МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Національний університет кораблебудування імені адмірала Макарова

Факультет морського права

Кафедра адміністративного та конституційного права

«Допущений до захисту»
В. о. завідувача кафедри
_____ Н. П. Бортник
«__22__» ____12_____ 2025 р.

УДК 342.9:004.056.5(477)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття ступеня вищої освіти «магістр»

на тему:

«ІНФОРМАЦІЙНА БЕЗПЕКА В КОНТЕКСТІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ: АДМІНІСТРАТИВНО-ПРАВОВА ХАРАКТЕРИСТИКА»

Виконав:
студент 6 курсу, групи 6511м
_____ ***Прядко К. О.***
Керівник роботи:
в. о. завідувача кафедри адміністративного
та конституційного права,
доктор юридичних наук, професор
_____ ***Бортник Н. П.***

Миколаїв – 2025 р.

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет кораблебудування імені адмірала Макарова
Факультет морського права

Кафедра **адміністративного та конституційного права**
Спеціальність **081 Право**
Освітня програма **Право**

«ЗАТВЕРДЖУЮ»
Гарант ~~освітньої~~ програми
_____ **О. Ю. Дубинський**
(підпис)
«02» ____12____ 2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТА
на здобуття ступеня вищої освіти «магістр»

Студенту **Прядку Костянтину Олександровичу**
(Прізвище, ім'я, по батькові)

1. Тема роботи: **«Інформаційна безпека в контексті національної безпеки: адміністративно-правова характеристика»**

Керівник роботи **д.ю.н., професор Бортник Надія Петрівна**
Затверджені наказом ректора **№ 1155-уч від « 30 » вересня 2025 року**

2. Термін подання роботи: __ **01.12.2025 року** _____

3. Вихідні дані до роботи: __**чинне законодавство, фахова література, матеріали конференцій, репозитарій університету** _____

4. Перелік питань, що належать до розробки (найменування розділів) _____
Розділ 1. Теоретико-правові основи дослідження інформаційної безпеки
Розділ 2. Адміністративно-правові механізми забезпечення інформаційної безпеки
Розділ 3. Проблеми та перспективи вдосконалення адміністративно-правового регулювання інформаційної безпеки в Україні

5. Перелік презентаційних матеріалів **виконаний в програмі Power Point**

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
	Сторонні консультанти до підготовки розділів роботи не залучалися		

7. Дата видачі завдання **06 вересня 2025 року**

КАЛЕНДАРНИЙ ПЛАН

Номер	Назва етапів роботи	Терміни виконання етапів роботи	Примітка
1.	Вивчення літературних джерел з предмета дослідження	вересень 2025 р.	виконано
2.	Складання розгорнутого плану роботи та ознайомлення керівника з планом кваліфікаційної роботи	вересень 2025 р.	виконано
3.	Написання розділу 1	вересень 2025 р.	виконано
4.	Написання розділу 2	жовтень 2025 р.	виконано
5.	Написання розділу 3	листопад 2025 р.	виконано
6.	Оформлення кваліфікаційної роботи	до 25 листопада 2025 р.	виконано
7.	Передача кваліфікаційної роботи науковому керівнику для написання відгуку	до 27 листопада 2025 р.	виконано
8.	Передача кваліфікаційної роботи рецензенту для рецензування	до 30 листопада 2025 р.	виконано
9.	Попередній захист кваліфікаційної роботи	02 грудня 2025 р.	виконано
10	Захист кваліфікаційної роботи	16 грудня 2025 р.	виконано

Студент _____ **Прядко К. О.**

Керівник роботи _____ **Бортник Н. П.**

ЗМІСТ

АНОТАЦІЯ

Прядко К. О. Інформаційна безпека в контексті національної безпеки: адміністративно-правова характеристика – Кваліфікаційна наукова праця на правах рукопису.

Випускова кваліфікаційна робота на здобуття ступеня вищої освіти «магістр» (081 Право). – Національний університет кораблебудування імені адмірала Макарова, Миколаїв, 2025.

Кваліфікаційна робота присвячена адміністративно-правовій характеристиці інформаційної безпеки в контексті національної безпеки.

У першому розділі *"Теоретико-правові основи дослідження інформаційної безпеки"* з'ясовано сутність, значення та місце інформаційної безпеки в системі національної безпеки, розглянуто правові аспекти та особливості регулювання інформаційної безпеки як складової адміністративного права, встановлено загрози інформаційній безпеці в контексті національної безпеки України.

Другий Розділ *"Адміністративно-правові механізми забезпечення інформаційної безпеки"* містить характеристику стратегічних напрямів та принципів реалізації державної політики у сфері інформаційної безпеки, аналіз повноважень органів державної влади у забезпеченні інформаційної безпеки в контексті адміністративно-правового аспекту, порівняльний аналіз та можливості імплементації в Україні міжнародного досвіду регулювання інформаційної безпеки.

Третій Розділ *"Проблеми та перспективи вдосконалення адміністративно-правового регулювання інформаційної безпеки в Україні"* присвячений аналізу існуючих проблем у сфері інформаційної безпеки у контексті прогалин нормативно-правової бази та організаційних аспектів, а також вивченню ролі громадянського суспільства у забезпеченні інформаційної безпеки через розгляд правових механізмів співпраці з державою.

У *Висновках* підведено підсумки роботи. Зокрема, констатовано, що

інформаційна безпека є стратегічним пріоритетом держави, оскільки сучасні виклики, зокрема кіберзагрози, інформаційні війни та дезінформація, мають потенціал значно впливати на політичну, економічну, соціальну та культурну стабільність країни. Вона охоплює захист інформаційних ресурсів, забезпечення кіберстійкості та протидію інформаційним загрозам.

Окрім того акцентовано на доцільності системного підходу, інтеграції зусиль державних органів, приватного сектору та громадянського суспільства, що сприятиме належному забезпеченню інформаційної безпеки держави.

Ключові слова: інформація, право на інформацію, інформаційна безпека, національна безпека, кібербезпека, захист стратегічних сфер держави, міжнародна інформаційна безпека, адміністративно-правове регулювання, загрози інформаційній безпеці, інформаційні війни.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

РНБО	Рада національної безпеки і оборони України
ЄС	Європейський Союз
НАТО	Організація Північноатлантичного договору
СБУ	Служба безпеки України
ЗСУ	Збройні Сили України
ООН	Організація Об’єднаних Націй
ENISA	Європейська агенція з кібербезпеки

ВСТУП

Актуальність теми. У сучасних умовах стрімкого розвитку інформаційних технологій та глобалізації інформаційного простору питання забезпечення інформаційної безпеки набуває особливої актуальності. Інформаційна безпека є одним із ключових елементів національної безпеки, оскільки вона забезпечує захист держави, суспільства та особи від загроз, пов'язаних із несанкціонованим доступом, маніпуляцією або руйнуванням інформаційних ресурсів.

Значення інформаційної безпеки зростає в умовах поширення гібридних загроз, кіберзлочинності, інформаційних війн та пропаганди. Відтак, держави змушені адаптувати свої правові системи до нових викликів, розробляючи ефективні механізми адміністративно-правового регулювання у сфері інформаційної безпеки. Україна, як держава, що перебуває в умовах збройного конфлікту та інформаційного протистояння, також стикається з необхідністю удосконалення правових інструментів для захисту національних інтересів в інформаційному просторі.

Адміністративно-правова характеристика інформаційної безпеки передбачає аналіз правової бази, яка регулює діяльність державних органів у цій сфері, визначення їхніх функцій, повноважень та відповідальності. Зокрема, це стосується питань запобігання кіберзагрозам, боротьби з дезінформацією, захисту критичної інформаційної інфраструктури, а також забезпечення прав громадян на доступ до достовірної інформації.

Теоретичною та методологічною основою цієї кваліфікаційної роботи стали праці відомих вітчизняних і зарубіжних вчених, з-поміж яких: В. Авер'янов, Н. Армаш, О. Баранов, К. Бєляков, Н. Бортник, М. Гуцалюк, С. Єсімов, О. Золотар, Т. Коломоєць, В. Колпаков, Б. Кормич, А. Марущак, Н. Мороз, А. Нашинець-Наумова, Р. Радейко, А. Собакарь, В. Цимбалюк, Л. Чистоклетов, М. Швець та багато інших.

Мета і завдання дослідження. *Мета* кваліфікаційної роботи полягає в

адміністративно-правовій характеристиці інформаційної безпеки в контексті національної безпеки, з урахуванням того, що ефективна система забезпечення інформаційної безпеки є не лише умовою стабільності держави, але й запорукою її суверенітету та розвитку.

Для досягнення поставленої мети у кваліфікаційній роботі планується вирішити такі *завдання*:

– з'ясувати сутність, значення та місце інформаційної безпеки в системі національної безпеки;

– розкрити правові аспекти та особливості регулювання інформаційної безпеки як складової адміністративного права;

– проаналізувати загрози інформаційній безпеці в контексті національної безпеки України;

– охарактеризувати стратегічні напрями та принципи реалізації державної політики у сфері інформаційної безпеки;

– визначити повноваження органів державної влади у забезпеченні інформаційної безпеки;

– розглянути міжнародний досвід регулювання інформаційної безпеки;

– здійснити аналіз існуючих проблем у сфері інформаційної безпеки щодо прогалини нормативно-правової бази та організаційних аспектів;

– з'ясувати роль громадянського суспільства у забезпеченні інформаційної безпеки шляхом аналізу правових механізмів співпраці з державою.

Об'єктом дослідження є суспільні відносини, що виникають у процесі забезпечення інформаційної безпеки як складової національної безпеки адміністративно-правовими засобами.

Предметом дослідження виступає адміністративно-правова характеристика інформаційної безпеки в контексті національної безпеки.

Методи дослідження. Кваліфікаційна робота базується на теоретичних засадах та визнаних методологічних підходах до наукового дослідження, що включають світоглядні, загальнонаукові та спеціалізовані методи. У дослідженні застосовано такі методи, як індукція, дедукція, аналіз, синтез, діалектичний

підхід та порівняльно-правовий метод. Це дозволило здійснити перехід від загальних положень до конкретних аспектів, що сприяло визначенню ключових напрямів наукового пошуку та комплексному аналізу проблеми в її соціальному контексті та юридичній площині. Застосування такого методологічного підходу забезпечило всебічне та системне висвітлення адміністративно-правових аспектів інформаційної безпеки у зв'язку з питаннями національної безпеки.

Апробація результатів дослідження. Підсумки роботи загалом, узагальнення та висновки були оприлюднені на Міжнародній науково-практичній конференції *“”* (м. Львів, жовтня 2025 року).

Структура кваліфікаційної роботи зумовлена метою та її завданнями і складається з анотації, переліку умовних позначень, вступу, трьох розділів, що містять вісім підрозділів, висновків, списку використаних джерел і додатків. Загальний обсяг кваліфікаційної роботи становить 76 сторінок, з яких основного тексту – 62 сторінки. Список використаних джерел налічує 70 найменування і розміщений на 7 сторінках, додатки – на 2 сторінках.

РОЗДІЛ 1
ТЕОРЕТИКО-ПРАВОВІ ОСНОВИ ДОСЛІДЖЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

1.1. Сутність, значення та місце інформаційної безпеки в системі національної безпеки

З огляду на здобуття Україною суверенітету та взяття курсу на утвердження демократичних, гуманістичних ідей та цінностей, питання формування та впровадження інформаційної безпеки набуває дедалі більшої гостроти та значущості. При цьому сучасний світ демонструє багатоаспектність та різноманітність ознак, які характеризують інформаційну безпеку у динамічному вимірі, що виходить далеко за межі лише доктринальних уявлень про це поняття, особливо у світлі формування глобальної інформаційної спільноти [1].

Настання третього тисячоліття ознаменувало появу суспільства нового типу – інформаційного, де інформація виступає ключовим стратегічним активом. Вплив інформаційних процесів на усі сфери як державного, так і суспільного життя загострює найважливіші проблеми соціального буття, включаючи питання інформаційної взаємодії, що нерозривно пов’язане з боротьбою за інформаційний простір та протидією різноманітним інформаційним загрозам. У цьому контексті, неминуче трансформується і підхід до дослідження ціннісних орієнтацій особистості, її інформаційної обґрунтованості та забезпечення інформаційної безпеки [1].

Роль сфери інформації, яка охоплює сукупність даних, інформаційної інфраструктури суб’єктів, залучених до збору, створення, поширення та використання інформації, а також системи регулювання суспільних відносин, що виникають у цьому процесі, суттєво зросла на сучасному етапі розвитку суспільства. Будучи критично важливим чинником життєдіяльності соціуму, інформаційна сфера має вагомий вплив на стан як політичної, так і оборонної та

економічної складових безпеки України. Від ефективності забезпечення інформаційної безпеки значною мірою залежить національна безпека держави, і ця залежність посилюватиметься паралельно з технічним прогресом та інкорпорацією інформаційних технологій у всі аспекти діяльності сучасного суспільства [1].

Усвідомлення цього зумовлює те, що інформаційна безпека стає життєво важливим, фундаментальним елементом усієї системи забезпечення безпеки української державності. Причина цього криється, насамперед, у стрімкому зростанні технологічних спроможностей сучасних інформаційних систем, які на сьогодні набули вирішального та всеохоплюючого впливу на політичні процеси, господарсько-економічне життя, духовно-ідеологічне поле, а також правові та соціально-економічні погляди громадян [1].

Інформаційна безпека є одним із ключових елементів сучасної системи національної безпеки, що обумовлено стрімким розвитком інформаційних технологій та зростанням ролі інформації у всіх сферах суспільного життя. У статті розглянуто сутність поняття інформаційної безпеки, її значення для держави, суспільства та особистості, а також її місце в структурі національної безпеки.

Згідно з поглядами Б. А. Кормича, національна безпека – це таке становище, за якого держава захищена від небезпек, що походять як зсередини, так і ззовні. Це забезпечує умови для життєдіяльності особи, соціуму та самої держави, які гарантуються Основним Законом України та чинним законодавством. [2, с. 37].

Інформаційна безпека визначається як стан захищеності інформаційного середовища, який забезпечує збереження конфіденційності, цілісності та доступності інформації, а також захист прав і свобод особистості, суспільства та держави в інформаційній сфері. Це поняття охоплює не лише технічні аспекти захисту даних, але й правові, організаційні та соціальні механізми, спрямовані на запобігання загрозам і мінімізацію ризиків.

Чимало фахівців у наукових колах розглядають проблематику

інформаційної безпеки у світлі гарантування національної безпеки, вказуючи на їх пряму взаємозалежність. Поміж науковців, як зазначається, наразі відсутня уніфікована позиція стосовно дефініції терміну «інформаційна безпека». У межах цього визначеного вектору, інформаційну безпеку можна трактувати як стан обороноздатності країни, захисту її ключових інтересів у інформаційній площині, що підсумовується збалансованістю потреб індивіда, соціуму та самої держави. Безпосередньо національна безпека держави значною мірою детермінована належним рівнем інформаційної безпеки, і ця кореляція лише посилюється з розвитком технологій. Водночас, О. А. Панченко окреслює три головні вектори, спрямовані на забезпечення інформаційної безпеки:

– гарантування захисту інформаційних прав та вольностей особистості й громадянина;

– охорона інформаційних активів, зокрема тих, що мають обмежений обіг, від несанкціонованого доступу;

– убезпечення суспільства від інформації, що є потенційно шкідливою чи недоброякісною [3, с. 58].

Питання правового регулювання інформаційної безпеки викликає значний інтерес у науковій спільноті. Зокрема, у сучасній науковій літературі детально досліджуються чинники, що впливають на забезпечення безпеки держави, а також їх взаємозв'язок із процесами сталого розвитку. Більшість науковців сходяться на думці, що інформаційна безпека є невід'ємною складовою загальної безпеки держави.

Цікаві і змістовні авторські думки стосовно розуміння терміну «інформаційна безпека» викладені також у працях А. Фороса [4, с. 222-226], В. Цимбалюка [5, с. 88-91], О. Золотар [6, с. 109-113], В. Гурковського [7], Б. Кормича [8], А. Нашинець-Наумової [9], Т. Ткачука [10, с. 104-110], Є. Рогової [11, с. 190-196], В. Шатуна [12, с. 174-180], М. Гуцалюка [13, с. 71-74], С. Домбровської [14, с. 203-207], А. Марущака [15, с. 17-21] та ін.

