ХМЕЛЬНИЦЬКА ОБЛАСНА РАДА

ХМЕЛЬНИЦЬКИЙ УНІВЕРСИТЕТ УПРАВЛІННЯ ТА ПРАВА
ІМЕНІ ЛЕОНІДА ЮЗЬКОВА
(повне найменування вищого навчального закладу)

ФАКУЛЬТЕТ ПУБЛІЧНОГО УПРАВЛІННЯ
(повне найменування інституту, факультету)

Кафедра: публічного управління та адміністрування
(повна назва кафедри)

МАГІСТЕРСЬКА РОБОТА

на тему: «Публічне управління в сфері інформаційної безпеки в умовах воєнного стану»

Виконав: студент магістратури за спеціальністю 281 Публічне управління та адміністрування заочної форми навчання
Кирил ВОРОБЙОВ

Керівник: доцентка кафедри публічного управління та адміністрування, кандидатка економічних наук, доцентка
Леся ОМЕЛЬЧУК

Рецензент: _____

Хмельницький – 2025 рік

АНОТАЦІЯ

Кирил ВОРОБЙОВ. Публічне управління в сфері інформаційної безпеки в умовах воєнного стану. – Магістерська робота.

У магістерській роботі досліджено публічне управління у сфері інформаційної безпеки в умовах воєнного стану з позицій забезпечення національної та інформаційної стійкості держави.

Проаналізовано теоретико-методологічні підходи до розуміння інформаційної безпеки, національної стійкості та зарубіжний досвід їх інституційного забезпечення, узагальнено нормативно-правові засади регулювання інформаційної безпеки в Україні та оцінено стан її забезпечення в умовах сучасних гібридних і воєнних загроз.

Обґрунтовано доцільність застосування ризик-орієнтованого підходу до моделювання публічного управління захистом інформаційного простору, запропоновано трирівневу систему моніторингу інформаційних процесів і модель забезпечення інформаційної стійкості держави як циклічного та безперервного процесу.

Визначено стратегічні пріоритети розвитку публічного управління в сфері інформаційної безпеки, зокрема через інтеграцію інформаційної стійкості до національної системи стійкості, що сприяє підвищенню адаптивності, передбачуваності та спроможності держави ефективно протидіяти сучасним інформаційним загрозам і забезпечувати захист національних інтересів України.

Ключові слова: публічне управління, інформаційна безпека, інформаційна стійкість, національна стійкість, інформаційний простір, воєнний стан, інформаційні загрози, дезінформація, кібербезпека, ризик-орієнтований підхід, моніторинг інформаційних процесів, стратегічні пріоритети.

SUMMARY

Kyryl VOROBYOV. Public administration in the field of information security under martial law. – Master's thesis.

The master's thesis examines public administration in the field of information security under martial law from the standpoint of ensuring national and informational stability of the state.

Theoretical and methodological approaches to understanding information security, national stability and foreign experience of their institutional support are analyzed, the regulatory and legal principles of information security regulation in Ukraine are summarized and the state of its provision in conditions of modern hybrid and military threats is assessed.

The feasibility of using a risk-oriented approach to modeling public administration of information space protection is substantiated, a three-level system of monitoring information processes and a model of ensuring informational stability of the state as a cyclical and continuous process are proposed.

Strategic priorities for the development of public administration in the field of information security have been identified, in particular through the integration of information resilience into the national resilience system, which contributes to increasing the adaptability, predictability and ability of the state to effectively counteract modern information threats and ensure the protection of the national interests of Ukraine.

Keywords: public administration, information security, information resilience, national resilience, information space, martial law, information threats, disinformation, cybersecurity, risk-based approach, monitoring of information processes, strategic priorities.

ЗМІСТ

ВСТУП

Актуальність теми. Сучасний світ змінюється під впливом новітніх загроз і викликів, породжених суспільною дійсністю. У цьому контексті державі відводиться консолідуюча роль, проявом якої має стати рішуча й однозначна позиція щодо її спроможності ефективно на них реагувати та протидіяти. Відповідні завдання мають бути закріплені в основоположних державних документах і реалізовуватися шляхом упровадження стратегічних рішень у пріоритетних галузях і сферах з урахуванням динаміки зовнішнього середовища та впливу внутрішніх чинників.

Аналіз основоположних державних документів дає підстави стверджувати, що Україна змушена протидіяти загрозам глобального й національного рівнів, кожен із яких потребує окремих комплексних управлінських рішень та системи відповідних заходів. Зазначене підтверджується тим, що стаття 17 Конституції України [1] закріплює: «захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього Українського народу».

Реалії сьогодення переконливо доводять, що проблематика публічного управління у сфері інформаційної безпеки набуває особливої ваги в умовах воєнного стану, що зумовлює її комплексний, міждисциплінарний теоретико-прикладний характер. Це положення узгоджується зі стратегічними документами загальнодержавного значення, зокрема Стратегією інформаційної безпеки [2], в якій наголошено, що забезпечення безпеки держави в інформаційній сфері належить до ключових функцій держави.

Актуальність означеного напряму державної політики підсилюється перманентністю, потужністю та довготривалістю інформаційних чинників, здатних впливати як у консолідуючому, так і в дестабілізаційному вимірах соціальної, суспільної та політичної стабільності. У ретроспективному й перспективному аспектах вони можуть проявлятися як конструктивно, так і деструктивно щодо забезпечення суверенітету, незалежності й територіальної

цілісності, оборони держави, захисту прав і свобод громадян, а також підтримання належного рівня національної безпеки.

До глобальних загроз у цій сфері належать дезінформаційні кампанії, спрямовані на маніпулювання суспільною свідомістю, спеціальні інформаційні операції держави-агресора та тривала гібридна війна проти України, цифрові трансформації й вплив соціальних мереж на внутрішню та зовнішню суспільно-політичну ситуацію, а також недостатній рівень медіаграмотності в умовах стрімкого розвитку цифрових технологій.

Національний рівень загроз охоплює інформаційний вплив і тиск держави-агресора на населення України з метою підриву національної безпеки, ліквідації української державності та знищення української ідентичності; обмежені можливості реагування на дезінформаційні кампанії; несформованість системи стратегічних комунікацій; недосконалість законодавства щодо регулювання відносин у сфері інформаційної діяльності медіа; маніпуляції суспільною свідомістю та недостатнє забезпечення інформаційних потреб громадян; низький рівень інформаційної культури й медіаграмотності як чинник вразливості до маніпулятивних і деструктивних інформаційних впливів.

Теоретико-методологічним підґрунтям магістерської роботи стали наукові праці таких зарубіжних авторів, як Д. Белл [3], Н. Вінер [4], М. Мак-Люен [5], Е. Тоффлер [6], К. Шеннон [7], присвячені проблематиці місця й ролі інформації в суспільних відносинах.

Значну увагу аналізу теоретичних і прикладних засад інформаційної проблематики приділено у наукових публікаціях вітчизняних дослідників, зокрема О.В. Буньківської [8], С.С. Єсімова [9], О.В. Нестеренка [10], О.О. Резнікової [11], В.О. Торічного [12] та ін.

Незважаючи на широкий спектр наукових досліджень інформаційної сфери, у галузі знань «Публічне управління та адміністрування» недостатньо уваги приділено комплексному вивченню проблематики публічного управління у сфері інформаційної безпеки в умовах воєнного стану. Відтак

недостатній ступінь розробленості зазначеної проблематики та її виняткове значення для забезпечення стійкого функціонування держави дають підстави стверджувати про актуальність обраної теми.

Мета та завдання магістерської роботи. *Метою* магістерської роботи є обґрунтування теоретичних засад та практичних положень розвитку публічного управління в сфері інформаційної безпеки в Україні в умовах воєнного стану.

