розбудова інфраструктури електронної ідентифікації відповідно до вимог регламенту eIDAS; 4) модернізація системи електронного управління, що сприятиме прозорості процесів розгляду кримінальних справ.

Ініціативи Європейського Союзу є важливим кроком на шляху до цифрового урядування України, яке відповідає європейським стандартам і сприяє ефективному функціонуванню державних сервісів в умовах сучасних викликів.

Однак серед усіх країн Європейського Союзу, у питанні вдосконалення адміністративно-правового регулювання інформаційних технологій, особливої уваги заслуговує безцінний досвід Естонії.

Естонія є світовим лідером у сфері електронного урядування, демонструючи, як цифровізація може змінити публічне управління, зробивши його прозорим, ефективним та зручним для громадян. Її досягнення у цьому напрямі мають важливе значення для країн, які прагнуть розвивати цифрову трансформацію, включаючи Україну.

Естонія одна з перших країн Європи, яка забезпечила онлайн-доступ до майже всіх державних послуг, за винятком реєстрації нерухомості та укладання чи розірвання шлюбу, що значно спростило бюрократичні процедури, та економить час громадян й знижує витрати держави.

Всі державні реєстри Естонії об’єднані у єдину систему X-Road, що дозволяє обмінюватися даними між установами в реальному часі. Це зменшує дублювання інформації та виключає необхідність громадян подавати одну й ту саму інформацію до різних органів [191].

Унікальною є й естонська програма електронного резидентства (e-Residency). Відповідна програма дозволяє іноземним громадянам отримати цифрову ідентичність Естонії, відкривати компанії, вести бізнес та керувати ним дистанційно. Ця ініціатива значно підвищила інвестиційну привабливість країни та залучила підприємців з усього світу [192].

Естонія активно впроваджує штучний інтелект на державному рівні. Так, зокрема, він використовується для автоматизації юридичних процесів,

адміністрування державних послуг та прогнозування потреб громадян, що дозволило оптимізувати роботу державного апарату та знизити людський фактор у рутинних завданнях [193, с. 42].

Варто відзначити, що Естонія є першою країною у світі, яка запровадила можливість голосувати онлайн на виборах. Онлайн-голосування значно підвищило рівень участі громадян у виборах, особливо серед молоді та людей, які перебувають за кордоном [193, с. 43].

Естонський підхід до цифровізації підвищив рівень довіри громадян до уряду, зменшив корупцію та забезпечив прозорість управління. Для України, де питання корупції та ефективності публічних послуг є критичними, досвід Естонії може стати основою для побудови прозорого управління.

Впровадження Україною окремих практик Естонії не лише модернізує публічне управління, але й сприятиме зміцненню довіри до влади, підвищенню ефективності економіки та інтеграції у європейський цифровий простір. Україна має всі можливості для запозичення цього досвіду, створюючи власну цифрову державу, що відповідає сучасним викликам.

На окрему увагу заслуговує досвід адміністративно-правового регулювання інформаційних технологій у Сполучених Штатах Америки.

Сполучені Штати Америки відомі своїм прагматичним та гнучким підходом до регулювання інформаційних технологій, що поєднує державне регулювання з ініціативами саморегулювання індустрії. Цей підхід спрямований на створення сприятливого середовища для інновацій, водночас забезпечуючи захист споживачів та національну безпеку.

У США значна частина регулювання інформаційних технологій покладається на саморегулювання індустрії. Великі технологічні компанії, такі як Google, Microsoft та Amazon, розробляють власні етичні кодекси та стандарти роботи з даними, прагнучи забезпечити відповідальне використання технологій та захист приватності користувачів [194].

Цей підхід базується на припущенні, що індустрія має глибоке розуміння технологічних процесів і здатна оперативно реагувати на виклики,

пов'язані з новими технологіями. Однак ефективність саморегулювання часто залежить від добровільної участі компаній та може потребувати державного нагляду для забезпечення дотримання встановлених стандартів.

Федеральний уряд США активно підтримує розвиток приватно-державного партнерства у сфері кібербезпеки. Закон «Про модернізацію інформаційної безпеки» (Federal Information Security Modernization Act) зобов'язує державні органи дотримуватися чітких стандартів безпеки та заохочує співпрацю з приватним сектором для підвищення загального рівня кіберзахисту. Таке партнерство дозволяє об'єднати ресурси та експертизу обох секторів, сприяючи ефективнішому реагуванню на кіберзагрози та захисту критичної інфраструктури [195].

Американське законодавство орієнтоване на створення умов для інновацій, уникаючи надмірно детального регулювання окремих технологій. Такий підхід забезпечує швидку адаптацію до змін у галузі та стимулює розвиток нових технологічних рішень. Замість встановлення жорстких правил для кожної технології, законодавці зосереджуються на загальних принципах, таких як захист споживачів, конкуренція та національна безпека, залишаючи простір для саморегулювання та адаптації індустрії до нових викликів.

Прагматичний та гнучкий підхід США до регулювання інформаційних технологій, що поєднує саморегулювання індустрії з державним наглядом та партнерством, створює сприятливе середовище для інноваційного розвитку. Водночас, такий підхід вимагає постійного моніторингу та адаптації до швидких технологічних змін, а також забезпечення балансу між свободою інновацій та необхідністю захисту суспільних й державних інтересів.

Особливої уваги заслуговує досвід адміністративно-правового регулювання інформаційних технологій у наступних країнах: Республіка Сінгапур, Республіка Корея та Китайська Народна Республіка, які демонструють унікальні підходи до регулювання інформаційних технологій у своїх державах.

Так, Республіка Сінгапур (далі – Сінгапур) є світовим лідером у сфері розробки нормативно-правових актів для регулювання штучного інтелекту.

У сучасному світі, де штучний інтелект (далі –ШІ) стає невід'ємною частиною повсякденного життя, питання його етичного та відповідального використання набувають особливої актуальності. Сінгапур, як один із лідерів у сфері технологічних інновацій, активно працює над створенням нормативно-правових актів для регулювання ШІ. Однією з ключових ініціатив у цьому напрямі є «Model AI Governance Framework» — модельна структура управління ШІ, яка містить рекомендації щодо етичного використання штучного інтелекту [196].

Запроваджена у 2019 році, ця структура стала результатом зусиль Управління з розвитку інфокомунікацій та медіа (IMDA) [197] та Комісії із захисту персональних даних (PDPC) [198] Сінгапуру. Її метою є надання організаціям практичних рекомендацій для відповідального впровадження ШІ, забезпечуючи баланс між інноваціями та захистом прав громадян. Структура є універсальною, тобто не залежить від конкретної галузі чи технології, що робить її застосовною в різних секторах економіки.

Основними принципами «Model AI Governance Framework» є: 1) людиноцентричність та безпека (ШІ-системи повинні бути орієнтовані на благо людини та забезпечувати її безпеку); 2) прозорість та зрозумілість (рішення, прийняті ШІ, мають бути обґрунтованими та зрозумілими для користувачів); 3) справедливість (використання ШІ не повинно призводити до дискримінації чи упередженості); 4) підзвітність (організації несуть відповідальність за впровадження та використання ШІ-систем).

У 2020 році було представлено друге видання цієї структури, яке враховує досвід організацій, що вже успішно впровадили ШІ, та міжнародні рекомендації. Це видання надає більш чіткі та ефективні вказівки для відповідального використання ШІ.

Крім того, Республіка Сінгапур розробила інструмент «AI Verify» — платформу для тестування та оцінки ШІ-систем на відповідність етичним

принципам. Цей інструмент допомагає організаціям перевіряти свої ШІ-моделі на предмет прозорості, безпеки та справедливості, сприяючи підвищенню довіри до технологій штучного інтелекту [199].

Завдяки таким ініціативам, Сінгапур демонструє прагнення створити в своїй державі екосистему, де інновації у сфері штучного інтелекту будуть розвиватись в гармонії з етичними стандартами та правами людини. Цей підхід може слугувати прикладом для України та інших країн, що прагнуть впроваджувати технології штучного інтелекту відповідально та етично.

Республіка Корея (далі - Південна Корея), також відома своєю технологічністю, активно впроваджує концепцію «розумних міст», інтегруючи передові технології для підвищення якості життя своїх громадян. Цей процес супроводжується розробкою та впровадженням законодавчих актів, що регулюють використання великих даних, Інтернету речей (IoT) та автоматизованих транспортних засобів [200].

Концепція «розумного міста» передбачає використання цифрових технологій для оптимізації міських функцій, покращення зв'язку між мешканцями та урядовими структурами, а також забезпечення сталого розвитку міст. У Південній Кореї ця концепція реалізується через низку ініціатив, спрямованих на інтеграцію IoT, великих даних та автоматизованих транспортних систем у міське середовище.

Інтернет речей відіграє ключову роль у створенні розумних міст, забезпечуючи з'єднання між різноманітними пристроями та системами для збору та обміну даними. Це дозволяє містам ефективніше керувати ресурсами, такими як енергія та вода, а також покращувати транспортну інфраструктуру. Використання IoT у міському плануванні сприяє зменшенню втрат води через старіння інфраструктури труб та підвищенню ефективності перевезень

Великі дані (Big Data) та аналітика є невід'ємною частиною розумних міст, оскільки вони дозволяють збирати та аналізувати інформацію в режимі реального часу. Це сприяє прийняттю обґрунтованих рішень щодо

управління міськими системами та покращенню якості життя громадян. Обробка та аналітика великих даних відіграють ключову роль у розумних містах, допомагаючи виявляти тенденції та закономірності, прогнозувати потреби міста та приймати більш обґрунтовані управлінські рішення

Автоматизовані транспортні засоби є ще одним важливим елементом розумних міст, оскільки вони можуть зменшити затори на дорогах, підвищити безпеку руху та знизити викиди шкідливих речовин. Інтелектуальні транспортні системи використовують передові технології, такі як датчики, аналітика даних та машинне навчання, для покращення міської мобільності [200].

Уряд Південної Кореї активно підтримує розвиток розумних міст, запроваджуючи відповідні законодавчі ініціативи та інвестуючи в інфраструктуру. Це включає розробку стандартів для IoT-пристроїв, захист даних громадян та забезпечення безпеки автоматизованих транспортних систем. Такі зусилля сприяють створенню більш стійких та інклюзивних міських просторів, покращуючи якість життя мешканців та підвищуючи ефективність міського управління.

Таким чином, досвід Південної Кореї у впровадженні розумних міст демонструє, як інтеграція передових технологій та відповідне законодавче регулювання можуть сприяти сталому розвитку міських територій та покращенню добробуту громадян.

У сучасному світі технологічні інновації дедалі більше інтегруються й у сфери правового життя, зокрема в систему правосуддя. Китайська Народна Республіка (далі – Китай), відома своїм прагненням до технологічного лідерства, активно впроваджує штучний інтелект у судову систему.

Так, зокрема, у китайських судах було впроваджено систему штучного інтелекту Smart Court SoS, метою якої є автоматизація судових процесів, зменшення витрат часу та коштів, а також мінімізація корупційних ризиків і зловживань посадовими повноваженнями суддів [201].

До 2016 року кожен суд у Китаї користувався власною інформаційною системою, яка не була інтегрована в загальнодержавну базу. Судді рідко обмінювалися даними між судами або з Пекіном. Однак створення національної системи розумного судочинства зобов'язало всі судові установи перейти на єдиний цифровий формат документів та інтегрувати свої бази даних до центральної системи. Спочатку ШІ-алгоритми використовувалися для ведення реєстру судових справ, автоматизації запису судових засідань, розпізнавання мовлення та обслуговування дистанційних судових процесів.

Згодом функціональність системи було розширено: штучний інтелект отримав можливість аналізувати справи, рекомендувати відповідні правові норми, судові рішення та нормативні акти, що можуть бути застосовані у кожній конкретній справі. Алгоритми опрацьовують величезний обсяг правової інформації, навчаються на основі раніше ухвалених судових рішень та пропонують найбільш релевантні правові рекомендації.

«Розумний суд» застосовує великі дані та технології машинного навчання, що дозволяє не лише зберігати й оновлювати бази даних, а й автоматично перевіряти юридичні документи, знаходити неточності або помилки, генерувати правові висновки та рекомендації. Деякі алгоритми спеціалізуються на певних напрямах права, таких як комерційні (корпоративні) спори чи трудові конфлікти (спори).

Штучний інтелект також допомагає суддям знаходити аналогічні справи минулих років, швидко ідентифікувати відповідні статті законодавства, формувати тексти рішень і додаткових судових документів. Враховуючи, що 120 000 суддів Китаю щороку розглядають приблизно 19 мільйонів справ, впровадження такої технології значно полегшило їхню роботу.

Система Smart Court SoS інтегрована в робоче середовище суддів по всій країні. У 2022 році Верховний суд зобов'язав суддів у кожній справі консультуватися зі штучним інтелектом, а якщо ухвалене рішення не збігається з рекомендаціями системи, вони повинні надати обґрунтоване

письмове пояснення. Прихильники цієї ініціативи наголошують, що метою нововведення є підвищення прозорості судових процесів, зниження корупції та забезпечення об’єктивності, а не заміна суддів електронними алгоритмами [201].

Проте критики стверджують, що судді часто слідують рекомендаціям ШІ, аби уникнути необхідності додаткового обґрунтування своїх рішень. Це може призводити до механічного ухвалення рішень без належного врахування індивідуальних обставин справи.

Система Smart Court SoS вийшла за межі залів суду й отримала доступ до баз даних, що належать поліції, прокуратурі та державним установам. Одна з її функцій – забезпечення виконання судових рішень, що раніше було проблемним через кадровий дефіцит. Завдяки інтеграції з державними реєстрами ШІ може миттєво знаходити активи засуджених, накладати арешт та ініціювати їх продаж на онлайн-аукціонах. Також система здатна запроваджувати додаткові санкції, наприклад, забороняти боржникам користуватися громадським транспортом, авіаперельотами чи соціальними послугами.

Впровадження ШІ в судову систему Китаю дозволило значно скоротити навантаження на суддів – більш ніж на третину, а також зекономити близько 1,7 мільярда робочих годин громадян країни у 2019–2021 роках. За цей же період заощаджено понад 300 мільярдів юанів (близько 45 мільярдів доларів США) [201].

Верховний суд Китаю повідомляє, що щодня система аналізує приблизно 100 000 справ, відстежуючи їхній розгляд та виявляючи можливі випадки корупції чи зловживання службовим становищем. Оскільки людські рішення часто схильні до упередженості, алгоритми можуть сприяти більш об’єктивному судочинству, виключаючи вплив несуттєвих факторів, таких як стать чи етнічна приналежність підсудного. Крім того, ШІ може об’єктивно оцінювати ймовірність рецидиву, уникаючи суб’єктивного сприйняття окремих суддів.