Згідно з думкою Н. І. Верхоглядової та І. В. Кононової, у найширшому сенсі, інформаційна безпека являє собою такий ступінь захищеності середовища

обробки даних, котрий гарантує його становлення, функціонування та прогрес на користь населення, установ та держави. Ці фахівці підкреслюють, що інформаційне середовище слід розуміти як арену діяльності різних акторів, котра стосується генерації, зміни та використання відомостей. Зазначене інформаційне середовище прийнято розчленовувати на три складові:

1. Формування та поширення первинних та вторинних даних.
2. Створення фондів даних, готової інформаційної продукції та сервісів.
3. Процес споживання відомостей [16, с. 386].

Згідно з баченням М. О. Шевчука, інформаційна безпека є унікальним явищем сучасності, чия поява має всесвітнє значення для людства, що диктує нагальну потребу у формулюванні її об'єктивного, прикладного визначення. Воістину, інформаційна безпека являє собою досить заплутане явище. Існує низка обставин, які ускладнюють надання цьому поняттю чіткого визначення. Науковець акцентує на найбільш вагомих з них: 1. Інформаційна безпека – це об'єктивна реальність, детермінована об'єктивними умовами суспільного поступу. Її формування відбувається у контексті процесу інформатизації суспільства, котрий, своєю чергою, ще не завершений і вимагає подальшого поглибленого дослідження. До того ж, специфіка інформаційної безпеки в Україні безпосередньо пов'язана з реорганізацією самої системи національної безпеки держави. Унаслідок зазначених факторів виникають перешкоди, які заважають сформувати достатньо вичерпну дефініцію цього поняття [17, с. 134-138].

На переконання О. М. Шевчука, практично всі дослідники, розробляючи визначення, мали спільне прагнення внести методологічну, а не лише термінологічну ясність у розуміння сутності терміна «інформаційна безпека». Відштовхуючись від засади, що суть безпеки будь-якої системи полягає у її здатності зберігати свою цілісність та розвиватися, реалізуючи ці можливості навіть у складних умовах (конфлікти, ризики, невизначеність тощо), ми доходимо ключового методологічного висновку: система забезпечення безпеки, а саме інформаційної, орієнтована на реалізацію згаданих адаптивних

потенціалів. Тому інформаційну безпеку слушно розглядати як захищеність об’єкта в інформаційному просторі та безпеку самої інформаційної сфери. Це означає, що інформаційна безпека досягається не лише завдяки застосуванню засобів, методів та заходів для захисту інформаційного середовища і захисту суб’єкта від деструктивних впливів, а й через формування у суб’єкта здатності протистояти негативним інформаційним діям. Таким чином, завдання забезпечення інформаційної безпеки полягає у створенні оптимальних умов для функціонування інформаційної інфраструктури, головним елементом якої є людина (а не комп'ютер), яка має мати можливість прогресувати та діяти відповідно до своїх цінностей і цілей [17, с. 137-138].

На думку вченого, складнощі з дефініцією «інформаційної безпеки» також зумовлені тим, що цей феномен розглядається крізь призму різноманітних аспектів: технічного, правового, психологічного, соціального та інших. Фахівці, аналізуючи це явище з позицій своєї наукової дисципліни, насичують термін «інформаційна безпека» власним змістом, що ще раз підкреслює його багатогранність і ускладнює досягнення універсального визначення [17, с. 137-138].

Основними складовими інформаційної безпеки є:

1. Конфіденційність – забезпечення доступу до інформації лише уповноваженим особам.

2. Цілісність – захист інформації від несанкціонованих змін.

3. Доступність – гарантування можливості отримання інформації за потреби.

Інформаційна безпека є міждисциплінарною категорією, яка охоплює сфери права, кібербезпеки, соціології, психології та інших наук. Її основною метою є створення умов для сталого функціонування суспільства в умовах глобальної інформаційної взаємодії.

Варто погодитись з Н. С. Грабар у тому, що забезпечення інформаційної безпеки в умовах формування світового інформаційного соціуму нерозривно пов’язане із захистом безпеки як окремої особистості, так і суспільства в цілому.

Це особливо помітно на прикладі України, де інформаційні мережі тісно переплетені з державними інституціями. З огляду на багатоаспектність та складність державного регулювання виникає нагальна потреба у продовженні наукових досліджень механізмів забезпечення інформаційної безпеки [1].

Значення інформаційної безпеки для сучасного суспільства важко переоцінити. У цифрову епоху інформація стала стратегічним ресурсом, що визначає економічний, політичний і соціальний розвиток держави. Втрата або спотворення інформації може мати катастрофічні наслідки для національної безпеки, зокрема:

– порушення функціонування державних органів;

– підрив економічної стабільності;

– маніпуляція громадською думкою;

– загроза приватному життю громадян.

На даний час інформаційний простір пронизує майже кожну сферу життєдіяльності суспільства, зачіпаючи політичні, економічні, оборонні, культурні, управлінські питання, міжнародну взаємодію, наукові здобутки, освіту, сімейні стосунки, повсякденний ужиток та багато іншого. На погляд В. М. Абакумова, інформаційна сфера являє собою область, яка постає та набуває розвитку внаслідок реалізації певного комплексу заходів, націлених на задоволення інформаційних запитів як окремих громадян, так і юридичних осіб, і держави в цілому. Йдеться як про потребу в отриманні, застосуванні, розповсюдженні та зберіганні відомостей, так і про потребу у вільному доступі до найсучасніших інформаційно-телекомунікаційних засобів [18, с. 11].

Інформаційна безпека також є важливим фактором забезпечення демократичних процесів. Наприклад, у контексті виборів вона гарантує захист від зовнішнього втручання та забезпечує прозорість і чесність виборчого процесу.

У міжнародному вимірі інформаційна безпека є складовою глобальної безпеки. Кіберзлочинність, інформаційний тероризм і гібридні загрози створюють нові виклики для держав і міжнародних організацій. У цьому

контексті особливе значення має співробітництво між країнами у сфері кібербезпеки та розробка спільних стандартів захисту.

Інформаційна безпека посідає центральне місце в системі національної безпеки, оскільки вона впливає на всі її складові: політичну, економічну, військову, екологічну та соціальну. У стратегічних документах багатьох держав, зокрема України, вона визначається як пріоритетний напрям забезпечення національної безпеки. В Україні правове регулювання інформаційної безпеки здійснюється відповідно до Конституції України та низки Законів України, що прийняті на її основі.

Основними напрямами державної політики у сфері інформаційної безпеки є:

1. Захист національного інформаційного простору від зовнішніх і внутрішніх загроз.

2. Розвиток національної інфраструктури кібербезпеки.

3. Забезпечення захисту персональних даних.

4. Протидія пропаганді та дезінформації.

5. Підвищення рівня медіаграмотності населення.

Особливе місце в забезпеченні інформаційної безпеки займає боротьба з кіберзлочинністю. В умовах цифровізації економіки та суспільства кіберзлочини стають дедалі складнішими та масштабнішими. Це вимагає від держави впровадження новітніх технологій і методів захисту, а також ефективного міжнародного співробітництва.

Натомість, як підкреслює О. О. Золотар, чинне законодавство, визначаючи поняття інформаційної безпеки, оминає увагою безпеку саме юридичних осіб. Проте велика кількість правовідносин виникає через реалізацію юридичними особами своїх інформаційних прав, і ці відносини також підлягають державному регулюванню. З цієї причини ми вважаємо за необхідне виділити ще один різновид інформаційної безпеки, класифікуючи її за об’єктною ознакою, а саме – інформаційну безпеку юридичних осіб [6, с. 111].

При цьому О. О. Золотар доходить висновку, що об’єктна ознака дозволяє

класифікувати інформаційну безпеку наступним чином:

– інформаційна безпека людини;

– інформаційна безпека суб'єктів господарювання (юридичних осіб);

– інформаційна безпека суспільства;

– інформаційна безпека держави (національна інформаційна безпека);

– інформаційна безпека світового співтовариства [6, с. 111].

З іншого боку, підкреслює вчена, коли йдеться про безпеку людини в інформаційній сфері, ми можемо говорити про громадян, іноземців та осіб без громадянства, а також про осіб із особливим статусом – держслужбовців, журналістів, неповнолітніх, і так далі; щодо безпеки юридичних осіб – це стосується комерційних та некомерційних формування, включно з громадськими об’єднаннями, релігійними структурами тощо [6, с. 111].

Інформаційна безпека будь-якого об’єкта означає його здатність функціонувати та розвиватися незалежно від наявності загроз інформаційного характеру, як внутрішніх, так і зовнішніх. Звідси випливає, що другим критерієм для класифікації може слугувати характер загроз для інформаційної безпеки. Враховуючи розподіл загроз на зовнішні та внутрішні, можливим є виділення внутрішньої та зовнішньої інформаційної безпеки [6, с. 111].

Відповідно до потенційних загроз інформаційній безпеці, пропонується розрізняти внутрішній та зовнішній аспекти інформаційної безпеки. При цьому сутність кожного з цих аспектів визначається тим, хто або що виступає об’єктом захисту в інформаційній сфері [6, с. 111].

Отже, інформаційна безпека є невід’ємною складовою національної безпеки, яка забезпечує стійкість держави та суспільства в умовах сучасних викликів і загроз. Її значення зростає в умовах глобалізації та стрімкого розвитку технологій, що потребує постійного вдосконалення механізмів захисту та адаптації до нових реалій. Україна, як частина світового інформаційного простору, повинна приділяти особливу увагу формуванню ефективної системи інформаційної безпеки для забезпечення свого суверенітету, стабільності та розвитку.

1.2. Інформаційна безпека як складова адміністративного права: правові аспекти та особливості регулювання

Інформаційна безпека є однією з ключових складових сучасної правової системи, яка забезпечує стабільність функціонування держави, суспільства та кожного окремого громадянина в умовах цифровізації. У контексті адміністративного права інформаційна безпека виступає об’єктом регулювання, що потребує чіткого визначення правових механізмів її забезпечення, а також встановлення відповідальності за порушення норм, які спрямовані на захист інформаційних ресурсів.

Інформаційна безпека визначається як стан захищеності інформаційного середовища, який забезпечує недоторканність, конфіденційність, доступність і цілісність інформації. У межах адміністративного права це поняття охоплює як захист державних інформаційних ресурсів, так і забезпечення прав громадян на доступ до інформації та захист їхніх персональних даних.

На думку Є. Кобко, у наш час, у двадцять першому столітті, сфера національних гарантій безпеки бачить інформаційну безпеку на чільному місці. Протягом значного відтинку часу це поняття переважно обмежувалося інтересами самої держави. Однак, з огляду на розвиток сучасних інформаційно-комунікаційних систем, теорія інформаційної безпеки зазнала суттєві зміни та набула іншого змісту. Зараз у межах країни інформаційна безпека охоплює такі площини: державну, суспільну (чи окремі групи/спільноти) та індивідуальну. Окремою, фундаментальною складовою є міжнародна інформаційна безпека. Таким чином, сутність інформаційної безпеки має дві рівні: 1) національний; 2) міжнародний [19, с. 49].

Шалений поступ інформаційних технологій у промислово розвинених державах спричинив виникнення доктрин «інформаційних протистоянь», головним завданням яких є здобуття відомостей або ж їхня трансформація задля власної вигоди. Ясно, що в нинішній дійсності ІТ-інструменти виконують

критично значущу функцію не лише у гарантуванні державності, а й у формуванні індивіда, соціуму та самої держави. Започаткування людиною зусиль зі збереження таємності даних дало поштовх формуванню наукових підвалин інформаційної безпеки. Із прогресом технічних засобів та механізмів пересилання відомостей еволюціонували й підходи до захисту інформаційних активів. На поточному етапі розвитку цивілізації надійна охорона інформаційної сфери дає змогу врегульовувати принципові аспекти майже усіх сфер державної безпеки. Інформаційна безпека є неподільною частиною загальної системи національного захисту, і від успішного розв'язання викликів у цій галузі детермінована глобальна безпека [17, с. 135].

Національне законодавство України визначає інформаційну безпеку як одну з основних складових національної безпеки, що закріплено в Законі України «Про національну безпеку України» від 21 червня 2018 року № 2469-VIII [20]. Водночас адміністративно-правове регулювання інформаційної безпеки охоплює низку напрямів, таких як протидія кіберзагрозам, контроль за обігом інформації, захист персональних даних і забезпечення прозорості діяльності органів державної влади.

Формування законодавчої бази для захисту інформації в цілому, а також забезпечення інформаційної та кібербезпеки в Україні є процесом, що триває протягом значного часу. Історичний аналіз правового регулювання цієї сфери бере свій початок фактично з моменту проголошення державного суверенітету України [33].

Регулювання інформаційної безпеки в Україні базується на Конституції України, міжнародних договорах, а також спеціальних нормативно-правових актах. Основними джерелами права в цій сфері є:

1. Конституція України [21], яка гарантує право на інформацію (стаття 34) та захист персональних даних (стаття 32).

2. Закон України «Про інформацію» [22], який регулює суспільні відносини у сфері створення, збирання, зберігання, використання та поширення інформації.

3. Закон України «Про захист персональних даних» [23], що встановлює правила обробки персональних даних та відповідальність за їх незаконне

використання.

4. Закон України «Про основні засади забезпечення кібербезпеки України» [24], який визначає правові й організаційні засади забезпечення кібербезпеки як складової інформаційної безпеки.

Особливістю правового регулювання у сфері інформаційної безпеки є його міжгалузевий характер. Наприклад, у кримінальному праві передбачено відповідальність за кіберзлочини (статті 361–363-1 Кримінального кодексу України [25]), тоді як адміністративне право зосереджене на запобіжних заходах і санкціях за порушення правил інформаційної безпеки [26].

Для створення належних умов для гарантування інформаційної безпеки індивіда необхідно усунути таке явище, як інформаційна нерівність (дискримінація). Інформаційна дискримінація постає як багатовимірне явище, що охоплює: соціально-економічний аспект (нездатність отримати доступ до передових технологій не тільки для задоволення особистих потреб, але й для самозахисту та своєчасного отримання важливої інформації), який є найбільшою проблемою; віковий аспект (пов’язаний із тривалим впливом певних ідеологічних установок, що призводить до відсутності мотивації до перманентного здобуття нових знань, умінь, навичок, що спостерігається навіть серед частини молоді; це вимагає створення умов та постійної стимуляції людей до усвідомленого розвитку); мовний аспект (переважна більшість інформаційного контенту та програм в мережі Інтернет представлена англійською мовою); фізичний аспект (значна частина вебсайтів та програмного забезпечення не адаптована для осіб із порушеннями слуху, зору тощо) та низку інших складових. Подальше формування науковцями концептуального бачення щодо правового регулювання у сфері інформаційної безпеки як компоненту національної безпеки, яке б передбачало зважений підхід до інтересів індивіда, соціуму та держави, розглядається як одне з найактуальніших завдань сучасної правової науки [19, с. 49].

Адміністративне право відіграє важливу роль у формуванні ефективної системи забезпечення інформаційної безпеки. Основними механізмами

регулювання є:

1. Ліцензування та сертифікація. Держава встановлює обов'язкові вимоги до суб'єктів господарювання, які надають послуги у сфері телекомунікацій, зокрема щодо захисту інформації.

2. Контроль і нагляд. Органи державної влади, такі як Державна служба спеціального зв'язку та захисту інформації України, здійснюють моніторинг дотримання норм законодавства у сфері інформаційної безпеки.

3. Адміністративна відповідальність. Кодекс України про адміністративні правопорушення передбачає відповідальність за порушення правил зберігання та обробки інформації (наприклад, стаття 188-39) [26].

4. Освітні та просвітницькі заходи. Адміністративні органи активно працюють над підвищенням рівня обізнаності громадян і суб'єктів господарювання щодо правил поведінки в інформаційному середовищі.

На базі Стратегії національної безпеки України [27], Президентом країни була схвалена Доктрина інформаційної безпеки України [28], яка слугувала фундаментальною основою для національної політики у цій царині. Основна мета цієї Доктрини полягає у конкретизації засад формування та впровадження державної інформаційної політики, зокрема у контексті протидії руйнівному впливу з боку рф в умовах гібридної війни, яку вона розпочала. Документ визначає національні інтереси України у сфері інформації, загрози, що стоять на заваді їх реалізації, а також ключові напрямки та пріоритети державної політики у цій важливій галузі [29, с. 200].