Для досягнення мети магістерської роботі було визначено такі *завдання* дослідження:

- розкрити сутність інформаційної безпеки як об'єкта публічного управління;
- провести аналіз зарубіжного досвіду публічного управління в сфері інформаційної безпеки;
- охарактеризувати нормативно-правове регулювання інформаційної безпеки в Україні;
- проаналізувати стан забезпечення інформаційної безпеки та захисту інформаційного простору України в умовах воєнного стану;
- визначити напрями моделювання публічного управління в сфері інформаційної безпеки як складової національної безпеки України;
- запропонувати стратегічні пріоритети розвитку публічного управління в сфері інформаційної безпеки.

Об'єктом дослідження є суспільні відносини, що виникають в сфері інформаційної безпеки.

Предмет дослідження – публічне управління в сфері інформаційної безпеки України в умовах воєнного стану.

Методи дослідження. Для досягнення мети роботи та вирішення поставлених завдань використано комплекс загальнонаукових та спеціальних методів, а саме: *аналізу та синтезу* - для розгляду сутності інформаційної безпеки як об'єкта публічного управління; *порівняльного аналізу* – при аналізі зарубіжного досвіду публічного управління в сфері інформаційної безпеки;

статистичного аналізу – при аналізі стану забезпечення інформаційної безпеки та захисту інформаційного простору України в умовах воєнного стану; *метод моделювання* – при розробці моделі публічного управління в сфері інформаційної безпеки як складової національної безпеки України; *стратегічного аналізу* – при визначенні стратегічних пріоритетів розвитку публічного управління в сфері інформаційної безпеки тощо.

Інформаційною базою дослідження становили нормативно-правові акти, праці зарубіжних і вітчизняних учених, Інтернет-ресурси, статистична інформація тощо.

Практичне значення одержаних результатів полягає у можливості використання висновків та практичних рекомендацій, які містяться в магістерській роботі, як в теоретичному, так і в прикладному значенні при удосконаленні публічного управління в сфері інформаційної безпеки в Україні в умовах воєнного стану.

РОЗДІЛ 1
ТЕОРЕТИЧНІ ЗАСАДИ ПУБЛІЧНОГО УПРАВЛІННЯ В СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

1.1. Сутність та основний зміст інформаційної безпеки як об'єкта публічного управління

Соціальна дійсність сьогодення формує нові умови суспільного життя, у яких інформаційний чинник набуває особливої ваги. Водночас доцільно враховувати, що він охоплює низку взаємопов'язаних складових, які в сукупності визначально впливають на поточний стан та перспективи суспільного розвитку як у прогресивному, так і в регресивному вимірах. З одного боку, простежується об'єктивна необхідність організації інформаційної взаємодії під час формування та структурування всіх сфер суспільного життя, експоненціальне зростання й інтенсивний розвиток нових форм інформаційно-комунікативної взаємодії, а також потреба забезпечення збалансованості, скоординованості та керованості інформаційних процесів. З іншого боку, інформаційний чинник здатний здійснювати потенційний вплив на індивідуальну та масову свідомість, що може призводити до маніпулювання суспільною думкою, посилення негативного впливу на інформаційно-комунікативну взаємодію та, як наслідок, спричиняти небажані деструктивні наслідки, трансформуючи потенційні виклики у реальні загрози.

На думку авторів монографії, «наявність в Україні достатніх передумов для виникнення надзвичайних ситуацій, тенденція зростання їх кількості, важкість ліквідації наслідків і нормалізації обстановки створюють серйозну загрозу безпеці …, а також стабільності розвитку країни» [13, с. 51]. Разом із тим у контексті дослідження публічного управління у сфері інформаційної безпеки в умовах воєнного стану зазначене положення доцільно розглядати ширше, з огляду на загальний характер ризиків та загроз, що можуть впливати на стійкість функціонування держави. Означена теза кореспондує з нормативно визначеним поняттям «загроз національній безпеці України», під

якими розуміються «явища, тенденції і чинники, що унеможливлюють чи ускладнюють або можуть унеможливити чи ускладнити реалізацію національних інтересів та збереження національних цінностей України» [14].

В умовах загроз і викликів сьогодення, що загострюються під час дії правового режиму воєнного стану, забезпечення інформаційної безпеки держави має передбачати формування належного інформаційного середовища та розвиток інформаційної інфраструктури, здатних гарантувати реалізацію конституційних прав і свобод у сфері доступу до інформаційних ресурсів, свободи інформаційної взаємодії, отримання необхідної інформації та користування нею. Водночас такі заходи повинні сприяти забезпеченню ефективного функціонування держави, збереженню непорушності державного устрою й територіальної цілісності, захисту державного суверенітету, досягненню соціальної та політичної стабільності, охороні державних інтересів та потреб, а також розвитку рівноправного й взаємовигідного внутрішньодержавного та міжнародного співробітництва, що в сукупності створює підґрунтя для гармонійного та динамічного розвитку держави.

Проблематика захисту від нових видів небезпек і загроз, що сформувалися у третьому тисячолітті внаслідок процесів інформатизації, активно порушується в наукових дослідженнях сучасного суспільства. Кількість наукових розвідок, присвячених питанням інформаційної безпеки, а також публічного управління в цій сфері, зокрема в умовах воєнного стану, демонструє стійку тенденцію до зростання, що зумовлено посиленням інформаційних впливів, трансформацією характеру загроз та необхідністю формування ефективних управлінських механізмів їх нейтралізації.

З метою формування системного розуміння досліджуваної проблематики доцільно звернутися до лексикографічних джерел. Так, в Енциклопедичному словникові з державного управління зазначається, що під поняттям інформаційного простору слід розуміти «…сукупність сховищ, банків і баз даних, технологій їх супроводу і використання, інформаційних телекомунікаційних систем, що функціонують на основі загальних принципів

і забезпечують інформаційну взаємодію організацій і громадян, а також спрямовані на задоволення їхніх інформаційних потреб» [15, с. 298].

Схожий підхід до визначення технічного аспекту цього поняття пропонує С. С. Єсімов, який розглядає інформаційний простір «…як сукупність баз і банків даних, технологій їх ведення та використання, інформаційно-телекомунікаційних систем і мереж, що функціонують на основі єдиних принципів і за загальними правилами, що забезпечує інформаційну взаємодію організацій і громадян, а також задоволення їх інформаційних потреб» [9, с. 32].

Аналогічної позиції дотримується і О. В. Нестеренко, який зазначає, що «під інформаційним простором будемо розуміти розподілену інформаційну інфраструктуру, що складається з сукупності баз даних і сховищ даних, технологій їхнього супроводу й використання, інформаційних телекомунікаційних систем, що забезпечують інформаційну взаємодію організацій і громадян і задоволення їх інформаційних потреб» [10, с. 51]. Окрім того, дослідник наголошує, що «розглядаючи з інформаційної точки зору середовище адміністративного управління, його можна структурувати на безпосередньо інформаційний простір сфери адміністративного управління, що складається з інформаційних середовищ окремих органів управління, національного інформаційного простору, і навіть глобального інформаційного простору… При цьому на управлінську діяльність мають місце усе більш суттєвий вплив саме останні складові» [10, с. 51–52]. У межах дослідження публічного управління в сфері інформаційної безпеки в умовах воєнного стану така теза є важливою, оскільки підтверджує багаторівневість інформаційного простору та наявність зовнішніх інформаційних впливів, які можуть визначально впливати на державні управлінські процеси.

Сучасний інформаційний простір, за твердженням дослідників, являє собою «…певне високодинамічне комунікаційне середовище, яке функціонує за принципом превалювання цілодобових горизонтальних зв’язків, має практично необмежену джерельну базу й потужний взаємодоповнюваний

вплив на учасників (об'єкти та суб'єкти – індивідів, окремі групи або співтовариства) комунікаційного процесу» [16, с. 12].