Водночас постає питання контролю над ШІ та перевірки його рішень. Деякі експерти висловлюють занепокоєння, що централізація судочинства за допомогою штучного інтелекту може надати непропорційний вплив вузькому колу технічних фахівців, які розробляли алгоритми або адмініструють бази даних. Крім того, залишається ризик, що алгоритми можуть успадковувати упередження, на яких вони навчалися, ґрунтуючись на попередніх судових рішеннях.

Досвід Китаю може стати цінним уроком для України та інших країн, які розглядають можливість інтеграції штучного інтелекту в свої правові системи, демонструючи як переваги, так і потенційні ризики такого підходу.

Імплементація зарубіжного досвіду в національне законодавство України є складним та багатогранним процесом, що вимагає врахування низки факторів, зокрема особливостей правової системи, рівня цифрової обізнаності населення, політичної волі та ефективності державних органів.

Україна належить до континентальної правової системи, яка характеризується кодифікованим законодавством та значною роллю писаних норм права. Натомість, Сполучені Штати Америки функціонують на основі прецедентного права, де судові рішення відіграють ключову роль у формуванні правових норм. Ця відмінність ускладнює пряме перенесення правових інститутів та механізмів з однієї системи до іншої без відповідної адаптації. Зокрема, імплементація американських підходів до регулювання інформаційних технологій вимагає ретельного аналізу та модифікації з урахуванням українських правових традицій та реалій.

Зарубіжні країни, особливо розвинені, часто мають високий рівень цифрової грамотності населення, що сприяє успішному впровадженню нових технологій та відповідного законодавства. В Україні, попри значний прогрес у сфері цифровізації, існують регіональні та соціальні диспропорції в доступі до цифрових навичок та технологій. Це може стати перешкодою для ефективної реалізації запозичених правових норм без попереднього підвищення рівня цифрової обізнаності громадян.

Успіх впровадження зарубіжних практик значною мірою залежить від політичної волі керівництва країни та спроможності державних інституцій ефективно реалізовувати реформи. В Україні спостерігається активна співпраця з міжнародними партнерами, зокрема з Європейським Союзом та США, що надає технічну та експертну допомогу у впровадженні передових практик. Наприклад, у грудні 2024 року Міністерство оборони України домовилося з представниками США про поглиблення співпраці у сфері кібербезпеки, що передбачає збільшення інвестицій в українські інновації та посилення цифрової інфраструктури [202].

Україна активно інтегрується в міжнародний цифровий простір, переймаючи досвід та отримуючи підтримку від розвинених країн. Співпраця з ЄС та США охоплює різні аспекти, від розробки законодавства до впровадження новітніх технологій. Зокрема, підписання меморандуму між Міністерством цифрової трансформації України та Європейською організацією кібербезпеки (ECSO) сприяє зміцненню кібербезпеки та інтеграції України в європейський цифровий простір [202].

Підбиваючи підсумки необхідно зазначити, що зарубіжний досвід є надзвичайно цінним ресурсом для вдосконалення адміністративно-правового регулювання інформаційних технологій в Україні. Успішне впровадження найкращих практик сприятиме розвитку цифрової економіки, зміцненню інформаційної безпеки та підвищенню довіри громадян до публічного управління. Однак використання цього досвіду повинно бути збалансованим, із врахуванням національних реалій та інтересів. Орієнтуючись на міжнародні стандарти, Україна має можливість стати активним учасником глобального цифрового простору, забезпечуючи сталий розвиток суспільства та держави.

3.3 Перспективи розвитку нормативно-правового забезпечення використання інформаційних технологій в Україні

Розвиток інформаційних технологій в Україні є одним з головних чинників економічного зростання та інтеграції до глобального інформаційного простору. Проте, для повноцінного використання потенціалу сфери інформаційних технологій, Україні необхідно створити ефективну нормативно-правову базу, яка б відповідала сучасним викликам та тенденціям.

На сьогодні в Україні існує низка законодавчих актів, що регулюють інформаційну сферу. Проте, швидкий розвиток технологій вимагає постійного оновлення та адаптації цих нормативних документів. Деякі з них мають декларативний характер або не враховують сучасних реалій, що ускладнює їх практичне застосування. Зокрема, чимало науковців відзначають, що в Україні відсутнє дійсно ефективне законодавство у цій сфері, що стримує розвиток інформаційних відносин.

Однією з основних проблем, про яку систематично згадувалось у дисертаційному дослідженні, є недостатня гармонізація національного законодавства з європейськими стандартами, що значно ускладнює інтеграцію України до європейського цифрового ринку та обмежує можливості для міжнародної співпраці.

Крім того, існують значні прогалини у правовому регулюванні Україною новітніх технологій, таких як блокчейн, штучний інтелект та Інтернет речей, що створює правову невизначеність для учасників цієї сфери правовідносин.

Серед ключових проблем правового регулювання інформаційних технологій в умовах цифрової трансформації та повномасштабної війни важливе місце займає проблема належного забезпечення Україною кібербезпеки, у зв’язку із відсутністю чітко визначеної системи заходів державного регулювання у цій сфері.

Для подолання всіх вищезазначених проблем на державному рівні мають бути здійснені комплексні заходи з удосконалення нормативно-правової бази України.

Перспективним етапом покликаним удосконалити нормативно-правове забезпечення використання інформаційних технологій в Україні має стати адаптація національних нормативних актів до вимог Європейського Союзу, що сприятиме інтеграції України до Єдиного цифрового ринку та підвищить конкурентоспроможність вітчизняних ІТ-компаній.

Маємо зазначити, що Єдиний цифровий ринок (Цифровий єдиний ринок; ЄЦР ЄС) є політичним документом, що належить до Єдиного європейського ринку, та охоплює цифровий маркетинг, електронну комерцію та телекомунікації.

ЄЦР ЄС передбачає вільний обіг товарів, послуг, капіталу та персональних даних у цифровому просторі без внутрішніх бар'єрів. Для України інтеграція до цього ринку відкриє можливість спрощеного доступу українських ІТ-компаній до європейських замовників, а відповідність нормативам ЄС дозволить українському бізнесу стати привабливішим для міжнародних партнерів.

Інтеграція до Єдиного цифрового ринку надасть Україні право брати участь у європейських інноваційних проєктах (таких як Horizon Europe), дозволивши українським компаніям отримувати фінансування для впровадження своїх ідей та залучати іноземні інвестиції у свої проєкти.

Загальний регламент про захист даних (General Data Protection Regulation; GDPR) є ключовим регламентом Європейського Союзу у сфері захисту персональних даних, який, з однієї сторони встановлює достатньо жорсткі вимоги до обробки інформації про громадян, з іншої покликаний забезпечити надійний контроль та захист персональних даних громадян та резидентів ЄС, а також спростити регуляторне середовище для міжнародного бізнесу.

Варто зауважити, що Україна може повністю адаптувати Загальний регламент захисту даних навіть без членства в Європейському Союзі. Вже є приклади країн, які впровадили GDPR або узгодили своє законодавство з його вимогами, не будучи членами ЄС. Так, Велика Британія після Brexit ухвалила UK GDPR, який повторює відповідні європейські правила, але дозволяє адаптувати їх під внутрішні потреби. Швейцарія, аналогічно, не будучи членом ЄС, має власний закон про захист даних, який повністю гармонізований з GDPR. А Ізраїль, Канада та Японія, не будучи європейськими країнами, отримали від Європейського Союзу статус «країни з адекватним рівнем захисту», що дозволяє їм передавати персональні дані без додаткових юридичних бар'єрів.

Повне впровадження Україною Загального регламенту про захист даних (GDPR) надасть державі наступні переваги: 1) визнання українських компаній як надійних партнерів (відповідність GDPR дозволить українським IT-компаніям обробляти персональні дані громадян ЄС без додаткових правових обмежень); 2) підвищення рівня безпеки даних (впровадження вимог GDPR сприятиме посиленню захисту персональної інформації, що є критично важливим для фінансового, медичного, інформаційно-телекомунікаційного секторів, сектору електронної комерції); 3) мінімізація юридичних ризиків для бізнесу (компанії, що працюють з клієнтами з ЄС, зможуть уникнути штрафів та правових колізій, дотримуючись європейських стандартів).

Іншою нагальною задачею необхідною для розвитку нормативно-правового забезпечення використання інформаційних технологій в Україні є створення правових засад для регулювання технологій блокчейн, штучного інтелекту та Інтернету речей, що забезпечить правову визначеність та стимулюватиме інновації, а також сприятиме залученню іноземних інвестицій для розвитку стартап-екосистеми в Україні.

Розвиток цифрових технологій, таких як блокчейн, штучний інтелект (ШІ) та Інтернету речей (IoT), відкриває нові можливості для державної

економіки, публічного адміністрування та суспільства. Водночас відсутність чіткої нормативно-правової бази для їх використання створює ризики правової невизначеності, уповільнює розвиток інновацій і зменшує привабливість України для іноземних інвесторів та стартапів.

Блокчейн є основою для криптовалют, смарт-контрактів, децентралізованих фінансових систем (DeFi) та інших інновацій. В Україні було зроблено перші кроки у цьому напрямку, зокрема прийнято Закон України «Про віртуальні активи», який мав регулювати правовідносини, що виникають у зв'язку з оборотом віртуальних активів в Україні, визначити права та обов'язки учасників ринку віртуальних активів, засади державної політики у сфері обороту віртуальних активів. Проте, як відомо, цей Закон був ветований Президентом й подальша доля цього нормативного акту залишається невідомою.

Основною перешкодою для набуття чинності закону стала необхідність внесення змін до Податкового кодексу України, які б встановлювали правила оподаткування операцій із віртуальними активами. Це рішення було цілком логічним, адже без чітких правил оподаткування неможливо ефективно регулювати обіг криптовалют. Але саме ці зміни викликали найбільші труднощі.

Законопроєкт про внесення змін до Податкового кодексу України було подано ще у березні 2022 року. Він передбачав зрозумілі й вигідні умови: оподаткування доходів від операцій із цифровими активами за ставкою 5% та звільнення таких операцій від ПДВ. Однак після початку повномасштабної війни питання регулювання криптовалютного ринку втратило пріоритетність, поступившись місцем нагальним проблемам, пов'язаним із воєнним станом.

Сам Закон України «Про віртуальні активи», навіть після внесення правок, залишався недосконалим. Він поділяв віртуальні активи лише на дві групи: забезпечені та незабезпечені. Однак такий підхід був занадто спрощеним і не враховував специфіку різних видів цифрових активів, таких

як NFT, утилітарні токени чи DeFi-продукти. Це могло створити правові колізії та сприяти можливим зловживанням у сфері оподаткування.

Ще одним викликом було ставлення Національного банку України до проблеми врегулювання ринку віртуальних активів, який у період війни був зосереджений на підтримці фінансової стабільності. Запуск регулювання криптовалютного ринку міг створити нові загрози для монетарної політики. Все це, разом із загальноекономічними труднощами, спонукало НБУ висловити застереження щодо доцільності впровадження нового законодавства у сфері віртуальних активів.

На міжнародній арені також відбувалися важливі події. У червні 2023 року Європейський Союз ухвалив Регламент про ринки криптоактивів (Markets in Crypto-Assets; MiCA) - нормативно-правовий акт Європейського Союзу, метою якого є оптимізація впровадження технології блокчейну та децентралізованої бази даних як частини регулювання віртуальних активів у Європейському Союзі, одночасно захищаючи при цьому користувачів та інвесторів.

Україна, яка отримала статус кандидата на членство в ЄС, має гармонізувати своє законодавство з європейськими стандартами. А Закон України «Про віртуальні активи» потребує серйозного доопрацювання, щоб відповідати вимогам MiCA.

Враховуючи поточний стан законодавства та міжнародний досвід, для ефективного впровадження віртуальних активів в Україні необхідно дотримуватись поетапного підходу, який дозволить знайти баланс між інноваційністю, безпекою та фінансовою стабільністю держави та виконанням Україною міжнародних зобов’язань.

Ефективними заходами, які б могли сприяти Україні вирішити проблему регулювання віртуальних активів вбачаються наступні:

1. Адаптація законодавства до стандартів Європейського Союзу (MiCA).

Оскільки Україна є кандидатом на вступ до ЄС, регулювання криптоактивів має бути повністю гармонізоване з Регламентом MiCA. Для цього необхідно оновити діючу редакцію Закону України «Про віртуальні активи», доповнивши його класифікацією активів згідно з MiCA: токени електронних грошей (EMT); токени, прив'язані до активів (ART); утилітарні токени; криптовалюти, що не є фінансовими інструментами.

Необхідним заходом, що забезпечить захист інвесторів, прозорість та відповідність міжнародним стандартам ринку віртуальних активів має бути ліцензування криптовалютних операторів та утворення наглядового органу (регулятора крипторинку), який координуватиме виконання MiCA в Україні.

2. Впровадження адекватної та зрозумілої системи оподаткування.

Одна з головних проблем у регулюванні криптовалют – відсутність чітких податкових правил. Україна може запровадити спрощену та привабливу систему оподаткування за аналогією з країнами ЄС: фіксована ставка 5% на прибуток від операцій із криптовалютами для фізичних осіб, податок на прибуток компаній – 10% (нижче, ніж стандартні 18%), та звільнення криптовалютних транзакцій від ПДВ, як це здійснено у ЄС.

В результаті реалізації відповідних заходів буде створено сприятливий податковий клімат для криптокомпаній, зменшено тіньовий обіг коштів та збільшено надходження до бюджету України.

3. Визначення регуляторного органу та його функцій

В Україні немає єдиного регулятора крипторинку, що створює правову невизначеність. Оптимальним варіантом міг бути розподіл відповідальності між кількома державними структурами: Національний Банк України – регулює цифрові валюти, випуск цифрової валюти центрального банку (електронної гривні); Національна комісія з цінних паперів та фондового ринку – регулює ринок токенів, прирівняних до фінансових інструментів; Державна служба фінансового моніторингу – здійснює комплекс заходів, спрямованих на запобігання використанню фінансових систем для відмивання доходів, отриманих незаконним шляхом.

В результаті реалізації відповідних заходів відбудеться чіткий розподіл функцій між органами державної влади, що зменшить хаос і дублювання повноважень.

4. Захист прав споживачів.