Варто зазначити, що важливою складовою адміністративно-правового механізму є створення умов для міжнародного співробітництва у сфері кібербезпеки. Україна є учасником Будапештської конвенції про кіберзлочинність, що дозволяє ефективно взаємодіяти з іншими державами у боротьбі з кіберзагрозами.

На думку М. Т. Гаврильців, нормативно-правове врегулювання становлення єдиного інформаційного простору на території України має стимулювати збалансований розвиток як інформаційних надбань, так і послуг та

продукції у цій сфері по всій державі. Вагомість проблеми вдосконалення законодавства стосовно інформаційних питань та безпеки, а також розбудови інформаційного соціуму зумовлена значним впливом правових норм цієї галузі на регулювання взаємовідносин суб'єктів у всіх сферах життєдіяльності країни [29, с. 200].

Отож, попри існування розвиненої нормативно-правової бази, у сфері забезпечення інформаційної безпеки залишається низка проблем. Серед основних викликів можна виділити:

1. Швидкий розвиток технологій. Законодавство не завжди встигає адаптуватися до нових викликів, таких як штучний інтелект, Інтернет речей або блокчейн-технології.

2. Недостатній рівень технічного оснащення державних органів для протидії сучасним кіберзагрозам.

3. Низький рівень цифрової грамотності населення, що створює умови для поширення дезінформації та шахрайства.

Для вирішення цих проблем необхідно вдосконалювати законодавство з урахуванням міжнародного досвіду, розвивати інституційну спроможність органів державної влади та посилювати співпрацю між державою, бізнесом і громадянським суспільством.

Отже, інформаційна безпека є невід'ємною складовою адміністративного права, яка спрямована на захист національних інтересів в умовах цифрової трансформації суспільства. Ефективне правове регулювання цієї сфери потребує комплексного підходу, що поєднує законодавчі ініціативи, адміністративні механізми та міжнародне співробітництво. Лише за таких умов можна забезпечити належний рівень захищеності інформаційного середовища та створити передумови для сталого розвитку суспільства в епоху цифровізації.

1.3. Загрози інформаційній безпеці в контексті національної безпеки України

Слід наголосити, що розвиток інформаційних технологій і передача даних у віртуальному просторі сприяють підвищенню якості інформаційних процесів, а також забезпечують вищий рівень конкурентоспроможності та ефективності функціонування багатьох сфер суспільного життя. Водночас такий прогрес супроводжується низкою негативних наслідків, серед яких особливо варто відзначити втрату важливої інформації, збереженої в електронному форматі, а також поширення такого небезпечного явища, як кіберзлочинність. Зростання кількості кіберінцидентів створює загрозу не лише для окремих осіб, але й для національної безпеки держави. Кібератаки дедалі частіше стають інструментами політичного й економічного тиску, а в умовах серйозних криз можуть використовуватися як засіб впливу поряд із традиційними методами військової сили (наприклад, така тактика застосовується російською федерацією у війні проти України).

Забезпечення інформаційної безпеки є надзвичайно важливим і специфічним напрямом діяльності, що потребує чіткого та детального правового регулювання. Варто зазначити, що нині інформаційна безпека розглядається як фундаментальна складова інформаційного суспільства. Цей факт підтверджується тим, що на регіональному рівні та на рівні окремих держав спостерігається зростання уваги до питань інформаційної безпеки та відповідного правового забезпечення цієї сфери. Україна, у свою чергу, також приділяє значну увагу цим аспектам.

Інформаційна безпека є невід'ємною складовою національної безпеки кожної держави. В умовах сучасного світу, коли інформаційні технології проникають у всі сфери життя, забезпечення захисту інформаційного простору стає одним із ключових завдань державної політики. Для України, яка перебуває в умовах гібридної війни, питання інформаційної безпеки набувають особливої

актуальності. У цій статті розглянуто основні загрози інформаційній безпеці України та їхній вплив на національну безпеку.

Інформаційна безпека визначається як стан захищеності інформаційного середовища, що забезпечує недоторканність, доступність і цілісність інформації, а також захист прав суб'єктів інформаційних відносин. У контексті національної безпеки це поняття охоплює як захист державних інформаційних ресурсів, так і протидію зовнішнім і внутрішнім загрозам, спрямованим на дестабілізацію суспільно-політичної ситуації, маніпуляцію свідомістю громадян та підрив довіри до державних інституцій.

Інформаційна безпека є багатогранним утворенням, що має зв'язки різного рівня та систему стейкхолдерів. Її можна розглядати з кількох боків: 1) як незалежне явище суспільно-державного значення; 2) як фундамент для прогресу політичних, соціальних, економічних та культурних аспектів суспільства; 3) стабільність політична та економічна всередині держави слугує інструментом (ресурсом) для розвитку інформаційної структури суспільства. Загрози щодо інформаційної безпеки походять як ззовні, так і зсередини. Несприятливий вплив на цю сферу у більшості випадків ставить під загрозу економічну та політичну системи суспільства (особливо під час електоральних кампаній). Лише нещодавно науковці та владні структури почали приділяти належну увагу саме цим останнім аспектам (порівняно з безпекою на державному рівні), що частково зумовлене ухваленням відповідної профільної законодавчої бази [19, с. 49].

Україна, як держава, що перебуває у стані збройного конфлікту з російською федерацією, стикається з численними викликами в інформаційному просторі. Ворожі інформаційні операції спрямовані не лише на дискредитацію української влади, але й на формування негативного іміджу України на міжнародній арені. У таких умовах забезпечення інформаційної безпеки стає стратегічним завданням для збереження суверенітету та територіальної цілісності країни.

Згідно з баченням Н. І. Верхоглядової та І. В. Кононової, експансія росії у сфері інформації та культури, а також її ідеологічний наступ, що

розповсюджуються через глобальні телекомунікаційні системи, є джерелом занепокоєння для багатьох світових держав. Загроза потрапляння в залежність та потенційна втрата суверенітету хвилюють як очільників країн, так і громадські організації та пересічних громадян. Відтак, на часі першочерговим завданням для держави постає охорона власної культури, спадщини та духовних надбань від деструктивного інформаційного тиску, а також розбудова дієвого механізму гарантування інформаційної безпеки. Відстоюючи свої інформаційні переваги, кожна нація зобов'язана дбати про власний інформаційний захист. Ця вимога також випливає з потреби у зміцненні української державності. Зважена державна стратегія України формується як невід'ємна частина її соціоекономічної програми, базуючись на першості національних пріоритетів та загроз, що стоять перед державною безпекою. [16, с. 384].

До складу інформаційних надбань входять: фонди бібліотек, матеріали архівів, відомості науково-технічного характеру, юридично значуща інформація, дані від державних органів, інформація по галузях, фінансово-господарські відомості, відомості про природні скарби, а також дані, що містяться у розпорядженні установ та фірм. Інформаційні активи постають одним із ключових результатів функціонування інформаційна орієнтованого соціуму. Ці інформаційні надбання класифікують на дві категорії: класичні та цифрові. До класичних належать друковані матеріали, картографічні зображення тощо. Цифрові ж – це усяка інформація, зафіксована у форматі комп'ютерних файлів [16, с. 387].

Як підкреслює М. Т. Гаврильців, протягом останніх двадцяти п'яти років світ пережив безпрецедентне прискорення у розвитку мереж, що поєднує у собі комп'ютери та соціальні комунікації, явище, яке можна назвати винятковим. Людство увійшло у фазу інформаційного суспільства, де відомості набули статусу ключового елементу у численних життєвих аспектах. Нині практично не існує сфери соціальної взаємодії, яка б не відчула впливу ІТ: від політики та юриспруденції до економіки, охорони здоров'я, освіти, культури, віросповідання, обслуговування та дозвілля. Попит на інструменти для

накопичення, структурування, збереження, пошуку, передачі даних та гарантування їхньої захищеності постійно наростає [29, с. 200].

Ситуацію загострює той факт, що інформаційний компонент є неминучим об'єктом маніпуляцій у контексті гібридних конфліктів. Адже складна геополітична обстановка, в якій опинилася Україна протягом останніх шести років, і перманентне погіршення образу країни на світовій арені зумовлені цілою низкою факторів, серед яких неналежний стан системи захисту інформації відіграє суттєву роль. Деякі експерти взагалі стверджують, що в Україні як такої не існує системи інформаційної безпеки, здатної якісно ідентифікувати, аналізувати інформаційні виклики національній безпеці, а також ефективно протистояти їм [29, с. 200].

Основними загрозами інформаційній безпеці України можна назвати такі:

1. Кібератаки та шкідливе програмне забезпечення. Однією з найбільш поширених загроз є кібератаки на державні установи, інфраструктурні об'єкти та приватний сектор. Такі атаки можуть мати різні цілі: від викрадення конфіденційної інформації до паралізації критично важливих систем. Відомими прикладами є атаки на енергетичну систему України у 2015–2016 роках, які призвели до масштабних перебоїв у подачі електроенергії, а також інші випадки, які вчинялись стосовно операторів зв'язку, банківської системи, Укрзалізниці тощо.

Шкідливе програмне забезпечення, зокрема віруси-шифрувальники (наприклад, NotPetya), використовується для завдання економічних збитків та створення хаосу. Відсутність належного рівня кіберзахисту в багатьох державних структурах лише посилює ризики.

Згідно з поглядами Н. С. Грабар, сучасна система автоматизованої обробки відомостей постає як складна конструкція, що складається із значної кількості елементів із різним рівнем самостійності, які взаємопов'язані та здійснюють обмін даними. Фактично кожен елемент може зазнати зовнішнього втручання або вийти з ладу. Усі складники автоматизованої системи можна класифікувати за такими групами:

– апаратне забезпечення – сюди входять обчислювальні машини та їхні складові (центральні процесори, дисплеї, термінали, периферійні пристрої, як-от накопичувачі, друкарські апарати, контролери, сполучні кабелі, комунікаційні лінії тощо);

– програмне забезпечення – придбані прикладні програми, вихідні тексти, об’єктні коди, завантажувальні блоки; операційні системи та системні утиліти (компілятори та аналогічні);

– дані – інформація, збережена у тимчасовому чи постійному режимі, на магнітних носіях, у роздрукованому вигляді, архівні копії, системні журнали обліку та ін.;

– людський чинник (персонал) – як обслуговуючий персонал, так і кінцеві користувачі [1].

Водночас, Т. П. Яцик та О. М. Бодунова звертають увагу на те, що з поширенням комп’ютеризованих систем та автоматизованих засобів, усе поступово змістилося у сферу ІТ. Первинно, захист інформації зводився до обмеження доступу до фінансових даних, різноманітної документації, патентної інформації та подібного. Однак XXI століття принесло нам ІТ-бум: комп’ютери стали невід’ємною частиною кожного помешкання, а доступ до мережі Інтернет був офіційно визнаний правом людини резолюцією ООН від 2016 року. Із наростанням кількості пристроїв, "розумних" речей, збільшенням обсягів трафіку та потоків даних, люди почали масово переносити у віртуальний простір такі сфери, як облік, управління процесами та виконання робіт. Таким чином, виникла гостра потреба у забезпеченні захисту інформації саме у цифровому кіберсередовищі [30, с. 74-76].

Ґрунтуючись на порівнянні результатів аналізу проблем, пов’язаних із визначенням термінів «кібербезпека» та «інформаційна безпека», вчені констатують: кібербезпека є окремим вектором у межах інформаційної безпеки, виникнення якого прямо пов'язане із застосуванням обчислювальних систем та/або мереж зв’язку. Слідуючи думці науковців, варто розглядати кібербезпеку як такий ступінь захищеності критично важливих інтересів індивіда, соціуму та

держави в умовах експлуатації комп'ютерних систем та/або телекомунікаційних мереж, при якому ризик завдання шкоди мінімізується через: неповноту, запізнення чи недостовірність застосовуваної інформації; ворожий інформаційний вплив; негативні результати роботи інформаційних технологій; а також несанкціоноване поширення, використання та порушення забезпечення цілісності, конфіденційності та доступності даних [30, с. 74-76].

2. Інформаційно-психологічні операції. Так, російська федерація активно використовує методи інформаційно-психологічного впливу для маніпуляції свідомістю громадян України. Ці операції включають поширення фейкових новин, пропагандистських матеріалів, а також створення та підтримку конфліктів у суспільстві на основі мовних, етнічних чи релігійних відмінностей.

Потужним інструментом таких операцій є соціальні мережі, які дозволяють швидко поширювати дезінформацію серед широкої аудиторії. Особливо небезпечними є спроби впливу на виборчі процеси в Україні через маніпуляцію громадською думкою.

Ключовим елементом сучасної системи державності, охоплюючи її політичні, військові, фінансові, енергетичні та інші грані – тобто усі складові стабільного збалансованого поступу країни та нації, на сьогоднішній день є безпека інформаційна. Поява таких нових загроз та викликів спонукає державу до формування на загальнонаціональному рівні основоположних настанов щодо гарантування інформаційної захищеності. З огляду на прогрес у сфері технологій обробки даних та зростаючу вагу самої інформації, на перший план виходять завдання щодо вироблення методологій оцінки інформаційного складника економічної стійкості. [16, с. 389].

У нинішніх воєнно-політичних обставинах, вважають Д. В. Смотрич та Л. Браілко, заперечувати значення інформації як засобу протиборства, по суті – зброї, складно і навіть недоречно. Інформація дає змогу здобувати перемогу у конфліктах та політичних кризах зовсім без застосування зброї, розпалюючи та створюючи внутрішні розколи. Подібна стратегія властива новітнім видам воєн – гібридним, де прямий військовий аспект є лише частиною загальної картини

[31, с. 122].

Дослідники підкреслюють, що у ситуації, коли весь масив інформації спрямований на маніпулювання загальною думкою, світоглядом індивіда, і подається з використанням фізіологічних та психологічних прийомів і способів її сприйняття, на перший план виходить проблема недостатнього рівня інформаційної грамотності. Це, своєю чергою, призводить до ослаблення здатності людини до критичного осмислення, що робить аналіз та оцінка здобутих відомостей вкрай важливими [31, с. 122].

Аспекти інформаційної безпеки та культури в умовах бойових дій є питанням життєздатності як індивіда, так і соціуму та держави загалом. Адже гарантування інформаційної безпеки визначається не лише державними інтересами, а й потребами приватної особи у контексті захисту її прав та вольностей. Фундаментом сучасної інформаційної безпеки виступають непорушність даних, можливість доступу до потрібної інформації, а також збереження конфіденційності та надійності її зберігання [31, с. 122].

3. Недостатня правова регламентація. Законодавча база України у сфері інформаційної безпеки поступово розвивається, однак досі залишається недостатньо ефективною для протидії сучасним викликам. Зокрема, існує потреба в удосконаленні нормативно-правових актів, що регулюють діяльність у сфері кіберзахисту, а також у створенні механізмів оперативного реагування на нові загрози.

За думкою Л. Чистоклетова та С. Обрембальського, уважне ведення інформаційної роботи та коректне імплементування ключових міжнародно-правових актів, особливо у часи російської навали, здатні значно посилити спроможність держави у плані гарантування інформаційної безпеки. Конкретно, залучення інформаційних технік здатне примножити потенціал у сфері забезпечення обороноспроможності нації. Інтенсивне впровадження ІТ-рішень сприяє Україні у проведенні інформаційної дуелі з російською стороною, досягненні стратегічних завдань та зміцненні життєво важливих інтересів держави [32].

Водночас, науковці підкреслюють, що дані (у вигляді інформації) становлять собою невід'ємний елемент людського існування, адже сама особистість являє собою певну концентрацію відомостей. Початок життєдіяльності – це злиття генетичного коду. Розвиток індивіда відбувається через акумуляцію, застосування та обмін відомостями. Весь життєвий шлях людини, як складу елемента інформаційного суспільства, немислимий поза межами інформаційного простору. Людина виступає як джерело, контрагент, зберігач та транслятор даних. Однак, попри те, що інформація настільки тісно переплетена з буттям людини, нечасто хтось ретельно роздумує над її природою, функцією та вагомістю. Переважна більшість громадян у щоденному режимі під «інформацією» розуміє здобуття звітів, доступ до конкретних фактів та усвідомлення власних «прав на дані» [32].