В умовах сьогодення, на думку О. В. Буньківської, фактично сформовано новий інформаційний простір, у межах якого суттєво трансформовано комунікативну систему сучасного світу. Характерними ознаками такого простору визначено: глобальність і відсутність реальних міжнаціональних кордонів; доступність та швидкість комунікації в режимі реального часу; відсутність чітких видимих ієрархій, що зумовлює мережеві принципи організації; уявну анонімність за умов реальної прозорості, що створює можливості контролю будь-яких дій; інтеграцію різних видів інформації, зокрема аудіо, відео, друкованої тощо [8, с. 86–87]. Зазначені характеристики є визначальними для дослідження публічного управління у сфері інформаційної безпеки в умовах воєнного стану, оскільки саме вони формують середовище, у якому виникають, поширюються та реалізуються інформаційні загрози, що потребують належної управлінської реакції з боку держави.

Нині пріоритетними напрямами державної політики у сфері інформаційної безпеки в умовах воєнного стану, за словами Р. Ю. Права, мають стати: удосконалення підходів до вітчизняного виробництва контенту; осучаснення нормативно-правового інструментарію забезпечення прав громадян на безперешкодний доступ до інформації; модернізація нормативно-правового забезпечення інформаційної сфери з урахуванням потенційних загроз національній безпеці; задоволення потреб громадян, які проживають на тимчасово окупованих територіях, у неупередженій, оперативній та правдивій інформації [17, с. 49].

Загрози національній безпеці України в інформаційній сфері доцільно розглядати як систему чинників та умов, що становлять суттєву небезпеку інтересам особи, суспільства та держави й проявляються через інформаційний вплив на свідомість людей, їх поведінку, а також негативно впливають на інформаційні ресурси країни. У зв'язку з цим одним із ключових завдань

держави у сфері інформаційної безпеки є забезпечення захисту інформаційного суверенітету, формування, підтримка та розвиток ефективної мережі й інформаційної інфраструктури, а також розробка та результативне впровадження стратегій і планів дій щодо протидії інформаційним та кіберзагрозам [17, с. 72–74].

У контексті зазначеного заслуговує на увагу позиція О. В. Власенко, відповідно до якої негативні тенденції розвитку національного інформаційного простору, кризові явища в економіці України та інші чинники зумовлюють ескалацію загроз, що призводить до значних втрат політичного, економічного, воєнного та іншого характеру, завдаючи шкоди громадянам України [18, с. 46].

Досліджуючи сутність інформаційної безпеки, С. А. Палій розкриває її через характеристику стану інформаційного простору держави. Так, інформаційна безпека визначається як стан інформаційного простору, у межах якого забезпечуються потреби всіх суб'єктів інформаційних відносин у необхідних обсягах інформаційних ресурсів, гарантується їх безпечність, а також захист громадян, організацій, суспільства та держави загалом від виникнення негативного інформаційного впливу [19, с. 51].

Розвиваючи наведений підхід, В. О. Торічний акцентує увагу на тому, що ефективність функціонування соціально-економічних комплексів і систем управління безпосередньо залежить від стану інформаційної безпеки, під якою переважно розуміється стан захищеності інформаційного середовища (простору) суспільства, що забезпечує його формування та розвиток в інтересах громадян, організацій і держави [12, с. 189].

Водночас у наукових джерелах висловлюється думка, що загрозою національній безпеці України в інформаційній сфері залишається невиваженість державної політики, оскільки державне управління інформаційною сферою продовжує бути однією з найбільш неврегульованих сфер державно-управлінської діяльності [20, с. 70]. Поряд із цим підкреслюється, що складова національних інтересів в інформаційній сфері,

обумовлена інтересами суспільства, полягає у використанні інформації для розвитку всіх сфер життя, зміцнення демократії та досягнення суспільної злагоди, тоді як інтереси держави в інформаційній сфері полягають у створенні умов для зміцнення конституційного ладу, суверенітету й територіальної цілісності країни, політичної та соціальної стабільності, економічного процвітання, збереження правопорядку та розвитку міжнародного співробітництва [20, с. 71].

Дослідження останніх років засвідчують, що в сучасних умовах інформаційних протистоянь національний інформаційний простір України залишається недостатньо захищеним від зовнішніх інформаційних впливів і загроз. У зв'язку з цим захист інформаційного суверенітету, формування потужної та ефективної системи інформаційної безпеки в Україні, а також розробка дієвих стратегій і тактик протидії медійним загрозам мають розглядатися як пріоритетні завдання органів державної влади та інших інституцій в умовах воєнного стану [21, с. 153].

Таким чином, результати аналізу наукових досліджень у зазначеному напрямі дають підстави констатувати, що більшість авторів зосереджують увагу на обґрунтуванні теоретико-прикладних засад публічного управління у сфері забезпечення інформаційної безпеки, аналізі наукових підходів до публічного управління інформаційними процесами та визначенні механізмів реалізації державної політики в означеній сфері. На цій основі можна резюмувати, що науковий дискурс здебільшого концентрується на трьох ключових аспектах проблематики публічного управління у сфері інформаційної безпеки: технічному, комунікаційному та інформаціологічному.

1.2. Зарубіжний досвід публічного управління в сфері інформаційної безпеки

У сучасних умовах воєнного стану питання забезпечення інформаційної безпеки набуває особливої актуальності, оскільки інформаційний простір

перетворюється на один із ключових напрямів протиборства, що впливає на стійкість державного управління, суспільну стабільність та рівень довіри до публічних інституцій. З огляду на зростання масштабів дезінформаційних кампаній, спеціальних інформаційних операцій, кіберзагроз та маніпулятивних впливів на масову свідомість, публічне управління в сфері інформаційної безпеки потребує комплексного підходу, який поєднує нормативно-правові, організаційні, технологічні та комунікаційні інструменти з метою захисту інформаційного суверенітету та забезпечення національних інтересів.

Водночас ефективність державної політики у сфері інформаційної безпеки значною мірою визначається здатністю застосовувати перевірені управлінські практики та адаптувати їх до національних умов і реалій воєнного часу. Саме тому особливого значення набуває вивчення зарубіжного досвіду публічного управління в сфері інформаційної безпеки, зокрема моделей організації системи стратегічних комунікацій, механізмів протидії дезінформації, інституційної координації кіберзахисту, а також підходів до забезпечення балансу між безпековими потребами держави та дотриманням демократичних стандартів і прав людини. Аналіз таких практик створює підґрунтя для визначення перспективних напрямів удосконалення національної системи публічного управління інформаційною безпекою в умовах воєнного стану.

Сьогодні сфера інформаційної діяльності та забезпечення інформаційної безпеки держави набуває особливої ваги, зокрема в умовах воєнного стану, коли інформаційні чинники в системі публічного управління мають одночасно консолідуючий і дестабілізуючий потенціал. За таких обставин інформаційний простір перетворюється на стратегічно важливий ресурс, а ефективність управлінських рішень у цій сфері безпосередньо впливає на здатність держави забезпечувати стійкість, керованість та належний рівень національної безпеки.

Недооцінювання або ігнорування інформаційних загроз у період воєнного стану може призвести до значних негативних наслідків, зокрема

ресурсних втрат, послаблення суспільної довіри, погіршення міжнародного іміджу та зниження репутаційної стійкості державних інституцій. У зв'язку з цим актуалізується потреба у формуванні результативних механізмів публічного управління в сфері інформаційної безпеки, здатних забезпечити системну протидію дезінформаційним впливам, кіберзагрозам та іншим деструктивним чинникам, що супроводжують воєнні конфлікти.

Розуміючи важливість і складність порушених питань, держави світу намагаються віднаходити дієві інструменти й вживати ефективних заходів задля забезпечення власної інформаційної безпеки.

