МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ МЕНЕДЖМЕНТУ ТА ПІДПРИЄМНИЦТВА
КАФЕДРА ПУБЛІЧНОГО УПРАВЛІННЯ ТА АДМІНІСТРУВАННЯ

КВАЛІФІКАЦІЙНА РОБОТА

на тему

«ІНФОРМАЦІЙНА БЕЗПЕКА ПУБЛІЧНОГО УПРАВЛІННЯ: ЗАГРОЗИ, ВИКЛИКИ ТА ПЕРСПЕКТИВИ РОЗВИТКУ»

на здобуття освітнього ступеня магістра
зі спеціальності 281 «Публічне управління та адміністрування»
освітньо-професійної програми «Публічне управління та адміністрування»

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

_____ Каріна АНДРОСОВА
(підпис)

Виконала: здобувачка вищої освіти,
гр. ПУДМ-61
Каріна АНДРОСОВА

Керівник: к.філол.н., доцент
Ліна СТОРОЖЕНКО

Рецензент: к.е.н., доцент
Людмила ПАРІЙ

Київ, 2025

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
Навчально-науковий інститут менеджменту та підприємництва

Кафедра публічного управління та адміністрування
Ступінь вищої освіти «Магістр»
Спеціальність 281 «Публічне управління та адміністрування»
Освітньо-професійна програма «Публічне управління та адміністрування»

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Ірина АНТИПЕНКО
«31» жовтня 2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ
Андросової Каріни Олександрівни

1. Тема роботи «**Інформаційна безпека публічного управління: загрози, виклики та перспективи розвитку»**;
   керівник кваліфікаційної роботи – Стороженко Ліна Григорівна, к.філол.н., доцент, затверджені наказом Державного університету інформаційно-комунікаційних технологій від «30» жовтня 2025 р. № 467.
2. Термін подання кваліфікаційної роботи – «22» грудня 2025 р.
3. Вихідні дані до кваліфікаційної роботи: спеціальна теоретична і методична наукова література; наукові публікації (статті, монографії, дисертаційні дослідження) провідних вітчизняних та закордонних дослідників за темою кваліфікаційної роботи; результати науково-дослідної роботи кафедри публічного управління та адміністрування «Теоретико-прикладні аспекти розвитку цифрової держави в Україні»; нормативно-правові документи; матеріали переддипломної практики.
4. Перелік ілюстративного матеріалу: *презентація*
5. Дата видачі завдання: «27» червня 2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Структура роботи, вступ	27.06.2025 – 29.08.2025	Виконано
2.	Розділ І	01.09.2025 – 26.09.2025	Виконано
3.	Розділ ІІ	29.09.2025 – 24.10.2025	Виконано
4.	Розділ ІІІ	27.10.2025 – 28.11.2025	Виконано
5.	Висновки, додатки	01.12.2025 – 12.12.2025	Виконано
6.	Презентація	15.12.2025 – 19.12.2025	Виконано

Здобувачка вищої освіти _____ Каріна АНДРОСОВА

Керівник
кваліфікаційної роботи _____ Ліна СТОРОЖЕНКО

РЕФЕРАТ

Андросова К.О. Інформаційна безпека публічного управління: загрози, виклики та перспективи розвитку: кваліф. робота на здобуття освіт. ступеня магістра; спец. 281 «Публічне управління та адміністрування»; Держ. у-т інформац.-комунікац. технолог.; каф. публічного управління та адміністрування; наук. керівник Л.Г. Стороженко, к. філол. н., доц. Київ, 2025. 84 с.

Метою дослідження є комплексний аналіз теоретико-методологічних основ, сучасних загроз та перспектив розвитку інформаційної безпеки публічного управління в Україні, а також обґрунтування науково-практичних рекомендацій щодо вдосконалення системи інформаційної безпеки в умовах цифрової трансформації та гібридних викликів.

Об'єктом дослідження є система інформаційної безпеки публічного управління в Україні.

Предмет дослідження – управлінські, організаційні та технологічні аспекти забезпечення інформаційної безпеки органів публічної влади в умовах цифровізації та гібридних загроз.

Короткий зміст роботи. Розкрито сутність поняття «інформаційна безпека» у публічному управлінні та визначено її роль у системі національної безпеки України; проаналізовано теоретико-методологічні підходи до забезпечення інформаційної безпеки в умовах цифровізації та визначено базові принципи й аналітичні інструменти її оцінювання; досліджено нормативно-правове регулювання інформаційної безпеки в Україні та ЄС, окреслено проблеми національного законодавства та напрями його вдосконалення; ідентифіковано та класифіковано сучасні загрози інформаційній безпеці публічного управління (кібератаки, інформаційні операції, маніпуляції в медіа та соціальних мережах) та оцінено їхній вплив; оцінено стан захисту критичної інформаційної інфраструктури в умовах гібридної війни та обґрунтовано шляхи підвищення її стійкості, зокрема із застосуванням цифрових технологій (AI, Big Data); визначено стратегічні пріоритети державної політики у сфері інформаційної безпеки та напрями формування культури інформаційної безпеки серед держслужбовців і громадян з урахуванням європейських стандартів.

Ключові слова: інформаційна безпека, публічне управління, кіберзагрози, гібридна війна, цифрова трансформація, критична інформаційна інфраструктура, кіберстійкість, інформаційні операції, дезінформація, цифрові комунікації, штучний інтелект, державна політика, захист даних, інформаційні ризики.

ABSTRACT

Androsova K. Information Security of Public Administration: Threats, Challenges and Development Prospects: Qualification Thesis for the Master's Degree; Specialty 281 «Public Administration»; State University of Information and Communication Technologies; Department of Public Administration and Governance; Academic Supervisor – L. Storozhenko, PhD in Philology, Associate Professor. Kyiv, 2025. 84 p.

The purpose of the study is to provide a comprehensive analysis of the theoretical and methodological foundations, current threats, and development prospects of information security in public administration in Ukraine, as well as to substantiate scientific and practical recommendations for improving the system of information security under conditions of digital transformation and hybrid challenges.

The object of the study is the system of information security in public administration in Ukraine.

The subject of the study comprises managerial, organizational and technological aspects of ensuring information security in public authorities under conditions of digitalization and hybrid threats.

Summary. The thesis reveals the essence of the concept of "information security" in public administration and determines its role within the national security system of Ukraine; analyzes theoretical and methodological approaches to information security in the context of digitalization and identifies key principles and analytical tools for its assessment; examines the regulatory framework of information security in Ukraine and the EU, outlining the shortcomings of national legislation and the directions for its improvement; identifies and classifies modern threats to information security in public administration (cyberattacks, information operations, manipulations in media and social networks) and assesses their impact; evaluates the state of protection of critical information infrastructure under hybrid warfare conditions and substantiates ways to enhance its resilience, including through digital technologies (AI, Big Data); identifies strategic priorities of state policy in the field of information security and outlines approaches to forming a culture of information security among civil servants and citizens in line with European standards.

Key words: information security, public administration, cyber threats, hybrid warfare, digital transformation, critical information infrastructure, cyber resilience, information operations, disinformation, digital communications, artificial intelligence, state policy, data protection, information risks.

ЗМІСТ

ВСТУП 6
РОЗДІЛ 1. ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ОСНОВИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В СИСТЕМІ ПУБЛІЧНОГО УПРАВЛІННЯ 12
1.1. Сутність і зміст поняття «інформаційна безпека» у контексті публічного управління 12
1.2. Теоретичні підходи до забезпечення інформаційної безпеки в умовах цифровізації публічного управління 17
1.3. Методологічні принципи та інструменти аналізу інформаційної безпеки у публічному управлінні 23
РОЗДІЛ 2. СУЧАСНІ ЗАГРОЗИ ТА ВИКЛИКИ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ ПУБЛІЧНОГО УПРАВЛІННЯ В УКРАЇНІ 31
2.1. Вплив кібератак та інформаційних кампаній на ефективність державного управління 31
2.2. Ризики витоку, підробки та маніпулювання інформацією у цифрових комунікаціях органів влади 36
2.3. Проблеми захисту критичної інформаційної інфраструктури в умовах гібридних війн 40
2.4. Соціальні мережі як фактор інформаційної вразливості та інструмент впливу на публічне управління 43
РОЗДІЛ 3. НАПРЯМИ ТА ПЕРСПЕКТИВИ РОЗВИТКУ СИСТЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПУБЛІЧНОГО УПРАВЛІННЯ 49
3.1. Стратегічні орієнтири державної політики у сфері інформаційної безпеки 49
3.2. Механізми цифрової трансформації та підвищення кіберстійкості органів публічної влади 53
3.3. Використання штучного інтелекту, Big Data та аналітичних систем у моніторингу інформаційних ризиків 57
3.4. Формування культури інформаційної безпеки серед державних службовців та громадян 61
3.5. Міжнародне співробітництво та імплементація європейських стандартів у сфері інформаційної безпеки 65
ВИСНОВКИ 70
ДОДАТКИ 74
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 75

ВСТУП

Актуальність теми дослідження. У сучасних умовах глобальної цифровізації та стрімкого розвитку інформаційно-комунікаційних технологій питання інформаційної безпеки публічного управління набувають критичного значення для забезпечення національної безпеки держави, ефективності функціонування органів влади та захисту прав громадян. Інформаційна безпека є невід'ємною складовою національної безпеки України, що закріплено в Стратегії національної безпеки України, Доктрині інформаційної безпеки України та Стратегії кібербезпеки України.

Трансформація публічного управління в умовах цифрової епохи супроводжується появою принципово нових загроз і викликів, пов'язаних із захистом інформаційних ресурсів державних органів, забезпеченням стійкості критичної інформаційної інфраструктури, протидією кіберзлочинності та інформаційним операціям впливу. Ці виклики посилюються в умовах гібридної війни, яку Російська Федерація веде проти України з 2014 року, та повномасштабної військової агресії, розпочатої у лютому 2022 року. Інформаційний компонент гібридної війни включає масштабні кібератаки на критичну інфраструктуру, державні інформаційні ресурси, поширення дезінформації та пропаганди через соціальні мережі, що створює безпрецедентні загрози для системи публічного управління.

Водночас цифрова трансформація публічного управління відкриває нові можливості для підвищення ефективності державного управління, покращення якості надання публічних послуг, забезпечення прозорості та підзвітності органів влади. Впровадження систем електронного урядування, використання технологій штучного інтелекту, Big Data та аналітичних систем дозволяє оптимізувати процеси прийняття управлінських рішень та своєчасно виявляти інформаційні загрози. Однак ці процеси мають супроводжуватися адекватними заходами забезпечення інформаційної безпеки, що вимагає комплексного наукового осмислення теоретико-методологічних основ,

актуальних загроз та перспективних напрямів розвитку системи інформаційної безпеки публічного управління.

Особливої актуальності набуває питання адаптації вітчизняної системи інформаційної безпеки до європейських стандартів в контексті євроінтеграційних прагнень України. Імплементація положень Директиви ЄС NIS2, стандартів GDPR та інших європейських нормативних актів потребує суттєвого вдосконалення національного законодавства, інституційних механізмів та практик забезпечення інформаційної безпеки. Міжнародне співробітництво у сфері кібербезпеки, обмін досвідом та кращими практиками стають важливими чинниками підвищення рівня захищеності національного інформаційного простору.

Нинішній етап розвитку української державності характеризується необхідністю побудови стійкої, адаптивної та технологічно розвиненої системи публічного управління, здатної ефективно протистояти сучасним інформаційним загрозам, що вимагає не лише технічних рішень у сфері кіберзахисту, а й формування комплексної державної політики інформаційної безпеки, розвитку відповідної інституційної інфраструктури, підвищення кваліфікації державних службовців та формування культури інформаційної безпеки в суспільстві.

Відтак актуальність дослідження інформаційної безпеки публічного управління зумовлена сукупністю факторів: критичною важливістю захисту інформаційних ресурсів держави в умовах гібридної війни; необхідністю забезпечення безпечної цифрової трансформації публічного управління; потребою адаптації національної системи інформаційної безпеки до європейських стандартів; необхідністю наукового обґрунтування стратегічних напрямів розвитку системи інформаційної безпеки в контексті викликів сучасності.

Стан наукової розробки проблеми. Проблематика інформаційної безпеки в контексті публічного управління є предметом активних наукових

досліджень представників різних галузей знань – державного управління, інформаційного права, кібербезпеки, соціальних комунікацій.

Фундаментальні теоретичні основи інформаційної безпеки закладено у працях вітчизняних науковців: О. Данільяна, В. Ліпкана, О. Литвиненка, В. Остроухова, В. Петрика, Г. Почепцова та інших [1; 5; 7; 8; 9; 94]. Окреслені дослідження розкривають сутність та зміст інформаційної безпеки, її місце в системі національної безпеки, основні загрози та механізми їх нейтралізації.

Питання кібербезпеки та захисту критичної інфраструктури досліджували С. Бєлай, А. Войціховський, М. Ковалів, Д. Корнієнко, Р. Скриньковський та інші науковці [19; 20; 22; 23; 24]. Їхні роботи присвячені аналізу кіберзагроз, правовому регулюванню кібербезпеки, захисту об’єктів критичної інфраструктури.

Проблеми цифровізації публічного управління та розвитку електронного урядування розглядаються у працях В. Арутюнян, Є. Кравця, В. Саприкіна, Т. Камінської та інших дослідників [25; 27; 29; 59]. Вказані наукові розвідки аналізують сучасні тенденції цифрової трансформації державного управління, особливості впровадження електронних послуг, виклики та перспективи розвитку е-урядування в Україні.

Важливий внесок у дослідження застосування штучного інтелекту та великих даних у публічному управлінні зробили Ю. Магиляс, Н. Максименцева, М. Максименцев, В. Корсун, М. Миргородська [33; 34; 35]. Їхні роботи розкривають можливості та ризики використання сучасних інформаційних технологій для підвищення ефективності державного управління.

Феномен гібридної війни та інформаційних операцій досліджували В. Горбулін, Г. Гребньов, Є. Магда, Г. Сащук, В. Рихлік [10; 36; 43; 47; 95]. Зазначені науковці аналізують сутність гібридних загроз, інформаційний компонент російської агресії проти України, механізми поширення дезінформації та пропаганди.

Проблеми дезінформації в соціальних мережах та медіаманіпуляцій вивчали Д. Дубова, Н. Войтович та інші дослідники [37; 38; 88]. Їхні праці присвячені аналізу механізмів поширення фейків, формуванню медіаграмотності та критичного мислення як інструментів протидії інформаційним загрозам.

Питання державної інформаційної політики та нормативно-правового регулювання інформаційної безпеки розглядали О. Войтко, Т. Гуржій, Л. Коцур, О. Грига, О. Ніщименко, Ю. Кунєв [11; 12; 13; 14; 91; 92]. Ці роботи аналізують теоретико-методологічні засади державної інформаційної політики, правові механізми забезпечення інформаційної безпеки в умовах воєнного стану.

Зарубіжний досвід забезпечення інформаційної безпеки та цифрової трансформації досліджували С. Чукут, Т. Камінська, А. Камінський та інші науковці [59; 60]. Їхні праці розкривають особливості реалізації політики інформаційної безпеки та електронного урядування в країнах ЄС та світу.

Попри значний доробок вітчизняних та зарубіжних науковців, комплексне дослідження інформаційної безпеки публічного управління з урахуванням сучасних викликів гібридної війни, стрімкої цифровізації та євроінтеграційних процесів залишається недостатньо вивченим. Потребують поглибленого аналізу питання адаптації системи публічного управління до нових інформаційних загроз, механізми імплементації європейських стандартів кібербезпеки, використання штучного інтелекту для моніторингу інформаційних ризиків, формування культури інформаційної безпеки в органах публічної влади. Саме ці обставини визначили вибір теми, мету, завдання та структуру дослідження.

Мета і завдання дослідження. Метою дослідження є комплексний аналіз теоретико-методологічних основ, сучасних загроз та перспектив розвитку інформаційної безпеки публічного управління в Україні, а також обґрунтування науково-практичних рекомендацій щодо вдосконалення

системи інформаційної безпеки в умовах цифрової трансформації та гібридних викликів.

Для досягнення поставленої мети визначено такі завдання:

- розкрити сутність поняття «інформаційна безпека» у публічному управлінні та визначити її роль у системі національної безпеки України;
- проаналізувати теоретико-методологічні підходи до забезпечення інформаційної безпеки в умовах цифровізації та визначити базові принципи й аналітичні інструменти її оцінювання;
- дослідити нормативно-правове регулювання інформаційної безпеки в Україні та ЄС, окреслити проблеми національного законодавства та напрями його вдосконалення;
- ідентифікувати та класифікувати сучасні загрози інформаційній безпеці публічного управління (кібератаки, інформаційні операції, маніпуляції в медіа та соціальних мережах) та оцінити їхній вплив;
- оцінити стан захисту критичної інформаційної інфраструктури в умовах гібридної війни та обґрунтувати шляхи підвищення її стійкості, зокрема із застосуванням цифрових технологій (AI, Big Data);
- визначити стратегічні пріоритети державної політики у сфері інформаційної безпеки та напрями формування культури інформаційної безпеки серед держслужбовців і громадян з урахуванням європейських стандартів.

Об’єктом дослідження є система інформаційної безпеки публічного управління в Україні.

Предмет дослідження – управлінські, організаційні та технологічні аспекти забезпечення інформаційної безпеки органів публічної влади в умовах цифровізації та гібридних загроз.

Методи дослідження. Для досягнення мети та виконання поставлених завдань використано комплекс загальнонаукових і спеціальних методів дослідження. Системний підхід застосовано для аналізу інформаційної безпеки як цілісної системи взаємопов’язаних елементів у структурі

національної безпеки держави. Структурно-функціональний метод використано для визначення функцій та взаємозв'язків елементів системи інформаційної безпеки публічного управління. Порівняльний аналіз дозволив виявити особливості правового регулювання та організаційних механізмів забезпечення інформаційної безпеки в Україні та країнах ЄС.