Обставини, в яких наразі перебуває Україна, змушують нас переосмислити наші погляди на захищеність інформаційного середовища. Якщо до лютого 2022 року оточення видавалося нам задовільно безпечним, то нинішні труднощі породжують суттєво більше небезпек, аніж у мирний час. Дія російського пропагандистського апарату простежується не лише на рівні окремих індивідів чи спільнот, а й на рівні цілих державних утворень. Психологічний тиск реалізується за допомогою медіа-каналів, причому в основі цього тиску лежать методи, що оперують поверхневим сприйняттям. Сучасна ситуація демонструє, що регулярні інформаційні наступи, залучення ботів та фальсифікація контенту (створення «фейків») виявляються ефективними інструментами для дезорієнтації, залякування, маніпулювання настроями та розповсюдження паніки серед населення. Спеціально сконструйовані інформаційні потоки мимоволі впливають на те, як сприймаються дані, змушуючи людей приймати їх за істину [32].

4. Відсутність культури інформаційної безпеки. Ще однією суттєвою проблемою є низький рівень обізнаності громадян щодо основ інформаційної гігієни. Багато користувачів не знають, як розпізнати фейкову інформацію або захистити свої персональні дані в Інтернеті. Це створює сприятливе середовище

для поширення дезінформації та кіберзлочинності.

Як підкреслює Є. Кобко, створення сучасної системи цінностей (тобто інформаційної культури) та її інтеграція у суспільство послугують основою для забезпечення безпеки інформаційної сфери як для особи, так і для держави. Проте, такий підхід дає повний ефект лише у межах кордонів держави, адже, як відомо, небезпеки часто виникають і за її межами. Галузь інформаційної безпеки охоплює два головні напрями: захист інформаційних активів (як державних, так і приватних) та оборона від інформаційного впливу (що стосується здебільшого окремих громадян чи певних спільнот). Наразі першочерговим завданням для України є вироблення стратегій та імплементація єдиної державної політики у цій сфері. Від якості цієї інформаційної політики залежить не лише розвиток окремих секторів, а й ступінь демократичності суспільства. Немає чітко визначеної державної інформаційної стратегії та оцінки реальних можливостей держави у цій галузі ускладнює відстоювання інформаційних інтересів суспільства та сприяє успішним інформаційним атакам з боку як внутрішніх, так і зовнішніх опонентів [19, с. 49].

Одна з визначальних рис гарантування інформаційної безпеки у функціонуючій автоматизованій системі, на думку Н. С. Грабар, полягає у тому, що абстрактні поняття, як то інформація, об’єкти та суб’єкти системи, знаходять своє матеріальне вираження у комп’ютерному середовищі:

– для представлення відомостей – це апаратні засоби зберігання даних, як-от зовнішні пристрої ЕОМ, оперативна пам’ять, файлові структури та інше;

– об’єктами системи вважаються пасивні елементи системи, які зберігають, приймають або передають інформацію. Доступ до такого об’єкта рівнозначний доступу до даних, що в ньому містяться;

– суб’єктами ж системи є активні компоненти, здатні ініціювати переміщення інформації від об’єкта до суб’єкта або спричинити зміну загального стану системи. У ролі суб’єктів можуть виступати як люди-користувачі, так і активні програмні комплекси чи процеси [1].

Для ефективного забезпечення інформаційної безпеки необхідно

реалізувати комплекс заходів на державному, інституційному та індивідуальному рівнях.

Передусім, це удосконалення законодавства. Україна повинна продовжувати роботу над гармонізацією свого законодавства із міжнародними стандартами у сфері кібербезпеки та захисту інформації. Прийняття нових законів і внесення змін до чинних нормативно-правових актів мають забезпечити чітке регулювання відповідальності за порушення у сфері інформаційної безпеки.

Водночас, подальшого розвитку потребує інфраструктура кібербезпеки. Необхідно створити сучасну інфраструктуру для моніторингу та реагування на кіберзагрози. Це включає розширення можливостей державних органів, таких як Державна служба спеціального зв'язку та захисту інформації України, а також залучення приватного сектору до спільної роботи у сфері кіберзахисту.

Важливе значення має освіта та підвищення обізнаності. Важливим напрямом є просвітницька робота серед населення щодо питань інформаційної гігієни та кібербезпеки. Впровадження освітніх програм у школах і вищих навчальних закладах сприятиме формуванню культури безпечного використання інформаційних технологій.

Окрім того, надзвичайно важливою є протидія дезінформації. Для боротьби з дезінформацією необхідно створити ефективні механізми виявлення фейкових новин і їхнього спростування. Держава має підтримувати незалежні медіа та забезпечувати доступ громадян до достовірної інформації.

Отже, інформаційна безпека є ключовим елементом системи національної безпеки України, особливо в умовах сучасної гібридної війни. Загрози в цій сфері мають багатовимірний характер і потребують комплексного підходу до їхньої нейтралізації. Лише завдяки поєднанню зусиль держави, бізнесу та громадянського суспільства можливо забезпечити належний рівень захисту інформаційного простору України та зміцнити її суверенітет і стабільність.

Забезпечення інформаційної безпеки – це не лише питання технологій, але й свідомості кожного громадянина щодо важливості захисту інформації та

критичного мислення у сприйнятті будь-якої інформації. Лише спільними зусиллями можна протистояти сучасним викликам і гарантувати стабільний розвиток українського суспільства в умовах глобалізованого світу.

Натомість, у результаті проведеного дослідження, присвяченого теоретико-правовим та методологічним основам інформаційної безпеки, було досягнуто низки важливих висновків, які мають значення для подальшого розвитку цієї сфери і в науковій, і в практичній площинах.

По-перше, з'ясовано, що інформаційна безпека є багатогранним явищем, що охоплює технічні, правові, соціальні та етичні аспекти. Аналіз правових норм дозволяє стверджувати, що інформаційна безпека виступає не лише як елемент національної безпеки, але й як самостійний об'єкт правового регулювання. Це зумовлює необхідність удосконалення законодавства в цій сфері з урахуванням динамічного розвитку інформаційних технологій.

По-друге, дослідження підтвердило, що теоретико-правові підходи до забезпечення інформаційної безпеки базуються на принципах верховенства права, захисту прав людини, співвідношення свободи інформації та її обмеження в інтересах національної безпеки. Особливу роль відіграють міжнародні стандарти, гармонізація яких із національним законодавством є основою для забезпечення ефективного правового регулювання у сфері кібербезпеки.

По-третє, у ході аналізу було виявлено, що дослідження інформаційної безпеки вимагає міждисциплінарного підходу, який поєднує юридичну, технічну, соціологічну та економічну складові. Методологія дослідження повинна враховувати не лише аналіз чинного законодавства, але й прогнозування ризиків, моделювання загроз та розробку превентивних заходів.

По-четверте, сучасне правове регулювання інформаційної безпеки стикається з рядом викликів, серед яких: відсутність єдиної термінології, недостатня узгодженість між національними та міжнародними нормами, швидкий розвиток кіберзагроз, що випереджає адаптацію законодавства. Це потребує створення комплексного правового механізму, здатного оперативно реагувати на нові виклики.

По-п’яте, встановлено, що інформаційна безпека є ключовим елементом функціонування правової держави в умовах цифровізації суспільства. Її забезпечення сприяє захисту прав і свобод громадян, зміцненню демократичних інститутів та підтримці економічної стабільності. Тому питання інформаційної безпеки повинні залишатися пріоритетними у державній політиці.

Отже, можна стверджувати, що забезпечення інформаційної безпеки є комплексним завданням, яке вимагає системного підходу та консолідації зусиль науковців, законодавців і практиків. Ефективне правове регулювання у цій сфері є запорукою сталого розвитку суспільства та держави в умовах сучасних глобальних викликів.

РОЗДІЛ 2
АДМІНІСТРАТИВНО-ПРАВОВІ МЕХАНІЗМИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

2.1. Державна політика у сфері інформаційної безпеки: стратегічні напрями та принципи реалізації

У сучасному світі інформаційна безпека набуває все більшого значення як ключовий елемент забезпечення національної безпеки. Інформаційний простір є стратегічною сферою, яка впливає на політичну стабільність, економічний розвиток, обороноздатність та соціальну згуртованість держави. Україна, як держава, що перебуває в умовах гібридних загроз, зокрема з боку агресивних інформаційних впливів, змушена приділяти особливу увагу розробці та реалізації ефективної державної політики у сфері інформаційної безпеки.

Як зауважують С. Є. Антонова та Г. Ф. Мартинюк, впровадження передових інформаційно-комунікаційних технологій (ІКТ) є фундаментальною засадою для соціально-економічного та науково-технічного поступу – по суті, для інформатизації суспільства. Така інформатизація допомагає гарантувати національні пріоритети, підвищувати ефективність праці, збагачувати культурне життя та сприяти подальшому поглибленню демократичних засад у суспільстві. У нинішній глобальній ситуації розвиток суспільної інформатизації відбувається досить інтенсивно, що, своєю чергою, змушує приділяти дедалі більше уваги питанням, пов'язаним із гарантуванням інформаційної безпеки як для кожного громадянина, так і для держави загалом. У зв’язку з цим, вирішальне значення набуває якісне та дієве втілення державної інформаційної стратегії, фокусом якої є охорона інформаційного середовища країни [34].

Загалом, політика інформаційної безпеки як суспільний феномен є багатогранною, охоплюючи внутрішньо- та зовнішньополітичні аспекти, економічні, технологічні, військові та інші складові, що вимагає відповідного комплексного підходу. Дії державних владних структур мають бути зорієнтовані

на виконання конкретних завдань у цій сфері та об’єднані спільною метою – створення належних умов для гарантування інформаційної безпеки України [29, с. 200].

Стратегічними напрямами державної політики у сфері інформаційної безпеки варто назвати:

1. Захист національного інформаційного простору. Одним із ключових пріоритетів є створення умов для запобігання деструктивному впливу на національний інформаційний простір. Це передбачає протидію пропаганді, дезінформації, маніпулятивним технологіям та іншим формам інформаційного впливу, які можуть зашкодити державним інтересам. Для цього необхідно розвивати інструменти моніторингу медіа, соціальних мереж та інших цифрових платформ.

2. Кібербезпека як складова інформаційної безпеки. Інформаційна безпека нерозривно пов'язана із захистом критичної інформаційної інфраструктури, включаючи державні реєстри, системи управління, енергетичні мережі та фінансову систему. Це вимагає впровадження сучасних технологій кіберзахисту, розробки національних стандартів кібербезпеки та створення системи оперативного реагування на кіберінциденти.

3. Розвиток медіаграмотності населення. Одним із ключових аспектів протидії інформаційним загрозам є підвищення рівня медіаграмотності громадян. Інформоване суспільство здатне критично оцінювати інформацію, що надходить із різних джерел, і протистояти маніпулятивним впливам. Держава має сприяти впровадженню освітніх програм у школах, вишах та через громадські ініціативи.

4. Регулювання інформаційного простору. Ефективне регулювання медіа та цифрових платформ є важливим елементом забезпечення інформаційної безпеки. Законодавство має бути адаптоване до нових викликів цифрової епохи, враховуючи баланс між свободою слова та необхідністю захисту національних інтересів.

5. Міжнародна співпраця у сфері інформаційної безпеки. Інформаційні

загрози мають глобальний характер, тому їх подолання вимагає тісної співпраці з міжнародними партнерами. Україна повинна активно долучатися до ініціатив Європейського Союзу, НАТО та інших міжнародних організацій у сфері кібербезпеки та боротьби з дезінформацією.

Натомість, доречно погодитись з М. Т. Гаврильців у тому, що державна інформаційна політика в умовах глобалізаційних процесів матиме ефективний вигляд лише тоді, коли вона буде мати комплексний та системний характер, будучи, безумовно, відкритою та спрямованою на забезпечення інтересів громадян, суспільства загалом та держави [29, с. 200].

Державна стратегія щодо забезпечення інформаційної безпеки країни, яка охоплює ключові вектори роботи органів державної виконавчої влади у цій галузі, націлена на збереження національних інтересів держави, соціуму та індивіда. Базуючись на цьому, головна її мета полягає у зменшенні потенційної шкоди, спричиненої застосуванням неповної, запізнілої або неправдивої інформації, або ж негативним інформаційним впровадженням за допомогою інформаційних технологій, а також запобіганні несанкціонованому поширенню відомостей. Саме з огляду на це, інформаційна безпека досягається через функціонування визначених державних інституцій та умов, у яких існують її суб’єкти, що регламентовані як міжнародними, так і вітчизняними правовими актами [34].

Важливо звернути увагу на принципи реалізації державної політики у сфері інформаційної безпеки. Насамперед, це принцип законності. Усі заходи у сфері інформаційної безпеки мають базуватися на законодавстві України та відповідати міжнародним правовим нормам. Це забезпечує легітимність дій держави та сприяє довірі громадян до відповідних ініціатив.

Прозорість і підзвітність є не менш важливим принципом, адже реалізація політики у сфері інформаційної безпеки повинна бути відкритою для суспільства. Громадяни мають право знати про заходи, які вживаються для захисту їхніх прав в інформаційному просторі.

Необхідно акцентувати на принципі балансу між свободою слова та

безпекою. Свобода слова є фундаментальною цінністю демократичного суспільства. Водночас держава має право і обов'язок обмежувати діяльність, яка загрожує національній безпеці. Цей баланс має бути чітко визначений у законодавстві.

Вагомість інноваційності є беззаперечною. Інформаційні загрози постійно еволюціонують, тому держава повинна активно впроваджувати новітні технології для їх нейтралізації. Це стосується як технічних рішень, так і методів аналізу та прогнозування загроз.

Окремий аспект складає співпраця між державою і суспільством. Ефективна реалізація політики можлива лише за умови активної участі громадянського суспільства, експертного середовища та приватного сектору. Держава має створювати умови для діалогу та партнерства.

Сучасна епоха комп'ютеризації суттєво змінила підходи до роботи з інформацією, а також вимоги до забезпечення її безпеки. Інформаційна безпека сьогодні набула значення, яке є не менш важливим, ніж фізичний захист ресурсів. Це обумовлює стрімке зростання дослідницької активності у сфері інформаційної безпеки.

В умовах сьогодення рівень безпеки суспільства значною мірою залежить від захищеності інформаційних систем, якими користується людина. Забезпечення безпеки таких систем має ґрунтуватися на принципах конфіденційності, цілісності та доступності. Зважаючи на те, що економіки провідних країн світу дедалі більше залежать від інформаційних технологій і глобальної мережі Інтернет, інформаційна безпека стає ключовим пріоритетом як для окремих громадян, так і для організацій, підприємств та держав загалом. Це зумовлює зростання інвестицій у розробку програмного забезпечення для автоматичного резервного копіювання даних, створення антивірусних програм, брандмауерів, складних систем шифрування, а також засобів виявлення несанкціонованого доступу.

Однак результати досліджень свідчать про наявність значного рівня загроз. Наприклад, згідно з даними дослідження Power (2001), 91% респондентів

зафіксували порушення комп'ютерної безпеки протягом року [35, с. 33]. Хоча ці дані датуються початком XXI століття, сучасна ситуація залишається далекою від ідеальної. Основною причиною цього є недостатнє усвідомлення критичної важливості інформаційної безпеки та неадекватне фінансування заходів із її забезпечення відповідно до масштабів загроз. Таким чином, вимоги до інформаційної безпеки залишаються невирішеними, особливо в умовах глобалізованого електронного середовища.

Значущість інформаційної безпеки в контексті комп'ютерних технологій стимулювала розвиток наукових досліджень у таких напрямах, як технічний захист даних, забезпечення конфіденційності, виявлення несанкціонованого втручання та правове регулювання цієї сфери. Окремим аспектом досліджень є запобігання правопорушенням у сфері інформаційної безпеки та розробка економічних моделей для оцінки ефективності інвестицій у цю галузь. Увага до економічних аспектів дозволяє визначити оптимальні обсяги фінансування заходів із забезпечення інформаційної безпеки та підвищити їхню ефективність. У цьому контексті заслуговують на увагу праці таких науковців як: П. Д. Біленчук [36], І. В. Арістова [37], А. В. Войціховський [38, с. 281-288], В. А. Ліпкан [39], О. А. Баранов [40], В. П. Горбулін, М. М. Биченок [41], В. К. Конах [42], А. І. Марущак [43, с. 36-41] та ін.