Відповідно до Постанови Ради міністрів про заснування посади Урядового уповноваженого з питань безпеки інформаційного простору Республіки Польща 2022 року [22] до завдань відповідної посадової особи віднесено:

1. Координацію діяльності органів державного управління, до компетенції яких належить виявлення, моніторинг і нейтралізація інформаційних загроз інтересам держави, зокрема у частині розпізнавання та нейтралізації загроз інформаційній безпеці держави, а також реагування на них. До таких загроз, зокрема, належать:

– виявлення та аналіз інформаційної діяльності, основним фокусом якої є безпека, інтереси та імідж Республіки Польща;

– ідентифікація суб'єктів, насамперед іноземних, які організовують та здійснюють інформаційну діяльність всупереч інтересам Республіки Польща;

– відстеження проявів інформаційно-психологічних операцій, що здійснюються в інформаційному просторі проти держави;

– реалізація заходів, спрямованих на нейтралізацію виявлених загроз інформаційній безпеці Республіки Польща;

– упровадження заходів щодо підвищення стійкості держави в інформаційній сфері шляхом:

а) публікації досліджень з питань забезпечення інформаційної безпеки;

б) здійснення інформаційної діяльності, спрямованої на зміцнення безпеки, інтересів та іміджу держави;

в) координації інформаційно-комунікативної діяльності установ, відповідальних за формування інформаційної політики Республіки Польща.

2. Розроблення рекомендацій для Ради міністрів з метою пошуку системних рішень, спрямованих на підвищення здатності Республіки Польща протистояти інформаційним загрозам в умовах загострення безпекових викликів.

Аналіз повноважень Урядового уповноваженого з питань безпеки інформаційного простору Республіки Польща свідчить, що відповідна посадова особа за своїми функціональними обов'язками охоплює широкий спектр завдань щодо забезпечення інформаційної безпеки держави як загалом, так і в умовах загрози чи виникнення надзвичайних і кризових явищ, що є релевантним і для періоду воєнного стану. Це дає підстави припустити, що запровадження аналогічних посад в інших державах і поширення позитивного досвіду окремих країн у межах загального підходу Європейського співтовариства може сприяти суттєвим позитивним зрушенням у напрямі зміцнення національної стійкості в інформаційній сфері.

Подібна практика функціонує і в Канаді, зокрема у провінції Онтаріо, починаючи з 1987 року. Уповноважений з питань інформації та конфіденційності здійснює нагляд за дотриманням вимог інформаційного законодавства, призначається Законодавчою асамблеєю Онтаріо та звітує перед нею, залишаючись незалежним від чинного уряду.

Основні завдання цієї посадової особи зводяться до такого:

– розгляд звернень щодо надання доступу до інформації;

– проведення розслідувань у зв'язку з поданням скарг стосовно порушення права на конфіденційність;

– здійснення експертизи проєктів урядових нормативних актів і програм;

– моніторинг та перегляд політики конфіденційності й практик управління інформацією;

– проведення досліджень з питань доступу до інформації та забезпечення конфіденційності;

– інформування громадськості, засобів масової інформації та інших заінтересованих сторін про нормативні документи провінції Онтаріо щодо забезпечення доступу й конфіденційності, а також про актуальні питання, що впливають на реалізацію політики у відповідній сфері [23].

Зазначені пріоритети спрямовані на розв'язання ключових проблем у сфері забезпечення конфіденційності та гарантування прав мешканців провінції Онтаріо на доступ до інформації в сучасних умовах, коли світ дедалі більше функціонує на основі даних, а організації прискорюють використання цифрових інструментів і технологій штучного інтелекту.

Уповноважений з питань інформації Великої Британії є незалежним суб'єктом, створеним у 1984 році з метою забезпечення захисту права на інформацію в суспільних інтересах, сприяння відкритості діяльності органів державної влади та забезпечення конфіденційності персональних даних.

Відповідно до стратегічного плану діяльності на період до 2025 року довгострокові стратегічні цілі його діяльності визначено так:

– захист і розширення можливостей людей;

– сприяння відповідальним інноваціям і сталому економічному зростанню;

– підтримка відкритості, прозорості та підзвітності;

– безперервний розвиток організаційної культури, можливостей і потенціалу установи [24].

Г. М. Проскура щодо перспектив створення інституту інформаційного комісара в Україні наведить дані, що у світі відповідні функції реалізуються різними інституційними моделями, зокрема через:

– інформаційного комісара (Шотландія, Велика Британія, Угорщина, Словенія, Сербія);

– комісію або інститут (Португалія, Франція, Мексика);

– омбудсмена, наділеного повноваженнями нагляду (Нова Зеландія, Боснія, Норвегія, Швеція);

– інші уповноважені органи (Туреччина, ПАР) [25, с. 120–121].

Авторка підкреслює необхідність інституціоналізації подібної посади в українських реаліях. Цю позицію підтримують і автори публікації [26], наголошуючи, що актуальність її запровадження посилюється сучасними подіями в Україні, коли держава перебуває в умовах гібридного протистояння, а інформація виступає одним із ключових інструментів його ведення.

З метою формування цілісного уявлення про успішні практики публічного управління у сфері інформаційної безпеки доцільно звернутися до аналізу функціонування відповідних систем у Сполучених Штатах Америки та в Європейському Союзі.

Забезпечення інформаційної безпеки у Сполучених Штатах Америки розглядається як невід'ємна складова національної безпеки, що визначає високий рівень інституційної залученості держави та системність управлінських підходів у цій сфері. Одним із ключових системоутворюючих суб'єктів державного регулювання виступає Міністерство оборони США, яке охоплює значну кількість підвідомчих структур та забезпечує реалізацію безпекових функцій у межах відповідної політики. Фінансування заходів у сфері інформаційної безпеки здійснюється на підставі бюджетних рішень Конгресу, при цьому запит на фінансування формується Адміністрацією Президента. Водночас стратегічні орієнтири розвитку галузі визначаються за участю Президента, Ради національної безпеки та Комітету начальників штабів, що свідчить про пріоритетність інформаційної безпеки в державній політиці США.

Суттєвим показником стратегічної уваги до зазначеної сфери є масштаб фінансових ресурсів, які спрямовуються на діяльність численних інститутів, агентств та органів влади. Зокрема, прямі видатки на вирішення питань кібербезпеки демонструють стійку тенденцію до зростання. Так, Адміністрація Президента запропонувала у федеральному бюджеті США на

2025 рік передбачити 27,5 млрд доларів на кібербезпеку, що відображає послідовне зосередження на захисті кіберпростору як важливого елементу загальної системи національної безпеки [27].

Нормативно-правове регулювання інформаційної безпеки США характеризується складністю та розгалуженістю, а відповідні питання врегульовуються переважно на рівні федерального законодавства. Одним із перших фундаментальних законодавчих актів у цій сфері став Закон про інформаційну безпеку [28], який визначив мінімальні вимоги до захисту федеральних інформаційних систем і сформував правову основу для становлення федеральної системи забезпечення інформаційної безпеки. Відповідно до положень цього закону оператори федеральних інформаційних систем, що містять конфіденційну інформацію, були зобов'язані розробляти власні плани забезпечення інформаційної безпеки.

Подальший розвиток інституційного механізму управління інформаційною безпекою відбувався через ухвалення стратегічних документів і створення нових координаційних органів. Так, у 2000 році "Національним планом захисту інформаційних систем на 2000–2003 рр." [29] було започатковано новий координуючий орган – Національну консультативну раду з інфраструктури (NIAC), а також підтримано формування спеціальних відомчих центрів інформаційної безпеки. Їх діяльність, зокрема, передбачала використання федеральної мережі виявлення вторгнень (FIDNet), що забезпечувала виявлення атак і сповіщення державних, приватних та інших суб'єктів про загрози інформаційній безпеці.

У жовтні 2001 року було ухвалено "Акт про патріотизм" [30], яким визначено системи й засоби, критично важливі для США настільки, що їх вихід з ладу або знищення може спричинити суттєві негативні наслідки для оборони, економіки, охорони здоров'я та загальної безпеки нації. У межах цього підходу було окреслено поняття критичної інформаційної інфраструктури, до якої віднесено широке коло сфер, зокрема економіку,

соціальну сферу, засоби зв'язку, енергетику, транспорт, органи державної влади тощо.