Методи аналізу та синтезу застосовано для дослідження наукових підходів до визначення сутності інформаційної безпеки, класифікації загроз та виявлення закономірностей їх розвитку. Метод експертних оцінок використано для аналізу стану інформаційної безпеки критичної інфраструктури та визначення пріоритетних напрямів її захисту. Прогностичний метод дозволив обґрунтувати перспективні напрями розвитку системи інформаційної безпеки публічного управління з урахуванням тенденцій цифровізації та еволюції інформаційних загроз.

Нормативно-правовий аналіз застосовано для дослідження вітчизняного та міжнародного законодавства у сфері інформаційної безпеки, кібербезпеки та захисту даних. Контент-аналіз використано для вивчення інформаційних кампаній, дезінформації та пропаганди в соціальних мережах. Методи статистичного аналізу дозволили кількісно оцінити масштаби кіберзагроз та їх вплив на функціонування органів публічної влади.

Комплексне застосування зазначених методів забезпечило всебічність, об'єктивність та достовірність результатів дослідження.

Структура та обсяг роботи. Робота складається зі вступу, трьох розділів, висновків, додатку та списку використаних джерел. Загальний обсяг роботи складає 84 сторінки. Список використаних джерел нараховує 100 позицій.

РОЗДІЛ 1. ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ОСНОВИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В СИСТЕМІ ПУБЛІЧНОГО УПРАВЛІННЯ

1.1. Сутність і зміст поняття «інформаційна безпека» у контексті публічного управління

Інформаційна безпека як феномен сучасності набуває дедалі більшого значення в контексті функціонування системи публічного управління. Розуміння сутності та змісту цього поняття є необхідною передумовою для формування ефективної державної політики у сфері захисту інформаційних ресурсів та інтересів держави, суспільства і громадян.

Поняття «інформаційна безпека» в науковій літературі та нормативно-правових актах трактується неоднозначно, що зумовлено багатоаспектністю цього явища та різними методологічними підходами до його вивчення. У широкому розумінні інформаційна безпека розглядається як стан захищеності національних інтересів в інформаційній сфері, що визначається сукупністю збалансованих інтересів особи, суспільства і держави [65].

Відповідно до Доктрини інформаційної безпеки України, інформаційна безпека держави визначається як стан захищеності національних інтересів у інформаційній сфері, що визначаються сукупністю збалансованих інтересів особи, суспільства і держави [65]. Це визначення носить комплексний характер і відображає багатовимірність інформаційної безпеки як об’єкта правового регулювання та управлінського впливу.

У вітчизняній науковій літературі сформувалося кілька підходів до розуміння сутності інформаційної безпеки. Перший підхід пов’язує інформаційну безпеку виключно із захистом інформації від несанкціонованого доступу, втрати, модифікації чи знищення [3]. Такий технократичний підхід зосереджує увагу на технічних аспектах захисту інформаційних ресурсів та інформаційних систем.

Другий підхід розглядає інформаційну безпеку як складову національної безпеки держави, що охоплює захист інформаційного простору, інформаційного суверенітету та інформаційних інтересів особи, суспільства і держави [5; 92]. Цей підхід акцентує увагу на стратегічному вимірі інформаційної безпеки та її зв'язку з іншими видами безпеки – політичною, економічною, воєнною, екологічною тощо.

Третій підхід визначає інформаційну безпеку через призму захисту прав і свобод людини в інформаційній сфері, забезпечення доступу громадян до інформації, захисту від маніпулятивного впливу та дезінформації. Цей гуманітарний підхід наголошує на антропоцентричному характері інформаційної безпеки.

У контексті публічного управління інформаційна безпека набуває специфічного змісту, пов'язаного з особливостями функціонування органів державної влади та місцевого самоврядування. Інформаційна безпека публічного управління може бути визначена як стан захищеності інформаційних ресурсів, інформаційних систем та інформаційних процесів органів публічної влади, що забезпечує їх ефективне функціонування, прийняття обґрунтованих управлінських рішень та надання якісних публічних послуг громадянам [16; 17].

Зміст інформаційної безпеки публічного управління охоплює кілька взаємопов'язаних компонентів. По-перше, це захист конфіденційної інформації, що знаходиться у володінні органів публічної влади, включаючи інформацію з обмеженим доступом, персональні дані громадян, інформацію, що становить державну таємницю. Забезпечення конфіденційності такої інформації є критично важливим для захисту прав громадян, національних інтересів держави та ефективності діяльності органів влади.

По-друге, інформаційна безпека публічного управління включає забезпечення цілісності та достовірності інформації, що використовується органами влади для прийняття управлінських рішень [8]. Маніпулювання даними, підробка документів, викривлення статистичної інформації можуть

призвести до прийняття хибних рішень з негативними наслідками для держави та суспільства. Тому забезпечення автентичності та незмінності інформації є важливою складовою інформаційної безпеки.

По-третє, важливим компонентом інформаційної безпеки публічного управління є забезпечення доступності інформаційних ресурсів та інформаційних систем для авторизованих користувачів [63]. Це означає, що державні службовці та інші уповноважені особи повинні мати можливість у будь-який час отримати доступ до необхідної інформації для виконання своїх службових обов'язків. Порушення доступності інформаційних систем внаслідок технічних збоїв, кібератак чи інших причин може паралізувати роботу органів влади та зірвати надання публічних послуг.

По-четверте, інформаційна безпека публічного управління охоплює захист від інформаційно-психологічних впливів, спрямованих на маніпулювання громадською думкою, дискредитацію органів влади, поширення дезінформації та пропаганди [9; 36]. В умовах гібридної війни, яку Росія веде проти України, цей аспект інформаційної безпеки набуває критичного значення.

По-п'яте, інформаційна безпека публічного управління передбачає забезпечення стійкості критичної інформаційної інфраструктури до різноманітних загроз, включаючи кібератаки, природні та техногенні катастрофи. Критична інформаційна інфраструктура включає інформаційні системи, які є життєво важливими для функціонування держави, і порушення їх роботи може спричинити серйозні негативні наслідки.

Структурно інформаційна безпека публічного управління може бути представлена як система, що включає кілька рівнів. На макрорівні це національна система забезпечення інформаційної безпеки, що включає сукупність державних органів, нормативно-правову базу, стратегічні документи та механізми координації [67; 68]. На мезорівні це відомчі системи інформаційної безпеки окремих органів влади та секторів публічного

управління. На мікрорівні це локальні системи захисту інформації в окремих структурних підрозділах та інформаційних системах.

Важливим аспектом розуміння сутності інформаційної безпеки публічного управління є її об'єкти. До об'єктів інформаційної безпеки публічного управління належать: інформаційні ресурси органів публічної влади, що містять відомості про діяльність держави, персональні дані громадян, статистичну та аналітичну інформацію; інформаційні системи та інформаційно-комунікаційні мережі органів влади; інформаційна інфраструктура, включаючи центри обробки даних, сервери, засоби зв'язку; процеси збирання, обробки, зберігання, передачі та використання інформації в органах влади; інформаційні відносини між органами влади, громадянами та іншими суб'єктами.

Суб'єктами забезпечення інформаційної безпеки публічного управління виступають: держава в особі органів законодавчої, виконавчої та судової влади; спеціалізовані органи у сфері інформаційної безпеки та кібербезпеки; органи місцевого самоврядування; інститути громадянського суспільства; міжнародні організації та іноземні держави в рамках міжнародного співробітництва [67].

Принципами забезпечення інформаційної безпеки публічного управління є: пріоритет прав і свобод людини в інформаційній сфері; верховенство права та законність; прозорість і відкритість діяльності органів влади за винятком інформації з обмеженим доступом; співробітництво держави з громадянським суспільством; інтеграція національної системи інформаційної безпеки в міжнародні системи; постійне вдосконалення механізмів захисту інформації відповідно до еволюції загроз [65; 66].

Функції інформаційної безпеки публічного управління включають: захисну функцію, спрямовану на запобігання та нейтралізацію загроз інформаційним ресурсам та системам; регулятивну функцію, що полягає в упорядкуванні інформаційних відносин через нормативно-правове регулювання; контрольну функцію, пов'язану з моніторингом стану

інформаційної безпеки та виявленням порушень; превентивну функцію, спрямовану на попередження інформаційних інцидентів; відновлювальну функцію, що передбачає ліквідацію наслідків порушень інформаційної безпеки.

У сучасних умовах стрімкої цифровізації публічного управління зміст інформаційної безпеки трансформується та розширюється. Впровадження систем електронного урядування, використання технологій Big Data, штучного інтелекту, хмарних обчислень створює нові можливості для підвищення ефективності державного управління, але водночас породжує нові виклики та загрози. Інформаційна безпека в цифрову епоху має забезпечувати не лише захист від традиційних загроз, а й гарантувати безпечну цифрову трансформацію публічного управління.

Окремого розгляду потребує співвідношення понять «інформаційна безпека» та «кібербезпека» в контексті публічного управління. Кібербезпека є більш вузьким поняттям і стосується захисту кіберпростору, комп'ютерних систем, мереж та даних від кіберзагроз [67]. Інформаційна безпека є ширшим поняттям, що охоплює не лише технічні, а й правові, організаційні, психологічні та інші аспекти захисту інформації та інформаційного простору. У системі публічного управління забезпечення кібербезпеки є важливою, але не єдиною складовою інформаційної безпеки.

Таким чином, інформаційна безпека публічного управління є комплексним, багатовимірним феноменом, що охоплює технологічні, правові, організаційні, економічні та соціокультурні аспекти захисту інформації та інформаційних систем органів публічної влади. Забезпечення інформаційної безпеки є необхідною умовою ефективного функціонування системи публічного управління, реалізації конституційних прав і свобод громадян та захисту національних інтересів держави в інформаційній сфері. Розуміння сутності та змісту інформаційної безпеки публічного управління створює методологічну основу для аналізу загроз, викликів та розробки механізмів їх нейтралізації.

1.2. Теоретичні підходи до забезпечення інформаційної безпеки в умовах цифровізації публічного управління

Цифровізація публічного управління є об'єктивним процесом, що відображає загальносвітові тенденції технологічного розвитку та трансформації взаємовідносин між державою і суспільством. Перехід від традиційних форм організації державного управління до цифрових моделей кардинально змінює підходи до забезпечення інформаційної безпеки, вимагаючи нового теоретичного осмислення цього феномену.

У науковій літературі сформувалося кілька теоретичних підходів до забезпечення інформаційної безпеки в умовах цифровізації публічного управління, кожен з яких акцентує увагу на певних аспектах цієї проблематики.

Технократичний підхід розглядає інформаційну безпеку переважно через призму технічних засобів захисту інформації. Прихильники цього підходу вважають, що основою забезпечення інформаційної безпеки є впровадження сучасних технологій кіберзахисту: систем виявлення та запобігання вторгненням, засобів криптографічного захисту, систем управління інцидентами, технологій блокчейн тощо [20; 63]. Технократичний підхід підкреслює необхідність постійного оновлення технічних засобів захисту відповідно до еволюції кіберзагроз.

Перевагою технократичного підходу є його практична спрямованість та можливість вимірювання ефективності заходів захисту через технічні показники. Однак обмеженість цього підходу полягає в недооцінці організаційних, правових та соціокультурних факторів інформаційної безпеки. Досвід показує, що навіть найсучасніші технічні засоби не можуть гарантувати абсолютну безпеку, якщо не підкріплені належною організаційною культурою та компетентністю персоналу.

Системний підхід трактує інформаційну безпеку як цілісну систему взаємопов'язаних елементів, що включають технічні, організаційні, правові та

соціокультурні компоненти [8]. Згідно з цим підходом, забезпечення інформаційної безпеки вимагає комплексних заходів на всіх рівнях системи публічного управління – від стратегічного планування до оперативного реагування на інциденти.

Системний підхід передбачає розгляд інформаційної безпеки як підсистеми загальної системи національної безпеки держави з притаманними їй зворотними зв'язками, механізмами саморегуляції та адаптації до змін зовнішнього середовища. Цей підхід акцентує увагу на необхідності координації зусиль різних державних органів, узгодження нормативно-правових актів, інтеграції технічних рішень та формування єдиного інформаційного простору публічного управління.

Системний підхід дозволяє виявити системні властивості інформаційної безпеки, які не зводяться до простої суми властивостей окремих елементів. Зокрема, синергетичний ефект від взаємодії технічних засобів захисту, організаційних процедур та компетентного персоналу значно перевищує ефективність кожного з цих компонентів окремо [99].

Ризик-орієнтований підхід фокусується на виявленні, оцінці та управлінні інформаційними ризиками [24]. Цей підхід виходить з того, що абсолютна безпека є недосяжною, і завданням системи інформаційної безпеки є зменшення ризиків до прийнятного рівня з урахуванням наявних ресурсів та пріоритетів.

Ризик-орієнтований підхід передбачає регулярне проведення аудиту інформаційної безпеки, ідентифікацію вразливостей, оцінку ймовірності реалізації загроз та можливих наслідків інцидентів. На основі цієї інформації розробляються пріоритетні заходи з мінімізації найбільш критичних ризиків [69]. Цей підхід дозволяє раціонально розподіляти обмежені ресурси, зосереджуючи увагу на захисті найбільш критичних інформаційних активів та систем.

Важливою складовою ризик-орієнтованого підходу є план реагування на інциденти та відновлення після них. Визнаючи неможливість запобігання всім

інцидентам, цей підхід наголошує на необхідності готовності до швидкого виявлення, локалізації та усунення наслідків порушень інформаційної безпеки.

Процесний підхід розглядає забезпечення інформаційної безпеки як безперервний процес, що включає планування, впровадження, моніторинг та вдосконалення заходів захисту [99]. Цей підхід базується на циклі Демінга (Plan-Do-Check-Act) і передбачає постійне покращення системи інформаційної безпеки на основі аналізу її ефективності та змін у середовищі загроз.

Процесний підхід акцентує увагу на необхідності інтеграції заходів інформаційної безпеки в бізнес-процеси органів публічної влади. Інформаційна безпека не повинна розглядатися як окрема функція, відірвана від основної діяльності, а має бути органічно вбудована в усі процеси збирання, обробки, зберігання та використання інформації.

Впровадження процесного підходу в органах публічної влади передбачає розробку регламентів, стандартних операційних процедур, чек-листів для забезпечення інформаційної безпеки на різних етапах роботи з інформацією. Це дозволяє формалізувати і стандартизувати практики інформаційної безпеки, зменшити залежність від суб'єктивних факторів та забезпечити передбачуваність результатів [54; 56].

Адаптивний підхід підкреслює необхідність гнучкості та здатності системи інформаційної безпеки швидко реагувати на нові загрози в умовах динамічного розвитку інформаційних технологій [67]. Цей підхід виходить з того, що статичні системи захисту швидко застарівають і не можуть ефективно протидіяти новим видам кіберзагроз.

Адаптивний підхід передбачає використання технологій штучного інтелекту та машинного навчання для автоматичного виявлення аномалій, прогнозування атак та адаптації механізмів захисту до нових загроз [34; 35]. Системи інформаційної безпеки повинні мати властивості самонавчання,

здатність аналізувати великі обсяги даних про інциденти та автоматично коригувати параметри захисту.

Важливою складовою адаптивного підходу є концепція кіберстійкості (cyber resilience), яка передбачає не лише запобігання атакам, а й здатність системи продовжувати функціонування в умовах кібератаки, швидко відновлюватися та навчатися на основі інцидентів [67]. Кіберстійкість публічного управління означає, що органи влади повинні мати резервні системи, плани забезпечення безперервності діяльності та механізми швидкого відновлення критичних функцій.

Інтегрований підхід об'єднує елементи різних підходів і розглядає інформаційну безпеку як багатовимірний феномен, що вимагає комплексного впливу на технологічному, організаційному, правовому та соціокультурному рівнях. Цей підхід визнає, що жоден окремий підхід не може забезпечити всебічний захист інформації в умовах складності та динамічності сучасного інформаційного середовища.

Інтегрований підхід передбачає координацію різних аспектів інформаційної безпеки: технічний захист інформаційних систем має підкріплюватися правовим регулюванням, організаційними процедурами, підготовкою кваліфікованих кадрів та формуванням культури інформаційної безпеки [53; 99]. Ефективність інтегрованого підходу залежить від збалансованості всіх компонентів системи інформаційної безпеки.

Екосистемний підхід є порівняно новим напрямом теоретичного осмислення інформаційної безпеки в умовах цифровізації [32]. Цей підхід розглядає інформаційну безпеку публічного управління як частину більш широкої екосистеми цифрової безпеки, що включає державний, приватний та громадський сектори.

Екосистемний підхід підкреслює взаємозалежність різних учасників цифрового простору та необхідність їх співпраці для забезпечення колективної безпеки. Органи публічної влади не можуть забезпечити інформаційну безпеку ізольовано – вони залежать від безпеки

телекомунікаційних мереж, послуг хмарних провайдерів, програмного забезпечення тощо. Тому екосистемний підхід наголошує на необхідності державно-приватного партнерства у сфері кібербезпеки, обміну інформацією про загрози та координації зусиль.

Антропоцентричний підхід ставить людину в центр системи інформаційної безпеки [14; 88]. Згідно з цим підходом, захист інформації є не самоціллю, а засобом забезпечення прав і свобод людини, захисту персональних даних, недопущення маніпулятивного впливу та дезінформації.

Антропоцентричний підхід акцентує увагу на необхідності балансу між безпекою та приватністю, між захистом інформації та правом на доступ до інформації, між інтересами держави та правами громадян. В умовах цифровізації публічного управління, коли держава отримує доступ до величезних обсягів персональних даних громадян, цей баланс стає особливо критичним.