Для мінімізації ризиків шахрайства та запобігання використанню фінансових систем для відмивання доходів, отриманих незаконним шляхом та для фінансування тероризму, слід впровадити для криптобірж систему заходів ідентифікації та встановлення особи контрагента перед здійсненням фінансової операції (Know Your Customer; KYC), ввести правила і стандарти по боротьбі з відмиванням коштів (FATF) (моніторинг транзакцій) та створити механізм компенсації втрачених коштів у разі злочинних дій.

Результатом реалізації відповідних заходів буде підвищення рівня безпеки та довіри до крипторинку України.

5. Освіта та популяризація блокчейну.

Розвиток криптоіндустрії неможливий без підготовки кваліфікованих фахівців та інформування громадян. Державні та приватні ініціативи можуть включати навчальні програми у вишах з блокчейну, DeFi, NFT, освітні кампанії для громадян про безпечне використання криптоактивів.

Результатом реалізації вищевикладених заходів стане підвищення фінансової грамотності населення України.

Отже, запуск ринку віртуальних активів в Україні можливий лише за умови комплексного та поступового підходу. Реалізація вищенаведених заходів дозволить Україні стати одним із центрів криптоінновацій у Східній Європі та інтегруватися в глобальну цифрову економіку.

Як показує час, Закон України «Про віртуальні активи» виявився амбітним, але дещо передчасним проєктом. Його історія вкотре доводить, як складно поєднати між собою інновації, економічну стабільність та дотримання міжнародних зобов’язань. Однак є сподівання, що у майбутньому, з урахуванням досвіду інших країн та власних уроків, Україна матиме шанс створити ефективне правове середовище для крипторинку, яке

сприятиме його розвитку та водночас захищатиме інтереси держави і громадян.

В розрізі питання перспектив розвитку нормативно-правового забезпечення використання інформаційних технологій в Україні не можна обійти стороною питання нормативно-правового регулювання Інтернету речей.

Інтернет речей (Internet of Things, IoT) вже перестав бути чимось фантастичним — сьогодні це частина нашого повсякденного життя. Смартфони, смарт-годинники, «розумні» будинки, системи управління енергоспоживанням і навіть автономні транспортні засоби — усе це приклади IoT, які поступово стають звичними. Однак разом із розвитком цих технологій виникає потреба у створенні відповідного нормативно-правового регулювання. Україна, прагнучи інтегруватися в європейський цифровий простір, обов’язково має звернути увагу на цей виклик.

IoT — це мережа пристроїв, що з'єднані між собою через Інтернет для збору, передачі та аналізу даних. Це може бути будь-що: від «розумних» холодильників до складних систем управління містами. Впровадження IoT дозволяє оптимізувати процеси, економити ресурси і створювати нові сервіси. Наприклад, у сільському господарстві IoT дозволяє фермерам контролювати полив, уникаючи зайвих витрат води, а в енергетиці — автоматично регулювати споживання енергії залежно від конкретних потреб.

Для України, яка шукає шляхи для економічного зростання та модернізації, післявоєнної відбудови, IoT може стати важливим рушієм. Але без належного адміністративно-правового регулювання впровадження цих технологій можуть бути створені ризики для безпеки, приватності та інфраструктури.

На сьогодні в Україні відсутній єдиний нормативно-правовий акт, який регулює сферу IoT. Незважаючи на це, окремі аспекти цієї технології регулюються законами про електронні комунікації, кібербезпеку та захист

персональних даних, проте комплексного підходу немає, що створює правові прогалини, які можуть використовуватися недобросовісними компаніями.

У сфері захисту персональних даних IoT-пристрої збирають величезну кількість даних про користувачів, включаючи їхні звички, місцезнаходження і навіть стан здоров'я. Захист цих даних стає надзвичайно важливим.

В питанні кібербезпеки IoT-пристрої можуть стати вразливими до кіберзагроз. Закон «Про основні засади забезпечення кібербезпеки України» створює базу для захисту, але він не враховує специфіку IoT.

Для ефективної роботи IoT пристрої повинні взаємодіяти між собою. Відсутність стандартів може призвести до несумісності різних систем, що уповільнює їхнє впровадження.

IoT-пристрої часто працюють автономно, приймаючи рішення без втручання людини. Це викликає питання: хто має нести відповідальність за помилки пристрою? Наприклад, якщо автономний автомобіль спричинить ДТП, хто повинен нести відповідальність — виробник, власник чи розробник програмного забезпечення?

Враховуючи зростаючу роль IoT у цифровій трансформації України, необхідно розробити комплексний законодавчий акт, який забезпечить безпеку, приватність, стандартизацію та відповідальність у сфері Інтернету речей.

Ефективними заходами, які б могли допомогти Україні вирішити проблему регулювання Інтернету речей вбачаються наступні:

1. Розробка спеціального закону.

Необхідно розробити Закон України «Про Інтернет речей», який визначить основні поняття (IoT-пристрій, IoT-мережа, оператор IoT-сервісів, користувач тощо), встановить правові рамки для обробки даних, сертифікації пристроїв, підключення до державних інформаційних систем та регулюватиме відповідальність виробників, операторів та користувачів IoT.

Результатом реалізації відповідних заходів стане правова визначеність для всіх учасників ринку IoT.

2. Гармонізація із законодавством Європейського Союзу.

Україна повинна адаптувати своє законодавство до європейських стандартів, зокрема: Регламенту ЄС про електронні комунікації (EECC), Cybersecurity Act (Акт про кібербезпеку), NIS2 Directive (Директива про мережеву та інформаційну безпеку), Data Act (Акт про дані, який регулює доступ до даних IoT).

Для цього слід визначити орган, відповідальний за гармонізацію IoT-законодавства (наприклад, Мінцифра або НКРЗІ), розробити національні стандарти IoT на основі європейських норм, включити положення про транскордонний обмін IoT-даними для інтеграції з європейськими партнерами.

Результатом реалізації відповідних заходів стане відповідність IoT європейським стандартам та можливість українських компаній працювати на ринку ЄС.

3. Вимоги до безпеки IoT-пристроїв.

Законодавство має зобов’язати виробників IoT-пристроїв використовувати обов’язкове шифрування даних та аутентифікацію користувачів, гарантувати регулярне оновлення програмного забезпечення для усунення вразливостей, заборонити використання дефолтних паролів, як у країнах ЄС та впровадити «захист за замовчуванням» (security by default) у всіх пристроях.

Результатом реалізації наведених заходів стане зменшення ризиків кібератак на IoT-мережі.

4. Сертифікація та стандартизація IoT-пристроїв.

На державному рівні необхідно запровадити обов’язкову сертифікацію IoT-пристроїв, яка підтвердить їхню відповідність стандартам безпеки. Для цього необхідно утворити національний орган сертифікації IoT (або ж делегувати ці повноваження Держспецзв’язку), вимагати від виробників сертифікацію пристроїв перед їх виходом на ринок та зобов’язати операторів зв’язку фільтрувати незахищені IoT-пристрої (з метою кібербезпеки).

Результатом реалізації відповідних заходів стане підвищення рівня довіри користувачів до IoT-пристроїв.

5. Захист персональних даних користувачів IoT.

IoT-пристрої збирають значні обсяги персональних даних, тому необхідно впровадити механізми анонімізації та мінімізації збору даних, встановити обмеження на передачу IoT-даних третім сторонам без згоди користувача.

Результатом реалізації відповідних заходів стане належний захист конфіденційної інформації користувачів.

6. Відповідальність за «збої» в системі та кібератаки

Необхідно передбачити чітку відповідальність за проблеми безпеки IoT. Виробники мають нести відповідальність за вразливості в пристроях, оператори IoT-мереж відповідають за захист каналів зв'язку, а користувачі в свою чергу повинні оновлювати пристрої та дотримуватись передбачених виробником правил безпеки.

В результаті реалізації відповідних заходів матимемо чіткий механізм вирішення інцидентів і належної відповідальності.

Реалізація всіх вищенаведених заходів допоможе Україні створити безпечну, сучасну та конкурентоспроможну IoT-екосистему, інтегровану в європейський цифровий ринок.

Таким чином, Інтернет речей відкриває перед Україною величезні можливості, але водночас ставить й серйозні виклики. Без належного регулювання впровадження IoT може стати джерелом ризиків для приватності, безпеки та економіки. Проте, якщо створити ефективне нормативно-правове середовище, Україна зможе стати одним зі світових лідерів у впровадженні IoT, залучаючи інвестиції, розвиваючи інновації та підвищуючи якість життя своїх громадян.

Окремої уваги заслуговують перспективи нормативно-правового регулювання штучного інтелекту в Україні.

Штучний інтелект (далі – ШІ) стає важливим інструментом у сфері аналізу даних, прогнозування, автоматизації та прийняття рішень. Його впровадження створює значні переваги, але водночас породжує низку юридичних та етичних питань: 1) відповідальність за дії ШІ (необхідно визначити, хто має нести відповідальність за помилки чи шкоду, спричинену ШІ-системами (розробник, власник чи оператор); 2) етичні аспекти (розробка стандартів для забезпечення прозорості, недискримінації та етичного використання ШІ); 3) право на конфіденційність (гарантування захисту персональних даних, оброблюваних ШІ); 4) правовий статус ШІ (дослідження можливості надання обмеженого правового статусу автономним системам (наприклад, у сфері медицини, торгівлі чи страхуванні тощо).

Враховуючи глобальні тенденції у регулюванні штучного інтелекту (ШІ) та необхідність правової визначеності, в Україні має бути розроблена чітка та ефективна нормативно-правова база для використання ШІ. Регулювання має відповідати міжнародним стандартам, забезпечувати гарантії безпеки, етичність та відповідальність у використанні ШІ, а також сприяти розвитку інноваційного бізнесу.

Ефективними заходами, які б могли допомогти Україні вирішити проблему регулювання штучного інтелекту вбачаються наступні:

1. Прийняття спеціального закону.

В Україні має бути ухвалено Закон України «Про штучний інтелект», який визначить офіційні терміни та класифікацію ШІ, обов’язки та відповідальність розробників, операторів і власників ШІ, сфери застосування ШІ з посиленим регулюванням (медицина, правосуддя, фінанси, безпека тощо) та механізми державного контролю за безпекою ШІ.

Результатом реалізації відповідних заходів стануть чіткі правила використання ШІ, правова визначеність для бізнесу та держави.

2. Гармонізація з європейським законом про штучний інтелект.

Україна, як кандидат у ЄС, повинна адаптувати ШІ-законодавство до Європейського закону про штучний інтелект (Artificial Intelligence Act), що передбачає надання класифікації систем ШІ за рівнем ризику (нульовий, низький, високий, неприйнятний ризик), заборону шкідливих систем (наприклад, ШІ для масового спостереження без згоди громадян), обов'язкову сертифікацію критичних ШІ-рішень (у сфері медицини, правосуддя, фінансів), вимоги до прозорості ШІ-систем (обов'язкове маркування контенту, створеного ШІ).

Результатом реалізації відповідних заходів стане відповідність національного законодавства європейським стандартам, а також можливість українських компаній безперешкодно працювати в ЄС.

3. Визначення відповідальності за дії ШІ.

Одна з головних проблем – хто відповідальний за шкоду, спричинену штучним інтелектом? Для цього необхідно встановити принцип «людського контролю» – остаточне рішення має приймати людина, а не автономна система. Окрім того, слід розподілити відповідальність між розробниками (за алгоритми та дані навчання), операторами ШІ (за правильне використання), користувачами (за неналежне застосування).

В результаті реалізації відповідних заходів будуть мінімізовані юридичні ризики, а також, буде забезпечено захист прав постраждалих осіб.

4. Захист персональних даних та конфіденційності.

ШІ обробляє величезні масиви даних, що потребує посилення захисту конфіденційності. Для цього необхідно встановити правила обробки даних за принципами Загального регламенту про захист даних (GDPR), вимагати анонімності даних при навчанні ШІ та заборонити дискримінаційні алгоритми, які можуть порушувати права людини.

Результатом реалізації відповідних заходів стане безпечне використання ШІ без загрози для конфіденційності громадян.

5. Етичні принципи використання ШІ.

У Законі України «Про штучний інтелект» необхідно передбачити етичні норми ШІ, які включатимуть принципи недискримінації (заборона алгоритмів, що створюють упередження) та прозорі алгоритми (користувачі повинні розуміти, як працює ШІ та знати, на якій основі ШІ приймає рішення).

Результатом реалізації відповідних заходів стане зменшення ризиків соціальної несправедливості та довіра громадян до технологій ШІ.

6. Впровадження державного контролю за ШІ.

Для регулювання сфери ШІ слід створити Державне агентство з питань штучного інтелекту, яке контролюватиме дотримання стандартів безпеки, займатиметься сертифікацією ШІ-рішень високого ризику та здійснюватиме моніторинг випадків зловживання ШІ (наприклад, deepfake у політичній рекламі).

В результаті реалізації відповідних заходів будуть мінімізовані випадки використання ШІ в небезпечних або злочинних цілях.

Всі вищенаведені заходи допоможуть Україні отримати лідерські позиції у сфері регулювання штучного інтелекту, розвинути інновації та забезпечити безпечне використання технологій.

В межах розгляду перспектив розвитку нормативно-правового забезпечення використання інформаційних технологій в Україні не можна залишитись осторонь питання забезпечення інформаційної безпеки в Україні.

Інформаційна безпека стала однією з головних тем сучасного світу. Кібератаки, витоки персональних даних, дезінформація — це вже не лише проблеми окремих компаній чи людей, а й виклики для цілих держав. Україна, яка знаходиться в центрі цифрової трансформації та бореться за своє існування та суверенність, стоїть перед нагальною потребою зміцнення інформаційної безпеки.

Більшість процесів, від фінансових транзакцій до публічного управління, залежать від надійності інформаційних систем. Якщо ці системи

будуть порушені, наслідки можуть бути катастрофічними (фінансові втрати, втрата довіри громадян, політична нестабільність).

В умовах війни Україна вже відчула на собі, що таке кібератаки: хакерські групи ворожої держави намагаються знищити критичну інфраструктуру, викрасти конфіденційні дані або поширити дезінформацію. Тому забезпечення інформаційної безпеки — це не просто технічне завдання, це питання національної безпеки.

Україна має значний потенціал для зміцнення своєї інформаційної безпеки.

Перш за все Україна потребує оновленої національної стратегії кібербезпеки, яка б враховувала сучасні виклики. Цей документ має визначити ключові та актуальні загрози, пріоритети для захисту критичної інфраструктури та механізми співпраці з міжнародними партнерами.

