ДЕРЖАВНА СЛУЖБА УКРАЇНИ З НАДЗВИЧАЙНИХ СИТУАЦІЙ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ЦИВІЛЬНОГО ЗАХИСТУ УКРАЇНИ

Кваліфікаційна наукова
праця на правах рукопису

КУРИЛО Артем Геннадійович

УДК 351:004.056

ДИСЕРТАЦІЯ

ПУБЛІЧНЕ УПРАВЛІННЯ У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ

281 – публічне управління та адміністрування
Галузь знань – публічне управління та адміністрування

Подається на здобуття ступеня доктора філософії .
Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело
_____ А. Г. Курило
Науковий керівник: Домбровська Світлана Миколаївна, доктор наук з державного управління, професор, Заслужений працівник освіти України

Харків 2024

АНОТАЦІЯ

Курило А.Г.. Публічне управління у сфері інформаційної безпеки держави. Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття ступеня доктора філософії з галузі знань "Публічне управління та адміністрування" за спеціальністю 281 "Публічне управління та адміністрування". Національний університет цивільного захисту України, Харків, 2024.

У дослідженні запропоновано розв'язання актуальної проблеми з обґрунтування теоретичних засад та розробки практичних рекомендацій щодо удосконалення у публічного управління у сфері інформаційної безпеки держави.

Метою дисертаційної роботи є обґрунтування теоретичних засад та розробка практичних рекомендацій щодо удосконалення публічного управління у сфері інформаційної безпеки держави. Визначено стратегічні орієнтири функціонування та розвитку публічного управління у сфері інформаційної безпеки через розробку і реалізацію державної інформаційної політики, яка відповідає сучасним викликам, що стоять перед державою, та приділяє увагу формалізації цієї політики на відповідній нормативно-правовій базі.

Об'єктом дослідження виступає інформаційна безпека держави, а предметом дослідження є публічне управління у сфері інформаційної безпеки держави.

Для реалізації мети та завдань дослідження використовувалась сучасна наукова методологія заснована на принципах перетворення абстрактного в конкретні результати та єдності дослідження для досягнення наукового результату у вигляді науково обґрунтованих пропозицій щодо удосконалення публічного управління у сфері інформаційної безпеки держави.

Для досягнення мети дисертаційного дослідження вирішено ряд наукових взаємозалежних завдань:

- визначено місце та роль інформаційної безпеки в системі національної безпеки держави;

- оцінено стан реалізації публічного управління у сфері інформаційної безпеки;
- проаналізовано механізми публічного регулювання у сфері інформаційної безпеки України;
- систематизовано закордонний досвід розробки та впровадження інформаційного забезпечення державної безпеки;
- розкрито використання цифрових технологій в публічному управлінні у контексті модернізації інформаційної безпеки держави;
- запропоновано підходи до вдосконалення соціально-політичного та організаційно-правового механізмів публічного управління у сфері інформаційної безпеки.

В основу методології дослідження було покладено сукупність способів наукового пізнання та загальнонаукових методів, необхідних для його проведення. Ці способи гуртуються на фундаментальних положеннях і працях науковців з питань публічного управління та споріднених із нею наук.

Методологічна специфіка системного підходу визначається що віно орієнтує дослідження на розкриття об’єкта та механізмів що її забезпечують. Використано сукупності методів, які забезпечують реалізацію системного підходу, а саме: 1) загальнонауковий (індукції, дедукції, аналізу, синтезу, порівняння, аналогії); 2) філософсько-аксіологічний (діалектичного, системного та порівняльного); 3) спеціально-науковий (інституційного, структурно-функціонального та структурно-динамічного, діяльнісного, ситуативного); 4) порівняльно-історичний (при побудові періодизації еволюційних етапів становлення та реалізації державної інформаційної політики); 5) моделювання й логічного узагальнення (під час визначення підходів до вдосконалення соціально-політичного та організаційно-правового механізмів публічного управління у сфері інформаційної безпеки України).

У роботі вдосконалено напрями функціонування організаційно-правових та соціально-політичних механізмів публічного управління у сфері інформаційної безпеки в умовах використання цифрових технологій, що

дозволило розкрити особливості сучасного стану, концептуального, стратегічного та нормативно-правового забезпечення реалізації державної інформаційної політики, надало можливість сформулювати відповідні науково-теоретичні та практичні рекомендації для покращення інформаційної безпеки в умовах цифровізації. Інструменти розробки та впровадження інформаційного забезпечення держави на основі впровадження закордонного досвіду у вигляді удосконалення законодавства для забезпечення інформаційної безпеки, впровадження сучасних методів управління ризиками у сфері забезпечення інформаційної безпеки, взаємодії з міжнародними організаціями та країнами в напрямі обміну досвідом, створення спільних стратегій і протидії кіберзагрозам, розвитку системи підготовки кваліфікованих кадрів у галузі забезпечення інформаційної безпеки країни.

У межах розв’язаного науково-прикладного завдання дістало подальшого розвитку періодизація інформаційного розвитку України, на основі якої аналізується практика застосування сучасних цифрових технологій у публічному управлінні, що дозволяє розглядати сучасні цифрові технології як фактор модернізації інформаційної політики України. Запропоновано наукові підходи до визначення тенденцій функціонування публічного управління у сфері інформаційної безпеки через розробку і реалізацію державної інформаційної політики, яка відповідає сучасним викликам, що стоять перед державою, та формалізації цієї політики на відповідній нормативно-правовій базі.

Таким чином у дослідженні запропоновано розв’язання актуальної проблеми, що полягає в обґрунтуванні теоретичних засад та розробці практичних рекомендацій щодо удосконалення публічного управління в сфері інформаційної безпеки держави, а результати проведеного дослідження дозволяють зробити обґрунтовані висновки.

Ключові слова: публічне управління, захист інформації, інформаційна безпека, цифровізація, інформаційне забезпечення, національна безпека, державна інформаційна політика, концепції державної інформаційної політики.

ABSTRACT

Kurilo A.G. - administration in the field of information safety of the state. Qualification scientific work as a manuscript.

Dissertation for obtaining the degree of Doctor of Philosophy in the field of knowledge "Public management and administration" in specialty 281 "Public management and administration". National University of Civil Defense of Ukraine, Kharkiv, 2024.

The research proposes a solution to the pressing problem of substantiating theoretical foundations and developing practical recommendations for improving public administration in the field of state information safety.

The purpose of the dissertation is to substantiate the theoretical foundations and develop practical recommendations for improving public administration in the field of state information safety. Strategic guidelines for the functioning and development of public administration in the field of information safety have been determined through the development and implementation of the state information policy, which meets the modern challenges facing the state, and pays attention to the formalization of this policy on the appropriate regulatory and legal basis.

The object of research is information safety of the state, and the subject of research is public administration in the field of information safety of the state.

To implement the goal and tasks of the research, a modern scientific methodology was used, based on the principles of transforming abstract into concrete results and the unity of research to achieve a scientific result in the form of scientifically based proposals for improving public administration in the field of information safety of the state.

To achieve the goal of the dissertation research, a number of scientific interdependent tasks were solved:

• determination of the place and role of information safety in the state's national safety system;

• the state of implementation of public administration in the field of information

safety was assessed;

• mechanisms of public regulation in the field of information safety of Ukraine were analyzed;

• systematized foreign experience of development and implementation of information provision of state safety;

• the use of digital technologies in public administration in the context of modernization of state information safety is disclosed;

• approaches to improving social-political and organizational-legal mechanisms of public management in the field of information safety are proposed.

The methodology of the research was based on a set of methods of scientific knowledge and general scientific methods necessary for its implementation. These methods are based on the fundamental provisions and works of scientists on issues of public administration and related sciences.

The methodological specificity of the system approach is determined by the fact that it focuses research on the disclosure of the object and the mechanisms that provide it. A set of methods are used that ensure the implementation of a systemic approach, namely: 1) general scientific (induction, deduction, analysis, synthesis, comparison, analogy); 2) philosophical and axiological (dialectical, systematic and comparative); 3) special-scientific (institutional, structural-functional and structural-dynamic, operational, situational); 4) comparative-historical (when constructing a periodization of the evolutionary stages of the formation and implementation of the state information policy); 5) modeling and logical generalization (when determining approaches to improving socio-political and organizational-legal mechanisms of public management of social conflicts in Ukraine).

The areas of functioning of the organizational-legal and socio-political mechanisms of public administration in the field of information safety in the conditions of the use of digital technologies have been improved, which made it possible to reveal the features of the modern state, conceptual, strategic and regulatory legal support for the implementation of the state information policy, provided an opportunity to formulate relevant scientific and theoretical and practical recommendations for improving

information safety in conditions of digitization.

Tools for the development and implementation of state information safety based on the implementation of foreign experience in the form of improving legislation to ensure information safety, implementing modern risk management methods in the field of information safety, interaction with international organizations and countries in the direction of sharing experience, creating joint strategies and countering cyber threats, development of the system of training qualified personnel in the field of information safety of the country.

Within the scope of the solved scientific and applied task, the periodization of the information development of Ukraine received further development, based on which the practice of using modern digital technologies in public administration is analyzed, which allows considering modern digital technologies as a factor in the modernization of the information policy of Ukraine. Scientific approaches to determining trends in the functioning of public administration in the field of information safety through the development and implementation of state information policy, which meets the modern challenges facing the state, and the formalization of this policy on the appropriate regulatory and legal basis are proposed.

Thus, the research proposed a solution to the current problem, which consists in substantiating the theoretical foundations and developing practical recommendations for improving public administration in the field of information safety of the state, and the results of the conducted research allow us to draw reasonable conclusions. Thus, the research proposed a solution to the current problem , which consists in substantiating the theoretical foundations and developing practical recommendations for improving public administration in the field of information safety of the state, and the results of the conducted research allow us to draw well-founded conclusions.

Keywords: public administration, information protection, information safety, information support, national safety, state information policy, concepts of state information policy.

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Наукові праці, в яких опубліковані основні наукові результати дисертації:

Статті у фахових наукових виданнях з публічного управління:

1. Kurilo A. Analysis of the subject branch of public administration of the risks of emergency situations. *Public administration and state security aspects* Series: Vol.1/2023.URL:http://repositsc.nuczu.edu.ua/bitstream/123456789/16910/1/Kurilo.pdf

2. Kurilo A. Sociological monitoring of formation processes of public management society's information security. *Public administration and state security aspects* Series: Vol.2/2022. URL:http://repositsc.nuczu.edu.ua/bitstream/123456789/16910/1/Kurilo.pdf

3. Kurilo A. The place and role of forming information security in the system of public policy. *Public administration and state security aspects*. Series: Vol.1/2022. URL :http://repositsc.nuczu.edu.ua/bitstream/123456789/15387/3/Kurilo.pdf.

4. Курило А.Г. Міжнародно-правові стандарти забезпечення права особи на інформаційну безпеку. *Вісник Національного університету цивільного захисту України.* Серія: Державне управління. 2022. № 2 (15). С. 17-124 URL:http://repositsc.nuczu.edu.ua/bitstream/123456789/14591/1/Kurilo.pdf124URL :http://repositsc.nuczu.edu.ua/bitstream/123456789/14591/1/Kurilo.pdf

5. Курило А.Г. Місце інформаційної безпеки в системі національної безпеки. *Вісник Національного університету цивільного захисту України*. Серія: Державне управління. 2022. № 1 (14). URL:http://repositsc.nuczu.edu.ua/bitstream/123456789/13266/1/Kurilo.pdf

Наукові праці, які засвідчують апробацію матеріалів дисертації:

6. Курило А.Г. Інституційні особливості формування інформаційних інформаційних систем публічного управління в умовах глобалізації VIII *Міжнародної заочної науково-практичної конференції «Формування ефективних механізмів державного управління та менеджменту в умовах сучасної економіки: теорія і практика»* (м. Запоріжжя, 2020 р.) С. 67-71 ;

7. Курило А.Г. Формування у студентів поняття публічного управління у сфері інформаційної безпеки держави. *Міжнародної науково-практичної інтернет-конференції «Організаційно-методологічне забезпечення підготовки фахівців: тенденції, проблеми та шляхи їх вирішення (з нагоди 90-річчя ХНАДУ)»* м. Харків, 2020. С. 196-200.;

8. Курило А.Г. Питання публічного управління у сфері інформаційної безпеки для неповнолітніх. *Міжнародної науково-практичної конференції MicroCAD-2020 «Інформаційні технології: наука, техніка, технологія, освіта, здоров'я» (м. Харків, 18–20.10.2020 р.).* Ч. IV / за ред. проф. Сокола Є.І. Харків : НТУ «ХПІ». С. 71;

9. Курило А.Г. Питання правового регулювання в системі публічного управління у сфері інформаційної безпеки. *Формування дієвих механізмів державного управління з забезпечення державної безпеки : матеріали круглого столу (м. Харків, 14.05.2021 р.).* Харків: НУЦЗУ, 2021. С. 256-257.

10. Курило А.Г. Деякі аспекти розвитку інформаційного забезпечення державної безпеки. *Міжнародної науково-практичної інтернет-конференції «Публічне управління у сфері цивільного захисту: освіта, наука, практика» (*29 березня 2024 р.*).* Харків: НУЦЗУ, 2024. С. 236-238.

ЗМІСТ

ВСТУП

Актуальність теми. Геополітичні зміни останніх десятиліть суттєво трансформували систему міжнародних відносин. Ключовими факторами цього процесу є зміщення геополітичного центру ваги, зростання впливу нових глобальних акторів, посилення міжнародних конфліктів і виникнення нових загроз через розвиток технологій і зміни в суспільстві. Україна активно бере участь у цих змінах і відчуває їхній вплив на собі.

Одним із найпомітніших аспектів для України є військова агресія з боку російської федерації та анексія частини території. Це створює серйозні виклики для національної безпеки України і міжнародної стабільності в регіоні. У відповідь на ці загрози, Україна посилює свої зусилля щодо інтеграції в Європейський Союз та НАТО, що може значно змінити баланс сил у регіоні та вплинути на міжнародні відносини. Ці кроки змушують країни переосмислити нову реальність у Східній Європі та переглянути свої стратегії в сфері міжнародної безпеки. Разом з тим, швидкий розвиток інформаційних технологій і їх широке впровадження в усі сфери суспільного життя створюють як нові можливості, так і нові загрози.

Сьогодні в Україні тривають наукові дослідження щодо вдосконалення публічного управління в сфері інформаційної безпеки держави. Це прагнення проявляється у намаганні покращити правове поле, здійснюваних реформах та підтримці сталого розвитку країни. Наприклад, були прийняті укази Президента України «Про Стратегію національної безпеки України» (2020 р.) та «Про Стратегію інформаційної безпеки України» (2021 р.). Ці нормативно-правові документи підкреслюють важливість мінімізації зовнішніх і внутрішніх уразливостей, а також здатність суспільства та держави швидко адаптуватися до змін у безпековому середовищі та забезпечувати стабільне функціонування. Проте сучасне організаційно-правове забезпечення публічного управління у сфері інформаційної безпеки в Україні потребує вдосконалення. Наразі воно відзначається недосконалістю та не системністю, що зумовлює появу нових

викликів, можливостей та загроз для України. Серед них кібербезпека, ШІ, конфіденційність даних та захист від інформаційних атак. Ефективне публічне управління в цій сфері є критично важливим для забезпечення національної безпеки, захисту інтересів держави, суспільства та громадян. Відсутність належного регулювання та координації з боку державних органів унеможливлює досягнення високого рівня інформаційної безпеки, що, у свою чергу, впливає на стабільність і розвиток держави загалом. Ефективна адаптація до геополітичних змін вимагатиме скоординованих зусиль на всіх рівнях. Інформаційна політика, її розробка та реалізація виходять на передній план державної стратегії, оскільки від якості розробки концепції державної інформаційної політики та її успішної реалізації залежить ефективність роботи всіх державних і громадських структур, а зрештою – їх інформаційна безпека.

Особливості формування та реалізації публічного управління в сфері інформаційної безпеки та інформаційного суспільства визначені в наукових роботах зарубіжних дослідників Значний внесок у розвиток знань у сфері інформаційного суспільства зробили такі вчені, як В сфері інформаційного суспільства значний внесок у розвиток знань зробили такі вчені, як А. Берг, Е. Тоффлер, Ю. Харари, М. Кастельс, Д. Тапскотт, Ф. Уебстер, Д. Белл, Е. Масуда, З. Бжезинський, Г. Хакен, А. Блюменау, П. Браун, К. Шеннон, Б. Ківі, Н. Вінер Д. Фонтейн,Ф., Т. Парсонса, Ю. Хабермаса, Н. Лумана, В. Майер-Шенбергер, К. Кукьерта інші.

Науково-теоретичні та методологічні аспекти розвитку публічного управління в сфері інформаційної безпеки держави досліджувалися в працях вітчизняних учених, зокрема В. Горбулин, О. Власюк, О. Кохановський, В. Ліпкан, О. Крюков, Є. Макаренко, А. Марущак, Я. Романовський, О. Сенченко, В. Тертічко, С. Луценко, В., Радченко, П. Маслянко, Г. Почепцов, О. Данільян, В. Степанов, О. Валевський, Б. Кормич, Ю. Древаль та інші, присвятили свої праці різним аспектам проблеми інформаційного суспільства та забезпечення національної безпеки.

За останні роки в сфері інформаційного розвитку держави та суспільства

спостерігалися значні зміни, які вплинули на зміст та сутність державної інформаційної політики. Незважаючи на це, ці трансформації ще не отримали необхідного глибокого відображення у комплексних дослідженнях в рамках сучасної науки публічного управління.

У контексті формування та розвитку цифровізації в Україні та її впливу на соціально-економічний розвиток країни в найближчому майбутньому до 2024-2030 років, державна інформаційна політика набуває особливого значення. Сучасний теоретичний підхід до цієї політики характеризується фактичною "розкиданістю" і дублюванням проведених досліджень. Це створює певні ризики, оскільки існуюча система знань може вже завтра не відповідати умовам нового цифрового суспільства та держави, а також новим інформаційним відносинам.

Отже, важливо зосередити увагу на систематизації та узагальненні досліджень у сфері інформаційної політики, а також на створенні нових концепцій, які відповідали б сучасним викликам цифрового суспільства. Це допоможе забезпечити ефективну адаптацію держави та суспільства до швидкозмінних умов інформаційного середовища та досягнення стійкого розвитку в цифровій епохі.

Зв’язок роботи з науковими програмами, планами, темами. Дисертацію виконано в межах науково-дослідної роботи за темами «Розробка наукових основ державного управління у сфері безпеки ринку соіально-економічних послуг України з точки зору цивільного захисту» (ДР № 0112U002587), що розробляється навчально-науково-виробничим центром Національного університету цивільного захисту України У межах цієї теми автором обґрунтовано підходи до вдосконалення публічного управління у сфері інформаційної безпеки держави.

Мета та завдання дослідження. Метою дисертаційної роботи є обґрунтування теоретичних засад та розробка практичних рекомендацій щодо удосконалення публічного управління у сфері інформаційної безпеки держави.

Для досягнення мети дисертаційного дослідження знадобилося вирішення

низки взаємозалежних завдань:

- визначити місце та роль інформаційної безпеки в системі національної безпеки держави;
- оцінити стан реалізації публічного управління у сфері інформаційної безпеки;
- проаналізувати механізми публічного управління у сфері інформаційної безпеки України;
- систематизувати закордонний досвід розробки та впровадження інформаційного забезпечення державної безпеки;
- розкрити використання цифрових технологій в публічному управлінні у контексті модернізації інформаційної безпеки держави;
- запропонувати підходи до вдосконалення соціально-політичного та організаційно-правового механізмів публічного управління у сфері інформаційної безпеки.

Об'єкт дослідження – інформаційна безпека держави.

Предмет дослідження – публічне управління у сфері інформаційної безпеки держави.

Методи дослідження. Методологічну базу дисертаційної роботи становить сукупність способів наукового пізнання та загальнонаукових методів, необхідних для проведення дослідження. Вони ґрунтуються на фундаментальних положеннях і працях науковців з питань публічного управління та пов'язаних із нею наук.

Дисертаційне дослідження побудовано на *концептуальному, системному й організаційно-функціональному підходах*, а також сукупності методів, які забезпечують їх реалізацію, а саме: 1) загальнонаукових (індукції, дедукції, аналізу, синтезу, порівняння, аналогії); 2) філософсько-аксіологічних (діалектичного, системного та порівняльного); 3) спеціально-наукових (інституційного, структурно-функціонального та структурно-динамічного (перш за все, в рамках осмислення сучасного стану публічного управління у сфері інформаційної безпеки держави), діяльнісного, ситуативного); 4)

порівняльно-історичного (при побудові періодизації еволюційних етапів становлення та реалізації державної інформаційної політики з кінця 1990-х рр. до теперішнього часу). Крім того, особливо наголосимо на методі концептуального аналізу, а також міждисциплінарного політико-правового аналізу (в контексті осмислення стану повноти нормативно-правової забезпеченості інформаційної безпеки та достатності програмно-стратегічних документів); 5)*моделювання й логічного узагальнення* (під час визначення підходів до вдосконалення соціально-політичного та організаційно-правового механізмів публічного управління у сфері інформаційної безпеки) тощо.

Нормативно-інформаційну базу дослідження склали закони України, укази Президента України, постанови Кабінету Міністрів України, нормативні документи органів державної влади України, Міністерства освіти і науки України, матеріали анкетування, результати особистих напрацювань автора, а також зарубіжні й вітчизняні наукові джерела з досліджуваної проблематики.

Наукова новизна одержаних результатів полягає у визначенні науково-теоретичних засад та практичних рекомендацій щодо удосконалення публічного управління у сфері інформаційної безпеки держави.

Наукова новизна результатів конкретизується в таких положеннях:

уперше:

– визначено стратегічні орієнтири функціонування та розвитку публічного управління у сфері інформаційної безпеки через розробку і реалізацію державної інформаційної політики, яка відповідає сучасним викликам, що стоять перед державою, та приділяє увагу формалізації цієї політики на відповідній нормативно-правовій базі;

удосконалено:

– напрями функціонування організаційно-правових та соціально-політичних механізмів публічного управління у сфері інформаційної безпеки в умовах використання цифрових технологій, що дозволило розкрити особливості сучасного стану, концептуального, стратегічного та нормативно-

правового забезпечення реалізації державної інформаційної політики, надало можливість сформулювати відповідні науково-теоретичні та практичні рекомендації для покращення інформаційної безпеки в умовах цифровізації.

- інструменти розробки та впровадження інформаційного забезпечення держави на основі впровадження закордонного досвіду у вигляді удосконалення законодавства для забезпечення інформаційної безпеки, впровадження сучасних методів управління ризиками у сфері забезпечення інформаційної безпеки, взаємодії з міжнародними організаціями та країнами в напрямі обміну досвідом, створення спільних стратегій і протидії кіберзагрозам, розвитку системи підготовки кваліфікованих кадрів у галузі забезпечення інформаційної безпеки країни;

дістали подальшого розвитку:

– періодизація інформаційного розвитку України, на основі якої аналізується практика застосування сучасних цифрових технологій у публічному управлінні, що дозволяє розглядати сучасні цифрові технології як фактор модернізації інформаційної політики України;

- наукові підходи до визначення тенденцій функціонування публічного управління у сфері інформаційної безпеки через розробку і реалізацію державної інформаційної політики, яка відповідає сучасним викликам, що стоять перед державою, та формалізації цієї політики на відповідній нормативно-правовій базі.

Практичне значення одержаних результатів. Основні положення й висновки дисертації можуть використовуватися фахівцями під час написання підручників і навчальних посібників, створення навчально-методичної літератури; в роботі органів державної влади та у процесі формування сучасних засад публічного управління у сфері інформаційної безпеки держави.

Теоретичні та практичні напрацювання автора використовуються в Управлінні у справах молоді та спорту Харківської обласної військової адміністрації (довідка про впровадження № 01-29/915 від 25.06.2024).

Практичні рекомендації автора використовуються Черкаською районною

радою Черкаської області в питаннях удосконалення інформаційної безпеки при впровадженні нових автоматизованих систем обробки даних та обміну інформації (довідка №36/01-13 від 26.06.2024 р.).

Особистий внесок здобувача. Дисертаційна робота є самостійною науковою працею, теоретичні та прикладні результати якої отримано особисто здобувачем. Конкретний внесок здобувача в науковій праці, підготовленій у співавторстві, зазначений у списку опублікованих праць за темою дисертації [77;78;195-197].

Апробація результатів дисертації.

VIII Міжнародної заочної науково-практичної конференції «Формування ефективних механізмів державного управління та менеджменту в умовах сучасної економіки: теорія і практика» (м. Запоріжжя, 2020 р.); Міжнародної науково-практичної інтернет-конференції «Організаційно-методологічне забезпечення підготовки фахівців: тенденції, проблеми та шляхи їх вирішення (з нагоди 90-річчя ХНАДУ)» (м. Харків, 2020 р.); Міжнародної науково-практичної конференції MicroCAD-2020 «Інформаційні технології: наука, техніка, технологія, освіта, здоров'я» (м. Харків, 2021 р.); Круглого столу «Формування дієвих механізмів державного управління з забезпечення державної безпеки» (м. Харків, 2021 р.); Міжнародної науково-практичної інтернет-конференції «Публічне управління у сфері цивільного захисту: освіта, наука, практика» (м. Харків, 2024 р.).

Публікації. Основні положення дисертаційної роботи опубліковано в 10 наукових працях, із них: 2 статті у вітчизняних наукових фахових виданнях, 3 в іноземних наукових виданнях та 5 тез доповідей на конференціях. Загальний обсяг публікацій автора відповідно до теми дослідження становить 5,313 друк. арк.

Структура та обсяг дисертації. Робота складається зі вступу, трьох розділів, висновків, списку використаних джерел, додатків. Загальний обсяг дисертації 197 сторінок. Обсяг основного тексту становить 171 сторінок. Список використаних джерел включає 215 найменувань.

РОЗДІЛ І .
ТЕОРЕТИЧНІ ОСНОВИ ПУБЛІЧНОГО УПРАВЛІННЯ У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ

1.1. Інформаційна безпека в системі національної безпеки: управління процесами її формування

Сучасне геополітичне та соціально-економічне становище України робить особливо актуальним захист її інтересів та забезпечення національної безпеки. Україна стикається зі зростаючим військовим протистоянням з російською федерацією, а також із складними процесами формування нового соціально-економічного та політичного ладу. Це відбувається в умовах кризового періоду, що впливає на всі аспекти життя суспільства. Водночас з військовою конфронтацією з'явилася низка нових зовнішніх та внутрішніх загроз. Подолання цих загроз вимагає глибокого усвідомлення та осмислення питань, пов'язаних із сутністю національної безпеки та напрямками її забезпечення.

Національна безпека є найважливішою складовою системи безпеки і тісно пов'язана з економічним, політичним, соціальним та духовно-моральним розвитком держави. Це питання постійно знаходиться в центрі уваги органів влади, громадськості та науковців всіх країн. Можна впевнено стверджувати, що проблеми національної безпеки мають загальносвітовий характер.

У сучасних умовах в Україні та світі вивчення проблем національної безпеки набуло критичної важливості. Останніми роками з'явилися значні методологічні та світоглядні роботи, присвячені дослідженню цього соціального явища. Дослідження в галузі національної безпеки, попри їх загальні спільні риси, можна розділити на кілька категорій, базуючись на різних підходах до цієї проблеми [82]. Одна з таких позицій полягає у здатності національної безпеки протистояти будь-яким негативним та деструктивним впливам, незалежно від їхнього походження. Інша позиція, що визначає проблеми національної безпеки України, акцентує на рівні захищеності країни від негативного впливу різноманітних факторів – економічного, політичного, військового,

гуманітарного, екологічного та інших. Елементи національної безпеки відображають соціальні інтереси особистості, суспільства та держави. Серед найбільш традиційних і актуальних на сьогодні елементів національної безпеки можна виділити:

- Політичну безпеку;
- Економічну безпеку;
- Соціальну безпеку;
- Правову безпеку;
- Енергетичну безпеку;
- Технологічну безпеку;
- Продовольчу безпеку;
- Екологічну безпеку;
- Інформаційну безпеку.

Ці елементи охоплюють різні аспекти життя суспільства і держави, забезпечуючи їхню стабільність і безпеку в різних сферах.

Беручи до уваги стрімкий розвиток технологій та збільшення кількості цифрових загроз, інформаційна безпека стає все важливішою складовою національної безпеки. Цей елемент відображає не лише захист інформації від несанкціонованого доступу, а й управління даними, кібербезпеку, захист від кібератак та інші аспекти цифрової безпеки. Таким чином, інформаційна безпека стає ключовим фактором у забезпеченні стійкості та безпеки суспільства і держави в цифрову епоху.

Зростання кількості інформації та її легка доступність відкривають необмежені можливості для розвитку, але водночас постає і загроза збільшення ризиків у сфері безпеки. У сучасному цифровому світі, де обмін інформацією відбувається миттєво, захист конфіденційності, цілісності та доступності цієї інформації стає додатково важливим завданням для кожної держави. Інформаційна безпека стає основою, на якій ґрунтується загальна національна безпека [52]. Вона не тільки забезпечує захист державних та особистих інформаційних ресурсів від небажаного втручання, а й регулює та контролює

потоки інформації, що циркулюють в суспільстві. Отже, інформаційна безпека є ключовим елементом національної безпеки, адже забезпечення конфіденційності, цілісності та доступності інформації має стратегічне значення для держави.

Проблеми, пов'язані з інформаційним забезпеченням безпеки держави, не нові, і вони систематично розглядаються як вітчизняними, так і зарубіжними дослідниками. Різні аспекти цієї проблематики вивчаються в наукових працях відомих авторів, таких як Белінська М. [183], Бейкер Дж. [182], Власюк О. [11], Довгань О. [35], Доронін І. , Золотар О. [50], Койен Г. [17*], Абомхара М. [179], Г. Почепцов, [118], В. Степанов [159], С. Чукут[119], А. Фомін та інші. Проте питання співвідношення інформаційних аспектів у формуванні національної безпеки сучасних держав у контексті державно-управлінської проблематики залишається маловивченим у науковій літературі.

В цьому контексті першим підрозділом нашого дослідження є аналіз основних напрямків забезпечення і управління інформаційною безпекою держави, як найважливішою складовою національної безпеки в умовах глобалізаційних процесів. Сучасні умови вказують на те, що інформація стала одним із найважливіших ресурсів для розвитку цивілізації. Проте її необережне використання може мати негативні наслідки для інтересів окремих осіб, суспільства та держави.

Розвиток інформаційно-комунікаційних технологій (ІКТ) та їх широке розповсюдження у всіх аспектах людського життя стали ключовими факторами глобальної інтеграції, соціального прогресу та економічного зростання. Однак разом із розвитком ІКТ виникають як явні, так і потенційні загрози. Це робить питання забезпечення інформаційної безпеки надзвичайно актуальним, оскільки вона є однією з ключових складових національної безпеки. У постіндустріальному світі, де інформація стала головним ресурсом і визначає тактичні та стратегічні рішення на рівні публічного управління, інформаційна безпека є фундаментальним елементом національної безпеки держави.

Попри значний інтерес науковців до питання забезпечення інформаційної безпеки, багато аспектів залишаються недостатньо дослідженими. Це ускладнює процес розробки ефективної системи захисту інформації для України. Подальше вивчення цих аспектів є важливим для створення надійних механізмів захисту інформації на рівні суспільства та держави.

Активне і необоротне впровадження ІКТ змінює не лише спосіб життя, але й діяльність особистості, суспільства та держави. Терміни, які кілька років тому були новими, такі як "інформаційна революція", "інформаційне суспільство" та "інформаційна безпека", сьогодні стали загальновідомими та зрозумілими не лише експертам і науковцям, але й звичайним користувачам інформації. Інформаційна безпека означає забезпечення належного захисту особистості, суспільства та держави від ризиків, загроз і небезпек інформаційного характеру.

В Стратегії національної безпеки України простежуються елементи інформаційної безпеки стосовно засобів національної безпеки, таких як "засоби забезпечення національної безпеки". Це включає технології, а також різноманітні технічні, програмні, лінгвістичні, правові та організаційні засоби. Такі засоби використовуються в системі забезпечення національної безпеки для збору, обробки, передачі або отримання інформації про стан національної безпеки та заходів щодо її зміцнення [140].

У контексті інформаційної безпеки важливо аналізувати та прогнозувати негативні впливи глобальних подій на національні інтереси України. Особлива увага приділяється діям російської федерації, яка використовує енергетичну та інформаційну "зброю" для посилення своїх позицій у Європі, впливаючи на внутрішню політичну ситуацію у європейських країнах та підтримуючи тривалі конфлікти [139].

Зростаюче глобальне інформаційне протистояння створює серйозні загрози для стабільності як індустріальних, так і країн, що розвиваються. Ці загрози можуть підірвати їх соціально-економічний розвиток та демократичні інститути. Збільшується націоналізм, ксенофобія, сепаратизм та екстремізм,

ускладнюючи соціальну гармонію та міжнаціональну взаємодію [90]. Ключові аспекти цієї ситуації включають:

- дезінформація та кіберпропаганда, що стали одними з найсерйозніших загроз у сучасному інформаційному просторі. Ці явища включають використання масштабних інформаційних кампаній для маніпулювання громадською думкою в інших країнах через поширення дезінформації, фейкових новин та кібератак. Дезінформація часто використовується для впливу на вибори та політичні процеси. Вплив на громадську думку через поширення панічних чи провокаційних повідомлень може призвести до громадських заворушень чи підриву довіри до урядових інституцій. Кіберпропаганда включає використання цифрових технологій та інтернет-ресурсів для поширення пропагандистських матеріалів. Основні методи становлять соціальні мережі, використання платформ, таких як Facebook, Twitter, Instagram для поширення фейкових новин та маніпуляцій. Боти та тролі можуть штучно збільшувати охоплення пропагандистських матеріалів та створення та підтримка фейкових новинних сайтів та блогів, які виглядають як легітимні джерела інформації, але поширюють неправдиву інформацію.

- кіберзагрози, інформаційні та кібератаки можуть завдати значних матеріальних збитків, порушити діяльність критично важливих інфраструктур та призвести до витоку конфіденційної інформації. Це особливо небезпечно для країн, що залежать від інформаційних технологій для свого економічного та соціального розвитку;

- поляризація суспільства, спричинена інформаційним протистоянням, є серйозною загрозою для стабільності як індустріальних країн, так і країн, що розвиваються [21]. Вона може призвести до зростання соціальної напруги, коли різні групи населення стають все більш ворожими одна до одної. Це може проявлятися у вигляді протестів, заворушень та навіть насильницьких конфліктів. Суспільство часто має проблеми з досягненням політичного консенсусу, що ускладнює прийняття важливих рішень та здійснення реформ.

Це може послабити демократичні інститути і створити умови для авторитарних тенденцій. Постійна дезінформація та маніпуляції можуть призвести до того, що громадяни втрачають довіру до традиційних медіа та державних інституцій, підриваючи здатність уряду ефективно керувати країною та реагувати на кризи. Таким чином, інформаційне протистояння та його наслідки є критичними викликами, що вимагають адекватних відповідей та стратегій для збереження стабільності та розвитку суспільства.

- економічні наслідки. Соціальна та політична нестабільність , зростаючи кіберзагрози негативно впливають на економіку. Інвестори можуть уникнути данні країни, що призводить до скорочення інвестицій та повільного економічного зростання.

Інформаційне протистояння продовжує наростати, і перевага буде на боці тих, хто володіє більш вдосконаленими технологіями, що дозволяють оптимально використовувати їх у своїх цілях. Особливо це стосується розвитку націоналізму, ксенофобії, сепаратизму, екстремізму та релігійного радикалізму, де інформаційні технології відіграють ключову роль у пропаганді ідеологій.

Завдання інформаційної безпеки полягає в виявленні, припиненні та контрпропаганді зазначених явищ для забезпечення стабільності України. Ефективність цієї діяльності залежить від комплексного підходу з використанням всіх механізмів публічного управління[53].

Постійний розвиток інформаційних технологій суттєво впливає на всі аспекти публічного управління, охоплюючи як рутинні операції, так і вирішення складних стратегічних завдань. Використання комп'ютерних та інформаційних систем та технологій поширюється від звичайного користувача до публічних управлінських структур, включаючи і силові відомства. Це відкриває нові можливості не лише для інформаційного обміну та отримання інформації про дійсність, а й для різноманітних видів кримінальної діяльності, таких як хакерство, злам електронних та комп'ютерних систем для здійснення економічного та політичного шантажу чи навіть терористичних актів. Використання цих технологій вимагає постійного вдосконалення заходів

безпеки, щоб убезпечити систему від можливих загроз і атак [36].

Рівень розвитку промисловості та економіки країни суттєво визначається використанням інформаційно-комунікаційних технологій, які мають вплив на організацію суспільства, склад соціальних груп, рівень життя та освітні процеси. Ця залежність лише посилюється з кожним днем.

Негативні інформаційні процеси можуть серйозно впливати на різні сфери життя, включаючи організацію праці, соціальні відносини, охорону здоров'я тощо. Такі впливи можуть включати технологічні неполадки, витік конфіденційної інформації, а також використання інформаційних технологій для формування асоціальних норм поведінки та ворожості до національних і державних цінностей та інтересів. Пропаганда насильства, жорстокості, сексу та матеріалізму, а також ідеалізація багатства та успіху незалежно від ціни, можуть сприяти руйнуванню духовних та моральних цінностей у суспільстві. Цей негативний вплив може поширюватися та поглиблюватися завдяки інформаційно-комунікаційним технологіям, які дозволяють масово розповсюджувати різноманітний контент.

На сьогоднішній день немає сумніву у тому, що з розвитком інформаційного та технологічного суспільства можлива кібернетична війна. З урахуванням постійного вдосконалення і зростання якості інформаційно-комунікаційних технологій, а також їх доступності, сучасна міжнародна обстановка відзначається наростанням міжнаціональної напруги, територіальними та конфесійними конфліктами, а також активністю радикальних груп та могутніх держав. Зрозуміло, що науково-технічний прогрес, включаючи інформаційно-комунікаційні технології, буде використовуватися для досягнення конкретних та загрозливих для цивілізації цілей. Нейтралізація таких тенденцій, включаючи активну протидію відповідним інформаційним війнам, пропаганді, інтелектуальному маніпулюванню поряд з технологічними аспектами, такими як захист від несанкціонованого вторгнення власних інформаційних ресурсів, також є одним із пріоритетних напрямків захист [80].

Різні категорії суб'єктів публічного управління можуть мати різне розуміння та тлумачення проблем інформаційної безпеки. Проте загалом можна виділити кілька основних інтересів суб'єктів, які використовують інформаційно-комунікаційні технології, зокрема забезпечення доступності, цілісності та конфіденційності інформації, а також безпеки її інфраструктури. Метою заходів у сфері інформаційної безпеки є захист цих інтересів у контексті інформаційних відносин. Ці інтереси можуть бути різноманітними, але їх всі можна об'єднати навколо трьох основних характеристик: доступності, цілісності та конфіденційності. Так само, інформаційну безпеку можна тлумачити як відсутність недопустимого ризику, пов'язаного з можливою прямою або непрямою шкодою, спричиненою порушенням конфіденційності, цілісності та доступності інформації.

Основні напрями публічного управління в сфері інформаційної безпеки можна розділити наступним чином:

- в сфері діяльності державних органів;
- суспільна інформаційна безпека;
- в сфері захисту особистих інтересів [45].

Однією з важливих характеристик інформаційної безпеки суспільства і держави є їх захищеність. Це означає стійкість усіх головних сфер життєдіяльності, таких як економіка, наука, технології, публічне управління тощо, до всіх можливих небезпечних інформаційних впливів, які можуть бути дестабілізуючими або деструктивними. Ці впливи можуть бути спрямовані на зацікавленість країни, незалежно від того, чи їх виконують у формі впровадження (підкидання) чи навпаки, вилучення інформації.

В умовах сучасності інформаційна безпека набуває вирішального значення для захисту держави та суспільства від різноманітних негативних впливів і загроз. Цей аспект національної безпеки зумовлюється здатністю нейтралізувати небезпечний інформаційний вплив, який може бути спрямований на людську свідомість, психіку, а також на інформаційно-технічні системи будь-якого масштабу та призначення [170]. Серед соціальних об'єктів,

які потребують захисту, можна виділити особу, групи людей (спільноти), суспільство в цілому та державу [21].

Інформаційна безпека передбачає захист цих об'єктів не тільки від технічних загроз, але й від соціальних. Соціальні аспекти інформаційної безпеки включають протидію дестабілізуючому та деструктивному інформаційному контенту, що може бути впроваджений у інформаційно-комунікаційні технології з метою маніпуляції свідомістю та поведінкою особистості, а також впливу на суспільство та державні інтереси.

Ефективність реалізації Стратегії національної безпеки України великою мірою залежить від формування єдиної та цілісної інформаційної політики по всій території країни. Розриви між центром та регіонами в організаційному та технологічному освоєнні інформаційного простору створюють суттєві проблеми в оперативній комунікації та взаємодії між органами державного та регіонального публічного управління. Слабкість регіонів у сфері інформаційного забезпечення безпосередньо впливає на загальну ефективність інформаційної безпеки, що, в свою чергу, ускладнює вирішення завдань національної безпеки [11].

Для забезпечення національної безпеки та стабільності держави необхідно ретельно враховувати соціальні аспекти інформаційної безпеки та постійно вдосконалювати інформаційну політику на всій території країни. Це дозволить реалізувати Стратегію національної безпеки України не лише на декларативному рівні, але й на практиці, забезпечуючи захист усіх її елементів. Інформаційна складова виступає головним комунікатором, який об'єднує всі аспекти загальнонаціональної безпеки в єдине управлінське ціле.

Інформаційна безпека визначається як стан захищеності інформаційного середовища суспільства, що гарантує його формування, використання та розвиток на благо особистості, суспільства та держави. [45]. Це означає, що важливо гарантувати захист конституційних прав і свобод, особисту безпеку, підвищення рівня життя, а також сприяти фізичному, духовному та інтелектуальному розвитку кожного громадянина.

Захист інформаційного середовища включає в себе не лише технічні заходи, такі як кібербезпека, а й соціальні заходи, які спрямовані на підвищення медіаграмотності населення, розвиток критичного мислення та створення позитивного інформаційного контенту. Консолідація зусиль регіональних та державних органів влади для створення належного інформаційного простору є надзвичайно важливою. Це допоможе забезпечити реальну охорону інформаційного середовища та сприятиме ефективній реалізації національної стратегії безпеки [39].

Співробітництво з міжнародними партнерами у сфері інформаційної безпеки також є надзвичайно важливим. Обмін досвідом і кращими практиками допоможе Україні зміцнити свої позиції та протистояти сучасним викликам і загрозам в інформаційному просторі. Інформаційна безпека у сучасному світі стає ключовим елементом національної безпеки кожної країни, і її значення для забезпечення стабільності, розвитку та захисту інтересів особистості, суспільства і держави важко переоцінити.

Отже, інтеграція технічних і соціальних аспектів інформаційної безпеки, удосконалення національної інформаційної політики та зміцнення співпраці на всіх рівнях управління є критично важливими для забезпечення національної безпеки України. В сучасних умовах це дозволить не тільки захистити інформаційне середовище, але й сприятиме зміцненню загальної стабільності та розвитку держави.