Важливою складовою антропоцентричного підходу є принцип безпеки за замовчуванням (security by default) та конфіденційності за замовчуванням (privacy by default), закріплені в Загальному регламенті захисту даних ЄС (GDPR) [73]. Ці принципи передбачають, що інформаційні системи публічного управління повинні проектуватися з урахуванням максимального захисту прав користувачів, а не розглядати безпеку як додаткову опцію.

В умовах цифровізації публічного управління особливого значення набуває концепція *цифрового суверенітету*, яка стає важливим елементом теоретичного осмислення інформаційної безпеки [35]. Цифровий суверенітет передбачає здатність держави контролювати національний сегмент кіберпростору, приймати самостійні рішення щодо регулювання цифрових технологій, захищати національні інформаційні ресурси від зовнішніх загроз.

Цифровий суверенітет не означає ізоляцію від глобального інформаційного простору, а передбачає збалансоване поєднання інтеграції у світову цифрову економіку та захисту національних інтересів у кіберпросторі.

Для України в контексті гібридної війни забезпечення цифрового суверенітету є критично важливим завданням [13; 18].

Окрему увагу в теоретичних підходах до забезпечення інформаційної безпеки в умовах цифровізації займає концепція *довіреної цифровізації* [26; 28]. Ця концепція підкреслює, що впровадження цифрових технологій у публічному управлінні має супроводжуватися заходами забезпечення довіри громадян до цифрових послуг та електронних взаємодій з органами влади.

Довірена цифровізація передбачає прозорість алгоритмів прийняття автоматизованих рішень, захист персональних даних, забезпечення доступності та інклюзивності цифрових послуг, можливість оскарження автоматизованих рішень. Без довіри громадян цифрова трансформація публічного управління не досягне своїх цілей, оскільки громадяни не користуватимуться електронними послугами, побоюючись витоку персональних даних чи зловживань.

Важливою складовою теоретичного осмислення інформаційної безпеки є *концепція безпечного життєвого циклу інформаційних систем* [64]. Ця концепція передбачає, що заходи безпеки повинні впроваджуватися на всіх етапах життєвого циклу інформаційної системи – від проектування та розробки до експлуатації та виведення з експлуатації.

Традиційний підхід, коли безпека розглядається як додаткова функція, що впроваджується після створення системи, є неефективним і затратним. Натомість концепція Security by Design передбачає вбудовування механізмів безпеки на етапі проектування архітектури системи [24]. Це дозволяє створювати більш стійкі та захищені інформаційні системи при менших витратах.

Сучасні теоретичні підходи до забезпечення інформаційної безпеки в умовах цифровізації публічного управління все більше уваги приділяють *проактивному характеру* заходів захисту [76]. Замість реактивної моделі, коли реагування відбувається після інциденту, проактивний підхід передбачає

активне виявлення загроз, аналіз вразливостей, моделювання можливих атак та превентивне впровадження заходів захисту.

Проактивний підхід реалізується через технології threat intelligence (розвідка загроз), які передбачають систематичне збирання, аналіз та поширення інформації про актуальні та потенційні кіберзагрози [76]. Органи публічної влади повинні не лише захищатися від відомих загроз, а й прогнозувати появу нових загроз і завчасно готуватися до них.

Таким чином, теоретичне осмислення інформаційної безпеки в умовах цифровізації публічного управління характеризується множинністю підходів, кожен з яких висвітлює певні грані цього складного феномену. Ефективна система інформаційної безпеки публічного управління має базуватися на інтегрованому підході, що поєднує технічні, організаційні, правові та соціокультурні аспекти, враховує динамічний характер загроз та забезпечує баланс між безпекою, ефективністю та дотриманням прав громадян.

1.3. Методологічні принципи та інструменти аналізу інформаційної безпеки у публічному управлінні

Аналіз інформаційної безпеки у публічному управлінні вимагає застосування відповідного методологічного інструментарію, що дозволяє системно оцінити стан захищеності інформаційних ресурсів, виявити вразливості, оцінити ризики та обґрунтувати заходи їх мінімізації. Методологія аналізу інформаційної безпеки базується на певних принципах та включає сукупність методів, інструментів та технологій.

Принципи аналізу інформаційної безпеки становлять методологічний фундамент для проведення досліджень у цій сфері. До основних принципів належать:

принцип системності передбачає розгляд інформаційної безпеки як цілісної системи взаємопов’язаних елементів у структурі публічного управління [5; 8]. Аналіз має охоплювати всі компоненти системи – технічні

засоби, організаційні процедури, нормативно-правове забезпечення, кадровий потенціал, а також взаємозв'язки між ними. Ігнорування хоча б одного елементу може призвести до неповних або хибних висновків.

Принцип комплексності вимагає багатоаспектного аналізу інформаційної безпеки з урахуванням технічних, правових, організаційних, економічних та соціокультурних факторів [99]. Інформаційна безпека не може бути забезпечена виключно технічними засобами – необхідний комплексний підхід, що охоплює всі виміри проблеми.

Принцип об'єктивності передбачає використання достовірних даних, перевірених фактів, науково обґрунтованих методів аналізу та уникнення упереджених оцінок [91]. Об'єктивність аналізу забезпечується через використання кількісних показників, незалежних експертних оцінок, статистичних даних про інциденти інформаційної безпеки.

Принцип динамічності наголошує на необхідності врахування постійних змін у середовищі загроз, технологіях захисту та умовах функціонування системи публічного управління [67; 76]. Аналіз інформаційної безпеки не може бути одноразовою акцією – він має здійснюватися регулярно з урахуванням еволюції загроз та змін в інформаційних системах.

Принцип пріоритетності передбачає зосередження аналітичних зусиль на найбільш критичних інформаційних активах та найбільш ймовірних і небезпечних загрозах [22; 24]. Оскільки ресурси для аналізу та захисту завжди обмежені, необхідно визначити пріоритети на основі оцінки цінності інформаційних активів та рівня ризиків.

Принцип адекватності означає, що методи аналізу та заходи захисту повинні відповідати рівню загроз та цінності інформаційних активів, що захищаються [69]. Надмірний захист може бути економічно недоцільним, тоді як недостатній захист створює неприйнятні ризики.

Принцип безперервності вимагає систематичного моніторингу стану інформаційної безпеки, постійного аналізу нових загроз та регулярного

оновлення оцінок ризиків [84]. Аналіз інформаційної безпеки не завершується розробкою рекомендацій – він має бути безперервним процесом.

Методи аналізу інформаційної безпеки можна класифікувати за різними критеріями. За характером підходу виділяють якісні та кількісні методи. Якісні методи базуються на експертних оціках, описових характеристиках, класифікаціях [93]. Кількісні методи використовують чисельні показники, статистичні дані, математичні моделі [33].

Метод аналізу ризиків є одним з найбільш поширених інструментів оцінки інформаційної безпеки [22; 24]. Процес аналізу ризиків включає кілька етапів: ідентифікацію інформаційних активів та визначення їх цінності; виявлення загроз та вразливостей; оцінку ймовірності реалізації загроз; оцінку можливих наслідків інцидентів; розрахунок рівня ризику; визначення пріоритетних заходів з мінімізації ризиків.

Існують різні методології оцінки ризиків інформаційної безпеки, зокрема OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation), CRAMM (CCTA Risk Analysis and Management Method), ISO/IEC 27005 та інші. Ці методології відрізняються ступенем деталізації, складністю та сферою застосування, але всі вони базуються на спільних принципах ідентифікації активів, загроз, вразливостей та оцінки ризиків.

Метод аудиту інформаційної безпеки передбачає систематичну перевірку відповідності стану інформаційної безпеки встановленим вимогам, стандартам та процедурам [56; 99]. Аудит може бути внутрішнім, коли його проводять власні фахівці організації, або зовнішнім, коли залучаються незалежні експерти. Аудит інформаційної безпеки включає перевірку технічних засобів захисту, організаційних процедур, документації, компетентності персоналу.

Метод тестування на проникнення (penetration testing) полягає в імітації кібератаки для виявлення вразливостей інформаційних систем [20]. Етичні хакери намагаються зламати систему, використовуючи ті ж методи, що й зловмисники, але з метою виявлення слабких місць та їх усунення.

Тестування на проникнення дозволяє оцінити реальну стійкість систем до атак і виявити вразливості, які можуть бути не очевидними при інших видах аналізу.

Метод моделювання загроз (threat modeling) передбачає систематичну ідентифікацію потенційних загроз на етапі проектування або аналізу інформаційної системи [76]. Моделювання загроз включає опис архітектури системи, ідентифікацію потенційних зловмисників та їх мотивації, визначення можливих векторів атак, оцінку ймовірності та наслідків успішної атаки. Популярними методологіями моделювання загроз є STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege) та DREAD (Damage, Reproducibility, Exploitability, Affected Users, Discoverability).

Метод аналізу інцидентів базується на систематичному дослідженні інцидентів інформаційної безпеки, що вже відбулися, з метою виявлення їх причин, механізмів реалізації, наслідків та розробки заходів запобігання подібним інцидентам у майбутньому [84]. Аналіз інцидентів включає збирання та аналіз логів, дослідження артефактів атаки, встановлення хронології подій, визначення використаних інструментів та техніків зловмисників.

Метод бенчмаркінгу передбачає порівняння практик інформаційної безпеки організації з кращими практиками галузі або провідних організацій [60]. Бенчмаркінг дозволяє виявити прогалини у власних практиках, визначити напрями вдосконалення, запозичити успішний досвід. Для публічного управління особливо цінним є міжнародний бенчмаркінг, що дозволяє вивчати досвід країн з розвиненими системами інформаційної безпеки.

Метод SWOT-аналізу застосовується для комплексної оцінки стану інформаційної безпеки через виявлення сильних сторін (Strengths), слабких сторін (Weaknesses), можливостей (Opportunities) та загроз (Threats) [93]. SWOT-аналіз дозволяє побачити цілісну картину, поєднуючи внутрішні

фактори (сильні та слабкі сторони) та зовнішні фактори (можливості та загрози).

Інструменти аналізу інформаційної безпеки передбачають як програмні засоби, так і методичні документи, стандарти та фреймворки.

До програмних інструментів належать: сканери вразливостей (Nessus, OpenVAS), які автоматично виявляють технічні вразливості в інформаційних системах; системи управління інформацією та подіями безпеки (SIEM – Security Information and Event Management), які збирають та аналізують великі обсяги даних про події безпеки; системи виявлення та запобігання вторгненням (IDS/IPS), які моніторять мережевий трафік та виявляють підозрілу активність; інструменти аналізу шкідливого програмного забезпечення; засоби криптографічного аналізу.

Методичними інструментами є міжнародні стандарти та фреймворки у сфері інформаційної безпеки. Серія стандартів ISO/IEC 27000 надає комплексний підхід до управління інформаційною безпекою, включаючи вимоги до систем управління інформаційною безпекою (ISMS), рекомендації з оцінки ризиків, керівництва з впровадження заходів захисту [99].

Фреймворк NIST Cybersecurity Framework, розроблений Національним інститутом стандартів і технологій США, надає структурований підхід до управління кіберризиками через п’ять ключових функцій: ідентифікація (Identify), захист (Protect), виявлення (Detect), реагування (Respond), відновлення (Recover) [74].

Фреймворк COBIT (Control Objectives for Information and Related Technologies) зосереджується на управлінні та аудиті IT-систем, включаючи аспекти інформаційної безпеки. Модель зрілості процесів інформаційної безпеки дозволяє оцінити рівень розвитку практик безпеки в організації та визначити напрями вдосконалення.

Для аналізу специфічних загроз кібербезпеки використовується фреймворк MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge), який систематизує тактики та техніки кіберзловмисників на

основі аналізу реальних атак. Цей фреймворк дозволяє організаціям краще розуміти, як діють зловмисники, і розробляти відповідні контрзаходи.

Важливим інструментом аналізу є *показники та метрики інформаційної безпеки*. До ключових показників належать: кількість виявлених інцидентів інформаційної безпеки за період; час виявлення інциденту (mean time to detect); час реагування на інцидент (mean time to respond); кількість критичних вразливостей; відсоток усунених вразливостей; рівень дотримання політик безпеки; рівень обізнаності персоналу з питань інформаційної безпеки; витрати на інформаційну безпеку як частка від IT-бюджету; збитки від інцидентів інформаційної безпеки.

Ці показники дозволяють кількісно оцінити стан інформаційної безпеки, відстежувати динаміку змін, порівнювати різні організації, обґрунтовувати інвестиції в інформаційну безпеку. Однак важливо розуміти обмеження кількісних метрик – вони не завжди відображають реальний рівень захищеності, оскільки деякі аспекти безпеки важко виміряти чисельно [84].

Методика комплексного аналізу інформаційної безпеки публічного управління може включати такі етапи:

- Підготовчий етап: визначення цілей та завдань аналізу, формування робочої групи, планування робіт, збирання вихідних даних.
- Інвентаризація інформаційних активів: ідентифікація та опис інформаційних ресурсів, інформаційних систем, інформаційної інфраструктури органу публічної влади.
- Класифікація інформаційних активів за рівнем критичності та цінності з урахуванням їх значення для виконання функцій органу влади.
- Ідентифікація загроз: виявлення потенційних загроз інформаційній безпеці, включаючи зовнішні та внутрішні загрози, технічні, організаційні та соціальні загрози [36; 46].
- Виявлення вразливостей: аналіз слабких місць в інформаційних системах, організаційних процедурах, кадровому забезпеченні, що можуть бути використані для реалізації загроз.

– Оцінка ризиків: визначення ймовірності реалізації загроз, оцінка можливих наслідків, розрахунок рівня ризику для кожного інформаційного активу.
– Аналіз існуючих заходів захисту: оцінка ефективності впроваджених технічних засобів захисту, організаційних процедур, навчання персоналу.
– Виявлення прогалин у захисті: порівняння існуючого стану захищеності з вимогами стандартів, нормативних актів, кращих практик.
– Розробка рекомендацій: обґрунтування пріоритетних заходів з підвищення рівня інформаційної безпеки, розрахунок необхідних ресурсів, планування впровадження.
– Підготовка звіту: документування результатів аналізу, формулювання висновків та рекомендацій для керівництва.

Особливістю аналізу інформаційної безпеки у публічному управлінні є необхідність врахування специфіки державного сектору: багатоманітність та взаємозв'язок інформаційних систем різних органів влади; наявність інформації, що становить державну таємницю; високі вимоги до доступності інформаційних систем через потребу забезпечення безперервності надання публічних послуг; обмеження у фінансуванні; складні процедури закупівель; необхідність прозорості та підзвітності [17].

Важливим аспектом методології аналізу інформаційної безпеки у публічному управлінні є *врахування людського фактору* [53]. Дослідження показують, що значна частина інцидентів інформаційної безпеки пов'язана з помилками персоналу, недостатньою обізнаністю, порушенням процедур або навмисними діями інсайдерів. Тому аналіз має включати оцінку рівня обізнаності державних службовців з питань інформаційної безпеки, їх дотримання політик та процедур, наявність програм навчання та підвищення кваліфікації.

Сучасні тенденції розвитку методології аналізу інформаційної безпеки пов'язані з використанням *технологій штучного інтелекту та великих даних* [33; 34; 35]. Машинне навчання дозволяє автоматично виявляти аномалії в поведінці користувачів та систем, прогнозувати можливі атаки,

аналізувати величезні обсяги логів та подій безпеки. Технології Big Data надають можливість обробляти та аналізувати різнорідні дані з множини джерел для виявлення складних багатоступеневих атак.

Таким чином, методологія аналізу інформаційної безпеки у публічному управлінні базується на чітких принципах, включає різноманітні методи та інструменти, вимагає системного, комплексного та динамічного підходу. Ефективний аналіз є основою для прийняття обґрунтованих рішень щодо вдосконалення системи інформаційної безпеки та раціонального розподілу обмежених ресурсів на захист найбільш критичних інформаційних активів.

РОЗДІЛ 2. СУЧАСНІ ЗАГРОЗИ ТА ВИКЛИКИ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ ПУБЛІЧНОГО УПРАВЛІННЯ В УКРАЇНІ

2.1. Вплив кібератак та інформаційних кампаній на ефективність державного управління

Кібератаки та інформаційні кампанії є одними з найбільш серйозних загроз для ефективності публічного управління в сучасних умовах. Ці загрози набувають особливої гостроти для України в контексті гібридної війни, яку Російська Федерація веде з 2014 року, та повномасштабної військової агресії, розпочатої у лютому 2022 року.

Типологія кібератак на системи публічного управління включає різноманітні види зловмисної діяльності. DDoS-атаки (розподілені атаки типу «відмова в обслуговуванні») спрямовані на перевантаження інформаційних систем та мереж з метою зробити їх недоступними для легітимних користувачів [20]. Такі атаки можуть паралізувати роботу веб-сайтів органів влади, систем електронного урядування, критично важливих інформаційних систем.

Під час повномасштабної війни Україна зіткнулася з безпрецедентною хвилею DDoS-атак на державні ресурси [21]. Атаки на сайти міністерств, державних служб, банківської системи мали на меті дезорганізувати роботу держави та посіяти паніку серед населення. Однак завдяки скоординованим зусиллям фахівців з кібербезпеки, підтримці міжнародних партнерів та волонтерської спільноти вдалося мінімізувати наслідки цих атак.

Атаки з використанням шкідливого програмного забезпечення включають віруси, троянські програми, програми-шифрувальники (ransomware), шпигунське ПЗ тощо [19]. Зловмисне ПЗ може використовуватися для крадіжки конфіденційної інформації, знищення даних, блокування доступу до систем з вимогою викупу, створення прихованих каналів управління зламаними системами.

Особливо небезпечними є цільові атаки (Advanced Persistent Threats, APT), які проводяться добре організованими групами, часто пов’язаними з державними структурами інших країн [76]. Такі атаки характеризуються тривалою підготовкою, використанням складних технік, націленістю на конкретні об’єкти. APT-групи можуть місяцями перебувати в зламаних системах, збираючи розвідувальну інформацію та очікуючи найбільш сприятливого моменту для завдання максимальної шкоди.