Важливо, щоб стратегія була не просто декларативною, а мала чіткий план дій та належне ресурсне забезпечення.

На жаль, станом на сьогодні у багатьох випадках кіберзлочини залишаються безкарними. Для зміни цієї ситуації необхідно уточнити визначення кіберзлочинів у Кримінальному кодексі України, встановити суворіші покарання за такі дії, як несанкціонований доступ до інформаційних систем, поширення шкідливого програмного забезпечення, викрадення персональних даних та запровадити спеціальні процедури розслідування кіберзлочинів.

На сьогодні в Кримінальному кодексі України вже передбачено відповідальність за деякі кіберзлочини (ст. 361–363-1), однак законодавство не враховує сучасні загрози, такі як кібератаки на критичну інфраструктуру (енергетичні мережі, державні реєстри, фінансові системи), блокчейн-злочини, використання штучного інтелекту у злочинних цілях (наприклад, з використанням deepfake-технологій).

Крім того, існуючі санкції за вчинені кіберзлочини не відповідають рівню їх реальної загрози. При цьому чимало правопорушників не несуть

відповідальності за скоєні злочини або ж відбуваються лише умовним терміном чи невеликими штрафами.

Справедливо зауважимо, що Україна вже почала рухатися у правильному напрямку. У 2021 році було ухвалено нову Стратегію кібербезпеки, яка стала дорожньою картою для захисту цифрового простору. Проте виклики війни вимагають її перегляду та актуалізації.

Європейський Союз розробив Закон про кібербезпеку (Cybersecurity Act), який встановлює стандарти для кіберзахисту, включаючи обов'язкову сертифікацію інформаційно-технологічних продуктів. А США запровадили й діють за концепцією «Модель з нульовою довірою» (Zero Trust), яка передбачає систематичний моніторинг та перевірку доступу до даних, всередині компаній та державних органів.

Україна може й повинна переймати ці практики, адаптуючи їх до своїх реалій.

Забезпечення інформаційної безпеки — це складний, але вкрай необхідний процес. Без надійного правового регулювання та технічних рішень жодна держава не зможе ефективно захистити своїх громадян у цифровому світі. Для України це не лише питання сучасних викликів, але й питання подальших перспектив: від того, наскільки ефективно будемо готові до кіберзагроз, залежить стабільність, економічний розвиток та національна безпека України.

Ще однією вимогою часу та важливою умовою для розвитку нормативно-правового забезпечення використання інформаційних технологій в Україні вбачається необхідність у систематизації та унормуванні правовідносин у цифровій сфері.

Україна, прагнучи інтегруватися до глобального цифрового простору, активно розвиває нормативно-правову базу у цій сфері. Однак, наявні законодавчі акти часто розпорошені, що ускладнює їх застосування та створює правову невизначеність. У цьому контексті постає питання про необхідність створення Цифрового кодексу України як єдиного

кодифікованого акту, який би систематизував та унормував правовідносини у цифровій сфері.

Стрімкий розвиток цифрових технологій вимагає адекватного та оперативного правового реагування. Фрагментарність чинного законодавства призводить до прогалин та колізій, що можуть стримувати інновації та створювати ризики для учасників цифрового ринку. Цифровий кодекс дозволить об'єднати розрізнені нормативні акти, забезпечивши цілісність та узгодженість правового регулювання. Такий підхід сприятиме підвищенню правової визначеності, прозорості та передбачуваності у сфері інформаційних технологій.

Варто зазначити, що запровадження Цифрового кодексу України матиме низку переваг, серед яких: 1) систематизація законодавства (об'єднання розрізнених нормативних актів у єдиний документ, що значно спростить їх застосування та підвищить ефективність правового регулювання); 2) гармонізація з міжнародними стандартами (адаптація європейського досвіду сприятиме інтеграції України до глобального цифрового простору та підвищенню конкурентоспроможності на міжнародному ринку); 3) захист прав громадян та бізнесу (чітке визначення цифрових прав та обов'язків забезпечить захист інтересів усіх учасників цифрових відносин); 4) стимулювання інновацій (створення сприятливого правового середовища сприятиме розвитку новітніх технологій та залученню інвестицій у IT-сектор).

З огляду на вищевикладене, створення Цифрового кодексу України є необхідним кроком для забезпечення ефективного та сучасного правового регулювання у сфері інформаційних технологій. Впровадження Цифрового кодексу стане важливим етапом на шляху до побудови розвиненого цифрового суспільства в Україні.

Таким чином, перспективи нормативно-правового забезпечення інформаційних технологій в Україні базуються на необхідності комплексної модернізації законодавства, його гармонізації з міжнародними стандартами,

запровадженні сучасних технологічних рішень та розвитку правової культури у цифровій сфері. Лише за таких умов Україна зможе стати повноцінним учасником глобального цифрового суспільства.

Висновки до розділу 3

1. Цифрова трансформація відкриває нові можливості для держави та суспільства, але водночас породжує численні виклики у сфері правового регулювання використання інформаційних технологій. Основна проблема правового регулювання інформаційних технологій в Україні в умовах цифрової трансформації полягає в тому, що розвиток технологій значно випереджає темпи законодавчого регулювання, створюючи правові прогалини та невизначеність правового статусу багатьох інформаційно-технологічних явищ.

В Україні правова система залишається консервативною, що ускладнює адаптацію до швидких технологічних змін. Ситуація з віртуальними активами яскраво демонструє цю проблему: попри зростаючу популярність цифрових активів, їх правовий статус залишається невизначеним на державному рівні.

Ще одним викликом для України є правове регулювання Інтернету речей та штучного інтелекту. Визначення статусу та відповідальності за рішення, ухвалені автоматизованими алгоритмами, залишається складним питанням для законодавця.

В умовах повномасштабної війни особливої актуальності набуває проблема забезпечення кібербезпеки. Масовані кібератаки та дестабілізаційні інформаційні операції з боку РФ вимагають вдосконалення державної політики у сфері кіберзахисту. Україна потребує оновлення Стратегії кібербезпеки, забезпечення захисту критичної інфраструктури та підвищення рівня цифрової грамотності громадян.

Таким чином, ефективне правове регулювання інформаційних технологій потребує адаптації національного законодавства до міжнародних стандартів, прискорення процесів правотворення та впровадження сучасних механізмів контролю та безпеки. Лише за таких умов Україна зможе ефективно використовувати цифрові технології, мінімізуючи ризики та забезпечуючи правовий захист громадян та бізнесу.

2. В умовах цифрової трансформації України запозичення та адаптація зарубіжного досвіду у сфері правового регулювання інформаційних технологій є важливим чинником розвитку. Досвід розвинених країн демонструє ефективні підходи до регулювання персональних даних, кібербезпеки, електронного урядування та використання штучного інтелекту.

Зокрема, Європейський Союз має комплексне правове регулювання інформаційних технологій, представлене GDPR (захист персональних даних), NIS2 (кібербезпека), MiCA (регулювання криптоактивів) та ініціативами цифрового урядування. Естонія є взірцем успішної цифровізації публічного управління, демонструючи ефективні рішення для розвитку електронного уряду та цифрової ідентифікації.

США застосовують гнучкий підхід, поєднуючи саморегулювання технологічних компаній із державним наглядом, що сприяє інноваціям й активному розвитку IT-сфери. Сінгапур активно впроваджує етичні стандарти штучного інтелекту, Південна Корея, завдяки грамотному впровадженню у національне законодавство Інтернету речей, є лідером у розбудові «розумних міст», а Китай успішно інтегрує штучний інтелект у систему правосуддя, що підвищує ефективність судочинства.

Україна, орієнтуючись на європейські та світові стандарти, має адаптувати своє законодавство до міжнародних вимог, зокрема у сфері захисту персональних даних, цифрової ідентифікації та кібербезпеки. Водночас важливо враховувати національні особливості, рівень цифрової грамотності населення та ефективність державних інституцій.

Отже, використання зарубіжного досвіду має стати ключовим інструментом для вдосконалення адміністративно-правового регулювання використання інформаційних технологій в Україні. Це дозволить забезпечити якість та прозорість публічного адміністрування, підвищити рівень довіри громадян до цифрових сервісів та інтегрувати країну у міжнародний цифровий простір.

3. До перспективних напрямів удосконалення нормативно-правового забезпечення використання інформаційних технологій в Україні слід віднести:

– повне виконання Угоди про асоціацію між Україною та ЄС, що передбачає у тому числі імплементацію в національне законодавство та юридичну практику європейських правил використання інформаційних технологій, а також форм і способів їх адміністрування з боку органів публічної адміністрації;

– повне впровадження в національне законодавство Загального регламенту Європейського Союзу про захист даних (GDPR) для забезпечення надійного контролю та захисту персональних даних громадян та спрощення регуляторних процедур для бізнесу;

– внесення змін до Закону України «Про віртуальні активи» шляхом адаптування положень цього Закону до стандартів Регламенту про ринки криптоактивів (Markets in Crypto-Assets; MiCA);

– запровадження спрощеної системи оподаткування віртуальних активів за аналогією з країнами Європейського Союзу: фіксована ставка 5% на прибуток від операцій із криптовалютами для фізичних осіб, податок на прибуток компаній – 10% та звільнення криптовалютних транзакцій від ПДВ;

– розробку Закону України «Про Інтернет речей» (IoT), який визначить основні поняття, встановить правові рамки для обробки даних, сертифікації пристроїв, підключення до державних інформаційних систем та регулюватиме відповідальність виробників, операторів та користувачів IoT.

– запровадження обов’язкової сертифікації IoT-пристроїв з метою підтвердження їхньої відповідності стандартам безпеки;

– розробку Закону України «Про штучний інтелект», який визначить офіційні терміни та класифікацію штучного інтелекту, обов’язки та відповідальність розробників, операторів і власників штучного інтелекту, сфери його застосування та механізми державного контролю за його безпекою;

– впровадження державного контролю за штучним інтелектом шляхом утворення Державного агентства з питань штучного інтелекту, яке контролюватиме дотримання ним стандартів безпеки, займатиметься сертифікацією ШІ-рішень високого ризику та здійснюватиме моніторинг випадків зловживання штучного інтелекту;

– оновлення національної Стратегії кібербезпеки України, яка враховуватиме європейські стандарти Закону про кібербезпеку (Cybersecurity Act);

– уточнення визначення кіберзлочинів у Кримінальному кодексі України, встановлення суворіших покарань за такі злочинні дії, як несанкціонований доступ до інформаційних систем, поширення шкідливого програмного забезпечення, викрадення персональних даних;

– розробку Цифрового кодексу України як єдиного кодифікованого акту, який систематизує та унормує правовідносини у сфері використання інформаційних технологій.

Таким чином, оновлення та удосконалення нормативно-правового забезпечення інформаційних технологій є стратегічним завданням для України. Комплексна правова реформа, спрямована на гармонізацію з міжнародними стандартами, забезпечення кібербезпеки та створення ефективного правового поля для інноваційних цифрових технологій, дозволить Україні посилити свій потенціал у сфері інформаційних технологій та стати повноправним учасником світового цифрового ринку.

ВИСНОВКИ

За результатами проведеного дослідження сформульовано наукові положення та отримано результати, які у сукупності розв'язують важливе наукове завдання розроблення теоретичних положень та науково обґрунтованих рекомендацій щодо вдосконалення адміністративно-правового регулювання використання інформаційних технологій в Україні. Найсуттєвішими з них є такі:

1. Дослідження значення інформаційних технологій у сучасному суспільстві вчергове підтверджує, що цифровізація є невід'ємною частиною сучасного світу та охоплює всі сфери життєдіяльності – від побутової сфери до економіки, публічного управління та соціальної комунікації. Їхня інтеграція в суспільні процеси суттєво змінює традиційні механізми взаємодії між державою, бізнесом та громадянами, вимагаючи належного адміністративно-правового регулювання.

На основі існуючих наукових визначень й трактувань проаналізовано поняття «адміністративно-правове регулювання» та «інформаційні технології» з метою визначення основних напрямів їхньої взаємодії.

Здійснено концептуальне визначення поняття «адміністративно-правове регулювання інформаційних технологій» як діяльності органів виконавчої влади, інших суб'єктів публічної адміністрації, яка спрямована на створення, впровадження та застосування адміністративно-правових норм, що забезпечують ефективне функціонування, розвиток і безпеку інформаційних технологій, а також регулювання відносин між суб'єктами у сфері використання інформаційних технологій із метою забезпечення публічного порядку, захисту прав і свобод людини, підтримки економічної стабільності та національної безпеки.

2. Дослідження розвитку становлення адміністративно-правового регулювання використання інформаційних технологій в Україні з метою виокремлення відповідного позитивного історичного досвіду дозволило

виявити кілька важливих етапів, що відображають зміни в суспільних відносинах, технічному прогресі та законодавчій базі.

Перший етап – доінституційний період (до 1991 р.) – характеризувався відсутністю власного національного правового регулювання та використанням інформаційних технологій переважно у військових, промислових і наукових сферах у межах централізованої політики СРСР. На цьому етапі закладалися лише технологічні основи, а правове регулювання було обмежене директивами радянського уряду.

Другий етап – період формування національного законодавства (1991–2010 рр.) – розпочався з проголошення незалежності України та необхідності розробки правової бази для регулювання інформаційних технологій. Було прийнято основоположні закони, що заклали правовий фундамент для подальшого розвитку сфери інформаційних технологій.

Третій етап – сучасний період цифрової трансформації (з 2010 р.) – ознаменувався активним впровадженням цифрових технологій в публічному управлінні, економіці та суспільному житті. Було ухвалено стратегічні законодавчі акти та запущено інноваційні електронні платформи, що стало потужним стимулом для цифрової трансформації України. Було створено фундамент для прозорої, ефективної та доступної системи адміністративних послуг, який сприяє покращенню взаємодії між державою, громадянами та бізнесом.

3. Розвиток інформаційного суспільства та цифрових технологій в Україні зумовив необхідність створення ефективної нормативно-правової бази, що регулює використання інформаційних технологій. В Україні діє значна кількість законодавчих та підзаконних актів, які регулюють цифровізацію суспільства, проте їхня фрагментарність і недостатня узгодженість створюють певні виклики у сфері правозастосування.

З’ясовано, що нормативно-правову основу регулювання використання інформаційних технологій в Україні складають наступні напрями державної

політики: впровадження електронного документообігу, забезпечення захисту персональних даних та забезпечення кібербезпеки.