Наступним етапом стало формування державної політики у сфері внутрішньої безпеки, де захист критичної інформаційної інфраструктури посів одне з центральних місць. У 2002 році Міністерство внутрішньої безпеки США представило Національну стратегію внутрішньої безпеки [31], у якій захист критичної інформаційної інфраструктури визначено як ключове завдання забезпечення національної безпеки. Закон "Про внутрішню безпеку" 2002 року [32] закріпив створення спеціального Комітету та Міністерства внутрішньої безпеки, основним пріоритетом яких стало зниження вразливості інформаційної інфраструктури США. У структурі Міністерства внутрішньої безпеки було сформовано низку спеціалізованих підрозділів, серед яких Управління аналізу інформації та захисту інфраструктури (IAIP), Управління науки та технологій (S&T), Національний підрозділ кібернетичної безпеки (NCSD), а також Центр екстреного реагування на комп'ютерні інциденти (US-CERT), утворений шляхом об'єднання кількох раніше існуючих структур негайного реагування.

Особливістю американського підходу є те, що регулювання безпеки критичної інформаційної інфраструктури здійснюється з урахуванням специфіки кожного критично важливого сектору, який має власні операційні моделі, характеристики та профілі ризиків. Відповідно, у межах кожної сфери функціонують галузеві агентства, які володіють спеціалізованими інституційними знаннями та повноваженнями. При цьому нормативне регулювання окремих секторів (наприклад, енергетики чи зв'язку) забезпечують уповноважені органи, здатні видавати обов'язкові до виконання нормативно-правові акти.

Водночас значна кількість регуляторів і нормативних актів є характерною рисою американської моделі, що створює складність її прямої імплементації в інших юрисдикціях. Крім того, Державний департамент у взаємодії з Міністерством національної безпеки та іншими федеральними

структурами залучає іноземні уряди й міжнародні організації до діяльності, спрямованої на зміцнення безпеки та стійкості критичної інформаційної інфраструктури за межами США, а також сприяє обміну кращими практиками у цій сфері.

У 2003 році було прийнято "Національну стратегію фізичного захисту критичної інфраструктури та найважливіших об'єктів" [33], яка визначила стратегічні цілі, принципи та завдання державних структур щодо забезпечення безпеки критичної інфраструктури. У тому ж році оприлюднено "Національну стратегію захисту кіберпростору" [34], у якій акцент зроблено на стандартизації та координації взаємодії державного й недержавного секторів, а також на підвищенні ролі приватних суб'єктів у забезпеченні інформаційної безпеки.

В американській системі до регуляторів, що здійснюють повноваження у сфері інформаційної безпеки, належать, зокрема, Федеральна комісія зв'язку (FCC), Міністерство внутрішньої безпеки (DHS), Міністерство оборони (DoD), Міністерство юстиції (DoJ), Федеральне бюро розслідувань (FBI), Агентство з кібербезпеки та захисту інфраструктури (CISA), Національний інститут стандартів і технологій (NIST), а також Національна об'єднана робоча група з кіберрозслідувань (NCIJTF). Їх діяльність охоплює визначення пріоритетів у сфері комунікаційної інфраструктури, аналіз загроз та уразливостей, координацію взаємодії між державним і приватним секторами, розроблення національних планів, проведення розслідувань кіберзлочинів, нарощування національного потенціалу кіберзахисту та методологічне забезпечення стандартів інформаційної безпеки.

Узагальнюючи, можна констатувати, що організаційна структура системи забезпечення інформаційної безпеки США демонструє тісний взаємозв'язок між інформаційною безпекою та національно-оборонним компонентом, оскільки ключову роль у відповідному регулюванні відіграють Міністерство оборони та Міністерство внутрішньої безпеки. Водночас ефективність такої моделі значною мірою забезпечується масштабним

фінансуванням, наявністю спеціалізованих структур у межах різних відомств та високими кадровими вимогами. Разом із тим зазначений підхід потребує значних ресурсів на координацію між уповноваженими органами, а також може ускладнювати реалізацію відповідних програм за умов дефіциту висококваліфікованих фахівців у сфері інформаційної та кібербезпеки.

З метою забезпечення комплексності аналізу зарубіжного досвіду доцільно розглянути європейські підходи до публічного управління у сфері інформаційної безпеки. Слід відзначити, що в державах Європейського Союзу впродовж останніх років простежується тенденція до посилення державного контролю в межах контрольно-наглядової діяльності, що проявляється у прийнятті нових законодавчих норм, розширенні повноважень спеціальних служб, уточненні вимог до суб'єктів інформаційних відносин, а також запровадженні фінансових санкцій за порушення встановлених правил.

Одним із ключових пріоритетів ЄС у сфері інформаційної безпеки є захист персональних даних. Міжнародне визнання важливості цієї проблематики було закріплено ще у 1981 році шляхом ухвалення країнами Ради Європи Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних [35]. Водночас показовим прикладом системного підходу Європейського Союзу до захисту даних виступає Загальний регламент із захисту даних (GDPR) [36], розроблений та схвалений Європейським парламентом у 2016 році, який набрав чинності у 2018 році. Важливо, що GDPR має екстериторіальний характер і поширює свою дію на широкий спектр сфер суспільного життя, забезпечуючи захист персональних даних громадян ЄС не лише в межах держав-членів, а й поза територією Європейського Союзу. У разі порушення його вимог передбачено значні фінансові санкції, що можуть сягати 20 млн євро або 4% обороту порушника.

З метою дотримання стандартів GDPR суб'єкти, які здійснюють обробку персональних даних, мають впроваджувати внутрішні політики захисту даних, організовувати навчання персоналу, проводити перевірки діяльності з обробки інформації, вести документацію щодо відповідних процесів, реалізовувати

принципи вбудованої конфіденційності, а також визначати відповідальних осіб за обробку персональних даних. У цілому GDPR розглядається як базовий нормативний акт, що суттєво підвищив рівень захисту даних у ЄС та за його межами, забезпечивши уніфікованість правил і підвищивши довіру громадян. Крім того, він сприяв спрощенню процедур дотримання єдиного набору вимог для позаєвропейських суб'єктів та зменшенню витрат і бюрократичних процедур, що в підсумку розглядається як фактор стимулювання економічного розвитку.

Нормативно-правові акти ЄС у сфері інформаційної безпеки засвідчують, що, попри наявні виклики, пов'язані з відмінностями у рівні розвитку держав-членів, підходи до формування та вдосконалення систем інформаційної безпеки в Європейському Союзі активно розвиваються. Цей процес відбувається завдяки накопиченню практичного досвіду регулювання, посиленню координації між державами та застосуванню системних стратегій, що підтверджує важливість реагування на нові виклики й загрози в кіберпросторі як стимулу формування спільного політичного простору ЄС.

У межах організації робіт у сфері інформаційної безпеки ЄС суттєве значення має співпраця з міжнародними структурами, зокрема в контексті координації заходів із протидії злочинам у сфері інформаційних технологій. Разом із тим аналіз функцій і повноважень ключових органів ЄС свідчить, що системний підхід до забезпечення інформаційної безпеки реалізується як на рівні Союзу та держав-членів, так і на рівні державних і приватних організацій. У Європі чітко простежується усвідомлення необхідності посилення взаємодії та координації між різними інституціями. Для підтримки належного рівня кібербезпеки ЄС взаємодіє з низкою міжнародних організацій, при цьому центральне місце посідає співробітництво ЄС із НАТО.

Серед ключових регуляторів у сфері інформаційної безпеки ЄС важливу роль відіграє Європейське агентство з мережевої та інформаційної безпеки (ENISA) [37], яке сприяє державам-членам у виконанні чинних і майбутніх вимог законодавства ЄС, підтримує організацію загальноєвропейських

навчань з кібербезпеки та виступає центром експертних знань для держав-членів і установ ЄС. Європейський центр боротьби з кіберзлочинністю (EC3) [38] функціонує як центр кіберкримінальної інформації та розвідки, забезпечує підтримку операцій з розслідування кіберзлочинів, реалізує стратегічний аналіз, сприяє кооперації правоохоронних органів із приватним сектором і науковими колами, а також надає спеціалізовану технічну підтримку. Європейський контролер із захисту даних (EDPS) [39] здійснює моніторинг дотримання правил захисту персональних даних у межах установ і органів ЄС, надає консультації, аналізує технології, що можуть впливати на конфіденційність, та взаємодіє з іншими наглядовими органами з метою підвищення узгодженості процедур. Координаційну функцію між державами-членами забезпечує Група співробітництва (NIS) [40], діяльність якої спрямована на підтримку стратегічного співробітництва та обміну інформацією.