Серед дослідників зарубіжного походження, які активно вивчають аспекти сучасного інформаційного розвитку держави та суспільства, особливе місце займають такі вчені, як Джейн Фонтейн, К. Бвалія, С. М'ючал, До. Реддік, М. Барранекіа, Т. Дженкінс та В. Еггерс. Вони досліджують питання ефективності функціонування "електронного уряду", особливості публічного управління в інформаційну епоху та технологічні аспекти модернізації державних інформаційних систем. Останнім часом також активно досліджуються питання використання хмарних сервісів і технологій, мобільних технологій у системі публічного управління, а також розвитку цифрових державних стратегій. Серед

вчених, що приділяють увагу цим аспектам, варто відзначити С. Фолка, А. Рememеле, М. Сільвермана, А. Бінея та інших.

Незважаючи на значну увагу, яку науковці, що вивчають проблеми інформаційного суспільства, приділяють питанням забезпечення інформаційної безпеки, і попри зусилля у розробці засад і реалізації державної політики в цій галузі, багато аспектів залишаються мало розробленими. Це ускладнює розбудову ефективної системи забезпечення інформаційної безпеки Української держави.

Ефективна державна політика в інформаційній сфері, включаючи аспекти інформаційної безпеки, залежить від правильного визначення пріоритетів у наукових дослідженнях цих проблем, розробки наукових моделей і підходів до їх вирішення. Особливо важливо проводити публічно-управлінський аналіз проблем інформаційної безпеки у сучасних умовах. Останнім часом з'явилася низка робіт зарубіжних дослідників, присвячених використанню хмарних сервісів і технологій, мобільних технологій у системі публічного управління, розвитку цифрових державних стратегій. Серед цих дослідників можна відзначити С. Фолка, А. Рememеле, М. Сільвермана, А. Бінея та інших. На жаль, зарубіжний досвід державної інформаційної політики у вітчизняній науці досліджено недостатньо широко.

Публічне управління переходить на новий етап, який характеризується використанням цифрових технологій [33]. Ці технології вже починають визначати новий зміст державної інформаційної політики України. Швидкий розвиток цифрових технологій та їх інтеграція у повсякденне життя громадян і функціональну діяльність державних органів лише підсилює усвідомлення того факту, що розробка нового змісту "державна інформаційна політика" неможлива без аналізу складу та особливостей інформації, її нових форм у вигляді "Великих даних" (BigData) і "Відкритих даних" (OpenData), а також інформаційних і цифрових технологій, які впливають на її реалізацію [207].

Очевидно, що зміст державної інформаційної політики та її напрями сильно трансформувалися за останні 25-30 років. Якщо на етапі становлення

української державності основним інформаційним законом був Закон про інформацію, то сьогодні нормативно-правове регулювання інформаційної сфери кардинально змінилося в бік інформаційних та цифрових технологій, «великих» та «відкритих» даних, Інтернет-участі, розвитку електронної демократії, політико-адміністративних механізмів електронної взаємодії органів державної влади та структур громадянського суспільства.

Сучасний етап розвитку державної інформаційної політики України характеризується широким впровадженням цифрових технологій, що змінюють не лише спосіб взаємодії громадян з органами влади, але й саму сутність адміністративних процесів. Зокрема, розвиток електронних послуг та систем електронного урядування дозволяє забезпечити більш прозоре, швидке та ефективне управління державними ресурсами [215]. Це включає впровадження електронного документообігу, систем електронного голосування, платформ для громадських обговорень та інші інструменти, які сприяють підвищенню рівня участі громадян у процесах прийняття рішень.

Виходячи з викладеного, розробка авторського операційного визначення поняття «державної інформаційної політики» є важливим дослідницьким завданням. Це передбачає врахування чинної практики інформаційної діяльності у сфері публічного управління, розвиток проектів електронного уряду, визначення політичного курсу на цифровізацію економіки, а також дедалі ширше застосування цифрових технологій у публічному управлінні та формуванні інформаційного суспільства[202].

Слід зазначити, що загалом опублікованих наукових праць у галузі використання цифрових технологій у публічному управлінні вкрай недостатньо. Сучасні дослідження державної інформаційної політики поки що практично не враховують так званий «цифровий фактор».

Термін «цифровізація» останнім часом вживається все частіше. Він пов'язаний не лише з трансформацією технологічного укладу та переходом від використання електронних технологій до цифрових, але й з державною інформаційною політикою у сфері інформаційних та цифрових технологій [178].

У цифрову епоху основним фактором, що впливає на трансформацію інформаційного устрою суспільства та інформаційний розвиток держави, стають так звані «великі дані» (BigData) та їх аналітика. «Інформаційний» фактор у структурі та змісті державної інформаційної політики продовжує займати домінуючі позиції за одночасного використання цифрових технологій пошуку, збору, обробки інформації та аналітики великих даних. Отже, в умовах розвитку процесів використання цифрових технологій дослідження державної інформаційної політики набувають ще більшої актуальності.

Виходячи з вищевикладеного, вважаємо за необхідне запропонувати авторське визначення поняття «державна інформаційна політика» в умовах використання цифрових технологій. «Державну інформаційну політику» в умовах використання цифрових технологій слід розуміти у вузькому та широкому значенні.

У вузькому, найбільш узагальненому значенні, це політика держави у використанні сучасних цифрових технологій у всіх сферах суспільства (політичній, економічній, соціальній, духовній) та публічному управлінні.

У широкому значенні, завдяки використанню сучасних цифрових технологій у всіх сферах суспільства, розширюється традиційне розуміння державної інформаційної політики, сформоване за останні більш ніж чверть століття. Таким чином, державна інформаційна політика в широкому розумінні - це діяльність, спрямована на формування та реалізацію політики у галузі засобів масової інформації, зв'язку, розвитку інформаційного суспільства та активного використання інформаційних технологій органами публічної влади, бізнесом і населенням країни, включаючи Інтернет та сучасні цифрові технології. З урахуванням цифрового фактора, державна інформаційна політика повинна забезпечувати ефективне використання цифрових технологій у всіх сферах суспільного життя, сприяти розвитку інформаційного суспільства та зміцненню національної безпеки. Це завдання вимагає систематичних досліджень і вдосконалення підходів до реалізації інформаційної політики в умовах цифрової трансформації[9].

Одним із важливих аспектів сучасної державної інформаційної політики є забезпечення кібербезпеки. З ростом використання цифрових технологій зростає і кількість загроз, пов'язаних з кіберзлочинністю, хакерськими атаками та іншими формами інформаційних загроз. Це вимагає розробки та впровадження комплексних заходів захисту інформаційних систем, які включають як технічні рішення, так і нормативно-правові механізми. Забезпечення кібербезпеки стає невід'ємною частиною національної безпеки, що підкреслює важливість цього питання для стабільного розвитку держави [16].

Крім того, важливим напрямом державної інформаційної політики є розвиток системи освіти та підвищення рівня цифрової грамотності населення. В умовах стрімкого розвитку інформаційних технологій важливо забезпечити громадянам доступ до сучасних знань та навичок, необхідних для ефективного використання цифрових інструментів [47]. Це включає як формальну освіту в навчальних закладах, так і програми підвищення кваліфікації для дорослих, що дозволяє їм адаптуватися до нових вимог ринку праці та суспільства в цілому.

Суттєвим елементом сучасної інформаційної політики є також питання захисту персональних даних. У зв'язку зі зростанням обсягів оброблюваної інформації, особливо персональних даних громадян, виникає необхідність у створенні ефективних механізмів їхнього захисту. Це включає як технічні засоби, так і правові норми, що регламентують збір, зберігання та обробку персональних даних, забезпечуючи при цьому права громадян на приватність.

Безумовно, змінилися зміст та структура державної інформаційної політики України. У зв'язку з цим правомірно стверджувати про динамізм змісту та структури державної інформаційної політики в сучасній Україні. Одним з важливих завдань науки публічного управління є на постійній основі, з урахуванням впливу сучасних ІКТ та цифрових технологій на розвиток держави та суспільства, переглядати та модернізувати поняття «державна інформаційна політика».

Наука публічного управління має постійно враховувати швидкоплинні зміни в інформаційній сфері та розробляти рекомендації щодо вдосконалення

державної інформаційної політики [171]. Це включає не лише реагування на нові виклики та загрози, але й проактивний підхід до впровадження інновацій та передових технологій. Розробка стратегій та політик, які враховують глобальні тенденції та специфіку національного контексту, є запорукою успішного розвитку інформаційного суспільства в Україні.

Таким чином, сучасна державна інформаційна політика повинна бути гнучкою, динамічною та орієнтованою на майбутнє. Вона повинна забезпечувати належний рівень безпеки та захисту інформації, сприяти розвитку цифрових навичок населення, підтримувати інновації та враховувати глобальні тенденції розвитку інформаційного суспільства. Лише за таких умов можна досягти стабільного та сталого розвитку держави та забезпечити високий рівень життя громадян у сучасному інформаційному світі.

1.2 Основні напрями забезпечення інформаційної безпеки держави

Інформаційна безпека сьогодні є однією з найбільш важливих проблем у сучасному світі. З розвитком технологій та поширенням цифрових загроз виникає необхідність ефективних заходів забезпечення безпеки інформації. Протягом останніх десятиліть інформаційний аспект розвитку суспільства привертав увагу як зарубіжних, так і вітчизняних науковців.

Галузь інформаційного забезпечення державної влади спирається на теоретичні основи, закладені як зарубіжними, так і вітчизняними дослідниками. Серед зарубіжних авторів, чиї праці стали фундаментальними для цієї галузі, варто згадати таких відомих науковців, як Деніел Белл, Елвін Тоффлер, Мануель Кастельс та Фрэнк Вебстер. Їхні роботи зосереджуються на дослідженні інформаційного суспільства, впливу інформаційних технологій на суспільство та ролі інформації в сучасному світі.

Значний внесок у розвиток теорії інформаційного забезпечення зробили і вітчизняні вчені, такі як Олександр Бухтатий, Сергій Луценко, Олександр Крюков, Георгій Почепцов, Володимир Степанов та Сергій Чукут [119]. Їхні дослідження охоплюють широкий спектр питань, пов’язаних з інформаційною безпекою, державним управлінням та комунікаційними технологіями.

Мета досліджень у цій галузі полягає у вивченні інформаційного забезпечення як окремого виду управлінської діяльності. Особливу увагу приділяють аналізу ролі інформації в діяльності державних органів та її впливу на національну безпеку. Інформаційне забезпечення включає в себе процеси збору, аналізу та розповсюдження інформації, що безпосередньо впливають на прийняття рішень у сфері безпеки держави.

Національна безпека включає широкий спектр заходів, таких як політико-дипломатичні ініціативи, публічне управління, економічні стратегії, правове регулювання, військові дії та інформаційні заходи. Ключовим елементом цього комплексу є інформаційне забезпечення, яке формує основу для ефективного прийняття рішень та координації дій державних органів [72].

Інформаційне забезпечення сприяє збору, аналізу та розповсюдженню критично важливої інформації серед відповідних органів влади. Це дозволяє своєчасно реагувати на потенційні загрози, забезпечувати належний рівень безпеки та стабільності держави. У сучасних умовах, коли інформаційні технології швидко розвиваються, важливо розуміти та ефективно використовувати інформаційне забезпечення для підтримання національної безпеки.

Інформаційне забезпечення включає такі найважливіші аспекти, як збір даних, їх обробка та аналіз, передача інформації, а також збереження інформаційних ресурсів [95]. Кожен з цих аспектів має значення для забезпечення національної безпеки, оскільки від своєчасного та точного інформаційного забезпечення залежить ефективність рішень, що приймаються державними органами. Таким чином, інформаційне забезпечення як окремий вид управління відіграє важливу роль у впровадженні стратегій національної безпеки. Воно забезпечує стійкість та стабільність держави, дозволяючи їй ефективно реагувати на виклики та загрози сучасного світу.

З часів здобуття незалежності в Україні поступово сформувалася нормативно-правова база для забезпечення інформаційної безпеки, яка еволюціонувала протягом кількох десятиліть [50]. Цей процес можна розділити на кілька основних етапів, кожен з яких відзначений прийняттям важливих законодавчих актів та підзаконних нормативних документів.

1990-ті роки

1. Закон України «Про інформацію» (1992). Цей закон встановлює основні принципи інформаційної діяльності, її правовий режим та механізми захисту. Він є основою для розвитку інформаційного законодавства в Україні.

2. Закон України «Про захист інформації в автоматизованих системах» (1994). Закон встановлює правові основи захисту інформації, що обробляється в автоматизованих системах, що було важливим на початку цифрової ери.

3. Постанова Кабінету Міністрів України «Про затвердження Положення про технічний захист інформації в Україні» (1998). Ця постанова визначає

порядок захисту інформації, що циркулює в інформаційних системах, закріплюючи основні вимоги до технічного захисту даних.

2000-ті роки

4. Закон України «Про державну таємницю» (2003). Цей закон регулює питання охорони державної таємниці, встановлюючи правові основи для захисту секретної інформації [124].

5. Закон України «Про основні засади забезпечення кібербезпеки України» (2005). Закон окреслює основи політики держави у сфері кібербезпеки, забезпечуючи нормативне підґрунтя для захисту кіберпростору.

2010-ті роки

6. Закон України «Про захист персональних даних» (2010). Закон встановлює правові основи захисту персональних даних під час їх обробки, що є важливим аспектом захисту приватності громадян [133].

7. Закон України «Про доступ до публічної інформації» (2011). Цей закон регулює порядок доступу до публічної інформації, забезпечуючи її відкритість та прозорість для громадськості [126].

8. Закон України «Про електронну ідентифікацію та електронні довірчі послуги» (2017). Закон регулює відносини, пов'язані з наданням електронних довірчих послуг, що є важливим для забезпечення безпеки електронних транзакцій [128].

9. Закон України «Про основні засади забезпечення кібербезпеки України» (2017). Оновлений закон закріплює сучасні напрями кібербезпеки, враховуючи нові виклики та загрози в кіберпросторі.

10. Закон України «Про національну безпеку України» (2018). Закон містить положення про забезпечення кібербезпеки та інформаційної безпеки як ключових аспектів національної безпеки.

11. Указ Президента України «Про рішення Ради національної безпеки і оборони України «Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації» (2017). Указ встановлює основні заходи щодо нейтралізації загроз кібербезпеці, визначаючи пріоритетні напрями діяльності.

2020-ті роки

12. Рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України на 2021-2025 роки». Ця стратегія передбачає створення єдиної системи реагування на кіберзагрози та розвиток співпраці з міжнародними партнерами.

13. Рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки». Документ визначає основні напрями забезпечення інформаційної безпеки в умовах сучасних викликів.

14. Розробка нових законів та підзаконних актів. Цей період характеризується активною розробкою та впровадженням нових законів і нормативних актів з урахуванням сучасних викликів у сфері інформаційної безпеки, що забезпечує адекватну відповідь на нові загрози.

15. Інтеграція міжнародних стандартів та директив ЄС у національне законодавство. З метою підвищення ефективності захисту інформації та кібербезпеки відбувається адаптація національних нормативних актів до міжнародних стандартів і директив Європейського Союзу. Це сприяє підвищенню рівня безпеки та узгодженості з міжнародними вимогами.

Таким чином, нормативно-правова база забезпечення інформаційної безпеки в Україні постійно еволюціонує, відповідаючи на нові виклики та загрози. Розвиток цієї бази включає як внутрішнє законодавство, так і адаптацію міжнародних стандартів, що дозволяє забезпечувати належний рівень захисту інформаційного простору держави.

Ґрунтуючись на результатах проведеного аналізу вітчизняної та міжнародної нормативно-правової документації, в рамках дисертаційного дослідження були визначені основні напрями в області забезпечення інформаційної безпеки:

1. Забезпечення та реалізація національної стратегії інформаційної безпеки, що включає в себе:

- визначення стратегічних цілей та пріоритетів у сфері інформаційної безпеки;

- створення національних стандартів і нормативно-правових актів, що регулюють діяльність у цій області;

- координація дій між різними державними органами та установами для забезпечення єдиної політики інформаційної безпеки.

2. Забезпечення технічного захисту інформаційної інфраструктури, що включає в себе:

- використання передових технологій для захисту критичної інформаційної інфраструктури, включаючи державні мережі та системи зв'язку.

- впровадження систем виявлення та запобігання кібератакам, а також використання технологій шифрування та резервного копіювання даних.

- підтримка та оновлення технічних засобів захисту відповідно до сучасних викликів і загроз.

3. Забезпечення кібербезпеки та захисту від кібератак передбачає:

- розвиток державних кіберпідрозділів, здатних оперативно реагувати на кібератаки та інші інциденти;

- проведення регулярних кібернавчань та тестувань на проникнення для оцінки захищеності інформаційних систем;

- впровадження програм моніторингу та аналізу загроз у кіберпросторі.

4. Забезпечення правового та нормативного поля інформаційної безпеки включає:

- розробку та вдосконалення законодавства, що стосується інформаційної безпеки та захисту персональних даних;

- встановлення правових механізмів відповідальності за порушення у цій сфері.

- створення та підтримка нормативно-правової бази для міжнародного співробітництва у галузі кібербезпеки.

5. Забезпечення навчання та підвищення кваліфікації фахівців включає:

- організацію систематичних навчальних програм та тренінгів для державних службовців та спеціалістів у галузі інформаційної безпеки;

- розробку та впровадження програм, які сприяють підвищенню

обізнаності серед населення щодо питань інформаційної безпеки;

- підтримку наукових досліджень та освітніх ініціатив у сфері інформаційної безпеки.

6. Управління інформаційними ризиками та інцидентами охоплює:

- оцінку та визначення інформаційних ризиків, а також розробку відповідних заходів для їх зменшення;

- впровадження систем управління інцидентами в галузі інформаційної безпеки, що дозволяють оперативно виявляти, реагувати та ліквідовувати наслідки подій;

- розробку планів безперервності діяльності та відновлення після виникнення інцидентів.

7. Міжнародне співробітництво у сфері інформаційної безпеки включає:

- участь у міжнародних ініціативах та угодах, спрямованих на підвищення глобальної інформаційної безпеки;

- обмін досвідом та інформацією про потенційні загрози та найкращі практики з іншими країнами та міжнародними організаціями;

- підтримка міжнародних проектів з розробки та впровадження нових технологій захисту інформації.

Ці напрями спрямовані на захист інформації та інформаційних систем від кіберзагроз для забезпечення національної безпеки та ефективного функціонування державних структур. Вони є основними у забезпеченні захисту інформації, а будь-який процес у рамках діяльності по захисту інформації може бути пов'язаним з ними, вводячи єдину систему класифікації діяльності щодо забезпечення публічного управління інформаційною безпекою держави.

Необхідність пропорційного розвитку кожного з цих напрямків обумовлюється їх взаємозв'язком. Відсутність належного рівня розвитку одного з напрямків, порівняно з іншими, неминуче призведе до нераціонального та непродуктивного використання ресурсів системи захисту інформації, а також до фінансових втрат [11].

З огляду на явний безперервний розподіл діяльності даних напрямків, а

також асоційовану децентралізацію їх реалізації, забезпечення своєчасного і раціонального управління даними процесами є одним з основоположних питань сучасної системи захисту інформації [87]. Управління даними напрямами забезпечить значне спрощення реалізації механізмів захисту інформації, забезпечить систематичний моніторинг розвитку кожного напрямку і дозволить більш ефективно розподіляти матеріальні ресурси між ними. Це сприятиме значному підвищенню ефективності реалізованих заходів захисту інформації при збереженні поточного рівня витрат.

Отже, управління процесами забезпечення інформаційної безпеки є ключовою та необхідною складовою будь-якої системи захисту інформації.

Слід звернути увагу, що реалізація системи забезпечення інформаційної безпеки не повинна переслідувати за собою мету забезпечення інформаційної безпеки і поєднувати або дублювати засоби захисту інформації, а повинна бути спрямована лише на збільшення ефективності діючих засобів захисту, підтримувати процеси розвитку інформаційно-телекомунікаційної структури організації і надавати актуальну інформаційно-довідкову підтримку з питань забезпечення інформаційної безпеки, з метою своєчасного прийняття коригувальних та запобіжних впливів і рішень, ґрунтуючись на:

- регламентації процесів захисту інформації;
- обліку і класифікації активів, що підлягають захисту;
- обліку і класифікації ресурсів системи захисту інформації;
- постійного аналізу ризиків інформаційної безпеки і актуалізації моделі загроз інформації;
- моніторинг подій інформаційної безпеки;
- рівні компетенції і професійних можливостей співробітників і обслуговуючого персоналу;
- ступеня навантаження, зайнятості та професійної історії фахівців із захисту інформації;
- аналізі накопичених даних з питань інформаційної безпеки.

Таким чином, одними з невід'ємних складових будь-якої системи

управління інформаційною безпекою повинні бути регламентація і реалізація механізмів щодо:

- централізованого сигналізування і повідомлення співробітників і фахівців із захисту інформації про події всередині системи захисту інформації в цілому;

- аналізу подій всередині системи захисту інформації, що дозволить істотно спростити управління інформаційною безпекою та знизити навантаження на аналітиків з інформаційної безпеки.

Згідно з чинним положенням, система захисту інформації - це взаємопов'язана сукупність організаційних, інженерно-технічних заходів, засобів і методів захисту інформації. Розглянемо типовий підхід до побудови системи захисту інформації, згідно з визначенням і спільного розуміння, така система буде складатися з: технічних засобів захисту інформації; об'єкта захисту; органів і\або виконавців (персоналу, відповідальний за забезпечення інформаційної безпеки); організаційних заходів захисту інформації [134].

Залежно від складу оброблюваної інформації (що входить в об'єкт захисту), вимоги нормативно-правових документів, як внутрішніх, так і зовнішніх встановлюватимуть певні правила взаємодії персоналу, технічних засобів, організаційних заходів і об'єктів захисту.

При типовому підході в складі системи захисту інформації не передбачена єдина підсистема управління організаційними заходами і технічними засобами захисту, яка б дозволяла вести стратегічне, тактичне та оперативне управління інформаційною безпекою, включаючи персонал, наявні засоби захисту, а також організаційні заходи для забезпечення інформаційної безпеки в організації .

Такий стан справ негативно впливає не тільки на ефективність окремо взятих застосовуваних організаційних заходів і технічних засобів захисту, а й на сумарний показник ефективності всієї системи захисту інформації в цілому, а також не дозволяє співробітникам мати впевненість в своєчасності і доцільності застосування тих чи інших заходів захисту , що по суті своїй на певному етапі роботи може бути сприйнята як сигнал про можливість посереднього

відношення до виконуваних процедур.

Один з головних недоліків стандартного підходу до створення системи захисту інформації полягає у відсутності аналітичного компонента для процесів розвитку та підтримки цієї системи. На сьогоднішній день в державі не існує аналітичних інформаційно-аналітичних систем, спрямованих на аналіз та підтримку управлінських рішень у сфері інформаційної безпеки. Ця відсутність суттєво обмежує можливості державних органів та організацій у здійсненні ефективного управління інформаційною безпекою, збільшує ризики виникнення інцидентів та знижує загальний рівень захищеності інформаційної інфраструктури.

Наслідком цього є відсутність розвитку підходів і аналітичних викладок щодо вдосконалення систем захисту інформації, побудова якої зводитися до виконання вимог щодо усунення відомих на даний момент каналів витоку інформації, перекриття та усунення базових загроз інформаційній безпеці, при цьому такий підхід є повністю неефективним в плані протидії новим нестандартним діям ймовірних порушників, а також в разі використання ними нетипових методів обходу засобів захисту [80]. Найчастіше роботи по вдосконаленню систем захисту інформації, що проводяться без урахування поточного стану захищеності об'єктів захисту, а також ефективності застосовуваних методів і способів захисту в конкретних умовах функціонування, як самих об'єктів захисту, так і захисних механізмів, що в кінцевому підсумку призводить до нераціонального планування і витрачання бюджету, що виділяється на забезпечення інформаційної безпеки. Дані фактори також негативно позначаються і на персоналі організації, відповідальному за забезпечення інформаційної безпеки, що відображається на сукупній ефективності системи захисту інформації в цілому, і компетенції співробітників з інформаційної безпеки, зокрема.

Таким чином, в рамках дослідження були проаналізовані чинні міжнародні та вітчизняні нормативно-правові документи, з метою виявлення і систематизації вимог, що пред'являються до систем захисту інформації, за

результатами якого були виявлені основні супутні недоліки типового підходу реалізації системи захисту інформації, які полягають в відсутності єдиної підсистеми управління, що призводить до:

-проблеми відсутності єдиного підходу до управління інформаційною безпекою;

-проблеми створення документів, які не відповідають реальним потребам і вимогам з інформаційної безпеки для реалізації організаційних заходів захисту;

-проблеми неможливості прийняття своєчасних і ефективних управлінських рішень з інформаційної безпеки для забезпечення безперервності роботи системи захисту інформації.

- не використання засобів автоматизації при реалізації організаційних заходів захисту, що призводить до:

-проблеми низької ефективності роботи персоналу, відповідального за забезпечення інформаційної безпеки, при реалізації організаційних заходів захисту;

-проблеми відсутності замкнутості життєвого циклу організаційно-розпорядчих документів щодо інформаційної безпеки;

-проблеми наявності істотних тимчасових розривів між процедурами впровадження технічних засобів захисту і супроводжуючих їх організаційними заходами.

- відсутність аналітичної складової процесів розвитку і забезпечення системи захисту інформації, що призводить до:

- проблеми відсутності можливості протидії новим, нестандартним діям ймовірних порушників, при використанні ними нетипових методів обходу засобів захисту інформації;

- проблеми нераціонального планування і витрачання бюджету, що виділяється на забезпечення інформаційної безпеки через відсутність аналізу поточного стану захищеності об'єктів захисту, а також відсутність аналізу ефективності застосованих методів і способів захисту в конкретних умовах функціонування об'єктів захисту.

На основі результатів аналізу чинних міжнародних і вітчизняних нормативно-правових документів було виявлено основні процеси забезпечення та управління інформаційною безпекою. У ході дослідження сформульовані й детально описані ключові недоліки, а також супутні їм проблеми, що виникають при побудові системи захисту інформації в межах типового підходу.

Додатково можна зробити висновок, що як теоретичний, так і практичний підходи до управління інформаційною безпекою мають ряд суттєвих недоліків. Ці недоліки призводять до невідповідності класичному контуру управління, який має забезпечувати зв'язок між суб'єктами та об'єктами управління через інформаційні канали.

Отже, існує потреба в перегляді та вдосконаленні поточних методик і практик управління інформаційною безпекою для досягнення більш високого рівня відповідності сучасним вимогам і викликам у сфері інформаційної безпеки [95].

В умовах поточного розвитку інформаційної безпеки в Україні будь-яка установа стикається зі строго фіксованими вимогами і обмеженнями при побудові системи захисту інформації, зафіксованих у вигляді нормативно-методичної документації в області ІБ. Це включає як загальнонаціональні стандарти, так і власні вимоги кожної конкретної установи. Проте, механізми забезпечення інформаційної безпеки часто не передбачають реалізацію зворотного зв'язку між суб'єктами та об'єктами взаємодії, і спрямовані лише на виконання кінцевого, чітко визначеного набору функцій.

При цьому можливість вдосконалення використовуваних підходів, а також інструментів для проведення детального аналізу ІБ просто відсутні. Загальне розуміння цілей і завдань по управлінню ІБ можуть по-різному трактуватися кожним з фахівців, зважаючи на відсутність уніфікованих стандартних підходів і науково-методичного апарату з управління ІБ. У зв'язку з цим, ефективність прийняття рішень з ІБ (і їх обґрунтованість) безпосередньо залежить від сукупності досвіду і компетенції експертів, а також урахування специфіки зв'язків і логічних залежностей інформації всередині процесів

забезпечення ІБ, що протікають в СЗІ організації.

Тимчасові витрати, необхідні на прийняття відповідних управлінських рішень і їх обґрунтування, завжди обмежені, а отже, час і коректність прийняття рішень безпосередньо впливають на показники ефективності СЗІ. З урахуванням постійно зростаючих обсягів оброблюваної інформації, а також ускладнення логічних залежностей процесів забезпечення ІБ, ефективність реалізації СЗІ в кожній організації з часом починає погіршуватися.

Вирішення цієї ситуації можливе за рахунок розробки та застосування нового науково-методичного апарату з управління ІБ, здатного привести до скорочення витрат часу на прийняття управлінських рішень та суттєво підвищити ефективність СЗІ.

Забезпечення інформаційної безпеки та захист інформації є по суті близькими поняттями, що охоплюють діяльність, спрямовану на запобігання витоку захищеної інформації, а також несанкціонованих та ненавмисних дій, які можуть зашкодити інформації, що потребує захисту. Це включає усунення (нейтралізацію, парування) внутрішніх та зовнішніх загроз інформаційної безпеки установи або мінімізацію збитків від можливих реалізацій таких загроз. Виходячи з цього визначення та аналізу нормативно-правової документації України щодо захисту інформації, основні заходи для забезпечення інформаційної безпеки включають:

1. Забезпечення безперервності роботи інформаційних систем та інформаційно-телекомунікаційних сервісів:

- Розробка та впровадження планів безперервності бізнесу та відновлення після аварій.

- Регулярне тестування та актуалізація планів безперервності для забезпечення їх ефективності.

2. Моніторинг, виявлення та реагування на події інформаційної безпеки:

- Впровадження систем моніторингу для виявлення потенційних загроз і підозрілих дій у реальному часі.

- Розробка та впровадження планів реагування на інциденти для швидкого

усунення загроз та мінімізації їх впливу.

3. Забезпечення інформаційної безпеки на різних етапах розвитку інформаційних систем, а також підтримка і продовження їх життєвих циклів:

- Застосування процедур безпеки на всіх етапах життєвого циклу інформаційних систем від проектування до виведення з експлуатації.

-Регулярне оновлення систем для усунення вразливостей та забезпечення актуальності засобів захисту.

4. Забезпечення інформаційної безпеки при роботі з співробітниками організації:

- Проведення регулярного навчання та підвищення кваліфікації співробітників з питань інформаційної безпеки.

- Створення культури безпеки в організації, яка сприяє відповідальному ставленню до захисту інформації.

5. Забезпечення інформаційної безпеки при здійсненні інформаційного обміну та взаємодії з третіми сторонами:

- Використання шифрування та інших засобів захисту при передачі інформації.

- Укладання угод про рівень захисту інформації з третіми сторонами, які отримують доступ до інформації організації.

6. Раціональне розмежування прав доступу до інформації та інформаційних систем користувачів організації:

- Впровадження принципу найменших привілеїв, за яким користувачі мають доступ лише до тієї інформації, яка необхідна їм для виконання службових обов'язків.

- Регулярний аудит прав доступу для забезпечення їх відповідності поточним ролям та обов'язкам співробітників.

7. Забезпечення процесу ідентифікації та аутентифікації суб'єктів доступу до відповідних об'єктів доступу:

- Використання технологій ідентифікації та аутентифікації для забезпечення, що доступ до інформації мають лише авторизовані особи.

- Використання багатофакторної аутентифікації для підвищення рівня захисту доступу.

8. Забезпечення процесу управління доступом суб'єктів доступу до відповідних об'єктів доступу:

- Встановлення чітких політик доступу, які визначають, хто, коли і до якої інформації може мати доступ.

- Впровадження системи контролю доступу, яка дозволяє забезпечити дотримання встановлених політик.

- Регулярний перегляд та оновлення політик доступу для відповідності актуальним загрозам та потребам організації.

Ці заходи є критично важливими для ефективного забезпечення інформаційної безпеки та захисту інформації в сучасних умовах зростаючих кіберзагроз.

Таким чином, вищенаведені основні заходи щодо забезпечення інформаційної безпеки в установах можуть бути повністю (або по складовим частинам) реалізовані, в рамках раніше визначених основних процесах забезпечення та відповідним їм процесам управління інформаційною безпекою. Для визначення складу і основних функцій управління інформаційною безпекою слід розглянути і деталізувати основні процесні складові управління інформаційною безпекою, виходячи з результатів проведеного аналізу міжнародної та вітчизняної нормативно правової документації в галузі забезпечення інформаційної безпеки.

1.3. Інструменти управління інформаційною безпекою

Інформаційна безпека становить важливий компонент публічного управління в умовах сучасного цифрового світу, де практично кожен аспект життя перетинається з використанням інформаційних технологій. Швидкий технологічний прогрес та загальний розвиток Інтернету призвели до вибухового зростання обсягу цифрової інформації, яка зберігається, передається та обробляється. Це створює нові виклики та загрози для безпеки даних та інформаційних систем.

Збільшення обсягу цифрової інформації також означає зростання потенційних точок доступу для зловмисників, які можуть використовувати різноманітні техніки для незаконного доступу до даних або їх пошкодження. Це може призвести до втрати конфіденційності, порушення цілісності даних або навіть припинення роботи інформаційних систем.

У зв'язку з цим, розумне та ефективне публічне управління в сфері інформаційної безпеки є надзвичайно важливим завданням. Для цього потрібно використовувати передові технології та інструменти, які дозволять ефективно виявляти, запобігати та реагувати на потенційні загрози [68].

Після детального аналізу міжнародних та вітчизняних нормативно-правових документів в галузі інформаційної безпеки було визначено склад процесів управління інформаційної безпеки, до яких будемо відносити:

1. Управління активами. Систематичний підхід до ідентифікації, захисту та оптимізації використання інформаційних активів. Це охоплює всі аспекти, пов'язані з управлінням цифровими та фізичними ресурсами, які містять конфіденційну інформацію або можуть бути використані для здійснення критичних функцій організації. Управління активами включає в себе їхню інвентаризацію, класифікацію, захист, моніторинг та оновлення, а також визначення власників активів та встановлення відповідних політик безпеки.

2. Управління ресурсами системи захисту інформації. Цей процес охоплює широкий спектр дій та стратегій, спрямованих на ефективне використання та

забезпечення безпеки інформаційних ресурсів. Управління ресурсами системи захисту інформації включає такі складові:

- планування та розподіл ресурсів - це процес ретельного аналізу потреб у ресурсах та їхнього розподілу для забезпечення ефективного функціонування системи захисту інформації. Він включає в себе розробку стратегій виділення ресурсів, призначення бюджетів, планування ресурсів для конкретних проектів і ініціатив;

- забезпечення безпеки ресурсів - це процес визначення та впровадження заходів забезпечення конфіденційності, цілісності та доступності інформаційних ресурсів. Це включає в себе встановлення політик безпеки, ідентифікацію та вирішення потенційних загроз, впровадження заходів контролю доступу та моніторингу, а також реагування на інциденти безпеки;

- оптимізація використання ресурсів - це процес максимізації використання інформаційних ресурсів, забезпечення їхньої ефективності та ефективності. Це включає в себе постійне вдосконалення і оптимізацію процесів, використання інструментів моніторингу та аналізу, а також впровадження інноваційних технологій для підвищення продуктивності та забезпечення безпеки ресурсів;

3. Управління ризиками та загрозами інформаційній безпеці. Ефективне управління ризиками та загрозами інформаційної безпеки є надзвичайно важливим для забезпечення стабільності та надійності інформаційних систем. [111]. Цей процес включає в себе ряд ключових складових:

- ідентифікація ризиків; це перший крок у процесі управління ризиками. Необхідно регулярно оцінювати потенційні загрози і визначати ймовірність їх виникнення в системі інформаційної безпеки;

- оцінка ризиків; після ідентифікації ризиків, їхнього впливу та ймовірності, проводиться оцінка загального рівня ризику. Це допомагає прийняти рішення про те, які ризики потрібно найбільше уникати або зменшувати пріоритетно;

- управління ризиками; після оцінки ризиків приймаються стратегії

управління ризиками, включаючи уникнення, перенесення, зменшення чи прийняття ризику. Ці стратегії можуть включати в себе застосування технічних, організаційних або процедурних заходів безпеки;

- моніторинг та аналіз; після прийняття стратегій управління ризиками, система повинна систематично моніторитися та аналізуватися для виявлення нових загроз або змін у існуючих ризиках;

- відповідь на інциденти; у разі виникнення інцидентів або порушень безпеки, команда інформаційної безпеки повинна негайно реагувати, вживаючи відповідних заходів для ліквідації наслідків і відновлення нормального функціонування системи;

- неперервність діяльності та відновлення; підготовка планів неперервності діяльності та відновлення допомагає забезпечити швидке відновлення системи після інциденту та зменшити вплив на систему.

Усі ці складові спільно допомагають ефективно управляти ризиками та загрозами інформаційної безпеки та забезпечити надійність та захищеність їхніх інформаційних ресурсів.

4. Управління документами і інформаційною довідковою системою - це процес організації та контролю за документами та інформацією з метою забезпечення їх доступності, цілісності, конфіденційності та зручності використання. Ця складова є критичною для здійснення ефективного управління інформацією. Ось деякі ключові аспекти контролю документів і інформаційної довідкової системи:

- управління документами; це включає в себе створення, збереження, організацію, пошук, оновлення та видалення документів згідно з встановленими процедурами та політиками;

- класифікація і каталогізація; документи повинні бути ясно класифіковані та каталогізовані, щоб забезпечити їх легкий пошук та доступність;

- контроль доступу; забезпечення того, щоб тільки авторизовані користувачі мали доступ до конфіденційної інформації, і регулювання прав доступу до різних типів документів;

- захист інформації; застосування методів шифрування та інших заходів безпеки для запобігання несанкціонованому доступу та зламу інформаційної системи;

- аудит і моніторинг; постійний моніторинг та аудит системи для виявлення будь-яких порушень безпеки чи невідповідностей з встановленими стандартами;

- резервне копіювання і відновлення даних; регулярне створення резервних копій даних та процедури для відновлення інформації в разі її втрати або пошкодження;

- зберігання даних; розробка і виконання політик щодо тривалості зберігання документів і інформації відповідно до вимог законодавства та потреб;

- оновлення та покращення; регулярне оновлення системи контролю документів та інформаційної довідкової системи з метою вдосконалення їх ефективності та відповідності змінам внутрішніх та зовнішніх умов.

Ці аспекти допомагають забезпечити ефективний контроль над документами та інформаційною системою в організації, зменшуючи ризик втрати даних, забезпечуючи їх конфіденційність та цілісність, і полегшуючи доступ до необхідної інформації для користувачів [105].

5. Управління аудитом системи захисту інформації є важливою складовою процесу забезпечення безпеки інформації. Тут наведено деякі ключові аспекти управління аудитом системи захисту інформації:

- планування аудиту; це включає визначення обсягу, цілей, завдань та методів аудиту. Планування аудиту повинно бути здійснене з урахуванням ризиків безпеки, регуляторних вимог і внутрішніх політик організації.

- виконання аудиту; аудитори проводять перевірку системи захисту інформації на відповідність встановленим стандартам, політикам та процедурам. Це може включати технічні та організаційні аспекти безпеки, такі як перевірка мережевої інфраструктури, оцінка політик доступу та тестування вразливостей.

- оцінка результатів аудиту; після завершення аудиту аудитори аналізують отримані результати для виявлення потенційних проблем безпеки, ризиків та

невідповідностей вимогам. Вони також можуть надати рекомендації щодо подальших дій для виправлення виявлених проблем.

- звітність; після завершення аудиту генерується звіт, в якому представлені виявлені проблеми, відповідність стандартам безпеки, рекомендації щодо вдосконалення системи захисту інформації. Цей звіт може бути переданий керівництву організації для подальшого аналізу та вжиття заходів.

- після завершення аудиту необхідно вжити заходів для виправлення виявлених проблем і вдосконалення системи захисту інформації. Ці дії можуть включати розробку та впровадження нових політик, процедур та технологій безпеки, навчання персоналу та вдосконалення існуючих систем.

- моніторинг та перевірка; після впровадження виправлень і покращень важливо здійснювати моніторинг та перевірку ефективності нових заходів безпеки для впевненості в їх правильності та ефективності.

Управління аудитом системи захисту інформації є невід'ємною частиною процесу забезпечення безпеки інформації в організації і допомагає виявляти та усувати потенційні проблеми безпеки до того, як вони можуть призвести до серйозних інцидентів.

6. Управління аналізом ефективності системи захисту інформації, що включає в себе ретельне оцінювання та моніторинг заходів захисту інформації для забезпечення їх ефективності та відповідності вимогам.

7. Управління завданнями і діяльністю співробітників, які здійснюють процеси забезпечення інформаційної безпеки в організації [164].

8. Управління процесами забезпечення безперервності роботи інформаційних систем та інформаційно-телекомунікаційних сервісів.

9. Управління процесами забезпечення моніторингу, виявлення та реагування на події інформаційної безпеки.

10. Управління процесами забезпечення інформаційної безпеки на різних етапах розвитку інформаційних систем, а також підтримки і продовження життєвих циклів інформаційних систем організації.

11. Управління процесами забезпечення інформаційної безпеки при

здійсненні роботи з співробітниками організації, підвищенні їх кваліфікації та загальної компетенції з питань інформаційної безпеки.

12. Управління процесами забезпечення інформаційної безпеки при здійсненні інформаційного обміну та взаємодії з третіми сторонами.

13. Управління процесами забезпечення розмежування прав доступу до інформації та інформаційних систем користувачів, а також подальшого контролю за даним процесом.

На основі новітніх комунікаційних та інформаційних технологій весь світ поступово інтегрується у відкриту систему суспільно-політичних, фінансово-економічних та соціально-культурних зв'язків. Ця інтеграція є визначальною рисою процесу, який ми називаємо глобалізацією. У цьому контексті глобалізацію можна визначити як процес залучення всіх країн до формування єдиного економічного, соціального та культурного простору, що забезпечує можливість інтерактивного спілкування в реальному часі на основі сучасних інформаційних і телекомунікаційних технологій. Таким чином, глобалізацію можна розглядати як інформаційну глобалізацію[200].

Погоджуючись з позицією М. Кастельса, який в фундаментальному дослідженні «InformationAge: Economy, SocietyandCulture», присвяченому всебічному аналізу цивілізаційних процесів, викликаних до життя принципово новою роллю в сучасному світі інформаційних технологій, характеризує ситуацію, в останні десятиліття економіку нового типу, називаючи її глобальною та інформаційною, важливо відзначити, що М. Кастельс робить істотне розрізнення між відомими концепціями «інформаційного суспільства» (informationsociety) і власною концепцією «інформаціональне суспільства» (informationalsociety) [184].

Якщо в першому випадку акцентується ключова роль інформації в суспільстві, то за словами М. Кастельса, обмін інформацією супроводжував розвиток цивілізації на протязі всієї історії людства і мав критичне значення для усіх суспільств. Таким чином, сучасний світ переживає кардинальні зміни, і ядро трансформацій пов'язано з технологіями обробки інформації і комунікацією.

Революція в інформаційних технологіях є основою в аналізі труднощів становлення нової економіки, суспільства і культури.

Інформаційні технології піднімають значення знання та інформаційних потоків, зростаюча роль яких відзначалася Д. Беллом, А. Туреном, О. Тоффлером та іншими теоретиками постіндустріального суспільства

Класична теорія постіндустріалізму об'єднує три твердження:

1 Джерело продуктивності і зростання знаходиться в знанні, що постачається на всі сфери економічної діяльності через обробку інформації.