Нормативно-правове регулювання використання інформаційних технологій в Україні продовжує активно розвиватися, проте для ефективної цифровізації держави необхідно усунути прогалини в законодавстві, гармонізувати його з міжнародними стандартами та забезпечити належний рівень правозастосування.

4. Адміністративно-правове забезпечення правового режиму інформаційної безпеки є важливим елементом національної безпеки України, особливо в умовах цифрової трансформації та гібридної агресії. Інформаційна безпека охоплює захист інформаційного середовища від загроз, забезпечення прав громадян на доступ до достовірної інформації та захист персональних даних. У цьому контексті правовий режим виступає механізмом забезпечення цілісності, конфіденційності та доступності інформації.

Правовий режим інформаційної безпеки ґрунтується на нормах Конституції України, Законах «Про національну безпеку України», «Про інформацію», «Про захист персональних даних», а також стратегічних документах, таких як Стратегії інформаційної та кібербезпеки України. Це забезпечує ефективність управління інформаційними ризиками, координацію між органами державної влади та приватним сектором, а також інтеграцію України у світовий цифровий простір.

З’ясовано, що органам публічної влади особливу увагу слід приділяти гармонізації національного законодавства із міжнародними стандартами та розвитку правових механізмів протидії новим загрозам, включаючи кібератаки, дезінформацію та пропаганду.

Таким чином, адміністративно-правове забезпечення інформаційної безпеки є не лише основою для розвитку інформаційного суспільства та зміцнення довіри громадян до цифрових технологій, але й умовою для збереження національного суверенітету. Вдосконалення правового режиму

інформаційної безпеки є важливим кроком для забезпечення сталого розвитку України у цифрову епоху.

5. Система суб'єктів адміністративно-правового регулювання у сфері інформаційних технологій є багатогранною та охоплює різноманітних учасників, які взаємодіють задля забезпечення розвитку інформаційного суспільства, захисту прав і свобод громадян, а також гарантування національної безпеки. До цієї системи належать органи державної влади, органи місцевого самоврядування, приватний сектор, громадянське суспільство та окремі громадяни.

Державні органи відіграють ключову роль у формуванні, впровадженні та контролі за реалізацією державної політики у сфері інформаційних технологій. Органи місцевого самоврядування забезпечують розвиток локальної інфраструктури та сприяють цифровій трансформації на місцевому рівні. Приватний сектор виступає рушієм технологічного прогресу, забезпечуючи інноваційні рішення, необхідні для цифровізації. Громадянське суспільство та окремі громадяни забезпечують демократичний контроль, прозорість і баланс інтересів між державою, бізнесом і суспільством.

Ефективність адміністративно-правового регулювання у сфері інформаційних технологій забезпечується через чітку взаємодію між суб'єктами на основі правової, організаційної та функціональної основ. Взаємодія спрямована на досягнення прозорості, підзвітності та передбачуваності у процесах регулювання, що відповідає європейським стандартам та сприяє інтеграції України до глобального цифрового простору.

Успішна реалізація адміністративно-правового регулювання у сфері інформаційних технологій залежить від збалансованого залучення всіх суб'єктів, вдосконалення нормативно-правової бази та постійної адаптації до нових викликів цифрової епохи. Це створює передумови для сталого розвитку інформаційного суспільства, захисту прав громадян і забезпечення національної безпеки в умовах глобалізації та цифрової трансформації.

6. Адміністративні процедури відіграють ключову роль у регулюванні інформаційних технологій в Україні, забезпечуючи правову визначеність, ефективність та прозорість процесів публічного адміністрування в цифровій сфері. Вони створюють нормативні механізми, що регулюють діяльність державних органів, приватного сектору та громадянського суспільства у сфері інформаційних технологій.

Дослідження показало, що адміністративні процедури в сфері інформаційних технологій мають складну структуру та охоплюють управлінські, реєстраційні, організаційно-кадрові, дозвільно-ліцензійні, контрольні та інтернаціоналізаційні аспекти. Цей комплексний підхід дозволяє ефективно впроваджувати державну політику цифрової трансформації, сприяти інноваціям та захисту інформаційного простору.

Цифровізація адміністративних процедур, яка активно розвивається в Україні, сприяє підвищенню ефективності публічного управління, мінімізації бюрократії та корупційних ризиків, покращенню якості надання адміністративних послуг. Впровадження електронного урядування та цифрових платформ демонструє прагнення держави до створення зручного та доступного правового середовища у сфері інформаційних технологій.

Таким чином, адміністративні процедури у сфері інформаційних технологій є важливим елементом сучасного публічного управління. А їх ефективне впровадження та вдосконалення сприяє розвитку інформаційного суспільства, посиленню демократичних принципів управління та інтеграції України у глобальний цифровий простір.

7. Цифрова трансформація відкриває нові можливості для держави та суспільства, але водночас породжує численні виклики у сфері правового регулювання використання інформаційних технологій. Основна проблема правового регулювання інформаційних технологій в Україні в умовах цифрової трансформації полягає в тому, що розвиток технологій значно випереджає темпи законодавчого регулювання, створюючи правові

прогалини та невизначеність правового статусу багатьох інформаційно-технологічних явищ.

В Україні правова система залишається консервативною, що ускладнює адаптацію до швидких технологічних змін. Ситуація з віртуальними активами яскраво демонструє цю проблему: попри зростаючу популярність цифрових активів, їх правовий статус залишається невизначеним на державному рівні.

Ще одним викликом для України є правове регулювання Інтернету речей та штучного інтелекту. Визначення статусу та відповідальності за рішення, ухвалені автоматизованими алгоритмами, залишається складним питанням для законодавця.

В умовах повномасштабної війни особливої актуальності набуває проблема забезпечення кібербезпеки. Масовані кібератаки та дестабілізаційні інформаційні операції з боку РФ вимагають вдосконалення державної політики у сфері кіберзахисту. Україна потребує оновлення Стратегії кібербезпеки, забезпечення захисту критичної інфраструктури та підвищення рівня цифрової грамотності громадян.

Таким чином, ефективне правове регулювання інформаційних технологій потребує адаптації національного законодавства до міжнародних стандартів, прискорення процесів правотворення та впровадження сучасних механізмів контролю та безпеки. Лише за таких умов Україна зможе ефективно використовувати цифрові технології, мінімізуючи ризики та забезпечуючи правовий захист громадян та бізнесу.

8. В умовах цифрової трансформації України запозичення та адаптація зарубіжного досвіду у сфері правового регулювання інформаційних технологій є важливим чинником розвитку. Досвід розвинених країн демонструє ефективні підходи до регулювання персональних даних, кібербезпеки, електронного урядування та використання штучного інтелекту.

Зокрема, Європейський Союз має комплексне правове регулювання інформаційних технологій, представлене GDPR (захист персональних даних),

NIS2 (кібербезпека), MiCA (регулювання криптоактивів) та ініціативами цифрового урядування. Естонія є взірцем успішної цифровізації публічного управління, демонструючи ефективні рішення для розвитку електронного уряду та цифрової ідентифікації.

США застосовують гнучкий підхід, поєднуючи саморегулювання технологічних компаній із державним наглядом, що сприяє інноваціям й активному розвитку IT-сфери. Сінгапур активно впроваджує етичні стандарти штучного інтелекту, Південна Корея, завдяки грамотному впровадженню у національне законодавство Інтернету речей, є лідером у розбудові «розумних міст», а Китай успішно інтегрує штучний інтелект у систему правосуддя, що підвищує ефективність судочинства.

Україна, орієнтуючись на європейські та світові стандарти, має адаптувати своє законодавство до міжнародних вимог, зокрема у сфері захисту персональних даних, цифрової ідентифікації та кібербезпеки. Водночас важливо враховувати національні особливості, рівень цифрової грамотності населення та ефективність державних інституцій.

Отже, використання зарубіжного досвіду має стати ключовим інструментом для вдосконалення адміністративно-правового регулювання використання інформаційних технологій в Україні. Це дозволить забезпечити якість та прозорість публічного адміністрування, підвищити рівень довіри громадян до цифрових сервісів та інтегрувати країну у міжнародний цифровий простір.

9. До перспективних напрямів удосконалення нормативно-правового забезпечення використання інформаційних технологій в Україні слід віднести:

– повне виконання Угоди про асоціацію між Україною та ЄС, що передбачає у тому числі імплементацію в національне законодавство та юридичну практику європейських правил використання інформаційних технологій, а також форм і способів їх адміністрування з боку органів публічної адміністрації;

– повне впровадження в національне законодавство Загального регламенту Європейського Союзу про захист даних (GDPR) для забезпечення надійного контролю та захисту персональних даних громадян та спрощення регуляторних процедур для бізнесу;

– внесення змін до Закону України «Про віртуальні активи» шляхом адаптування положень цього Закону до стандартів Регламенту про ринки криптоактивів (Markets in Crypto-Assets; MiCA);

– запровадження спрощеної системи оподаткування віртуальних активів за аналогією з країнами Європейського Союзу: фіксована ставка 5% на прибуток від операцій із криптовалютами для фізичних осіб, податок на прибуток компаній – 10% та звільнення криптовалютних транзакцій від ПДВ;

– розробку Закону України «Про Інтернет речей» (IoT), який визначить основні поняття, встановить правові рамки для обробки даних, сертифікації пристроїв, підключення до державних інформаційних систем та регулюватиме відповідальність виробників, операторів та користувачів IoT.

– запровадження обов’язкової сертифікації IoT-пристроїв з метою підтвердження їхньої відповідності стандартам безпеки;

– розробку Закону України «Про штучний інтелект», який визначить офіційні терміни та класифікацію штучного інтелекту, обов’язки та відповідальність розробників, операторів і власників штучного інтелекту, сфери його застосування та механізми державного контролю за його безпекою;

– впровадження державного контролю за штучним інтелектом шляхом утворення Державного агентства з питань штучного інтелекту, яке контролюватиме дотримання ним стандартів безпеки, займатиметься сертифікацією ШІ-рішень високого ризику та здійснюватиме моніторинг випадків зловживання штучного інтелекту;

– оновлення національної Стратегії кібербезпеки України, яка враховуватиме європейські стандарти Закону про кібербезпеку (Cybersecurity Act);

– уточнення визначення кіберзлочинів у Кримінальному кодексі України, встановлення суворіших покарань за такі злочинні дії, як несанкціонований доступ до інформаційних систем, поширення шкідливого програмного забезпечення, викрадення персональних даних;

– розробку Цифрового кодексу України як єдиного кодифікованого акту, який систематизує та унормує правовідносини у сфері використання інформаційних технологій.

Таким чином, оновлення та удосконалення нормативно-правового забезпечення інформаційних технологій є стратегічним завданням для України. Комплексна правова реформа, спрямована на гармонізацію з міжнародними стандартами, забезпечення кібербезпеки та створення ефективного правового поля для інноваційних цифрових технологій, дозволить Україні посилити свій потенціал у сфері інформаційних технологій та стати повноправним учасником світового цифрового ринку.

Наведений перелік актуальних напрямів удосконалення адміністративно-правового регулювання використання інформаційних технологій в Україні не є вичерпним, адже в умовах євроінтеграції перед громадянами України та органами публічної адміністрації з’являються нові виклики, які потребуватимуть подальшої системної наукової роботи.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Mayer O. Deutsches Verwaltungsrecht. Leipzig: Duncker & Humblot, 1895–1896. Vol. 2. P. 15–23.

2. Авер'янов В. Б., Цвєтков В. В., Шаповал В. М., Кисіль С. П., Кривенко Л. Т. Державне управління: теорія і практика. К.: Юрінком Інтер, 1998. 431 с. [Електронний ресурс]. Режим доступу: http://ukrkniga.org.ua/ukrkniga-text/692/38/.

3. Галунько В. В., Єщук О. М. Поняття та зміст адміністративно-правового регулювання // Actual Problems of Corruption Prevention and Counteraction. 2011. [Електронний ресурс]. Режим доступу: http://www.law-property.in.ua.

4. Теорія держави та права: навч. посіб. / Є. В. Білозьоров, В. П. Власенко, О. Б. Горова, А. М. Завальний, Н. В. Заяць та ін.; за заг. ред. С. Д. Гусарєва, О. Д. Тихомирова. Київ: НАВС, Освіта України, 2017. 320 с.

5. Єсімов С. С., Перепелиця А. В. Адміністративно-правове регулювання внутрішньовідомчого контролю в органах Національної поліції // Соціально-правові студії. 2021. Вип. 2 (12). С. 72–78. DOI: 10.32518/2617-4162-2021-2-72-78. URL: https://sls-journal.com.ua/web/uploads/pdf/S&LS_2021_Vol.%204,%20No.%202_72-78.pdf

6. Загальна теорія держави і права: підручник / М. В. Цвік, О. В. Петришин, Л. В. Авраменко та ін.; за ред. М. В. Цвіка, О. В. Петришина. Харків: Право, 2009. 584 с.

7. Рабінович П. М. Теорія держави та права: навч. посіб. Вид. 9-те зі змінами. Львів: Край, 2007. 192 с.

8. Теорія держави і права: підручник / за ред. Ю. О. Ведєрнікова. 3-тє вид., перероб. і доп. Дніпро: ДДУВС, Ліра ЛТД, 2016. 480 с.

9. Авер'янов В. Б. Реформування українського адміністративного права: необхідність переосмислення теоретичних постулатів // Актуальні проблеми держави і права. 2003. Вип. 19. С. 6–12.

10. Шопіна І. М. Адміністративно-правове забезпечення та адміністративно-правове регулювання: співвідношення понять // Аналітично-порівняльне правознавство. 2023. № 06. С.550–554. DOI: https://doi.org/10.24144/2788-6018.2023.06.96

11. Шопіна І. М. Феномен адміністративно-правового забезпечення в адміністративному праві України // Наука і правоохорона. 2018. № 4. С. 67–71.

12. Про Національну програму інформатизації: Закон України від 04.02.1998 № 74/98-ВР // Відомості Верховної Ради України (ВВР). 1998. № 27-28. Ст. 181.

13. Угода про правовий режим інформаційних ресурсів Прикордонних військ держав-учасниць СНД: Міжнародний документ від 25.11.1998 [Електронний ресурс]. Режим доступу: http://zakon4.rada.gov.ua/laws/show/997_344.

14. ISO/IEC 38500:2015 «Управління інформаційними технологіями в організаціях» (Governance of IT for the organization): Міжнародний стандарт [Електронний ресурс]. Режим доступу: https://www.iso.org/obp/ui/#iso:std:iso-iec:38500:ed-2:v1:en.