Для гарантування економічної стійкості компанії, вважають В. А. Нехай та В. В. Нехай, необхідно впровадити комплекс заходів, спрямованих на протидію як можливим, так і вже існуючим небезпекам. Розробка проактивних кроків для усунення чи зменшення цих загроз має дозволити господарському агенту успішно функціонувати в умовах мінливого зовнішнього й внутрішнього середовища. Варто зазначити, що захист на рівні підприємства має охоплювати низку ключових сфер: фінансову, технологічну, цифрову, кадрову, соціальну, екологічну, фізичний захист та інші аспекти [44, с. 137-140].

Ключовою складовою діяльності з охорони інформаційних активів організації є процес ідентифікації, аналізу ризиків та превентивні дії стосовно

загроз, що стосуються інформаційно-комунікаційних мереж та накопичених даних. Актуальна система корпоративного захисту інформації націлена на збереження конфіденційності відомостей від несанкціонованого перегляду, унеможливлення шкідливих чи ненавмисних модифікацій (збереження цілісності) та надання коректного рівня доступу. Гарантування інформаційної недоторканності реалізується через поєднання трьох головних складових: технічних рішень, управлінських регламентів та організаційних процедур [44, с. 137-140].

Отже, в сучасному бізнес-середовищі, де цифрові технології набули всесвітнього значення, захист інформації стає невід'ємною частиною загальної системи економічної безпеки як окремого суб'єкта господарювання, так і держави в цілому [44, с. 137-140].

Отже, державна політика у сфері інформаційної безпеки є невід'ємною складовою забезпечення суверенітету України в умовах сучасних викликів. Її успішна реалізація потребує комплексного підходу, який включає як стратегічне планування, так і дотримання принципів законності, прозорості та інноваційності. Лише за таких умов можна гарантувати захист національних інтересів в інформаційному просторі та забезпечити стійкість держави до зовнішніх і внутрішніх загроз.

2.2. Повноваження органів державної влади у забезпеченні інформаційної безпеки

Інформаційне суспільство, зважаючи на його багатогранність у процесах формування та розвитку, охоплює численні аспекти державної політики у різних сферах, таких як економіка, освіта, наука, оборона тощо. Однією з ключових умов створення інформаційного суспільства є забезпечення інформаційної безпеки, що виступає невід'ємною складовою національної безпеки України. У цьому контексті науковці підкреслюють, що відповідно до Конституції України забезпечення інформаційної безпеки є однією з основних функцій держави [45,

с. 46-47].

Інформаційна безпека є однією з ключових складових національної безпеки держави, що визначає її здатність ефективно функціонувати у сучасному інформаційному просторі. В умовах зростання обсягів інформаційних потоків, розвитку цифрових технологій та підвищення рівня кіберзагроз, забезпечення інформаційної безпеки стає пріоритетним завданням для органів державної влади. У цьому контексті адміністративно-правовий аспект набуває особливого значення, оскільки саме через механізми адміністративного права держава регулює діяльність суб'єктів у сфері інформаційної безпеки.

Варто погодитись з тезою, що висловлюють С. Є. Антонова та Г. Ф. Мартинюк, стосовно того, що державна стратегія щодо забезпечення інформаційної безпеки країни, яка охоплює ключові вектори роботи органів державної виконавчої влади у цій галузі, націлена на збереження національних інтересів держави, соціуму та індивіда. Базуючись на цьому, головна її мета полягає у зменшенні потенційної шкоди, спричиненої застосуванням неповної, запізнілої або неправдивої інформації, або ж негативним інформаційним впровадженням за допомогою інформаційних технологій, а також запобіганні несанкціонованому поширенню відомостей. Саме з огляду на це, інформаційна безпека досягається через функціонування визначених державних інституцій та умов, у яких існують її суб’єкти, що регламентовані як міжнародними, так і вітчизняними правовими актами [34].

Система забезпечення інформаційної безпеки держави є інтегральною складовою загального механізму національної безпеки країни. Вона являє собою сукупність державних органів влади, недержавних формувань та громадян, які зобов’язані злагоджено діяти задля гарантування інформаційної безпеки на основі уніфікованих правових засад, ефективно протистоячи сучасним інформаційним викликам та загрозам [29, с. 202-203].

Органи державної влади, відповідальні за забезпечення інформаційної безпеки, виконують свої функції у межах визначених законодавством повноважень. До таких органів належать:

1. Рада національної безпеки і оборони України (РНБО). РНБО є ключовим координаційним органом у системі забезпечення національної безпеки, включаючи інформаційну. Вона розробляє стратегії та програми, спрямовані на протидію інформаційним загрозам, а також координує діяльність інших органів державної влади у цій сфері.

Правове регулювання діяльності РНБО визначено Законом України «Про Раду національної безпеки і оборони України», який прийнятий 5 березня 1998 року № 183/98-ВР [46].

2. Державна служба спеціального зв'язку та захисту інформації України (ДССЗЗІ). Цей орган здійснює технічний та організаційний захист інформації в державних інформаційних системах. Основними завданнями ДССЗЗІ є розробка стандартів захисту інформації, контроль за їх дотриманням, а також реагування на кіберінциденти, що визначено Законом України «Про Державну службу спеціального зв'язку та захисту інформації України» від 23 лютого 2006 року № 3475-IV [47].

3. Служба безпеки України (СБУ). СБУ виконує функції щодо контррозвідувального захисту у сфері інформаційної безпеки. Зокрема, вона виявляє та нейтралізує загрози, пов'язані з діяльністю іноземних спецслужб, терористичних груп чи інших суб'єктів, які здійснюють деструктивну діяльність у кіберпросторі, що передбачено Законом України «Про Службу безпеки України» від 25 березня 1992 року № 2229-XII [48].

4. Національна поліція України. Поліція займається розслідуванням злочинів у сфері інформаційної безпеки, зокрема кіберзлочинів, а також забезпечує правопорядок у цифровому середовищі. Порядок і підстави цієї діяльності регламентовано Законом України «Про Національну поліцію» від 2 липня 2015 року № 580-VIII [49].

5. Міністерство цифрової трансформації України. Це відносно новий орган виконавчої влади, який відповідає за розвиток цифрової інфраструктури та впровадження інновацій у сфері електронного урядування. Міністерство також бере участь у розробці політик, спрямованих на підвищення рівня кібербезпеки

[50].

6. Інші державні органи. До забезпечення інформаційної безпеки можуть залучатися й інші органи виконавчої влади, залежно від їхньої компетенції. Наприклад, Міністерство оборони України виконує завдання щодо захисту військових інформаційних систем, що визначено [51].

Адміністративно-правові механізми забезпечення інформаційної безпеки включають такі основні інструменти:

1. Ліцензування та сертифікація. Держава здійснює ліцензування діяльності у сфері захисту інформації та сертифікацію технічних засобів захисту. Це дозволяє контролювати якість послуг і продукції, що використовуються для захисту інформації.

2. Контроль і нагляд. Органи державної влади здійснюють контроль за дотриманням законодавства у сфері інформаційної безпеки. Зокрема, проводяться перевірки державних установ та приватних компаній на предмет дотримання вимог із захисту даних.

3. Адміністративні санкції. У разі порушення законодавства у сфері інформаційної безпеки до винних осіб можуть застосовуватися адміністративні санкції, такі як штрафи або припинення діяльності.

4. Розробка та впровадження стандартів. Важливим елементом є розробка державних стандартів у сфері кібербезпеки та захисту інформації. Це дозволяє забезпечити єдність підходів до захисту даних і мінімізувати ризики.

5. Навчання та підвищення кваліфікації. Органи державної влади проводять навчання для своїх працівників і громадян з метою підвищення рівня обізнаності щодо основ кібергігієни та методів захисту інформації.

Попри значний прогрес у розбудові системи забезпечення інформаційної безпеки в Україні, існують певні проблеми, які потребують вирішення: 1) недостатність фінансування (багато державних органів стикаються з обмеженими ресурсами для впровадження сучасних технологій захисту); 2) координація між органами (відсутність чіткої координації між різними органами державної влади може призводити до дублювання функцій або

прогалин у роботі); 3) динамічність загроз (кіберзагрози постійно змінюються, що вимагає від держави гнучкості та швидкого реагування); 4) міжнародна співпраця (в умовах глобалізації кіберзагроз важливою є співпраця з міжнародними організаціями та іншими державами для обміну досвідом і спільного протистояння загрозам.

Отже, забезпечення інформаційної безпеки є складним і багатогранним процесом, який потребує ефективної роботи всіх органів державної влади в межах їхніх повноважень. Адміністративно-правові механізми відіграють ключову роль у регулюванні цієї сфери, створюючи правові підстави для захисту національних інтересів в умовах сучасного інформаційного суспільства. Для подальшого вдосконалення системи необхідно посилювати міжвідомчу координацію, розвивати законодавчу базу відповідно до нових викликів та активно залучати громадськість до процесу формування політики у сфері інформаційної безпеки.

2.3. Міжнародний досвід регулювання інформаційної безпеки

У сучасному світі інформаційна безпека є однією з ключових складових національної та міжнародної безпеки. З огляду на зростання кіберзагроз, глобалізацію інформаційних технологій та їх інтеграцію у всі сфери суспільного життя, питання ефективного регулювання інформаційної безпеки набуває особливої актуальності. У цій статті здійснено порівняльний аналіз міжнародного досвіду у сфері інформаційної безпеки та розглянуто можливості його імплементації в Україні.

У контексті цієї проблематики варто розглянути деякі міжнародні підходи до регулювання інформаційної безпеки.

Так, Європейський Союз активно розвиває правову базу у сфері інформаційної безпеки. Основоположним документом стала Директива Європейського Парламенту і Ради (ЄС) 2016/1148 від 6 липня 2016 року «Про заходи для високого спільного рівня безпеки мережевих та інформаційних

систем на території Союзу [52].

Наступним документом, що замінив попередню директиву стала Директива Європейського Парламенту і Ради (ЄС) 2022/2555 від 14 грудня 2022 року «Про заходи для високого спільного рівня кібербезпеки на всій території Союзу, внесення змін до Регламенту (ЄС) № 910/2014 та Директиви (ЄС) 2018/1972 та скасування Директиви (ЄС) 2016/1148 (Директива NIS 2)» [53]. Суть цієї Директиви зводиться до встановлення оновлених стандартів та вимог для досягнення високого рівня кібербезпеки на всій території Європейського Союзу. Вона передбачає впровадження єдиного підходу до управління ризиками, моніторингу інцидентів, обміну інформацією та координації дій між державами-членами. Основна мета полягає у зміцненні стійкості критичних інфраструктур, забезпеченні надійності цифрових послуг та підвищенні захисту від кіберзагроз. Директива NIS 2 розширює сферу застосування порівняно з попередньою версією, охоплюючи нові сектори та посилюючи вимоги до суб'єктів, які надають важливі послуги. Вона також встановлює чіткі обов'язки для суб'єктів, включаючи обов'язкове повідомлення про інциденти, запровадження заходів з управління ризиками та співпрацю з національними компетентними органами. Крім того, документ спрямований на вдосконалення механізмів реагування на кіберінциденти на рівні Союзу через створення ефективної мережі співпраці між державами-членами та Європейською агенцією з кібербезпеки (ENISA). Таким чином, Директива NIS 2 закладає основу для посилення кіберстійкості та безпеки в умовах постійно зростаючих цифрових загроз.

Директива NIS (Directive on Security of Network and Information Systems), є тією, яка встановлює вимоги до забезпечення кібербезпеки критично важливих інфраструктур, таких як енергетика, транспорт, фінанси та охорона здоров’я. Основними принципами цієї директиви є обов’язковість повідомлення про інциденти, створення національних стратегій кібербезпеки та функціонування команд реагування на інциденти (CSIRT)

Крім того, Загальний регламент про захист даних (GDPR) визначає жорсткі вимоги до обробки персональних даних, що суттєво підвищує рівень захисту

інформації. Важливою особливістю регулювання в ЄС є інтеграція правових норм із технічними стандартами, що забезпечує комплексний підхід до інформаційної безпеки.

Натомість, США мають одну з найрозвиненіших систем регулювання кібербезпеки, яка базується на поєднанні законодавчих актів, виконавчих указів президента та галузевих стандартів. Ключовими документами є Закон про кібербезпеку (Cybersecurity Act) та Національна стратегія кібербезпеки. Особливістю американської моделі є активна участь приватного сектору у забезпеченні інформаційної безпеки, що досягається через партнерство між державою та бізнесом.

Національний інститут стандартів і технологій (NIST) розробив Кібербезпекову структуру (Cybersecurity Framework), яка широко використовується як у державному, так і в приватному секторах. Ця структура базується на ризик-орієнтованому підході і передбачає п’ять основних функцій: ідентифікація, захист, виявлення, реагування та відновлення.

Отож, як підкреслює О. О. Терзі, Сполучені Штати Америки можна вважати лідером у сфері інформаційної безпеки, оскільки вони не лише вперше в історії запровадили електронне урядування з використанням передових технологій, але також розробили унікальну структуру для захисту національного інформаційного суверенітету та безпеки інформаційних ресурсів. Згадувати в першу чергу Сполучені Штати Америки (США), найпотужнішу в політичному, економічному та військовому плані державу, є цілком розумним підходом з огляду на її великий досвід забезпечення інформаційної безпеки [54, с. 54].

Цікавою є китайська модель регулювання інформаційної безпеки, яка відрізняється централізованим підходом. Закон про кібербезпеку КНР передбачає суворий контроль над інтернет-інфраструктурою та діяльністю іноземних компаній у кіберпросторі. Особлива увага приділяється захисту критичної інформаційної інфраструктури, а також моніторингу та цензурі контенту.

Китай активно розвиває власні технологічні стандарти у сфері кібербезпеки, що забезпечує незалежність від західних рішень. Проте така модель викликає критику через обмеження прав і свобод користувачів.

Водночас, Ізраїль є одним із лідерів у сфері кібербезпеки завдяки високому рівню державного управління та інновацій. Національний орган з кібербезпеки Ізраїлю координує діяльність усіх суб'єктів у цій сфері, включаючи військові структури, бізнес і наукові установи. Особливістю ізраїльської моделі є акцент на превентивних заходах, таких як прогнозування загроз і створення технологій для їх нейтралізації.

Як зазначає Л. Д. Куренда, враховуючи глобальний та актуальний характер процесу забезпечення інформаційної безпеки в умовах інформаційного століття, держави-члени ООН розробили уніфіковану термінологію та узгодили зміст основних понять у сфері міжнародного інформаційного співробітництва. Зокрема, поняття “міжнародна інформаційна безпека” визначається як взаємодія суб’єктів міжнародних відносин, спрямована на підтримання стабільного миру шляхом захисту міжнародної інфосфери, глобальної інфраструктури та суспільної свідомості світової спільноти від актуальних і потенційних інформаційних загроз. Термін “інфосфера” охоплює міжнародний інформаційний простір, що включає інформаційні потоки, ресурси та всі аспекти діяльності цивілізації. На підставі цієї дефініції Л. Д. Куренда доходить висновку, що забезпечення міжнародної інформаційної безпеки охоплює три ключові напрямки: технічний аспект, що стосується захисту глобальної інфраструктури; психологічний аспект, який передбачає захист суспільної свідомості світової спільноти; а також аспект, пов’язаний із правами та свободами, що включає захист міжнародної інфосфери [55, с. 37].

Натомість, варто вказати, що нині Україна стикається з унікальними викликами у сфері інформаційної безпеки через гібридну агресію з боку російської федерації, яка включає кібератаки, дезінформацію та маніпуляції громадською думкою. У відповідь на ці загрози Україна поступово формує власну систему регулювання інформаційної безпеки.

Законодавча база України у цій сфері включає Закон «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року № 2163-VIII, який визначає основні напрями державної політики у сфері кібербезпеки [56]. Також діють закони «Про захист інформації в інформаційно-телекомунікаційних системах» від 5 липня 1994 року № 80/94-ВР [57] та «Про доступ до публічної інформації» від 13 січня 2011 року № 2939-VI [58]. Однак українське законодавство потребує подальшої гармонізації з європейськими стандартами.

Важливим кроком стало створення Національного координаційного центру кібербезпеки при РНБО України, який відповідає за координацію дій державних органів у цій сфері. Проте ефективність його роботи обмежується недостатнім фінансуванням та браком кваліфікованих кадрів.

Україна може використати найкращі практики міжнародного регулювання для вдосконалення власної системи інформаційної безпеки:

1. Адаптація європейського законодавства. Прийняття норм, аналогічних Директиві NIS та GDPR, дозволить підвищити рівень захисту критичної інфраструктури та персональних даних. Це також сприятиме інтеграції України до цифрового ринку ЄС.