2. Економічна діяльність зміщується від виробництва товарів до надання послуг.

3.В новій економіці буде зростати значення професій, пов'язаних з високою насиченістю їх представників інформацією і знаннями.

Зазвичай виділяють три етапи в процесі формування і становлення постіндустріального суспільства:

- початок першого етапу пов'язують з нафтовим шоком 1973 року закінчується на початку 1980-х рр .;

- початок 1980-х рр. - 1989 г. - другий етап, коли виникає протистояння постіндустріальних країн і нових індустріальних країн;

- третій етап розпочався в 1992 р і триває по теперішній час, будучи пов'язаним з інформаційною революцією в западних країнах.

Постіндустріальне суспільство виділяється такими рисами, як індивідуалізація, глобалізація, високе технологічне розвиток, пов'язане з отриманням і поширенням знань [184].

В рамках постіндустріальної теорії ряд авторів звертає увагу на характерні риси, зародження нової технологічної цивілізації, при цьому, коли прихильники постіндустріальної теорії показують значення мінливих технічних змін, вони найчастіше як приклад наводять інформаційні технології.

Теорія інформаційного суспільства формується як модифікація концепції постіндустріального суспільства, в рамках якої наукове знання і технологічний прогрес підкреслюються в ще більш явно вираженій формі.

Термін «інформаційне суспільство» вводиться в науку на початку 1960-х рр. незалежно один від одного Ф. Махлуп в США і Т. Умесао в Японії. Знання, інформація і способи її обробки стають вирішальними факторами інноваційного розвитку суспільства, прискорюючи інноваційний цикл.

Японський економіст За визначенням економіста Й. Масуди, інформаційне суспільство характеризується тим, що воно засноване на інформаційних цінностях, які мають більший вплив, ніж матеріальні цінності. Економіка цього суспільства оцінюється за капіталом, втіленим у знання (knowledge capital), який вважається важливішим за матеріальний капітал.

За визначенням американського економіста В. Мартина, інформаційне суспільство є таким, де якість життя, можливості соціальних змін і економічного розвитку в значній мірі залежать від інформації та її ефективного використання.

Далі він наводить п'ять критеріїв інформаційного суспільства:

- економічний - інформаційний сектор розглядається, по-перше, як рух до інформаційного суспільства, а по-друге, як складова частина сучасного економічного життя;

- технологічний - показує, на скільки технології проникають в усі сфери діяльності індивідів;

- соціальний - змінюється соціальна поведінка індивідів під впливом інформаційних технологій;

- політичний - формується свого роду глобальний форум, в якому рядові громадяни можуть безпосередньо брати участь в управлінні;

культурний - відбувається взаємодія і взаємопроникнення культур в глобальному масштабі.

Формування теорії інформаційного суспільства підтримує ідею, що виробництво інформаційних продуктів стає ключовим процесом, подібним до виробництва матеріальних цінностей. Прихильники цієї теорії пов'язують зародження інформаційного суспільства з домінуванням четвертого сектора економіки, який виникає після сільського господарства, промисловості та сектора послуг. У цьому новому контексті капітал і праця, які були основою

індустріального суспільства, поступово заміщаються інформацією, яка стає ключовим ресурсом інформаційного суспільства. Частка інформаційного сектора за останні десять років значно зросла і становить в розвинених країнах 45 - 65%.

Перехід глобального суспільства до постіндустріальної епохи та впровадження наукомістких технологій значно залежать від інформаційних ресурсів, що підвищує вимоги до кваліфікації робочої сили. Сучасні управлінські та сервісні технології, а також виробництво продукції та послуг є неможливими без інформаційних технологій, які забезпечують інформаційні потреби управлінських, виробничих, постачальницьких, торговельних, збутових та інших функціональних підрозділів установ. Інформаційні технології дозволяють ефективно керувати всіма видами ресурсів. Матеріальні та фінансові ресурси завжди обмежені, тому ключовим фактором успіху економічної діяльності є прийняття правильних управлінських рішень щодо того, де і як слід їх зосередити для досягнення максимального ефекту.

Країни і регіони, що активно використовують сучасні засоби інформаційно-комунікаційних технологій, досягають найбільшого економічного, соціального і державного успіху. Інформація, яка легко доступна для обробки за допомогою комп'ютерів, стає важливим фактором соціального розвитку, ставши стратегічним ресурсом нарівні з матеріальними та енергетичними. Вона відіграє ключову роль у захисті держави від різноманітних інформаційних загроз і викликів у глобалізованому світі [21].

Інформаційне суспільство характеризується наявністю інформаційної економіки та управління, високим рівнем потреб у інформації для всіх членів суспільства та їхнього задоволення, високою інформаційною культурою та загальнодоступністю інформації, обмеженою лише захищеністю особистої інформації, груп та держави.

У зв'язку з цим, ефективне публічне управління інформаційною безпекою стає критично важливим завданням у всіх сферах діяльності. Для цього необхідно використовувати передові технології та інструменти, які дозволять

ефективно виявляти, запобігати та реагувати на потенційні загрози. Особливу увагу слід звернути на сфери, які є економічно важливими, для забезпечення стабільності та економічного розвитку країни. Важливо розвивати кібербезпеку у фінансовому, торговельному, транспортному, медичному та інших секторах, щоб забезпечити безпеку та стабільність національної економіки [16].

Добре структурована, своєчасна і актуальна інформація дозволяє концентрувати ресурси в потрібний час і в потрібному місці для реалізації головних, пріоритетних завдань розвитку соціально-економічної системи - перехід до інноваційної економіки на базі інформаційної підтримки управлінських і технологічних процесів.

Світова економіка XXI ст. характеризується глобальними змінами, які орієнтовані на зростання якості соціального рівня суспільства, на вдосконалення структури економіки, на підвищення накопичення високоінтелектуального людського та інформаційного капіталу шляхом прискорення інновацій, головним інструментом яких в умовах нової економіки стає інвестиційна складова. Перед об'єктивною необхідністю активізації інвестиційної діяльності на створення конкурентоспроможних господарських систем, модернізацію діючих структур, забезпечення диверсифікації капіталу в напрямку соціально орієнтованих структурних перетворень в сьогоднішній час поставлені багато країн світу.

Пожвавлення інноваційної та інвестиційної політики є головною умовою для сталого розвитку соціально орієнтованої ринкової економіки України.

Економічне відновлення, зростання капіталу, розвиток ринкової інфраструктури та збільшення конкурентоспроможності виробників на внутрішніх і зовнішніх ринках безпосередньо залежать від якості, обсягу та структури інвестицій. Інвестиції виступають матеріальною основою для розвитку країни, створюючи позитивний ефект, який служить джерелом коштів для нових капітальних та інтелектуальних вкладень. Уряд України активно працює над стимулюванням інвестиційної діяльності як вітчизняних, так і іноземних компаній.

Новітні технології стають факторами економічного зростання, інформаційні системи розширюють професійні можливості фахівців і дозволяють здійснювати діяльність господарюючого суб'єкта раціональніше, цілеспрямовано і ефективно.

Нова модель ринкового господарства в Україні формується в результаті трансформаційних перетворень, модернізації національних фінансових інститутів, що обумовлено не тільки внутрішніми потребами і стратегічними інтересами країни, а й сучасними тенденціями розвитку в умовах глобалізації. Сучасна епоха - це епоха глобалізації, що відрізняється поглибленням міжнародного поділу праці і міжнародної кооперації, бурхливим розвитком інтеграційних процесів, насамперед на регіональному рівні, а також взаємозв'язком різних сфер суспільного життя, включаючи економіку, політику, соціальну сферу, екологію, безпеку, культуру.

Прогрес в технологіях переробки інформації, системах телекомунікацій, фінансових технологіях тягне за собою подальшу глобалізацію економіки, формування єдиного світового ринку. Матеріальною основою глобалізації послужило динамічний розвиток усіх видів інформаційних технологій, які визначають картину сьогодення і в ще більшій мірі будуть визначати картину майбутнього.

В Україні спостерігається активний розвиток IT-ринку, що виходить за рамки західноєвропейських показників. З'являються нові галузі бізнесу, в яких інформаційні технології виступають не просто інструментом, але й ключовою складовою для підвищення конкурентоспроможності [20]. Цей тренд відображає динамічний розвиток та високий потенціал українського IT-сектору, який перетворюється на важливий драйвер економічного зростання країни. Рівень зрілості IT-ринку визначається співвідношенням частки окремих сегментів, таких як апаратне та програмне забезпечення, у загальній структурі ринку інформаційних технологій. У розвинених країнах витрати на обладнання майже рівні витратам на програмне забезпечення, але менше, ніж на оплату IT-послуг. Однак у країнах, що розвиваються, спостерігається переважання витрат на

обладнання, і витрати на IT-послуги практично в 1,6 рази перевищують витрати на придбання апаратного забезпечення. Цей відмінний розподіл витрат свідчить про специфіку розвитку IT-індустрії в різних економічних умовах і показує різницю в підходах до використання технологічних ресурсів.

У країнах, що розвиваються картина зворотня: частка сектора апаратного забезпечення переважає частку сектора IT -послуг. Наприклад, в Україні більш ніж в 2,7 рази, що однозначно говорить про те, що IT -ринок тільки розвивається. Однак рух вперед все ж має місце і на українському ринку інформаційних технологій, так як поступово відбувається скорочення апаратної складової і збільшується частка IT -послуг Індекси мережевої готовності (Networked Readiness Index, NRI) також вимірюють рівень розвитку інформаційних і телекомунікаційних технологій за багатьма параметрами і в комплексі оцінюють ІКТ-потенціал країн і активність використання даних технологій для їх розвитку та підвищення рівня конкурентоспроможності. Дані індекси щорічно розраховуються і публікуються Основними джерелами виручки на IT- ринку є послуги системної і мережевий інтеграції та розробки програмного забезпечення. Все це говорить про те, що поступово інформаційні технології починають використовуватися як інструмент вирішення бізнес-завдань [19].

В Україні є необхідні умови для інтенсивного інформаційного розвитку:

- ринок послуг зв'язку стрімко розвивається, інформаційна інфраструктура активно вдосконалюється, що відображається як важлива складова частина глобальної інформаційної інфраструктури. Цей процес сприяє зростанню доступності та якості комунікаційних послуг, а також забезпечує підтримку широкого діапазону сучасних інформаційних технологій та послуг, що відповідають потребам сучасного світу;

- інформаційно-комунікаційні технології широко використовуються у всіх сферах суспільного життя, включаючи економіку, політику, соціальну та духовну сфери. При цьому постійний розвиток цих технологій породжує потребу в системі правового регулювання, яка відповідала б викликам та потребам сучасного інформаційного суспільства. Така система має створювати

ефективні механізми контролю, захисту даних, приватності та інтелектуальної власності, сприяючи сталому та етичному розвитку цифрового середовища;

У той же час, рівень розвитку вітчизняної інформаційної інфраструктури та використання інформаційно-комунікаційних технологій у суспільному виробництві і публічному управлінні не повністю відповідає вимогам та завданням диверсифікації економіки, підвищення конкурентоспроможності країни, збільшення добробуту і покращення якості життя громадян, а також зміцнення національної безпеки. Зусилля, що вживаються державними органами для створення умов сприятливого постіндустріального розвитку суспільства, часто характеризуються недостатньою координацією. Також використання потенціалу бізнесу та громадянського суспільства залишається недостатнім.

У процесі неперервного розвитку інформаційних технологій та зростання впливу інформаційних процесів на економіку, політику, культуру та суспільство в цілому відбувається глибоке переосмислення теоретичних концепцій, які відображають ці динамічні тенденції. Засновані на попередніх моделях, такі концепції, як дії нового індустріального суспільства та постіндустріального суспільства, перетворюються і адаптуються відповідно до нових реалій, вибухового росту інформаційних технологій та поширення цифрової культури [33]. Цей процес приводить до формування концепції інформаційного суспільства, яке характеризується своєрідними особливостями та вимогами. Основні риси цієї концепції включають:

1. У сучасному світі спостерігається зростаюча тенденція до переважання діяльності, що пов'язана зі створенням, використанням та обробкою інформаційних технологій, а також інформації та знань. Цей процес є невід'ємною складовою сучасного глобального розвитку, оскільки відображає стрімке вдосконалення інформаційно-технологічного сектору та його вплив на різні сфери діяльності людей і суспільства в цілому. Переважання цієї діяльності відкриває нові можливості для ефективного розвитку економіки, науки, освіти, культури та інших сфер, водночас вимагаючи адаптації до постійних змін і викликів, що ставлять перед сучасними суспільствами;

2. Істотне розширення можливостей громадян у сфері пошуку, накопичення, передачі, виробництва та розповсюдження інформації і знань є ключовим аспектом сучасного інформаційного суспільства. Цей процес стимулює активну участь громадян у вільному доступі до різноманітної інформації, сприяє розвитку самоосвіти та саморозвитку, сприяє обміну ідеями і думками. Завдяки інформаційним технологіям та платформам інтернету, люди мають можливість взаємодіяти з інформацією швидше, ефективніше та масштабніше, що відкриває нові перспективи для особистого і професійного зростання.

3. Глобалізація всіх сфер життя суспільства є складним та багатогранним процесом, що впливає на всі аспекти людського існування. Цей явище спричиняє зростання взаємозалежності між країнами та регіонами, змінює парадигми економічного розвитку, впливає на структуру та функціонування політичних систем, а також формує нові культурні та духовні вподобання. Глобалізація сприяє зближенню народів, розширенню можливостей для міжнародного співробітництва та обміну ідеями, але також породжує виклики у збереженні національної ідентичності, розподілі ресурсів та боротьбі з нерівністю.

У сучасних умовах глобалізації надзвичайно важливим стає розвиток національної інформаційної інфраструктури та її ефективне включення у глобальну інформаційну мережу [41]. Цей процес є критичним для кожної країни, оскільки він визначає її конкурентоспроможність у міжнародному контексті.

Важливим фундаментальним принципом інформаційної парадигми сучасного суспільства є розуміння того, що інформація є ключовим ресурсом, що має унікальну цінність. Інформація, як самостійний ресурс, легко перетинає всі кордони та перешкоди, і тому вона стає головним мотором глобальних процесів глобалізації. Цей феномен підтримує зв'язки між національними та міжнародними економічними системами та сприяє подальшій інтеграції країн у світовий економічний ландшафт.

Висновки до першого розділу

Дослідження теоретичних основ публічного управління у сфері інформаційної безпеки держави дозволило дійти таких висновків.

Національна безпека є складним багатофункціональним явищем, яке включає систему взаємопов'язаних елементів, стратегічних і концептуальних принципів, установок і положень, соціально-політичних інститутів та організацій, а також засобів, методів і способів, що дозволяють превентивно або адекватно реагувати на ризики, загрози та небезпеки. Інформаційна безпека, як один із найважливіших елементів національної безпеки, охоплює захист інформації від несанкціонованого доступу, управління даними, кібербезпеку, захист від кібератак та інші аспекти цифрової безпеки. Це підкреслює актуальність питання забезпечення інформаційної безпеки, оскільки інформація стала одним із найзначніших ресурсів розвитку цивілізації, а її недбале використання може призвести до негативних наслідків для інтересів особи, суспільства та держави.

Ефективна реалізація державної інформаційної політики є важливою умовою для забезпечення безпеки та сприяння розвитку інформаційного суспільства в епоху цифрової трансформації. Незважаючи на значну увагу науковців і зусилля у розробці державної політики в інформаційній сфері, багато аспектів потребують подальших досліджень та вдосконалення Аналіз основних напрямів забезпечення та управління інформаційною безпекою передбачає розробку нових стратегій державної інформаційної політики з орієнтацією на цифрові технології., зокрема Big Data та Open Data. У вузькому значенні, державна інформаційна політика охоплює стратегії держави з використання цифрових технологій у всіх сферах суспільства та публічного управління.

У широкому значенні, це включає діяльність, спрямовану на формування та реалізацію політики у галузі засобів масової інформації, зв'язку, розвитку інформаційного суспільства та інтенсивного використання інформаційних технологій. Сучасний етап розвитку державної інформаційної політики України характеризується впровадженням електронних послуг та систем електронного

урядування, що підвищує прозорість, швидкість та ефективність управління державними ресурсами. Інформаційне забезпечення включає збір, обробку, аналіз, передачу та збереження інформаційних ресурсів, що є важливим для національної безпеки.

Розробка стратегій та політик, які враховують глобальні тенденції і враховують специфіку національного контексту, є важливою умовою успішного розвитку інформаційного суспільства в Україні. Основні напрями забезпечення інформаційної безпеки включають реалізацію національної стратегії, технічний захист, кібербезпеку, правове забезпечення, навчання фахівців, управління ризиками та міжнародне співробітництво. Основні заходи щодо забезпечення інформаційної безпеки охоплюють забезпечення безперервності роботи інформаційних систем, моніторинг та реагування на події, захист інформаційних систем на різних етапах розвитку, управління доступом, ідентифікацію та аутентифікацію суб'єктів доступу.

Визначено склад процесів публічного управління інформаційною безпекою, включаючи управління активами, ресурсами системи захисту інформації, ризиками та загрозами, документами, аудитом, ефективністю системи захисту, діяльністю співробітників, безперервністю роботи інформаційних систем, моніторингом, інформаційним обміном та правами доступу. Систематичний підхід є надзвичайно важливим для забезпечення стабільності та надійності інформаційних систем. Впровадження процесів, що охоплюють забезпечення безперервності роботи інформаційних систем, моніторинг подій в галузі інформаційної безпеки, обмін інформацією та контроль доступу користувачів, формує основу для ефективного управління в галузі інформаційної безпеки держави.

Важливим завданням є визначення пріоритетів у наукових дослідженнях та розробка механізмів для вирішення проблем публічного управління в сфері інформаційної безпеки. Необхідно проводити публічно-управлінський аналіз цих проблем, враховуючи зарубіжний досвід і розвиток цифрових технологій, таких як хмарні сервіси, мобільні технології та цифрові державні стратегії.

Сучасний етап розвитку державної інформаційної політики України характеризується активним впровадженням цифрових технологій, що змінюють взаємодію громадян з органами влади та сутність адміністративних процесів. Електронні послуги та системи електронного урядування забезпечують прозорість, швидкість і ефективність управління державними ресурсами.

Отже, систематичні дослідження та вдосконалення підходів до реалізації державної інформаційної політики в умовах цифрової трансформації є необхідними для успішного розвитку України в сучасному світі.

АНАЛІЗ СУЧАСНОГО СТАНУ ПУБЛІЧНОГО УПРАВЛІННЯ В СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ

2.1. Оцінка сучасного стану механізмів публічного управління у сфері інформаційної безпеки

Аналіз досліджень, проведених протягом останніх двадцяти років в Україні з питань становлення та реалізації публічного управління в сфері інформаційної безпеки держави, свідчить про їхню відповідність етапам інформаційного розвитку країни. Цей процес може бути розглянутий через призму наступних періодів:

1. На першому етапі, що розпочався у початку 1990-х років і тривав до другої половини 1990-х років, відбувалася інтенсивна робота у сфері інформатизації суспільства та органів влади, що стало результатом активного розвитку комп'ютеризації. Також на цьому етапі почалася розробка нормативно-правового регулювання масової інформації, включаючи прийняття Закону про інформацію [134]. Він встановлював загальні принципи свободи слова, регулював видавничу справу, встановлював вимоги до засобів масової інформації (ЗМІ), а також визначав правові основи діяльності журналістів. Незважаючи на важливість законодавчих ініціатив у цій галузі, вони не стали ефективним інструментом регулювання взаємовідносин між владою та ЗМІ. Це можна пояснити відсутністю історичних традицій правового регулювання в різних сферах та недостатньою розробленістю механізмів взаємодії цих інтересів. У рамках першого етапу можна виділити два підетапи:

- 1991-1995 роки - період підготовки державних ресурсів та суспільства до кардинальних трансформаційних процесів на основі впровадження проекту інформатизації.

- 1995-1998 роки - перехід від політики інформатизації до проблеми формування єдиного інформаційного простору з урахуванням впливу інформаційно-комунікаційних технологій (у цей період починається і новий етап становлення та реалізації державної інформаційної політики).

2. Другий етап: друга половина 1990-х років - Початок 2000-х гг. На

даний період припала безпосередня розробка програмних документів у сфері інформаційної діяльності. У 1998 році в Україні було прийнято Концепцію Національної програми інформатизації, яка мала на меті забезпечення громадян та суспільства своєчасною, достовірною та повною інформацією шляхом широкого впровадження інформаційних технологій. Також основною ціллю програми було зміцнення інформаційної безпеки держави. Основна увага у документі приділялася розвитку інформаційних технологій, телекомунікацій та зв'язку як головних інструментів створення інформаційного суспільства. Не заперечуючи важливості розробки та прийняття цієї Концепції, слід зазначити, що її зміст багато в чому мало декларативний характер. Незважаючи на важливість зазначених принципів взаємовідносин влади, ЗМІ та суспільства, конкретних заходів щодо їх реалізації у зазначеній Концепції запропоновано не було. Вона багато в чому розділила долю інших офіційних документів, які мали найкращі наміри, але не опрацьовані в реальному часі і не мали практичного механізму реалізації. Зазначимо, що в рамках даного етапу є найбільш значущі часові віхи, на цьому підетапі починається третій етап становлення та реалізації державної інформаційної політики в Україні [136].

3. Третій етап: перша половина 2000-х років - теперішній час. Цей етап був відзначений появою цілої низки документів, що заклали основи реалізації державної політики у сфері масової інформації в Україні. Ними стали Стратегія розвитку інформаційного суспільства України (2002), закон України основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки (2007) і ряд інших. Варто наголосити на своєчасності появи цих документів, оскільки вони відкрили шлях для інтенсифікації процесів інформаційної взаємодії між бізнесом та публічним управлінням. Стимулювання інновацій, розвиток електронних технологій, покращення управління та забезпечення безпеки інформації відіграли значну роль у підвищенні конкурентоспроможності бізнесу та покращенні ефективності публічного управління. Ці документи мали позитивний вплив на розвиток технологічних та інформаційних процесів у суспільстві. Проте, слід відзначити,

що змістовні пріоритети інформаційної політики на той час не отримали достатнього аналізу та уточнень. Названі документи не конкретизували перспектив розвитку масової інформації, не регламентували взаємодію ЗМІ з їх власниками, засновниками та аудиторією. Ці питання стали актуальними в умовах розвитку ринкової економіки, де зростала роль суспільства у вирішенні політичних, економічних та соціальних питань. Зросла роль громадського суспільства у вирішенні політичних питань. та ефективність його впливу на формування публічної думки та прийняття стратегічних рішень[84].

Говорячи про внутрішню диференційованість даного періоду, зазначимо, що в ньому можна, на наш погляд, виділити найбільшу кількість під етапів: 1) 2002 р. - 2008 р. - подальший розвиток державної політики у сфері інформаційних технологій, етап супроводжується інформатизацією органів державної влади та управління, побудовою основної конфігурації «електронного уряду» (електронні державні закупівлі, розвиток системи державних інформаційних послуг тощо); 2) 2008 р. - 2017 р. - становлення та розвиток державної політики щодо побудови інформаційного суспільства; 3) 2017 р. – тепер – початок формування державної політики щодо цифрового розвитку держави й суспільства.

Швидкий розвиток інформаційно-комунікаційних технологій та використання їх у процесі публічного управління зумовлює появи та розвиток поняття e-governance або електронне державне керування. Взаємодія між громадськими інститутами, органами державної влади, громадянами та організаціями здійснюється за допомогою використання інформаційно-комунікаційних технологій [56]. E-governance є новою формою публічного управління, з використанням інформаційно-комунікаційних технологій, інформаційної мережі «Інтернет», на основі якої здійснюється прозорий, ефективний, швидкий обмін інформацією та надання інформації громадянам, органами державної влади для забезпечення успішного функціонування держави. ІКТ застосовуються для надання державних послуг, обміну інформацією, комунікаційних транзакцій, інтеграції різних автономних систем

та послуг між урядом-громадянином, публічне управління, управління державними службовцями. Відсутність належного рівня забезпечення інформаційної безпеки призведе до витоку циркулюючої інформації, що негативно позначиться на публічному управлінні.

Розвиток електронного уряду, або e-governance, стає необхідним у сучасному світі, оскільки це сприяє підвищенню ефективності, прозорості та доступності публічного управління.

Багато країн вже успішно впроваджують моделі електронного уряду і продовжують розвивати їх, вдосконалюючи процеси взаємодії між громадянами, бізнесом та урядовими органами. Застосування сучасних технологій, таких як інформаційні системи, електронні сервіси та онлайн-платформи, дозволяє забезпечити швидку та ефективну обробку інформації, зменшити бюрократичні бар'єри та спростити взаємодію з органами влади для громадян та бізнесу.

При цьому важливо враховувати не лише технічні аспекти, але й забезпечити відповідність зваженим правовим та етичним стандартам, щоб забезпечити конфіденційність та захист персональних даних громадян. Такий підхід дозволить створити надійну та довірену електронну інфраструктуру, яка підтримується довгостроковими цілями забезпечення демократії, прозорості та розвитку суспільства.

Державам у сучасних умовах властива зростаюча потреба у впровадженні нових владно-управлінських технологій. У зв'язку з цим для сучасного етапу характерний інтенсивний перехід у сфері публічного управління на технології on-line, активний розвиток технології «електронного уряду» [144].

Активний розвиток технології "електронного уряду" в Україні підкреслюється кількома ключовими аспектами:

- Цифрові послуги для громадян. Уряд активно впроваджує цифрові сервіси, що дозволяють громадянам звертатися до державних органів онлайн без відвідування офісів та черг.

- Електронний документообіг. Застосування електронного документообігу

спрощує та прискорює взаємодію між державними органами та підприємствами.

- Відкриті дані та прозорість. Запровадження принципів відкритих даних сприяє збільшенню прозорості в управлінні та підвищує рівень довіри до державних інституцій.

- Кібербезпека та захист даних. Розвиток електронного уряду супроводжується зростанням уваги до кібербезпеки та захисту персональних даних громадян, що є важливим аспектом у цифровій епохі.

- Електронна ідентифікація. Впровадження сучасних систем електронної ідентифікації дозволяє забезпечити безпеку та достовірність інформації, що обмінюється між учасниками електронного уряду[128].

Ці напрями спрямовані на покращення якості надання державних послуг, зменшення бюрократичних бар'єрів та підвищення ефективності публічного управління в цілому.

Розглянемо конкретний приклад активного розвитку технології "електронного уряду" в Україні. Одним із ключових досягнень впровадження "електронного уряду" в Україні є система електронної декларації майна та доходів посадових осіб. Ця система була створена для забезпечення прозорості та боротьби з корупцією серед державних службовців та посадових осіб.

Основні особливості системи:

1. Онлайн-подання декларацій. Посадові особи мають змогу подати свої декларації майна та доходів через онлайн-сервіс, що значно спрощує процес і дозволяє уникнути бюрократичних перешкод.

2. Публічність і доступність даних. Інформація про декларації стає публічною та доступною для громадськості через спеціальний реєстр, що сприяє контролю за діяльністю посадових осіб.

3. Перевірка та аналіз даних. Система дозволяє автоматизовано перевіряти та аналізувати дані з декларацій, що допомагає виявляти випадки недекларування майна чи незаконного збагачення.

Цей приклад ілюструє, як технологія "електронного уряду" впливає на підвищення прозорості та ефективності публічного управління в державному

секторі, сприяючи побудові довіри громадян до державних інституцій.

На підставі вищесказаного можна відзначити, що концепції модернізації публічного управління орієнтовані так чи інакше на підвищення соціальної ефективності. На цій основі мають розроблятися сучасні інформаційно-комунікаційні технології, методи публічного управління та управлінські механізми за допомогою нових ІКТ. У контексті публічного управління, взаємовідносини між державними інститутами та громадянським суспільством в інформаційному просторі відіграють вирішальну роль у визначенні його якості. Ці взаємини формують основу відкритості, прозорості та взаємодії між владними структурами та громадянами, що є критичними аспектами сучасного демократичного публічного управління. Інформація при різних сучасних засобах її трансляції має надзвичайну швидкість поширення і проникність. Це, у свою чергу, передбачає своєчасність та адекватність обліку та реагування на факти. Очевидно, що різними суб'єктами можуть виставлятися та обґрунтовуватися різні критерії «небезпечного» та «безпечного», «шкідливого» та «корисного». Кардинальне розрізнення та прийняття як зміст «небезпечного» в диспозиції норми залежить від соціокультурних, ідеологічних установок, стану ментальності соціальної групи. У рамках цієї роботи здійснено соціально-політичний моніторинг за низкою основних параметрів та позицій дослідження, опитування відбувалося із застосуванням анкети, із якою учасники опитування могли ознайомитися у вигляді відповідної Google-форми[196].

Завдання проведеного дослідження:

- оцінка рівня розвитку інституційної системи інформаційного середовища у суспільстві;
- виявлення соціальних суб'єктів, здатних найбільш ефективно здійснювати соціальне управління інформаційною безпекою;
- найважливіші загрози для інформаційної безпеки, визначення ключових каналів небезпечного інформаційно-культурного змісту та вибір найбільш ефективних типів інструментів протидії інформаційним загрозам;
- аналіз основних процесів формування інформаційної безпеки суспільства;

- вивчення видів основних інформаційних ризиків, небезпек та загроз та їх джерел, їх соціальної сутності та впливу на процеси формування інформаційної безпеки суспільства.

Вибірка становила 58 осіб. Із загальної кількості респондентів чоловіки склали - 56%, жінки - 44%. Віковий ценз визначився так: до 20 років – 10, до 30 років 27 - чоловік, 30-40 років - 12 чоловік, 40-50 років - 9 чоловік. На запитання: чи знаєте Ви про існування Стратегії інформаційної безпеки України, були отримані відповіді «так» – 12 опитаних, «ні» – 46, які відображені у наступній діаграмі

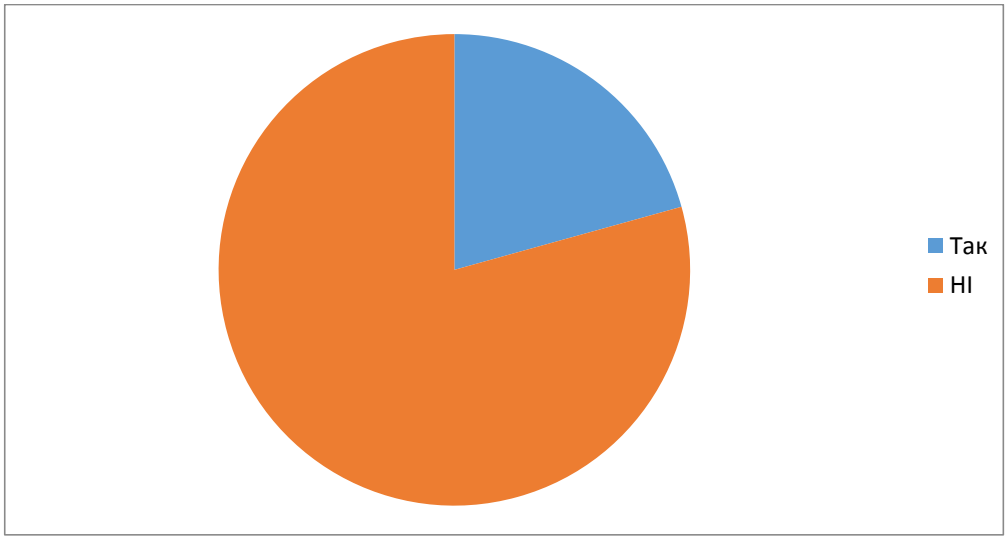

Рис. 1. Розподіл відповідей респондентів про знання, щодо існування Стратегії інформаційної безпеки України

Джерело: авторська розробка

Аналізуючи отримані результати, можна зробити висновок, що більшість українців, у тому числі молодих респондентів не знають про існування Стратегії інформаційної безпеки України, і співвідношення тих, хто знає про Стратегію і не має про неї ніякого поняття, становить приблизно 1:3,8. Ці результати можна вважати типовими, що відображають загальне знання з даного предмета в загальнодержавному форматі, з чого можна зробити висновок: або громадяни України не вважають інформаційну безпеку пріоритетною або не зачіпає їх життєво важливі інтереси, тому і не цікавляться подібними документами, або недостатньо ефективно діє механізм популяризації подібного знання, і за всієї

його соціальної актуальності, люди мають про нього уявлення через неналежної інформованості про нього.

Цікаві дані отримані в результаті наступного соціологічного опитування щодо актуальності поточних процесів формування інформаційної безпеки суспільства. На запитання: які процеси формування інформаційної безпеки суспільства – технічні (захист інформаційних ресурсів) чи психофізичні (захист соціальних, морально-психологічних, культурних та духовних інтересів особистості та суспільства) – на даний час є найбільш актуальними, отримані відповіді респондентів, що наводяться у наступній діаграмі :

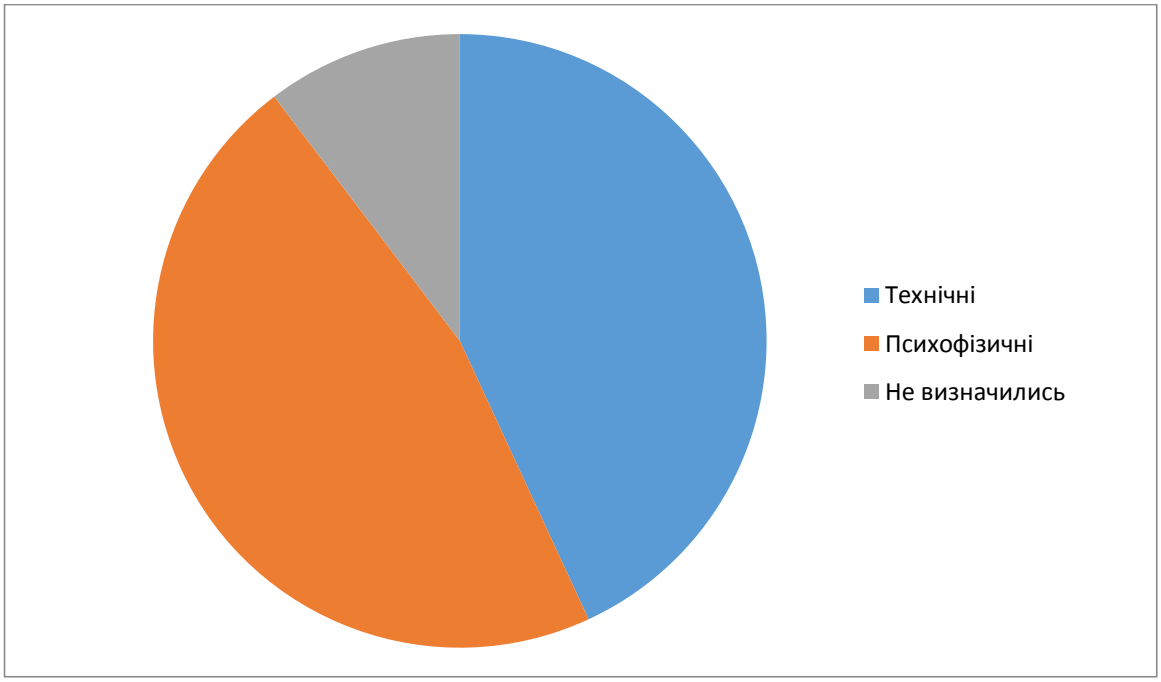

Рис. 1.2. Розподіл відповідей респондентів щодо актуальності процесів формування інформаційної безпеки

Джерело: авторська розробка

Пріоритетність технічним процесам формування інформаційної безпеки віддали перевагу 25 опитаних, психофізичним - 27 опитаних, 6 осіб не визначилися. Дані опитування показують, що, по суті, респонденти майже рівною мірою (з незначною перевагою у бік психофізичних процесів формування інформаційної безпеки) вважають актуальність обох. Таким чином, соціальна спрямованість процесів формування інформаційної безпеки хвилює та цікавить суспільство і при всьому розумінні важливості технічних процесів

інформаційного захисту люди досить зацікавлені й у належному інформаційному захисті свого соціального та духовного функціонування в існуючому інформаційному суспільстві.

Досить цікаво простежити і ставлення самого суспільства, особливо його молодої інтелектуальної складової до нової якості (або статусу), що народжується всередині його, - інформаційного. Було проведено соціологічне опитування, що досліджує формат розуміння громадянами засад інформаційного суспільства. На питання: чи вважаєте Ви, що в Україні формується інформаційне суспільство, були отримані відповіді («так» - 43 особи; «ні» - 10 осіб; «не знаю» - 3 особи), які зображені на наступній діаграмі:

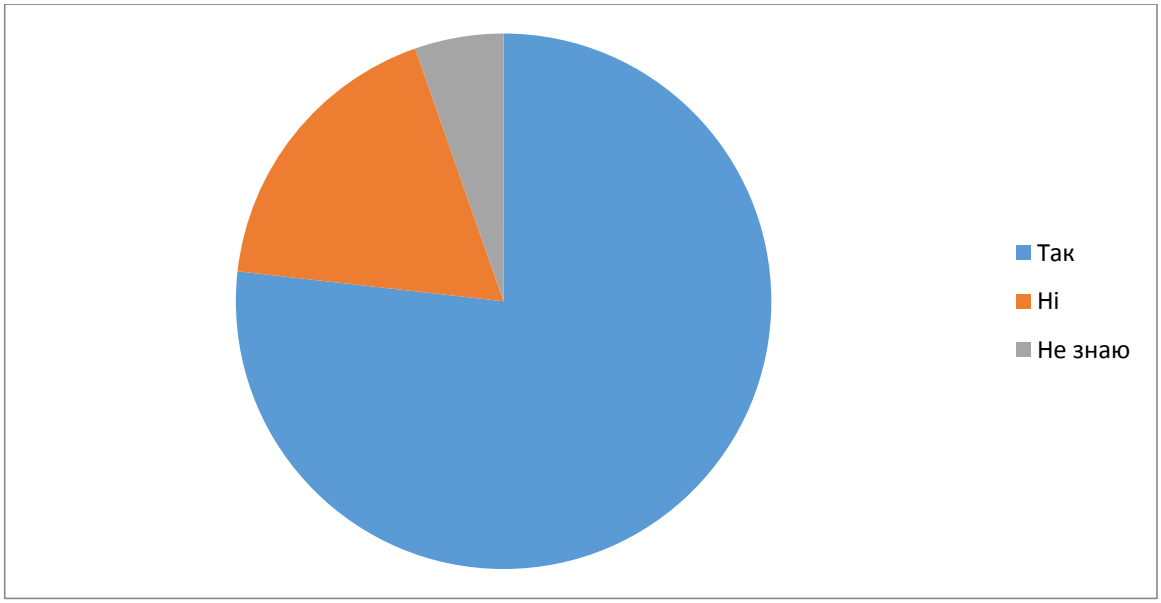

Рис. 1.3. Оцінка ступеня сформованості інформаційного суспільства

Джерело: авторська розробка

На питання дослідження про те, наскільки інформаційне суспільство, що формується, здатне вирішувати, навпаки, або посилювати соціальні проблеми, отримані відповіді респондентів («вирішувати» - 37 чол.; «погіршувати» - 15 чол.; «не знаю» - 6 чол.), які відображені у наступній діаграмі

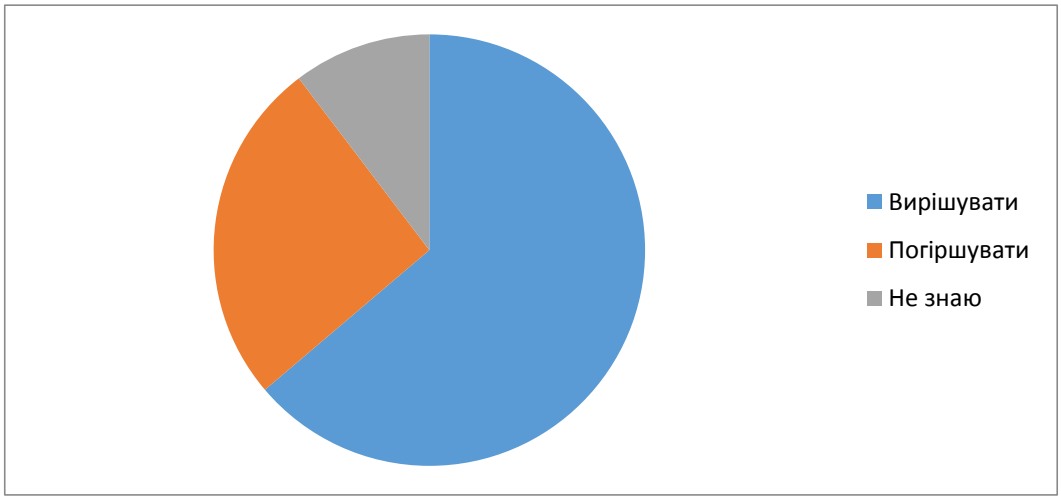

Рис. 1.4. Розподіл відповідей респондентів щодо впливу формування інформаційного суспільства на соціальні проблеми

Джерело: авторська розробка

Розглядаючи отримані результати (а нагадаємо, що основними респондентами опитування є студентство, тобто - інтелектуальний потенціал нації, який незабаром безпосередньо займатиметься питаннями розвитку та публічного управління країни), можна абсолютно впевнено стверджувати, що молоде покоління переконане, що живе в умовах формування інформаційного суспільства та ототожнює свої плани разом з ним, вважаючи, що таке суспільство сприятиме рішенню соціальних проблем та сприятиме розвитку прогресу цивілізації. Позитивні відповіді на ці запитання, згідно з цифрами, майже вдвічі перевищують негативні та обережні («не знаю») результати. Безперечно, нинішнє молоде покоління країни вже виховувалося на основі інформаційно-комунікаційних ресурсів та технологій, «дорослішаючи» разом з їх постійним удосконаленням і не представляючи активної життєдіяльності без них. Певною мірою також можна, характеризуючи отримані результати, вважати, що підкріплюється наш висновок про те, що сучасні покоління, які завтра прийдуть до управління країною, вже сьогодні соціально та психологічно адаптовані до свідомої життєдіяльності в інформаційному суспільстві. Більше того, їхнє соціальне самопочуття невіддільне від прогресу такого суспільства, і публічного управління державою, як і вирішення соціальних проблем, що виникають у ньому, вони ототожнюють з інформаційним середовищем.

Наступне опитування про те, які інформаційні загрози на Ваш погляд є найнебезпечнішими, було в сукупності зазначено 9 найбільш, на думку респондентів, небезпечних, які відображені в наступній діаграмі:

- ЗМІ;
- інтернет;
- віруси;
- чутки, плітки;
- збої програм;
- хакери;
- інформаційні атаки з боку рф;
- несанкціонований доступ до ПК;
- інше.