15. Триняк В. Ю. Інформаційна безпека як соціокультурний феномен (соціально-філософський аналіз): дис. ... канд. філос. наук. Д., 2009. 189 с. + автореф. [Електронний ресурс]. Режим доступу: library.dsu.dp.ua/0610.rtf.

16. Селезньова О. М. Роль та переваги використання інформаційних технологій в навчальному процесі (на прикладі навчальної дисципліни "Інформаційне право") // Інформація і право. 2012. № 3. С. 153–158. [Електронний ресурс]. Режим доступу: http://ippi.org.ua/seleznova-om-rol-ta-perevagy-vykorystannya-informatsijnykh-tekhnologij-v-navchalnomu-protsesi-na-pry.

17. Побережна Н. О. Дидактичні умови впровадження інформаційних технологій у навчальний процес вищого навчального закладу: автореф. дис. ... канд. пед. наук. Кривий Ріг: Б. в., 2010. 20 с. [Електронний ресурс]. Режим доступу: http://liber.onu.edu.ua/opacunicode/index.php?url=/notices/index/IdNotice:368638/Source:default.

18. Юдкова, К. В. Особливості визначення поняття «Інформаційні технології» // Інформація і право. – 2015. – № 1(13). – С.18-21.

19. Саушкін Б. П. Основи технології. Розділ 8 [Електронний ресурс]. Режим доступу: http://chemanalytica.com/book/novyy_spravochnik_khimika_i_tekhnologa/12_obshchie_svedeniya/6289.

20. Інформаційні технології. Захист інформації [Електронний ресурс]. Режим доступу: http://lab314.brsu.by/sil/sil_IT/sil_IT/sil_theory/sil_t1.htm.

21. Гапоненко А. Л., Орлова Т. М. Управління знаннями. Як перетворити знання у капітал [Електронний ресурс]. Режим доступу: http://qame.ru/book/management/upravlenie_znaniyami_kak_prevratit_znaniya_v_kapital.pdf.

22. Harvey L. Poppel, Bernard Goldstein. Information Technology: The Trillion-Dollar Opportunity. McGraw-Hill, 1987 [Електронний ресурс]. Режим доступу: http://books.google.com.ua/books/about/Information_technology.html?id=xPyiWvji2lAC&redir_esc=y.

23. Юдкова К. В. Інформаційні технології у правовій сфері України: основні підходи до визначення // Science and Education a New Dimension. 2021. № 9(97). С. 45–50. URL: https://www.seanewdim.com/wp-content/uploads/2021/03/Information-technologies-in-the-legal-sphere-of-Ukraine-basic-approaches-to-the-definition-K.-V.-Yudkova.pdf

24. Дорогих С. О. Правові та організаційні основи інформаційної діяльності законодавчої гілки влади в Україні: автореф. дис. ... канд. юрид. наук: 12.00.07. Київ: НДІ інформатики і права Нац. акад. прав. наук України, 2017. 19 с. [Електронний ресурс]. Режим доступу: http://ippi.org.ua/sites/default/files/dis_dorogih.pdf.

25. Єсімов С. С. Використання інформаційних технологій як предмет адміністративно-правового регулювання / С. С. Єсімов // Навчально-науковий інститут права та психології Національного університету "Львівська політехніка". – 2015. – С. 24–29.

26. Бурило Ю. П. Організаційно-правові питання державного управління в інформаційній сфері: автореф. дис. ... канд. юрид. наук: 12.00.07 "Адміністративне право і процес; фінансове право; інформаційне право" / Ю. П. Бурило. – Київ, 2008. – 18 с.

27. Глушков В. М. Основи електронного урядування / В. М. Глушков. Київ: Наукова думка, 1985. 320 с.

28. Внеочередной XXI съезд Коммунистической партии Советского Союза (27 января — 1 февраля 1959 г.): стенограф. отчет. М.: Госполитиздат, 1959. Т. 2. 615 с.

29. XXIII съезд Коммунистической партии Советского Союза (29 марта — 8 апреля 1966 г.): стенограф. отчет. М.: Госполитиздат, 1966. Т. 2. 672 с.

30. XXIV съезд Коммунистической партии Советского Союза (30 марта — 9 апреля 1971 г.): стенограф. отчет. М.: Госполитиздат, 1971. Т. 2. 592 с.

31. Материалы XXVII съезда Коммунистической партии Советского Союза. М.: Политиздат, 1986. 352 с.

32. Про створення республіканської телевізійно-комп'ютерної системи масового розповсюдження інформації. Постанова Президії Академії наук Української РСР № 63 від 01.03.1991 р.

33. Пилипчук В. Г. Актуальні проблеми становлення і розвитку правової науки в інформаційній сфері / В. Г. Пилипчук // Інформація і право. 2012. № 1(4). С. 15–22. URL: https://ippi.org.ua/sites/default/files/maket_ot_20.11.19._1.pdf

34. Конституція України: Закон України від 28.06.96 р. № 254к/96-ВР. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text.

35. Про державну політику інформатизації України: Указ Президента України від 31.05.1993 р. Там само. 1993. № 186/93 [Електронний ресурс]. Режим доступу: http://zakon.rada.gov.ua/.

36. Про утворення Національного агентства з питань інформатизації: Указ Президента України від 13.03.1995 р. Там само. 1995. № 206/95 [Електронний ресурс]. Режим доступу: http://zakon.rada.gov.ua/.

37. Про вдосконалення державного управління інформаційною сферою: Указ Президента України від 16.09.1998 р. Там само. 1998. № 1033/98 [Електронний ресурс]. Режим доступу: http://zakon.rada.gov.ua/.

38. Про Положення про Державний комітет зв'язку та інформатизації України: Указ Президента України від 03.06.1999 р. / Верховна Рада України. К.: Відомості Верховної Ради України (ВВР), 1999. № 601/99 [Електронний ресурс]. Режим доступу: http://zakon.rada.gov.ua/.

39. Про Положення про Міністерство транспорту та зв'язку України: Указ Президента України від 27.08.2004 р. Там само. 2004. № 1009/2004 [Електронний ресурс]. Режим доступу: http://zakon.rada.gov.ua/.

40. Про Положення про Міністерство транспорту та зв'язку України: Постанова Кабінету Міністрів України від 26.03.2008 р. Там само. 2008. № 272 [Електронний ресурс]. Режим доступу: http://zakon.rada.gov.ua/.

41. Про утворення Державного комітету України з питань науки, інновацій та інформатизації: Постанова Кабінету Міністрів України від 05.07.2010 р. Там само. 2010. № 548 [Електронний ресурс]. Режим доступу: http://zakon.rada.gov.ua/.

42. Про оптимізацію системи центральних органів виконавчої влади: Указ Президента України від 09.12.2010 р. Президент України, офіційне Інтернет-представництво, 2010. № 1085/2010 [Електронний ресурс]. Режим доступу: http://www.president.gov.ua/documents/12584.html.

43. Деякі питання діяльності Державного комітету з питань науки, інновацій та інформатизації: Постанова Кабінету Міністрів України від 21.07.2010 р. № 675 [Електронний ресурс]. Режим доступу: http://zakon.rada.gov.ua/.

44. Закон України «Про інформацію» від 02.10.1992 № 2657-XII. URL: https://zakon.rada.gov.ua/laws/show/2657-12

45. Закон України «Про науково-технічну інформацію» від 25.06.1993 № 3322-XII. URL: https://zakon.rada.gov.ua/laws/show/3322-12

46. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 05 липня 1994 року № 80/94-ВР (Редакція від 31.12.2023). URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text

47. Про Концепцію Національної програми інформатизації: Закон України від 04.02.1998 р. № 75/98-ВР // Відомості Верховної Ради України. – 1998. – № 27–28. – Ст. 182. – [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/75/98-%D0%B2%D1%80#Text

48. Про електронний цифровий підпис: Закон України від 22.05.2003 р. № 852-IV (втратив чинність на підставі Закону № 2155-VIII від 05.10.2017 р.) // Відомості Верховної Ради України. – 2003. – № 36. – Ст. 276. – [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/852-15#Text

49. Про внесення змін до Закону України «Про захист інформації в автоматизованих системах»: Закон України від 31 травня 2005 р. № 2594-IV. Дата набуття чинності: 23.06.2005. URL: https://zakon.rada.gov.ua/laws/show/2594-15#Text

50. Про схвалення Стратегії розвитку інформаційного суспільства в Україні: Розпорядження Кабінету Міністрів України від 15.05.2013 р. № 386-р // Офіційний вісник України. – 2013. – № [вказати номер випуску]. – [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/386-2013-%D1%80#Text

51. Про затвердження Положення про Державне агентство з питань електронного урядування України: Постанова Кабінету Міністрів України від 01.10.2014 р. № 492 (втратила чинність на підставі Постанови КМ № 645 від 27.06.2023) // Офіційний вісник України. – 2014. – № [вказати номер випуску]. – [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/492-2014-%D0%BF#Text

52. У Мінекономрозвитку презентували проєкт Цифрової адженди України – 2020 [Електронний ресурс] // Міністерство економічного розвитку і торгівлі України. – Режим доступу: https://me.gov.ua/News/Detail?lang=uk-UA&id=bd512af7-5e94-430a-9842-452d843a5c1a&title=UMinekonomrozvitkuPrezentuvaliProekttsifrovoiAdzhendiUkraini2020-?nynhfbclgtkeplwz

53. Кабінет Міністрів України. Про схвалення Концепції розвитку цифрової економіки та суспільства України на 2018–2020 роки та затвердження плану заходів щодо її реалізації: Розпорядження від 17 січня 2018 р. № 67-р. – Київ, 2018. – Режим доступу: https://zakon.rada.gov.ua/laws/show/67-2018-%D1%80#Text

54. Кабінет Міністрів України. Питання Міністерства цифрової трансформації: Постанова від 18 вересня 2019 р. № 856. – Київ, 2019. – Режим доступу: https://zakon.rada.gov.ua/laws/show/856-2019-%D0%BF#Text

55. Асанова Л. Місце електронного документообігу в загальній системі діловодства // Адміністративне право і процес. 2021. № 3. С. 156–160. DOI: https://doi.org/10.32849/2663-5313/2021.3.24.

56. Про заходи щодо розвитку національної складової глобальної інформаційної мережі Інтернет та забезпечення широкого доступу до цієї мережі в Україні: Указ Президента України від 31 липня 2000 року № 928/2000. URL: https://zakon.rada.gov.ua/laws/show/928/2000#Text

57. Про порядок розміщення інформації про діяльність органів виконавчої влади в мережі Інтернет: Постанова Кабінету Міністрів України від 04 січня 2002 р. № 3 (Редакція від 25.07.2023). URL: https://zakon.rada.gov.ua/laws/show/3-2002-%D0%BF#Text

58. Петрович В. Застосування систем електронного документування в органах державного управління // Політологічні читання імені професора Богдана Яроша: зб. наук. пр. / за заг. ред. В. І. Бортнікова, Я. Б. Яроша. Луцьк-с. Світязь, 16–17 квіт. 2021 р. Луцьк: Вежа-Друк, 2021. Вип. 10. С. 96–100.

59. Лаба О. В. До питання визначення місця електронного діловодства у структурі традиційного діловодства // Соціум. Документ. Комунікація. 2020. Вип. 8/2. Переяслав-Хмельницький: ФОП Домбровська Я. М., 2020. С. 137–156.

60. Про Національну програму інформатизації: Закон України від 01 грудня 2022 року № 2807-IX (Редакція від 01.12.2022). URL: https://zakon.rada.gov.ua/laws/show/2807-20#Text

61. Про електронні документи та електронний документообіг: Закон України від 22 травня 2003 р. № 851-IV (Редакція від 31.12.2023). URL: https://zakon.rada.gov.ua/laws/show/851-15#Text

62. Про електронну ідентифікацію та електронні довірчі послуги: Закон України від 5 жовтня 2017 р. № 2155-VIII // Відомості Верховної Ради України (ВВР), 2017, № 45, ст. 403. URL: https://zakon.rada.gov.ua/laws/show/2155-19#Text.

63. Про електронну комерцію: Закон України від 03.09.2015 р. № 675-VIII (Редакція від 01.01.2024). URL: https://zakon.rada.gov.ua/laws/show/675-19#Text

64. Про обов’язковий примірник документів: Закон України від 09 квітня 1999 року № 595-XIV (Редакція від 31.03.2023). URL: https://zakon.rada.gov.ua/laws/show/595-14#Text

65. Про електронні комунікації: Закон України від 16 грудня 2020 року № 1089-IX (Редакція від 01.01.2024). URL: https://zakon.rada.gov.ua/laws/show/1089-20#Text

66. Про Національну систему конфіденційного зв’язку: Закон України від 10 січня 2002 року № 2919-III (Редакція від 01.01.2022). URL: https://zakon.rada.gov.ua/laws/show/2919-14#Text

67. Про заходи щодо створення електронної інформаційної системи «Електронний уряд»: Постанова Кабінету Міністрів України від 24 лютого 2003 р. № 208. URL: https://zakon.rada.gov.ua/laws/show/208-2003-%D0%BF#Text

68. Деякі питання документування управлінської діяльності: Постанова Кабінету Міністрів України від 17 січня 2018 р. № 55 (Редакція від 01.12.2022). URL: https://zakon.rada.gov.ua/laws/show/55-2018-%D0%BF#Text

69. Петрович В., Надольська В., Чарікова І. Запровадження системи електронного документообігу в Україні: особливості законодавчого регулювання // Актуальні питання гуманітарних наук. 2024. Вип. 72, т. 3. С. 10–16. URL: https://doi.org/10.24919/2308-4863/72-3-2

70. Закон України «Про захист персональних даних» від 01.06.2010 № 2297-VI // Відомості Верховної Ради України. – 2010. – № 34. – Ст. 481. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text.

71. Кримінальний кодекс України: Закон України від 5 квітня 2001 р. № 2341-III // Відомості Верховної Ради України (ВВР). – 2001. – № 25-26. – Ст. 131. – Режим доступу: https://zakon.rada.gov.ua/laws/show/2341-14#Text

72. Цивільний кодекс України: Закон України від 16 січня 2003 р. № 435-IV // Відомості Верховної Ради України (ВВР). – 2003. – №№ 40-44. – Ст. 356. – Режим доступу: https://zakon.rada.gov.ua/laws/show/435-15#Text

73. Про адміністративні правопорушення: Кодекс України від 7 грудня 1984 р. № 80731-10. Дата оновлення: ..2024. URL: https://zakon.rada.gov.ua/laws/show/80731-10#Text

74. Регламент Європейського Парламенту і Ради (ЄС) 216/679 від 27.04.2016 р. про захист фізичних осіб при обробці персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних (GDPR). URL: https://ips.ligazakon.net/document/MU16144.