Атаки на ланцюги постачання (supply chain attacks) передбачають компрометацію програмного забезпечення, обладнання або послуг, які використовуються органами влади. Зловмисники можуть впровадити шкідливий код у легітимне програмне забезпечення на етапі його розробки або оновлення, що дозволяє отримати доступ до систем усіх організацій, які використовують це ПЗ.

Фішингові атаки використовують соціальну інженерію для обману користувачів з метою отримання конфіденційної інформації (паролів, ключів доступу) або встановлення зловмисного ПЗ. Фішингові електронні листи можуть маскуватися під офіційні повідомлення, використовувати актуальну тематику для підвищення довіри жертв.

Масштаби та наслідки кібератак на системи публічного управління можуть бути катастрофічними. Успішна кібератака може призвести до витоку конфіденційної інформації, включаючи державну таємницю, персональні дані громадян, комерційну таємницю. Втрата контролю над критично важливими інформаційними системами може паралізувати роботу органів влади, зірвати надання публічних послуг, порушити функціонування критичної інфраструктури.

Кібератаки на енергетичну інфраструктуру України в 2015 та 2016 роках продемонстрували уразливість критичних систем та можливість реальних фізичних наслідків від кіберінцидентів. Атаки призвели до знеструмлення сотень тисяч споживачів, показали здатність зловмисників впливати на промислові системи керування.

Економічні збитки від кібератак включають прямі витрати на відновлення систем, втрату даних, простої у роботі, а також непрямі витрати, пов’язані з репутаційними ризиками, втратою довіри громадян, зниженням інвестиційної привабливості. За оцінками експертів, глобальні збитки від кіберзлочинності сягають сотень мільярдів доларів щорічно.

Інформаційні кампанії як інструмент впливу на публічне управління включають координовані дії з поширення дезінформації, пропаганди, маніпулятивного контенту з метою формування потрібних настроїв у суспільстві, підриву довіри до влади, дестабілізації політичної ситуації [36]. Інформаційні кампанії є важливою складовою гібридної війни.

Російська Федерація систематично проводить інформаційні операції проти України, спрямовані на деморалізацію населення, підрив довіри до державних інституцій, поглиблення суспільних розколів, виправдання агресії. Ці операції використовують контрольовані Кремлем ЗМІ, соціальні мережі, ботів та тролів, псевдоекспертів та агентів впливу.

Типові наративи російської пропаганди включають: заперечення української ідентичності та державності; звинувачення України у «русофобії» та «фашизмі»; дискредитацію європейського та євроатлантичного вибору України; поширення панічних настроїв щодо економічної ситуації; провокування міжконфесійних та міжетнічних конфліктів.

Механізми впливу інформаційних кампаній на ефективність публічного управління є багатовимірними. По-перше, підрив довіри до влади ускладнює комунікацію між державою та громадянами, знижує легітимність управлінських рішень, провокує соціальну напруженість. Коли громадяни не довіряють офіційній інформації, вони стають більш схильними до маніпуляцій з боку ворожих акторів.

По-друге, дезінформація може безпосередньо впливати на процес прийняття рішень. Якщо особи, які приймають рішення, спираються на викривлену або неправдиву інформацію, це може призвести до хибних рішень з негативними наслідками. Дезінформація про епідеміологічну ситуацію,

економічні показники, міжнародну ситуацію може дезорієнтувати органи влади.

По-третє, інформаційні кампанії створюють додаткове навантаження на державні структури, які змушені витрачати ресурси на спростування фейків, протидію пропаганді, відновлення довіри замість зосередження на виконанні основних функцій. Це знижує загальну ефективність державного управління.

Соціальні мережі відіграють ключову роль у сучасних інформаційних кампаніях. Вони дозволяють швидко поширювати контент серед великої аудиторії, таргетувати повідомлення на конкретні групи, використовувати алгоритми для максимізації охоплення. Водночас соціальні мережі стали полем битви за інформаційний простір.

Боти та тролі використовуються для штучного посилення певних наративів, створення ілюзії масової підтримки певних позицій, атак на опонентів. Автоматизовані акаунти можуть генерувати величезні обсяги контенту, маніпулювати трендами, формувати штучну повістку дня. Виявлення та блокування ботів є складним технічним завданням, оскільки вони постійно вдосконалюються.

Дипфейки (deepfakes) – синтетичні медіа, створені з використанням технологій штучного інтелекту, які можуть імітувати голос, обличчя та поведінку реальних людей – представляють нову загрозу. Дипфейки можуть використовуватися для створення фальшивих заяв політиків, підробки доказів, дискредитації опонентів. З розвитком технологій виявлення дипфейків стає все складнішим.

Вплив на демократичні процеси є особливо небезпечним аспектом інформаційних кампаній. Вибори, референдуми та інші форми демократичного волевиявлення стають мішенями для інформаційних маніпуляцій, спрямованих на вплив на результати голосування. Дезінформація про кандидатів, програми, процедури голосування може спотворити вибір громадян.

Протидія кібератакам та інформаційним кампаніям вимагає комплексного підходу. На технологічному рівні необхідне постійне вдосконалення систем кіберзахисту, впровадження сучасних технологій виявлення та нейтралізації загроз, регулярне оновлення програмного забезпечення, використання багатофакторної автентифікації, шифрування даних.

На організаційному рівні критично важливим є підвищення обізнаності державних службовців з питань кібергігієни, дотримання процедур безпеки, регулярне проведення навчань та тренінгів з реагування на інциденти. Людський фактор залишається одним з найслабших ланок у ланцюгу безпеки.

На стратегічному рівні необхідна координація зусиль різних державних органів, співпраця з приватним сектором, міжнародне співробітництво. Створення ситуаційних центрів, команд реагування на інциденти, систем раннього попередження дозволяє швидше виявляти та нейтралізувати загрози.

Протидія інформаційним кампаніям вимагає розвитку стратегічних комунікацій, медіаграмотності населення, ефективного спростування дезінформації, співпраці з соціальними мережами для видалення маніпулятивного контенту. Важливим є баланс між протидією дезінформації та збереженням свободи слова.

Таким чином, кібератаки та інформаційні кампанії створюють серйозні виклики для ефективності публічного управління. Вони здатні порушити функціонування критичних систем, викрасти конфіденційну інформацію, підірвати довіру до влади, вплинути на процес прийняття рішень. Ефективна протидія цим загрозам вимагає постійної пильності, інвестицій у кіберзахист, розвитку компетентностей персоналу та координації зусиль на національному та міжнародному рівнях.

2.2. Ризики витоку, підробки та маніпулювання інформацією у цифрових комунікаціях органів влади

Цифровізація комунікацій органів публічної влади, впровадження електронного документообігу, електронних послуг, використання хмарних технологій створюють нові канали для витоку, підробки та маніпулювання інформацією. Ці ризики мають специфічний характер і потребують особливої уваги з огляду на чутливість інформації, якою оперують державні структури.

Витік інформації є однією з найсерйозніших загроз інформаційній безпеці публічного управління. Витік може відбуватися через різні канали та з різних причин. Технічні вразливості інформаційних систем дозволяють зловмисникам отримати несанкціонований доступ до баз даних, серверів, мереж. Незахищені API, застарілі протоколи, невиправлені вразливості створюють лазівки для проникнення.

Інсайдерська загроза, коли витік здійснюється власними співробітниками організації, є особливо небезпечною. Інсайдери мають легітимний доступ до систем та інформації, знають внутрішні процедури, можуть діяти непомітно тривалий час. Мотивами інсайдерів можуть бути фінансова вигода, ідеологічні переконання, помста, шантаж або просто недбалість.

Соціальна інженерія дозволяє зловмисникам маніпулювати людьми для отримання доступу до інформації. Через фішинг, претекстинг, підкуп або шантаж зловмисники можуть змусити співробітників розкрити паролі, надати доступ до систем, передати конфіденційні документи.

Наслідки витоку інформації для публічного управління можуть бути катастрофічними. Розголошення інформації, що становить державну таємницю, загрожує національній безпеці, може завдати шкоди обороноздатності, дипломатичним відносинам, економічним інтересам держави. Витік персональних даних громадян порушує їхні конституційні права, може призвести до шахрайства, шантажу, дискримінації.

Витік службової інформації може підірвати ефективність діяльності органів влади, розкрити стратегію дій, зашкодити переговорним позиціям. Передчасне розголошення проектів рішень, аналітичних матеріалів, службових записок може бути використане для протидії впровадженню реформ, лобіювання вузькогрупових інтересів.

Репутаційні наслідки витоку інформації включають втрату довіри громадян, критику з боку міжнародних партнерів, політичні кризи. Організація, яка не може захистити конфіденційну інформацію, ставить під сумнів свою спроможність виконувати покладені на неї функції.

Підробка інформації у цифрових комунікаціях стала технічно простішою з розвитком технологій. Підробка електронних документів, електронних підписів, службової кореспонденції може використовуватися для різних зловмисних цілей. Фальсифіковані документи можуть використовуватися для незаконного отримання доступу до ресурсів, проведення шахрайських операцій, дискредитації посадових осіб.

Особливу небезпеку представляє підробка офіційних повідомлень органів влади. Фальшиві розпорядження, накази, листи, які виглядають автентичними, можуть ввести в оману інші органи влади, підприємства, громадян. У критичних ситуаціях, таких як надзвичайні стани або воєнний стан, підроблені розпорядження можуть спричинити хаос.

Механізми захисту від підробки включають використання кваліфікованих електронних підписів, які забезпечують автентичність відправника та цілісність документа [27]. Впровадження систем електронного документообігу з вбудованими механізмами криптографічного захисту дозволяє виявляти спроби несанкціонованих змін.

Технології блокчейн можуть використовуватися для створення незмінних записів про документи та транзакції, що ускладнює підробку. Децентралізований характер блокчейну робить практично неможливою зміну даних без виявлення.

Маніпулювання інформацією у цифрових комунікаціях може набувати різних форм. Вибіркове цитування, вирвання фраз з контексту, підміна акцентів дозволяють спотворити зміст повідомлень без прямої підробки. Такі маніпуляції особливо небезпечні, коли їх важко виявити та спростувати.

Маніпулювання статистичними даними через некоректне представлення, вибіркові вибірки, зміну методології підрахунків може створювати хибне враження про стан справ. Органи влади, які спираються на такі дані, можуть приймати неоптимальні рішення.

Темпоральні маніпуляції, коли старі дані видаються за актуальні або навпаки, можуть дезорієнтувати. Публікація застарілої інформації про критичні ситуації, економічні показники, політичні події може мати серйозні наслідки.

Ризики використання хмарних технологій заслуговують окремої уваги. Хмарні сервіси надають переваги у вигляді масштабованості, доступності, зниження витрат, але водночас створюють нові ризики [32]. Розміщення даних на серверах третіх сторін означає часткову втрату контролю над інформацією.

Юрисдикційні ризики виникають, коли дані розміщуються на серверах, що знаходяться в інших країнах. Законодавство цих країн може вимагати надання доступу до даних правоохоронним органам, спецслужбам. Це створює ризики для конфіденційності державної інформації.

Залежність від провайдера хмарних послуг означає, що технічні проблеми, банкрутство, зміна умов обслуговування можуть порушити доступ до критично важливих даних та систем. Вибір надійних провайдерів, диверсифікація, регулярне резервне копіювання є важливими заходами мінімізації ризиків.

Захист інформації у цифрових комунікаціях вимагає комплексу технічних та організаційних заходів. Шифрування даних при передачі та зберіганні є базовою вимогою. Використання надійних криптографічних алгоритмів, регулярна зміна ключів, захищені протоколи комунікацій забезпечують конфіденційність інформації.

Управління доступом на основі принципу найменших привілеїв означає, що користувачі отримують доступ лише до тієї інформації, яка необхідна для виконання їхніх службових обов'язків [36]. Рольова модель доступу, багаторівнева автентифікація, регулярний перегляд прав доступу допомагають мінімізувати ризики несанкціонованого доступу.

Моніторинг та аудит дій користувачів дозволяють виявляти підозрілу активність, несанкціоновані спроби доступу, порушення політик безпеки. Системи SIEM збирають та аналізують великі обсяги даних про події безпеки, виявляють аномалії, генерують сповіщення про потенційні інциденти.

Класифікація інформації за рівнями конфіденційності дозволяє диференціювати заходи захисту відповідно до цінності та чутливості інформації. Критично важлива інформація потребує найсуворіших заходів захисту, тоді як публічна інформація може мати мінімальні обмеження.

Організаційні заходи включають розробку та впровадження політик інформаційної безпеки, регламентів роботи з конфіденційною інформацією, процедур реагування на інциденти. Навчання персоналу, регулярні інструктажі, тестування знань забезпечують обізнаність співробітників з вимогами безпеки.

Перевірка благонадійності при прийнятті на роботу, особливо на посади з доступом до конфіденційної інформації, допомагає зменшити інсайдерські ризики. Моніторинг поведінки співробітників, виявлення ознак можливої нелояльності, створення атмосфери довіри та поваги сприяють попередженню інсайдерських загроз.

Таким чином, ризики витоку, підробки та маніпулювання інформацією у цифрових комунікаціях органів влади вимагають постійної уваги та систематичних зусиль з їх мінімізації. Комплексний підхід, що поєднує технічні засоби захисту, організаційні процедури, навчання персоналу, є необхідною умовою забезпечення конфіденційності, цілісності та доступності інформації в системі публічного управління.

2.3. Проблеми захисту критичної інформаційної інфраструктури в умовах гібридних війн

Критична інформаційна інфраструктура є сукупністю інформаційних систем, мереж та інформаційних ресурсів, порушення функціонування яких може мати серйозні негативні наслідки для національної безпеки, економіки, здоров'я та безпеки населення. В умовах гібридної війни захист критичної інформаційної інфраструктури набуває стратегічного значення.

Сектори критичної інфраструктури включають енергетику, транспорт, фінансовий сектор, охорону здоров'я, водопостачання, телекомунікації, державне управління. Кожен з цих секторів значною мірою залежить від інформаційних технологій, що робить їх вразливими до кіберзагроз.

Енергетичний сектор є одним з найбільш критичних, оскільки від нього залежить функціонування всієї економіки та життєдіяльність населення. Системи диспетчерського управління та збору даних (SCADA), промислові системи керування (ICS) використовуються для управління електростанціями, електромережами, нафтогазовими об'єктами. Кібератаки на ці системи можуть призвести до масштабних відключень електроенергії, аварій, екологічних катастроф.

Транспортна інфраструктура, включаючи залізничний, авіаційний, морський транспорт, також критично залежить від інформаційних систем. Системи управління рухом, диспетчеризації, продажу квитків, логістики є потенційними мішенями для кібератак. Порушення їх роботи може паралізувати транспортне сполучення, спричинити аварії.

Фінансовий сектор є привабливою мішенню для кіберзловмисників через можливість прямого фінансового зиску. Атаки на банківські системи, платіжні системи, біржі можуть призвести до крадіжок коштів, порушення функціонування фінансової системи, підриву довіри до банків.

Специфіка загроз в умовах гібридної війни полягає в тому, що кібератаки є частиною координованої стратегії, спрямованої на дестабілізацію

держави [42]. На відміну від звичайної кіберзлочинності, метою якої є фінансова вигода, кібератаки в рамках гібридної війни мають політичні та стратегічні цілі.

Росія систематично проводить кібератаки на критичну інфраструктуру України [21]. Атаки на енергетичний сектор у 2015-2016 роках, атаки на державні установи, використання деструктивного зловмисного ПЗ NotPetya та BadRabbit демонструють цілеспрямованість та масштаб загрози.

Координація кібератак з іншими елементами гібридної війни – інформаційними операціями, економічним тиском, військовими провокаціями – підсилює їх ефект. Кібератака, проведена одночасно з інформаційною кампанією, може створити паніку, посилити суспільну напруженість, підірвати довіру до влади.

Вразливості критичної інформаційної інфраструктури мають об'єктивний характер та зумовлені кількома факторами. Застарілість обладнання та програмного забезпечення в багатьох секторах критичної інфраструктури створює численні вразливості. Промислові системи керування часто використовують застарілі операційні системи, для яких більше не випускаються оновлення безпеки.

Взаємозв'язок та взаємозалежність різних секторів критичної інфраструктури означає, що порушення в одному секторі може спричинити каскадний ефект в інших. Припинення електропостачання впливає на роботу транспорту, телекомунікацій, охорони здоров'я.

Людський фактор залишається одним з найслабших ланок. Помилки персоналу, недостатня обізнаність з питань кібербезпеки, порушення процедур можуть призвести до компрометації систем. Соціальна інженерія ефективно експлуатує ці слабкості.

Нормативно-правове регулювання захисту критичної інфраструктури в Україні перебуває в процесі розвитку. Закон України «Про основні засади забезпечення кібербезпеки України» визначає правові основи захисту критичної інфраструктури [63]. Постанова Кабінету Міністрів України «Про

затвердження Загальних вимог до кіберзахисту об’єктів критичної інфраструктури» встановлює мінімальні технічні та організаційні вимоги [69].

Однак повноцінна імплементація цих вимог вимагає значних зусиль та ресурсів. Необхідні інвентаризація об’єктів критичної інфраструктури, оцінка ризиків, розробка планів забезпечення кіберзахисту, впровадження технічних засобів, навчання персоналу, регулярні перевірки та аудити.

Технічні заходи захисту критичної інфраструктури включають сегментацію мереж, що передбачає розділення промислових мереж від корпоративних та ізоляцію критичних систем. Це обмежує можливість поширення зловмисного ПЗ та несанкціонованого доступу.

Системи виявлення та запобігання вторгненням (IDS/IPS) моніторять мережевий трафік, виявляють підозрілу активність, блокують атаки. Спеціалізовані рішення для промислових мереж враховують специфіку промислових протоколів та обладнання.