Окремим напрямом діяльності ЄС у межах забезпечення інформаційної безпеки є протидія дезінформації. Для координації зусиль у цій сфері ЄС зосереджується на посиленні інституційних спроможностей щодо виявлення та аналізу дезінформації, забезпеченні скоординованої відповіді, залученні приватного сектору, а також підвищенні обізнаності й стійкості суспільства. У Плані дій щодо боротьби з дезінформацією [41] наголошено, що дезінформація є суттєвим викликом для демократичних систем, оскільки підриває довіру громадян до інститутів, сприяє поляризації суспільства та впливає на процеси ухвалення рішень. У зв'язку з цим у 2018 році було прийнято Кодекс практики ЄС щодо протидії дезінформації [42], який у 2022 році доповнено й розширено. Документами передбачено заходи, спрямовані на впровадження політик протидії введенню в оману, інвестування в технологічні рішення для просування достовірної інформації, зменшення видимості дезінформації, надання користувачам інструментів для пошуку надійного контенту та повідомлення про дезінформацію, забезпечення

доступу до даних із дотриманням конфіденційності, а також підвищення рівня медіаграмотності населення.

РОЗДІЛ 2
СУЧАСНИЙ СТАН ПУБЛІЧНОГО УПРАВЛІННЯ В СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

2.1. Нормативно-правове регулювання інформаційної безпеки в Україні

Проблематика формування та подальшого розвитку правового поля щодо захисту інформаційного простору держави набуває особливої актуальності з огляду на мінливість зовнішніх і внутрішніх чинників, які мають критичний вплив на відповідну сферу публічного управління. Інформаційний фронт у глобальних і національних конфліктах посідає провідне місце та охоплює, зокрема, контроль над засобами масової інформації, протидію дезінформації та підтримку свободи медіа. Захист критично важливих інформаційних систем, державних електронних інформаційних ресурсів і даних є одним із ключових завдань забезпечення національної безпеки та суспільної стабільності, а також належного функціонування національної системи стійкості.

Україна послідовно здійснює роботу з удосконалення правової бази у сфері захисту інформаційного простору держави, яка охоплює різні напрями цієї комплексної проблематики. Саме тому, з урахуванням наведених вище чинників, становлення та розвиток правового поля України у сфері захисту інформаційного простору доцільно розглядати як невід'ємну складову забезпечення національної безпеки та збереження інформаційного суверенітету держави.

Захист суверенітету, територіальної цілісності та забезпечення національної безпеки належать до найважливіших завдань будь-якої держави, зокрема й України, що закріплено статтею 17 Конституції України [1]. Зазначені положення виступають фундаментом для гарантування всіх інших прав і свобод громадян, а також для забезпечення соціального й економічного розвитку держави.

У Законі України «Про національну безпеку України» визначено, що державна політика «…спрямовується на забезпечення… інформаційної,… кібербезпеки України та на інші її напрями» [14]. Відповідні напрями конкретизовано у Стратегії національної безпеки України [43], у якій зазначено про наявність критичних проблем в інформаційній сфері, посилення інструментів національної сили (зокрема інформаційно-психологічних і кіберзасобів), застосування інформаційної «зброї», а також констатовано відсутність цілісної державної інформаційної політики.

Інформаційна безпека передбачає захист інформаційного простору держави від зовнішнього впливу, дезінформації та інших загроз, здатних завдати шкоди суспільству та державі. Забезпечення всіх складових національної безпеки потребує спільних зусиль держави й громадян, а також розроблення результативних стратегій і політик у відповідних сферах.

Стратегією інформаційної безпеки України [2] унормовано загальні положення щодо забезпечення інформаційної безпеки держави, зокрема шляхом визначення актуальних викликів і загроз у цій сфері. Документом встановлено стратегічні цілі та завдання, спрямовані на протидію загрозам, а його мета полягає в посиленні спроможностей держави в інформаційній сфері, захисті її інформаційного простору та забезпеченні стійкості суспільства і держави. У тексті Стратегії наведено визначення ключових понять, зокрема «інформаційна безпека України», «інформаційна загроза», «інформаційні заходи оборони держави» тощо.

Так, інформаційна безпека України відповідно до визначення, поданого у Стратегії, є «складовою частиною національної безпеки України, станом захищеності державного суверенітету, територіальної цілісності, демократичного конституційного ладу, інших життєво важливих інтересів людини, суспільства і держави, за якого належним чином забезпечуються конституційні права і свободи людини на збирання, зберігання, використання та поширення інформації, доступ до достовірної та об’єктивної інформації, існує ефективна система захисту і протидії нанесенню шкоди через поширення

негативних інформаційних впливів, у тому числі скоординоване поширення недостовірної інформації, деструктивної пропаганди, інших інформаційних операцій, несанкціоноване розповсюдження, використання й порушення цілісності інформації з обмеженим доступом» [2].

Стратегія визначає основні напрями та принципи забезпечення інформаційної безпеки України, формуючи правову, стратегічну й організаційну основу відповідної діяльності держави.

У документі наведено низку глобальних викликів і загроз у сфері інформаційної безпеки. Зокрема, збільшення масштабів дезінформаційних кампаній, ініційованих авторитарними режимами та радикальними активістами, стало характерною ознакою сучасності, створюючи ризики для демократичного розвитку та міжнародної стабільності. Окрема увага приділяється інформаційній політиці Російської Федерації, яка впливає на демократичні інституції та поглиблює протиріччя в демократичних державах через спеціальні інформаційні операції та гібридну війну.

Також у Стратегії підкреслюється роль соціальних мереж у сучасному інформаційному просторі, значення яких зросло під впливом глобалізації та пандемії COVID-19. Наголошується, що розвиток цифрових технологій може створювати загрози праву на приватність і призводити до ускладнень у гарантуванні безпеки персональних даних. Окремим викликом визначено недостатній рівень медіаграмотності, що спричиняє некритичне сприйняття інформації. Поєднання широкої доступності інформації та низької медіаграмотності сприяє поширенню дезінформації, конспірологічних теорій і маніпуляцій, що може негативно позначатися на стабільності демократичних держав.

Розділ «Національні виклики та загрози» висвітлює інформаційні загрози, з якими стикається Україна на національному рівні. До таких загроз віднесено інформаційний вплив рф як держави-агресора на населення України. рф використовує різні методи інформаційного впливу, спрямовані на

підрив національної безпеки, ліквідацію української державності та знищення української ідентичності, що спричиняє дестабілізацію суспільства.

На тимчасово окупованих територіях рф забезпечує інформаційне домінування через придушення свободи слова, контроль над засобами масової інформації, повне обмеження доступу до незалежних джерел та формування альтернативної викривленої інформаційної реальності. Україна стикається зі складнощами реагування на зазначені загрози через обмежені можливості протидії інформаційній агресії. Відсутність дієвої системи реагування та розвиненої інформаційної інфраструктури обмежує спроможність ефективно протидіяти дезінформаційним кампаніям, що створює ризики для національної безпеки та інтересів держави.

Зазначений розділ підкреслює необхідність розвитку стратегічних підходів і національних заходів протидії інформаційним загрозам, зокрема шляхом підготовки та розбудови інформаційної стійкості суспільства.