75. Лист Уповноваженого Верховної Ради України з прав людини від 03.03.2014 № 2/9-227067.14-1/НД-129. URL: https://zakon.rada.gov.ua/laws/show/v7067715-14#Text.

76. Бліхар М. М. Організаційно-правовий механізм захисту персональних даних // Науковий вісник Ужгородського національного університету. Серія: Право. 2023. Вип. 77, ч. 2. С. 31–36. DOI: https://doi.org/10.24144/2307-3322.2023.77.2.4.

77. Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки: Закон України від 09.01.2007 № 537-V // Відомості Верховної Ради України (ВВР), 2007. № 12, ст. 102. URL: https://zakon.rada.gov.ua/laws/show/537-16#Text

78. ISO/IEC 27032:2012 Information technology – Security techniques – Guidelines for cyber security. URL: www.iso.org/standard/44375.html

79. ДСТУ ISO/IEC 27032:2016 (ISO/IEC 27032:2012, IDT) Інформаційні технології. Методи захисту. Настанови щодо кібербезпеки (ISO/IEC 27032:2012, IDT). URL: http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=69128

80. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII // Відомості Верховної Ради (ВВР), 2017. № 45, ст. 403. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text

81. Про національну поліцію: Закон України від 02.07.2015 № 580-VIII // Відомості Верховної Ради (ВВР), 2015. № 40-41, ст. 379. URL: https://zakon.rada.gov.ua/laws/show/580-19#Text

82. Про утворення територіального органу Національної поліції: Постанова Кабінету Міністрів України від 13.10.2015 № 831. URL: https://zakon.rada.gov.ua/laws/show/831-2015-%D0%BF#Text

83. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року "Про стратегію кібербезпеки України": Указ Президента України від 15.03.2016 № 96/2016. URL: https://zakon.rada.gov.ua/laws/show/96/2016#Text

84. Веселова Л. Ю. Адміністративно-правові основи кібербезпеки в умовах гібридної війни: дис. … д-ра юрид. наук: 12.00.07. Одеса, 2021. 500 с.

85. Третяк Ю. І. Нормативно-правове регулювання кібербезпеки в Україні [Електронний ресурс] / Ю. І. Третяк. – Режим доступу: https://revolution.allbest.ru/law/01501192_0.html

86. Діордіца І. В. Поняття і зміст кіберзагроз на сучасному етапі // Підприємство, господарство і право. 2017. № 4. С. 99–107.

87. Великий енциклопедичний юридичний словник / за ред. акад. НАН України Ю. С. Шемшученка. 2-ге вид., перер. і доп. Київ: Вид-во "Юридична думка", 2021. 1020 с.

88. Закон України "Про національну безпеку України" [Електронний ресурс]. URL: https://zakon.rada.gov.ua/laws/show/2469-19#n355.

89. Біленчук П. Д. та ін. Правові засади інформаційної безпеки України: монографія / за ред. П. Д. Біленчука. Харків, 2018. 289 с.

90. Войціховський А. В. Інформаційна безпека як складова системи національної безпеки (міжнародний і зарубіжний досвід) // Вісник Харківського національного університету імені В. Н. Каразіна. Серія "Право". 2020. Вип. 29. С. 281–288. DOI: 10.26565/2075-1834-2020-29-38.

91. Нашинець-Наумова А. Ю. Інформаційна безпека: питання правового регулювання: монографія. Київ: "Гельветика", 2017. 168 с.

92. Резолюція A/RES/53/70 ГА ООН "Досягнення в сфері інформатизації і телекомунікації в контексті міжнародної безпеки" [Електронний ресурс]. URL: https://documents.un.org/doc/undoc/gen/n99/760/05/pdf/n9976005.pdf.

93. Резолюція A/RES/54/49 ГА ООН "Досягнення в сфері інформатизації і телекомунікації в контексті міжнародної безпеки" [Електронний ресурс]. URL: https://undocs.org/ru/A/RES/54/49.

94. Фролова О. М. Роль ООН в системі міжнародної інформаційної безпеки [Електронний ресурс]. URL: http://journals.iir.kiev.ua/index.php/pol_n/article/viewFile/3468/3140.

95. Network and information security: proposal for a European policy approach [Електронний ресурс]. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52001DC0298&from=EN.

96. Council framework decision 2005/222/JHA on attacks against information systems [Електронний ресурс]. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32005F0222.

97. Towards a general policy on the fight against cyber crime [Електронний ресурс]. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM%3Al14560.

98. Communication from the Commission on Critical Information Infrastructure Protection "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience" [Електронний ресурс]. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52009DC0149.

99. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace [Електронний ресурс]. URL: https://ec.europa.eu/digital-single-market/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security.

100. Concerning measures for a high common level of security of network and information systems across the Union [Електронний ресурс]. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN.

101. Resilience, Deterrence and Defence: Building strong cybersecurity for the EU [Електронний ресурс]. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017JC0450&from=EN.

102. European Union Agency for Network and Information Security [Електронний ресурс]. URL: https://www.enisa.europa.eu/about-enisa.

103. Гассельбах К., Завгородня І. Європейський центр боротьби з кіберзлочинністю починає роботу [Електронний ресурс]. URL: http://p.dw.com/p/17HRW.

104. Бородакий Ю. В., Добродеев А. Ю., Бутусов І. В. Кібербезпека як основний фактор національної і міжнародної безпеки XXI століття [Електронний ресурс]. URL: https://cyberleninka.ru/article/n/kiberbezopasnost-kak-osnovnoy-faktor-natsionalnoy-i-mezhdunarodnoy-bezopasnosti-hh-veka-chast-1/viewer.

105. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року "Про Стратегію інформаційної безпеки" // Офіційний вісник України. URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text.

106. Указ Президента України від 14 вересня 2020 року № 392/2020 "Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року "Про Стратегію національної безпеки України". URL: https://zakon.rada.gov.ua/laws/show/392/2020#Text.

107. Про введення воєнного стану в Україні. URL: https://www.president.gov.ua/documents/642022-41397

108. Про внесення змін до Кримінального та Кримінального процесуального кодексів України щодо забезпечення протидії несанкціонованому поширенню інформації про направлення, переміщення зброї, озброєння та бойових припасів в Україну, рух, переміщення або розміщення Збройних Сил України чи інших утворених відповідно до законів України військових формувань, вчиненому в умовах воєнного або надзвичайного стану. URL: https://zakon.rada.gov.ua/laws/show/2160-20#n10

109. Про внесення змін до Кримінального процесуального кодексу України та Закону України "Про електронні комунікації" щодо підвищення ефективності досудового розслідування "за гарячими слідами" та протидії кібератакам. URL: https://zakon.rada.gov.ua/laws/show/2137-20#Text

110. Про внесення змін до деяких законодавчих актів України щодо посилення кримінальної відповідальності за виготовлення та поширення забороненої інформаційної продукції: Закон України. URL: https://zakon.rada.gov.ua/laws/show/2110-20#Text

111. Котерлін І. Б. Інформаційна безпека в умовах воєнного стану у аспекті забезпечення інформаційних прав та свобод // Актуальні проблеми вітчизняної юриспруденції. 2022. Вип. 1. С. 73–78.

112. Пьянов Н. А. Консультации по теории государства и права: правовое регулирование и его механизм // Сибирский юридический вестник. 2003. № 2. URL: http://window.edu.ru/resource/647/24647/files/1124952.pdf.

113. Смородинський В. С. Роль держави у правовому регулюванні // Державне будівництво та місцеве самоврядування. 2013. № 25. С. 17–28.

114. Про інформацію: Закон України від 02.10.1992 № 2657-XII. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text.

115. Державна стратегія регіонального розвитку на 2021-2027 роки: постанова Кабінету Міністрів України від 5.06.2020 № 695. URL: https://www.kmu.gov.ua/npas/pro-zatverdzhennyaderzhavnoyi-strategiyi-regionalnogo-rozvitku-na-20212027-t50820.

116. Кабінет Міністрів України. Деякі питання реформування державного управління України: розпорядження від 21.07.2021 № 831-р. Офіційний вісник України, 2021. URL: https://zakon.rada.gov.ua/laws/show/831-2021-р.

117. Кабінет Міністрів України. Про схвалення Концепції розвитку електронного урядування в Україні: розпорядження від 20.09.2017 № 649-р. Офіційний вісник України, 2017. URL: https://zakon.rada.gov.ua/laws/show/649-2017-р.

118. Верховна Рада України. Про центральні органи виконавчої влади: Закон України від 17.03.2011 № 3166-VI // Відомості Верховної Ради України (ВВР), 2011. № 38, ст. 385. URL: https://zakon.rada.gov.ua/laws/show/3166-17.

119. Верховна Рада України. Про місцеві державні адміністрації: Закон України від 09.04.1999 № 586-XIV // Відомості Верховної Ради України (ВВР), 1999. № 20-21, ст. 190. URL: https://zakon.rada.gov.ua/laws/show/586-14.

120. Про адміністративну процедуру: Закон України від 17.02.2022 № 2073-IX // Відомості Верховної Ради України, 2023. № 15. Ст. 50. URL: https://zakon.rada.gov.ua/laws/show/2073-20#Text.

121. Офіційний вебпортал "Дія" [Електронний ресурс]. URL: https://diia.gov.ua/.

122. Про План реалізації Стратегії кібербезпеки України: Рішення Ради національної безпеки і оборони України від 30 грудня 2021 р. [Електронний ресурс] / Введено в дію Указом Президента України від 1 лютого 2022 р. № 37/2022. URL: https://zakon.rada.gov.ua/laws/show/n0087525-21#Text.

123. Про Державну службу спеціального зв’язку та захисту інформації України: Закон України від 23 лютого 2006 р. № 3475-IV // Відомості Верховної Ради України (ВВР). – 2006. – № 30. – Ст. 258. – Режим доступу: https://zakon.rada.gov.ua/laws/show/3475-15#Text

124. Кабінет Міністрів України. Про затвердження Положення про Адміністрацію Державної служби спеціального зв'язку та захисту інформації України: Постанова від 3 вересня 2014 р. № 411. – Київ, 2014. – Режим доступу: https://zakon.rada.gov.ua/laws/show/411-2014-%D0%BF#Text

125. Марченко В. В. Електронне урядування в органах виконавчої влади: адміністративно-правові засади: монографія. Харків: Панов, 2016. 444 с.

126. Бойко І. В. Адміністративна процедура – поняття, ознаки і види // Державне будівництво та місцеве самоврядування: зб. наук. пр. / ред. кол.: С. Г. Серьогіна та ін. – Х.: Право, 2017. – Вип. 33. – С. 113–122.

127. Бевзенко В. М. Деякі теоретичні міркування щодо адміністративних процесуальних і процедурних категорій у вітчизняній адміністративноправовій та адміністративно-процесуальній науці // Вісник Вищого адміністративного суду України. – 2011. – № 3. – С. 56–62.

128. Юрійчук І. В. Правове поняття адміністративних процедур / Підприємництво, господарство і право // Адміністративне право і процес. – 2018. – № 5. – С. 151–155

129. Фролов Ю. М. Адміністративні процедури: зміст та особливості // Форум права. – 2013. – № 3. – С. 692–698.

130. Басова Ю. Ю. Теоретико-правовий аналіз поняття «адміністративна процедура» // Науковий вісник Міжнародного гуманітарного університету. – 2014. – № 11. – Т. 1. – С. 121–123. – (Серія: Юриспруденція).

131. Братель С. Г. Природа та особливості адміністративних процедур // Visegrad Journal on Human Rights. – 2014. – № 2. – С. 99–103.

132. Буханевич О. М. Поняття та сутність процедури надання адміністративних послуг // Право і суспільство. – 2015. – № 5. – С. 126–131.

133. Губерська Н. Л. Адміністративні процедури у сфері вищої освіти: автореф. дис. ... д-ра юрид. наук / Н. Л. Губерська; Національний юридичний університет ім. Ярослава Мудрого. – Харків, 2016. – 34 с.

134. Левченко О. В. Адміністративна процедура як правова форма надання адміністративних послуг: поняття, ознаки та співвідношення із суміжними правовими поняттями // Прикарпатський юридичний вісник. – 2015. – Вип. 2(8). – С. 106–111.

135. Луцик А. М. Адміністративні процедури у сфері оподаткування в Україні: автореф. дис. ... канд. юрид. наук / А. М. Луцик; Національний авіаційний університет. – Київ, 2015. – 22 с.

136. Адміністративне право України: навч. посіб. / [В. В. Галунько, В. І. Курило, С. О. Короєд, О. Ю. Дрозд, І. В. Гиренко, О. М. Єщук, І. М. Риженко, А. А. Іванищук, Р. Д. Саунін, І. М. Ямкова]; за ред. проф. В. В. Галунька. – Херсон: Грінь Д. С., 2015. – Т. 1. Загальне адміністративне право. – 272 с.

137. Авер'янов В. Б. Значення адміністративних процедур у реформуванні адміністративного права // Часопис Київського університету права. – 2009. – № 1. – С. 8–14.

138. Бойко І. В., Соловйова О. М., Ченереллі А. Цифровізація адміністративної процедури як спосіб забезпечення права на належне адміністрування // Права людини в умовах цифрової трансформації суспільства: монографія / Д. В. Лученко, О. В. Капліна, В. Я. Настюк та ін.; за ред. проф. Д. В. Лученка. – Харків: НЮУ ім. Ярослава Мудрого, 2022. – С. 127–148.

139. Negroponte N. Being Digital. New York: Knopf, 1995. – 256 p.

140. Руденко М. В. Цифровізація: категоріальні особливості та специфіка трактування // Економічний форум. – 2021. – № 4. – С. 3–13.

141. Стратегія здійснення цифрового розвитку, цифрових трансформацій і цифровізації системи управління державними фінансами на період до 2025 року, схвалена розпор. КМ України від 17.11.2021 р. № 1467-р. URL: https://zakon.rada.gov.ua/laws/show/1467-2021-p#Text.

142. Україна долучилася до програми «Цифрова Європа»: новини Міністерства цифрової трансформації України [Електронний ресурс]. – Режим доступу: https://thedigital.gov.ua/news/ukraina-doluchilasya-do-programitsifrova-evropa-shcho-tse-oznachae

143. Пітер Д., Стівенс К. Майбутнє ближче, ніж здається. Як технології змінюють бізнес, промисловість і наше життя / пер. з англ. Дмитро Кожедуб. – Київ: Лабораторія, 2021. – 320 с.