Регулярне оновлення програмного забезпечення та виправлення вразливостей є базовою, але критично важливою практикою. Для застарілих систем, для яких оновлення недоступні, необхідні компенсаційні заходи – ізоляція, додатковий моніторинг, обмеження функціональності.

Резервування критичних систем та створення планів забезпечення безперервності діяльності дозволяють продовжувати функціонування навіть у разі компрометації основних систем. Регулярне тестування цих планів забезпечує їх дієвість у реальних умовах.

Організаційні заходи включають створення центрів реагування на кіберінциденти (CERT/CSIRT) у секторах критичної інфраструктури. Ці центри забезпечують моніторинг загроз, координацію реагування на інциденти, обмін інформацією про загрози.

Державно-приватне партнерство є необхідною умовою ефективного захисту критичної інфраструктури, оскільки значна її частина належить приватним компаніям. Обмін інформацією про загрози, координація зусиль, спільні навчання підвищують загальний рівень захищеності.

Регулярні навчання та тренінги з реагування на кіберінциденти дозволяють відпрацьовувати процедури, виявляти слабкі місця, підвищувати готовність персоналу. Кіберучення на національному рівні залучають різні сектори та державні органи для відпрацювання координації у кризових ситуаціях.

Міжнародне співробітництво є важливим аспектом захисту критичної інфраструктури. Обмін інформацією про загрози, кращі практики, технічна допомога від міжнародних партнерів підвищують спроможності України. Участь у міжнародних ініціативах з кібербезпеки, співпраця з НАТО, ЄС, окремими країнами сприяє зміцненню захисту [67].

Волонтерська ІТ-спільнота світу також надала безпрецедентну підтримку Україні під час повномасштабної війни. ІТ-армія України, міжнародні хакери-активісти, компанії кібербезпеки безкоштовно надавали послуги захисту, моніторингу загроз, реагування на інциденти. Це продемонструвало солідарність глобальної спільноти та важливість неурядового співробітництва.

Таким чином, захист критичної інформаційної інфраструктури в умовах гібридної війни є комплексним завданням, що вимагає технічних, організаційних, правових та міжнародних заходів. Підвищення стійкості критичної інфраструктури до кіберзагроз є пріоритетом національної безпеки України та вимагає постійних зусиль і значних інвестицій.

2.4. Соціальні мережі як фактор інформаційної вразливості та інструмент впливу на публічне управління

Соціальні мережі стали невід’ємною частиною сучасного інформаційного простору та відіграють подвійну роль у контексті інформаційної безпеки публічного управління. З одного боку, вони є важливим каналом комунікації між владою та громадянами, інструментом публічної дипломатії, засобом оперативного інформування. З іншого боку,

соціальні мережі створюють нові вразливості та можуть використовуватися як інструмент деструктивного впливу на суспільство та державні інституції.

Роль соціальних мереж у сучасному інформаційному просторі неможливо переоцінити. За даними досліджень, переважна більшість українців регулярно користуються соціальними мережами, отримуючи через них значну частину інформації про поточні події. Facebook, Instagram, Telegram, TikTok, X (колишній Twitter) стали основними платформами для обміну інформацією, формування громадської думки, мобілізації суспільних рухів.

Органи публічної влади активно використовують соціальні мережі для комунікації з громадянами. Офіційні сторінки міністерств, відомств, посадових осіб надають оперативну інформацію про свою діяльність, реагують на звернення громадян, роз'яснюють політику. Соціальні мережі дозволяють владі бути ближчою до громадян, отримувати зворотний зв'язок, формувати позитивний імідж.

Однак ризики та вразливості, пов'язані з використанням соціальних мереж, є значними. Поширення дезінформації та фейків у соціальних мережах набуло масштабів епідемії [10]. Швидкість поширення неправдивої інформації часто перевищує швидкість її спростування. Емоційно забарвлені, шокуючі фейки розповсюджуються вірусно, охоплюючи мільйони користувачів за короткий час.

Механізми алгоритмічної видачі контенту в соціальних мережах сприяють формуванню «інформаційних бульбашок» та «ехо-камер», де користувачі бачать переважно контент, що підтверджує їхні існуючі погляди. Це поглиблює поляризацію суспільства, утруднює конструктивний діалог, робить людей більш сприйнятливими до маніпуляцій.

Технології маніпулювання в соціальних мережах постійно вдосконалюються. Автоматизовані акаунти (боти) використовуються для штучного посилення певних повідомлень, створення ілюзії масової підтримки,

атак на опонентів. Боти можуть генерувати контент, коментувати публікації, маніпулювати трендами, формувати штучну повістку дня.

Тролі – особи, які навмисно провокують конфлікти, поширюють ненависть, дискредитують опонентів – отримали в соціальних мережах потужний інструмент впливу [10]. Координовані тролінгові кампанії можуть цілеспрямовано атакувати державних службовців, політиків, активістів, створюючи токсичну атмосферу та змушуючи їх припинити активність.

Мікротаргетинг дозволяє доставляти персоналізовані повідомлення конкретним групам користувачів на основі їхніх демографічних характеристик, інтересів, поведінки. Ця технологія може використовуватися для легітимних цілей, але також для маніпуляцій, коли різним групам показуються суперечливі повідомлення, розпалюються конфлікти.

Дезінформаційні кампанії в соціальних мережах мають системний характер і часто є частиною більш широких інформаційних операцій [36]. Російська Федерація систематично використовує соціальні мережі для проведення деструктивних кампаній проти України. Ці кампанії спрямовані на деморалізацію населення, підрив довіри до влади, поглиблення суспільних розколів, поширення паніки.

Типові теми російської дезінформації в соціальних мережах включають: заперечення української державності та ідентичності; дискредитацію української влади та силових структур; поширення панічних настроїв щодо економічної та гуманітарної ситуації; провокування міжконфесійних та міжетнічних конфліктів; підрив довіри до західних партнерів України.

Вплив на процес прийняття рішень є серйозною проблемою. Органи влади, аналізуючи настрої в соціальних мережах, можуть отримувати спотворену картину реальності. Штучно створена активність ботів може сприйматися як прояв реальної громадської думки, що впливає на політичні рішення.

Інформаційний тиск через соціальні мережі може змушувати владу приймати популістські рішення, відступати від довгострокових стратегічних

цілей заради короткострокового заспокоєння громадської думки. Це особливо небезпечно, коли хвиля обурення в соціальних мережах штучно створюється зловмисниками.

Загрози для державних службовців у соціальних мережах включають витік конфіденційної інформації через необережні публікації. Державні службовці, які діляться у соціальних мережах деталями своєї роботи, місцезнаходження, контактами, створюють можливості для збору розвідувальної інформації, соціальної інженерії, цільових атак.

Дискредитаційні кампанії проти державних службовців можуть включати поширення неправдивої інформації, компрометуючих матеріалів (реальних або сфабрикованих), кібербулінг [28]. Це створює психологічний тиск, може змушувати осіб залишати державну службу, утримувати талановитих фахівців від приходу в публічний сектор.

Фішинг через соціальні мережі дозволяє зловмисникам встановлювати довіру через тривалу взаємодію, а потім використовувати її для отримання конфіденційної інформації або впровадження зловмисного програмного забезпечення.

Протидія деструктивному впливу через соціальні мережі вимагає комплексного підходу. На технологічному рівні необхідне впровадження систем моніторингу та аналізу інформаційного простору соціальних мереж. Штучний інтелект та машинне навчання можуть використовуватися для виявлення ботів, розпізнавання дезінформації, відстеження координованих кампаній [34].

Співпраця з платформами соціальних мереж є критично важливою. Facebook, Google, Twitter та інші компанії мають технічні можливості та доступ до даних для виявлення та блокування зловмисних акаунтів, видалення дезінформації, припинення координованих маніпулятивних кампаній [54]. Під час повномасштабної війни багато платформ посилили свої зусилля з протидії російській дезінформації.

Стратегічні комунікації держави мають бути проактивними, а не реактивними. Замість постійного спростування фейків, що є вичерпною стратегією, необхідно формувати власну позитивну повістку, насичувати інформаційний простір достовірною та релевантною інформацією, будувати довіру через прозорість та підзвітність.

Центр протідії дезінформації при РНБО України здійснює систематичну роботу з виявлення та спростування дезінформації, координує зусилля різних державних органів, співпрацює з громадським сектором та міжнародними партнерами [82].

Медіаграмотність населення є довгостроковою інвестицією в інформаційну безпеку суспільства [83]. Здатність критично оцінювати інформацію, перевіряти джерела, розпізнавати маніпуляції робить громадян менш вразливими до дезінформації. Навчання медіаграмотності має впроваджуватися в освітніх закладах, через публічні кампанії, тренінги для різних аудиторій.

Правове регулювання діяльності в соціальних мережах є складним питанням, що вимагає балансу між протидією зловживанням та захистом свободи слова. Надмірні обмеження можуть створити ризики для демократії, тоді як відсутність регулювання дозволяє безконтрольне поширення дезінформації.

Європейський підхід, закріплений у Акті про цифрові послуги (Digital Services Act), передбачає відповідальність платформ за контент, що поширюється через них, з одночасним збереженням принципів свободи слова [71]. Україні доцільно орієнтуватися на європейські стандарти при розробці власного законодавства.

Рекомендації для державних службовців щодо безпечного використання соціальних мереж включають: не публікувати конфіденційну інформацію або деталі службової діяльності; використовувати надійні паролі та двофакторну автентифікацію; бути обережними при прийнятті запитів на дружбу від

незнайомих осіб; критично оцінювати інформацію перед її поширенням; повідомляти про підозрілу активність відповідним службам.

Офіційні акаунти державних органів у соціальних мережах мають бути верифікованими, щоб уникнути підробок. Всі публікації мають проходити перевірку перед розміщенням, щоб запобігти випадковому розголошенню чутливої інформації.

Таким чином, соціальні мережі є потужним інструментом комунікації, але водночас створюють значні виклики для інформаційної безпеки публічного управління. Дезінформація, маніпуляції, цільові атаки через соціальні мережі вимагають постійної пильності, розвитку спроможностей виявлення та протидії загрозам, підвищення медіаграмотності, балансу між безпекою та свободою слова. Ефективне використання можливостей соціальних мереж при мінімізації ризиків є важливим завданням для органів публічної влади в цифрову епоху.

РОЗДІЛ 3. НАПРЯМИ ТА ПЕРСПЕКТИВИ РОЗВИТКУ СИСТЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПУБЛІЧНОГО УПРАВЛІННЯ

3.1. Стратегічні орієнтири державної політики у сфері інформаційної безпеки

Формування ефективної державної політики у сфері інформаційної безпеки є критично важливим завданням для України в контексті викликів цифрової епохи та гібридної війни. Стратегічні орієнтири цієї політики визначають довгострокові цілі, пріоритети та механізми забезпечення захисту інформаційного простору держави.

Концептуальні засади державної політики у сфері інформаційної безпеки закладено в низці стратегічних документів. Стратегія національної безпеки України визначає інформаційну безпеку як один з пріоритетів національної безпеки і наголошує на необхідності захисту інформаційного простору, протидії дезінформації та пропаганді, забезпечення кібербезпеки [68].

Доктрина інформаційної безпеки України формулює основні напрями державної політики: забезпечення інформаційного суверенітету; захист інформаційного простору та протидія руйнівним інформаційним впливам; розвиток інформаційного суспільства та інформаційної інфраструктури; захист інформаційних ресурсів держави [65].

Стратегія кібербезпеки України визначає пріоритетні напрями: захист критичної інформаційної інфраструктури; розвиток спроможностей кіберзахисту; розбудова національної системи кіберзахисту; міжнародне співробітництво; розвиток кадрового потенціалу; підвищення кіберобізнаності суспільства [67].

Пріоритетні напрями державної політики у сфері інформаційної безпеки включають кілька ключових векторів. По-перше, це зміцнення

інформаційного суверенітету України. Інформаційний суверенітет передбачає здатність держави контролювати національний сегмент інформаційного простору, приймати самостійні рішення щодо регулювання інформаційних процесів, захищати національні інформаційні ресурси від зовнішніх загроз [13].

Зміцнення інформаційного суверенітету вимагає розвитку національного виробництва контенту, підтримки української мови в цифровому просторі, забезпечення доступу громадян до різноманітних джерел інформації, протидії монополізації інформаційного ринку іноземними корпораціями. Важливим є також забезпечення технологічної незалежності через розвиток власних інформаційних технологій, зменшення критичної залежності від іноземних технологій.

По-друге, це забезпечення кіберстійкості держави. Кіберстійкість передбачає здатність держави функціонувати в умовах постійних кіберзагроз, швидко виявляти та нейтралізувати кібератаки, відновлювати порушені системи, навчатися на основі інцидентів [67]. Досвід повномасштабної війни показав критичну важливість кіберстійкості для забезпечення функціонування держави.

Підвищення кіберстійкості вимагає створення комплексної системи кіберзахисту, що включає технічні засоби, організаційні процедури, кваліфікований персонал, координацію між різними акторами. Необхідні інвестиції в модернізацію інформаційних систем, впровадження сучасних технологій захисту, розвиток спроможностей виявлення та реагування на інциденти.

По-третє, це протидія дезінформації та інформаційним маніпуляціям. Російська агресія супроводжується масштабними інформаційними операціями, спрямованими на деморалізацію українського суспільства, підрив довіри до влади, дискредитацію України на міжнародній арені [36]. Ефективна протидія вимагає не лише спростування фейків, а й формування позитивної повістки, розвиток стратегічних комунікацій, підвищення медіаграмотності.

По-четверте, це розвиток цифрової інфраструктури та електронного урядування при забезпеченні належного рівня безпеки. Цифровізація публічного управління створює нові можливості для підвищення ефективності, прозорості, доступності державних послуг [25]. Однак ці процеси мають супроводжуватися адекватними заходами захисту, щоб цифрові системи не стали новими вразливостями.

Цілі державної політики у сфері інформаційної безпеки визначаються виходячи з аналізу загроз та викликів. Довгостроковою метою є створення безпечного, відкритого, вільного інформаційного простору, що забезпечує реалізацію прав громадян на інформацію, сприяє демократичному розвитку суспільства, захищає національні інтереси.

Конкретні цілі включають: забезпечення захисту критичної інформаційної інфраструктури від кіберзагроз; мінімізацію ризиків витоку конфіденційної державної інформації; протидію дезінформаційним кампаніям та інформаційно-психологічним операціям; розвиток національного кіберпростору та цифрової економіки; підвищення рівня медіаграмотності та цифрової грамотності населення; інтеграцію України у світовий інформаційний простір при збереженні національної ідентичності.

Механізми реалізації державної політики мають бути комплексними та скоординованими. Нормативно-правовий механізм передбачає вдосконалення законодавства у сфері інформаційної безпеки, приведення його у відповідність з європейськими стандартами, усунення прогалин та суперечностей [50]. Необхідне прийняття нових законів у сферах захисту персональних даних, критичної інфраструктури, боротьби з дезінформацією.

Інституційний механізм передбачає розвиток та зміцнення інституцій, відповідальних за інформаційну безпеку. Це включає забезпечення належного фінансування, кадрового забезпечення, технічного оснащення відповідних органів. Важливим є чітке розмежування повноважень між різними органами, уникнення дублювання функцій, забезпечення ефективної координації.

Економічний механізм передбачає виділення достатніх бюджетних коштів на забезпечення інформаційної безпеки, стимулювання приватних інвестицій у цю сферу, підтримку національних компаній з кібербезпеки. Інвестиції в інформаційну безпеку мають розглядатися не як витрати, а як необхідна умова економічного розвитку та національної безпеки.

Освітньо-виховний механізм спрямований на формування культури інформаційної безпеки в суспільстві, підготовку кваліфікованих фахівців, підвищення обізнаності громадян з питань безпеки в цифровому середовищі [53]. Необхідне впровадження відповідних дисциплін у навчальні програми, проведення інформаційних кампаній, розвиток програм підвищення кваліфікації для державних службовців.

Роль міжнародного співробітництва у реалізації державної політики інформаційної безпеки є критично важливою. Інформаційні загрози мають транснаціональний характер і не можуть бути ефективно подолані зусиллями однієї держави. Міжнародна співпраця у сфері кібербезпеки, обмін інформацією про загрози, спільні навчання та операції підвищують колективну безпеку.

Для України пріоритетним є поглиблення співпраці з країнами НАТО та ЄС. Участь у програмах НАТО з кібероборони, імплементація європейських стандартів кібербезпеки, технічна допомога від партнерів сприяють зміцненню національних спроможностей [67]. Важливим є також розвиток двосторонніх відносин з країнами-лідерами у сфері кібербезпеки для обміну досвідом та технологіями.

Виклики та перешкоди на шляху реалізації державної політики інформаційної безпеки включають обмеженість фінансових ресурсів, дефіцит кваліфікованих кадрів, застарілість технічної інфраструктури, бюрократичні перешкоди, недостатню координацію між органами влади. В умовах війни ці виклики посилюються через необхідність перерозподілу ресурсів на оборонні потреби.

Подолання цих викликів вимагає системного підходу, політичної волі, залучення ресурсів міжнародних партнерів, ефективного державно-приватного партнерства. Важливим є встановлення чітких пріоритетів, фокусування на найбільш критичних напрямах, використання гнучких та швидких механізмів реагування на нові загрози.

Таким чином, стратегічні орієнтири державної політики у сфері інформаційної безпеки визначають комплексний, системний підхід до захисту інформаційного простору України. Успішна реалізація цієї політики є необхідною умовою забезпечення національної безпеки, демократичного розвитку, ефективного функціонування публічного управління в цифрову епоху.

3.2. Механізми цифрової трансформації та підвищення кіберстійкості органів публічної влади

Цифрова трансформація публічного управління є об'єктивним процесом, що відкриває нові можливості для підвищення ефективності, прозорості та якості державних послуг. Водночас цей процес створює нові виклики для інформаційної безпеки і вимагає паралельного розвитку спроможностей кіберзахисту.