У Стратегії також розглянуто інші аспекти інформаційної безпеки, зокрема:

– попри здійснення заходів щодо посилення інституційної спроможності у сфері стратегічних комунікацій, в Україні відсутній ефективний механізм координації та взаємодії між органами державної влади, що ускладнює комплексне стратегічне планування інформаційних потоків, співпрацю між ключовими суб'єктами інформаційних відносин і реалізацію політики захисту національного інформаційного простору;

– наявні проблеми нормативного регулювання у сфері медіа та журналістики, оскільки недостатність адаптованих до сучасних викликів правових рамок ускладнює розвиток медіаринку, зберігає залежність ЗМІ та інколи призводить до посягань на свободу журналістської діяльності й безпеку журналістів;

– спроби дестабілізувати суспільну консолідацію щодо європейської та євроатлантичної інтеграції через поширення міфів і дезінформаційних

стереотипів, що може впливати на реформи та зовнішньополітичний курс держави;

– потреба підвищення рівня інформаційної грамотності населення для більш ефективної протидії дезінформації та маніпуляціям.

Стратегічні цілі та напрями реалізації Стратегії інформаційної безпеки України [2] охоплюють різні складові інформаційної безпеки та спрямовані на захист національних інтересів, забезпечення стабільності суспільства і підвищення інформаційної культури, що сприяє консолідації суспільства.

Очікувані результати реалізації Стратегії виступають індикаторами її ефективності та відображають позитивні зміни, яких передбачається досягти завдяки реалізації визначених стратегічних напрямів, а саме:

– захищений інформаційний простір України, що передбачає належний рівень протидії негативним впливам, дезінформації та маніпуляціям, здатним завдати шкоди національній безпеці та суспільній стабільності;

– ефективне функціонування системи стратегічних комунікацій, що забезпечить взаємодію органів влади та інших суб'єктів публічного управління, координацію інформаційної діяльності та досягнення спільних цілей;

– результативна протидія поширенню незаконного контенту в глобальній телекомунікаційній мережі;

– забезпечення інформаційної реінтеграції громадян, які проживають на тимчасово окупованих територіях, шляхом доступу до українського інформаційного простору та телерадіомовлення;

– підвищення рівня медіакультури та медіаграмотності населення, що сприятиме критичному сприйняттю інформації та зменшенню ризиків поширення дезінформації;

– дотримання конституційних прав, включаючи право на свободу вираження поглядів і переконань, гарантування приватності та захист журналістів;

– формування громадянської ідентичності на основі українських цінностей, традицій, культури та історії.

Зазначені результати мають сприяти зміцненню інформаційної безпеки, стабільності та суверенітету України.

Стратегія кібербезпеки України, затверджена відповідним указом Президента України [44] і така, що, зокрема, ґрунтується на положеннях Закону України «Про основні засади забезпечення кібербезпеки України» [45], визначає актуальність кібербезпеки як одного з пріоритетів національної безпеки України. У документі відзначено роль інформаційних технологій і кіберпростору в сучасному світі та акцентовано увагу на ризиках, пов'язаних з їх використанням. Підкреслюється значення захисту від новітніх кіберзагроз у контексті активізації кібертероризму, а також важливість захисту об'єктів критичної інформаційної інфраструктури й інших інфраструктурних об'єктів від кібератак.

Документ наголошує, що Російська Федерація є одним із основних джерел кіберзагроз та гібридної війни проти України, що актуалізує потребу в зміні стратегій і тактик протидії кіберзагрозам та розвідувально-підривній діяльності у кіберпросторі. Також підкреслено важливість взаємодії всіх суб'єктів, залучених до забезпечення кібербезпеки, для гарантування безпеки в цифровому середовищі.

Водночас Україна розглядається як держава, яка здатна і повинна забезпечити власний розвиток у цифровому світі та гарантувати безпеку свого кіберпростору, зокрема шляхом визначення пріоритетів і завдань у цій сфері.

Сприятливий стан кібербезпеки є важливим для національної безпеки та належного функціонування всіх сфер, які використовують інформаційні технології. Його забезпечення неможливе без урахування сучасних викликів і загроз, що стоять перед Україною в цій сфері, а також без конкретизації труднощів і завдань, які потребують розв'язання.

Отже, для подолання окреслених проблем та забезпечення кібербезпеки України необхідно реалізувати комплекс заходів, серед яких:

– розвиток і вдосконалення нормативно-правової бази у сфері кібербезпеки, включаючи законодавство, що регулює функціонування критичної інфраструктури;

– створення системи оцінювання та сертифікації безпеки інформаційних систем і продуктів;

– удосконалення підходів до кібергігієни та впровадження заходів із підвищення цифрової грамотності населення;

– забезпечення належного фінансування та контролю за кіберзахистом у державних органах;

– розвиток систем інформаційно-аналітичного забезпечення кібербезпеки для виявлення та реагування на загрози;

– підвищення кваліфікації фахівців у сфері кібербезпеки;

– розвиток міжнародної співпраці для обміну інформацією та спільного реагування на кіберзагрози.

Зазначені заходи, що корелюють із пріоритетами кібербезпеки України, стратегічними цілями та завданнями, визначеними у Стратегії кібербезпеки України [44], сприятимуть поліпшенню стану кібербезпеки та посиленню стійкості в умовах зростання кіберзагроз. Артикуляція стратегії розвитку кібербезпеки України відображає послідовне ставлення держави до захисту в кіберпросторі та підкреслює значення багатосторонньої співпраці, внутрішніх механізмів координації й відкритості для різних учасників. Орієнтація на права і свободи людини, а також на соціальний, політичний та економічний розвиток, засвідчує важливість збалансованого підходу до забезпечення кібербезпеки в Україні.

Сформульовані індикатори та механізм моніторингу реалізації Стратегії кібербезпеки України відображають системний і проактивний підхід, оскільки застосування індикаторів стану кібербезпеки дає змогу вимірювати досягнення визначених завдань і цілей, забезпечуючи прозорість та можливість коригування стратегії в режимі реального часу.

Відповідно до Стратегії забезпечення державної безпеки інформаційна безпека визначається як «стан захищеності національних інтересів людини, суспільства і держави в інформаційній сфері, за якого унеможливлено завдання шкоди через: неповноту, невчасність та невірогідність інформації, що використовується, негативний інформаційний вплив; витік державної таємниці та службової інформації; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації, у тому числі шляхом проведення іноземними спецслужбами, окремими організаціями, групами, особами спеціальних інформаційних операцій та деструктивних інформаційних впливів, а також забезпечується своєчасне виявлення, запобігання та нейтралізація реальних і потенційних загроз національним інтересам та національній безпеці України. Інформаційна безпека є складовою національної безпеки України» [46].

У документі наведено розгорнутий огляд загроз державній безпеці України. Підкреслено, що рф продовжує застосовувати гібридні методи впливу, включаючи кібератаки, з метою досягнення стратегічних цілей в Україні. Окупаційна адміністрація та самопроголошені органи на тимчасово окупованих територіях порушують міжнародне право та створюють загрози державній безпеці. Деструктивна пропаганда та відсутність цілісної інформаційної політики ускладнюють безпекову ситуацію. У зв’язку з цим наголошується на необхідності підтримки та посилення заходів щодо підвищення кібербезпеки, розвитку інформаційної інфраструктури, зміцнення системи стратегічних комунікацій та реформування сектору безпеки з метою нейтралізації загроз і забезпечення національної безпеки загалом. Особливу увагу у документі приділено необхідності впровадження проактивного підходу, заснованого на управлінні ризиками.

Таким чином, можна констатувати, що стан нормативно-правового регулювання питань захисту інформаційного простору України є складним і

потребує постійного оновлення та вдосконалення відповідно до сучасних викликів і загроз, які з часом набувають більшої різноманітності та складності.