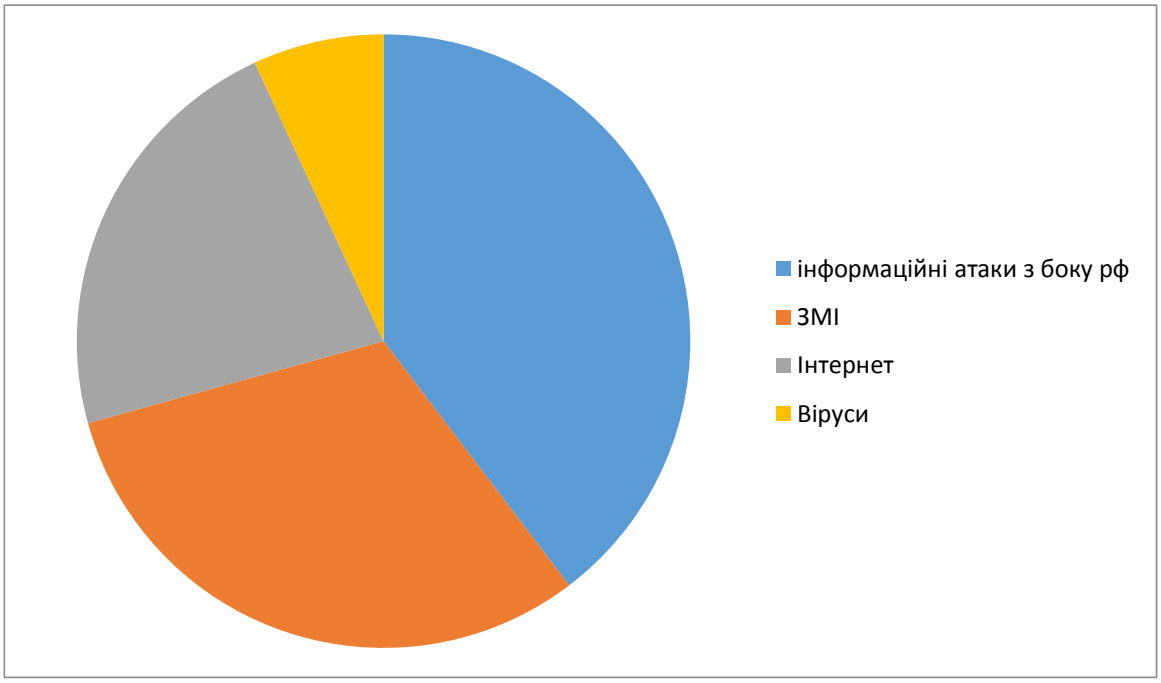

Рис. 1.5. Розподіл відповідей респондентів щодо оцінки ступеня небезпеки різних інформаційних загроз

Джерело: авторська розробка

Відповіді розподілилися наступним чином (за низхідною небезпекою інформаційних загроз): інформаційні атаки з боку рф - 23, ЗМІ - 18, Інтернет - 13, віруси - 4.

З наведених вище даних опитування, вочевидь одне: найбільше

занепокоєння респондентів викликають інформаційні атаки ворогів України та нинішній стан ЗМІ. На наш погляд, це пов'язано з тим, що більшість громадян у повсякденному житті постійно стали стикатися з погрозами, що мають національний та глобальний характер, які далеко назад відсунули всі інші позиції. Ні хакерство, ні технічні проблеми (збої, поломки, виведення з ладу, несанкціонований доступ) занепокоєння респондентів не викликають. Серед причин, чому ЗМІ становлять підвищену інформаційну загрозу, багато опитаних відзначили агресивність, вульгарність, еротичність, примітивізм багатьох інформаційних продуктів ЗМІ. Інтернет на думку респондентів є загрозою тому, що в ньому гранично доступні порнографічні сайти, сайти, що демонструють екстремізм, жорстокість, тортури та насильство, сайти, що навчають негативної, асоціальної та кримінальної поведінки, сайти, що пропагують людиноненависницькі ідеї та ін.

Інші позиції, на думку респондентів, відносяться до випадкових фактів життєдіяльності і не надають постійного інформаційного негативного впливу, до того ж багато респондентів самі не стикалися з такими загрозами і припускають їхню наявність потенційно, як явище, не обтяжене власним емпіричним пізнанням.

Нарівні з цим людей куди хвилює соціальна сфера, те, що відбувається з ними, у їхніх сім'ях, у їхньому оточенні, що деструктивно позначається на їхньому соціальному житті. І в цьому плані людей, перш за все, хвилює моральне та психічне здоров'я їх самих, їхніх дітей та близьких, друзів і товаришів по службі, тому вони відзначають як загрози соціальному, духовному, культурному, психічному та моральному благополуччю те, з чим стикаються найчастіше в своїй інформаційній сфері.

Таким чином, підбиваючи підсумок соціально-політичного моніторингу в рамках досліджень, ми можемо стверджувати, що результати моніторингу підтверджують авторську позицію, соціологічний аспект для вивчення інформаційної безпеки нам видається актуальним та обов'язковим. Соціально-політичних формат процесів формування інформаційної безпеки суспільства на

відміну від правового, економічного чи технічного та інших форматів, сьогодні є найбільш важливим і задіяний у безпосередньому публічному управлінні захисту інтересів суспільства в інформаційній сфері.

Отже, якість публічного управління в значній мірі визначається якістю взаємин між державними інститутами та громадянським суспільством в інформаційному просторі, що робить цей аспект невід'ємною складовою демократичного та відкритого публічного управління. Публічне управління являє собою процес послідовної розробки та прийняття управлінських рішень, організації виконання даних управлінські рішення, а також організації контролю за ходом їх виконання. Основним інструментом публічного управління є державна політика [99]. Насамперед необхідно виявити сутність терміна державна політика» з погляду сучасної науки. Бачиться обґрунтованою думка, що зміст політики представлена цілями, способами досягнення даних цілей, стратегічними та тактичними рішеннями управлінського характеру, принципами, методами прийняття та здійснення управлінських рішень з метою регулювання та розвитку конкретної сфери (соціального, економічного, інформаційного, зовнішньополітичного та іншого характеру) існування суспільства та держави. Держава та суспільство може ефективно функціонувати за умови правильно збудованої державної інформаційної політики (на міжнародному, державному та регіональному рівнях) з урахуванням внутрішньої зовнішньополітичних факторів. Формування та проведення державної інформаційної політики є комплексним завданням, яке має вирішуватися на основі розроблених методологічних концепцій та підходах щодо формування та реалізації інформаційної політики, що вимагає проведення системного аналізу інформаційного простору держави, яка потребує державного регулювання [90].

В рамках інформаційної політики, потрібно вирішувати такі завдання:

- забезпечувати надання інформації громадянам, а також інститутам, що належать до громадянського суспільства. У цьому потрібно розвивати масові комунікації, зокрема. комунікації транскордонного характеру, та масовий обмін

інформацією. При цьому слід враховувати необхідність реалізації профілактичних заходів та забезпечення захищеності від інформаційних загроз, які можуть бути обумовлені внутрішніми та зовнішніми факторами;

- забезпечувати інформацією органи, які здійснюють державну влада, органи місцевого самоврядування. При цьому також слід здійснювати транскордонний інформаційний обмін, а також виконувати профілактичні заходи та забезпечувати захищеність від загроз, які є як усередині держави, так і ініціюються ззовні;

- забезпечувати інформаційну взаємодію між владними структурами, зокрема державними органами, органами місцевого самоврядування і цивільним суспільством.

На думку деяких науковців, державна інформаційна політика являє собою сукупність офіційних поглядів і практичних заходів щодо їх реалізації державними органами влади [159]. На основі даного визначення можна зробити висновок, що державна інформаційна політика визначає напрями діяльності органів влади на державному та регіональному рівнях, організацій та підприємств у сфері інформаційних технологій, включаючи забезпечення інформаційної безпеки.

Інформація є ключовим ресурсом суб'єктів публічного управління.

У випадку, якщо особи, які ухвалюють рішення, мають можливість отримання більш детальної інформації, що характеризує зміни існуючої ситуації, вони мають широкі можливості щодо оперативного реагування на такі зміни. У рамках здійснення інформаційної комунікації як засобу політичної діяльності політичні керівники застосовують технічні системи одержання та передачі інформації. Застосування подібних систем - комп'ютерних мереж, автоматизованих систем, що забезпечують управління силами та засобами, навігаційних систем та ін, сприяє зростанню ефективності публічного управління.

Відбувається активне розширення можливостей щодо отримання та обробки інформації, яка використовується для прийняття управлінських рішень.

На основі цієї інформації можуть оцінюватися альтернативи розвитку ситуації для прийняття рішень із найвищим ступенем оптимальності. Отже, за допомогою активного використання інструментів інформаційної комунікації, якість ухвалених рішень покращується, оскільки рішення приймаються швидше та в короткі терміни. Реагування на те, як змінюється соціально-політична обстановка стає більш гнучким. Збільшуються можливості прогнозування зазначеної ситуації. Потенційні та реальні противники розглядають засоби інформаційної комунікації як об'єкт деструктивного впливу.

Інформаційні комунікації, відповідна інфраструктура, сама інформація набувають значення критично значущих компонентів, при несанкціонованому впливі на які можуть виникнути масштабні негативні наслідки. Забезпечення інформаційної безпеки є основним показником отримання достовірної та повної інформації, необхідної для формування державної політики. В умовах сьогодення механізми та способи забезпечення інформаційної безпеки стають особливо актуальними в процесі публічного управління. Забезпечення інформаційної безпеки органів державної влади розглядається як одне з пріоритетних завдань держави, що важливо для національної безпеки. Сучасні процеси публічного управління виявляються вразливими без належного рівня забезпечення інформаційної безпеки. Швидкий розвиток інформаційних технологій породжує нові виклики і загрози з інформаційного простору, які можуть значно пошкодити процесам публічного управління [91].

Документом, який є сукупністю офіційних поглядів у галузі забезпечення національної безпеки в інформаційному просторі, інформаційної безпеки у світі, включає в себе основні інформаційні загрози, стратегічні цілі та напрями, організаційними засадами захисту інформації є Стратегія інформаційної безпеки України [140].

Стратегія передбачає основні принципи, що визначають діяльність публічного управління в сфері інформаційної безпеки України, з основним завданням захисту інформаційних ресурсів та розвитку системи забезпечення інформаційної безпеки Положення Стратегії націлені на досягнення

ефективного функціонування системи публічного управління, а також спрямовані на організацію міжгалузевої та міжвідомчої взаємодії в частині що стосується системи забезпечення інформаційної безпеки.

З огляду на те, що інформаційна безпека впливає на стан та розвиток усіх складових національної безпеки, будучи її безпосередньою частиною Стратегія закріпила основні національні інтереси у цій сфері.

По-перше, це протидія дезінформації та інформаційним операціям, що здійснюються державою-агресором з метою ліквідації незалежності України, повалення конституційного ладу, порушення суверенітету і територіальної цілісності держави. Ці операції також спрямовані на пропаганду війни, насильства і жорстокості, а також на розпалювання національної, міжетнічної, расової та релігійної ворожнечі та ненависті. Вони можуть включати в себе вчинення терористичних актів та посягання на права і свободи людини..

По-друге, забезпечення розвитку української культури в усіх аспектах та підтримка української громадянської ідентичності.

По-третє, підвищення рівня медіакультури та медіаграмотності всіх шарів суспільства.

По-четверте, забезпечення прав особи на збирання, зберігання, використання та передачу інформації, вільне вираження своїх поглядів і переконань, захист приватного життя, доступ до об'єктивної та достовірної інформації, а також забезпечення захисту прав журналістів і їх безпеки під час виконання професійних обов'язків, протидія поширенню незаконного контенту.

По-п'яте, відновлення інформаційної інтеграції громадян України, що проживають на тимчасово окупованих територіях та прилеглих до них територіях України, в загальноукраїнський інформаційний простір і відновлення їх права на отримання інформації для збереження зв'язку з Україною, є одним із основних напрямів внутрішньополітичної діяльності держави. Це включає захист прав, свобод і законних інтересів громадян на тимчасово окупованих територіях, реалізацію ініціатив щодо реінтеграції цих територій, а також захист прав і свобод корінних народів України. [140].

Особливої актуальності набуває процес прогнозування та аналізу всього спектра загроз національній безпеці в інформаційній сфері.

Причини загроз необхідно виявляти, проводити їх аналіз для визначення їх системності впливу та виробляти шляхи, методи та засоби їх нейтралізації. Загрози, що виходять з інформаційного простору, є на цьому етапі світового розвитку найактуальнішими через те, що впливати на об'єкт можливо за допомогою різних інформаційних заходів, інформаційних атак та ін. Дані заходи мають на увазі широке використання ІКТ, що діють у глобальному інформаційному просторі, характеризуються високою швидкістю поширення інформації великого обсягу, можуть бути нанесені з будь-якої точки землі. Проведення більшості спеціальних операцій в інформаційній сфері виявляється на той момент, коли операцію вже завершено і всі її цілі реалізовані. Інформаційні атаки проводяться блискавично та анонімно, і мають детально сплановане прикриття [92].

В науковій літературі зустрічаються різні підходи, щодо класифікації загроз інформаційної безпеки. Загрози можна класифікувати за кількома аспектами. Одним із найпоширеніших підходів є розділення їх на технічні, організаційні, людські та природні. Однак ми можемо виділити шість основних загроз:

1. Розкриття конфіденційної інформації: Це включає неправомірний доступ до чутливої інформації, що може призвести до її розголошення, що порушує приватність та безпеку.

2. Знищення та спотворення інформації: Ця загроза охоплює видалення або зміну даних, що може призвести до втрати інформації або її спотворення, що може призвести до помилкових рішень або неправильних дій.

3. Злом (неправомірне) втручання в роботу: Це означає несанкціонований доступ до комп'ютерних систем або мереж, зокрема шляхом використання хакерських методів або злому паролів.

4. Виведення комп'ютерних систем із ладу, зниження їхньої працездатності: Ця загроза передбачає атаки на інфраструктуру, спрямовані на

те, щоб призвести до вимкнення систем або зниження їхньої працездатності.

5.Перевищення повноважень непривілейованих користувачів: Це може включати недбале використання привілеїв або намагання непривілейованих користувачів отримати доступ до даних або ресурсів, до яких вони не мають доступу.

6. Відмова від авторства та трансакцій: Це включає в себе ситуації, коли сторона відмовляється від відповідальності за власні дії або трансакції, що може призвести до порушення прав та відповідальності.

Ці загрози можуть мати серйозний вплив на індивідуальність, суспільство та державу, оскільки інформація є ключовим ресурсом у сучасному світі, і її недбале використання чи неправильне використання може призвести до серйозних наслідків[111].

У політологічному аспекті основні інформаційні загрози України виділяє Стратегія інформаційної безпеки України:

1. Інформаційний вплив російської федерації як держави-агресора на населення України. Інформаційна війна та спеціальні інформаційні операції, спрямовані з боку російської федерації на підрив національних інтересів та суверенітету України, є серйозною загрозою для національної безпеки та стабільності країни. Продуктивність цих операцій полягає в їхній систематичності та використанні різноманітних методів та технологій, що можуть впливати на суспільно-політичну, економічну та культурну ситуацію в Україні. Створення панічних настроїв, поширення дезінформації, підрив довіри до уряду та інституцій, а також провокація конфліктів та екстремізму — це лише деякі зі способів, які можуть використовувати зловживання.

Боротьба з цими загрозами вимагає комплексного підходу на рівні національних та міжнародних стратегій. Це означає посилення кібербезпеки, підвищення обізнаності громадян з питань інформаційної безпеки, розвиток механізмів виявлення та протидії дезінформації, а також співпрацю з міжнародними партнерами для підтримки міжнародної безпеки та правопорядку. Важливо також підкреслити роль міжнародного співтовариства у

підтримці суверенітету та територіальної цілісності України, а також у виявленні та припиненні дестабілізаційних дій, спрямованих ззовні.

2. Обмежені можливості ефективно реагувати на дезінформаційні кампанії.

Деструктивна пропаганда та поширення дезінформації можуть стати основною причиною підриву стійкості суспільства та дестабілізації держави. Недостатня ефективність системи реагування на такі загрози та відсутність розвиненої національної інформаційної інфраструктури обмежують можливості відповіді на інформаційну агресію та захист національної безпеки. Для ефективної боротьби з дезінформацією та пропагандою необхідно розвивати національну інформаційну інфраструктуру. Це включає в себе механізми перевірки фактів, забезпечення доступу до об'єктивної та достовірної інформації, підвищення медіаграмотності населення та підтримку незалежних медіа. Також важливо удосконалювати механізми реагування на дезінформацію та пропаганду, залучати до цього різноманітні суспільні та державні структури, включаючи медіаоргани, громадянське суспільство, експертні групи та міжнародних партнерів[140].

Нові інформаційні технології різко підвищили ефективність засобів впливу на психічний стан особистості та суспільства [46]. Подальший розвиток ІКТ лише розширить можливості засобів маніпулювання інформацією. Особливу увагу слід приділити розвитку міждисциплінарних напрямків, таких як інформаційно-психологічна безпека, для ефективного протидії негативним впливам. ЗМІ, як цілодобове джерело інформації, повинні бути надійними та об'єктивними. Розвиток медіаорганів, які дотримуються етичних та професійних стандартів, сприятиме формуванню правильної громадської думки. Просвітницька робота серед громадян, підвищення медіаграмотності та забезпечення прозорості державних органів є ключовими компонентами для забезпечення інформаційної безпеки та захисту національних інтересів.

3. *Недостатній розвиток системи стратегічних комунікацій.*

Недостатній розвиток системи стратегічних комунікацій в Україні є

серйозним викликом, особливо в умовах інформаційної війни та гібридної загрози, які виникають ззовні. Необхідність ефективних стратегічних комунікацій стає важливою для зміцнення національної безпеки, захисту національних інтересів та підвищення відповідальності держави перед громадянами та міжнародним співтовариством. Україна перебуває на етапі активного формування системи стратегічних комунікацій, де органи державної влади здійснюють значні зусилля для посилення своєї інституційної спроможності в цій сфері. Втім, необхідно признати, що поки що не було належним чином розроблено ефективний механізм координації та взаємодії між різними органами влади, що беруть участь у протидії загрозам в інформаційному просторі [171].

На нашу думку комп'ютерна розвідка та збирання інформації від іноземних держав є однією з ключових загроз інформаційній безпеці. Розвідницькі агентства інших країн займаються збором інформації, спрямованої на отримання конфіденційної інформації, включаючи державні таємниці і наукові розробки. Вони використовують комп'ютерну розвідку, включаючи програмні закладки в технічні пристрої, спеціальні програми доступу і сканери мереж для незаконного доступу до баз даних і інформаційних систем. Це дозволяє їм обходити захист, а також перехоплювати комунікації для отримання повідомлень [163]. Однією з основних цілей такої розвідки є отримання інформації про економічний, військово-технічний і науковий потенціал країни. Комп'ютерна розвідка доповнюється іншими глобальними розвідувальними системами, що активно пристосовуються до нових завдань.

Широке використання терористичними та екстремістськими організаціями світових інформаційних ресурсів та механізмів інформаційного впливу на поширення ідеології тероризму, нагнітання міжнаціональної та соціальної напруженості тощо. Діяльність терористів також перемістилася в інформаційний простір, даний напрямок названо «інформаційний тероризм», або «кібертероризм».Інформаційний тероризм ґрунтується, насамперед, на використанні інформаційних технологій. Поняття кібертероризму було введено

у науковий обіг у середині вісімдесятих років минулого століття Б. Коліном, співробітником Інституту безпеки та розвідки (США). Вказаним терміном були позначені прояви терористичного характеру у межах віртуальний простір. Останнім часом спостерігається тенденція активного використання екстремістськими угрупованнями сучасних ІКТ з метою пропаганди своєї ідеології та досягнення поставлених цілей. Дані організації та терористичні угруповання активно займаються розробкою та використанням різних засобів деструктивного впливу на об'єкти критичної інформаційної інфраструктури.

Нові способи та механізми інформаційної дії стали активно використовуватись у технічних та віртуальних системах. Цей розвиток призвів до збільшення застосування та поширення інформаційної зброї, що створює загрозу інформаційних війн та інформаційного тероризму як нових форм впливу на геополітичну обстановку. Головна мета використання цієї зброї - це порушення функціонування інформаційної структури суспільства, підрив авторитету державних органів та створення сумнівів у дієвості проводжених ними державних стратегій.

На нашу думку, наявність потенційних загроз можливого застосування інформаційної зброї проти України обумовлено низкою причин:

- застосування зарубіжних інформаційно-комунікаційних систем у структурах органів виконавчої влади, промисловості, кредитно банківській сфері, паливно-енергетичному комплексі та інших сферах створює передумови до впровадження іноземними спецслужбами спеціальних програмних та апаратних закладок. Вони призначені для руйнування програмних засобів у вибраний момент, або створюють канали несанкціонованого знімання чи спотворення інформації;

- незаконне поширення на вітчизняному ринку несертифікованих імпортних та вітчизняних програмно-апаратних засобів;

- вихід українських користувачів державних органів влади, підприємств, установ у глобальну соціальну мережу «Інтернет» без необхідних технічних засобів захисту інформації [89].

Не менш актуальною загрозою є комп'ютерні атаки на промислову сферу, яка стає все більш актуальною в сучасному світі, де технології все більше використовуються в промислових процесах. Ці атаки можуть мати різні цілі, такі як крадіжка конфіденційної інформації, руйнування промислового обладнання або вплив на виробничі процеси. Зросла кількість комп'ютерних атак (хакерських операцій) на інформаційні мережі, інформаційні державні системи та інформаційні системи персональних даних, кредитно-фінансову сферу

На основі розглянутих загроз інформаційній безпеці, можна виділити основні загрози в інформаційній сфері для України, які також можна класифікувати як внутрішні та зовнішні. До внутрішніх загроз можна віднести:

- низькі темпи інформатизації та розробки нових сучасних видів засобів обробки та видобутку інформації (технологічна залежність вітчизняних інформаційних технологій від іноземних виробників);

- навмисні дії, помилки фахівців, відповідальних за забезпечення захисту інформації;

- недостатня координація та фінансування робіт в організаціях та підприємствах, органах влади із захисту інформації;

- недостатня розробленість законодавчої бази.

До зовнішніх загроз можна віднести:

- втручання в інформаційне забезпечення державної політики держави;

- проникнення в діяльність та організаційну структуру інформаційної інфраструктури України (а також впровадження та вплив на критичну інформаційну інфраструктуру об'єктів захисту);

- технічні впливи шляхом проникнення у будь-які функціонуючі мережі, системи зв'язку, інформаційні системи тощо;

- розробка рядом країн концепцій інформаційних війн, створення інформаційної зброї;

- збільшення технологічного відриву провідних держав світу;

- інформаційно-пропагандистська діяльність іноземних держав;

- діяльність міжнародних терористичних організацій.

Підбиваючи підсумки вищезазначеного дозволяє зробити наступні висновки:

1. Необхідно зазначити, що формування та оновлення публічного управління в сфері інформаційної безпеки має відбуватися системно з урахуванням національних інтересів України, постійно змінюваних умов і нових загроз інформаційної безпеки, що походять як з зовнішнього інформаційного простору, так і обумовлені внутрішніми змінами в країні. Лише при державному підході до розв'язання проблеми захисту інформації в інформаційних системах та телекомунікаційних мережах можуть бути створені умови для ефективного протистояння зростаючим загрозам в інформаційній сфері. Це передбачає вдосконалення національної інформаційної інфраструктури, що охоплює електронні ЗМІ, банківські системи, транспортні та енергетичні системи, промисловість та сферу послуг. Крім того, ця інфраструктура активно розвивається і доповнюється мережею "Інтернет".

2. На основі політики, що проводиться державою щодо забезпечення інформаційної безпеки можна сказати, що рівень захисту інформації не відповідає сучасним процесам, потребам держави та суспільства.

3. Розробка комплексної державної політики в галузі забезпечення інформаційної безпеки України, яка враховує як внутрішні, так і зовнішньополітичні аспекти, а також організація ефективних процесів публічного управління, є актуальним завданням нашого часу.

2.2. Методичні засади використання механізмів публічного управління у сфері інформаційної безпеки

Реалізація публічного управління в сфері інформаційної безпеки України забезпечується проведенням єдиних організаційно-технічних заходів на території держави органами влади різних рівнів, організаціями та підприємствами щодо забезпечення безпеки інформації від внутрішніх та зовнішніх загроз. Інформаційне забезпечення органів публічного управління є основною умовою для сталого розвитку та ефективного функціонування державних механізмів, а також проведення процесу публічного управління, яке відповідає сучасним міжнародним реаліям, а також для внутрішньодержавних потреб [169].

Законодавча база, в сфері інформаційної безпеки перебуває в стадії становлення. Однак, позитивним є спостереження за покращенням нормативно-правового середовища для розвитку інформаційно-комунікативних функцій держави. Відмінною особливістю державної інформаційної політики в Україні за останню чверть століття став її стрімкий динамізм [90]. Можливо, саме ця характеристика спричинила відсутність досі розробленої та затвердженої, як мінімум на урядовому рівні, концепції державної інформаційної політики як цілісного політичного документа. На жаль, досі не було запропоновано концептуальну модель державної інформаційної політики

Аналізуючи нормативно-правову базу виконання розглянутої функції держави, стає очевидним, що, незважаючи на деякі прогресивні зміни, законодавство в цьому напрямку не є достатньо розвиненим через свою суперечливість, переважно декларативний характер та значні прогалини. Ці обставини утворюють юридичні перешкоди для реалізації державою інформаційно-комунікативної функції. Наприклад, в різних законодавчих актах перелічується велика кількість інформаційних об'єктів, що мають статус таємниці, проте за розголошення не всіх із них передбачається юридична

відповідальність, що робить деякі норми суто формальними. Також варто звернути увагу на те, що сучасне українське законодавство, яке регулює питання забезпечення інформаційної безпеки, не враховує захист інформаційної свободи у повному обсязі. Крім того, недосконалість правової бази стає особливо помітною в період, коли суспільні відносини розвиваються швидше, ніж встигає змінюватися законодавство. Це призводить до ситуації, коли громадяни, суспільство, підприємства та організації змушені самостійно захищати свої права, часто виходячи за межі чинних законів [20].

Оцінка сучасного стану виявила численні проблеми в правовій системі, коли окремі норми порушують Конституцію, а підзаконні акти стають інструментом зловживання владою чиновниками. Це приводить до ситуації, коли громадяни й організації, намагаючись захистити свої права, змушені діяти самостійно, оскільки держава не може повністю забезпечити їх безпеку в інформаційному середовищі. Такий самозахист є конституційним принципом, але його регулювання на законодавчому рівні залишається неповним, що залишає великий простір для випадковостей у практиці."

Підзаконні акти, такі як постанови чи розпорядження, часто залишаються поза увагою громадськості, але вони можуть мати значний вплив на права та свободи громадян. Наприклад, нормативні акти міністерств можуть надавати широкі повноваження чиновникам, що створює передумови для волі виконавчої влади. Для вирішення цих проблем потрібні системні реформи в правовій системі. Це може включати перегляд норм законів з урахуванням конституційних принципів, зміни у процесі ухвалення підзаконних актів для забезпечення прозорості та відкритості, а також посилення механізмів контролю за дотриманням прав громадян та обмеженням можливостей свавільного використання влади [5].

Науковці окрім нормативно-правового компоненту визначають наступні компоненти публічного управління у сфері інформаційної безпеки:

- організаційно-технологічний компонент, який охоплює структуру та функціонування інформаційно-комунікаційної інфраструктури;

- техніко-економічний компонент, що включає в себе розробку та виробництво інформаційно-комунікаційних технологій;

- соціальний компонент, який забезпечує підготовку кадрів, правильне використання технічних засобів та інформаційних систем.

У рамках розгляду механізмів здійснення публічного управління у сфері інформаційної безпеки держави ми дотримуватимемося освітлення даних компонентів.

Публічне управління в сфері інформаційної безпеки держави проводиться і здійснюється у вигляді прийняття управлінських рішень, які ґрунтуються відповідно до законодавства держави, і є основним обов'язком уповноважених посадових осіб. Для здійснення та проведення публічного управління, яке має бути спрямоване на реалізацію національних інтересів України в інформаційній сфері, державною владою формуються:

- концептуальні документи, які визначають перспективи розвитку інформаційної сфери в Україні, в сфері забезпечення інформаційної безпеки - розробляються та приймаються відповідно з положеннями, закріпленими у Конституції України;

- законодавство України в інформаційній сфері, що визначає правила та обмеження у сфері регулювання суспільних відносин в інформаційній сфері;

- організаційне та технологічне забезпечення діяльності держави в інформаційній сфері, а також організація державного контролю як об'єкта публічного управління.

У сучасному швидкозмінюваному світі виникає значна кількість нових викликів у сфері інформаційної безпеки. Це включає інформаційний тероризм, кібертероризм, кібербезпеку, дестабілізацію публічного управління, комп'ютерні атаки, напади на віртуальні системи, психологічні операції, а також різні типи інформаційних конфліктів, такі як кібервійна, мережева війна, сетецентрична війна та інші. Нові високотехнологічні загрози, такі як використання інформаційної зброї та розробка високотехнологічних засобів розвідки, також потребують уваги.

Ця ситуація ставить перед нами завдання постійного розвитку, удосконалення та оновлення нормативно-правової бази в сфері інформаційної безпеки і контролю кіберпростору. Організаційно-технологічний аспект передбачає функціонування інформаційно-комунікаційної інфраструктури, яка повинна бути надійною та відповідати сучасним вимогам безпеки та захисту інформації. Інформаційна діяльність держави визначається діяльністю органів державної влади, яка, з одного боку, спрямована на розвиток інформаційної інфраструктури та створення умов для її ефективного функціонування та вільного доступу громадян до інформаційних ресурсів. З іншого боку, ця діяльність також передбачає створення законних бар'єрів для доступу громадян до певного виду інформації, що може завдати значних втрат особистості, суспільству та державі.

У тексті Доктрини наголошується на важливості забезпечення інформаційної безпеки критичної інформаційної інфраструктури. Публічне управління в сфері інформаційної безпеки України реалізується у вигляді формування державними органами влади необхідних правових, економічних, організаційних та інших умов, що сприяють охороні та захисту інформаційної інфраструктури, а особливо критичної інформаційної інфраструктури [125].

Під критичною інформаційною інфраструктурою розуміються об'єкти, відключення або пошкодження яких може призвести до серйозних наслідків та втрат для функціонування держави. Наприклад, це може спричинити втрату управління державою та її економікою, непередбачувані зміни у публічному управлінні, а також становити загрозу національній безпеці та інші негативні наслідки. В Україні тільки почалася розробка нормативно-методичних документів, що регламентують забезпечення безпеки критичної інфраструктури, у тому числі в галузі забезпечення інформаційної безпеки.

Важливо відзначити, що порушення функціонування критичної інфраструктури може мати серйозні наслідки. Наприклад, перебої в постачанні електроенергії можуть призвести до зупинки промислових підприємств, порушення роботи комунальних служб та зниження якості життя населення.

Порушення в роботі транспортної інфраструктури може посилити затори, затримки в постачанні товарів та негативно вплинути на економіку.

Ці приклади демонструють, як уразлива може бути інфраструктура, яка забезпечує нормальне функціонування життєво важливих систем. Тому важливо приділяти належну увагу заходам забезпечення кібербезпеки та запобігання можливим атакам на інфраструктуру. Тільки таким чином можна забезпечити безпеку та стабільність роботи критичних систем інфраструктури для нашого суспільства.

Техніко-економічний компонент публічного управління в сфері інформаційної безпеки передбачає розробку та виробництво інформаційно-комунікаційних технологій. У зв'язку з уповільненими процесами інформатизації в Україні та застарілим програмним забезпеченням та засобами інформатизації, захист безпеки органів влади, організацій та підприємств під час розробки та функціонування систем захисту частково здійснюється за допомогою обладнання та програмного забезпечення іноземного виробництва. Проте не завжди при цьому відбуваються спеціальні перевірки та атестація технічних засобів обробки інформації та автоматизованих робочих місць.

Це призводить до збільшення ризиків несанкціонованого доступу до оброблюваної інформації. Недоліки в забезпеченні безпеки інформації можуть мати серйозні наслідки, включаючи витоки конфіденційної інформації, порушення захисту особистих даних, а також можливість кібератак та інших злочинних дій

Для зменшення цих ризиків необхідно удосконалювати процеси інформатизації, активно впроваджувати сучасні засоби захисту інформації, а також забезпечувати адекватну перевірку та сертифікацію використовуваного обладнання та програмного забезпечення [162]. Важливо також залучати внутрішні та зовнішні експертні ресурси для оцінки потенційних загроз та удосконалення систем захисту інформації з метою забезпечення їх ефективності та стійкості до сучасних викликів у сфері кібербезпеки.

Соціально-політичні механізми у контексті забезпечення інформаційної

безпеки включає підготовку кваліфікованих кадрів та ефективне використання технічних засобів інформаційних систем, також включає в себе комплекс заходів, спрямованих на підвищення усвідомлення громадськості щодо проблем інформаційної безпеки, формування культури безпеки в інформаційному середовищі та залучення громадськості до активної участі у заходах з цієї сфери. Це є ключовим аспектом успішності публічного управління у цій сфері.

Протягом останніх років проблема "недостатнього кадрового забезпечення в галузі інформаційної безпеки" не тільки залишається невирішеною, але й поглиблюється [2]. Це стає однією з основних слабкостей в системі забезпечення інформаційної безпеки будь-якої організації та основною причиною успіху атак, що використовують методи соціальної інженерії.

Зростання координованості та масштабності інформаційних атак на критично важливі об'єкти інформаційно-комунікаційної інфраструктури вимагає забезпечення високого рівня готовності сил та засобів попередження та виявлення комп'ютерних атак та ліквідації наслідків їх проведення. При недотриманні правил обробки та використання інформації, відсутності контролю, регламентів з технічного захисту інформації, розкриття інформації, що циркулюється в органах державної влади, може знизити ефективність публічного управління, що проводиться. Порушення правил експлуатації технічних засобів, зокрема, відбувається через слабкий рівень контролю керівництва та недостатньої відповідальності за порушення у сфері захисту інформації [87].

В даний час це завдання вирішується в рамках функціонуючої системи підготовки, перепідготовки та підвищення кваліфікації кадрів у зазначеній сфери. Водночас наростання нових викликів та погроз в інформаційному просторі обумовлює необхідність вжиття додаткових заходів щодо вдосконалення цієї системи.

Для вирішення цих проблем має бути забезпечена адресна підтримка та цільова підготовка фахівців з інформаційної безпеки в рамках окремої групи спеціальностей та напрямів підготовки, підвищена ефективність

функціонування профільних освітніх організацій, у тому числі за рахунок розвитку їхньої матеріально-технічної бази. Комплексність та взаємопов'язаність завдань щодо вдосконалення кадрового забезпечення безпеки в інформаційній сфері зумовлює необхідність вжиття додаткових заходів нормативно-правового, організаційного та матеріально-технічного характеру.

Зокрема, доцільною є розробка концепції розвитку кадрового забезпечення в галузі інформаційної безпеки, визначення порядку підвищення кваліфікації. Це дозволить систематизувати підходи до підбору, підготовки та підвищення кваліфікації фахівців з інформаційної безпеки.

Важливо визначити не лише порядок підвищення кваліфікації, а й створити систему постійного навчання та моніторингу знань спеціалістів. Це дозволить фахівцям бути в курсі останніх тенденцій та інновацій у галузі інформаційної безпеки, що є критичним у сучасній швидкозмінному технологічному середовищі.

Також важливо удосконалювати програми навчання та сертифікації, щоб вони відповідали сучасним викликам та потребам галузі. Це допоможе забезпечити високий рівень професійної підготовки спеціалістів, що у свою чергу позитивно відобразиться на рівні захисту інформації та загальної ефективності роботи системи інформаційної безпеки.

Доктрина інформаційної безпеки України передбачає, що публічне управління, націлене на те, щоб забезпечити інформаційну безпеку в Україні, реалізується у вигляді відповідної системи, яка включає комплекс заходів, спрямованих на захист інформаційних ресурсів, виявлення та протидію загрозам кібербезпеці, забезпечення конфіденційності, цілісності та доступності даних, а також належного використання інформаційних технологію. Ця система повинна бути побудована на засадах комплексності, координації та постійного удосконалення, залучаючи як державні, так і приватні ресурси для забезпечення ефективного функціонування та захисту інформаційного простору країни.

Система забезпечення інформаційної безпеки України проводить наступні

заходи:

- актуалізацію та оновлення нормативно-правових, керівних та методичних документів щодо захисту інформації в державі;

- формування середовища для реалізації громадянами своїх конституційних прав на використання та провадження діяльності в інформаційному просторі;

- координацію роботи на різних рівнях управління (державні, регіональні, місцеві), які здійснюють повноваження щодо забезпечення безпеки інформації;

- здійснення контрольно-наглядових заходів щодо оцінки діяльності та стану забезпечення інформаційної безпеки, підприємствах та організаціях;

- систематичну діяльність з виявлення загроз в інформаційній сфері та їх джерел, структуризації цілей та завдань забезпечення інформаційної безпеки у сфері оборони, їх реалізації;

- вироблення та визначення пріоритетних напрямів, що передбачають запобіганню, адекватне реагування, ліквідацію та усунення наслідків загроз;

- розробку державних та регіональних державних програм, спрямованих на підвищення рівня забезпечення інформаційної безпеки, розробку планів заходів, дорожніх карт щодо реалізації відповідних державних цільових програм;

- організацію системи захисту інформації в критичній інфраструктурі;

- розробку вітчизняних засобів інформатизації, телекомунікації та зв'язку, а також засобів захисту інформаційних ресурсів;

- організація взаємодії України з міжнародними організаціями та партнерами для захисту національних інтересів у сфері інформаційної безпеки.

Доктрина визначає організаційну основу, яка складається з органів управління та забезпечення інформаційної безпеки, а також основні функції цієї системи. Варто зазначити, що не прописано чітка структура системи забезпечення інформаційної безпеки.

Відповідно розділу VI Доктрини згідно з Конституцією України та встановленим законодавством, Рада національної безпеки і оборони України

здійснює координацію діяльності органів виконавчої влади з метою забезпечення національної безпеки в інформаційній сфері. [125].

Так, забезпечення інформаційної безпеки учасниками процесу здійснюється відповідно до чинного законодавства України. Це означає, що всі організації та особи, що беруть участь в обробці, передачі та зберіганні інформації, зобов'язані дотримуватися встановлених законом вимог щодо захисту цієї інформації від несанкціонованого доступу, втрати, пошкодження або розголошення.

Законодавство України в галузі інформаційної безпеки охоплює такі аспекти, як захист персональних даних, кібербезпека, захист державної інформації, захист інформації у комерційних структурах тощо. Ці закони встановлюють вимоги щодо технічних, організаційних та процедурних заходів, які повинні бути вжиті для забезпечення адекватного рівня захисту інформації. [132-134].

Дотримання правових норм у сфері інформаційної безпеки є критично важливим для підтримки надійності обробки та обміну інформацією та для запобігання можливим загрозам для безпеки та конфіденційності інформації.

Останнім часом особливу увагу у законодавчому регулюванні зосереджено на проблемах, пов'язаних з Інтернетом, обігом персональних даних, електронною взаємодією влади та громадськості, участю міністерств і відомств у соціальних мережах, наданням державними органами (зокрема, виконавчою владою) електронних державних послуг, електронною демократією, електронною комерцією та іншими сферами цифрового життя [93].

Важливо відзначити, що в діючій системі законодавства відсутній єдиний закон про державну інформаційну політику. У той же час, наявна нормативно-правова база, яка сформувалася, регулює безліч відносин, що виникли в інформаційній сфері.

Слід також зазначити, що основний категоріальний апарат науки, який пов'язаний з державною інформаційною політикою і закріплений у чинному законодавстві на той період, сформувався більше чверті століття тому.

Розвиток інформаційного законодавства відбувається по двох основних напрямках. Перший напрямок включає в себе розвиток законодавчого забезпечення державної інформаційної політики, а також інформаційного прогресу нашого суспільства та держави як науково-технологічного і соціально-економічного процесу. Другий напрямок спрямований на створення та втілення методів формування та реалізації державної інформаційної політики, що сприяє покращенню якості інформаційного розвитку суспільства та держави. Це має важливе значення, оскільки сучасна наука акцентує на двох основних принципах в інформаційній сфері: право на інформацію та право на доступ до неї. Сучасне інформаційне законодавство враховує ці аспекти.

Проведемо аналіз чинного інформаційного законодавства за основними напрямами, визначаючи його повноту та виявляючи прогалини.

Основне значення для інформаційної сфери дев'яностих років мав чинний і зараз Закон «Про інформацію» 1992 року. Тоді вперше на законодавчому рівні інформаційно-технологічний розвиток українського суспільств фіксувався як процес, метою якого була не тільки реалізація права громадян на інформацію, а й задоволення інформаційних потреб населення та органів державної влади на основі використання відповідних інформаційних ресурсів.

Таким чином, в організаційному плані законом ставилося нове для держави завдання формування інформаційних ресурсів на основі використання переваг комп'ютеризації, програмного забезпечення та ін.

Саме цей закон закріплює низку важливих понять інформаційної сфери – «інформація», «інформаційні технології», «інформаційна система» та низка інших [134].

Закон про інформацію постійно зазнає змін, оскільки відбувається швидкий розвиток технологій та суспільства. Останні зміни, які внесені, стосуються передусім регулювання взаємодії між органами влади та громадськими організаціями. Ці зміни стають актуальними в контексті вирішення різних аспектів інформаційної безпеки, забезпечення доступу до інформації, прав громадян на конфіденційність та інші аспекти.

Важливо зауважити, що ці зміни відбуваються в умовах посилення ролі Інтернету та цифрових технологій у суспільстві. Взаємодія з громадянами через Інтернет та використання онлайн-сервісів у сфері публічного управління також вимагають додаткових правових уточнень та адаптації законодавства до нових реалій. Такі зміни створюють необхідність удосконалення інформаційного законодавства та його відповідності сучасним викликам і потребам суспільства.

Результати проведеного аналізу свідчать про постійну динаміку у стані правового забезпечення державної інформаційної політики. Проте, очевидною є недостатність нормативного та правового регулювання нових відносин у сфері інформації, зокрема у зв'язку з широким використанням цифрових технологій у публічному управлінні.

Необхідність у більш широкому підході до правового регулювання нових видів відносин є надзвичайно важливою. Сучасні технології впливають на способи комунікації, управління та взаємодії у суспільстві [152]. Тому важливо розробляти та впроваджувати відповідні норми та правила, які враховуватимуть ці зміни та забезпечуватимуть ефективну та безпечну інформаційну діяльність. Особлива увага має бути приділена захисту особистої інформації, кібербезпеці та прозорості у використанні цифрових технологій в публічному управлінні.

Зважаючи на вищевикладене, можна зробити висновок про необхідність розробки спеціального законодавства та внесення відповідних поправок до чинних нормативних правових актів для відповідного регулювання використання цифрових технологій в публічному управлінні. Перехід значної частини механізмів адміністративно-правової взаємодії в Інтернет-простір породжує нові виклики та потребує уточнення правового регулювання.

Для цього можна розглянути внесення змін до Цивільного кодексу України щодо захисту прав в інформаційному середовищі, врегулювання відповідальності за цифрові правопорушення та захисту персональних даних. Також потрібно акцентувати увагу на аспектах кібербезпеки та прозорості у використанні цифрових інструментів у сфері публічного управління. Розробка такого законодавства допоможе узгодити цифрову трансформацію з вимогами

правового регулювання та забезпечити стабільну та безпечну діяльність у цифровому середовищі.