Концепція цифрової трансформації публічного управління передбачає не просте переведення існуючих процесів у цифровий формат, а їх фундаментальне переосмислення з використанням можливостей сучасних технологій [29]. Це включає автоматизацію рутинних процесів, використання даних для прийняття рішень, створення цифрових екосистем для взаємодії між державою, бізнесом та громадянами.

Україна досягла значних успіхів у цифровій трансформації. Система електронних послуг Дія стала прикладом успішної цифровізації, що отримала міжнародне визнання. Електронні документи, можливість отримання

різноманітних послуг онлайн, спрощення адміністративних процедур значно покращили взаємодію громадян з державою.

Однак безпека цифрової трансформації є критично важливою умовою її успіху. Впровадження нових цифрових систем без належного забезпечення їх захищеності створює нові вразливості. Принцип Security by Design передбачає, що безпека має закладатися на етапі проектування систем, а не додаватися як опція після їх створення [24].

Архітектура безпечних цифрових систем має базуватися на кількох ключових принципах. Принцип оборони в глибину передбачає створення багатошарового захисту, де компрометація одного рівня не призводить до повного злому системи. Це включає захист на рівні мережі, серверів, додатків, даних.

Принцип мінімізації поверхні атаки вимагає обмеження функціональності системи тільки необхідним мінімумом, відключення невикористовуваних сервісів, закриття непотрібних портів. Чим простішою є система, тим менше в ній потенційних вразливостей.

Принцип найменших привілеїв означає, що користувачі та додатки отримують тільки ті права доступу, які необхідні для виконання їх функцій. Це обмежує потенційну шкоду від компрометації облікового запису або додатка.

Хмарні технології відіграють все більшу роль у цифровій трансформації публічного управління [32]. Хмарні сервіси надають переваги масштабованості, гнучкості, зниження витрат на підтримку власної інфраструктури. Однак використання хмарних технологій у державному секторі вимагає ретельного підходу до безпеки.

Гібридна хмарна модель, що поєднує приватні хмари для критичних та конфіденційних даних з публічними хмарами для менш чутливих сервісів, може бути оптимальним рішенням. Важливим є вибір надійних провайдерів хмарних послуг, які забезпечують високі стандарти безпеки, мають

сертифікати відповідності міжнародним стандартам, надають прозорість щодо розміщення даних.

Суверенні хмари, де дані зберігаються на території України під юрисдикцією українського законодавства, можуть бути рішенням для найбільш критичних державних систем. Розвиток національних хмарних інфраструктур є стратегічним завданням для забезпечення цифрового суверенітету.

Кіберстійкість як концепція виходить за рамки традиційного кіберзахисту. Якщо кіберзахист фокусується на запобіганні атакам, то кіберстійкість визнає неможливість абсолютного захисту і акцентує на здатності продовжувати функціонування в умовах атаки, швидко відновлюватися та навчатися на інцидентах [67].

Компоненти кіберстійкості включають технічну стійкість, організаційну стійкість та людську стійкість. Технічна стійкість забезпечується через резервування критичних систем, створення резервних копій даних, впровадження систем автоматичного відновлення, диверсифікацію технологій для уникнення єдиної точки відмови.

Організаційна стійкість передбачає наявність чітких процедур реагування на інциденти, планів забезпечення безперервності діяльності, механізмів швидкого прийняття рішень в кризових ситуаціях. Регулярні навчання та тренування відпрацьовують ці процедури та виявляють слабкі місця.

Людська стійкість стосується психологічної готовності персоналу діяти в стресових умовах кіберінцидентів, здатності зберігати спокій, приймати рішення, координувати зусилля. Підготовка персоналу, створення культури безпеки, психологічна підтримка є важливими елементами людської стійкості.

Центри реагування на кіберінциденти (CERT/CSIRT) є критично важливими елементами кіберстійкості. Ці центри забезпечують цілодобовий моніторинг інформаційних систем, виявлення підозрілої активності,

координацію реагування на інциденти, аналіз загроз, обмін інформацією з іншими організаціями [76].

Державний центр кіберзахисту виконує роль національного CERT для органів публічної влади. Розвиток його спроможностей, технічне оснащення, кадрове забезпечення є пріоритетними завданнями. Секторальні CERT у критичних галузях забезпечують спеціалізоване реагування з урахуванням специфіки відповідних секторів.

Управління вразливостями є важливим елементом підвищення кіберстійкості. Регулярне сканування систем для виявлення вразливостей, пріоритизація їх усунення відповідно до рівня ризику, швидке застосування патчів безпеки дозволяють закривати потенційні лазівки для зловмисників.

Програми bug bounty, коли організації платять незалежним дослідникам за виявлення вразливостей, можуть бути ефективним доповненням до власних зусиль з пошуку вразливостей. Ці програми використовують колективний інтелект спільноти безпеки для виявлення проблем, які могли бути пропущені внутрішніми тестами.

Моніторинг та аналітика безпеки з використанням систем SIEM дозволяють виявляти складні багатоступеневі атаки, що можуть бути непомітними при аналізі окремих подій [33]. Збирання логів з усіх критичних систем, їх централізована обробка, кореляція подій, автоматичне виявлення аномалій підвищують швидкість виявлення інцидентів.

Використання штучного інтелекту та машинного навчання для аналізу великих обсягів даних про безпеку дозволяє виявляти раніше невідомі загрози, прогнозувати атаки, автоматично реагувати на типові інциденти [34]. Ці технології особливо корисні в умовах зростаючої кількості та складності загроз.

Тестування стійкості через регулярні кіберучення, симуляції атак, тестування планів реагування дозволяє виявляти слабкі місця до того, як вони будуть використані реальними зловмисниками. Red team / Blue team exercises,

коли одна команда імітує атаку, а інша захищається, надають цінний досвід та виявляють прогалини в захисті.

Таким чином, цифрова трансформація та підвищення кіберстійкості органів публічної влади є взаємопов'язаними процесами, що вимагають збалансованого підходу. Швидка цифровізація без належного забезпечення безпеки створює ризики, тоді як надмірна обережність може загальмувати інновації. Знаходження оптимального балансу між швидкістю впровадження та безпекою є ключовим завданням для управлінців.

3.3. Використання штучного інтелекту, Big Data та аналітичних систем у моніторингу інформаційних ризиків

Сучасні технології штучного інтелекту, обробки великих даних та аналітики відкривають принципово нові можливості для моніторингу, прогнозування та нейтралізації інформаційних ризиків у публічному управлінні. Ці технології дозволяють обробляти величезні обсяги даних, виявляти складні залежності, автоматизувати рутинні операції та підвищувати швидкість реагування на загрози.

Штучний інтелект у кібербезпеці застосовується для вирішення різноманітних завдань. Виявлення аномалій у поведінці користувачів та систем є однією з ключових областей застосування [34]. Машинне навчання дозволяє створювати моделі нормальної поведінки і автоматично виявляти відхилення, які можуть свідчити про компрометацію системи або зловмисну активність.

Системи на базі ШІ можуть аналізувати мільйони подій безпеки щосекунди, що неможливо для людини. Вони виявляють складні багатоступеневі атаки, які розтягнуті в часі та маскуються під легітимну активність. Автоматичне виявлення та блокування атак у режимі реального часу значно підвищує ефективність захисту.

Прогнозування загроз з використанням ШІ базується на аналізі історичних даних про інциденти, актуальних трендів у світі кібербезпеки, геополітичної ситуації. Системи можуть передбачати ймовірність певних типів атак, рекомендувати превентивні заходи, оптимізувати розподіл ресурсів для захисту.

Predictive analytics дозволяє виявляти потенційні вразливості до їх експлуатації, прогнозувати поведінку зловмисників, оцінювати ймовірність успішності різних сценаріїв атак. Це переміщує парадигму від реактивного реагування на інциденти до проактивного попередження загроз.

Автоматизоване реагування на інциденти з використанням ШІ дозволяє значно скоротити час між виявленням загрози та її нейтралізацією. Security Orchestration, Automation and Response (SOAR) платформи інтегрують різні інструменти безпеки, автоматизують процеси реагування, виконують стандартні процедури без людського втручання.

Автоматизація рутинних операцій звільняє фахівців з безпеки для роботи над більш складними завданнями, що вимагають креативності та експертизи. Водночас важливо зберігати людський контроль над критичними рішеннями, оскільки ШІ може помилятися і його рішення мають бути прозорими та пояснюваними.

Big Data у моніторингу інформаційної безпеки дозволяє обробляти та аналізувати величезні обсяги різнорідних даних з множини джерел [33]. Логи з мережевого обладнання, серверів, додатків, систем безпеки, дані з відкритих джерел, інформація про загрози з міжнародних баз даних – все це може бути інтегровано та проаналізовано для отримання комплексної картини стану безпеки.

Технології Big Data дозволяють зберігати історичні дані протягом тривалого періоду, що важливо для розслідування інцидентів, виявлення довготривалих кампаній APT, аналізу трендів. Ретроспективний аналіз може виявити ознаки компрометації, які були пропущені при первинному моніторингу.

Threat Intelligence платформи використовують Big Data та ШІ для збирання, обробки та аналізу інформації про актуальні загрози [76]. Ці платформи агрегують дані з різних джерел: комерційних провайдерів threat intelligence, державних CERT, спільнот безпеки, власних sensors. Автоматичний аналіз цих даних виявляє нові загрози, індикатори компрометації, тактики та техніки зловмисників.

Інтеграція threat intelligence в системи захисту дозволяє автоматично блокувати відомі зловмисні IP-адреси, домени, хеші шкідливого ПЗ. Проактивне полювання на загрози (threat hunting) з використанням intelligence дозволяє виявляти прихованих зловмисників у мережі до того, як вони завдадуть шкоди.

Аналіз соціальних мереж та відкритих джерел (OSINT) з використанням ШІ дозволяє моніторити інформаційний простір для виявлення дезінформаційних кампаній, координованих маніпулятивних операцій, загроз репутації. Автоматичний аналіз великих обсягів публікацій виявляє аномальні патерни активності, координовані дії ботів, поширення шкідливого контенту.

Сентимент-аналіз дозволяє оцінювати емоційний тон публікацій, виявляти спалахи негативних настроїв, прогнозувати потенційні кризи. Natural Language Processing (NLP) технології розуміють контекст, виявляють іронію та сарказм, класифікують контент за темами. Це дозволяє органам влади отримувати оперативну інформацію про настрої в суспільстві, своєчасно реагувати на дезінформацію.

Виявлення дипфейків стало критично важливим завданням в умовах розвитку технологій синтетичних медіа. Системи на базі ШІ можуть аналізувати відео та аудіо для виявлення ознак штучного створення або маніпуляцій. Хоча гонка між створювачами та детекторами дипфейків продовжується, сучасні системи виявлення досягають високої точності.

Превентивні технології, такі як цифрові водяні знаки та криптографічне підтвердження автентичності медіа, можуть забезпечити довіру до офіційного контенту державних органів. Блокчейн-технології можуть використовуватися

для створення незмінних записів про походження та автентичність офіційних документів та заяв.

Аналітика для прийняття рішень використовує дані про інформаційну безпеку для оптимізації розподілу ресурсів, планування інвестицій, оцінки ефективності заходів захисту [85]. Data-driven approach до управління інформаційною безпекою дозволяє приймати обґрунтовані рішення на основі фактичних даних, а не інтуїції.

Візуалізація даних безпеки через дашборди та інтерактивні звіти надає керівництву зрозуміле уявлення про стан безпеки, ключові ризики, ефективність впроваджених заходів. Можливість деталізації від агрегованих показників до конкретних подій дозволяє отримувати інформацію на потрібному рівні деталізації.

Етичні та правові аспекти використання ШІ та Big Data у моніторингу інформаційної безпеки вимагають уваги. Автоматичний аналіз комунікацій може створювати ризики для приватності громадян. Необхідний баланс між безпекою та правами людини, прозорість використання технологій, нагляд за їх застосуванням.

Алгоритмічні упередження (bias) в системах ШІ можуть призводити до несправедливих рішень, дискримінації певних груп. Важливо забезпечувати різноманітність тренувальних даних, регулярно тестувати системи на упередження, мати механізми оскарження автоматизованих рішень.

Виклики впровадження технологій ШІ та Big Data в органах публічної влади включають обмеженість фінансових ресурсів, дефіцит фахівців з відповідними компетенціями, застарілість технічної інфраструктури, опір змінам з боку персоналу. Подолання цих викликів вимагає стратегічного планування, поетапного впровадження, інвестицій у навчання персоналу, державно-приватного партнерства.

Початок можна зробити з пілотних проектів у обмежених масштабах, які демонструють цінність технологій та дозволяють набути досвіду. Успішні пілоти можна масштабувати на інші органи та системи. Важливо не прагнути

впровадити все одразу, а зосередитися на найбільш критичних завданнях, де технології можуть надати найбільшу віддачу.

Таким чином, штучний інтелект, Big Data та аналітичні системи представляють потужний інструментарій для підвищення ефективності моніторингу та управління інформаційними ризиками у публічному управлінні. Їх впровадження вимагає інвестицій, розвитку компетентностей, вирішення етичних питань, але потенційні вигоди значно перевищують витрати у довгостроковій перспективі.

3.4. Формування культури інформаційної безпеки серед державних службовців та громадян

Технічні засоби захисту, нормативно-правове регулювання, організаційні процедури не можуть забезпечити належний рівень інформаційної безпеки без відповідної культури безпеки серед людей, які працюють з інформаційними системами та даними. Людський фактор залишається найслабшою ланкою в ланцюгу безпеки, і водночас найбільшим потенціалом для підвищення захищеності.

Культура інформаційної безпеки може бути визначена як сукупність цінностей, переконань, знань, навичок та практик, що визначають відношення людини до питань безпеки інформації та її поведінку в цифровому середовищі. Висока культура безпеки означає, що дотримання вимог безпеки стає природною частиною повсякденної роботи, а не додатковим обтяжливим обов’язком.

Компоненти культури інформаційної безпеки включають знання та розуміння загроз, усвідомлення особистої відповідальності за безпеку, навички безпечної поведінки в цифровому середовищі, критичне мислення щодо інформації, готовність дотримуватися політик та процедур безпеки, проактивне повідомлення про підозрілу активність.

Формування культури серед державних службовців є пріоритетним завданням, оскільки вони мають доступ до конфіденційної державної інформації, працюють з критичними системами, приймають управлінські рішення [53]. Інциденти безпеки, спричинені помилками або недбалістю державних службовців, можуть мати серйозні наслідки для держави та суспільства.

Програми навчання з інформаційної безпеки мають бути обов'язковими для всіх державних службовців. Базове навчання при прийнятті на роботу має охоплювати основні принципи інформаційної безпеки, загрози, політики організації, процедури реагування на інциденти [54]. Регулярне підвищення кваліфікації має оновлювати знання відповідно до еволюції загроз.

Навчання має бути не формальністю, а практично орієнтованим. Інтерактивні тренінги, симуляції фішингових атак, ігрові формати навчання підвищують залученість та запам'ятовування. Реальні кейси інцидентів, особливо ті, що відбулися в самій організації або подібних установах, роблять навчання релевантним.

Диференційований підхід до навчання залежно від ролі та рівня доступу є важливим. Топ-менеджмент потребує розуміння стратегічних аспектів інформаційної безпеки, кіберризиків для організації, відповідальності керівництва. Технічний персонал потребує поглибленого навчання з технічних аспектів захисту. Звичайні користувачі потребують практичних навичок безпечної роботи.

Спеціалізовані програми для осіб, які працюють з особливо чутливою інформацією або критичними системами, мають включати поглиблене вивчення загроз, процедур захисту, реагування на інциденти [56]. Регулярна сертифікація та перевірка знань забезпечують підтримання необхідного рівня компетентності.

Внутрішні комунікаційні кампанії з питань інформаційної безпеки підвищують обізнаність та формують культуру. Регулярні розсилки з порадами безпеки, інформацією про актуальні загрози, нагадуваннями про

правила тримають питання безпеки в фокусі уваги. Постери, інфографіка, відео створюють постійне візуальне нагадування.

Тематичні місяці або тижні кібербезпеки з активностями, конкурсами, навчальними заходами привертають увагу до питань безпеки. Розповіді про успішне запобігання інцидентам, подяки співробітникам, які виявили загрози, створюють позитивне підкріплення.

Симуляційні вправи дозволяють працівникам практикувати навички безпечної поведінки в контрольованих умовах. Симуляції фішингових атак, коли працівникам надсилаються тестові фішингові листи, виявляють уразливих працівників та надають можливість для додаткового навчання без реальних наслідків.

Кіберучення, що моделюють різні сценарії інцидентів, дозволяють відпрацьовувати процедури реагування, координацію між підрозділами, комунікації в кризових ситуаціях [82]. Розбір результатів учень виявляє слабкі місця та можливості для покращення.

Формування культури серед громадян є довгостроковою інвестицією в національну інформаційну безпеку. Громадяни, які розуміють загрози, дотримуються базових правил кібергігієни, критично оцінюють інформацію, менш вразливі до кіберзлочинності та маніпуляцій.

Медіаграмотність як здатність критично оцінювати інформацію, перевіряти джерела, розпізнавати маніпуляції є ключовим елементом інформаційної безпеки громадян [83]. В умовах інформаційної війни, коли Україна зазнає масованих атак дезінформацією, медіаграмотність населення стає питанням національної безпеки.

Впровадження медіаграмотності у шкільні та університетські програми формує відповідні навички у молодого покоління [57]. Курси для різних вікових груп, професій, соціальних груп мають враховувати специфіку аудиторії. Для літніх людей, які є особливо вразливими до онлайн-шахрайства, потрібні спеціальні програми з базових навичок цифрової безпеки.