2. Ризик-орієнтований підхід. Використання американської Кібербезпекової структури NIST може допомогти українським організаціям краще оцінювати ризики та ефективніше реагувати на загрози.

3. Розвиток державно-приватного партнерства. Залучення приватного сектору до забезпечення кібербезпеки за прикладом США сприятиме розширенню ресурсної бази та впровадженню інноваційних рішень.

4. Інвестиції в освіту та науку. Ізраїльський досвід демонструє важливість розвитку наукових досліджень і підготовки фахівців у сфері кібербезпеки. Україна має підтримувати університетські програми та створювати умови для роботи стартапів.

5. Посилення міжнародного співробітництва. Україна повинна активніше співпрацювати з міжнародними організаціями, такими як НАТО, ООН та ЄС, для обміну досвідом і ресурсами.

Варто погодитись з думками В. І. Гурковського, стосовно того, що важливим елементом діяльності, спрямованої на задоволення потреб та інтересів особи, держав, а також міжнародного співтовариства в отриманні інформації із використанням різноманітних технологій, зокрема комп'ютерних засобів і глобальних електронних телекомунікаційних систем, є забезпечення інформаційної безпеки. Основними її складовими є захист інтересів людини, суспільства, держави та міжнародного співтовариства у сфері інформації [59, с. 73].

Отож, міжнародний досвід регулювання інформаційної безпеки пропонує широкий спектр ефективних рішень, які можуть бути адаптовані до українських реалій. Проте їх імплементація потребує комплексного підходу, що включає гармонізацію законодавства, розвиток інституційної спроможності, залучення приватного сектору та активізацію міжнародного співробітництва. Лише за умови системного підходу Україна зможе створити ефективну систему інформаційної безпеки, здатну протистояти сучасним викликам.

Підсумовуючи проведений у другому розділі аналіз адміністративно-правових механізмів забезпечення інформаційної безпеки, які є невід'ємною складовою сучасної системи національної безпеки зроблено декілька висновків, що полягають у такому.

1. З огляду на стрімкий розвиток інформаційно-комунікаційних технологій, а також зростання загроз у кіберпросторі, формування ефективних механізмів регулювання інформаційної сфери стає пріоритетним завданням держави. Адміністративно-правові механізми забезпечення інформаційної безпеки є основою для створення правового середовища, яке регулює відносини у сфері інформації. Вони включають нормативно-правові акти, інституційні структури, а також методи та засоби контролю за дотриманням законодавства. Ефективне функціонування цих механізмів сприяє захисту національних інтересів і прав громадян в інформаційній сфері.

2. Державні органи відіграють ключову роль у забезпеченні інформаційної безпеки. Зокрема, міністерства, агентства та спеціалізовані служби повинні

взаємодіяти для координації заходів, спрямованих на попередження, виявлення та нейтралізацію загроз. Важливою є розробка та впровадження державних стратегій, які враховують новітні виклики в інформаційному просторі.

3. Аналіз чинного законодавства України вказує на необхідність його вдосконалення та адаптації до сучасних умов. Зокрема, важливим є розроблення чітких норм щодо відповідальності за порушення в інформаційній сфері, а також створення правових механізмів реагування на кіберзагрози. Особливу увагу слід приділити гармонізації національного законодавства із міжнародними стандартами.

4. Кібербезпека є одним із ключових аспектів інформаційної безпеки. У цьому контексті адміністративно-правові механізми повинні забезпечувати створення умов для захисту критичної інформаційної інфраструктури, зокрема через впровадження сучасних технологій моніторингу та реагування. Також важливою є підготовка фахівців у галузі кібербезпеки та підвищення рівня обізнаності громадян щодо основ безпечного користування інформаційними ресурсами.

5. Ураховуючи глобальний характер загроз в інформаційному просторі, значну увагу доцільно приділити міжнародному співробітництву. Україна має активно брати участь у роботі міжнародних організацій, укладати угоди про співпрацю у сфері кібербезпеки та обмінюватись досвідом із зарубіжними партнерами.

Серед основних викликів можна виділити постійне вдосконалення методів здійснення кіберзлочинів, недостатній рівень фінансування заходів із забезпечення інформаційної безпеки та низький рівень правосвідомості населення. Перспективним напрямом є впровадження інноваційних технологій у сферу адміністративного управління, що дозволить підвищити ефективність правових механізмів.

Відтак, забезпечення інформаційної безпеки вимагає комплексного підходу, який базується на поєднанні адміністративно-правових, технічних та організаційних заходів. Удосконалення правового регулювання, підвищення

ефективності діяльності державних органів та активізація міжнародного співробітництва сприятимуть створенню надійної системи захисту інформаційного простору України.

РОЗДІЛ 3
ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ ВДОСКОНАЛЕННЯ АДМІНІСТРАТИВНО-ПРАВОВОГО РЕГУЛЮВАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УКРАЇНІ

3.1. Аналіз існуючих проблем у сфері інформаційної безпеки: прогалини нормативно-правової бази та організаційні аспекти

Сучасний розвиток інформаційних технологій створює нові можливості для суспільства, бізнесу та держави, водночас породжуючи численні виклики у сфері інформаційної безпеки. Ця сфера має критичне значення для забезпечення національної безпеки, захисту персональних даних, стабільності економічних і соціальних процесів. Проте, попри зростання важливості інформаційної безпеки, нормативно-правова база та організаційні аспекти її забезпечення залишаються недостатньо розвиненими, що створює ризики для ефективного функціонування державних і приватних структур.

Однією з ключових проблем у сфері інформаційної безпеки є недосконаліть та фрагментарність нормативно-правової бази. В Україні основним законодавчим актом у цій сфері є Закон України «Про національну безпеку України» [20] та Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» [57]. Однак ці нормативні акти не завжди відповідають сучасним викликам і загрозам.

На думку Р. А. Калюжного та О. О. Баєва, рівень нормативно-правового забезпечення інформаційної безпеки України залежить від ступеня врегульованості суспільних відносин у цій сфері національним законодавством, нормами міжнародного права та міжнародними договорами України. Загалом, система нормативно-правового регулювання інформаційної безпеки України, як єдина структура правового впливу на суспільні відносини у сфері протидії загрозам національним інтересам, є недостатньо розвиненою. Це суттєво обмежує можливості України щодо ефективної протидії загрозам її

інформаційній безпеці та послаблює здатність держави до зміцнення національної безпеки [60, с. 5].

Науковці зазначають важливість розробки комплексу інформаційних стандартів, зокрема у сфері інформаційної безпеки, вдосконалення системи сертифікації інформаційної продукції, створення механізмів ліцензування діяльності організацій за окремими напрямами формування єдиного інформаційного простору та його захисту відповідно до чинного законодавства, а також проведення експертизи проектів державних інформаційних систем і ресурсів [60, с. 11].

Необхідно зауважити, що нині все ще існує розрив між законодавчими нормами та їх практичною реалізацією. Наприклад, законодавство передбачає обов'язок захищати персональні дані громадян, але на практиці механізми контролю за виконанням цих норм залишаються слабкими. Брак дієвих санкцій за порушення вимог інформаційної безпеки лише посилює цю проблему.

За твердженням А. Марущака, інформація, яка входить до складу інформаційних ресурсів держави, може бути: відкритою або з обмеженим доступом; первинною, тобто створеною державним органом чи іншим суб'єктом, або вторинною – результатом аналітико-синтетичної обробки; належати як державним органам, так і недержавним юридичним чи фізичним особам, а також бути у змішаній формі власності чи спільного використання; зберігатися на паперових чи електронних носіях тощо [61, с. 68].

Окрім того, нормативно-правова база не враховує динаміку розвитку технологій. Наприклад, законодавство не завжди адекватно реагує на нові загрози, пов'язані з використанням штучного інтелекту, Інтернету речей та блокчейн-технологій. Відсутність відповідних актів регулювання створює прогалини у сфері захисту інформаційних систем.

Не менш важливими є організаційні аспекти забезпечення інформаційної безпеки. В Україні функції у цій сфері розподілені між кількома державними органами, включаючи Раду національної безпеки і оборони України (РНБО), Службу безпеки України (СБУ), Міністерство цифрової трансформації та інші

установи. Така розподіленість функцій часто призводить до дублювання повноважень, відсутності координації дій і неефективного використання ресурсів.

Однією з ключових проблем є недостатній рівень підготовки кадрів у сфері кібербезпеки. Брак кваліфікованих фахівців обмежує спроможність державних органів ефективно реагувати на кіберзагрози. Крім того, приватний сектор також відчуває дефіцит фахівців, що ускладнює захист корпоративних інформаційних систем.

Ще одним важливим аспектом є недостатнє фінансування заходів із забезпечення інформаційної безпеки. У багатьох випадках державні установи не мають достатніх ресурсів для впровадження сучасних технологій захисту даних або проведення навчань для персоналу.

Окремо варто зазначити про низький рівень обізнаності громадян щодо питань кібербезпеки. Відсутність систематичних просвітницьких кампаній призводить до того, що користувачі залишаються вразливими до фішингових атак, вірусів та інших кіберзагроз.

Згідно з позицією О. І. Косілової, із настанням інформаційної епохи розвитку людства найбільш актуальною стала проблема інформаційного протиборства. Його метою є деморалізація населення та військових сил, а також паралізація волі до опору у протилежної сторони. У сучасних умовах інформаційна безпека набуває статусу одного з ключових компонентів у забезпеченні національної безпеки України. Інформація та інформаційні технології дедалі частіше виступають найефективнішими засобами ведення боротьби в сучасному світі. Інформаційне протиборство відбувається між різними суб’єктами, такими як особи, суспільства, держави та наднаціональні утворення. Основними формами такого протиборства визначаються інформаційна війна, інформаційна злочинність та інформаційний тероризм. Сучасні інформаційні війни є індикатором високого рівня розвитку суспільств і належать до несилових методів вирішення конфліктів. У міжнародній політиці сформувалося нове явище – можливість досягнення політичних цілей, зміни

легітимних урядів, а також політичного, економічного та духовного підкорення народів і держав без використання військової сили [62, с. 24-25].

У сучасних умовах, як зазначає вчена, виділяють такі основні види інформаційних війн: знищення систем управління супротивника, створення перешкод для інформаційного забезпечення бойових дій, радіоелектронна атака, інформаційно-психологічний вплив, хакерські операції та війна в сфері економічної інформації [62, с. 25].

Аналізуючи дослідження питань інформаційної безпеки у сфері юридичної науки, А. І. Марущак доходить висновку, що сучасний стан правовідносин, пов'язаних із реалізацією законних прав та інтересів особи, суспільства й держави в інформаційній сфері, потребує оновлення та чіткого визначення напрямів дослідження теоретико-правових аспектів забезпечення інформаційної безпеки. Подальші дослідження в цьому напрямі мають зосереджуватися на уточненні основних понять і категорій, що дозволить застосовувати їх у розробленні прикладних проблем інформаційної безпеки. Зокрема, уніфікація ключових термінів і їхнє узгоджене використання в процесі нормотворчої діяльності сприятиме єдиному розумінню завдань із забезпечення інформаційної безпеки особи, суспільства та держави, що, своєю чергою, підвищить ефективність роботи суб'єктів, які відповідають за її забезпечення [63, с. 20].

Вирішення проблем у сфері інформаційної безпеки неможливе без вивчення міжнародного досвіду. Наприклад, у країнах Європейського Союзу діє Загальний регламент про захист даних (GDPR), який встановлює жорсткі вимоги до обробки персональних даних і передбачає значні штрафи за порушення. У США функціонує Національний інститут стандартів і технологій (NIST), який розробляє рекомендації для захисту критичної інфраструктури.

Україна може використати ці приклади для вдосконалення власної нормативно-правової бази та організаційних механізмів. Зокрема, необхідно адаптувати міжнародні стандарти до національних умов і забезпечити їх імплементацію на практиці.

Зважаючи на деструктивний інформаційний тиск, що його здійснює

країна-агресор російська федерація на населення України та світову спільноту, можна окреслити ключові напрями контрзаходів для захисту вітчизняного інформаційного поля та гарантування національної системи інформаційної безпеки України: по-перше, необхідно вдосконалити чинну нормативно-правову базу у сфері державної інформаційної політики, яка б чітко визначала механізми взаємодії між силовими структурами України, органами місцевого самоврядування, державними установами та громадськими організаціями; по-друге, створити єдиний координуючий орган на міжвідомчому рівні, відповідальний за керівництво, узгодження та контроль реалізації заходів інформаційної безпеки (як варіант, можна розглянути формування міжвідомчої комісії при Раді національної безпеки та оборони); по-третє, розробити механізм всеохоплюючого моніторингу як популярних засобів масової інформації (аудіовізуальних та друкованих), так і поширених інтернет-майданчиків; по-четверте, стимулювати подальші ґрунтовні наукові дослідження у сфері інформаційної безпеки [29, с. 200].

Окремим викликом є забезпечення інформаційної безпеки в сфері економіки, зокрема господарській діяльності. Згідно з поглядами В. В. Шемчук, незважаючи на розбіжності в об’єктах (економічна система проти інформаційного простору) та методах досягнення між економічною та інформаційною безпекою, вони також мають спільні моменти. До таких спільних характеристик належать:

1) Обидві входять до складу національної безпеки;

2) Держава несе першочергову відповідальність за їх підтримання;

3) Їхнє регулювання ґрунтується на законодавстві;

4) Рівні їхнього забезпечення збігаються: міжнародний, державний та локальний;

5) Групи суб’єктів, що займаються цим питанням, фактично тотожні – це можуть бути держави (відповідні інституції та посадовці), міжнародні об'єднання, громадяни та інші. Основними завданнями для них є запобігання та ліквідація небезпек, а також оборона суверенітету країни у відповідних сферах.

З огляду на вищезазначене, В. В. Шемчук дійшов думки, що економічна та інформаційна безпеки становлять собою конституційні поняття, хоча їхнє повне тлумачення відсутнє в Основному Законі. Огляд наукових праць показує, що для визначення сутності державної економічної безпеки застосовуються різні методологічні основи. Найбільш поширеними серед дослідників є статичний, динамічний, системно-структурний та інтегральний (комплексний) підходи. Єдине офіційне формулювання сутності економічної безпеки, зафіксоване у наказі Міністерства економічного розвитку і торгівлі від 2013 року, базується якраз на статичному підході. У правовому контексті, державну економічну безпеку можна трактувати як сукупність взаємозв'язків юридичного характеру, що виникають у процесі діяльності державних органів щодо гарантування невтрушності національної економічної структури. [68, с. 256-257].

З погляду захисту інформації на торговельних підприємствах, у контексті формування світового інформаційного соціуму, питанню інформаційної безпеки приділяють увагу такі дослідники, як Н. С. Акімова, Л. О. Кирильєва та Т. А. Наумова. Ці науковці наголошують, що сучасне інформаційне суспільство – це складна структура даних, яка вирізняється значним рівнем розвиненості інформаційної культури. У межах єдиного інформаційного поля нагальною потребою стає охорона систем електронної комерції від викрадення даних, неправомірного доступу до них, їхнього знищення та інших протиправних чи небажаних маніпуляцій, чисельність яких неухильно збільшується [69, с. 5-10].

Сучасні обставини відзначаються шаленим прогресом у сфері інформаційних та телекомунікаційних технологій, а також активним запровадженням найсучасніших інфотехнологій у всі аспекти буття. Усвідомлюючи це, саме інформація та передові інформаційно-телекомунікаційні системи набувають все більшого значення у формуванні курсу розвитку як держави, так і соціуму, стимулюючи розбудову інформаційного простору. Природно, що для забезпечення належної, продуктивної та скоординованої роботи цього інформаційного середовища є необхідним створення та введення в дію комплексу організаційних та нормативно-правових кроків, серед яких

ключове місце посідають заходи, спрямовані на оперативне налагодження функціонування системи захисту інформації. [70, с. 10].