У зв'язку з вище викладеним, важливо врахувати особливості формування інформаційного законодавства щодо взаємодії влади та суспільства, які полягають у попередньому закріпленні політико-адміністративних практик. Останні зміни до законів, що регулюють відносини в інформаційній сфері, враховують переваги та можливі наслідки використання інформаційних технологій у взаємодії держави та суспільства.

Також слід підкреслити, що терміни, які класифікують інформацію за функціональними ознаками, розподілені за різними нормативно-правовими актами і часто не враховують специфіки публічного управління. Ця проблема також виявляється у розкиданих визначеннях і термінах, які використовуються в законодавстві. Особливо це стосується діяльності державних органів виконавчої влади.

У сучасних умовах ця проблема частково вирішується прийняттям норм, що регулюють оперативний режим управління. Однак існують невирішені питання, які потребують більш детального та системного підходу до регулювання інформаційних процесів у публічному управлінні. Такий підхід дозволить вирішити проблеми, пов'язані з пошуком, отриманням та поширенням різних видів інформації у сфері управління та забезпечить більш ефективну роботу системи управління в цифровому віці.

У світлі аналізу організаційно-правових механізмів публічного управління в сфері інформаційної безпеки та розвитку в Україні, можна зробити висновок про те, що використання цифрових технологій у взаємодії держави з суспільством, а також перехід значної частини цієї взаємодії в Інтернет-простір, ставлять перед державою завдання постійного моніторингу відповідних нормативно-правових актів.

Цей моніторинг обумовлений необхідністю оновлення різних форм взаємодії держави та суспільства, оскільки застарілі організаційно-правові механізми не в змозі ефективно функціонувати в умовах цифрової

трансформації суспільства. Ця ситуація може завдати шкоди досягненню відповідних управлінських цілей.

Очевидною стає невідповідність традиційних організаційно-правових механізмів новим умовам використання цифрових технологій, і ця проблема стає однією з ключових у публічному управлінні України. Тому є необхідність розробки та впровадження більш сучасних та адаптованих механізмів, що враховують особливості цифрової епохи та забезпечують ефективну взаємодію між державою та суспільством у цьому контексті.

У сучасних умовах розвитку інформаційних технологій та зростання їх впливу на суспільство в Україні та з метою заповнення прогалин у законодавчому забезпеченні реалізації публічного управління в сфері інформаційної безпеки виникає потреба у вдосконаленні законодавчої бази, що регулює державну інформаційну політику [38]. Для цього варто розглянути можливість конституційного закріплення основ державної інформаційної політики, що сприятиме більш послідовному та узгодженому підходу до її реалізації з визначенням ролі державних інституцій у регулюванні та контролі інформаційного простору та забезпечення конституційних гарантій прав громадян на інформацію та захист їх персональних даних.

Такий крок є важливим для встановлення правового фундаменту для ефективної діяльності державних органів у цьому напрямку. Нова стаття має передбачати механізми координації діяльності між урядовими структурами, визначення відповідальності за реалізацію державної інформаційної політики, а також забезпечення відповідності законодавства сучасним викликам і вимогам цифрової епохи.

Важливо також враховувати досвід інших країн у цьому питанні та залучати експертів з різних галузей для розробки конструктивних пропозицій щодо формулювання нових нормативних положень. Це дозволить створити сучасну та ефективну систему публічного регулювання в інформаційній сфері, сприяти розвитку інновацій та підвищенню конкурентоспроможності країни у цифровому світі.

Також варто зазначити, що в контексті використання інформаційних та цифрових технологій для підвищення ефективності взаємодії держави та суспільства, дуже важливим стає розробка концепції державної інформаційної політики. Ця концепція має враховувати високу значущість інформаційно-технологічного фактора, який впливає на сучасну політико-управлінську діяльність.

Створення такої концепції дозволить визначити стратегічні напрями розвитку державної інформаційної політики в умовах цифрових технологій. Це може стати основою для подальшої роботи над відповідним державним інформаційним законодавством, яке має відповідати викликам та потребам цифрової епохи.

Важливою частиною такої концепції буде визначення принципів, цілей та завдань державної інформаційної політики, а також механізмів її реалізації в контексті використання сучасних технологій. Це дозволить створити більш прозору та ефективну систему управління інформаційними ресурсами держави, сприяючи розвитку сучасного інформаційного суспільства.

Таким чином, аналіз функціонуючої системи забезпечення інформаційної безпеки вказує на:

1. Необхідність уточнення та доопрацювання правових механізмів, зокрема щодо чіткого визначення повноважень контрольних органів щодо забезпечення захисту інформації. Також вимагають удосконалення технічні регламенти та процедури атестації.

2. Розвиток інновацій у різних сферах життєдіяльності, зокрема у сфері технологій та інформаційної безпеки, ускладнює своєчасне оновлення базового законодавства. Це виникає з того, що нові технології швидко змінюються, існуючі загрози безпеці інформації еволюціонують, а способи їх захисту постійно переглядаються. Такі зміни вимагають частого перегляду та уточнення нормативно-правової середовища, що визначає стратегічні завдання та заходи щодо захисту інформації в сучасному цифровому світі.

Крім того, інноваційні технології вимагають гнучкого та адаптивного

підходу до законодавства, оскільки вони можуть змінювати способи обробки, зберігання та передачі інформації. Наприклад, впровадження хмарних технологій або розширена реальність може потребувати нових нормативних рамок для забезпечення конфіденційності та безпеки даних.

3. Система забезпечення інформаційної безпеки в Україні базується на законодавчих актах та регулятивних документах, визначаючи структуру та функції відповідних органів і установ.

4. Недостатній рівень професійної підготовки фахівців з інформаційної безпеки та нерегулярність підвищення кваліфікації відбиваються на ефективності функціонування системи захисту інформації, що може призвести до порушень у сфері захисту інформації.

5. Для забезпечення ефективного функціонування системи захисту інформації важливо покращити роботу служб безпеки та структурних підрозділів. Це сприятиме оптимізації діяльності регіональних систем забезпечення інформаційної безпеки та підвищенню ефективності публічного управління.

2.3 Зарубіжний досвід розроблення та впровадження механізмів публічного управління у сфері інформаційної безпеки

Публічне управління в сфері інформаційної безпеки є однією з найбільш актуальних і складних проблем у сучасному міжнародному співтоваристві. Ця сфера включає в себе розробку і реалізацію стратегій, формулювання політик, створення процедур і впровадження технологій, спрямованих на забезпечення конфіденційності, цілісності та доступності інформації в умовах постійно зростаючих кіберзагроз. Це важливий аспект не лише для захисту державної та корпоративної інформації, а й для збереження довіри громадськості до цифрового середовища і ефективного функціонування всіх секторів суспільства.

Ця тема набуває все більшого значення через зростання кількості кібератак, загроз кібершпигунства та інших кіберзлочинів. Міжнародні організації, уряди, компанії та громадські організації активно зосереджують увагу на розвитку та вдосконаленні стратегій публічного управління в сфері інформаційної безпеки для захисту важливих даних та критичної інфраструктури від потенційних загроз.

Розробка та впровадження інформаційного забезпечення національної безпеки за кордоном - це складний та детальний процес, який вимагає узгодженого дії та співпраці різних суб'єктів. Зазвичай ці завдання виконують спеціалізовані установи та організації, спираючись на підтримку урядових структур [82].

Цей процес включає аналіз різних аспектів національної безпеки, виявлення потенційних загроз та вразливостей, розробку стратегій та планів дій, реалізацію технічних рішень для захисту інформації, навчання персоналу, а також постійний моніторинг та аналіз ситуації.

Основними елементами цього процесу є розуміння унікальності геополітичного контексту, аналіз ризиків, гнучкість у відповіді на швидкозмінні ситуації та співпраця з міжнародними партнерами для обміну досвідом та інформацією. Цей підхід сприяє ефективному забезпеченню інформаційної

безпеки національних інтересів за межами країни у сучасному глобалізованому світі. Такий процес включає наступні етапи:

- ретельний аналіз потенційних загроз та викликів для національної безпеки за кордоном, таких як політичні, військові, економічні, кібернетичні загрози, тероризм, дезінформація тощо;

- на основі аналізу розробляється стратегія інформаційного забезпечення, яка визначає цілі, завдання, пріоритети та методи впровадження.

- створення технічних та програмних інструментів для збору, обробки, аналізу та розповсюдження інформації про потенційні загрози та виклики.

- міжнародне співробітництво, у багатьох випадках інформаційне забезпечення національної безпеки за кордоном потребує міжнародного співробітництва з іншими країнами, міжнародними організаціями та іншими зацікавленими сторонами.

- підготовка та освіта персоналу, цей етап включає навчання персоналу для ефективного використання інформаційних засобів та систем безпеки.

- після розробки інформаційного забезпечення воно проходитиме тестування в реальних умовах, після чого вносяться необхідні корективи. Після успішного тестування система впроваджується на практиці.

- інформаційне забезпечення національної безпеки за кордоном повинно постійно моніторитися та оновлюватись для адаптації до змін в загрозах та технологіях.

Зацікавленість вчених і практиків у питаннях ефективного публічного управління інформаційними системами та технологіями сприяла швидкому розвитку різноманітних галузевих, національних та міжнародних стандартів, що стосуються управління цими технологіями та системами загалом, а також їх безпеки.

У першій половині XX століття, коли з'явилася велика кількість нових електроприладів, які швидко набували популярності, були розроблені й швидко прийняті загальновизнані міжнародні стандарти для поліпшення умов міжнародної торгівлі та забезпечення її якості у сфері електричних приладів. Це

призвело до створення Міжнародної Електротехнічної Комісії. Згодом, коли виникла потреба в міжнародних стандартах для інших галузей, зокрема у сфері якості, була створена Міжнародна Організація по Стандартизації (ISO). Оскільки комп'ютерні та телекомунікаційні системи потребують уваги як до електротехнічних, так і до якісних аспектів, Міжнародна Електротехнічна Комісія співпрацює з Міжнародною Організацією по Стандартизації у рамках Спільного Технічного Комітету.

Міжнародна організація зі стандартів (ISO) та Міжнародна електротехнічна комісія (IEC) спільно або окремо розробляють серію міжнародних стандартів з інформаційної безпеки. Нижче наведено кілька ключових стандартів, розроблених цими організаціями:

ISO/IEC 27001:2013 - Цей стандарт визначає вимоги до систем управління інформаційною безпекою (СУІБ), включаючи процеси для управління ризиками та захисту інформації в організаціях.

ISO/IEC 27002:2013 - Надає настанови та загальні принципи для встановлення, впровадження, управління та покращення систем управління інформаційною безпекою в організаціях.

ISO/IEC 27005:2018 - Цей стандарт надає керівництво з оцінки ризиків та встановлення керівництва з ризиками для інформаційних систем.

ISO/IEC 27017:2015 - Оснований на стандарті ISO/IEC 27002, цей стандарт надає конкретні настанови щодо управління інформаційною безпекою в хмарних оточеннях.

ISO/IEC 27018:2019 - Спеціально орієнтований на захист персональних даних у хмарних сервісах, цей стандарт надає вимоги щодо контролю та обробки цих даних.

Ці стандарти допомагають організаціям будь-яких розмірів та галузей керувати ризиками та забезпечувати адекватний рівень захисту інформації, незалежно від її форми чи місцезнаходження. Вони враховують сучасні загрози та вимоги щодо безпеки інформації у цифровій середовищі .Доказом цього факту є наявність серії міжнародних стандартів, розроблених спільними

зусиллями Міжнародною організацією зі стандартів та Міжнародною електротехнічною комісією [192,194].

Розробка стандартів публічного управління в сфері інформаційної безпеки розпочалася у 1999 році, і перша частина документів була оприлюднена на початку 2000 року. Цей процес відбувався в рамках Міжнародної організації зі стандартизації (ISO) і став важливим кроком у встановленні міжнародних стандартів інформаційної безпеки для різних галузей та секторів, включаючи публічний сектор. У цій першій частині висвітлювалася проблематика сучасних тенденцій розвитку інформаційної безпеки та надавалися практичні рекомендації щодо впровадження механізмів публічного управління інформаційною безпекою. У 2002 році була випущена друга частина документа, яка описує загальну специфікацію запропонованих першою частиною рішень, а також оприлюднені супутні документи серії. Слід зазначити, що серія стандартів продовжує розвиватися, і ряд стандартів, що входять до цієї серії, постійно переглядається та оновлюється.

Підсумкова версія другої частини документа набула широкої популярності та схвалення в міжнародному співтоваристві. Результатом цих досліджень став вихід стандарту ISO/IEC 27000, який став важливим керівним документом для багатьох організацій у сфері інформаційної безпеки.

У процесі проведення дисертаційного дослідження особливу увагу було приділено стандартам ISO/IEC 27001 [192] та ISO/IEC 27002 [193]. Перший стандарт описує основні засади організації управління інформаційною безпекою для організацій різноманітних діяльностей. Інший стандарт більш детально розглядає безпосередні механізми управління інформаційною безпекою, розбиваючи їх на послідовні кроки щодо реалізації кожного із запропонованих механізмів.

Стандарт ISO/IEC 27000 виступає своєрідною передмовою до інших документів серії. Його основне призначення полягає в описі сфери впливу кожного зі стандартів, а також у визначенні загальних принципів та причин виникнення стандарту. Він також надає посібник з використання змісту

стандартів під час впровадження системи менеджменту інформаційної безпеки, включаючи опис основних процесних складових та актуальності впровадження цієї системи.

Так, відповідно до структури ISO/IEC 27000, серія стандартів є дійсно логічно пов'язаними документами, спрямованими на створення системи менеджменту інформаційної безпеки. Стандарт ISO/IEC 27001 встановлює вимоги до такої системи публічного управління в сфері інформаційної безпеки.

Відповідно до вимог стандарту ISO/IEC 27001, система публічного управління в сфері інформаційної безпеки повинна мати процесний характер, який відповідає циклу Демінга – Шухарта. Він допомагає забезпечити постійне удосконалення системи управління інформаційною безпекою шляхом циклічного процесу аналізу, впровадження змін, оцінки ефективності та корекції. Цей підхід є ключовим для забезпечення ефективності та неперервності управління інформаційною безпекою в організації. Це означає послідовність дій з планування, виконання, перевірки та коригування.

Керівництво організації повинно визначити межі дії системи публічного управління в сфері інформаційної безпеки та сформулювати політику управління інформаційною безпекою. Політика має відображати концептуальні характеристики бізнесу, активи та інформаційні технології організації. Наступним кроком є оцінка ризиків та вибір методів їх обробки для створення єдиної системи управління інформаційною безпекою [201].

Після виявлення ризиків, які можуть вплинути на активи організації, необхідно оцінити їх та сформувати стратегію управління ризиками. Це може включати зміну параметрів захисту, прийняття ризиків, позбавлення від ризиків або передачу їх на сторонні організації.

Головною метою цих заходів є зниження рівня ризику до прийнятного рівня - залишкового ризику. Система управління інформаційною безпекою має бути документованою та готовою до впровадження.

У процесі реалізації та експлуатації системи управління інформаційною безпекою, відповідно до стандарту ISO/IEC 27001, важливо виконати наступні

кроки:

- Формулювання плану обробки ризиків.

- Реалізація плану обробки ризиків.

- Формування та застосування засобів управління.

- Оцінка ефективності прийнятих засобів управління.

- Підготовка та здійснення плану підвищення кваліфікації персоналу.

- Управління діяльністю системи управління інформаційною безпекою.

- Управління ресурсами системи управління інформаційною безпекою.

- Впровадження в дію системи виявлення інцидентів інформаційної безпеки.

Ці кроки спрямовані на забезпечення ефективного управління інформаційною безпекою та зменшення ризиків для організації.

Так, цикл Демінга - Шухарта (PDCA) визначає чотири основні етапи: планування (Plan), виконання (Do), перевірка (Check) та дія (Act). Ці етапи є ключовими для постійного вдосконалення системи управління інформаційною безпекою в організації.

Планування включає у собі розробку стратегій, політик, процедур та інших аспектів системи управління інформаційною безпекою. Виконання включає реалізацію цих стратегій та політик у практичні дії. Перевірка полягає в оцінці ефективності системи та виявленні можливих відхилень від поставлених цілей. Дія означає впровадження корекційних заходів для покращення системи.

Одним із важливих аспектів цього циклу є постійне удосконалення, яке може бути досягнуто через процеси документування вимог та політик організації в галузі інформаційної безпеки, а також механізми реагування на інциденти інформаційної безпеки, включаючи "Управління записами".

Управління записами передбачає постійне ведення журналів, протоколів та форм дозволу доступу, пов'язаних як з активами та їх ризиками, так і з процесами забезпечення інформаційної безпеки організації. Це допомагає забезпечити збереження інформації про всі аспекти системи управління

інформаційною безпекою та забезпечує можливість аналізу та удосконалення цих процесів у майбутньому.

Стандарт також наголошує на необхідності постійного удосконалення системи менеджменту інформаційної безпеки, що досягається через проведення власного аудиту системи. Мета такого аудиту - перевірити відповідність системи бізнес-вимог, ефективність механізмів управління інформаційною безпекою та коректність виконання функцій захисту. Результатом процедури аудиту є аналітичний висновок щодо можливості покращення, доповнення або зміни системи, що сприяє подальшому удосконаленню та розвитку системи управління інформаційною безпекою.

У додатку до стандарту подається перелік додатків, метою яких є формалізоване подання цілей та засобів управління інформаційною безпекою.

Стандарт ISO/IEC 27002 є логічним продовженням стандарту ISO/IEC 27001 та надає більш детальний опис дій, описаних у ISO/IEC 27001, розширюючи свій діапазон до управління активами, прийому та вибору нового персоналу, фізичної та екологічної безпеки, захисту від небезпечного коду, резервного копіювання інформації, управління засобами зв'язку та операцій та іншими аспектами.

Ці стандарти спрямовані на формування правил управління інформаційною безпекою та послідовне виконання відповідних дій, що сприяє ефективному захисту інформації та зменшення ризиків для організації.

Зазначена інформація зосереджена на основних засадах управління доступом, що є важливим компонентом забезпечення інформаційної безпеки в організації. Виокремленні логічні компоненти управління доступом включають формування політики, облік активності користувачів, управління привілеями, а також управління доступом до мереж, операційних систем, інформації та програм.

Незважаючи на важливість цих принципів, виправлення недоліків та удосконалення систем публічного управління в сфері інформаційної безпеки, зокрема управління доступом, потребує врахування специфіки діяльності

конкретної організації та врахування сучасних тенденцій розвитку вітчизняних підприємств у сфері інформаційних технологій.

Також, необхідно враховувати розмитість формулювань та поверховість опису в деяких нормативних документах з публічного управління в сфері інформаційної безпеки. Це може викликати складнощі для реалізації принципів і вимог, описаних у таких документах. Проте, важливо визнати, що ці документи становлять базову основу для розробки конкретних політик та процедур інформаційної безпеки у межах конкретної організації [198].

Для забезпечення ефективного захисту інформації, організаціям рекомендується ретельно аналізувати та адаптувати принципи та вимоги нормативної документації з управління інформаційною безпекою до своєї конкретної ситуації, враховуючи унікальні аспекти їхньої діяльності та специфіку внутрішніх процесів. Такий підхід дозволить ефективно забезпечити безпеку інформації та відповідати вимогам сучасного інформаційного середовища.

У цьому контексті досліджено та систематизовано закордонні практики реалізації публічного управління у сфері інформаційної безпеки. Критеріями вибору для аналізу закордонних практик у зазначеній сфері стали інтеграційні прагнення України, стан впровадження соціально орієнтованих реформ у зарубіжних країнах, а також вчасність і системність реагування на інформаційні виклики в межах цих країн. Було проаналізовано досвід Великої Британії, Сполучених Штатів Америки, Південної Кореї, Швеції та інших. Виявлено, що ці країни накопичили значний позитивний досвід у цій сфері. Загалом, досвід цих країн показує, що впровадження структурованих та стандартизованих підходів до управління інформаційними технологіями сприяє підвищенню ефективності та безпеки, а також забезпечує відповідність до законодавчих вимог та стандартів інформаційної безпеки.

Так, у багатьох країнах існують національні стандарти щодо управління та безпеки інформаційних технологій, які доповнюють міжнародні стандарти. Один із таких фреймворків – Control Objectives for Information and related

Technology (COBIT) - використовується в США та інших країнах для управління інформаційними технологіями.

COBIT є фреймворком управління інформаційними технологіями, розробленим ISACA (Раніше - Асоціація аудиторів та контролерів інформаційних систем) та IT Governance Institute (Інститут управління IT). Він надає структуровані підходи до управління та контролю IT-процесів в організаціях з метою забезпечення ефективності, ефективності та безпеки використання інформаційних технологій. COBIT включає набір зразкових практик та контрольних механізмів, які допомагають організаціям забезпечувати відповідність до вимог законодавства, стандартів безпеки та інших вимог. Цей фреймворк також сприяє зростанню відповідальності в управлінні IT-ресурсами та реалізації стратегічних цілей організації через оптимальне використання інформаційних технологій .Основні складові COBIT включають:

- надає зразки кращих практик для управління різними аспектами IT, включаючи стратегічне управління, управління ресурсами, управління операціями та управління моніторингом;

- визначає конкретні цілі, які організації повинні досягти для ефективного управління IT та забезпечення відповідності вимогам законодавства та стандартів;

- надає механізми для вимірювання ефективності та моніторингу виконання IT-процесів в організації;

- спрямований на забезпечення того, щоб IT-процеси відповідали бізнес-потребам та стратегії організації.

COBIT використовується для впровадження найкращих практик управління IT, забезпечення внутрішнього контролю та відповідності, а також для допомоги у керуванні ризиками та забезпеченні безпеки інформації. Він може застосовуватися у різних галузях, таких як фінанси, охорона здоров'я, державні установи та бізнес-сектор. У Великій Британії, Нідерландах та Австралії фреймворк ITIL (IT Infrastructure Library) має значний вплив на

практику управління IT-послугами (ITSM) та визнаний як світовий стандарт для керування IT-послугами. ITIL забезпечує структурований підхід до управління IT-послугами, що включає планування, реалізацію, контроль та покращення IT-послуг.

Зазвичай, великі організації відмовляються від створення власних політик інформаційної безпеки через високі витрати та невпевненість у досягненні бажаних результатів, у порівнянні із застосуванням стандарту ISO 17799. Переваги використання стандартів управління та безпеки інформаційних технологій стають очевидними, коли організація розглядає можливість залучення зовнішніх постачальників для виконання певних функцій. Використання відкритих стандартів як основи для укладання угод про рівень обслуговування між партнерами призводить до зменшення розбіжностей, а також знижує витрати і ризики.

Якщо раніше аудитори створювали власні набори стандартів, програми аудиту та контрольні списки для використання їх як еталонів, то зараз використання загальнодоступних міжнародних стандартів (наприклад, COBIT, ISO 17799 та ISO 9001) призводить до зниження витрат як для аудитора, так і для організації, яка підлягає аудиту, і сприяє кращому розумінню аудиторами потреб організацій.

Організації також можуть використовувати відкриті стандарти для внутрішнього аудиту, створюючи тим самим основу для інтегрованого аудиту. Навіть процес аудиту стандартизувань за міжнародними стандартами, такими як ISO 19011 та EA 7/03.

Посилення уваги до якості корпоративного управління призводить до зростання значимості незалежної сертифікації. Швидке оцінювання доцільності ведення торгівлі з організацією без зовнішнього аудиту, що дорого обходиться, або перевірки спрощується, якщо ця організація може довести відповідність критеріям, пред'явивши свідоцтва від зовнішньої, незалежної сторони, яка заздалегідь оцінила якість і безпечність цієї організації.

Для таких стандартів, як BS 15000 (BritishStandards), ISO 9001, стандарти

Європейського Фонду Управління Якістю та TickIT, також є процедури сертифікації.

Для аудиту інформаційних систем особливо важливими є різноманітні процедурні стандарти, які дозволяють перевіряти безпеку, ефективність, надійність та відповідність системних процесів прийнятим стандартам та вимогам. Ось кілька ключових процедурних стандартів, які найчастіше застосовуються для аудиту інформаційних систем:

ISO/IEC 27001 та ISO/IEC 27002: Ці стандарти визначають міжнародні вимоги та рекомендації щодо систем управління інформаційною безпекою та надають практичні поради з імплементації відповідних контрольних механізмів.

COBIT (ControlObjectivesforInformationandRelated Technologies) - це рамковий стандарт, що надає конкретні контрольні цілі та керівництво для управління та аудиту інформаційними технологіями.

ITIL (InformationTechnologyInfrastructureLibrary) - це набір практик для управління технологічними послугами, які забезпечують ефективне використання технологій у бізнес-середовищі.

NIST SP 800-53: Це федеральний стандарт безпеки США, що визначає набір контрольних заходів для федеральних інформаційних систем та організацій, що управляють цими системами.

PCI DSS (Payment CardIndustry DataSecurity Standard): Цей стандарт визначає вимоги щодо захисту платіжної інформації для організацій, що обробляють карткові транзакції.

Використання цих стандартів може бути важливою основою для аудиторів інформаційних систем, оскільки вони надають визнані рамки та нормативи для забезпечення безпеки та ефективності інформаційних систем.

У світі стандартизації та безпеки інформаційних технологій, крім широкого спектру процесуальних та тактичних вимог, існує велика кількість експлуатаційних та технічних стандартів. Такі організації, як Міжнародна організація зі стандартизації (ISO), Європейський Інститут Стандартів Телекомунікації (ETSI) та Національний Інститут Стандартів і Технологій

(NIST), на чолі з глобальними ініціативами, встановлюють стандарти для шифрування, оцінювання технічних критеріїв безпеки інформаційних технологій, стратегій забезпечення безперервності бізнесу та політики використання паролів.

Ці стандарти не лише регулюють використання криптографічних алгоритмів та методів шифрування, але також визначають вимоги щодо безпеки систем зберігання даних, перевірки доступу та аутентифікації користувачів. Вони також охоплюють аспекти планування відновлення після інцидентів, управління ризиками та заходи захисту від кібератак.

Ці стандарти відображають найкращі практики та актуальні технологічні вимоги у сфері інформаційної безпеки, сприяючи забезпеченню стійкості та надійності систем інформаційних технологій в умовах постійно зростаючих загроз кібербезпеки. Регулярне оновлення цих стандартів відображає швидкий темп розвитку технологій та зміни у вимогах безпеки, що відображає постійну боротьбу з новими викликами та загрозами в цифровій середовищі.

Дійсно, багато стандартів об'єднуються у сімейства або стають складовими частинами інших стандартів, що сприяє систематизації та уніфікації підходів у різних галузях.

Наприклад, BS 15000 є британським стандартом для управління послугами у сфері інформаційних систем, що складається з двох частин: перша частина – це специфікація для управління послугами, а друга – набір правил для управління цими послугами. На наступному рівні ієрархії знаходиться ITIL, який об'єднує найкращі практики для процесів, описаних у BS 15000, а також внутрішні процедури для організації цих процесів.

Аналогічну ієрархію можна помітити у стандартах, таких як BS 7799-2 (специфікація управління інформаційною безпекою), ISO 17799 (набір кращих практик управління інформаційною безпекою) та ITIL Security Management (опис процесів інформаційної безпеки).

Ця ієрархія дозволяє створювати систематичний підхід до управління різними аспектами інформаційної технології та інформаційної безпеки, а також

використовувати найкращі практики та стандарти відповідно до потреб та специфіки конкретної організації чи галузі. У зв'язку зі значною кількістю стандартів державного регулювання у галузі інформаційної безпеки, фахівцям потрібно мати великий арсенал знань для вибору найбільш відповідних. Використання цих стандартів вимагає створення карт сфер їх застосування та взаємозв'язків між ними. Це може призвести до необхідності розробки метастандарту - надстандарту, який визначав би загальні принципи для інших стандартів. На жаль, в умовах сучасного стану такого метастандарту ще не існує.

Більшість існуючих стандартів спрямовані на властивості конкретних процесів. Технічні стандарти, такі як ISO 15408 та критерії оцінювання безпеки інформаційних технологій, детально описують необхідні властивості систем.

Щоб правильно використовувати ці стандарти, фахівцям слід мати глбоке розуміння їх сфери застосування та взаємодії. Розробка метастандарту може сприяти упорядкуванню та спрощенню процесу вибору та застосування відповідних стандартів у галузі інформаційної безпеки.

ISO/IEC 27002, раніше відомий як ISO/IEC 17799:2005, є стандартом, що описує практичні заходи з управління інформаційною безпекою. Він був прийнятий та опубликований Міжнародною організацією зі стандартизації (ISO) та Міжнародною електротехнічною комісією (IEC) у 2005 році. Цей стандарт надає загальний набір вказівок та рекомендацій з інформаційної безпеки, які можуть бути використані організаціями для забезпечення відповідності, а також для удосконалення своїх систем управління інформаційною безпекою.

IT Governanc eImplementation Guide з високим ступенем деталізації описує кроки з впровадження корпоративного управління інформаційними технологіями. з високим рівнем деталізації розкриває етапи впровадження корпоративного управління інформаційними технологіями.

Підхід до порівняння стандартів і колекцій кращих практик є дуже важливим у сфері публічного управління сфері інформаційної безпеки та IT управління загалом. Розробка структури для порівняння стандартів дозволяє організаціям краще розуміти сутність кожного стандарту, його переваги та

обмеження, що допомагає їм вибирати найбільш підходящі для їх конкретних потреб. COBIT (Control Objectives for Information and Related Technologies) вважається одним з найбільш відомих та широко використовуваних стандартів управління IT. Він надає рамки та рекомендації для ефективного управління інформаційними технологіями в організаціях. ISO 17799 (зараз ISO/IEC 27002) є стандартом, спрямованим на управління інформаційною безпекою. Він містить набір керівних принципів та загальних рекомендацій з управління безпекою інформації, які можуть бути використані будь-якою організацією, незалежно від її розміру чи галузі діяльності. Порівняння COBIT з ISO 17799 (ISO/IEC 27002) допомагає організаціям краще розуміти, як ці два стандарти можуть доповнювати один одного, як вони можуть бути інтегровані в процеси управління організації та як вони можуть сприяти досягненню цілей щодо управління інформаційною безпекою та IT управління загалом. Такі порівняльні аналізи допомагають організаціям зрозуміти, які стандарти найкраще відповідають їхнім потребам та вимогам, і як вони можуть інтегрувати ці стандарти для покращення своїх процесів управління та забезпечення безпеки інформації.

Наприкінці зауважимо, що сучасні міжнародні стандарти у сфері публічного управління в сфері інформаційної безпеки належно висвітлюють різні ключові аспекти цієї проблематики. Наприклад, ISO 17799 акцентує увагу на важливості проведення аудиту інформаційної безпеки, але не надає конкретних директив щодо методів його проведення. У таких випадках корисними можуть бути керівні принципи аудиту, які пропонує COBIT, особливо у контексті активного порвняння COBIT із ISO 17799.

При стратегічному публічному управлінні інформаційною безпекою можна користуватися рекомендаціями, що містяться в BS 7799, а для оперативного складового управління безпекою інформаційних технологій - стандартами, розробленими в рамках Security Management ITIL. В цілому, фахівці у сфері безпеки повинні володіти здатністю вибирати найкращі практики з усіх цих стандартів та інтегрувати їх у систему ефективного

управління безпекою інформації. Такий підхід дозволяє забезпечити комплексний підхід для забезпечення безпеки даних та інформації.

Європейський парламент 13 березня 2024 року прийняв історичний законодавчий акт — Закон про штучний інтелект (Artificial Intelligence Act). Цей закон є першою в світі горизонтальною правовою базою для регулювання штучного інтелекту (ШІ) і встановлює загальні правила для використання та впровадження ШІ в Європейському Союзі. Основні аспекти цього закону включають класифікацію ризиків, вимоги до прозорості, обов'язки виробників, заборони на небезпечне застосування, а також створення органів контролю та контролю. Нижче наведено детальний розгляд основних положень закону. Системи ШІ будуть класифіковані за рівнями ризику, що дозволяє застосовувати диференційовані підходи до їх регулювання:

- Мінімальний ризик. Для систем, які становлять мінімальний ризик, не передбачено спеціальних вимог або обмежень. Приклади таких систем включають більшість ігрових програм або фільтри спаму.

- Обмежений ризик. Системи з обмеженим ризиком підлягатимуть мінімальним вимогам прозорості. Наприклад, чат-боти повинні інформувати користувачів, що вони взаємодіють з ШІ.

- Високий ризик. Високоризикові системи, які можуть впливати на безпеку, основні права або значні інтереси громадян, підлягатимуть суворим вимогам щодо прозорості, надійності та безпеки. Це включає системи, які використовуються у критичній інфраструктурі, освіті, працевлаштуванні, правосудді та управлінні державними ресурсами.

- Неприйнятний ризик. Системи, що становлять неприйнятний ризик, будуть заборонені. Це включає застосування ШІ для соціального оцінювання громадян державними органами, маніпуляцій поведінкою людей та експлуатації вразливих груп.

Закон про штучний інтелект забороняє використовувати системи ШІ для певних цілей з метою захисту прав громадян та уникнення зловживань. Конкретно, заборонено:

- Використання ШІ для збору зображень облич з інтернету або відеоспостереження для створення баз даних розпізнавання облич.

- Системи ШІ мають чітко ідентифікувати штучно створений контент, такий як deepfakes.

- Забезпечення дотримання авторських прав при використанні ШІ, включаючи захист даних, використаних для тренування моделей ШІ. Ці положення спрямовані на захист приватності, забезпечення прозорості та запобігання потенційним зловживанням технологіями штучного інтелекту. Користувачі повинні знати, коли вони взаємодіють із ШІ, і розуміти його роль у прийнятті рішень. У випадках високоризикових систем користувачам повинна бути надана інформація про принципи роботи алгоритмів та їх можливий вплив на результати.

Для забезпечення дотримання закону будуть створені спеціальні органи нагляду:

- Європейський комітет, відповідальний за координацію та контроль за дотриманням закону на рівні ЄС.

- Національні регулятори. Кожна держава-член ЄС зобов'язана створити або призначити національний орган, що буде здійснювати нагляд за виконанням закону на національному рівні.

Цей закон є значним кроком вперед у регулюванні ШІ, спрямованим на захист громадян та забезпечення етичного використання технологій. Він встановлює чіткі правила для всіх учасників ринку, сприяє інноваціям і гарантує безпечне впровадження ШІ у різних сферах життя.

Також слід звернути увагу на захист персональних даних, що дійсно має велике значення як для приватності, так і для конфіденційності громадян. Особисті дані, такі як ім'я, адреса, електронна пошта, номер телефону, фінансові дані та інша інформація, яка може ідентифікувати особу, є важливим активом кожної людини. Захист цих даних має велике значення для запобігання недозволеному доступу, зловживанням, крадіжкам, а також для збереження довіри користувачів до сервісів і продуктів, які вони використовують. Особисті

дані часто використовуються в онлайн середовищі, де вони можуть бути збережені на серверах різних компаній та організацій. Тому важливо, щоб ці компанії мали ефективні заходи безпеки для захисту цих даних від несанкціонованого доступу та втрати. Розробка та впровадження відповідних політик та стандартів безпеки, а також відповідність законодавству щодо захисту даних, стають ключовими завданнями для багатьох організацій у сучасному цифровому світі. У 2018 році в Каліфорнії, США, був ухвалений закон CCPA (California Consumer Privacy Act), який став одним з перших в країні і відзначається своїми строгими вимогами щодо захисту особистих даних та накладенням значних штрафів за порушення правил обробки даних. Цей закон свідчить про зростаючу увагу до приватності та захисту даних в онлайн середовищі, особливо у контексті великих технологічних компаній, які мають доступ до значних обсягів особистих даних користувачів по всьому світу. В Європейському Союзі у 2018 році був прийнятий Загальний регламент захисту даних (GDPR), який встановлює широкі та суворі вимоги стосовно обробки персональних даних громадян ЄС. Основні принципи GDPR включають законність, справедливість та прозорість у зборі та обробці даних, обмеження обробки до визначених, законних цілей, мінімізацію збирання даних, точність та актуальність даних, обмеження зберігання даних, інтегрованість та конфіденційність, а також захист даних від несанкціонованого доступу, втрати, знищення чи пошкодження.

Один із ключових аспектів GDPR - це розширений обсяг прав користувачів, включаючи право на доступ до своїх особистих даних, право на виправлення неточностей, право на видалення даних ("право на забобнення"), право на обмеження обробки, право на перенос даних, а також право висловлювати протест щодо обробки даних.

Нагадаємо, що GDPR також передбачає значні штрафи за порушення правил обробки персональних даних. Штрафи можуть бути значними, до 20 мільйонів євро або до 4% від річного світового обороту компанії за попередній фінансовий рік, в залежності від тяжкості порушення.

За два роки після введення в дію GDPR, було зафіксовано значну кількість порушень та накладено значні штрафи, що свідчить про серйозний підхід до захисту особистих даних в Європейському Союзі та про ефективність застосування цього регламенту.

Розвиток сучасних технологій та впровадження цифрових інструментів у сферу публічного управління та бізнесу необхідно супроводжувати ефективними заходами забезпечення інформаційної безпеки та захисту персональних даних. В контексті постійно зростаючих загроз кібербезпеки та несанкціонованого доступу до інформації, це стає одним із найбільш актуальних завдань для сучасних організацій та урядових структур.

Стандарти управління інформаційною безпекою, такі як ISO/IEC 27001, встановлюють важливі вимоги та практики для забезпечення стійкості та надійності систем інформаційних технологій. Вони допомагають організаціям впроваджувати найкращі стандарти управління та забезпечення безпеки, що сприяє покращенню якості послуг та зменшенню ризиків. Також, законодавчі акти, які регулюють захист персональних даних, такі як GDPR в Європейському Союзі та CCPA в Каліфорнії, свідчать про зростаючу увагу до приватності та захисту даних у цифровому світі. Ці закони встановлюють важливі принципи та права користувачів на контроль за своїми даними, а також накладають відповідальність на компанії за їхню правильну обробку та захист.

Узагальнюючи, захист персональних даних та забезпечення інформаційної безпеки є ключовими аспектами сучасного управління в умовах цифрової трансформації. Це вимагає не лише технічних заходів, але й ретельного вивчення та впровадження найкращих практик управління та законодавчих стандартів, які сприяють створенню довіри та стійкості інформаційних систем у сучасному світі.

Висновки до другого розділу

Підсумовуючи вищевикладене, підкреслимо основні висновки:

Так, формування та оновлення публічного управління в сфері інформаційної безпеки повинні відбуватися системно з урахуванням національних інтересів України, постійно змінюваних умов і нових загроз. Лише за державного підходу до цієї проблеми можна створити умови для ефективного протистояння зростаючим викликам в інформаційній сфері. Вдосконалення національної інформаційної інфраструктури, що охоплює електронні ЗМІ, банківські системи, транспорт та енергетичні мережі, промисловість та послуги, а також активний розвиток і доповнення мережі Інтернет є ключовими аспектами цього процесу.

Нинішній рівень захисту інформації в Україні не відповідає сучасним вимогам та потребам держави і суспільства, що вимагає розробки комплексної державної політики в галузі забезпечення інформаційної безпеки. Ця політика повинна враховувати як внутрішні, так і зовнішньополітичні аспекти, а також впроваджувати ефективні процеси публічного управління. Це означає створення ефективної системи публічного управління, яка забезпечить координацію та співпрацю між різними відомствами та органами влади. Така система має бути спрямована на протидію загрозам та викликам у сфері інформаційної безпеки, а також на забезпечення високого рівня захисту конфіденційної інформації. Отже, вдосконалення рівня захисту інформації та розробка ефективної державної політики в цій сфері є нагальним завданням для сучасного публічного управління, яке потребує комплексного та системного підходу.

Механізми публічного управління у сфері інформаційної безпеки держави потребують уточнень та доопрацювань, особливо щодо розроблення більш чітких повноважень для органів, що відповідають за контроль та нагляд за дотриманням вимог щодо захисту інформації.

Необхідно удосконалити механізми перевірок органів влади, організацій та підприємств на виконання вимог інформаційної безпеки. Це передбачає чітке визначення обов'язків та відповідальності кожного з учасників процесу, а також

розроблення ефективних інструментів для здійснення контролю.

Також важливо доопрацювати та уточнити технічні регламенти та регламенти атестації, щоб вони відповідали сучасним вимогам та технологіям. Це допоможе забезпечити високий рівень захисту інформації і відповідність його вимогам і стандартам.

Отже, уточнення та доопрацювання механізмів регулювання в сфері інформаційної безпеки держави є ключовими завданнями для підвищення ефективності захисту інформації та забезпечення безпеки в цілому.

РОЗДІЛ ІІІ. УДОСКОНАЛЕННЯ ПУБЛІЧНОГО УПРАВЛІННЯ У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

3.1. Механізми модернізації інформаційної безпеки України за допомогою інтеграції сучасних цифрових технологій

Використання цифрових технологій в Україні має значний потенціал для модернізації публічного управління в сфері інформаційної безпеки України. Цей процес не лише сприяє оптимізації внутрішніх процесів управління, а й впливає на сприйняття та взаємодію держави з громадськістю. Інтеграція сучасних цифрових технологій грає ключову роль у підвищенні рівня інформаційної безпеки в Україні. Застосування цих технологій сприяє ефективнішому виявленню та запобіганню кіберзагрозам, забезпечуючи стабільність та безпеку інформаційного простору країни. Для досягнення цієї мети необхідно поєднати зусилля державних органів, приватного сектору та міжнародних партнерів у розробці та впровадженні ефективних механізмів захисту.

Швидкий розвиток інформаційних і телекомунікаційних технологій викликає значні зміни в суспільстві та привертає увагу дослідників, політиків і фахівців. Ці зміни відображаються у всіх сферах життя, особливо в тих, де важливо враховувати вплив інформації. Саме через цей розвиток в Україні стає актуальною проблема інформаційної безпеки. Інформаційне суспільство - це стан, коли суспільство використовує передові технології для досягнення високого рівня розвитку у всіх галузях: політиці, економіці, науці, технологіях та культурі. З цим розвитком значно зростає обсяг доступної інформації, яка впливає на всі аспекти суспільного життя. Засоби масової інформації, зокрема, стають дуже важливими у контексті впливу на політичні процеси. Таким чином, наявність та розвиток інформаційних технологій невід'ємно пов'язані з розвитком сучасного суспільства і вимагають уваги та досліджень у сфері інформаційної безпеки та впливу на управлінські процеси [112].

Аналіз наукових публікацій показує, що протягом останніх трьох десятиліть інформаційного розвитку України ролі інформації в сучасному політичному процесі приділяли увагу багато вчених. Основними об'єктами їх

досліджень ставали, переважно, проблеми ЗМІ, інформаційних технологій, захисту інформації та інформаційної безпеки.

Останні кілька років спостерігається значна активність в управлінському дискурсі, який на ділі ставить перед собою завдання вивчення та аналізу проблем формування та розвитку електронного уряду в Україні, а також взаємодії органів громадської влади з суспільством у контексті розвитку мережевих технологій. Це стосується не лише технічних аспектів, але й важливих соціально-політичних та економічних наслідків цього процесу.