Публічні кампанії з підвищення обізнаності населення щодо кіберзагроз використовують різні канали комунікації. Телевізійні та радіо ролики, соціальні мережі, зовнішня реклама, інтернет-банери доносять прості та зрозумілі повідомлення про базові правила безпеки.

Партнерство з приватним сектором, зокрема з телекомунікаційними компаніями, банками, соціальними мережами, посилює ефект кампаній. Компанії можуть інформувати своїх клієнтів про типові схеми шахрайства, надавати поради безпеки, впроваджувати технічні заходи захисту.

Освітні ініціативи включають безкоштовні онлайн-курси з кібербезпеки для широкої аудиторії [57]. Платформи електронного навчання, такі як Prometheus в Україні, надають доступні курси з основ інформаційної безпеки, захисту персональних даних, безпечної поведінки онлайн.

Бібліотеки, громадські центри, центри надання адміністративних послуг можуть проводити безкоштовні тренінги та консультації для населення. Особливо важливо охопити вразливі групи – літніх людей, людей з обмеженими можливостями, мешканців сільської місцевості, які мають менший доступ до інформації.

Формування довіри між державою та громадянами є важливою складовою культури інформаційної безпеки. Коли громадяни довіряють державним інституціям, вони більш схильні дотримуватися рекомендацій, повідомляти про інциденти, співпрацювати в протидії загрозам. Прозорість у питаннях використання персональних даних, підзвітність органів влади, ефективне реагування на звернення громадян будують цю довіру.

Роль лідерів у формуванні культури безпеки є критичною. Керівники на всіх рівнях мають демонструвати особистим прикладом важливість дотримання вимог безпеки. Якщо топ-менеджмент ігнорує правила безпеки, очікувати їх дотримання від інших марно. Підтримка ініціатив безпеки з боку керівництва, виділення ресурсів, увага до питань безпеки на нарадах сигналізують про пріоритетність цього напряму.

Метрики культури безпеки дозволяють оцінити її рівень та відстежувати динаміку. Опитування працівників щодо їх знань, відношення, практик безпеки надають кількісні дані. Показники кількості інцидентів, спричинених людським фактором, результати тестів знань, успішність симуляцій фішингу є індикаторами ефективності заходів формування культури.

Таким чином, формування культури інформаційної безпеки є довгостроковим процесом, що вимагає систематичних зусиль, інвестицій у навчання, комунікації, залучення керівництва. Це не разова активність, а постійний процес, що має адаптуватися до змін у загрозах, технологіях, організаційному середовищі. Висока культура безпеки є найефективнішим захистом від широкого спектру загроз.

3.5. Міжнародне співробітництво та імплементація європейських стандартів у сфері інформаційної безпеки

Транснаціональний характер інформаційних загроз, глобалізація цифрового простору, євроінтеграційні прагнення України роблять міжнародне співробітництво у сфері інформаційної безпеки критично важливим напрямом. Інтеграція у міжнародні системи безпеки, імплементація європейських стандартів, обмін досвідом та кращими практиками підвищують спроможності України протистояти сучасним загрозам.

Рамки міжнародного співробітництва у сфері кібербезпеки включають участь у міжнародних організаціях та ініціативах. Україна є учасником Конвенції Ради Європи про кіберзлочинність (Будапештська конвенція), яка встановлює загальні стандарти кримінального законодавства у сфері кіберзлочинності та механізми міжнародної правової допомоги.

Співпраця з НАТО у сфері кібероборони включає участь у програмах навчання, обмін інформацією про загрози, доступ до експертизи Альянсу. Центр передових технологій кібероборони НАТО надає підтримку партнерам

у розвитку спроможностей. Кіберучення, що проводяться під егідою НАТО, дозволяють відпрацьовувати взаємодію в умовах кризових ситуацій.

Партнерство з Європейським Союзом у рамках Угоди про асоціацію передбачає гармонізацію українського законодавства з acquis ЄС у сфері кібербезпеки та захисту даних [50]. ЄС надає Україні фінансову та технічну підтримку для зміцнення спроможностей кіберзахисту, модернізації інфраструктури, підготовки фахівців.

Імплементація Директиви NIS2 є пріоритетним завданням для України [49]. Ця Директива встановлює високі стандарти кібербезпеки для операторів основних послуг та постачальників цифрових сервісів. Імплементація вимагає прийняття відповідного законодавства, створення регуляторних органів, встановлення обов'язкових вимог до захисту критичної інфраструктури.

Україна може використати досвід країн ЄС, які вже імплементували Директиву, уникнути помилок, запозичити кращі практики [51]. Технічна допомога ЄС може включати консультації експертів, надання методичних матеріалів, фінансування пілотних проектів.

GDPR як стандарт захисту персональних даних встановлює високу планку для захисту приватності громадян [72]. Хоча Україна не є членом ЄС, адаптація законодавства до вимог GDPR є важливою для захисту прав громадян та забезпечення довіри міжнародних партнерів.

Закон України «Про захист персональних даних» базується на принципах GDPR, але потребує подальшого вдосконалення для повної відповідності [84]. Створення незалежного органу з захисту персональних даних з реальними повноваженнями, запровадження ефективних санкцій за порушення, забезпечення прав суб'єктів даних є необхідними кроками.

Обмін інформацією про загрози є ключовим елементом міжнародного співробітництва. Кіберзагрози не знають кордонів, і атака, що відбулася в одній країні, може бути прелюдією до атак в інших. Своєчасний обмін

інформацією про нові загрози, індикатори компрометації, тактики зловмисників дозволяє всім учасникам краще захищатися.

Україна бере участь у міжнародних платформах обміну інформацією про кіберзагрози. Двосторонні угоди про співробітництво з окремими країнами встановлюють механізми оперативного обміну. Важливо забезпечити баланс між відкритістю та захистом конфіденційної інформації про вразливості національних систем.

Спільні навчання та учення з міжнародними партнерами підвищують готовність до реагування на транснаціональні інциденти. Кіберучення Locked Shields, що проводяться під егідою НАТО, є найбільшими у світі і дозволяють відпрацьовувати захист критичної інфраструктури від складних атак.

Участь українських фахівців у міжнародних навчаннях надає цінний досвід, дозволяє порівнювати власні спроможності з іншими країнами, виявляти прогалини. Організація спільних навчань на території України з залученням міжнародних експертів підвищує спроможності національних команд.

Технічна допомога від міжнародних партнерів включає фінансування проектів модернізації інформаційної інфраструктури, надання обладнання, програмного забезпечення, навчання фахівців. США, країни ЄС, Канада, Великобританія надали Україні значну підтримку у зміцненні кіберзахисту, особливо після початку повномасштабної агресії.

Волонтерська ІТ-спільнота світу також надала безпрецедентну підтримку Україні. ІТ-армія України, міжнародні хакери-активісти, компанії кібербезпеки безкоштовно надавали послуги захисту, моніторингу загроз, реагування на інциденти. Це продемонструвало солідарність глобальної спільноти та важливість неурядового співробітництва.

Гармонізація законодавства з міжнародними стандартами є тривалим процесом. Україна має привести своє законодавство у відповідність не лише з європейськими директивами, а й з міжнародними конвенціями, стандартами ISO/IEC, рекомендаціями міжнародних організацій.

Участь українських експертів у роботі міжнародних органів стандартизації дозволяє впливати на формування стандартів, враховувати специфіку України, отримувати інформацію про нові стандарти на ранніх етапах їх розробки.

Боротьба з транснаціональною кіберзлочинністю вимагає тісної співпраці правоохоронних органів різних країн. Кіберзлочинці часто діють з територій інших держав, використовують серверну інфраструктуру в різних юрисдикціях, відмивають кошти через міжнародні фінансові системи.

Євроюст та Європол надають платформи для координації розслідувань, обміну оперативною інформацією, спільних операцій. Україна активно співпрацює з цими організаціями у розслідуванні кіберзлочинів, екстрадиції злочинців, конфіскації незаконних активів.

Дипломатія кіберпростору стає все важливішою складовою зовнішньої політики. Україна просуває на міжнародних форумах принципи відповідальної поведінки держав у кіберпросторі, необхідність дотримання міжнародного права, захисту прав людини в цифровому середовищі. Участь у роботі спеціалізованих органів ООН, ОБСЄ, Ради Європи дозволяє формувати міжнародні норми та правила поведінки в кіберпросторі.

Україна підтримує ініціативи щодо розробки міжнародних механізмів атрибуції кібератак, притягнення до відповідальності держав-агресорів, які використовують кіберзброю проти цивільних об’єктів. Досвід протидії російським кібератакам має стати основою для зміцнення міжнародного режиму кібербезпеки.

Виклики імплементації міжнародних стандартів в Україні включають необхідність суттєвих фінансових інвестицій, дефіцит кваліфікованих кадрів, складність адаптації європейських норм до специфіки українського законодавства та практик, потребу в зміні організаційної культури. В умовах війни ці виклики посилюються через перерозподіл ресурсів на оборонні потреби, руйнування інфраструктури, міграцію фахівців.

Однак імплементація європейських стандартів є стратегічним пріоритетом, який не лише відповідає зобов'язанням України в рамках євроінтеграції, а й об'єктивно підвищує рівень захищеності національного кіберпростору. Європейські стандарти втілюють кращі світові практики, перевірені досвідом провідних країн.

Рекомендації щодо імплементації включають: поетапний підхід з фокусом на найбільш критичних сферах; залучення експертної підтримки ЄС та країн-членів; пілотні проекти для апробації нових норм; інвестиції в навчання та підготовку кадрів; державно-приватне партнерство для розподілу фінансового тягаря; використання технічної та фінансової допомоги міжнародних партнерів.

Побудова довіри між Україною та міжнародними партнерами через демонстрацію прогресу в імплементації стандартів, прозорість процесів, готовність до взаємних оцінок та аудитів є важливою складовою міжнародного співробітництва. Регіональна співпраця з країнами Східного партнерства, Балтії, Центральної та Східної Європи, які мають подібні виклики та загрози, дозволяє обмінюватися досвідом, координувати зусилля, розвивати спільні спроможності. Створення регіональних центрів компетенції, спільних навчальних програм, платформ обміну інформацією підвищує колективну безпеку.

Таким чином, міжнародне співробітництво та імплементація європейських стандартів є ключовими факторами підвищення рівня інформаційної безпеки публічного управління в Україні. Інтеграція у міжнародні системи безпеки, адаптація кращих практик, гармонізація законодавства не лише відповідають євроінтеграційним прагненням України, а й об'єктивно зміцнюють національну безпеку, підвищують стійкість до сучасних інформаційних загроз, створюють умови для довгострокового розвитку цифрової економіки та інформаційного суспільства.

ВИСНОВКИ

Проведене дослідження дозволило комплексно розглянути феномен інформаційної безпеки публічного управління в умовах цифрової трансформації, гібридних викликів та зростання ролі інформаційно-комунікаційних технологій. Реалії сучасного безпекового середовища засвідчують, що інформаційна сфера стала одним із ключових полів протистояння, впливаючи як на ефективність державних інституцій, так і на рівень суспільної довіри, політичну стабільність та спроможність держави реагувати на кризові ситуації. У межах роботи було послідовно проаналізовано теоретичні, правові, організаційні та технологічні аспекти забезпечення інформаційної безпеки, що дало можливість сформувати цілісне бачення її ролі та стратегічного значення для системи публічного управління. Узагальнення результатів дослідження подано у висновках, сформульованих відповідно до поставлених завдань.

1. У ході дослідження з’ясовано, що інформаційна безпека у сфері публічного управління виступає ключовим елементом національної безпеки України, оскільки охоплює комплекс заходів, спрямованих на захист державних інституцій, суспільства та громадян від деструктивних інформаційних впливів. Її сутність полягає у забезпеченні стійкого функціонування інформаційного простору, збереженні цілісності та достовірності інформаційних ресурсів, недопущенні маніпулятивного впливу та кібернетичних загроз. Визначено, що у сучасних умовах цифровізації інформаційна безпека стає визначальним чинником довіри громадян до державної влади, ефективності прийняття управлінських рішень та стабільності політичного середовища.

2. Проаналізовані теоретико-методологічні підходи дозволили встановити, що забезпечення інформаційної безпеки базується на системному, ризик-орієнтованому та проактивному підходах. Доведено, що методологія вивчення інформаційної безпеки охоплює ситуаційний, структурно-

функціональний, індикаторний, сценарний та кібермоніторинговий аналіз. До інструментів дослідження належать технології обробки даних, інтелектуального аналізу, комплекси виявлення аномалій, моделювання загроз. Узагальнення цих підходів дало змогу систематизувати принципи, які забезпечують комплексну стійкість інформаційного середовища публічного управління.

3. Дослідження нормативно-правової бази України та країн ЄС засвідчило неоднорідність та фрагментарність національного правового поля щодо забезпечення інформаційної безпеки. Виявлено проблемні аспекти: недостатня узгодженість між окремими законодавчими актами, повільна адаптація українських норм до вимог цифрової епохи, обмеженість інституційних механізмів реалізації політики кіберзахисту. Порівняльний аналіз показав, що європейське законодавство демонструє більш високий рівень деталізації, системності й інтегрованості. Це визначає необхідність гармонізації національної нормативної бази із стандартами ЄС, особливо в частині захисту критичної інфраструктури, управління інцидентами, персональних даних та цифрової безпеки.

4. У процесі ідентифікації сучасних загроз встановлено, що публічне управління перебуває під впливом багатовимірних інформаційних ризиків, які включають кібератаки, техногенні інциденти, інформаційно-психологічні операції, маніпулятивні кампанії, поширення фейків, використання бот-мереж, алгоритмічні втручання у цифрові комунікації. Доведено, що такі загрози здатні порушувати управлінські процеси, знижувати ефективність державних комунікацій, створювати викривлене сприйняття діяльності органів влади та підривати легітимність держави. Особливо небезпечними є інформаційні впливи у соціальних мережах, які через свою швидкість і масштабність формують середовище підвищеної вразливості.

5. Оцінка стану захисту критичної інформаційної інфраструктури України у контексті гібридної війни продемонструвала, що попри істотний прогрес у сферах кіберзахисту, цифрової модернізації та розвитку профільних

органів, рівень стійкості потребує подальшого зміцнення. Встановлено, що ефективний захист критичної інфраструктури неможливий без удосконалення системи управління інцидентами, підвищення оперативності реагування, модернізації інженерно-технічних засобів та впровадження інтелектуальних цифрових рішень. Обґрунтовано, що використання штучного інтелекту, машинного навчання, Big Data та аналітичних платформ може істотно підвищити здатність держави до раннього виявлення, прогнозування та нейтралізації загроз.

6. Узагальнення результатів дослідження дало змогу визначити стратегічні орієнтири державної політики у сфері інформаційної безпеки. До ключових напрямів належать формування сталого середовища цифрової безпеки, розвиток компетентностей державних службовців, удосконалення інституційної архітектури кіберзахисту, поглиблення міжнародної взаємодії та імплементація європейських стандартів. Важливим аспектом визначено формування культури інформаційної безпеки серед громадян, що охоплює розвиток критичного мислення, відповідального інформаційного споживання та здатності розпізнавати маніпулятивні впливи. Це забезпечує посилення інформаційної стійкості суспільства та підвищення ефективності державного управління.

Узагальнюючи результати проведеного дослідження, можна стверджувати, що інформаційна безпека є стратегічним чинником сучасного публічного управління, від якого залежить стабільність держави, її міжнародна конкурентоспроможність та рівень довіри суспільства до інституцій влади. Забезпечення інформаційної безпеки потребує комплексного підходу, який охоплює вдосконалення законодавчої бази, модернізацію інфраструктури, розвиток компетентностей державних службовців, впровадження інтелектуальних цифрових технологій та посилення міжнародної співпраці. Ефективна державна політика у цій сфері має спиратися на інтегровані інституційні, технологічні та соціальні механізми, здатні забезпечити стійкість до сучасних інформаційних загроз,

зміцнити потенціал держави у сфері кіберзахисту та сприяти формуванню безпечного цифрового середовища.

Водночас у контексті гібридної війни та глобальних інформаційних викликів особливого значення набуває розвиток культури інформаційної грамотності громадян, підвищення спроможності державних органів оперативно реагувати на інформаційні інциденти, а також формування партнерських моделей взаємодії між державою, приватним сектором і міжнародними інституціями. Саме поєднання цих чинників забезпечує можливість переходу до стійкої моделі інформаційної безпеки, яка підтримує процеси цифрової трансформації, зміцнює національну безпеку та створює умови для сталого суспільного розвитку. У цьому контексті інформаційна безпека постає не лише як захисний механізм, але і як стратегічний ресурс, що визначає траєкторію модернізації системи публічного управління та адаптацію України до глобальних інформаційних процесів.

Додаток

АПРОБАЦІЯ РЕЗУЛЬТАТІВ ДОСЛІДЖЕННЯ

Результати кваліфікаційної магістерської роботи були апробовані у ході науково-дослідної практики. Основні положення та висновки представлені на науковій конференції Результати кваліфікаційної магістерської роботи були апробовані у ході науково-дослідної практики. Основні положення та висновки представлені на XVI Міжнародній науково-практичній конференції «Концептуальні шляхи розвитку науки та освіти» (15-16 листопада 2025 року). Матеріали дослідження опубліковано у збірнику конференції: Андросова К. Формування культури інформаційної безпеки серед державних службовців та громадян. *Концептуальні шляхи розвитку науки та освіти*: матеріали XVI Міжнародної науково-практичної конференції м. Львів, 15-16 листопада 2025 року. Львів : Львівський науковий форум, 2025. С. 18-19.

Окремі результати дослідження опубліковано у фаховому науковому журналі у статті: Стороженко Л., Андросова К., Галич Н. Інтелектуальні технології та інформаційна безпека: стратегічні орієнтири розвитку цифрового публічного управління. *Публічно-управлінські та цифрові практики.* 2025. Вип. 4(7). URL: https://journals.duikt.edu.ua/index.php/public/about.