Варто підкреслити, що у сучасній юридичній доктрині на даний момент питанню з’ясування сутності інформаційної безпеки суб’єктів господарювання та розробки комплексних методів нейтралізації загроз цій безпеці приділяється недостатньо уваги. Переважно праці у цій галузі належать до сфери економіки та технологій. На погляд науковців, причина цього у тому, що протягом певного часу як державні органи влади України, так і самі підприємці не усвідомлювали повною мірою значущості захисту відомостей. Внаслідок цього, як на рівні законодавства, так і у внутрішніх настановах компаній, не було сформовано ефективних механізмів захисту даних та гарантування надійності інформаційних систем підприємств. Така ситуація спричинила стрімке зростання злочинності, пов'язаної з комп'ютерним шахрайством та промисловим шпигунством. Широкого розмаху також набули рейдерські захоплення, що стали можливими, зокрема, завдяки несанкціонованому проникненню до інформаційних комплексів бізнесу. Таким чином, враховуючи викладене, надзвичайної важливості набуває завдання створення дієвого адміністративно-правового інструментарію для забезпечення безпеки інформації у сфері підприємництва, що може бути реалізовано лише за умови чіткого розуміння природи інформаційної безпеки підприємництва як об'єкта, який потребує адміністративно-правового захисту [70, с. 10].

Таким чином, аналіз існуючих проблем у сфері інформаційної безпеки свідчить про необхідність комплексного підходу до їх вирішення. Для цього доречно:

1. Удосконалити нормативно-правову базу шляхом ухвалення нових законодавчих актів, які враховують сучасні виклики та загрози.

2. Забезпечити координацію дій між державними органами у сфері кібербезпеки.

3. Інвестувати в підготовку кадрів і підвищення кваліфікації фахівців.

4. Запровадити систематичні просвітницькі кампанії для населення.

5. Використовувати міжнародний досвід і стандарти для вдосконалення національної системи інформаційної безпеки.

Тільки за умови комплексного підходу можна створити ефективну систему захисту інформації, яка відповідатиме сучасним викликам і сприятиме сталому розвитку суспільства й держави.

3.2. Роль громадянського суспільства у забезпеченні інформаційної безпеки: правові механізми співпраці з державою

Інформаційна безпека є однією з ключових складових національної безпеки будь-якої держави. В умовах глобалізації, цифровізації та розвитку інформаційних технологій, загрози в інформаційному просторі набули нового рівня складності. У цьому контексті особливого значення набуває співпраця між державою та громадянським суспільством у забезпеченні інформаційної безпеки. Важливу роль у такій співпраці відіграють правові механізми, які регулюють взаємодію між цими суб'єктами.

Як підкреслює Д. В. Ланде, у сучасних умовах нестабільності світової економіки в інформаційному просторі проявляються виклики та загрози, що стосуються всіх аспектів людського життя. Однак саме події, що розгортаються в межах інформаційного середовища, можуть становити загрозу руйнування існуючих основ інформаційного суспільства, сприяти формуванню нових суспільних відносин, обумовлених специфікою інформаційної взаємодії. Виклики в інформаційній сфері здатні призвести до трансформації або навіть руйнування фундаментальних принципів сучасної економіки, зокрема у контексті питань, пов'язаних з авторським правом і суміжними правами, захистом приватності, екстериторіальністю та іншими аспектами [64, с. 19].

Громадянське суспільство охоплює широкий спектр організацій, ініціатив та індивідуальних активістів, які діють незалежно від влади, але взаємодіють із нею для досягнення суспільно важливих цілей. У сфері інформаційної безпеки громадянське суспільство виконує низку важливих функцій:

1. Моніторинг та аналіз загроз. Громадські організації та незалежні експерти часто виступають як суб’єкти моніторингу інформаційного простору, виявлення дезінформації, кіберзагроз і пропаганди.

2. Підвищення обізнаності населення. Завдяки освітнім кампаніям, тренінгам та іншим заходам громадянське суспільство допомагає підвищувати рівень цифрової грамотності населення, що є важливим елементом протидії інформаційним загрозам.

3. Адвокація та контроль. Громадські організації сприяють формуванню прозорих державних політик у сфері інформаційної безпеки, здійснюють контроль за їх виконанням і захищають права громадян в інформаційному просторі.

4. Розробка технологічних рішень. Багато громадських ініціатив спрямовані на створення інструментів для виявлення фейкових новин, захисту від кібератак і забезпечення конфіденційності даних.

Вагому роль у сприянні розвитку громадянського суспільства відіграє Національна стратегія сприяння розвитку громадянського суспільства в Україні на 2021–2026 роки, що затверджені Указом Президента України від 7 вересня 2021 року № 487/2021 [65]. У контексті забезпечення інформаційної безпеки, громадянське суспільство покликано сприяти цифровим трансформаціям, захисту інформації, перешкоджанню негативному впливу інформації на свідомість людей тощо. З цією метою Стратегія передбачає створення умов для активної участі громадян у процесах формування та реалізації державної політики, зокрема через застосування сучасних інформаційно-комунікаційних технологій.

Одним із ключових завдань Стратегії є забезпечення прозорості діяльності органів державної влади та місцевого самоврядування. Це включає впровадження механізмів електронної демократії, таких як електронні петиції, громадські консультації та інші інструменти, що дозволяють громадянам висловлювати свою думку та впливати на прийняття рішень. Такий підхід сприяє не лише підвищенню рівня довіри до інституцій влади, але й формуванню

стійкого інформаційного середовища, яке здатне протистояти маніпулятивним впливам.

Особлива увага у Стратегії приділяється питанням підвищення рівня медіаграмотності населення. У сучасних умовах інформаційного суспільства громадяни мають бути здатними критично оцінювати інформацію, розрізняти достовірні джерела від недостовірних, а також розуміти основи функціонування медіа. Для досягнення цієї мети передбачено реалізацію просвітницьких програм, організацію тренінгів та семінарів, спрямованих на розвиток навичок критичного мислення.

Крім того, Стратегія акцентує увагу на необхідності створення умов для розвитку цифрової інфраструктури. Це включає забезпечення доступу до швидкісного інтернету, особливо у віддалених регіонах, а також впровадження сучасних технологій для захисту персональних даних та забезпечення кібербезпеки. Такі заходи є важливими не лише для забезпечення інформаційної безпеки, але й для сприяння економічному розвитку та підвищення конкурентоспроможності України на міжнародній арені.

Важливим аспектом реалізації Стратегії є підтримка діяльності громадських організацій, які відіграють ключову роль у розвитку громадянського суспільства. Зокрема, передбачено створення сприятливих умов для їхньої роботи, включаючи спрощення процедур реєстрації, забезпечення доступу до фінансування та надання консультаційної допомоги. Громадські організації можуть стати ефективними партнерами держави у впровадженні ініціатив, спрямованих на зміцнення інформаційної безпеки та розвиток цифрових технологій.

Не менш важливим є питання правового регулювання у сфері інформаційної безпеки. Стратегія акцентує увагу на необхідності вдосконалення законодавчої бази з метою забезпечення ефективного захисту інформаційного простору України. Це включає розробку нових нормативно-правових актів та внесення змін до чинного законодавства для адаптації до сучасних викликів і загроз.

Таким чином, Національна стратегія сприяння розвитку громадянського суспільства в Україні на 2021–2026 роки є важливим інструментом для забезпечення сталого розвитку держави в умовах цифровізації та глобалізації. Її реалізація сприятиме не лише зміцненню демократичних інститутів і підвищенню рівня довіри до влади, але й створенню безпечного та стійкого інформаційного середовища, що є необхідною умовою для процвітання сучасного суспільства. Успіх цих заходів залежить від ефективної співпраці між державою, громадянським суспільством та міжнародними партнерами.

На думку В. М. Фурашева, якщо на свідомість або підсвідомість людини впливає інформація, яка є неповною, несвоєчасною, недостовірною чи упередженою, і це призводить до порушення або змін у її стані здоров’я, психічному стані чи поведінці, то це можна кваліфікувати як інформаційну небезпеку для людини. У випадках, коли наслідком отримання такої інформації є порушення або зміни стану здоров’я, психічного стану чи поведінки в групи осіб, це слід розглядати як інформаційну небезпеку для суспільства. Коли ж подібна інформація впливає на прийняття рішень, які суперечать інтересам суспільства, державним чи національним інтересам, то це вже створює інформаційну небезпеку для суспільства та держави. Зазвичай для досягнення таких наслідків необхідне багаторазове поширення подібної інформації за певним алгоритмом, що дозволяє досягти конкретної мети. Це свідчить про цілеспрямовану та свідому підготовку і поширення такого виду інформації [66, с. 52-53].

Ефективна взаємодія між громадянським суспільством і державою у сфері інформаційної безпеки можлива лише за умови наявності чіткої нормативно-правової бази. В Україні така співпраця регулюється низкою законодавчих актів, зокрема:

1. Конституція України [21]. Основний Закон гарантує свободу слова, доступ до інформації та право на об'єднання, що створює правові передумови для діяльності громадянського суспільства.

2. Закон України «Про національну безпеку України» [20]. У цьому законі

визначено інформаційну безпеку як складову національної безпеки, а також передбачено можливість залучення громадянського суспільства до вирішення відповідних питань.

3. Закон України «Про доступ до публічної інформації» [58]. Цей закон забезпечує прозорість діяльності державних органів і сприяє участі громадськості в контролі за їхньою діяльністю.

4. Закон України «Про захист персональних даних» [23]. Закон встановлює норми щодо захисту конфіденційної інформації, що є важливим аспектом забезпечення інформаційної безпеки.

5. Закон України «Про основні засади забезпечення кібербезпеки України» [24]. Він визначає основні принципи та напрями діяльності у сфері кібербезпеки, включаючи співпрацю з недержавними суб’єктами.

Крім того, міжнародні договори та стандарти, наприклад Резолюція Генеральної Асамблеї ООН щодо боротьби з дезінформацією, також створюють правову основу для взаємодії держави та громадянського суспільства [67].

Взаємодія між державою та громадянським суспільством у сфері інформаційної безпеки може здійснюватися в різних формах:

1. Консультації та дорадчі органи. Участь представників громадянського суспільства в обговоренні стратегій і політик у сфері інформаційної безпеки дозволяє враховувати різноманітні точки зору та потреби.

2. Спільні проєкти. Реалізація спільних ініціатив, наприклад розробка програм цифрової грамотності або створення платформ для перевірки фактів, є ефективним способом використання ресурсів і експертизи обох сторін.

3. Інформаційний обмін. Держава може надавати громадським організаціям доступ до певної публічної інформації, а ті, своєю чергою, можуть ділитися результатами своїх досліджень і моніторингу.

4. Фінансова підтримка. Надання грантів або іншої фінансової допомоги громадським організаціям сприяє реалізації важливих проєктів у сфері інформаційної безпеки.

5. Навчання та підвищення кваліфікації. Спільні тренінги для державних

службовців і представників громадських організацій допомагають підвищити рівень професійної підготовки у сфері інформаційної безпеки.

Попри значний потенціал співпраці між державою та громадянським суспільством у сфері інформаційної безпеки, існують і певні виклики:

1. Недостатня довіра. У деяких випадках відсутність довіри між державними органами та громадськістю може перешкоджати ефективній співпраці.

2. Обмежені ресурси. Як держава, так і громадянське суспільство часто стикаються з браком фінансових і людських ресурсів для реалізації спільних ініціатив.

3. Регуляторні бар'єри. Недосконаліть законодавства або його неоднозначне тлумачення можуть створювати перешкоди для взаємодії.

Проте перспективи такої співпраці залишаються оптимістичними. Зміцнення правової бази, розвиток інституційної спроможності громадських організацій і підвищення рівня довіри між сторонами є ключовими чинниками успішного партнерства.

Отже, громадянське суспільство відіграє важливу роль у забезпеченні інформаційної безпеки, доповнюючи зусилля держави своїм досвідом, ресурсами та інноваційними підходами. Правові механізми співпраці створюють основу для ефективної взаємодії між цими суб'єктами, сприяючи формуванню безпечного й стійкого інформаційного середовища. У сучасних умовах саме синергія державних і громадських зусиль є запорукою успішного протистояння викликам в інформаційному просторі.

Підсумувати проведений у третьому Розділі аналіз проблем та перспектив вдосконалення адміністративно-правового регулювання інформаційної безпеки в Україні можемо таким.

1. Інформаційна безпека є однією з ключових складових національної безпеки України, що обумовлює необхідність її належного адміністративно-правового регулювання. На сьогоднішній день в Україні існує значна кількість нормативно-правових актів, що регулюють питання інформаційної безпеки.

Однак ці акти часто мають фрагментарний характер, що ускладнює їх практичне застосування. Відсутність єдиного системного підходу до формування законодавства у сфері інформаційної безпеки призводить до прогалин у правовому регулюванні, зокрема щодо визначення відповідальності за кіберзлочини, захисту критичної інформаційної інфраструктури та регулювання роботи суб'єктів інформаційної діяльності.

2. Україна активно інтегрується в міжнародне співтовариство, зокрема у сфері кібербезпеки. Однак рівень гармонізації національного законодавства з міжнародними стандартами залишається недостатнім. Це ускладнює співпрацю з міжнародними партнерами та впровадження передових технологій захисту інформації.

3. Відсутність належної координації між органами державної влади, які відповідають за забезпечення інформаційної безпеки, створює ризики дублювання функцій та неефективного використання ресурсів. Крім того, недостатньо врегульовані питання співпраці між державними структурами та приватним сектором, який відіграє важливу роль у захисті інформаційного простору.

4. Забезпечення інформаційної безпеки потребує значних фінансових ресурсів для впровадження сучасних технологій, навчання персоналу та проведення наукових досліджень. Проте обмеженість бюджетних асигнувань на цю сферу значно знижує ефективність заходів із захисту інформаційного простору.

5. На практиці виникають труднощі із застосуванням чинних норм законодавства через їхню неоднозначність або застарілість. Це стосується як питань визначення складу правопорушень у сфері інформаційної безпеки, так і механізмів притягнення до відповідальності осіб, які їх вчинили.

З огляду на вищезазначене, вдосконалення адміністративно-правового регулювання інформаційної безпеки в Україні потребує комплексного підходу. Зокрема, необхідно: розробити та впровадити єдиний системний законодавчий акт, який би комплексно регулював питання забезпечення інформаційної

безпеки; посилити гармонізацію національного законодавства із міжнародними стандартами та практиками; створити ефективну систему координації між усіма суб'єктами забезпечення інформаційної безпеки, включаючи державні органи, приватний сектор та громадські організації; забезпечити належне фінансування заходів із захисту інформаційного простору; удосконалити механізми правозастосування для забезпечення невідворотності покарання за порушення у сфері інформаційної безпеки.

Відтак, вирішення зазначених проблем сприятиме створенню ефективної системи адміністративно-правового регулювання інформаційної безпеки в Україні, що є необхідною умовою для захисту національних інтересів у сучасному інформаційному просторі.

ВИСНОВКИ

У кваліфікаційній роботі розглянуто концептуальні та нормативно-правові аспекти забезпечення інформаційної безпеки як ключового елементу національної безпеки України. Адміністративно-правова характеристика інформаційної безпеки дозволила сформулювати низку таких висновків.

1. Інформаційна безпека є стратегічним пріоритетом держави, оскільки сучасні виклики, зокрема кіберзагрози, інформаційні війни та дезінформація, мають потенціал значно впливати на політичну, економічну, соціальну та культурну стабільність країни. Вона охоплює захист інформаційних ресурсів, забезпечення кіберстійкості та протидію інформаційним загрозам.

2. Законодавство України забезпечує базові основи для регулювання питань інформаційної безпеки. Зокрема, Закони України «Про національну безпеку України», «Про основні засади забезпечення кібербезпеки України» та «Про інформацію» створюють правову основу для відповідних заходів. Водночас існує потреба в удосконаленні нормативно-правових актів, спрямованих на адаптацію до нових викликів у сфері інформаційної безпеки.

3. Адміністративно-правова характеристика інформаційної безпеки передбачає активну роль державних органів. У сфері забезпечення інформаційної безпеки задіяні численні державні органи, серед яких Рада національної безпеки і оборони України, Служба безпеки України, Міністерство цифрової трансформації України, Національна поліція, Державна служба спеціального зв’язку та захисту інформації України тощо. Однак відсутність чіткої координації між ними, дублювання функцій та недостатній рівень співпраці знижують ефективність реалізації заходів у цій сфері.