Наукові дослідження з проблематики електронного уряду дедалі частіше звертають увагу на питання прозорості діяльності влади та важливість розробки справедливих і ефективних систем електронних державних закупівель. Ці аспекти стають ключовими у формуванні сучасного публічного управління, особливо в умовах цифрової трансформації та активного використання мережевих технологій. Використання цифрових технологій та їх стрімке проникнення в різні сфери суспільства безперечно відкриває нові можливості, однак водночас ставить перед урядом та бізнесом великі виклики. Зокрема, все більше інформаційні та мобільні технології, а також соціальні мережі, стають не лише інструментом комунікації, але й засобом впливу на формування управлінських рішень та результатів. Це відкриває шлях до розуміння їх як технології, яка може впливати на суспільство та управлінські процеси [7].

Отже, необхідність модернізації публічного управління в Україні стає наочною, адже ця трансформація вимагає не лише технічних рішень, але й нових стратегій управління та взаємодії з громадськістю, бізнесом та іншими зацікавленими сторонами.

У зв'язку з цим на підставі аналізу чинних документів, у тому числі міжнародного та європейського рівня, що обумовлюють в умовах сучасного стану процеси модернізації публічного управління в сфері інформації та інформаційної безпеки, можна виділити такі інформаційні та цифрові технології, які визначають пріоритети інформаційного розвитку держави та суспільства, а також державної інформаційної політики на період до 2024-2030 р.р.

Накопичений людством позитивний досвід використання інформації за останнє тридцятиріччя після відкриття Інтернету як інноваційної технології у взаєминах держав світу зі своїми громадянами та бізнес-спільнотою, а також розвиток нових теорій публічного управління, що активно обговорювалися науковою громадськістю наприкінці XX – на початку XXI століття, кардинальним чином трансформує як повсякденне життя громадян, але й політичну сферу і публічне управління.

Виникає нове розуміння, нові концепції, нові ініціативи та нове ставлення до презентації суспільно- та бізнес значущої інформації, головним накопичувачем якої є держава.

Відповідно до закону України, «інформація» - будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді. У сучасному публічному управлінні активно використовуються такі види інформації, як «інформація про діяльність державних органів та органів місцевого самоврядування», «Інформація про діяльність судів», «Інформація про становище на ринку праці», "інформація загальнодоступна", "інформація обмеженого доступу", "інформація офіційна", "офіційна статистична інформація" і т.д [6].

Однак на сучасному етапі цифрового розвитку, вважаємо, слід вести мову вже не лише про саму інформацію та її роль у публічному управлінні. Поточний практичний стан розвитку інформаційної сфери характеризується, на відміну від попередніх періодів, транскордонністю інформаційних технологій, їх застосуванням у всіх аспектах життєдіяльності людини та великою залежністю стану економічного розвитку держави від ефективності використання ІКТ та цифрових технологій [76].

Одночасно стан розвиненості інформаційної інфраструктури набуває характеру критичної технології для України і охоплює як питання інформаційної безпеки нашого суспільства та держави так і ефективність публічного управління в країні.

Інформаційний аспект державної інформаційної політики в Україні також

набуває нового значення у зв'язку з розширенням областей застосування ІКТ, формуванням та використанням величезної кількості «Великих даних», насамперед, у державному секторі.

У зв'язку з цим, на перший план виходять не лише сама інформація, а й створені на її основі масиви даних, відомі як «Великі дані», які набувають важливого значення для модернізації сучасної державної інформаційної політики. Основу сучасних цифрових «великих даних», що використовуються в публічному управлінні, в умовах сьогодення становлять різні банки та бази даних, зосереджені, у тому числі, у державних інформаційних системах, використання яких врегульоване законодавством. «Великі дані» також характеризуються високою швидкістю зміни інформації, різноманітністю та своєю різнорідністю[209].

Для ефективного публічного управління також важливим є перехід державних органів від методів традиційної аналітики, зверненої в минуле, до сучасних цифрових можливостей аналітики «Великих даних» - до передбачуваної та прогнозної аналітики, а також до можливості прийняття управлінських рішень он-лайн.

Сучасні держави з кожним днем дедалі більше віддаляються від аналогового світу і стає дедалі ближче до цифрового. У 2017 році на Глобальному симпозіумі, організованому Міжнародним союзом електрозв'язку, було підкреслено, що «Життя в цифровому сполученому світі призводить до багатьох нових можливостей та очікувань у сфері соціально-економічного розвитку. В умовах сьогодення більш, ніж будь-коли, при побудові «розумного» суспільства завтрашнього дня потрібно, щоб переваги цифрового світу були доведені до всіх громадян світу усвідомленим, відповідальним та безпечним способом» [170].

Принципи регулювання інформаційно-комунікаційних технологій п'ятого покоління набувають загального визнання та створюють умови для цифрового розвитку не лише на глобальному рівні, а й у межах національних держав.

Виникає також і нове поняття – "цифровізація". Очевидно, що сучасний

розвиток держави вже найближчим часом позначиться терміном "цифровий розвиток" або "цифровізація". У зв'язку з цим вважаємо за необхідне, говорячи про процес "цифровізації" (в англійській версії - digitization, а також іноді digitalization) економіки та суспільства, перш за все, необхідно внести визначеність у термінологію.

Цифровізація охоплює широкий спектр аспектів, включаючи перетворення аналогових даних у цифровий формат, впровадження цифрових технологій у виробництво та послуги, розвиток цифрових платформ для комунікації та взаємодії. Цей процес змінює спосіб функціонування бізнесу, управління державними інституціями, освіти та здоров'я, а також підвищує доступність та ефективність різних сервісів для громадян.

У контексті цифровізації важливо чітко розуміти різницю між термінами "цифровізація" та "цифровий розвиток". Цифровізація описує процес переходу від аналогових до цифрових технологій, тоді як цифровий розвиток включає в себе ширший спектр трансформацій, що відбуваються у суспільстві та економіці через цифрові технології, включаючи нові бізнес-моделі, інновації та зміни у способі життя людей.

Отже, розуміння та використання вірної термінології є ключовими аспектами для успішної адаптації до цифрової епохи та досягнення позитивних результатів у цифровому розвитку економіки та суспільства. Нагадаємо, що свого часу небувалий вплив інформаційно-комунікаційних технологій на трансформацію суспільно-політичної сфери і, перш за все, сфери публічного управління в Україні стало основою позначення даних процесів як процесів «інформатизації»[18].

Вступ українського суспільства та держави в епоху розвитку та використання цифрових технологій означає цифрову (на основі використання Великих даних та їх аналітики) трансформацію всіх сфер людського життя та публічного управління, створення необхідних умов політичного, економічного, інформаційно-технологічного та правового характеру для формування нової цифрової екосистеми, підготовки кадрів, що мають цифрові компетенції,

підготовлені до життя і роботи в цифрову епоху[170].

Цифровим трансформаціям піддаються і саме українське суспільство, і держава. У цьому правомірно також, з погляду, говоритиме і про "цифровізацію суспільства", "цифровізацію держави", простору публічного управління.

Цифрова трансформація включає в себе широкий спектр процесів, починаючи від розвитку цифрової інфраструктури та цифрових сервісів до впровадження цифрових інновацій у різні галузі, такі як медицина, освіта, економіка та інші. Це вимагає не лише технічних змін, але й культурних та організаційних перетворень, щоб адаптувати суспільство та державу до вимог цифрової епохи.

Зрозуміло, що цифрові технології стають ключовим фактором конкурентоспроможності і розвитку країни, тому важливо надавати пріоритетне значення цифровому розвитку та гарантувати його успішну інтеграцію на різних рівнях суспільства та в усіх сферах діяльності держави.

Більш ніж у 30 європейських державах вже прийнято та реалізовано документи різного рівня (програмні та стратегічні) розвитку цифрових технологій в публічному управлінні, економіках цих країн та промисловому виробництві. Основним державним документом у сфері науково-технологічної політики Південної Кореї став третій базовий план розвитку науки та технології (2013-2017). Цей план був ключовим стратегічним документом, спрямованим на сприяння інноваційного розвитку країни через наукові та технологічні досягнення.

Третій базовий план розвитку науки та технології орієнтувався на кілька стратегічних напрямків, таких як підтримка досліджень і розвитку у важливих галузях, зміцнення науково-технічного потенціалу країни, сприяння комерціалізації наукових розробок та інновацій, розвиток високотехнологічних галузей та підвищення конкурентоспроможності економіки через технологічні інновації.

У цьому плані були визначені конкретні цілі, завдання, інструменти та механізми реалізації, а також розподіл фінансових ресурсів для підтримки

наукових та технологічних проектів. Важливою складовою плану було створення сприятливої інноваційної екосистеми, яка б підтримувала та стимулювала розвиток новаторських ідей та технологій у різних сферах діяльності. Третій базовий план розвитку науки та технології відіграв важливу роль у забезпеченні стабільного та стратегічного розвитку науково-технологічного сектору Південної Кореї, що сприяло підвищенню її міжнародного статусу в галузі наукових досягнень та інновацій.

Курс на цифровізацію України увійшов до розпорядження Кабінету Міністрів України «Про схвалення Концепції розвитку електронного урядування в Україні» 2017 року [144]. Відповідно метою цієї Концепції є встановлення напрямів, механізмів і термінів формування ефективної системи електронного урядування в Україні з метою задоволення потреб інтересів фізичних та юридичних осіб, покращення системи публічного управління, збільшення конкурентоспроможності та прискорення соціально-економічного розвитку країни. Учасниками з боку державної влади та управління стають Державне агентство з питань електронного урядування, міністерства: Міністерство цифрової трансформації, фінансів, освіти, закордонних справ та ін.

На сказане важливо звернути увагу у зв'язку з тим, що, визначаючи ключову роль у процесах цифрової трансформації міністерств та відомств як державних регуляторів, а також активну участь державних підприємств, які мають максимальну експертизу, необхідні технологічні та промислові ресурси для реалізації масштабних проектів у цих процесах, ми можемо говорити про відмінність України від зарубіжних країн, в яких у цифровому розвитку держави та суспільства беруть активну участь бізнес-структури.

Великі дані, їх аналітика, швидкість обробки інформації в цифрову епоху дозволяють розвивати ідею «Цифрової держави» нової сучасної моделі публічного управління [18].

Програма "Дія" (Дія. Цифрова) в Україні є однією з найбільш значущих ініціатив у галузі електронного урядування. Вона спрямована на впровадження сучасних цифрових технологій для поліпшення доступності та якості державних

послуг для громадян та бізнесу. Програма розвивається в контексті стратегії "Дія" та має на меті покращення ефективності публічного управління та створення сприятливих умов для розвитку цифрової економіки в Україні. Ця програма стала важливим кроком в розвитку електронного урядування в Україні та дозволяє громадянам та бізнесу зручно отримувати доступ до різних державних послуг без необхідності особистого візиту до офісів чи установ[34].

Слід визнати, що у попередні етапи електронного розвитку держави та суспільства було зроблено досить багато для того, щоб надавати державні послуги у зручнішій формі для громадян та організацій. Етап формування електронного уряду та найважливіших його сегментів - державних та комунальних закупівель та системи електронних державних послуг - завершився і цілком успішно функціонує.

При реалізації цих проектів передбачається, що спілкування між громадянами та державою у життєвих ситуаціях пройде значну трансформацію - від окремих запитів до комплексних рішень щодо всіх аспектів життя кожної окремої особи. Це стане можливим завдяки створенню єдиного масиву державних даних та впровадженню алгоритмів роботи з цими даними, які розроблять усі органи виконавчої влади спільно.

Таким чином, буде створена державна інфраструктура з однією цифровою платформою для взаємодії всіх учасників процесу - державних службовців, громадян та бізнес-структур. Ця єдина точка доступу до необхідних сервісів значно спростить взаємодію та роботу всіх сторін, забезпечивши ефективніше та зручніше надання державних послуг та вирішення життєвих питань кожного громадянина.

Цифровізація публічного управління в сфері інформаційної безпеки - відповідальне і державно важливе завдання, що вимагає ефективного керівництва, у зв'язку з чим процеси цифровізації державного сектора та економіки України набувають статусу найважливішого політичного процесу сучасності. Потрібно, насамперед, грамотне визначення цілей цифрової трансформації, визначення системи координат для країни, визначення структури

державних сервісів, розробка необхідних програм цифрового розвитку стратегічного та оперативного характеру. Основними критеріями успішності електронних платформ для публічного управління є зниження вартості операцій для публічного управління, збільшення на порядок швидкості надання державних сервісів, відсутність «паперового» дублювання процесів та задоволеності споживачів - громадян та бізнесу, насамперед.

У Концепції розвитку електронного урядування в Україні 2017 року зазначається необхідність модернізації публічного управління через реінжиніринг існуючих та створення нових адміністративних процесів у владних органах. Ці процеси мають бути оптимізовані з використанням сучасних інформаційно-комунікаційних технологій, спрямованих на забезпечення електронної взаємодії та спільної роботи, а також на підвищення відкритості та прозорості перед громадянами. [64]. У цьому важливою стає проблема цифровізації публічного управління в Україні. Україна визнала цифрову трансформацію як основну стратегічну ініціативу, що вже відзначена високими досягненнями у впровадженні передових технологій. Нещодавно країна зазнала успіхів у розвитку систем "ProZorro" та "e-Health", а також у запровадженні мобільного покриття 4G та електронних послуг у різних секторах.

Останні роки свідчать про рост підтримки цифрової трансформації в Україні як основного каталізатора економічного розвитку. Уряд у 2018 році прийняв Концепцію та План дій для розвитку цифрової економіки та суспільства на 2018—2020 роки, а в 2019 році нова виконавча влада представила амбітний план, який покликаний прискорити перехід української економіки у цифровий формат.

Міністерство цифрової трансформації визначило основні цілі до 2024 року:

- Забезпечення доступності 100 % публічних послуг онлайн для громадян та бізнесу;

- Покриття 95 % транспортної інфраструктури, населених пунктів та

соціальних об'єктів високошвидкісним Інтернетом;

- Залучення до програми розвитку цифрових навичок 6 мільйонів українців;

- Збільшення частки ІТ-продуктів у ВВП до не менше 10 %. громадян [94].

Ці кроки включають прийняття правових основ для цифрових прав громадян, підвищення доступності технологій та розвиток інфраструктури для забезпечення безперебійної та ефективної цифрової трансформації країни.

Україна має певні передумови для просування цифрового порядку денного, які включають недавно ухвалене законодавство про цифрову економіку та телекомунікації, розвиток цифрової інфраструктури, досягнення в сфері безготівкової економіки через розвиток електронної торгівлі (e-Trade), електронного захисту (e-Trust) та кібербезпеки (Cybersecurity). Ініціатива "Smart City", що була недавно започаткована Міністерством цифрової трансформації, свідчить про впевненість владних інституцій у наявності необхідної законодавчої та інституційної бази для впровадження комплексних ініціатив з побудови ІКТ-екосистем на регіональному та місцевому рівнях [103].

Підтримка цифрового розвитку України на шляху до Єдиного цифрового ринку Європейського Союзу підтверджується розробкою Стратегії інтеграції України до цього ринку, яка відома як "дорожня карта".

Цифрові технології трансформують соціальну політику, найважливішим напрямом якої є регулювання сфери соціально-трудових відносин, виникає нова соціальна парадигма. Сфера соціально-трудових відносин у цифровий час набуває особливого значення, яка стосується цифрової трансформації системи взаємовідносин між роботодавцем і працівником, а й вирішує нове завдання - сприяти створенню ринку праці, що відповідає вимогам і стандартам цифрової епохи.

Ще одним із головних напрямів цифровізації у соціальній та державній сфері стає цифровізація послуг та сервісів. У зв'язку з цим зростає роль Міністерства соціальної політики України та Державної служби України з питань праці у цифровізації соціальних послуг. Особливе місце займає питання

впровадження цифрових технологій у взаємовідносини роботодавця та працівника. *З* з 10 червня 2021 року в Україні офіційно діють електронні трудові книжки. У 2022 році запущено «Єдину інформаційну систему соціальної сфери» (ЄІССС), яка виконує різноманітні функції, спрямовані на забезпечення ефективного управління соціальними послугами та підтримкою громадян [44].

У сфері використання цифрових технологій у публічному управлінні в Україні існує ряд недоліків та проблем, які обмежують їхню ефективність та впровадження. Серед основних проблем можна виділити нестачу кваліфікованих кадрів у сфері ІТ, недостатню фінансову підтримку для розвитку цифрових ініціатив, недостатню координацію між різними органами влади у реалізації технологічних проектів, а також брак механізмів моніторингу та оцінки ефективності цих проектів. Також слід звернути увагу на технічні обмеження та недостатність інфраструктури. Коли ми кажемо про інфраструктурні обмеження мається на увазі неусуненість цифрового розриву (digital divide) в Україні, що призводить до того, що деякі регіони мають обмежений доступ до швидкого Інтернету та сучасних технологій. Відсутність доступу до стабільної мережі Інтернет може ускладнювати проведення онлайн трансляцій, роботу з великими обсягами даних та інші аспекти, пов'язані з цифровими послугами. В деяких місцевостях відсутні або недостатньо розвинуті цифрові інфраструктурні об'єкти, такі як центри обробки даних, хмарні сервіси або мережеві системи, що ускладнює реалізацію сучасних технологій у цих регіонах [155].

Часто у менших або віддалених регіонах може бути обмежений доступ до електронних державних послуг, банківських сервісів, медичних систем тощо через відсутність або недостатність цифрової інфраструктури для їхнього надання. У регіонах із недостатньо розвиненою цифровою інфраструктурою населення часто не має достатнього рівня знань про використання цифрових технологій та Інтернету. Недостатня технологічна грамотність може стати суттєвою перешкодою для доступу до електронних послуг і засобів комунікації. Як приклад недостатньої розвиненості цифрової інфраструктури в Україні, що

ускладнює доступ до електронних послуг та інформації для мешканців наведемо українське село на Західній Україні, що має назву Малинівка, станом на 2022 рік має близько 1500 жителів. У цьому селі доступ до швидкого Інтернету є практично відсутнім. Місцева цифрова інфраструктура обмежується лише мобільним зв'язком з невеликою пропускною спроможністю. Це створює проблеми для мешканців у використанні електронних послуг, особливо у сферах, які вимагають великих обсягів даних, наприклад, онлайн-освіта, відеоконференції для роботи або звернення до медичних послуг за допомогою телемедицини.

Ця ситуація є прикладом того, як недостатність цифрової інфраструктури у віддалених або малонаселених регіонах може ускладнювати життя мешканців та обмежувати їхні можливості використання цифрових технологій для отримання різних послуг та інформації.

Для досягнення поставлених цілей рекомендується приділити увагу наступним аспектам:

1.Підвищення інформаційної освіченості та технологічної грамотності:

- Важливо закріпити основні принципи та цілі підвищення інформаційної освіченості та технологічної грамотності у відповідних законодавчих актах. Наприклад, можливо внести зміни до Закону про освіту або створити окремий закон про цифрову освіту, де будуть визначені завдання, обов'язки та механізми реалізації програм цифрової грамотності;

- посилення партнерства з галузями промисловості, а саме залучення технологічних компаній та представників індустрії до розробки освітніх програм та практичних курсів з технологічних навичок. Створення спільних програм стажування та практик для студентів з можливістю отримання практичного досвіду в сучасних ІТ-компаніях та інноваційних стартапах;

- розвиток мережі інноваційних центрів. Запровадження державної підтримки для розвитку інноваційних центрів та лабораторій, де проводитимуться дослідження, тестування та розробка нових технологій. Надання доступу до цих центрів для студентів, учителів та громадських

організацій для проведення практичних зайняття та проектної діяльності;

- створення інноваційних освітніх форматів. Розробка інтерактивних онлайн-курсів та платформ для самонавчання з акцентом на сучасні технології, програмування, штучний інтелект, великі дані тощо. Організація хакатонів та технічних змагань серед студентів та молодих спеціалістів для стимулювання інтересу до інновацій та розвитку технічних навичок;

- розширення доступу до електронних ресурсів. Забезпечення широкого доступу до електронних бібліотек, навчальних платформ та онлайн-курсів для всіх верств населення, включаючи віддалені та малозабезпечені регіони. Підтримка ініціатив з розробки безкоштовних освітніх ресурсів з використанням відкритих ліцензій.

2 Покращення цифрової інфраструктури в України:

- розвиток широкосмугового інтернету. Інвестування в розвиток інфраструктури широкосмугового інтернету в малозаселених та віддалених регіонах країни.

- створення програм підтримки для провайдерів, що дозволяють забезпечити доступ до високошвидкісного Інтернету у всіх куточках України.

- розширення мережі мобільного зв'язку: Збільшення покриття мереж мобільного зв'язку, зокрема 4G та 5G, щоб забезпечити швидкий та надійний доступ до Інтернету на всій території країни.

- підтримка розвитку мобільних операторів та стимулювання їхньої конкуренції для покращення якості послуг та зниження цін.

- створення "розумних" міст. Інтеграція цифрових технологій у міське планування та управління для покращення якості життя мешканців.

- розробка та впровадження "інтернету речей" (IoT) у таких сферах як транспорт, енергетика, комунальні послуги тощо.

3. Кібербезпека та захист даних:

- запровадження строгих стандартів кібербезпеки та захисту персональних даних у всіх цифрових сервісах та мережах.

- проведення навчання та підвищення обізнаності серед користувачів щодо

кібербезпеки та безпечного користування Інтернетом.

4. Підтримка інновацій та стартапів:

- створення сприятливого клімату для розвитку інноваційних технологій та стартапів у сфері ІТ;

- надання фінансової та інфраструктурної підтримки для ініціатив, що сприяють розвитку цифрової економіки та інноваційного середовища.

Загалом, розвиток цифрових технологій у публічному управлінні потребує комплексного підходу та активного впровадження заходів з усунення існуючих недоліків для досягнення максимальної ефективності та користі для суспільства. Використання цифрових технологій не лише стає глобальним трендом, але й є стратегічним кроком для розвитку України в сучасному світі. Це дозволяє країні збільшувати ефективність своєї економіки, покращувати якість життя громадян та зміцнювати національну безпеку. Однак, інфраструктурні обмеження, такі як обмежений доступ до швидкого Інтернету, варто вирішувати, щоб кожен регіон мав рівні можливості використовувати цифрові ресурси. Реалізація цих напрямків покликана не лише сприяти ефективному публічному управлінню та зміцненню інформаційної безпеки, але й забезпечити стабільний розвиток України у глобальному цифровому середовищі.

3.2 Напрями розвитку організаційно-правових механізмів публічного управління в сфері інформаційної безпеки в умовах використання цифрових технологій

У нинішніх умовах важливо розглядати адаптацію організаційно-правових механізмів публічного управління в сфері інформаційної безпеки до сучасних викликів. Це включає у себе міжвідомчу координацію та формування єдиної державної політики у цій сфері.

Інформаційна безпека стає все більш важливою у зв'язку з розвитком технологій та збільшенням кількості кіберзагроз. Тому необхідно підтримувати актуальність механізмів управління і забезпечення безпеки інформації. Міжвідомча координація дозволяє забезпечити більш ефективне використання ресурсів та обмін інформацією між різними відомствами та органами влади. Формування єдиної державної політики також сприяє узгодженому підходу до проблем інформаційної безпеки. Технології інформаційного століття вплинули на всі сфери життя та діяльності суспільства, охопивши різні типи країн, включаючи індустріальні, постіндустріальні та інші. Цей процес зміни структури економіки та соціокультурного середовища є свідченням глибокого впливу технологій на сучасний світ[33].

Державна інформаційна політика є важливим компонентом публічного управління в сфері інформаційної безпеки, який визначає стратегії, принципи та механізми регулювання інформаційних процесів в державі. Це охоплює не лише збір, зберігання та обробку даних, а й їхню захищеність та доступність. Розвиток цифрових технологій ставить перед урядом нові завдання у сфері інформаційної політики[18].

Одним з основних аспектів цієї політики є забезпечення безпеки та конфіденційності інформації, що обробляється державними органами. Це включає в себе захист від кібератак, використання шифрування та інших технологій, а також розробку відповідних нормативних актів.

Крім того, державна інформаційна політика повинна сприяти доступності та прозорості інформації для громадян. Це означає розвиток електронного уряду

(e-government), впровадження електронних сервісів та забезпечення відкритого доступу до даних про діяльність державних установ.

Загалом, державна інформаційна політика має сприяти ефективному публічному управлінню через використання сучасних інформаційних засобів, забезпечуючи захист інформації, її доступність та прозорість для всіх зацікавлених сторін.

За останню чверть століття в інформаційному розвитку України як держави, з одного боку, і українського суспільства, з іншого, відбулися кардинальні трансформації, що вплинули на сутність та зміст публічного управління і не знайшли досі необхідного глибокого відображення у комплексних дослідженнях у рамках сучасної науки публічного управління.

В умовах дедалі більшого використання цифрових технологій в публічному управлінні в Україні та, загалом, їх впливу на соціально-економічний розвиток країни в доступному для огляду стратегічному майбутньому на 2024-2030 роки [96]. Сучасна державна інформаційна політика теоретично характеризується фрагментарністю та дублюванням досліджень, що створює ризики, за яких існуюча система знань може швидко застаріти в умовах нової цифрової ери. Це вимагає модернізації, яка повинна охопити широкий спектр досліджень для забезпечення актуальності та відповідності новим цифровим відносинам у суспільстві та державі. Вже наголошувалося, що державна інформаційна політика в Україні пройшла серйозні структурні та змістовні трансформації - від політики в галузі ЗМІ до політики у сфері великих даних та інформаційних систем, цифровізації економіки.

При цьому підкреслимо також, що в Україні досі немає ні закону, ні концепції державної інформаційної політики. Це також, незважаючи на те, що відповідні рекомендації щодо формування основних напрямів реалізації інформаційної політики держави, починаючи з 2004 року, сформулювали низку міжнародних організацій, серед яких ЮНЕСКО.

Суть рекомендації даного компетентного органу, головним чином, полягала в необхідності розробки відповідного документа, який би носив,

безумовно, національно-державний характер і був свого роду керівництвом до дії в плані інформаційного розвитку суспільства і держави. Окрім того, об'єктивною недостатністю характеризується законодавче забезпечення реалізації державної інформаційної політики в умовах використання цифрових технологій. Це дозволяє зробити висновок про необхідність виправлення цього пробілу[122].

Очевидно, у зв'язку зі сказаним, що публічне управління та державна інформаційна політика України в умовах використання цифрових технологій має бути вдосконалена та модернізована не лише з погляду теорії науки, розвитку теорії управлінських процесів, технологій та інститутів, а й із практичної точки зору. У цьому механізми вдосконалення і, тим паче, модернізації державної інформаційної політики повинні мати як теоретико-методологічний, а й науково-практичний характер.

Вважаємо також практично необхідною розробку концептуально-цілісної моделі організаційно-правових механізмів реалізації публічного управління в сфері інформаційної політики. Така модель допоможе забезпечити системність, цілісність та ефективність публічного управління в сфері інформаційної безпеки та іншими аспектами інформаційної політики.

Під концептуально цілісною моделлю організаційно-правових механізмів реалізації публічного управління в сфері інформаційної безпеки України з урахуванням використання цифрових технологій з метою цього дисертаційного дослідження розуміється досягнення наступних основних завдань.

По-перше, у практичному аспекті необхідно виключити наявні прогалини в концептуальному та законодавчому забезпеченні реалізації державної інформаційної політики шляхом ухвалення Концепції державної інформаційної політики, закону про державну інформаційну політику або внесенням відповідних поправок до чинного законодавства.

По-друге, напрацьовані суб'єктами України організаційно-правові практики реалізації інформаційної політики необхідно гармонізувати з основними напрямками інформаційної діяльності Міністерства цифрової

трансформації.

Зазначені напрями становлять, на нашу думку, суть концептуально-цілісної моделі організаційно-правових механізмів реалізації державної інформаційної політики як складової механізму публічного управління в умовах використання цифрових технологій.

Зупинимося докладніше на основних напрямках запропонованої моделі.

Слід нагадати, що концептуалізація державної інформаційної політики, яка не відбулася у 1998 році, в умовах сучасного стану необхідна як у теоретичному, так і у прикладному плані. Концептуалізація інформаційної політики сучасної української держави можлива з урахуванням майже тридцятирічного періоду інформаційного розвитку.

За цей час досягнуто певних успіхів України як держави з інформатизації державних органів на всіх рівнях. Інформаційний розвиток забезпечується програмними та стратегічними документами, законодавством що постійно вдосконалюється. [172].

Цілком успішно розвиваються окремі напрями державної інформаційної політики. Тим часом, деякі з напрямків залишаються без належної уваги як на найвищому політичному рівні, так і на рівні законодавчого процесу. На нашу думку, це також виключно пов'язане з тим, що досі державну інформаційну політику в Україні не концептуалізовано.

Тим часом концептуалізація - це важливий процес введення нових уявлень у вже накопичений масив емпіричних даних, що діє. Вочевидь, що це загальнотеоретичний метод використовується практично у всіх науках. Це також і первинна теоретична форма, яка, безумовно, має у випадку з державною інформаційною політикою зазнавати певного коригування модернізації щоразу з урахуванням впливу на її склад сучасних інформаційних, цифрових та інших технологій .

Впровадження інформаційних технологій в сферу публічного управління на початку двохтисячних років викликало появу значної кількості наукових публікацій щодо проблеми державної інформаційної політики. Однак якщо

проаналізувати зміст цих публікацій, то виявляється, що багато вчених зупинялися на констатації факту незавершеної розробленості поняття «державна інформаційна політика», проте часто не пропонуючи свої концептуальні рішення.

Слід також зазначити, що сучасна інформаційна сфера суспільства та особливо розвиток ІКТ та цифрових технологій та їх практичне використання у життєдіяльності людей, публічному управлінні категорично випереджають дослідницькі роботи вчених. Ситуація, що склалася, цілком зрозуміла тим, що у вітчизняній науці практично відсутні дослідницькі роботи, в т.ч. дисертаційні дослідження, з прогнозування інформаційного розвитку держави та суспільства.

В науці зберігається ситуація найрізноманітнішого вживання терміна «державна інформаційна політика». При цьому широко відомо, що правильність і стабільність терміновживання досягається завдяки використанню тих самих понять, а також однакового їх розуміння. Вважаємо, що наука, незважаючи на значні зусилля, зроблені багатьма вченими, не змогла не лише концептуалізувати державну інформаційну політику, а й виробити єдине розуміння змісту державної інформаційної політики загалом [159].

Нові поняття і категорії, що виникають, повинні своєчасно вводитися в науковий обіг політичної науки. Завдяки актуалізації концептуального забезпечення державної інформаційної політики буде забезпечено теоретичну організацію новітнього дослідницького та практичного матеріалу, понять, категорій, що враховують модернізаційні тенденції в інформаційній сфері.

Як показує проведене дисертаційне дослідження, існує нагальна потреба в розробці концепції державної інформаційної політики в сучасних умовах. Мета концептуалізації державної інформаційної політики полягає у визначенні та обґрунтуванні теоретичного підґрунтя для розробки та реалізації інформаційних стратегій держави. Це включає в себе аналіз сучасних тенденцій у сфері інформаційних технологій, визначення ключових принципів та цілей інформаційної політики, а також розробку конкретних інструментів та методів для забезпечення ефективного публічного управління інформаційними

ресурсами держави.

До обґрунтувань необхідності концептуалізації державної політики можна віднести насамперед системне розуміння та уявлення про суспільну проблему, у тому числі пов'язану з розвитком, механізми її вирішення, внаслідок чого знижується ризик помилок управлінського характеру.

На практиці у процесі формування та реалізації державної політики бере участь велика кількість структур і, стикаючись з однією і тією самою проблемою, кожна з них вирішує їх відповідно до своїх тактичних та стратегічних показників. Так, наприклад, відбувалося і в процесі інформаційного розвитку державних органів, доки не було системи електронної взаємодії державних електронних інформаційних ресурсів**,** також системи інтероперабельності в Україні**,** чи просто системи "Трембіти"[14]**.**

Концепція дозволяє задавати політичний курс, ставити єдині цілі та завдання для всіх учасників публічного управління, консолідувати їх потенціал та ефективно використати всі наявні ресурси. Саме концепція державної політики дозволяє інформувати широкі верстви населення, громадськість, бізнес-середовища про декларовані управління, стадії її розробки та реалізації, а також з урахуванням можливостей, які в кінцевому рахунку надають цифрові технології – аналітики Великих даних та можливості доступу, залучати громадян та інститути громадянського суспільства до обговорення та оцінки результатів.

Як зазначають науковці розробка концепції є фундаментом для будь-якого проекту, стратегії чи програми, оскільки це перший крок у створенні чіткого розуміння мети, завдань та методів досягнення успіху[43].

Інша вагома причина полягає в тому, що в Україні відсутній визначений спеціальний закон "Про державну інформаційну політику". Ці дві ключові обставини - відсутність концепції і конкретного законодавства - також суттєво впливають на розвиток досліджень у цій сфері та визначення належного напрямку розв'язання проблематики інформаційної безпеки в країні. Це створює необхідність уваги та досліджень для розробки належних стратегій, концепцій

та законодавчих ініціатив, які б забезпечували ефективне управління інформаційними ресурсами держави та забезпечували належний рівень інформаційної безпеки. Важливо також те, що у побуті публічного управління поняття «державна інформаційна політика» використовується досить активно в останню чверть століття. Це загальне, універсальне позначення публічного управління в інформаційній сфері, яке найбільше «прижилося» у дослідному середовищі. Державна інформаційна політика має планово-програмний характер. У зв'язку з цим її оформлення має бути логічно завершеним. Вона повинна мати теоретичну базу та бути забезпеченою не лише законодавством, а й концептуально.

Наголосимо ще раз, що в Україні поки що немає ні закону, ні концепції державної інформаційної політики. Це дозволяє зробити висновок про необхідність виправлення цього пробілу.

Слід також зазначити, що остання спроба сформулювати державну інформаційну політику у вигляді концепції в 2010 році була зроблена в практичному аспекті. 13 жовтня 2010 року проекту закону «Про Концепцію державної інформаційної політики» № 7251, 11 січня 2011 року проект закону було прийнято у першому читанні, але 5 липня 2011 року його відхилили у другому читанні [135]. На той час вкрай незначною була кількість захищених дисертацій, присвячених даній проблемі. Отже, можна дійти невтішного висновку, що наука не довела до логічного завершення цей процес. Згодом дисертаційні роботи, захищені за останні двадцять років, щоразу пропонували власну інтерпретацію змісту державної інформаційної політики.

Крім того, дослідження, як правило, не завжди враховували тенденцію розвитку самого законодавства, а надалі і роль тих технологій, які кардинально змінили структуру інформаційної діяльності в політиці та публічному управлінні.

Концептуалізація державної інформаційної політики є ключовим елементом в публічному управлінні сучасними державами. Вона має велике значення як науково-теоретична основа, так і з практичної точки зору для

реалізації належного публічного управління.

Подальша розробка концептуально цілісної моделі механізмів реалізації державної інформаційної політики передбачає не лише теоретичне узгодження, а й вдосконалення правового регулятора. Законодавче забезпечення інформаційної політики повинно відповідати сучасним викликам та враховувати розвиток технологій та потреби суспільства у захисті інформації.

Одним із важливих аспектів є необхідність поєднання наукових досліджень з практичним досвідом публічного управління інформаційною сферою. Взаємодія між наукою та практикою допоможе удосконалити розуміння проблем та виявлення ефективних шляхів їх вирішення.

Також важливою є взаємодія інноваційних досліджень з основними положеннями існуючих інформаційних концепцій та норм інформаційного законодавства. Це дозволить розвивати сучасні підходи та стратегії управління інформаційними ресурсами з урахуванням актуальних потреб суспільства та вимог сучасної науки

Практичний підхід, що використовується Державною службою спеціального зв'язку та захисту інформації України, у визначенні напрямів державної інформаційної політики та сфер інформаційної діяльності держави в умовах використання цифрових технологій, не повністю збігається з напрямками досліджень інформаційної сфери у рамках сучасної вітчизняної науки.

Авторська пропозиція полягає в тому, щоб сфери, що є, доповнити сферою побудови інформаційного суспільства шляхом організація онлайн-консультацій та громадських обговорень з питань державної політики та запровадження системи електронного голосування для деяких видів виборів та голосувань.

На регіональному рівні в Україні зараз діє значна кількість "інформаційних" відділів, що часто ускладнює формування єдиної стратегії інформаційної політики на рівні суб'єкта. Ця ситуація є особливо недоцільною в умовах посиленого цифрового розвитку, де потрібна відповідна інформаційна інфраструктура. Однак, на жаль, така інфраструктура на сьогоднішній день

фактично ще не сформована [13].

Отже, стає очевидною необхідність комплексного підходу до цих питань, який має бути спрямований на створення інтегрованої та цільової інформаційної стратегії та інфраструктури на всіх рівнях управління. Цей підхід повинен враховувати не лише поточну ситуацію, але й перспективи розвитку, включаючи технологічні інновації та вимоги глобальних стандартів у сфері інформаційних технологій.

Враховуючи ці аспекти, важливим стає проведення оптимізації наявних регіональних "інформаційних" структур та створення єдиної системи в рамках державних органів влади на рівні регіонів. Ця система буде відповідальною за формування та реалізацію державної інформаційної політики на регіональному рівні, що дозволить забезпечити більш ефективне та координоване використання ресурсів та засобів у цифровій епохі. Регіонам слід здійснити подібну оптимізацію та приведення у відповідність до затверджених програм і стратегій цифрового розвитку України. Це можна зробити на основі узгоджених та єдиною методологією розроблених рекомендацій з урахуванням специфіки кожного регіону та його потреб у цифровому розвитку. Такий підхід дозволить забезпечити узгодженість ініціатив на рівні регіонів та сприятиме ефективному впровадженню цифрових технологій у всіх сферах життя.

Загалом для реалізації ефективної державної інформаційної політики необхідна постановка таких важливих завдань:

- розробка концептуального бачення розвитку держави та суспільства у цифрову епоху;
- інтенсифікація процесів нормативного правового регулювання інформаційних відносин із урахуванням розвитку цифрових технологій;
- створення в Україні ефективної системи взаємодії влади державного рівня з регіональними владою з питань формування інформаційної інфраструктури, зокрема формування та розвитку екосистеми цифрового розвитку;
- розвиток системи підготовки кадрів для роботи в умовах цифрової

економіки, розвиток цифрових компетенцій у державних службовців та населення та ін.

Виходячи зі сказаного, а також на основі проведеного дослідження, вважаємо за можливе стверджувати, що за останні десять-п'ятнадцять років інформаційного розвитку країни сформувалися нові напрями державної інформаційної політики - у галузі побудови інформаційного суспільства та у сфері ІКТ.

Дослідники сконцентрували значну увагу саме на напрямах розвитку інформаційних технологій та інформаційного суспільства. З ростом цифрових технологій, зростанням впливу та значення інформації у політичній сфері та застосуванням аналізу великих обсягів даних у сфері публічного управління стає очевидною необхідність коригування стратегічних напрямів цифрової трансформації на рівнях держави та регіонів.

Сучасний етап інформаційного розвитку в Україні характеризується домінуванням та визначенням державної інформаційної політики такими факторами, як використання великих обсягів даних, їх аналітика та інші передові цифрові технології. Важливою особливістю цього періоду є розгляд інформації у форматі Великих даних та їхнє використання, що відкриває нові можливості для управління та прийняття стратегічних рішень на різних рівнях влади [209]. Таким чином, використання цифрових технологій суттєво трансформує сучасне публічне управління, що відкриває нові можливості та вимагає активної адаптації управлінських підходів та практик. Завдяки цифровим технологіям можливе покращення ефективності управління через автоматизацію процесів, оптимізацію робочих потоків та зменшення бюрократії. Це також сприяє підвищенню прозорості рішень та доступності інформації для громадськості [178]. Цифрові технології створюють унікальні можливості для покращення взаємодії між урядом та громадянами, що є ключовим елементом сучасного публічного управління. Наприклад, вони дозволяють організувати онлайн-консультації, публічні обговорення рішень та збір відгуків від громадян. Ці технології також стимулюють розвиток нових сервісів у сфері публічного

управління, таких як електронні сервіси, відкриті дані (Open Data), електронна демократія тощо.

Ці зміни покликані зробити публічне управління більш доступним та зручним для громадян, а також підвищити рівень довіри до урядових органів та інституцій влади. Адаптація до цифрової епохи у сфері публічного управління є надзвичайно критичною для забезпечення високої якості та ефективності державних послуг. Вона не лише сприяє підвищенню прозорості, відкритості та участі громадян у прийнятті рішень, але й стає важливою складовою успішної модернізації суспільства [152].

У зв'язку з швидким розвитком цифрових технологій та визнанням важливості комплексного підходу до державної інформаційної політики та публічного управління в сфері інформаційної безпеки, наша пропозиція полягає у створенні незалежного Центру Цифрової Безпеки. Цей центр буде спрямований на координацію заходів з підвищення рівня інформаційної безпеки на рівні країни та регіонів.

Центр Цифрової Безпеки має багато переваг і потенціалу, враховуючи сучасні виклики у сфері інформаційної безпеки та необхідності координації та співпраці між різними секторами. Основні моменти, які роблять центр перспективним, включають:

По-перше, незалежність, що забезпечить об'єктивність і прозорість роботи центру.

По-друге, комплексний підхід, що включає координацію, навчання, інновації та швидке реагування.

По-третє, широке коло фінансування, що використовує різноманітні джерела, такі як державні гранти та субсидії ,приватні інвестиції, міжнародні гранти та фонди, доходи від консалтингу та послуг, роблячи центр стійким до змін у фінансуванні.

По-четверте, міжнародна співпраця, яка підвищує рівень обізнаності та впровадження найкращих світових практик.

Цей центр може стати ключовим елементом у системі інформаційної безпеки країни, допомагаючи ефективно реагувати на сучасні виклики цифрового світу та сприяючи розвитку суспільства в цілому. Центр забезпечить не лише ефективність публічного управління інформаційною безпекою, але й сприятиме створенню єдиної стратегії та стандартів щодо інформаційної безпеки. Це дозволить забезпечити високий рівень захисту державних інформаційних ресурсів та інфраструктури в умовах постійно зростаючих загроз цифрового світу.

Основні функції Центру Цифрової Безпеки можуть включати:

1. Моніторинг та аналіз загроз: постійний моніторинг і аналіз загроз для інформаційної безпеки, виявлення нових тенденцій та ризиків.

2. Розробка стратегій та політик: розробка стратегій та політик з питань інформаційної безпеки для держави та регіонів.

3. Координація дій: координація дій між державними органами, регіональними владами, приватним сектором та громадськістю у сфері інформаційної безпеки.

4. Проведення освітніх заходів: організація навчальних програм, тренінгів та курсів з питань кібербезпеки для державних службовців, бізнесу та громадськості.

Створення Центру Цифрової Безпеки (ЦЦБ) може доповнити та посилити роботу Національного Координаційного Центру Кібербезпеки (НКЦК) в Україні[114]. Основні принципи та завдання цих центрів можуть доповнювати один одного, забезпечуючи комплексний підхід до забезпечення цифрової та кібернетичної безпеки в країні.