Апробація засвідчує коректність застосованих методів, наукову обґрунтованість та практичну релевантність отриманих результатів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Данільян О. Г. Національна безпека України: сутність, структура та напрямки реалізації : навч. посіб. Харків : Фоліо, 2002. 285 с.

2. Інформаційна безпека / за ред. В. В. Остроухова. Київ : Видавництво Ліра-К, 2021. 412 с.

3. Кравець Є. А. Інформаційна безпека держави. Київ : Українська енциклопедія, 1992.

4. Лизанчук В. В. Інформаційна безпека України: теорія і практика : підручник. Львів : ЛНУ ім. Івана Франка, 2017. 725 с.

5. Ліпкан В. А. Теоретичні основи та елементи національної безпеки України. Київ : КНТ, 2003. 599 с.

6. Ліпкан В. А., Макименко Ю. Є., Желіховський В. М. Інформаційна безпека України в умовах євроінтеграції : навч. посіб. Київ : КНТ, 2006.

7. Литвиненко О. В. Інформаційні впливи та операції. Теоретико-аналітичні нариси : монографія. Київ : НІСД, 2003. 240 с.

8. Остроухов В. В., Петрик В. М., Присяжнюк М. М. та ін. Інформаційна безпека (соціально-правові аспекти) : підручник. Київ : КНТ, 2010. 776 с.

9. Почепцов Г. Г. Сучасні інформаційні війни. Вид. 2-ге, допов. Київ : Вид-во Києво-Могилянська академія, 2015. 497 с.

10. Світова гібридна війна: український фронт : монографія / за заг. ред. В. П. Горбуліна. Київ : НІСД, 2017.

11. Войтко О. В., Солонніков В. Г. Державна інформаційна політика основа забезпечення інформаційної безпеки в умовах гібридної війни. Актуальні проблеми управління інформаційною безпекою держави. 2021.

12. Гуржій Т. Інформаційне право: виклики гібридної війни. Журнал східноєвропейського права. 2018. № 53. С. 26–37.

13. Коцур Л., Грига О. Державна інформаційна політика України: теоретико-методологічні парадокси воєнного часу. Публічне управління: концепції, парадигма, розвиток, удосконалення. 2023. № 4. С. 52–60. DOI: https://doi.org/10.31470/2786-6246-2023-4-52-60

14. Ніщименко О. А. Інформаційна безпека України на сучасному етапі розвитку держави і суспільства. Наше право. 2016. № 1. С. 17–23.

15. Панченко О. А. Роль засобів масової інформації в системі державного управління інформаційною безпекою. Публічне управління та митне адміністрування. 2020. № 1 (24). С. 97–102. DOI: 10.32836/2310-9653-2020-1.18

16. Проблеми забезпечення інформаційної безпеки в системі публічного управління. Аспекти публічного управління. 2018. URL: https://aspects.org.ua/index.php/journal/article/view/442

17. Публічне управління у сфері інформаційної безпеки для забезпечення розвитку демократії в Україні (контекст воєнного стану). Публічне урядування. 2022. URL: https://journals.maup.com.ua/index.php/public-management/article/view/2562

18. Сілаєв В., Горінов П. Політика інформаційної безпеки в умовах цифрової трансформації України: виклики та шляхи попередження. Наукові праці Міжрегіональної Академії управління персоналом. Політичні науки та публічне управління. 2024. № 3(75). С. 81–87. DOI: https://doi.org/10.32689/2523-4625-2024-3(75)-12

19. Бєлай С. В., Корнієнко Д. М. Інформаційна безпека сьогодення – невід'ємна складова воєнної безпеки. Актуальні проблеми управління інформаційною безпекою держави. Київ : Національна академія Служби безпеки України, 2018. 408 с.

20. Войціховський А. В. Кібербезпека як важлива складова системи захисту національної безпеки європейських країн. Журнал східноєвропейського права. 2018. № 53. С. 26–37.

21. Кібербезпека критичної інфраструктури під час військової загрози. Глобальні та регіональні проблеми інформатизації в суспільстві і природокористуванні ’2024 : матеріали конф., 21–22 листопада 2024 року. URL: https://www.researchgate.net/publication/387737658

22. Ковалів М., Скриньковський Р., Назар Ю., Єсімов С., Красницький І., Кайдрович Х., Князь С., Кемська Ю. Правове забезпечення кібербезпеки критичної інформаційної інфраструктури України. Traektoriâ Nauki = Path of Science. 2021. № 4. Vol. 7. С. 2011–2018. DOI: https://10.22178/pos.69-12

23. Нормативно-правове забезпечення кібербезпеки об’єктів критичної інфраструктури. Науковий вісник Львівського державного університету внутрішніх справ (серія юридична). 2024. № 2. DOI: https://doi.org/10.32782/2311-8040/2024-2-11

24. Правове регулювання кібербезпеки в контексті захисту критичної інфраструктури. Information Technology: Computer Science, Software Engineering and Cyber Security. 2024. DOI: https://doi.org/10.32782/IT/2024-4-5

25. Арутюнян В. Сучасні тенденції використання ІТ у публічному управлінні. Аспекти публічного управління. 2024. Т. 12. № 1. С. 49–56. DOI: https://doi.org/10.15421/152407

26. Електронне урядування в Україні: правові аспекти та перспективи розвитку. Науковий вісник Ужгородського національного університету. Серія: Право. 2024. Т. 4. № 86.

27. Кравець Є. Цифровізація державного управління України: особливості та перспективи. Вісник Київського національного університету імені Тараса Шевченка. Державне управління. 2024. Том 19. № 1.

28. Правові засади розвитку електронного урядування в Україні в умовах європейської інтеграції. Київський часопис права. 2024. URL: https://kyivchasprava.kneu.in.ua/index.php/kyivchasprava/article/view/504

29. Саприкін В. Оцифровування, цифровізація та цифрова трансформація публічного управління в Україні. Вісник Київського національного університету імені Тараса Шевченка. Державне управління. 2024. Том 19. № 1.

30. Технології та інновації у публічному управлінні: сучасні тренди, вплив на якість державних послуг. Економіка та суспільство. 2024. DOI: https://doi.org/10.32782/2524-0072/2024-65-82

31. Цифрова державна послуга: український досвід цифрової трансформації в умовах воєнного часу. Філософія та управління. 2024. № 1.

32. Цифрове врядування: сучасні світові тренди та особливості розвитку в Україні. Публічне управління та місцеве самоврядування. 2024. URL: https://journals.politehnica.dp.ua/index.php/public/article/view/609

33. Застосування великих масивів даних (Big Data) для підвищення ефективності державного управління в Україні. Таврійський науковий вісник. Серія: Публічне управління та адміністрування. 2024. № 5. С. 86–91. DOI: https://doi.org/10.32782/tnv-pub.2024.5.10

34. Магиляс Ю., Корсун В., Миргородська М. Пріритетні напрямки впровадження штучного інтелекту в публічне управління. Аспекти публічного управління. 2023. Т. 11. № 4. С. 97–103. DOI: https://doi.org/10.15421/152358

35. Максименцева Н., Максименцев М. Штучний інтелект у публічному управлінні: переваги цифрових технологій та загрози суверенному інформаційному простору. Державне управління: удосконалення та розвиток. 2024. № 2. DOI: http://doi.org/10.32702/2307-2156.2024.2.7

36. Гребньов Г. Інформаційний аспект гібридної війни росії проти України. Український інформаційний простір. 2023. № 1(11). С. 107–118. DOI: https://doi.org/10.31866/2616-7948.1(11).2023.279598

37. Дезінформація в соціальних мережах: як розпізнати та протидіяти. Теорія та історія соціальних комунікацій. 2023.

38. Дубова Д. В. Фейки, пропаганда, дезінформація та виборчий процес: як нам захистити демократичні практики? Київ : ТОВ «Видавництво Сталь», 2019. 254 с.

39. Роль соціальних мереж у формуванні суспільної думки в період російсько-української війни. СОЦІОПОЛІС: Journal of Social and Political Sciences. 2024. № 1.

40. Соціальні мережі, медіа та маніпуляції: аналіз інформаційних загроз. Регіональні студії. 2023. № 35.

41. Гібридна війна в Україні: сучасні підходи. Вісник Прикарпатського університету. Серія: Політологія. 2024. DOI: https://journals.pnu.if.ua/index.php/politology/article/view/130

42. Гібридна війна: інформаційно-безпековий вимір. Вісник Прикарпатського університету. Серія: Політологія. 2024. DOI: https://journals.pnu.if.ua/index.php/politology/article/view/148

43. Горбулін В. П. «Гібридна війна» як ключовий інструмент російської геостратегії реваншу. Стратегічні пріоритети. 2014.

44. Досвід інформаційних війн в історії та сучасності як об’єкт досліджень сучасної науки та освіти. Українські історичні студії. 2024. URL: http://phh.dspu.edu.ua/article/view/305157

45. Інформаційна війна як інструмент міжнародної політики (досвід для України). Історико-політичні проблеми сучасного світу. 2024. № 50. С. 9–19.

46. Інформаційні війни як інструмент гібридної агресії: український досвід. Вісник НТУУ «КПІ» Політологія. Соціологія. Право. 2025. DOI: https://visnyk-psp.kpi.ua/article/view/332563

47. Магда Є. М. Гібридна війна: сутність та структура феномену. Міжнародні відносини. Серія «Політичні науки». 2014. № 4.

48. Поняття інформаційних та гібридних війн в умовах глобалізації. Український науковий журнал «Освіта регіону». URL: https://social-science.uu.edu.ua/article/1389

49. Gigacloud. NIS 2: A General Overview of the EU Cybersecurity Directive. 2025. URL: https://gigacloud.ua/en/articles/nis-2-a-general-overview-of-the-eu-cybersecurity-directive/

50. Кібербезпека на міжнародному рівні: Виклики та можливості NIS2 для українських компаній. Думка експерта IAA. URL: https://iaa.international/publication/kiberbezpeka-na-mizhnarodnomu-rivni

51. NIS2: оновлені стандарти кібербезпеки в Європі. BSO Privacy Group. 2025. URL: https://bsoprivacygroup.com/nis2-onovleni-standarty-kiberbezpeky-v-ievropi/

52. NIS2: Директива ЄС, що змінює правила кібербезпеки – чому Україна бере її на озброєння? Cybersec.net.ua. 2025. URL: https://cybersec.net.ua/statti/833-nis2-dyrektyva-yes-shcho-zminiuie-pravyla-kiberbezpeky

53. Інформаційна безпека особи, держави та суспільства в сучасну цифрову епоху : програма підвищення кваліфікації. Київський регіональний центр підвищення кваліфікації. URL: https://pdp.nacs.gov.ua/courses/informatsiina-bezpeka-osoby

54. Інформаційна безпека публічних службовців : програма підвищення кваліфікації. URL: https://pdp.nacs.gov.ua/courses/informatsiina-bezpeka-41f7a84d

55. Кібербезпека : програма підвищення кваліфікації. URL: https://pdp.nacs.gov.ua/courses/kiberbezpeka_

56. Організаційно-правове забезпечення кібербезпеки в органах публічної влади : програма підвищення кваліфікації. URL: https://pdp.nacs.gov.ua/courses/orhanizatsiino-pravove-zabezpechennia

57. Основи інформаційної безпеки : онлайн-курс Prometheus. 2024. URL: https://prometheus.org.ua/prometheus-free/info-security-basics/

58. Державна політика в умовах цифровізації суспільства. міжнародний досвід реалізації програм та стратегії цифровізації. Аналітично-порівняльне правознавство. 2022.

59. Зарубіжний досвід упровадження електронного урядування / авт. кол. : Т. Камінська, А. Камінський, М. Пасічник та ін. ; за заг. ред. С. А. Чукут. Київ, 2008. 200 с.

60. Цифрова трансформація та електронне врядування: наукові підходи дослідження в сфері публічного управління та адміністрування. ResearchGate. 2023. URL: https://www.researchgate.net/publication/375879898

61. Закон України «Про інформацію» : Закон України від 02.10.1992 № 2657-XII. Відомості Верховної Ради України. 1992.

62. Закон України «Про національну безпеку України» : Закон України від 21.06.2018 № 2469-VIII. Відомості Верховної Ради України. 2018. № 31. С. 241.

63. Закон України «Про основні засади забезпечення кібербезпеки України» : Закон України від 05.10.2017 № 2163-VIII.

64. Закон України «Про захист інформації в інформаційно-комунікаційних системах» : Закон України від 05.07.1994 № 80/94-ВР.

65. Доктрина інформаційної безпеки України : затв. Указом Президента України від 25.02.2017 № 47/2017. URL: https://zakon.rada.gov.ua/go/47/2017

66. Стратегія інформаційної безпеки : затв. Указом Президента України від 28.12.2021 № 685/2021. URL: https://www.president.gov.ua/documents/6852021-41069

67. Стратегія кібербезпеки України : затв. Указом Президента України від 26.08.2021 № 447/2021. URL: https://www.president.gov.ua/documents/4472021-40013

68. Стратегія національної безпеки України : затв. Указом Президента України від 14.09.2020 № 392/2020. URL: https://www.president.gov.ua/documents/3922020-35037

69. Про затвердження Загальних вимог до кіберзахисту об’єктів критичної інфраструктури : Постанова Кабінету Міністрів України від 19.06.2019 № 519.

70. Про затвердження плану заходів на 2023—2024 роки з реалізації Стратегії кібербезпеки України : Постанова Кабінету Міністрів України від 19.12.2023 № 1163.

71. Про схвалення Концепції розвитку електронного урядування в Україні : Розпорядження Кабінету Міністрів України від 20.09.2017 № 649-р.

72. Directive (EU) 2022/2555 of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union (NIS2 Directive). 2022.

73. General Data Protection Regulation (GDPR) – Regulation (EU) 2016/679.

74. Global Risks Report 2018. World Economic Forum. URL: http://www.weforum.org

75. UN global e-government survey 2022: The Future of Digital Government. Department of Economic and Social Affairs. United Nations. New York, 2022. 311 p.

76. Державний центр кіберзахисту. Офіційний сайт. URL: https://csirt.csi.cip.gov.ua/

77. Держспецзв’язку. Офіційний сайт. URL: https://cip.gov.ua/

78. Детектор медіа. Аналітичний центр. URL: https://detector.media/

79. Київський міжнародний інститут соціології. Дослідження споживання медіа. URL: https://www.kiis.com.ua/

80. Міністерство цифрової трансформації України. Офіційний сайт. URL: https://thedigital.gov.ua/

81. Національний інститут стратегічних досліджень. Аналітичні матеріали. URL: https://niss.gov.ua/

82. Рада національної безпеки і оборони України. Офіційний сайт. URL: https://www.rnbo.gov.ua/

83. Центр демократії та верховенства права. Епідемія дезінформації: чому фейки стали частиною нашого життя. 2022. URL: https://cedem.org.ua/analytics/epidemiya-dezinformatsiyi/

84. Центр протидії дезінформації при РНБО України. URL: https://cpd.gov.ua/

85. Цифрова трансформація економіки України в умовах війни. НІСД. 2023. URL: https://niss.gov.ua/news/komentari-ekspertiv

86. Захист інформації в системах електронного урядування / О. М. Хошаба та ін. Київ, 2017. 146 с.

87. Яковенко Я. Ю. Формування та реалізація стратегії стійкого розвитку промислових підприємств : дис. ... д-ра філос. : 051. Кременчук, 2020. 279 с.

88. Войтович Н. Розвиток навичок критичного мислення та медіаграмотності у населення як спосіб протидії російській агресії в інформаційній війні. Журналістика майбутнього: виклики, тенденції, перспективи. 2022. С. 297.

89. Войціховський А. В. Інформаційна безпека як складова системи національної безпеки (міжнародний і зарубіжний досвід). 2020.

90. Жайворонок О. І. Сучасні загрози інформаційного тероризму в умовах гібридної війни Росії проти України. Державне управління: удосконалення та розвиток. 2018. № 4. С. 1–5.

91. Кунєв Ю. Д. Правове забезпечення інформаційної безпеки як предмет правового дослідження. Юридичний вісник «Повітряне і космічне право». 2021. № 1(58). С. 95–102. DOI: 10.18372/2307-9061.58.15314

92. Ніщименко О. А. Інформаційна безпека України на сучасному етапі розвитку держави і суспільства. Наше право. 2016. № 1. С. 17–23.

93. Пилипчук В. Г. Забезпечення інформаційної безпеки України: сучасні тенденції та проблеми. Запобігання новим викликам та загрозам інформаційній безпеці України: правові аспекти : матеріали конф. Вип. 6. 2016.

94. Почепцов Г. Інформаційна політика : навч. посібник. 2-ге вид. Київ : Знання, 2008.

95. Сащук Г. М., Рихлік В. А. Інформаційний складник гібридної війни Росії проти України. Політологічний вісник КНУ ім. Т. Шевченка. 2022. № 89. С. 133–146. DOI: 10.17721/2415-88IX.2022.89.133-146

96. Скулиш Є. (ред.) Історія інформаційно-психологічного протиборства. Київ, 2012.

97. Сорокін О. Інформаційна безпека та її складові: проблеми визначення концепту. Держава та право. 2014. № 8. С. 18–22.

98. Тихомиров О. О. Забезпечення інформаційної безпеки як функція сучасної держави : моногр. 2019.

99. Ткачук Т. Ю. Державна політика у сфері забезпечення інформаційної безпеки на сучасному етапі. Інформаційна безпека в сучасному світі та її вплив на конституційний лад в Україні: теорія й практика : матеріали конф., м. Івано-Франківськ, 20 червня 2019 р. Івано-Франківськ, 2019. 116 с.

100. Шпекторенко І. В. Державна інформаційна політика: теоретико-методологічні засади. Гілея. 2019.