144. Білей М. Управлінські процедури як засіб реалізації організаційної функції державного управління. Матеріали інтернет-конференції «Інновації та традиції в сучасній науковій думці» (16-18.08.2016). URL: https://int-konf.org/ru/2016/innovatsiji-ta-traditsiji-v-suchasnij-naukovij-dumtsi-16-18-08-2016/1280-bilej-m-v-upravlinski-protseduri-yak-zasib-realizatsiji-organizatsijnoji-funktsiji-derzhavnogo-upravlinnya

145. Христинченко Н. Види адміністративних процедур у науковій сфері. Науковий вісник Міжнародного гуманітарного університету. Серія: Юриспруденція. 2014. Вип. 10–1(1). С. 165–167

146. Куркова К. М. Адміністративні процедури у сфері адміністративно-правового забезпечення науково-технологічного розвитку в Україні / К. М. Куркова // Науковий вісник Ужгородського національного університету. Серія «Право». – 2023. – Вип. 76, ч. 2. – С. 58 – 63

147. Джафарова О. Дозвільна діяльність органів публічної адміністрації в Україні: питання теорії та практики: монографія. – Харків: Панов, 2015. – 688 с.

148. Про електронні комунікації: Закон України від 16 грудня 2020 р. № 1089-IX // Відомості Верховної Ради України (ВВР), 2021, № 37-38, ст. 308. URL: https://zakon.rada.gov.ua/laws/show/1089-20#Text.

149. Про хмарні послуги: Закон України від 17 лютого 2022 р. № 2075-IX // Відомості Верховної Ради України (ВВР), 2022, № 32, ст. 283. URL: https://zakon.rada.gov.ua/laws/show/2075-20#Text.

150. Про публічні електронні реєстри: Закон України від 15 липня 2021 р. № 1907-IX // Відомості Верховної Ради України (ВВР), 2022, № 17, ст. 121. URL: https://zakon.rada.gov.ua/laws/show/1907-20#Text.

151. Соловйова О. Цифровізація адміністративної процедури: сучасний стан і перспективи розвитку [Електронний ресурс] / О. Соловйова // Громадська мережа публічного права та адміністрації UPLAN. – Режим доступу: https://uplan.org.ua/analytics/tsyfrovizatsiia-administratyvnoi-protsedury-suchasnyi-stan-i-perspektyvy-rozvytku/.

152. Про адміністративні послуги: Закон України від 6 вересня 2012 р. № 5203-VI // Відомості Верховної Ради України (ВВР), 2013, № 32, ст. 409. URL: https://zakon.rada.gov.ua/laws/show/5203-17#Text.

153. Про звернення громадян: Закон України від 2 жовтня 1996 р. № 393/96-ВР // Відомості Верховної Ради України (ВВР), 1996, № 47, ст. 256. URL: https://zakon.rada.gov.ua/laws/show/393/96-вр#Text.

154. Пашко Д. В., Омельчук Л. В. Потреба визначення статусу криптовалют в Україні: економічні та кримінальні процесуальні аспекти // Міжнародний юридичний вісник. – 2018. – № 1. – С. 173–179.

155. Скрипник В. Місце криптовалюти в системі об'єктів цивільних прав // Цивільне право і процес. – 2018. – № 8. – С. 38–43.

156. Про Національний Банк України: Закон України від 20.05.1999 № 679-XIV. Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/679-14.

157. Національний банк України. Лист від 08.12.2014 № 29-208/72889 [Електронний ресурс]. URL: https://zakon.rada.gov.ua/laws/show/v2889500-14#Text.

158. Про віртуальні активи: Закон України від 17 лютого 2022 р. № 2074-IX. URL: https://zakon.rada.gov.ua/laws/show/2074-20#Text.

159. Financial Action Task Force (FATF). Official website [Електронний ресурс]. URL: https://www.fatf-gafi.org/en/home.html.

160. Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення: Закон України від 06.12.2019 № 361-IX. URL: https://zakon.rada.gov.ua/laws/show/361-20#Text.

161. Європейський Союз. Regulation (EU) 2023/1114 on Markets in Crypto-Assets (MiCA). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=legissum:4626998.

162. Європейське управління з цінних паперів і ринків (ESMA). Markets in Crypto-Assets Regulation (MiCA). URL: https://www.esma.europa.eu/esmas-activities/digital-finance-and-innovation/markets-crypto-assets-regulation-mica.

163. Баранов О. А. Інтернет речей і право: погляд у майбутнє // Інтернет речей: проблеми правового регулювання та впровадження: зб. матеріалів доп. учасн. III наук.-практ. конф. – Київ, 2019. – С. 7–13.

164. Харитонов Є. О., Харитонова О. І. Категорія «Інтернет речей» та цивільні правовідносини // Наукові праці НУ ОЮА. – 2017. – С. 169–177. URL: http://dspace.onua.edu.ua/bitstream/handle/11300/12514.

165. Костенко О. В. Напрями розвитку права у сфері Інтернет речей (IoT) та штучного інтелекту / О. В. Костенко // Актуальні проблеми вітчизняної юриспруденції. – 2021. – № 3. – С. 130–136. – DOI: https://doi.org/10.15421/392161.

166. Баранов О. А. Інтернет речей (IoT) і блокчейн // Інформація і право. – 2018. – № 1 (24). – С. 59–71. URL: http://ippi.org.ua/baranov-oa-internet-rechei-iot-i-blokchein.

167. International Telecommunication Union (ITU). ITU-T Recommendation ITU-T Y.2060 (06/2012). URL: https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=y.2060.

168. N. Kong, Park Jungsoo, N. Crespi, G. Lee, Ilyoung Chong. The Internet of Things – Concept and Problem Statement. URL: https://www.semanticscholar.org/paper/The-Internet-of-Things-Concept-and-Problem-Kong-Jungsoo.

169. Lu Yan, Yan Zhang, Laurence T. Yang, Huansheng Ning. The Internet of Things: From RFID to the Next-Generation Pervasive Networked. eBook, ISBN 9780429133152. URL: https://doi.org/10.1201/9781420052824.

170. The Internet of Things. ITU Internet Reports 2005. URL: https://www.itu.int/net/wsis/tunis/newsroom/stats/The-Internetof-Things-2005.pdf.

171. Костенко О. В. Управління ідентифікаційними даними: правове регулювання анонімізації та псевдонімізації // Науковий вісник публічного та приватного права. – 2021. – № 1. – С. 110–118.

172. Гриценчук О. Використання штучного інтелекту в освіті: тенденції та перспективи в Україні та за кордоном // Вісник кафедри ЮНЕСКО «Неперервна професійна освіта XXI століття». – 2024. – Вип. 10. – С. 152–162. URL: https://lib.iitta.gov.ua/id/eprint/743864.

173. Про схвалення Концепції розвитку штучного інтелекту в Україні: розпорядження Кабінету Міністрів України від 2 грудня 2020 р. № 1556-р // Урядовий кур'єр. – 18.12.2020. – № 247.

174. Europe fit for the Digital Age: Commission proposes new rules and actions for excellence and trust in Artificial Intelligence. Press release (European Commission, 21 April 2021). URL: http://surl.li/gwhqa.

175. Європейська комісія. AI Act enters into force on 1 August 2024 [Електронний ресурс]. URL: https://commission.europa.eu/news/ai-act-enters-force-2024-08-01_en.

176. Європейський Союз. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 on harmonised rules on fair access to and use of data (Data Act) [Електронний ресурс] // Official Journal of the European Union. – 2024. – L 168/9. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L_202401689.

177. Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури: Постанова Кабінету Міністрів України від 19.06.2019 № 518. URL: https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text.

178. Кудінов В. А., Яровий К. В. Комплексний підхід щодо створення стійких паролів інформаційних систем спеціального призначення МВС та Національної поліції України (частина 1) // Сучасна спеціальна техніка. – 2023. – № 3 (74). – С. 42–49.

179. Директива 95/46/ЄС Європейського Парламенту і Ради «Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних» від 24 жовтня 1995 року. URL: https://zakon.rada.gov.ua/laws/show/994_242#Text.

180. Угода про Асоціацію між Україною та Європейським Союзом. URL: https://zakon.rada.gov.ua/laws/show/984_011#n2422.

181. Директива Європейського Парламенту і Ради (ЄС) 2016/1148 від 6 липня 2016 р. про заходи для високого рівня безпеки мережевих та інформаційних систем на території Союзу. URL: https://zakon.rada.gov.ua/laws/show/984_013-16#Text.

182. Директива (ЄС) 2022/2555 Європейського Парламенту і Ради від 14 грудня 2022 р. про заходи для досягнення високого рівня кібербезпеки в Європейському Союзі (Директива NIS2). URL: https://digital-strategy.ec.europa.eu/en/policies/nis2-directive.

183. Regulation (EU) 2019/881 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L_20190881.

184. ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection. URL: https://www.iso.org/standard/75652.html.

185. European Commission. Digital Single Market Strategy. URL: https://digital-strategy.ec.europa.eu/en.

186. Європейська комісія. Once-Only Principle Project (TOOP). URL: https://ec.europa.eu/isa2/isa2conf18/once-only-principle-project-toop_en/.

187. Європейська Комісія. 2030 Digital Compass: The European way for the Digital Decade. URL: https://eufordigital.eu/uk/library/2030-digital-compass-the-european-way-for-the-digital-decade/.

188. Решетова Г. І. Європейський досвід запровадження електронного урядування // Management and Entrepreneurship: Trends of Development. – 2023. – Вип. 1(23). – С. 60-70. DOI: 10.26661/2522-1566/2023-1/23-06.

189. Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions (eIDAS Regulation). URL: https://digital-strategy.ec.europa.eu/en/policies/eidas-regulation.

190. EU4DigitalUA. Цифрова трансформація для України (DT4UA). URL: https://eu4digitalua.eu/uk/dt4ua/.

191. Estonian X-Road Platform. URL: https://x-road.global.

192. E-Residency in Estonia. Official Website. URL: https://e-resident.gov.ee.

193. Серебро М. Адміністративно-правове регулювання використання технології штучного інтелекту: національний та зарубіжний досвід // Науковий вісник Міжнародного гуманітарного університету. Серія: Юриспруденція. – 2024. – № 70. – С. 40–44. DOI: https://doi.org/10.32782/2307-1745.2024.70.8.

194. ЮНЕСКО. Глобальний стандарт етики штучного інтелекту. URL: https://www.radiosvoboda.org/a/yunesko-hlobalnyy-standart-etyky-shtuchnoho-intelektu/31612648.html.

195. Cybersecurity and Infrastructure Security Agency (CISA). Federal Information Security Modernization Act. URL: https://www.cisa.gov/topics/cyber-threats-and-advisories/federal-information-security-modernization-act.

196. Clyde & Co. Singapore’s Model AI Governance Framework for Generative AI. URL: https://www.clydeco.com/en/insights/2024/05/singapore-s-model-ai-governance-framework-for-gene.

197. Infocomm Media Development Authority (IMDA). Contact Us. URL: https://www.imda.gov.sg/about-imda/contact-us.

198. Personal Data Protection Commission (PDPC). Офіційний сайт. URL: https://www.pdpc.gov.sg/.

199. AI Verify Foundation. Офіційний сайт. URL: https://aiverifyfoundation.sg/.

200. Smart City Korea. Офіційний сайт. URL: https://smartcitykorea.com/en/index.html.

201. Розумні суди у Китаї: як вони працюють та чому судді мають радитись зі штучним інтелектом? URL: https://processer.media/ua/rozumni-sudi-u-kitai-yak-voni-pracjujut-ta-chomu-suddi-majut-raditis-zi-shtuchnim-intelektom/.

202. Україна та США будуть поглиблювати співпрацю у сфері кібербезпеки – Рустем Умєров // Міністерство оборони України. URL: https://mod.gov.ua/news/ukrayina-ta-s-sh-a-budut-pogliblyuvati-spivpraczyu-u-sferi-kiberbezpeki-rustem-umyerov.

ДОДАТКИ

СПИСОК ПРАЦЬ, ОПУБЛІКОВАНИХ ЗА ТЕМОЮ ДИСЕРТАЦІЇ:

Статті, в яких опубліковано основні наукові результати дисертації:

1. Білоус Я.В. Основні проблеми нормативно-правового регулювання використання інформаційних технологій в Україні. *Юридичний науковий електронний журнал*. 2023. № 12. С. 650–653. DOI: https://doi.org/10.32782/2524-0374/2023-12/163.

2. Білоус Я.В. Етапи розвитку адміністративно-правового регулювання інформаційних технологій в Україні. *Право та державне управління*. 2024. № 2. С. 357–362. DOI: https://doi.org/10.32782/pdu.2024.2.47.

3. Білоус Я.В. Проблематика правового регулювання інформаційних технологій в Україні в умовах євроінтеграції та цифрової трансформації. *Держава та регіони. Серія: Право*. 2024. № 3. С. 103–107. DOI: https://doi.org/10.32782/1813-338X-2024.3.17.

4. Білоус Я.В. Європейський досвід адміністративно-правового регулювання інформаційних технологій: позитивний досвід для України. *KELM (Knowledge, Education, Law, Management)*. 2024. № 3(63). P. 210–214. DOI: https://doi.org/10.51647/kelm.2024.3.33.

5. Білоус Я.В. Перспективні напрями удосконалення адміністративно-правового регулювання інформаційних технологій в Україні. *Право і суспільство*. 2024. № 2. С. 670–677. DOI: https://doi.org/10.32842/2078-3736/2024.2.96.

Наукові праці, які засвідчують апробацію матеріалів дисертації:

1. Білоус Я.В. Проблеми правового регулювання використання інформаційних технологій в Україні. *Proceedings of the international scientific conference "The latest law developments"*, Wloclawek, Republic of Poland, April 3–4, 2024. Riga : Publishing House "Baltija Publishing", 2024. P. 277–282. DOI: https://doi.org/10.30525/978-9934-26-432-0-66.

2. Білоус Я.В. Перспективні заходи правового регулювання інформаційних технологій в Україні. *Proceedings of the international scientific conference "Scientific innovations in law amidst the impact of the Russian-Ukrainian w.ar on the legal system"*, Riga, the Republic of Latvia, February 7–8, 2024. Riga : Publishing House "Baltija Publishing", 2024. P. 300–304. DOI: https://doi.org/10.30525/978-9934-26-409-2-72.