Центр Цифрової Безпеки може відповідати за розвиток та вдосконалення інфраструктури та політик інформаційної безпеки на рівні країни та регіонів, а також за підготовку та навчання спеціалістів у цих сферах. Основна увага ЦЦБ може бути спрямована на розробку та впровадження стратегій захисту інформації та кібернетичних ресурсів на всіх рівнях публічного управління. НЦЦБ та НКЦК можуть працювати взаємно підтримуючи один одного,

забезпечуючи комплексний підхід до забезпечення кібербезпеки та захисту інформації в Україні на всіх рівнях.

3.3 Підходи до вдосконалення соціально-політичних механізмів публічного управління у сфері інформаційної безпеки держави

В епоху швидкого технологічного розвитку та нестримного зростання інформаційного простору, поняття інформаційної безпеки стає дедалі більш актуальним та складним. Результати розвитку інформаційних технологій відкривають нові горизонти, вносячи значні зміни у спосіб, якими ми збираємо, обробляємо та споживаємо інформацію. Сучасне суспільство, переповнене потоком даних та зв'язків, знаходиться перед викликом забезпечення інформаційної безпеки як важливої передумови для стабільності та розвитку.

Розвиток інформаційних технологій відкриває нові перспективи у сфері формування світової інформаційної моделі, яка в найближчому майбутньому може стати ще більш динамічною, ніж зараз. За останні роки інтенсивність споживання інформації зросла у всіх сферах життя і суспільства: політико-управлінській, соціальній, науково-технічній, технологічній, економічній тощо. Процеси збору, накопичення, переробки та поширення інформації стають ключовими для ефективного функціонування існуючих структур публічного управління, здійснення державно-політичних впливів на суспільство та вирішення масштабних економічних завдань. Однак інформація не лише потужний інструмент розвитку, але й має потенціал для дестабілізації, який може впливати на суспільство і систему публічного управління [21].

Сучасні умови використання інформаційних ресурсів створюють практично необмежені можливості впливу на людину, суспільство та публічне управління. Проте не завжди цей вплив відбувається в інтересах суспільства і держави [23].

Ми вважаємо, що інформаційне суспільство в контексті політико-управлінських відносин повинно втілювати принципи демократії, забезпечуючи громадянам широкі можливості впливу на владу та їх активну участь у формуванні та реалізації державних функцій. Нові технології, зокрема "електронний уряд", грають важливу роль у цьому процесі, сприяючи більш ефективній взаємодії між владою та громадянами.

Проте, на нашу думку, в найближчі роки ефективність публічного управління в сфері інформаційної безпеки держави буде визначатися значним впливом електронних засобів масової інформації та Інтернету. Ці технології стають домінуючими в політичному житті та публічному управлінні.

У зв'язку з швидким розвитком інформаційних технологій у публічно-управлінській сфері та політичному процесі стає дуже актуальною проблема забезпечення інформаційної безпеки. У стратегії інформаційної безпеки України інформаційна безпека розглядається як захист життєво важливих інтересів людини, громадянина, суспільства та держави від ризиків, пов'язаних з розповсюдженням недостовірної інформації, порушенням цілісності та доступності даних, несанкціонованим обігом конфіденційної інформації, а також негативним інформаційно-психологічним впливом та зловживанням інформаційними технологіями. [140].

За основними сферами прояву, системне вираження інформаційної безпеки локалізується в трьох наступних напрямках:

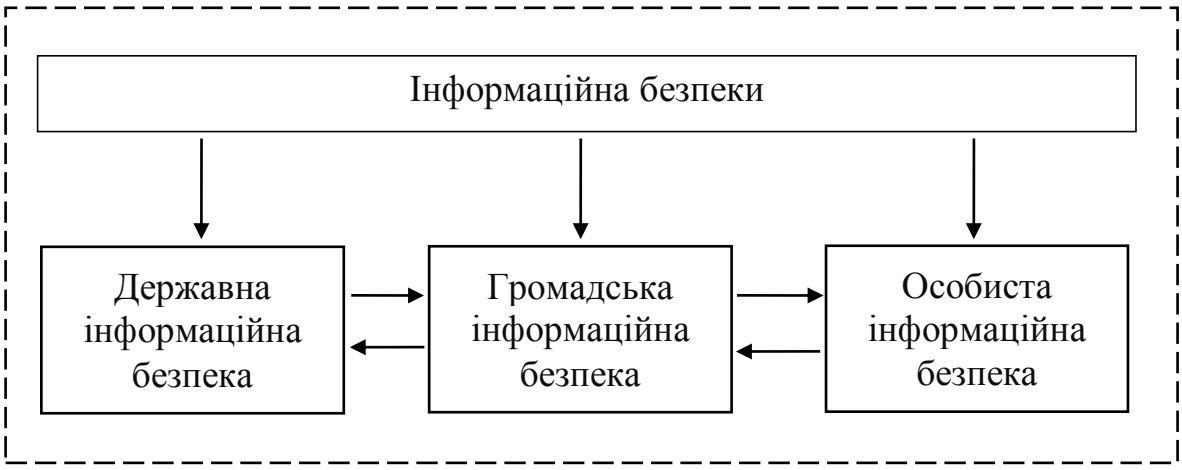

Рис. 2. Системне вираження інформаційної безпеки
Джерело: авторська розробка

1. Державна інформаційна безпека. Цей напрямок охоплює заходи та політики, спрямовані на захист інформаційних ресурсів та систем державних органів від кіберзагроз, зловживань та несанкціонованого доступу. Його мета - запобігти порушенням конфіденційності, цілісності та доступності даних в

управлінських структурах.

2. Громадська інформаційна безпека. Цей аспект стосується захисту громадськості від дезінформації, маніпуляцій та інших загроз інформаційної безпеки. Спрямований на розвиток медійної грамотності та критичного мислення серед громадян для запобігання негативним впливам дезінформації.

3. Особиста інформаційна безпека. Цей напрямок охоплює заходи та практики, спрямовані на захист особистих даних та конфіденційної інформації кожної особи. Включає в себе заходи для запобігання кіберзагрозам та крадіжкам особистої інформації, а також навчання кращому користуванню інтернетом та іншими цифровими сервісами[45].

Отже, в інформаційному суспільстві інформаційна безпека є багаторівневою системою, що охоплює захист інформації на рівні індивіда, суспільства та держави, які тісно взаємопов'язані. Безпека даних цих об'єктів значною мірою залежить від інформаційної безпеки ключових інститутів державно-політичної системи, зокрема системи масових електронних комунікацій.

Соціально-політичний механізм публічного управління у сфері інформаційної безпеки в Україні спрямований насамперед на захист національних інтересів, підтримку демократії та прав людини в інформаційному просторі. Він включає розвиток і впровадження стратегій та політик інформаційної безпеки, створення та підтримку ефективної системи контролю за інформаційними ресурсами, а також сприяння розвитку критичного мислення та медійної грамотності серед населення [38]. Крім того, цей механізм передбачає співпрацю з міжнародними партнерами для обміну досвідом і координації заходів з боротьби з кіберзагрозами та дезінформацією. Координація зусиль державних органів, громадянського суспільства, приватного сектору та міжнародних партнерів, впровадження сучасних технологій інформаційної безпеки, вдосконалення законодавства, розвиток освіти і підвищення обізнаності громадян щодо кібербезпеки та медійної грамотності є ключовими компонентами цього механізму.

Соціально-політичний механізм забезпечення інформаційної безпеки включає різноманітні заходи, спрямовані на підвищення обізнаності громадськості щодо проблем інформаційної безпеки, сприяння розвитку критичного мислення та медійної грамотності серед населення, формування культури безпеки в інформаційному середовищі та залучення громадян до активної участі в цих заходах. Управління процесами формування інформаційної безпеки в суспільстві повинно враховувати реалії комунікаційного ринку, зміст його продуктів, диспропорції між заявленими вимогами та імперативами Доктрини та Стратегії інформаційної безпеки України, а також поточний стан інформаційних ресурсів і якість їхнього продукту. Хоча глобальні та зовнішні джерела інформаційних загроз можуть мати серйозний вплив, у суспільній свідомості вони часто сприймаються як менш значущі, оскільки люди вірять, що державні структури та спеціальні служби зможуть ефективно протистояти цим загрозам. Проте внутрішні джерела інформаційних загроз, які накопичуються на інформаційно-комунікаційному ринку країни, викликають серйозне занепокоєння та потребують уваги [91].

Сучасний інформаційний режим відзначається унікальними можливостями інформаційно-комунікативної технології, які не мають аналогів в історії людства. Ці можливості стали основою для формування всіх глобалізаційних процесів. У свою чергу, глобалізація впливає на різні аспекти суспільної еволюції, зробивши сучасне суспільство проникливим для будь-яких інформаційних впливів та залежним від інформації. Інтеграційні процеси у світі різко посилилися, включаючи політичні та економічні інтеграції, такі як Європейський Союз. Глобальні інформаційні впливи відіграють ключову роль у цьому процесі. Зараз ми спостерігаємо зростання як кількості, так і якості обов'язкових глобальних управлінських рішень, що ставить під сумнів їхню ефективність та оперативність ухвалення. У той же час, традиційна ідентичність націй, конфесій, та національних звичаїв може зазнати впливу і стати менш помітною в контексті розвитку єдиного космополітичного світу. З іншого боку, саме цей процес може спричинити реакцію захисту ідентичності, що призводить

до посилення націоналізму та культурного консерватизму. Тобто, ідентичність буде залишатися важливим фактором, і її вплив не можна недооцінювати [12].

На наш погляд, в умовах сучасного стану спостерігається неготовність держави і суспільства до критичного та аналітичного сприйняття великої кількості інформаційних потоків. Ця неготовність у виокремленні негативних та руйнівних соціальних аспектів може призвести до духовної руйнації, культурної деградації, та моральної деградації нації. Це, в свою чергу, пов'язано з недостатнім розвитком громадянського суспільства в країні, яке ще перебуває на стадії формування.

Управління процесами формування інформаційної безпеки суспільства наразі вимагає дієвих заходів з боку державних інститутів. Одним із можливих шляхів у цьому контексті є регулювання державної інформаційної політики на державному та регіональному рівнях. Такий підхід може сприяти покращенню якості та ефективності публічного управління інформаційною безпекою в суспільстві.

Серед основних напрямів публічного управління інформаційною безпекою суспільства важливе місце займає право громадян та суспільства на доступ до інформації. Це право не лише визначає інформаційну захищеність соціуму в конституційних гарантіях на свободу інформації, але й формує взаємини між владою та суспільством. Однак, насправді право на доступ до інформації, особливо щодо отримання оперативної та повної інформації про актуальні соціальні проблеми, частково обмежується. Існує практика інформування населення про самі соціальні проблеми, але нерідко відсутні конкретні варіанти їх вирішення, що часто має декларативний абстрактний характер та викликає соціальне незадоволення[90].

Також до цього слід віднести практику закритості інформації про понесену відповідальність за непрофесіоналізм, бездіяльність та правопорушення посадових осіб на державному і регіональному рівнях, що особливо викликали широкий резонанс у суспільстві.

Усе це сприяє формуванню у суспільстві стійких негативних уявлень про

існуюче публічне управління, що призводить до втрати довіри до соціальної справедливості в країні та різкого зниження рівня довіри населення до владних структур. Також це підсилює наявні соціальні диспропорції та сприяє соціальній незахищеності. Така ситуація сприяє поширенню в масовій свідомості нігілізму щодо державних інститутів, особливо на регіональному рівні, де закритість інформації значно вища, а право на володіння необхідною інформацією розглядається як опозиційність режиму[100].

Сучасні інформаційні можливості надають кожній особі унікальні засоби для вираження своєї думки та формування громадської думки. Люди, які обмежені у доступі до інформації через традиційні ЗМІ на державному та регіональному рівнях, часто звертаються до Інтернету. Тут вони можуть вільно висловлювати свої погляди, часто у жорсткій та демонстративній формі, і залучати до обговорення значну кількість однодумців. Це сприяє формуванню громадської думки, яка може значно відрізнятися від тієї, що представлена у традиційних медіа[46].

Завдяки Інтернету, який стає платформою для висловлювання реальних ставлень до актуальних соціальних проблем, спостерігається тенденція до зниження довіри до періодичних видань, телебачення та радіо. Люди все більше покладаються на онлайн-ресурси для отримання інформації та обговорення важливих питань. Інтернет стає не лише виразником громадської думки, але й інструментом для її координації та управління, що дозволяє мобілізувати суспільство до дій.

Цей процес можна розглянути з кількох ключових аспектів:

1. Доступність та децентралізація інформації. Інтернет надає доступ до широкого спектру джерел інформації, включаючи незалежні новинні сайти, блоги, соціальні мережі та форуми, що дозволяє отримувати більш об'єктивну та багатогранну картину подій.

2. Вплив на громадську думку. Інтернет надає платформу для вираження альтернативних та менш популярних точок зору, які можуть бути проігноровані традиційними ЗМІ. Інформація, що швидко поширюється через соціальні

мережі, може мати сильний вплив на формування громадської думки та привертання уваги до певних питань.

3. Координація та мобілізація. Соціальні мережі та онлайн-платформи стають інструментами для організації протестів, акцій та інших суспільних рухів, що дозволяє швидко мобілізувати велику кількість людей. Через Інтернет можна координувати дії груп людей, планувати заходи та здійснювати спільні дії в реальному часі.

4. Дезінформація та фейкові новини. Відсутність контролю за достовірністю інформації в Інтернеті може призводити до поширення дезінформації та фейкових новин, що потребує розвитку критичного мислення серед користувачів.

5. Захист особистих даних та конфіденційність інформації стають важливими питаннями в умовах зростання кіберзагроз.

Таким чином, Інтернет відіграє ключову роль у сучасному інформаційному середовищі, надаючи можливості для вираження думок, формування громадської думки та мобілізації суспільства до дій. Це сприяє зростанню активності громадян та створює нові виклики для традиційних медіа та урядів [48]. Публічне управління процесами формування інформаційної безпеки суспільства має включати регулювання доступу населення до інформації через державну інформаційну політику. Для цього необхідно дослідити інформаційні ресурси країни, зокрема на рівні регіонів, та засоби доступу до них. Важливо провести аналіз стану періодичної друкованої преси, доступу до інформаційних радіо- та телепрограм, а також до Інтернету, особливо на регіональному рівні. Крім того, слід розглянути питання якості інформаційного продукту, розповсюдженого серед населення, та провести градацію за різними параметрами, такими як доступність місцевої, регіональної, державної та міжнародної інформації. Також важливо проаналізувати категорії одержувачів інформації, такі як керівні кадри різних рівнів, бізнесмени, громадськість, наукове співтовариство, молодь, школярі та студенти, пенсіонери, щоб з'ясувати ступінь доступності ЗМІ для цих верств населення.

Необхідно активізувати інформаційний діалог між державною та регіональною владою та суспільством [50]. Цей діалог повинен бути постійним, різноманітним і конкретним, уникаючи повчальності та декларативності. Кожен соціальний суб'єкт має отримати можливість в ході цього конструктивного діалогу висловлювати свою позицію, відстоювати свої погляди та спростовувати аргументи опонентів.

Перш за все, важливо забезпечити умови для відкритої та прозорої комунікації між різними рівнями влади та громадянами. Діалог повинен бути інклюзивним, залучаючи представників усіх верств суспільства, включаючи молодь, жінок, національні меншини, професійні спільноти та громадські організації. Це дозволить створити платформу для обміну думками, де кожен учасник зможе внести свій внесок у обговорення нагальних питань.

На додаток, потрібно запровадити регулярні зустрічі, форуми, громадські слухання та інші заходи, де громадяни можуть безпосередньо спілкуватися з представниками влади. Важливо, щоб ці заходи були структурованими та мали чітко визначені теми для обговорення, що дозволить уникнути загальних фраз та спрямувати увагу на конкретні проблеми.

Варто також розглянути можливість створення онлайн-платформ для діалогу, де громадяни можуть залишати свої коментарі, пропозиції та запитання до представників влади. Такі платформи повинні бути зручними у користуванні та доступними для всіх. Не менш важливо забезпечити зворотний зв'язок, щоб громадяни бачили, як їхні пропозиції та зауваження впливають на прийняття рішень. Це допоможе підвищити довіру до влади та стимулюватиме активну участь громадян у суспільному житті.

Потрібно шукати відкриті шляхи до зближення позицій, досягнення компромісу та вирішення обговорюваних проблем, як на регіональному, так і на загальнодержавному рівнях. Для цього важливо навчати державних службовців навичкам ефективної комунікації та ведення діалогу, а також сприяти розвитку громадянського суспільства, що здатне активно впливати на процес прийняття рішень.

Отже, активізація інформаційного діалогу між владою та суспільством є ключовим елементом у побудові ефективної та прозорої системи публічного управління, яка враховує інтереси всіх сторін та сприяє розвитку демократичних процесів у країні. Це вимагатиме прийняття управлінських та організаційних рішень, наявність державної волі, компетентності та уваги до соціальних потреб. Крім обговорення цих потреб, важливо представляти соціуму моделі рішень та безпосередні дії, які переконують громадськість у реальному вирішенні назрілих проблем. Все це сприятиме публічному управлінню процесами формування інформаційної безпеки та збереженню соціальної стабільності [152].

Наступним напрямом управління інформаційними процесами та формуванням інформаційної безпеки суспільства є вивчення типології ЗМІ та їхнього вмісту з огляду на розвиток культурного, духовного життя країни, морально-етичної свідомості та формування традицій патріотизму та гуманізму. Особлива увага має бути приділена інформаційним проектам, спрямованим на популяризацію культури, вітчизняної історії та науки, а також визначенню тенденцій їхнього розвитку як у кількісному, так і в якісному відношенні.

Розвиток масових засобів інформації необхідний для їх ефективного функціонування, і це неможливо без постійного удосконалення інформаційних технологій. Застосування інтерактивного телебачення, яке дає глядачам можливість взаємодії з телевізійним контентом, відкриває нові можливості для покращення ефективності масових медіа. Цей процес сприяє демократизації суспільства, введенню нових стандартів у взаємодії з інформацією та забезпеченню більшої доступності інформації для громадськості. Інформаційні технології дозволяють залучити широкі верстви населення до активної участі в політичному та державному житті, вираженні громадської думки з актуальних питань та забезпеченні громадян необхідною інформацією про діяльність державних органів, політичних партій та громадських організацій.

Використання комп'ютерних моделей у процесі ухвалення публічних управлінських рішень, доповнюючи цілеспрямовану практичну діяльність, може сприяти виявленню альтернативних можливостей та більш

обґрунтованому прийняттю рішень.

Як показав попередній аналіз використання інформаційних технологій для залучення громадськості до публічного управління є платформи електронного урядування (e-government platforms). Це урядові веб-портали, додатки та онлайн-системи, які надають громадянам можливість звертатися за послугами держави, подавати заявки, надавати відгуки та пропозиції, а також брати участь у громадських консультаціях та обговореннях законопроектів. Так, в Швеції існує система "Your Voice", де громадяни можуть висловлювати свої погляди та ідеї щодо різних аспектів державної політики через онлайн-платформу [79]. У Південній Кореї використовується платформа "e-People", яка дозволяє громадянам спілкуватися з урядовцями та висловлювати свої думки щодо різних питань.

Ці платформи дозволяють уряду отримати прямий зворотний зв'язок від громадян та враховувати їхні пропозиції та потреби під час прийняття рішень. Такий підхід сприяє збільшенню відкритості та прозорості публічного управління, а також активізує участь громадян у політичному процесі.

Існують альтернативні погляди на зв'язок між демократизацією та інформатизацією. За думкою Т. Роззака, комп'ютеризація може призвести до підриву демократичних цінностей, оскільки сприяє зміцненню влади політично-управлінської еліти. Це може загрожувати нашій свободі та навіть виживанню [207].

Розвиток та застосування інформаційної техніки у публічому управлінні ставлять перед нами дві ключові проблеми: збереження демократії та контролю за особою. Рівень демократії у суспільстві залежить від обізнаності громадян, але існує ризик, що абсолютна свобода інформації може бути використана для контролю над особистістю за допомогою комп'ютерних технологій, що може обмежити особисту свободу [50].

У такому контексті існує загроза розвитку поліцейського та політичного спостереження за індивідами за допомогою інформаційних технологій. Сучасні технології можуть використовуватися для підслуховування, перехоплення

переписки, перевірки банківських рахунків, моніторингу стану здоров’я, контролю за особистим життям та навіть шантажу. Будь-яка комерційна транзакція, яка включає електронні гроші та комп'ютеризовані угоди, може стати відомою стороннім особам. Інформаційні технології впливають на сучасний державно-політичний процес двома способами. З одного боку, вони позитивно впливають на людину і суспільство, покращуючи взаємодію між владою та громадянами, підвищуючи інформаційну незалежність і розширюючи можливості для участі у політичному процесі. З іншого боку, існують негативні тенденції, пов'язані зі зловживанням технологіями для пропаганди насильства, тероризму та інших небезпечних ідеологій, а також спробами маніпулювати суспільною свідомістю і політичними орієнтаціями.

Нині з’явилися нові інформаційні загрози, спрямовані на дестабілізацію суспільства за допомогою спеціально підібраної інформації. У сфері публічного управління з’являються можливості для маніпуляцій суспільною свідомістю та політичними орієнтаціями різних соціальних груп.Технологічні досягнення, їх широке впровадження і доступність сприяють формуванню нового світогляду. Віртуальна реальність значно трансформує сучасну політичну та управлінську дійсність. Розповсюдження інформаційних технологій у політиці та публічному управлінні має як позитивні, так і негативні наслідки. Вони сприяють ефективнішій взаємодії між владою та громадянами, але також створюють нові загрози і ризики для традиційних демократичних принципів та управлінських процесів, що може призвести до нових бар'єрів і нерівностей у суспільстві. Зважаючи на важливість забезпечення балансу між захистом інформаційної безпеки та збереженням основних прав і свобод громадян, а також необхідність ефективного захисту особистих даних і підвищення обізнаності населення, пропонуємо створення відділу з питань оцінки дотримання приватності в Україні при незалежному Центрі Цифрової Безпеки (ЦЦБ), що може стати важливим кроком у підвищенні рівня захисту особистих даних та забезпеченні приватності громадян. Цей відділ зможе виконувати низку ключових функцій, які сприятимуть підвищенню стандартів інформаційної безпеки.

Рис. 3. Функції діяльності відділу незалежної організації з оцінки дотримання приватності

Джерело: авторська розробка

Перелічені функції сприяють створенню більш захищеної інформаційної системи, підвищенню рівня обізнаності та захисту прав громадян щодо їхніх особистих даних.

1. Проведення навчань та семінарів. Організація та проведення регулярних навчальних заходів, спрямованих на підвищення обізнаності щодо захисту приватності та особистих даних. Цільовою аудиторією можуть бути школярі, студенти, державні службовці, представники приватного сектору та загальне населення.

2. Аналіз технологічних та дослідницьких тенденцій. Постійне вивчення нових технологій та їхнього впливу на приватність. Це включає аналіз новітніх технологічних рішень, які можуть впливати на збір, зберігання та обробку особистих даних.

3. Розробка стандартів та керівництва. Створення і впровадження

нормативних документів та керівництва щодо найкращих практик захисту приватності. Це допоможе організаціям правильно управляти особистими даними та відповідати законодавчим вимогам.

4. Проведення аналізу вразливостей. Виконання аудиту інформаційних систем та процесів для виявлення потенційних вразливостей і ризиків. Це включає тестування на проникнення (penetration testing) та інші методи аналізу безпеки.

5. Підтримка дотримання вимог законодавства. Надання консультацій та допомоги організаціям у виконанні вимог законодавства щодо захисту особистих даних. Це може включати допомогу у впровадженні процедур та політик, необхідних для відповідності законодавству.

6. Проведення досліджень та аналізу практик збирання і використання даних. Дослідження методів збору, зберігання та використання особистих даних різними організаціями з метою визначення етичних та правових аспектів цих практик.

7. Послуги по сертифікації та аудиту. Надання послуг сертифікації для підтвердження відповідності організацій принципам приватності. Це включає проведення регулярних аудитів та видачу сертифікатів відповідності.

8. Створення рекомендацій з політики захисту приватності. Розробка та рекомендація політик та процедур, спрямованих на захист особистих даних у різних сферах діяльності, включаючи освіту, охорону здоров'я, державне управління та бізнес.

9. Взаємодія з громадськістю та засобами масової інформації. Робота з громадськістю та ЗМІ для підвищення обізнаності щодо питань захисту приватності та особистих даних. Це може включати проведення прес-конференцій, публікацію інформаційних матеріалів та співпрацю з журналістами.

Незалежний центр цифрової безпеки може мати механізми контролю та нагляду за її діяльністю, які будуть автономними від парламенту чи інших органів влади. Наприклад, це може бути наглядова рада або комітет експертів,

відповідальний за оцінку діяльності. Важливо ретельно визначити правовий статус та повноваження такого центру у відповідних законах або конституції, щоб запобігти можливим спробам втручання в її роботу. Це може включати процедури призначення членів ЦЦБ, механізми прийняття рішень та засоби захисту незалежності.

Залучення громадськості до процесу контролю та нагляду за діяльністю ЦЦБ також може допомогти зберегти незалежність. Це може бути забезпечено шляхом включення представників громадських організацій, активістів та інших зацікавлених сторін до наглядових або консультативних органів центу.

Висновки до третього розділу

1.Зазначено, що стрімкий розвиток інформаційних та цифрових технологій у сфері державної політики та публічного управління ставить перед дослідницькою спільнотою нові виклики. Наукові уявлення про сутність та зміст сучасної державної інформаційної політики України потребують істотної модернізації та співвіднесення з чинними та реалізованими в державі програмами і стратегіями інформаційно-технологічного та цифрового розвитку. Важливо також завершити концептуалізацію державної інформаційної політики, яка була незавершеною у попередніх дослідженнях у сфері публічного управління. У зв'язку з цим автор дисертаційного дослідження пропонує розробити концептуально цілісну модель політико-адміністративних механізмів реалізації державної інформаційної політики України.

2. Доведено, що для реалізації ефективної державної інформаційної політики необхідна постановка таких важливих завдань:

- розробка концептуального бачення розвитку держави та суспільства у цифрову епоху;
- інтенсифікація процесів нормативного правового регулювання інформаційних відносин із урахуванням розвитку цифрових технологій;
- створення в Україні ефективної системи взаємодії влади державного рівня з регіональними владою з питань формування інформаційної інфраструктури, зокрема формування та розвитку екосистеми цифрового розвитку;
- розвиток системи підготовки кадрів для роботи в умовах цифрової економіки, розвиток цифрових компетенцій у державних службовців та населення та ін.

3. Відзначено, що в Україні доцільно розглянути питання створення незалежного Центру Цифрової Безпеки. Цей центр буде спрямований на координацію заходів з підвищення рівня інформаційної безпеки на рівні країни та регіонів.

Центр Цифрової Безпеки має багато переваг і потенціалу, враховуючи сучасні виклики у сфері інформаційної безпеки та необхідності координації та співпраці між різними секторами. Основні моменти, які роблять центр перспективним, включають:

По-перше, незалежність, що забезпечить об'єктивність і прозорість роботи центру.

По-друге, комплексний підхід, що включає координацію, навчання, інновації та швидке реагування.

По-третє, широке коло фінансування, що використовує різноманітні джерела, такі як державні гранти та субсидії ,приватні інвестиції, міжнародні гранти та фонди, доходи від консалтингу та послуг, роблячи центр стійким до змін у фінансуванні.

По-четверте, міжнародна співпраця, яка підвищує рівень обізнаності та впровадження найкращих світових практик.

ВИСНОВКИ

У дослідженні запропоновано вирішення актуального для науки публічного управління науково-прикладного завдання, яке полягає в обґрунтуванні теоретичних засад та розробки практичних рекомендацій щодо удосконалення публічного управління у сфері інформаційної безпеки держави.

Результати досліджень уможливлюють отримання таких висновків:

1. Визначено місце та роль інформаційної безпеки в системі національної безпеки держави. Інформаційна безпека є однією з ключових складових сучасного суспільства, що почала формуватися як окрема галузь у відповідь на нові загрози, пов'язані з розвитком інформаційних технологій. Якщо раніше питання безпеки стосувалися переважно фізичної безпеки, економічної стабільності та національної оборони, то з розвитком інформаційних технологій, Інтернету та ШІ виникли нові виклики. До таких викликів належать кібератаки, крадіжка даних, порушення конфіденційності та цілісності інформації. Інформаційні процеси стали настільки складними та різноманітними, що їх важко уявити без використання сучасних цифрових технологій. Інформаційна безпека, як окрема галузь, почала формуватися у відповідь на ці нові загрози, що виникли внаслідок розвитку інформаційних технологій.

Інформаційна складова виступає головним комунікатором, який об'єднує всі аспекти загальнонаціональної безпеки в єдине управлінське ціле та є критично важливим компонентом управлінської системи. Ця складова забезпечує координацію та інтеграцію різних елементів національної безпеки, дозволяючи більш ефективно реагувати на виклики сучасного інформаційного середовища.

2. Оцінено стан реалізації публічного управління у сфері інформаційної безпеки, держава активно працює над зміцненням системи публічного управління у сфері інформаційної безпеки, що включає створення відповідної законодавчої бази, розвиток інституційної структури та реалізацію стратегічних ініціатив. Законодавча база включає такі ключові закони, як "Про основні засади забезпечення кібербезпеки України", "Про захист інформації в інформаційно-

телекомунікаційних системах" та інші нормативно-правові акти, що регулюють захист інформації та інформаційної безпеки. Однак, постійний розвиток технологій і кіберзагроз вимагає регулярного оновлення та адаптації законодавства, а також гармонізації з міжнародними стандартами та нормами. Інституційна структура України у сфері інформаційної безпеки включає кілька ключових органів, таких як ДССЗЗІ, Національний координаційний центр кібербезпеки при РНБО, Міністерство цифрової трансформації та СБУ. Відсутність чіткої координації між різними органами влади та інституціями, а також недостатній рівень взаємодії між державним та приватним секторами є викликами, які потребують вирішення. Недостатній рівень інвестицій у новітні технології та інфраструктуру, а також потреба у висококваліфікованих кадрах стримують розвиток цієї сфери. Збільшення бюджетних асигнувань, створення стимулів для приватного сектора інвестувати у кібербезпеку та впровадження програм для підготовки кадрів є необхідними для забезпечення належного рівня ресурсів. Постійне зростання та еволюція загроз вимагає швидкої адаптації та впровадження нових заходів захисту. Регулярне проведення національних та міжнародних навчань, впровадження передових технологій для моніторингу та реагування на кіберзагрози, а також створення аналітичних центрів для дослідження нових загроз є важливими кроками для підвищення ефективності системи безпеки. Отже, публічне управління у сфері інформаційної безпеки в Україні потребує комплексного підходу, що включає постійне оновлення законодавчої бази, ефективну координацію між інституціями, належне фінансування та підготовку кадрів. Тільки за умови адаптації до нових викликів та загроз, забезпечення належного рівня ресурсів та активної міжнародної співпраці Україна зможе досягти високого рівня безпеки.

3. Проаналізовано сучасний стан функціонування механізмів публічного управління в сфері інформаційної безпеки держави. Доведено, що нормативне та правове регулювання нових відносин у сфері інформації є недостатнім, особливо у зв'язку з широким використанням цифрових технологій у публічному управлінні. Обґрунтовано, що сьогодні слід визнати і ряд суттєвих

проблем та викликів, які потребують негайного вирішення:

- діюче законодавство часто не встигає адаптуватися до швидких технологічних змін та нових загроз в інформаційному просторі. Закони та нормативні акти потребують оновлення та уточнення, щоб відповідати сучасним стандартам безпеки та враховувати нові види кіберзагроз;

- відсутність єдиної координаційної структури, яка б централізовано управляла та регулювала діяльність у сфері інформаційної безпеки, призводить до фрагментованості та неузгодженості дій різних державних органів;

- недостатня кількість фахівців у сфері кібербезпеки та інформаційної безпеки, а також низький рівень їх підготовки та обізнаності про сучасні загрози. Необхідно розробити та впровадити системи підготовки та перепідготовки кадрів у цій галузі;

- громадяни недостатньо поінформовані про способи захисту своїх персональних даних та засоби протидії інформаційним загрозам, що робить їх вразливими до атак;

- відсутність достатнього фінансування та сучасного технічного оснащення для забезпечення належного рівня кібербезпеки в державних структурах.

4. Систематизовано закордонний досвід розробки та впровадження інформаційного забезпечення державної безпеки. Інформаційна безпека є критично важливою складовою національної безпеки будь-якої країни. Для ефективного захисту інформаційних ресурсів та забезпечення державної безпеки багато країн використовують міжнародні стандарти та фреймворки. Серед них найбільш відомі: ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27000, COBIT, ITIL та NIST SP 800-53. Ці стандарти та фреймворки є ефективними інструментами для розробки та впровадження інформаційного забезпечення державної безпеки. Їх застосування сприяє захисту інформаційних ресурсів, підвищенню рівня національної безпеки та зміцненню довіри до державних і приватних організацій. Фахівці у сфері інформаційної безпеки повинні вміти обирати найкращі практики з усіх цих стандартів та інтегрувати їх у систему

ефективного управління безпекою інформації. Проте, через велику кількість стандартів державного регулювання в галузі інформаційної безпеки, необхідно мати значний арсенал знань для вибору найбільш відповідних. Використання цих стандартів потребує створення карт сфер їх застосування та взаємозв'язків між ними. Це може призвести до необхідності розробки метастандарту – надстандарту, який би визначав загальні принципи для інших стандартів. Наразі, такого метастандарту ще не існує [178].

5. Використання цифрових технологій у публічному управлінні стало ключовим напрямом модернізації інформаційної безпеки держави. Курс на цифровізацію України було закріплено розпорядженням Кабінету Міністрів України «Про схвалення Концепції розвитку електронного урядування в Україні» 2017 року. Основною метою цієї Концепції є визначення напрямків, механізмів та термінів створення ефективної системи електронного урядування в Україні. Це має задовольнити потреби фізичних та юридичних осіб, покращити систему публічного управління, підвищити конкурентоспроможність країни та прискорити її соціально-економічний розвиток. Нижче наведено основні напрями, як цифрові технології сприяють модернізації інформаційної безпеки у публічному управлінні:

– електронний уряд (E-Government), впровадження електронного уряду дозволяє забезпечити ефективне управління державними ресурсами та послугами через цифрові платформи;

– цифрова інфраструктура та кібербезпека Використання технологій машинного навчання та штучного інтелекту для виявлення та реагування на кіберзагрози в режимі реального часу, застосування криптографічних методів для захисту конфіденційних даних під час їх передачі та зберігання та програми підвищення обізнаності державних службовців щодо загроз кібербезпеки та методів їх запобігання відіграють вирішальну роль у захисті державних інформаційних систем від кіберзагроз;

– впровадження електронних ідентифікаційних систем, таких як електронні паспорти та цифрові підписи забезпечує автентифікацію

користувачів та підтвердження достовірності документів та полегшує доступ до державних сервісів, зменшуючи ризики пов'язані з використанням багатьох паролів;

– аналітика великих даних (Big Data Analytics), через збір та аналіз великих обсягів даних для покращення управлінських рішень;

- хмарні обчислення забезпечують гнучкість та масштабованість державних інформаційних систем через надання безпечних середовищ для зберігання та обробки великих обсягів даних та забезпечення безперервності роботи за рахунок резервних копій даних у хмарі.

- впровадження розумних систем управління міськими ресурсами (освітлення, транспорт, енергоспоживання) та використання сенсорів для моніторингу стану інфраструктурних об'єктів (мости, дамби, енергомережі).

- блокчейн-технології забезпечують прозорість та безпеку транзакцій та ведення реєстрів власності та прав користування з мінімізацією ризиків підробки даних.

Цифрові технології відіграють вирішальну роль у модернізації інформаційної безпеки держави, забезпечуючи як ефективне управління, так і захист інформаційних систем від сучасних загроз. Інвестиції у розвиток цифрових інфраструктур та кібербезпеки є необхідними для стійкого та безпечного функціонування публічного управління.

6. Запропоновано підходи до вдосконалення соціально-політичного та організаційно-правового механізмів публічного управління:

- концептуальні засади. Розробка й ухвалення Концепції державної інформаційної політики України, яка визначає стратегічні напрями розвитку інформаційної безпеки, захисту персональних даних, розвитку електронного уряду та інших аспектів;

- регулювання державної інформаційної політики. Пропонується регулювання державної інформаційної політики на різних рівнях, що сприятиме покращенню якості та ефективності публічного управління інформаційною безпекою в суспільстві;

- забезпечення права громадян на доступ до інформації. Висвітлено важливість цього права як конституційної гарантії на свободу інформації, що формує взаємини між владою та суспільством;

- міжвідомча координація. Забезпечення ефективного обміну інформацією та координації дій між різними відомствами і органами влади щодо захисту інформації, реагування на кіберзагрози та інші аспекти інформаційної безпеки;

- координація дій між різними суб'єктами: Зазначено про важливість координації зусиль державних органів, громадянського суспільства, приватного сектору та міжнародних партнерів для ефективної боротьби з кіберзагрозами та дезінформацією;

- розвиток освіти та підвищення обізнаності громадян: Зокрема, акцентується на необхідності формування критичного мислення та медійної грамотності серед населення для зменшення негативного впливу дезінформації та маніпуляцій;

- підвищення якості інформаційних ресурсів: Зокрема, в контексті медійних продуктів і продуктів комунікаційного ринку, щоб забезпечити високу якість інформації та зменшити диспропорції між імперативами і дійсністю.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Авер'янова Н.М. Гібридна війна: російсько-українське протистояння. *Молодий вчений*, 2017. №3 (43). С. 30-34.

2. Арсенович Л. А. Організація професійної підготовки фахівців із кібербезпеки основними суб'єктами національної системи кібербезпеки: практичний аспект. *Ефективність державного управління : зб. наук. пр.* 2020. Вип. 1 (62). С. 91–105. URL: https://doi.org/10.33990/2070-4011.62.2020.205817 (дата звернення: 13.02.2024).

3. Бабіч О. Особливості маніпуляції масовою свідомістю в друкованих ЗМІ під час висвітлення воєнних подій. *Вісник Київського національного університету імені Тараса Шевченка: військово-спеціальні науки*. 2007. Вип. 14 – 15, С. 89–93

4. Бєлоусова Н. Б. Основні вимоги НАТО щодо забезпечення безпеки в інформаційного простору. *Актуальні проблеми міжнародних відносин*. 2011. Вип. 102. Ч. І., С.196−202.

5. Бєляков К. І. Організаційно-правові проблеми формування державної інформаційної політики України. *Право України*. 2004. № 10. С. 16–19.

6. Бєляков К. І. Інформаційна діяльність: зміст та підходи до класифікації *Інформація і право*. 2012. № 1. С. 63−96.

7. Биркович Т.І., Биркович В.І., Кабанець О.С. Механізми публічного управління у сфері цифрових трансформацій. *Державне управління: удосконалення та розвиток.* 2019 №9. URL:http://www.dy.nayka.com.ua/?op=1&z=1488 (дата звернення: 13.02.2023).

8. Буравльов Є. Науково-технічна безпека України в контексті глобалізації. *Вісник НАН України.* 2005. № 3. С. 32–40.

9. Бухтатій О. Є. Реформування інформаційної сфери України :політичні та адміністративні аспекти. *Держава та регіони: зб. наук. пр*. – Запоріжжя: Класичний приватний університет. 2010. № 2. С. 24-28

10. Велігура А. В. Дослідження шляхів розробки комплексів інформаційної безпеки. *Вісник Східноукраїнського національного університету імені В. Даля*. 2009. № 6(136). Ч. 1 С. 154–161.

11. Власюк О. С. Національна безпека України: еволюція проблем внутрішньої політики. Київ : НІСД, 2016. 528 с.

12. Воропаєва Т.С. Національна ідентичність громадян України у контексті інформаційної безпеки. *Людинознавчі студії: Збірник наукових праць.* Дрогобич. 2009. Т. 20. С. 16-35.

13. Воротін В. Є. Державне управління регіональним розвитком України : монографія. Київ : Вид-во НІСД, 2010. 288 с.

14. В Україні розпочато впровадження «Трембіти»: налагоджено автоматичний обмін даними між держустановами. *Урядовий портал*. URL: https://www.kmu.gov.ua/news/v-ukrayini-rozpochato-vprovadzhennya-trembiti-nalagodzheno-avtomatichnij-obmin-danimi-mizh-derzhustanovami (дата звернення: 30.05.2023).

15. Гавриляк В. Б. Стратегія кібербезпеки ЄС (2021) на цифрове десятиліття: перспективи для України. *Вісник Національної академії державного управління при Президентові України. Сер. «Державне управління»*. 2021. № 1 (100). С. 46–52.

16. Гаєвський Б. А., Ребкало В.А., Туленков М.В. Політичне управління : навч. посіб. Київ: УАДУ, 2001. С.160.

17. Гладиш С. В. Формування вимог щодо безпеки державних інформаційних ресурсів в телекомунікаційній мережі загального користування. *Науково-технічний збірник «Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні»*, вип. 1 (14), 2007. С. 33-40

18. Голобородько Т.В. Використання інформаційних технологій в публічному адмініструванні: досвід України та європейські орієнтири. *Електронний журнал «Державне управління: удосконалення та розвиток»* №6. 2018. URL: http://www.dy.nayka.com.ua/pdf/6_2018/39.pdf (дата звернення: 13.11.2023).

19. Головне про українську ІТ-галузь у 2021 році: деталі дослідження IT Ukraine URL: https://speka.media/investiciyi/golovne-pro-ukrayinsku-it-galuz-v-2021-roci-detali-doslidzennya-it-ukraine-jv4xk9 (дата звернення: 13.11.2023).

20. Горбулін В. П. Стратегічне планування : вирішення проблем національної безпеки : монографія. Київ : НІСД, 2010. 288 с.

21. Горбулін В. П., Додонов О.Г.,Ланде Д. В Інформаційні операції та безпека суспільства: загрози, протидія, моделювання : монографія Київ: Інтертехнологія, 2009. 164 с.

22. Гуз А. М. Історія захисту інформації в Україні та провідних країнах світу : навч. посіб. Київ : КНТ, 2011. 260 с.

23. Гурковський В. І. Безпека як об’єкт правовідносин в умовах глобального інформаційного суспільства. Правова інформатика. 2010. № 2(26). С. 72−77.

24. Данільян О. Г., Дзьобань О.П., Панов М.І Національна безпека України: сутність, структура та напрями реалізації. Харків : Фоліо, 2010. 296 с.

25. Дереко В. Н. Теоретико-методологічні засади класифікації загроз об’єктам інформаційної безпеки. *Інформаційна безпека людини, суспільства, держави.* 2015. № 2 (18). с. 16−22.

26. Державна політика: аналіз та механізм її впровадження в Україні : навч. посіб. / кол. авт. ; за заг. ред. В. А. Ребкала, В. В. Тертички. Київ : УАДУ, 2000. – 232 с.

27. Державне регулювання економіки : навч. посіб. / С. М. Чистов, А. Є. Никифоров, Т. Ф. Куценко. Київ : КНЕУ, 2005. 440 с.