4. Забезпечення інформаційної безпеки потребує інтеграції міжнародного досвіду та співпраці з іншими державами і міжнародними організаціями. Україна повинна активно брати участь у формуванні міжнародних стандартів кібербезпеки та інформаційного захисту, а також розвивати партнерства у цій сфері. Забезпечення інформаційної безпеки є ключовим елементом сталого

розвитку держави, її національної безпеки та міжнародного авторитету. Україна, як суб'єкт міжнародних відносин, має значний потенціал для інтеграції в глобальну систему кібербезпеки, враховуючи зростаючі виклики у сфері інформаційного захисту. По-перше, необхідно акцентувати увагу на важливості адаптації міжнародного досвіду до національних умов. Це передбачає імплементацію міжнародних стандартів кібербезпеки, що дозволить не лише підвищити рівень внутрішньої безпеки, але й забезпечити ефективну координацію з іншими державами. По-друге, співпраця з міжнародними організаціями, такими як НАТО, ООН, ОБСЄ та Європол, є необхідною для створення ефективної системи обміну інформацією про кіберзагрози. Спільні навчання, тренінги та обмін досвідом сприятимуть підвищенню кваліфікації українських фахівців у сфері кібербезпеки. По-третє, важливо розвивати двосторонні та багатосторонні партнерства з іншими державами, які мають передовий досвід у боротьбі з кіберзлочинами. Укладення відповідних міжнародних договорів та меморандумів про співпрацю дозволить забезпечити доступ до новітніх технологій і методик у сфері інформаційного захисту. По-четверте, законодавче регулювання має відігравати вирішальну роль у створенні ефективної системи кібербезпеки. Гармонізація українського законодавства з міжнародними нормами та стандартами сприятиме підвищенню довіри до України як надійного партнера у сфері інформаційної безпеки. Відтак, інтеграція міжнародного досвіду та активна співпраця з іншими державами і міжнародними організаціями є стратегічно важливими для забезпечення інформаційної безпеки України. Реалізація зазначених заходів сприятиме зміцненню національної безпеки, підвищенню рівня захисту критичної інфраструктури та формуванню позитивного іміджу України на міжнародній арені.

5. Незважаючи на існування законодавчої бази, в Україні спостерігається низка проблем у сфері інформаційної безпеки, серед яких недостатнє фінансування, низький рівень цифрової грамотності населення та недосконаліть механізмів реалізації державної політики у цій сфері. Подальший розвиток адміністративно-правового регулювання має бути спрямований на усунення цих

недоліків.

6. Серед ключових пріоритетів державної політики у сфері інформаційної безпеки доречно виділити: посилення кіберзахисту критичної інфраструктури, вдосконалення системи моніторингу та реагування на інформаційні загрози, розвиток кадрового потенціалу у сфері кібербезпеки, а також проведення просвітницьких кампаній для населення.

7. З огляду на військову агресію російської федерації проти України, країна стикається з постійними кібератаками на критичну інфраструктуру, державні установи та приватний сектор. Відсутність належного технічного оснащення та нормативного забезпечення ускладнює боротьбу з цими загрозами.

8. Окремим викликом є кадровий дефіцит і низький рівень професійної підготовки. Забезпечення інформаційної безпеки вимагає висококваліфікованих фахівців, які володіють сучасними знаннями у сфері кібербезпеки, права та інформаційних технологій. Однак у державних органах часто спостерігається дефіцит таких кадрів, що обмежує можливості оперативного реагування на загрози.

Отже, на основі проведеного дослідження можна зробити висновок, що забезпечення інформаційної безпеки в контексті національної безпеки є комплексним завданням, яке потребує системного підходу, інтеграції зусиль державних органів, приватного сектору та громадянського суспільства. Удосконалення адміністративно-правового регулювання цієї сфери має стати одним із пріоритетів державної політики для гарантування стабільності та суверенітету України в умовах сучасних загроз.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Грабар Н. С. Інформаційна безпека в умовах становлення глобального інформаційного суспільства. *Державне управління: удосконалення та розвиток*. 2019. № 7. URL: http://www.dy.nayka.com.ua/?op=1&z=1461

2. Кормич Б. А. Інформаційна безпека: організаційно-правові основи: навч. посібник. К.: Кондор, 2004. 384 с.

3. Панченко О. А. Інформаційна безпека в контексті викликів і загроз національній безпеці. *Державне управління та місцеве самоврядування*. 2020. Вип. 2 (45). С. 57–63.

4. Форос А. В. Інформаційна безпека як складова національної безпеки України. *Правова держава*. 2009. № 11. С. 222–226.

5. Цимбалюк В. Інформаційна безпека підприємницької діяльності, визначення сутності та змісту поняття за умов входження України до інформаційного суспільства (глобальної кіберцивілізації). *Підприємництво, господарство і право*. 2004. № 3. С. 88–91.

6. Золотар О. О. Класифікація інформаційної безпеки. *Інформація і право*. 2011. № 2. С. 109–113.

7. Гурковський В. І. Організаційно-правові питання взаємодії органів державної влади у сфері національної інформаційної безпеки: автореф. дис. … канд. юрид. наук: 25.00.02. Київ, 2004. 20 с.

8. Кормич Б. А. Організаційно-правові засади політики інформаційної безпеки України: монографія. Одеса: Юрид. літ., 2003. 472 с.

9. Нашинець-Наумова А. Ю. Інформаційна безпека: питання правового регулювання: монографія. Київ: Гельветика, 2017. 168 с.

10. Ткачук Т. Ю. Забезпечення інформаційної безпеки в країнах Центральної Європи. *Юридичний науковий електронний журнал*. 2017. № 5. С. 104–110.

11. Рогова Є. І. Теоретичні основи правового забезпечення інформаційної безпеки. *Актуальні проблеми держави і права*. 2020. Вип. 86. С.

190–196.

12. Шатун В. Т. Інформаційна безпека – невід'ємна складова національної безпеки України. *Наукові праці. Державне управління*. 2016. Т. 267. Вип. 255. С. 174–180.

13. Гуцалюк М. Інформаційна безпека в сучасному суспільстві. *Право України*. 2005. №7. С. 71–74.

14. Домбровська С. М. Механізми забезпечення інформаційної безпеки як складової державної безпеки України. *Теорія та практика державного управління*. 2015. Вип. 1. С. 203–207.

15. Марущак А. І. Дослідження проблем інформаційної безпеки у юридичній науці. *Правова інформатика*. 2010. № 3(27). С. 17–21.

16. Верхоглядова Н. І., Кононова І. В. Інформаційна безпека як складова економічної безпеки. Колективна монографія. С. 382–396. DOI: https://doi.org/10.54929/monograph-02-2022-05-02

17. Шевчук М. О. До питання генези поняття інформаційної безпеки як складової національної безпеки. *Науковий вісник Ужгородського Національного Університету. Серія ПРАВО*. 2023. Вип. 78: частина 2. С. 134–139.

18. Абакумов В. М. Інформаційна безпека підприємництва як об'єкт адміністративно-правової охорони. *Форум права*. 2012. № 4. С. 10–16.

19. Кобко Є. Інформаційна безпека в системі національної безпеки: сучасність і перспективи. *Jurnalul Juridic Naţional: Teorie Şi Practică*. 2019. Martie. С. 46–50.

20. Про національну безпеку України: Закон України від 21 червня 2018 року № 2469-VIII. *Відомості Верховної Ради України*. 2018. № 31. Ст. 241.

21. Конституція України: Закон України від 28.06.1996 р. № 254к/96-ВР. URL: https://zakon.rada.gov.ua/laws/card/ 254%D0%BA/96-%D0%B2%D1%80

22. Про інформацію: Закон України від 2 жовтня 1992 року № 2657-XII. *Відомості Верховної Ради України*. 1992. № 48. Ст. 650.

23. Про захист персональних даних: Закон України від 1 червня 2010 року № 2297-VI. *Відомості Верховної Ради України*. 2010. № 34. Ст. 481.

24. Про основні засади забезпечення кібербезпеки України: Закон України від 5 жовтня 2017 року № 2163-VIII. *Відомості Верховної Ради України*. 2017. № 45. Ст. 403.

25. Кримінальний кодекс України від 5 квітня 2001 року № 2341-III. *Відомості Верховної Ради України*. 2001. № 25–26. Ст. 131.

26. Кодекс України про адміністративні правопорушення: Закон України від 07.12.1984 р. № 8073-X. *Відомості Верховної Ради Української РСР*. 1984. Додаток до № 51. Ст. 1122.

27. Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року «Про Стратегію національної безпеки України»: Указ Президента України від 14 вересня 2020 року № 392/2020 https://zakon.rada.gov.ua/laws/show/392/2020#Text

28. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України»: Указ Президента України від 25 лютого 2017 року № 47/2017. URL:

29. Гаврильців М. Т. Інформаційна безпека держави в системі національної безпеки України. Юридичний науковий електронний журнал. 2020. № 2. С. 200–203.

30. Яцик Т. П., Бодунова О. М. Щодо розмежування понять «інформаційна безпека» та «кібербезпека». *Науковий вісник Міжнародного гуманітарного університету. Сер.: Юриспруденція*. 2020. № 48. т. 2. С. 74–76.

31. Смотрич Д. В., Браілко Л. Інформаційна безпека в умовах воєнного стану. *Науковий вісник Ужгородського Національного Університету*. *Серія ПРАВО*. 2023. Вип. 77: частина 2. С. 121–127.

32. Чистоклетов Л., Обрембальський С. Особливості забезпечення інформаційної безпеки в умовах російсько-української війни. *Академічні візії*. 2024. Вип. 31. DOI: https://doi.org/10.5281/zenodo.11381101

33. Декларація про державний суверенітет України від 16 липня 1990 року № 55-XII. *Відомості Верховної Ради УРСР (ВВР)*. 1990. № 31. Ст. 429.

34. Антонова С.Є., Мартинюк Г.Ф. Інформаційна безпека. *Державне*

управління: удосконалення та розвиток. 2019. №11. URL: http://www.dy.nayka.com.ua/pdf/11_2019/38.pdf

35. Power, R. 2001. 2001CSI/FBI computer crime and security survey. *Comput. Sec. J. 17,2* (Spring), 29–51.

36. Біленчук П. Д. Правові засади інформаційної безпеки України. Харків, 2018. 289 с.

37. Арістова І. В. Державна інформаційна політика та її реалізація в діяльності органів внутрішніх справ України : організаційно-правові засади : дис. … д-ра юрид. наук : 12.00.07. К., 2002. 476 с.

38. 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. № 29. С. 281–288.

39. Ліпкан В. А. Теоретичні основи та елементи національної безпеки: монографія. Київ: «Текст», 2003. 600 с.

40. Баранов О. А. Інформаційне право України: стан, проблеми, перспективи. Київ: Видавничий дім «СофтПрес», 2005. 316 с.

41. Горбулін В. П., Биченок М. М. Проблеми захисту інформаційного простору України: монографія. Київ: Інтертехнологія, 2009. 136 с.

42. Конах В. К. Забезпечення інформаційної безпеки держави як складової системи національної безпеки (приклад США): дис. … канд. політ. наук: 21.01.01. Київ, 2005. 171 с.

43. Марущак А. І. Інформаційна безпека як об'єкт дослідження правової науки. *Актуальні проблеми управління інформаційною безпекою держави*: зб. матер. наук.-прак. конф. (м. Київ, 17.03.2010 р.). Київ: Наук. вид. відділ НА СБ України, 2010. С. 36–41.

44. Нехай В. А., Нехай В. В. Інформаційна безпека як складова економічної безпеки підприємств. *Науковий вісник Міжнародного гуманітарного університету*. рік. номер. С. 137–140.

45. Тацишин І. Б. Національна безпека України та її складові елементи. *Правова інформатика*. 2008. № 4 (20). С. 46–49.

46. Про Раду національної безпеки і оборони України: Закон України від 5 березня 1998 року № 183/98-ВР. *Відомості Верховної Ради України*. 1998. № 35. Ст. 237.

47. Про Державну службу спеціального зв'язку та захисту інформації України: Закон України від 23 лютого 2006 року № 3475-IV. Відомості Верховної Ради України. 2006. № 30. Ст. 258.

48. Про Службу безпеки України: Закон України від 25 березня 1992 року № 2229-XII. *Відомості Верховної Ради України.* 1992. № 27. Ст. 382.

49. Про Національну поліцію: Закон України від 2 липня 2015 року № 580-VIII. *Відомості Верховної Ради України*. 2015. № 40–41. Ст. 379.

50. Питання Міністерства цифрової трансформації: Постанова Кабінету Міністрів України від 18 вересня 2019 р. № 856. URL: https://zakon.rada.gov.ua/laws/show/856-2019-%D0%BF#Text

51. Про затвердження Положення про Міністерство оборони України: Постанова Кабінету Міністрів України від 26 листопада 2014 р. № 671. URL: https://zakon.rada.gov.ua/laws/show/671-2014-%D0%BF#Text

52. Про заходи для високого спільного рівня безпеки мережевих та інформаційних систем на території Союзу: Директива Європейського Парламенту і Ради (ЄС) 2016/1148 від 6 липня 2016 року URL: https://zakon.rada.gov.ua/laws/show/984_013-16#Text (Директиву скасовано на підставі Директиви № 2022/2555 від 14.12.2022).

53. Про заходи для високого спільного рівня кібербезпеки на всій території Союзу, внесення змін до Регламенту (ЄС) № 910/2014 та Директиви (ЄС) 2018/1972 та скасування Директиви (ЄС) 2016/1148 (Директива NIS 2): Директива Європейського Парламенту і Ради (ЄС) 2022/2555 від 14 грудня 2022 року. URL: https://zakon.rada.gov.ua/laws/show/9a3_001-22/print

54. Терзі О. О. Принципи забезпечення інформаційної безпеки держави: досвід України та зарубіжних країн. *Право та державне*. 2024. № 3. С. 51–57.

55. Куренда Л. Д. Окремі аспекти забезпечення інформаційної безпеки Європейського Союзу. *Правова інформатика*. 2011. № 3–4 (31). С. 36–42.

56. Про основні засади забезпечення кібербезпеки України: Закон України від 5 жовтня 2017 року № 2163-VIII. *Відомості Верховної Ради України*. 2017. № 45. Ст. 403.

57. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 5 липня 1994 року № 80/94-ВР. *Відомості Верховної Ради України*. 1994. № 31. Ст. 286.

58. Про доступ до публічної інформації: Закон України від 13 січня 2011 року № 2939-VI. *Відомості Верховної Ради України*. 2011. № 32. Ст. 314.

59. Гурковський В. І. Безпека як об'єкт правовідносин в умовах глобального інформаційного суспільства: методологічний аспект. *Правова інформатика*. 2010. № 2 (26). С. 72–77.

60. Калюжний Р. А., Баєв О. О. Нормативно-правове забезпечення інформаційної безпеки України. *Правова інформатика*. 2009. № 4 (24). С. 5–12.

61. Марущак А. І. Інформаційні ресурси держави: зміст та проблеми захисту. *Правова інформатика*. 2009. № 1 (21). С. 65–71.

62. Косілова О. І. Інформаційна безпека України в умовах глобалізації. *Правова інформатика*. 2010. № 3 (27). С. 22–28.

63. Марущак А. І. Дослідження проблем інформаційної безпеки у юридичній науці. *Правова інформатика*. 2010. № 3 (27). С. 17–21.

64. Ланде Д. В. Деякі інформаційні виклики сучасності та їх відображення в інформаційному просторі. *Правова інформатика*. 2012. № 2 (34). С. 19–27.

65. Про Національну стратегію сприяння розвитку громадянського суспільства в Україні на 2021–2026 роки: Указ Президента України від 7 вересня 2021 року № 487/2021. URL: https://zakon.rada.gov.ua/laws/show/487/2021/print

66. Фурашев В. М. Сутність та визначення понять «інформаційна безпека» і «безпека інформації». *Правова інформатика*. 2012. № 2 (34). С. 51–59.

67. Рада ООН з прав людини на запит України ухвалила заходи для протидії дезінформації. Інформація з сайту. URL: https://imi.org.ua/news/rada-

oon-z-prav-lyudyny-na-zapyt-ukrayiny-uhvalyla-zahody-dlya-protydiyi-dezinformatsiyi-i44799

68. Шемчук В. В. Економічна та інформаційна безпека держави: правові аспекти співвідношення. Вісник. 2019. Вип. С. 253–259.

69. Акімова Н. С., Кирильєва Л. О., Наумова Т. А. Інформаційна безпека підприємств торгівлі в умовах становлення глобального інформаційного суспільства. *Підприємництво і торгівля*. 2023. № 35. С. 5–10.

70. Абакумов В. М. Інформаційна безпека підприємництва як об’єкт адміністративно-правової охорони. *Форум права*. 2012. № 4. С. 10–16.