28. Державне управління : навч. посіб. / А. Ф. Мельник, О. Ю. Оболенський, А. Ю. Васіна ; за заг. ред. А. Ф. Мельник. Київ : Знання, 2009. 582 с.

29. Державне управління : словник-довідник / заг. ред. В. М. Князєв, В. Д. Бакуменко. Київ : Видавництво УАДУ, 2002. 228 с.

30. Державне управління в Україні : навч. посіб. / за заг. ред. В. Б. Авер’янова. Київ : Юрінком Інтер, 1998. 432 с.

31. Державне управління в Україні: наукові, правові, кадрові та організаційні засади : навч. посіб. / за заг. ред. Н. Р. Нижника, В. М. Олуйка. Львів : Вид-во Національного університету «Львівська політехніка», 2002. 352 с.

32. Деякі питання об'єктів критичної інформаційної інфраструктури : постанова Кабінету Міністрів України від 09.10.2020 № 943. URL: https://zakon.rada.gov.ua/laws/show/943-2020-%D0%BF#Text (дата звернення: 09.02.2024).

33. Дітковська М. Ю. Впровадження новітніх інформаційних технологій в органах державної влади та місцевого самоврядування. *Теорія та практика державного управління.* 2008. № 3. С. 147-151.

34. Дія: Державні послуги онлайн URL:https://diia.gov.ua/ (дата звернення: 09.04.2024).

35. Довгань О. Д. Національний інформаційний суверенітет – об'єкт інформаційної безпеки. *Інформація і право*. 2012. № 3(12). С.102−112.

36. Довгань О. Д. Сучасні інформаційні структури як компоненти інформаційної безпеки. *Інформація і право.* 2015. № 2(14). С. 111−120.

37. Довгань О.Д. Теоретико-правові основи забезпечення інформаційної безпеки України: дис. д-ра юрид. наук. Київ, 2016. 453 с.

38. Домбровська С. М. Механізми забезпечення інформаційної безпеки як складової державної безпеки України. *Теорія та практика державного управління*. 2015. Вип. 1 (48). с. 2−4.

39. Домбровська С. М., Коленко В. В. Державна політика з забезпечення безпеки інформаційного середовища. *Вісник Національного університету цивільного захисту України. Сер. «Державне управління» : зб. наук. пр.* Харків : НУЦЗУ, 2021. Вип. 1 (14). С. 3–10. URL: http://repositsc.nuczu.edu.ua/handle/123456789/13256(дата звернення: 20.05.2023).

40. Древаль Ю. Д. Безпека особистості як чинник сучасних державно-управлінських відносин. *Наукові записки до Інституту законодавства Верховної Ради України.* 2015. № 1. с. 123-126. URL:

http://nbuv.gov.ua/UJRN/Nzizvru_2015_1_28 (дата звернення: 09.03.2023).

41. Дубас О. П. Інформаційний розвиток сучасної України у світовому контексті : монографія. Київ : Генеза, 2011. 208 с.

42. Електронне урядування та електронна демократія. URL: https://pdp.nacs.gov.ua/courses/elektronne-uriaduvannia-ta-elektronna-demokratiia-52

43. Енциклопедія сучасної України URL: https://esu.com.ua/article-3256 (дата звернення: 30.11.2023).

44. Єдину інформсистему соціальної сфери відкрито для всіх держорганів. Мінсоцполітики URL: https://interfax.com.ua/news/general/944456.html (дата звернення: 30.09.2023).

45. Жарков Я. М. Інформаційна безпека особистості, суспільства, держави : підручник. Київ: Видавничо-поліграфічний цента «Київський університет», 2008. 256 с.

46. Жарков Я.М. Інформаційно-психологічне протиборство в сучасному світі: проблемно-історичний аналіз. *Вісник Київського національного університету імені Тараса Шевченка.* 2007. 14–15. С. 101–104.

47. Жиляєв І. Б., Семенченко О. І Сучасна державна політика розвитку цифрових навичок публічних службовців та громадян України. *Теорія та практика державного управління*. 2020 №1(68) С. 198-209.

48. Журавльов А. В. Інтернет-спільноти у новій хвилі інформаційних війн . URL:http://www.vidkryti-ochi.org.ua/2009/01/blog-post.html.

49. Захаренко К. В. Категорія інформаційної безпеки у вітчизняному філософсько-політологічному дискурсі. *Гуманітарний вісник ЗДІА*. 2018. Вип. 72. С. 44−52.

50. Золотар О.О. Правові основи інформаційної безпеки людини: дис. д-ра юрид. наук. Київ, 2018. 499 с.

51. Іляш О. І. Трансформації системи соціальної безпеки України: регіональний вимір : монографія. Львів : Львівська комерційна академія, 2012. 592 с.

52. Інформаційна безпека (соціально-правові аспекти) : підручник В. Остроухов та ін. Київ : КНТ, 2010.776 с.

53. Інформаційна безпека України : глосарій / за загальною редакцією доктора юридичних наук, професора Р. А. Калюжного. Київ: Текст, 2011. 180 с.

54. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / В. Л. Бурячок та ін. Київ: ДУТ, 2015. 288 с.

55. Інформаційне законодавство України. *Науково-практичний коментар*. Київ: Юридична думка, 2009. 241 с.

56. Інформаційно-комунікативна діяльність органів публічної влади : монографія / Куйбіда В.С. Київ : ЦП «Компринт», 2018. 364 с.

57. Каращук М. Г. Інформаційна влада в системі сучасних владних відносин. *Політологічний вісник.* Вип. 20. К. : ТОВ «XXI століття: діалог культур», 2005. С. 226–234

58. Карпенко О. В. Механізми формування та реалізації сервісно-орієнтованої державної політики в Україні : автореф. дис. … д-ра н. з держ. упр. спец. : 25.00.02. Нац. акад. держ. упр. при Президентові України. Київ, 2016. С. 37.

59. Карпенко О.В., С. О. Шайхет С.О. Застосування поняття «безпека» в галузі державного управління: етимологія та сучасне тлумачення. *Науковий вісник Академії муніципального управління*., 2016. Вип. 3. С. 26-35. – (Серія «Управління»). URL: http://academy.gov.ua/infpol/pages/dop/2/files/9f7f3c6b-004c-4403-848e-1410645127d4.pdf (дата звернення: 27.10.2023).

60. Качинський А. Б. Індикатори національної безпеки: визначення та застосування їх граничних значень : монографія. Київ : НІСД, 2013.101 с.

61. Колодій І. Поняття та зміст інформації: соціальні та правові аспекти. *Підприємство, господарство і право.* 2007. № 1. С.83-86.

62. Конах В. К. Нормативно-правові засади державної політики України у сфері інформаційно-психологічної безпеки. *Стратегічні пріоритети.* 2012. № 3 (24). С. 152−157.

63. Концептуальні засади взаємодії політики й управління : навч. посіб. / Е. А. Афонін та ін. Київ: НАДУ, 2010. 299 с.

64. Концепція розвитку електронного урядування в Україні : схвалено розпорядженням Кабінету Міністрів України від 20.09.2017 № 649-р. URL: https://zakon.rada.gov.ua/laws/show/649-2017-%D1%80#Text (дата звернення: 13.11.2022). .

65. Концепція формування системи національних електронних інформаційних ресурсів : затверджено Розпорядженням Кабінету Міністрів України від 05.05.2003 № 259-р. URL: https://zakon.rada.gov.ua/laws/show/259-2003-%D1%80 (дата звернення: 01.12.2023).

66. Кормич Б. А. Організаційно-правові засади політики інформаційної безпеки України : монографія. Одеса : Юридична література, 2007. 471 с.

67. Корнейко О. Застосування та визначення терміна «інформаційна безпека» в національному законодавстві. *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні*. Науково-технічний збірник. 2009. Вип. 2(19). С. 9−13.

68. Котух Є. В. Формування систем кібербезпеки в органах публічної влади. *Державне управління: удосконалення та розвиток.* № 3 (2020). URL: http://www.dy.nayka.com.ua/?op=1&z=1596 (дата звернення: 16.03.2023).

69. Кохановська О. В. Правове регулювання у сфері інформаційних відносин : монографія . Київ: Націон. акад. внутр. справ України, 2010. 212 с.

70. Кравченко М. С, Кєтриш О. С. Управління інформаційними ресурсами як інструмент управляння соціальними та економічними процесами в Україні. URL: http://ves.pstu.edu/article/viewFile/105569/100702 (дата звернення: 01.11.2023).

71. Криштанович М. Ф. Реалізація механізмів публічного управління у сфері цивільного захисту України щодо національної безпеки. *Вісник Національного університету цивільного захисту України.* Серія. Державне управління. 2017. Вип. 1 (6).С. 341–347.

72. Крюков О. І. Інформаційне забезпечення публічної влади як чинник національної безпеки держави в умовах глобалізації. *Вісник Національного університету цивільного захисту* : зб. наук. праць. Серія: Державне управління. Харків, 2016. № 1 (4). С. 142–149.

73. Куйбіда В. С., Карпенко О. В., Наместнік В. В. Цифрове врядування в Україні: базові дефініції понятійно-категоріального апарату. *Вісник Національної академії державного управління при Президентові України. Сер. «Державне управління»*. 2018. № 1. С. 5-11.

74. Курас І. Інтеграція інформаційних ресурсів – стратегічний напрям забезпечення інформаційних потреб суспільства. *Бібліотечний вісник*. 2009. №1. С. 2−6.

75. Курбан О. В. PR-аспекти інформаційної безпеки організаційних структур. *Вісник книжкової палати.* 2014. №5. С. 48– 51.

76. Курбан О.В. Соціальні мережеві комунікаційні технології в структурі сучасних інформаційних потоків. *Україна в системі глобального інформаційного обміну: теоретико-методологічні аспекти дослідження і підготовки фахівців. Матеріали ІІ Всеукраїнської наукової конференції*. Львів: Лігі-Прес, 2013. С.137–143.

77. Курило А.Г. Міжнародно-правові стандарти забезпечення права особи на інформаційну безпеку. *Вісник Національного університету цивільного захисту України.* Серія: Державне управління. 2022. № 2 (15). С. 17-124 URL:http://repositsc.nuczu.edu.ua/bitstream/123456789/14591/1/Kurilo.pdf (дата звернення: (22.04.2024).

78. Курило А.Г. Місце інформаційної безпеки в системі національної безпеки. *Вісник Національного університету цивільного захисту України*. Серія: Державне управління. 2022. № 1 (14). URL:http://repositsc.nuczu.edu.ua/bitstream/123456789/13266/1/Kurilo.pdf (дата звернення: (24.04.2024).

79. Куюмджиєва А. Міжнародна практика заходів, спрямованих на зміцнення довіри між державою та організаціями громадянського суспільства.

URL: https://www.osce.org/files/f/documents/9/c/75885.pdf (дата звернення: 30.01.2024).

80. Ленков С. В. Захист національних інформаційних ресурсів в аспекті інформаційної безпеки України. Вісн. Східноукр. нац. ун-ту ім. В. Даля. 2009. Т. 1. № 5. С. 21−28.

81. Лисенко В. Чутки - активний засіб модифікації суспільної свідомості. *Політичний менеджмент*. 2004.№ 6. С. 96–102.

82. Ліпкан В .А. Національна і міжнародна безпека у визначеннях та поняттях / В. А. Ліпкан, О. С. Ліпкан, О. О. Яковенко. Київ: Текст, 2011. – 256 с.

83. Ліпкан В. А. Національна безпека України : навч. посіб. / В. А. Ліпкан. Київ : КНТ, 2009. 574 с.

84. Луценко С. М. Особливості інформаційного забезпечення в державно-управлінській діяльності. *Держава та регіони : зб. наук. праць*. Запоріжжя: Класичний приватний університет, 2010. № 2. С. 41–45.

85. Макаренко Є. А. Європейська інформаційна політика : монографія. Київ : Наша культура і наука, 2010. 368 с.

86. Малик Я., . Малик, О. Береза, М. Криштанович. Національна безпека : навч. посіб. Львів. регіон. ін-т держ. упр. Нац. акад. держ. упр. при Президентові України. Львів : ЛРІДУ НАДУ, 2010. 280 с.

87. Маращук А. І. Інформаційні ресурси держави: зміст та проблеми захисту. URL: http://www.ndcpi.org.ua. (дата звернення: 24.04.2022).

88. Маріц Д.О. Право на анонімність як невід’ємне право людини. *Підприємництво, господарство і право.* 2018. № 2. С. 160–164. URL: http://www.pgp-journal.kiev.ua/archive/2018/2/30.pdf (дата звернення: 23.03.2024).

89. Маруненко О. Зовнішні і внутрішні інформаційні війни у медійному просторі України Освіта регіону. *Політологія, психологія, комунікації. Український науковий журнал.* 2011. № 4. с. 92.

90. Марущак А. І. Інформаційне право: регулювання інформаційної діяльності : навч. Посібник. Київ: Видавничий дім «Скіф», КНТ, 2010. 344 с.

91. Медвідь Ф. Інформаційна безпека України: виклики та загрози. URL: http://www.ndcpi.org.ua. (дата звернення: 24.04.2022).

92. Мельник Д. С. Щодо сучасних загроз національній безпеці України в інформаційній сфері. *Актуальні проблеми управління інформаційною безпекою держави :* зб. тез наук. доп. наук.-практ. конф. (Київ, 26 бер. 2021 р.). Київ : НА СБУ, 2021. С. 68–71. URL: http://academy.ssu.gov.ua/upload/file/конференція%2026.03.2021.pdf (дата звернення: 30.11.2021).

93. Мікуліна М. М. Гарантування персональних даних у глобалізованому сьогоденні. *Актуальні проблеми управління інформаційною безпекою держави :* зб. тез наук. доп. наук.-практ. конф. (Київ, 4 квіт. 2019 р.). Київ : Нац. акад. СБУ, 2019. С. 94–95. URL: https://academy.ssu.gov.ua/uploads/p_57_54325835.pdf (дата звернення: 23.09.2023).

94. Михайло Федоров: До 2024 року 90% українців будуть користуватися онлайн-послугами та іншими цифровими продуктами URL: https://thedigital.gov.ua/news/mihajlo-fedorov-do-2024-roku-90-ukrayinciv-budut-koristuvatisya-onlajn-poslugami-ta-inshimi-cifrovimi-produktami (дата звернення: 23.097.2022).

95. Момот А. Аналіз основних напрямків забезпечення інформаційної безпеки. *Актуальні проблеми міжнародних відносин*. Вип. 659 (Ч.1). №1. 2008 С. 265−278.

96. Національна стратегія доходів до 2030 року. *Міністерство фінансів України.* URL: https://mof.gov.ua/storage/files/National%20Revenue%20Strategy_2030_.pdf (дата звернення: 30.05.2024).

97. Нестеренко О. В. Єдина державна система електронних інформаційних ресурсів. *Науково-технічна інформація*. 2006. № 4. С. 3−9.

98. Ожеван М. А. Основні напрями зовнішніх інформаційно-маніпулятивних впливів на суспільні трансформації в Україні: засоби протидії. *Стратегічні пріоритети*. 2011. № 3. С. 118–126.

99. Олійник О. В. Державна політика інформаційної безпеки України. *Юридичний вісник*. 2012. №4(25). С.65−69.

100. Олійник О. В. Політико-правові аспекти формування інформаційного суспільства суверенної і незалежної держави. *Держава і право*. 2001. Вип. 13. С. 34–41.

101. Основи інформаційного права України : навч. посіб / В. С. Цимбалюк та ін. Київ . Знання, 2010. 274 с.

102. Основи інформаційної безпеки / за ред. проф. В. О. Хорошка. Київ : ДУІКТ, 2008. 186 с.

103. Осьмак А. Методологічні засади класифікації інструментів цифрових систем «smart city». *Теоретичні та прикладні питання державотворення* : електрон. наук. фах. вид. Одес. регіон. ін-ту держ. упр. Одеса : ОРІДУ НАДУ. 2019. Вип. 24. С. 9-15. URL: http://www.oridu.odessa.ua/9/buk/%D0%95-24.pdf (дата звернення: 30.09.2020).

104. Партико З. В. Теорія масової інформації та комунікації. Львів : Афіша, 2008. 290 с.

105. Пархоменко В. Д. Наукові і організаційні проблеми управління інформаційними ресурсами. *Науково-технічна інформація.* 2007. № 3. С. 31−36.

106. Петров С. Г. Правові основи взаємодії державних органів та приватних суб'єктів із метою захисту електронних інформаційних ресурсів України. *Інформація і право.* № 4(31)/2019. С. 107-112. URL: http://ippi.org.ua/sites/default/files/15_11.pdf (дата звернення: 01.12.2020)

107. Пилипчук В. Г. Еволюція наукових поглядів стосовно поняття «державна безпека». *Стратегічна панорама.* 2006. № 2. С.17−21.

108. Пирожков С. І. Національна та регіональна безпека: погляд України. *Нова безпека*. 2003. №2. С. 9–16.

109. Питання забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах: затверджено постановою Кабінету Міністрів України від 08.02.2021 № 92. URL: https://zakon.rada.gov.ua/laws/show/92-2021-%D0%BF#Text (дата звернення:

03.04.2021).

110. Питання Міністерства цифрової трансформації : постанова Кабінету Міністрів України від 18.09.2019 № 856. URL: https://zakon.rada.gov.ua/laws/show/856-2019-%D0%BF#Text (дата звернення: 22.05.2021).

111. Платоненко А. В. Сучасні загрози інформаційної безпеки для державних та приватних установ України. *Сучасний захист інформації*. 2015. №4. С. 86−90.

112. Політанський В. С. Інформаційне суспільство в Україні: від зародження до сьогодення. *Науковий вісник Ужгородського національного університету*. 2017. Вип. 42. С. 16−22.

113. Положення про Адміністрацію Державної служби спеціального зв'язку та захисту інформації України» : затверджено постановою Кабінету Міністрів від 03.09.2014 № 411. URL: https://zakon.rada.gov.ua/laws/show/411-2014-%D0%BF#n8 (дата звернення: 22.05.2021).

114. Положення про Національний координаційний центр кібербезпеки : затверджено Указом Президента України від 07.06.2016 № 242/2016. URL: https://zakon.rada.gov.ua/laws/show/242/2016/ed20200130#n9 (дата звернення: 20.05.2021).

115. Порядок взаємодії органів виконавчої влади з питань захисту державних інформаційних ресурсів в інформаційних та телекомунікаційних системах : затверджено постановою Кабінету Міністрів України від 16.11.2002 № 1772. URL: https://zakon.rada.gov.ua/laws/show/1772-2002-%D0%BF (дата звернення: 01.12.2020).

116. Порядок використання комп'ютерних програм в органах виконавчої влади : затверджено постановою Кабінету Міністрів України від 10.09.2003 № 1433. URL: https://zakon.rada.gov.ua/laws/show/1433-2003-%D0%BF#Text (дата звернення: 17.05.2021).

117. Порядок оприлюднення у мережі Інтернет інформації про діяльність органів виконавчої влади : затверджено постановою Кабінету Міністрів України

від 04.01.2002 № 3. URL: https://zakon.rada.gov.ua/laws/show/3-2002-%D0%BF/ed20200930#Text (дата звернення: 11.12.2020).

118. Почепцов Г. Сучасні інформаційні війни. К. : Вид.дім "Києво-Могилянська академія", 2015. 497 с.

119. Почепцов Г., Чукут С. Інформаційна політика : навч. посіб. 2-е вид. Київ : Знання, 2008. 663 с.

120. Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах. Постанова Кабінету Міністрів України від 29.03.2006 № 373. URL: https://zakon.rada.gov.ua/laws/show/373-2006-%D0%BF (дата звернення: 25.03.2021).

121. Прибутько П.С., Лук'янець І.Б. Інформаційні впливи: роль у суспільстві та сучасних воєнних конфліктах. Київ: Вид. А. В. Паливода, 2007. 252 с.

122. Проблеми інформаційного законодавства України в сфері створення, поширення та використання інформації та шляхи їх вирішення". *Аналітична записка* URL: https://niss.gov.ua/doslidzhennya/informaciyni-strategii/problemi-informaciynogo-zakonodavstva-ukraini-v-sferi (дата звернення: 30.05.2024).

123. Про Державну службу спеціального зв'язку та захисту інформації України. Закон України від 23.02.2006 № 3475-IV. URL: https://zakon.rada.gov.ua/laws/show/3475-15#Text (дата звернення: 22.03.2021).

124. Про державну таємницю. Закон України від 21.01.1994 № 3855-XII. URL: https://zakon.rada.gov.ua/go/3855-12 (дата звернення: 30.05.2024).

125. Про Доктрину інформаційної безпеки України. Указ Президента України від 25.02.2017 № 47/2017 URL: https://zakon.rada.gov.ua/go/47/2017 (дата звернення: 30.05.2024)

126. Про доступ до публічної інформації. Закон України від 13.01.2011 № 2939-VI. URL: https://zakon.rada.gov.ua/go/2939-17 (дата звернення: 30.05.2024).

127. Про електронні документи та електронний документообіг. Закон

України від 22.05.2003 № 851-IV. URL: https://zakon.rada.gov.ua/laws/show/851-15/ed20181107 (дата звернення: 12.12.2023).

128. Про електронну ідентифікацію та електронні довірчі послуги. Закон України від 05.10.2017 № 2155-VIII. URL: https://zakon.rada.gov.ua/laws/show/2155-19 (дата звернення: 12.12.2023).

129. Про затвердження Загальних вимог до кіберзахисту об’єктів критичної інфраструктури. Постанова Кабінету Міністрів України від 19.06.2019 № 518. URL: https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text (дата звернення: 07.05.2021).

130. Про затвердження Концепції «КИЇВ СМАРТ СІТІ 2020 : Рішення Київської міської ради від 21.11.2017 р. № 500/3507 URL: http://kmr.ligazakon.ua/SITE2/l_docki2.nsf/2cb81fc6e918119e422569b20056482e/7bc3bc24dc0d6752c2258212006de8e1?OpenDocument (дата звернення: 30.09.2020).

131. Про затвердження Положення про інтегровану систему електронної ідентифікації . Постанова Кабінету Міністрів України від 19.06.2019 р № 546 URL: https://zakon.rada.gov.ua/laws/show/546-2019-%D0%BF#Text (дата звернення: 30.09.2021).

132. Про захист інформації в інформаційно-телекомунікаційних системах. Закон України від 05.07.94 № 80/94-ВР. URL: http://zakon2.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80 (дата звернення: 07.06.2021).

133. Про захист персональних даних. Закон України від 01.06.2010 № 2297-VI. URL: https://zakon.rada.gov.ua/go/2297-17 (дата звернення: 30.01.2024).

134. Про інформацію. Закон України від 02.10.1992 № 2657-XII. URL: https://zakon.rada.gov.ua/go/2657-12 (дата звернення: 18.03.2024)

135. Про Концепцію державної інформаційної політики. Проект закону України № 7251 від 13.10.2010. URL: https://ips.ligazakon.net/document/JF5LF00A (дата звернення: 30.04.2024).

136. Про Концепцію Національної програми інформатизації. Закон України; Концепція від 04.02.1998 № 75/98-BPURL: https://zakon.rada.gov.ua/go/75/98-%D0%B2%D1%80 (дата звернення: 22.06.2023)

137. Про національну безпеку України. Закон України від 21.06.2018 № 2469-VIII. URL: https://zakon.rada.gov.ua/go/2469-19 (дата звернення: 30.05.2024).

138. Про Національну програму інформатизації. Закон України від 04.02.1998 № 74/98-ВР. URL: https://zakon.rada.gov.ua/go/74/98-%D0%B2%D1%80 (дата звернення: 18.06.2023)

139. Про стратегії здійснення цифрового розвитку, цифрових трансформацій і цифровізації системи управління державними фінансами на період до 2025 року та затвердження плану заходів щодо її реалізації. Розпорядження Кабінету Міністрів України; від 17.11.2021 № 1467-р. URL: https://zakon.rada.gov.ua/go/1467-2021-%D1%80 (дата звернення: 02.03.2024).

140. Про Стратегію інформаційної безпеки. Указ Президента України від 26.08.2021 № 447/2021 URL: https://zakon.rada.gov.ua/go/447/2021 (дата звернення: 30.03.2024).

141. Про стратегію національної безпеки України. Указ Президента України від 14.09.2020 № 392/2020 URL: https://zakon.rada.gov.ua/go/n0005525-20 (дата звернення: 02.03.2024)

142. Про стратегію реформування державного управління на 2022-2025 роки України. Розпорядження Кабінету Міністрів України від 21.07.2021 № 831-р. URL: https://zakon.rada.gov.ua/go/831-2021-%D1%80 (дата звернення: 02.02.2024)

143. Про стратегію цифрової трансформації соціальної сфери. Розпорядження Кабінету Міністрів України; від 28.10.2020 № 1353-р. URL: https://zakon.rada.gov.ua/go/1353-2020-%D1%80 (дата звернення: 02.04.2024)

144. Про схвалення Концепції розвитку електронного урядування в Україні. Розпорядження Кабінету Міністрів України; від 20.09.2017 № 649-р.

URL: https://zakon.rada.gov.ua/go/649-2017-%D1%80 (дата звернення: 02.06.2024)

145. Про схвалення Стратегії розвитку інформаційного суспільства в Україні. Розпорядження Кабінету Міністрів України від 15.07.2013 р. № 386 р. URL: http://zakon3.rada.gov.ua/laws/show/386-2013-р (дата звернення: 30.09.2020).

146. Проданюк Р. І. Інформаційна безпека в соціологічному контексті: до постановки проблеми. *Грані: науково-теоретичний альманах*. 2018. Т. 21. № 4. С. 84−90.

147. Прокоф'єва Д. М. Інформаційна війна та інформаційна злочинність. *Вісник Запорізького юридичного інституту*. 2000. №1. С. 288−307.

148. Пунченко О. П., Лазаревич А. А. Інформатизація як засіб репрезентації інформаційних ресурсів суспільства. URL: http://vestnikzgia.com.ua/article/view/57498 (дата звернення: 09.03.2021).

149. Рада національної безпеки і оборони України. URL: https://www.rnbo.gov.ua. (дата звернення: 30.09.2022).

150. Размєтаєва Ю. С. Приватність в інформаційному суспільстві: проблеми правового розуміння та регулювання. *Науковий вісник Ужгородського національного університету*. 2016. Вип. 37. Т. 1. С. 43−46. (Серія: Право).

151. Рождественська О. С. Особливий суб'єкт інформаційних правовідносин (загальнотеоретичний аспект). дис. канд. юрид. наук : 12.00.01. Харків, 2009. 203 с.

152. Сенченко О. П. Стратегія побудови та розвитку інформаційного суспільства. Перспективи. 2008. № 2. С. 8−19. (Серія : філософія, історія, соціологія, політологія).

153. Сідак В. С, Артемов В.Ю. Забезпечення інформаційної безпеки в країнах НАТО та ЄС : навч. посіб. Київ. КНТ, 2010. 160 с.

154. Сілкова Г. Інформаційно-аналітичні дослідження в структурі інформаційних ресурсів. Вісн. Кн. палати. 2005. № 2. С. 14−18.

155. Скільки українців не мають доступу до інтернету і коли ми подолаємо цифровий розрив. URL: https://speka.media/skilki-ukrayinciv-dosi-ne-mayut-dostupu-do-internetu-i-shho-robiti-z-cifrovim-rozrivom-plg4x9 (дата звернення: 30.02.2024).

156. Сороківська О. А. Інформаційна безпека підприємства: нові загрози та перспективи. *Вісник Хмельницького національного університету. Серія: Економічні науки.* 2010. № 2. Т. 2. С.32−35.

157. Соснін О. Передумови формування в Україні інформаційного права. Право України. 2005. № 11. С.99-103.

158. Соціально-правові основи інформаційної безпеки: навч. посіб. / В. М. Петрик та ін. Київ: Росава, 2007. 496 с.

159. Степанов В. Державна інформаційна політика: проблеми та перспективи: Монографія. Харків: С.А.М. , 2011. 548 с.

160. Степанов В. Ю. Сучасний інформаційний простір: особливості та тенденції розвитку: Монографія. Харків : САМ, 2010. 280 с.

161. Степанова О. М., Дегтярьова Л. М. Інформаційна безпека в умовах розвитку інформаційної системи підприємства. *Інформаційна безпека*. 2009. № 1. С. 59−63.

162. Тихомиров О. О. Діяльнісний підхід у дослідженнях забезпечення інформаційної безпеки: мета, засоби і методи, принципи, результати. Information Security of the Person, Society and State. 2012. № 3(10). С. 11−17.

163. Ткачук Т. Ю. Конкурентна розвідка. монографія. Коломия : Коломийська друкарня ім. Шухевича, 2015. 296 с.

164. Ткачук Т. Ю. Організаційне проектування у системі захисту конфіденційної інформації суб'єктів господарювання. *Інформаційна безпека людини, суспільства, держави*. 2014. № 1. С. 76–84.

165. Торічний В. О. Дослідження методів оцінки результативності державної інформаційної політики у контексті забезпечення державної безпеки. *Держава та регіони. Серія «Державне управління»*. 2019. № 3 (67). С. 200–203.

166. Торічний В. О. Інформаційне забезпечення безпеки держави в умовах інформаційного суспільства: державно-управлінський аспект: Монографія. Харків : НУЦЗУ, 2020. 274 с.

167. Торічний В. О. Критерії та умови ефективності впровадження механізму реалізації державної інформаційної політики. *Державне управління у сфері цивільного захисту: наука, освіта, практика : матеріали міжнар. наук.-практ. конф. інтернет-конф.* Харків : Вид-во НУЦЗУ, 2020. С. 80–81.

168. Хмелевський Р. М. Дослідження оцінки загроз інформаційній безпеці об'єктів інформаційної діяльності. *Сучасний захист інформації*. 2016. № 4. С. 65−70.

169. Цифрова трансформація публічного управління : кол. моногр. / О. В. Карпенко та ін. Київ : НАДУ, 2020. 256 с.

170. Цифрова трансформація як фактор покращення національної безпеки України. URL: https://censs.org/digital-transformation-as-a-factor-in-improving-the-national-security-of-ukraine/.

171. Шаповал Р. В. Вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України. *Наше право*. 2014. № 6. С. 5−9.

172. Шемшученко Ю. С. Інформаційне законодавство України : науково-практичний коментар. Київ : Юридична думка, 2011. 232 с.

173. Шемшученко Ю. С. Правове забезпечення інформаційної діяльності в Україні. Київ : Юридична думка, 2011. 384 с.

174. Шпига П. С. SMART-підхід до визначення завдань цифровізації робочих місць публічних службовців. *Вісник НАДУ. Серія «Державне управління».* 2020. № 4 (99). С. 77–83. URL: http://academy.gov.ua/infpol/pages/dop/2/files/7bb89df3-d121-4aaf-a6de-4792502589d1.pdf (дата звернення: 03.04.2022).

175. Щепанський Е. В. Впровадження сучасних інноваційних технологій надання державних і муніципальних послуг. *Вісник Національного університету цивільного захисту України. Сер. «Державне управління» : зб. наук. пр.* Харків : НУЦЗУ, 2021. Вип. 1 (14). С. 288–297. URL:

http://repositsc.nuczu.edu.ua/handle/123456789/13317 (дата звернення: 19.05.2023).

176. Юдін О. К. Інформаційна безпека держави : навч. посіб. Харків : Консул, 2011. 576 с.

177. Ярема О. Г. Предмет правового забезпечення інформаційної безпеки в інформаційному праві. *Науковий вісник Львівського державного університету внутрішніх справ. Серія: «Право».* 2016. № 2. С. 244−252.

178. Яременко О. І. Політико-правові засади цифровізації системи публічного управління: європейський досвід. *Побудова інформаційного суспільства: ресурси і технології* : матеріали XVIII Міжнар. наук.-практ. конф., Київ, 19-20 верес. 2019 р. Київ : УкрІНТЕІ, 2019. 260 с.

179. Abomhara M., Koien G. Cyber Security and the Internet Of Things: Vulnerabilities, Threats, Intruders and Attacks. Journal of Cyber Security. 2015. Vol. 4. P. 65-88.

180. Angell I. 'Winners and Losers in the Information Age', LSE Magazine, 7 (1),1995 P 10–12.

181. Arnstein S. A ladder of citizen participation in the USA. *Journal of the Royal Town Planning Institute*, vol. 57, no. 4, P. 176–182.

182. Baker J. Process, Practice and Principle: Teaching National Security Law and the Knowledge that Matters Most. *The Georgetown Journal of Legal Ethics*. 2014. Vol. 27. P. 163-189.

183. Bilynska M. The Formation of the Paradigm of National Resilience in the State Administration of Ukraine. *International Scientific Journal «Progress*. 2018. №.1-2. P. 41-45.

184. Castells M. The Information Age, Volume I: The Rise of the Network Society Blackwell, Oxford, 1996. URL: https://deterritorialinvestigations.wordpress.com/wp-content/uploads/2015/03/manuel_castells_the_rise_of_the_network_societybookfi-org.pdf

185. Dahl R. Development and Democratic Culture in Consolidating the Third

Wave Democracies. Ed. by L. Diamond. Baltimor; London, 1997. 360 p.

186. Diamond L. Developing Democracy. Toward Consolidation. / L.Diamond – Baltimore; London, 1999. 612 p.

187. Digital agenda for Europe. URL: https://eige.europa.eu/resources/digital_agenda_en.pdf (дата звернення: 30.09.2022).

188. Dizard Wilson J. Old media, mass communications in the information age. – New York: Longman, 1994. P. 215.

189. Goban-Klas'омT. Media i komunikowanie masowe: Teorie i analizy prasy, radia, telewizji i Internetu. Warszawa; Kraków: Wydawnictwo Naukowe PWN SA, 1999. C. 52–79.

190. Hundley R. O. The Global Course of the Information Revolution: Political, Economic and Social Conséquences. RAND, 2000. P. 109.

191. Internet Watch Foundation. Our remit and vision. URL: https://www.iwf.org.uk/what-we-do/why-we-exist/our-remit-and-vision (дата звернення: 09.04.2023).

192. ISO/EC 27002:2022 Information security, cyber security and privacy protection. Information security controls Requirements. URL: https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=104399 (дата звернення: 09.04.2022).

193. ISO/IEC 27001:2022 Information security, cyber security and privacy protection. Information security management systems. Requirements. URL: https://online.budstandart.com/ua/catalog/doc-page?id_doc=104398 (дата звернення: 09.04.2022).

194. ISO/IEC 27032:2016. Information technology. Security techniques. Guidelines for cybersecurity. URL: https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=69128 (дата звернення: 03.04.2022).

195. Kurilo A. Analysis of the subject branch of public administration of the risks of emergency situations. *Public administration and state security aspects*. Series: Vol.1/2023. URL: http://repositsc.nuczu.edu.ua/bitstream/123456789/16910/1/Kurilo.pdf

196. Kurilo A. Sociological monitoring of formation processes of public management society's information security. *Public administration and state security aspects* Series: Vol.2/2022. URL: http://repositsc.nuczu.edu.ua/bitstream/123456789/16910/1/Kurilo.pdf

197. Kurilo A.The place and role of forming information security in the system of public policy.*Public administration and state security aspects*. Series: Vol.1/2022. URL:http://repositsc.nuczu.edu.ua/bitstream/123456789/15387/3/Kurilo.pdf.

198. M. Carr. Public-private partnerships in national cyber-security strategies. URL: https://www.chathamhouse.org/sites/default/files/publications/ia/INTA92_1_03_Carr.pdf (дата звернення: 02.10.2022).

199. Margetts, H., Dunleavy, P. The second wave of digital-era governance: a quasi-paradigm for government on the Web. *Philosophical Transactions of the Royal Society.* URL: https://doi.org/10.1098/rsta.2012.0382 (дата звернення: 30.09.2020).

200. McQuail D. Media Performance. Mass Communication and the Public Interest. London ; Newbury Park ; New Delhi : SAGE Publications, 1993. – 350 p.

201. Morgan Nick; Moshiri Farrokh. Management communication : an anthology San Diego, Calif. : Cognella, 2011. 350 p.

202. Nicole de Montricher. Citizens and the Quality of Public Action: Seeking a New Form of Management. Public Participation and Contracting Practices in France // Citizens and the new Governance. Netherlands, 1999. 239 p.

203. O'Donnell G. Transition, Continuities, and Paradoxes. Issues in Democratic Consolidation: The New South American Democracies in Comparative Perspective / Ed. by Sc. Mainwaring, G. O'Donnell and J. S. Valenzuela. Notre Dame, 1992.

204. Pomaza-Ponomarenko A., Hren M., Durman O., Bondarchuk N., Vorobets V. Management mechanisms in the context of digitalization of all spheres of society. Revista San Gregorio. SPECIAL EDITION-2020. Núm. 42. URL: http://revista.sangregorio.edu.ec/index.php/REVISTASANGREGORIO/issue/view/RSAN42/showToc (дата звернення: 03.08.2023).

205. Publications Office of the European Union

URL:https://op.europa.eu/en/publication-detail/-/publication/2fcad39a-e777-11ee-9ea8-01aa75ed71a1 (дата звернення: 03.06.2023).

206. Rogers Everett M. Diffusion of Innovations. 4thed. New York: Free Press,1995.

207. Roszak T. The Cult of Information: The Folklore of Computers and the True Art of Thinking. T. Roszak. New York : Pantheon Book, 1986. P. 14.

208. Tech Trends 2019. Beyond the digital frontier. Deloitte Insights 2019. URL: https://www2.deloitte.com/content/dam/Deloitte/br/Documents/technology/DI_TechTrends2019.pdf page 19-20 (дата звернення: 03.11.2023).

209. The EU Data Protection Reform and Big Data: Factsheet». URL: http://ec.europa.eu/newsroom/just/document.cfm?doc_id=41523 (дата звернення: 09.06.2023).

210. Thomson, K.L., Von Solms, R., Louw, L. 2006. "Cultivating an organizational information security culture". *Computer Fraud & Security*. vol. 10, p. 7-11.

211. Von Solms R., Von Solms B. From policies to culture. *Computers & Security.* 2000. Vol. 23. Issue 4. P. 275–279.

212. Vroom C., von Solms R.. Towards information security behavioral compliance. *Computers & Security*. 2003. № 23 (1). P. 191–198.

213. Webster F, Erickson M (2004), 'Technology and Social Problems', in Ritzer, George (ed.), Handbook of Social Problems. Thousand Oaks, Calif.: Sage, P. 416–432.

214. Whitman M.E, Mattord H.J, Principles of Information Security, Course Technology, Boston. 2012. URL:https://scirp.org/reference/referencespapers?referenceid=1357711 (дата звернення: 09.10.2021).

215. William D. Eggers, Joel Bellman, The journey to government's digital transformation, 2015. URL: https://www2.deloitte.com/content/dam/insights/us/articles/digital-transformation-in-government/DUP_1081_Journey-to-govt-digital-future_MASTER.pdf.

ДОДАТКИ

Додаток А

Довідка про впровадження результатів дисертаційного дослідження

ХАРКІВСЬКА ОБЛАСНА ВІЙСЬКОВА АДМІНІСТРАЦІЯ

УПРАВЛІННЯ У СПРАВАХ МОЛОДІ ТА СПОРТУ

9 поверх, 7 під'їзд, Держпром, майдан Свободи, 5, м. Харків, 61022, тел. (057) 700-94-34, факс (057) 705-05-15,
E-mail: dsms.kharkivod@gmail.com, Web: http://dmskh.gov.ua, код ЄДРПОУ 24273286

25.06.2024 № 01-29/915 на № _____ від _____

ДОВІДКА
про впровадження результатів дисертаційного дослідження ад`юнкта Національного університету цивільного захисту України Курило Артема Геннадійовича на тему «Публічне управління у сфері інформаційної безпеки держави» на здобуття наукового ступеня доктора філософії у галузі знань 281 Публічне управління та адміністрування

Розвиток інформаційно-комунікаційних технологій і їх широке використання у всіх сферах життєдіяльності стають ключовими для світової інтеграції, соціального розвитку і економічного зростання. Одночасно ці технології створюють численні загрози, як відкриті, так і потенційно небезпечні. Це підкреслює важливість питань забезпечення інформаційної безпеки, яка є критичною складовою національної безпеки. У сучасному світі національна безпека значною мірою залежить від забезпечення інформаційної безпеки, що надає можливість припустити, що з розвитком технічного прогресу ця залежність лише зростатиме.

На цій підставі Курилом Артемом Геннадійовичем удосконалено напрями функціонування організаційно-правових та соціально-політичних механізмів публічного управління у сфері інформаційної безпеки в умовах використання цифрових технологій, що дозволило розкрити особливості сучасного стану, концептуального, стратегічного та нормативно-правового забезпечення реалізації державної інформаційної політики, надало можливість сформулювати відповідні науково-теоретичні та практичні рекомендації для покращення інформаційної безпеки в умовах цифровізації.

З огляду на вищевикладене, заслуговують на увагу окреслені Курилом Артемом Геннадійовичем напрями удосконалення механізмів публічного управління у сфері інформаційної безпеки. Тому пропозиції автора дисертаційного дослідження та розроблені ним практичні рекомендації є своєчасними та змістовними.

Довідка видана без фінансових зобов'язань.

000915

Начальник Управління Костянтин АНАНЧЕНКО

Ольга Муржа +3809727900746

Додаток Б

Довідка про впровадження результатів дисертаційного дослідження

ЧЕРКАСЬКА РАЙОННА РАДА

✉ вул. В.Чорновола, 157, м. Черкаси, 18003, ☎64-31-32, факс 64-34-76
E-mail: cherkaskarada@ukr.net Код ЄДРПОУ 25659510

26.06.2024 №36/01-13
на №_____від_____

ДОВІДКА
про впровадження результатів дисертаційного дослідження
Курило Артема Геннадійовича
на тему «Публічне управління у сфері інформаційної безпеки держави»
на здобуття наукового ступеня доктора філософії зі спеціальності 281
Публічне управління та адміністрування

Інформаційна безпека є критично важливим елементом національної безпеки в умовах сучасного світу. Розвиток інформаційних технологій створює безліч можливостей для покращення комунікації, економічного розвитку та суспільного добробуту, але також веде до нових загроз, які можуть впливати на національну безпеку. Основні аспекти інформаційної безпеки в контексті національної безпеки включають захист критичної інфраструктури, державних інформаційних систем, економічну безпеку, соціальну стабільність та національну оборону.

Представлене дослідження присвячено розв'язанню актуальної проблеми з обґрунтування теоретичних засад та розробки практичних рекомендацій щодо удосконалення у публічного управління у сфері інформаційної безпеки держави.

Автором удосконалено напрями функціонування організаційноправових та соціально-політичних механізмів публічного управління у сфері інформаційної безпеки в умовах використання цифрових технологій, що дозволило розкрити особливості сучасного стану, концептуального, стратегічного та нормативно-правового забезпечення реалізації державної інформаційної політики, надало можливість сформулювати відповідні науково-теоретичні та практичні рекомендації для покращення інформаційної безпеки в умовах цифровізації.

Зважаючи на актуальність наданих автором пропозицій, визнаємо за доцільне їх використання в практичній діяльності, зокрема, в організаційній, інформаційній, аналітичній, Черкаської районної ради Черкаської області. Довідка видана без фінансових зобов'язань.

Голова Олександр ВАСИЛЕНКО