2.2. Аналіз забезпечення інформаційної безпеки та захисту інформаційного простору України в умовах воєнного стану

Сучасний етап розвитку України характеризується функціонуванням держави в умовах повномасштабної воєнної агресії, що суттєво трансформує підходи до публічного управління у сфері інформаційної безпеки. Воєнний стан актуалізував інформаційний вимір безпеки як один із ключових напрямів національної стійкості, оскільки інформаційний простір став об'єктом системних атак, спрямованих на підрив державного суверенітету, дестабілізацію суспільства та деморалізацію населення. У цих умовах забезпечення інформаційної безпеки та захист інформаційного простору України набувають стратегічного значення і потребують комплексного аналізу ефективності застосовуваних механізмів публічного управління.

Воєнний стан зумовив запровадження особливих правових, організаційних та інституційних режимів у сфері інформаційної діяльності, що вплинуло на функціонування медіа, системи стратегічних комунікацій, кіберзахисту та протидії дезінформації. Зростання інтенсивності інформаційно-психологічних операцій держави-агресора, використання кіберзасобів та маніпулятивних інформаційних технологій вимагає від держави постійного удосконалення підходів до захисту інформаційного простору, координації дій суб'єктів публічного управління та підвищення рівня інформаційної стійкості суспільства. У цьому контексті особливої уваги потребує аналіз реального стану забезпечення інформаційної безпеки України саме в умовах воєнного стану.

Одним із індикаторів результативності національного законодавства у сфері забезпечення інформаційної безпеки, що наочно відображає рівень поступу держави, є міжнародне рейтингування країн за критеріями

оцінювання їхніх спроможностей у відповідній галузі. До найбільш авторитетних і загальновизнаних рейтингів у сфері інформаційної та кібербезпеки належать Global Cybersecurity Index [47] та National Cyber Security Index [48], кожен із яких доцільно розглянути більш детально.

Глобальний індекс кібербезпеки (Global Cybersecurity Index – GCI), перше видання якого було представлено у 2015 році, орієнтований на ідентифікацію сфер і напрямів кібербезпеки, що потребують подальшого вдосконалення з боку держав-учасниць цієї ініціативи. На основі отриманих результатів формуються практичні рекомендації на національному рівні з урахуванням регіональної та галузевої специфіки, що в сукупності сприяє підвищенню загальносвітового рівня кібербезпеки, поширенню та впровадженню кращих практик, а також формуванню глобальної культури кібербезпеки.

Сфера охоплення та структура GCI визначені Резолюцією 130 [49], якою нормативно закріплено посилення ролі та значущості Міжнародного союзу електрозв'язку (ITU) як спеціалізованої агенції ООН у сфері інформаційно-комунікаційних технологій. Оцінювання здійснюється за п'ятьма ключовими напрямами, а саме: правовим, технічним, організаційним, розвитком потенціалу та співробітництвом, що у своїй сукупності відображають рівень готовності держав до забезпечення безпеки в інформаційно-телекомунікаційному середовищі.

Відповідно до результатів Global Cybersecurity Index 2020 року [47] Україна посіла 78 місце серед 194 країн, залучених до загального анкетування, а також 39 місце з-поміж 46 держав європейського регіону, що відображено в таблиці 2.1. Національний індекс кібербезпеки (National Cyber Security Index – NCSI) – це глобальний індекс, який в режимі реального часу вимірює готовність країн запобігати кіберзагрозам й управляти кіберінцидентами. Цей індекс сфокусовано на окремих аспектах кібербезпеки, що запроваджуються урядами на національних рівнях за чотирма сферами – чинного законодавства, сформованих інституцій, форматами співпраці, результатами.

Таблиця 2.1

Рейтинг країн за Глобальним індексом кібербезпеки (GCI)

Рейтинг	*Країна*	*Оцінка*
1	США	**100**
2	Сполучене Королівство	**99,54**
2	Саудівська Аравія	**99,54**
3	Естонія	**99,48**
4	Корея	**98,52**
4	Сінгапур	**98,52**
4	Іспанія	**98,52**
5	ОАЕ	**98,06**
5	Малайзія	**98,06**
6	Литва	**97,93**
7	Японія	**97,82**
8	Канада	**97,67**
9	Франція	**97,6**
10	Індія	**97,5**
…		
70	Узбекистан	**71,11**
71	Йорданія	**70,96**
72	Уганда	**69,98**
73	Замбія	**68,88**
74	Чилі	**68,83**
75	Кот д'Івуар	**67,82**
76	Коста-Ріка	**67,45**
77	Болгарія	**67,38**
78	**Україна**	**65,93**
182	Мікронезія	0
182	Ватикан	0

Рейтинг	*Країна Європи*	*Оцінка*
1	Сполучене Королівство	**99,54**
2	Естонія	**99,48**
3	Іспанія	**98,52**
4	Литва	**97,93**
5	Франція	**97,6**
6	Туреччина	**97,5**
7	Люксембург	**97,41**
7	Німеччина	**97,41**
8	Португалія	**97,32**
9	Латвія	**97,28**
10	Нідерланди	**97,05**
…		
30	Грузія	**81,07**
31	Ісландія	**79,81**
32	Румунія	**76,29**
33	Молдова	**75,78**
34	Словенія	**74,93**
35	Чеська Республіка	**74,37**
36	Монако	**72,57**
37	Болгарія	**67,38**
39	**Україна**	**65,93**
40	Албанія	**64.32**
41	Чорногорія	**53,23**
42	Ліхтенштейн	**35,15**

Примітка. Складено автором на основі [47].

З метою підготовки оновленої редакції National Cyber Security Index за результатами моніторингу упродовж 2016–2023 років було здійснено

комплексне дослідження стану кібербезпеки у 176 державах світу. Оцінювання проводилося за низкою показників, що відображають ефективність законодавчого регулювання у сфері кібербезпеки, управління кіберінцидентами, забезпечення інформаційної безпеки, розвитку довірчих послуг, захисту персональних даних, протидії кіберзлочинності та інших суміжних напрямів. За результатами проведеного аналізу Україна посіла 24 місце серед 176 проаналізованих країн, що відображено в таблиці 2.2.

Таблиця 2.2

Рейтинг країн за Національним індексом кібербезпеки (NCSI)

Рейтинг	Країна	Національний індекс кібербезпеки	Рівень цифрового розвитку	Різниця
1.	Бельгія	**94,81**	74,07	20,74
2.	Литва	**93,51**	67,34	26,17
3.	Естонія	**93,51**	75,59	17,92
4.	Чеська Республіка	**90,91**	69,21	21,70
5.	Німеччина	**90,91**	80,01	10,90
6.	Румунія	**89,61**	59,84	29,77
7.	Греція	**89,61**	64,02	25,59
8.	Португалія	**89,61**	68,46	21,15
9.	Сполучене Королівство	**89,61**	79,96	9,65
10.	Іспанія	**88,31**	72,21	16,10
…				
20.	Нідерланди	**83,12**	81,86	1,26
21.	Сербія	**80,52**	59,81	20,71
22.	Малайзія	**79,22**	62,19	17,03
23.	Італія	**79,22**	67,26	11,96
24.	**Україна**	**75,32**	55,96	19,36
25.	Латвія	**75,32**	66,23	9,09
…				
176.	Південний Судан	**1,30**		

Примітка. Складено автором на основі [48].

Крім того, в межах порушеної проблематики доцільно навести дані щодо видатків Державного бюджету України у 2022–2024 роках, спрямованих на забезпечення захисту інформаційного простору держави (табл. 2.3). Основний акцент бюджетної політики у зазначений період було зосереджено на підтримці функціонування економіки України в умовах надзвичайних і кризових ситуацій.

Таблиця 2.3

Видатки Державного бюджету України 2022–2024 років на сферу захисту інформаційного простору

Показник	Сума (грн)		
	2022	2023	2024
Інформаційно-аналітичне забезпечення координаційної діяльності у сфері національної безпеки і оборони	335126,3	223141,2	255605,5
Інформаційно-аналітичне забезпечення діяльності у сфері інформаційної безпеки України	53006,2	52306,2	58274,5
Модернізація цифрових інформаційно-аналітичних систем	50000	–	–
Електронне урядування	651524	397514,2	749337,4
Розвиток пріоритетних проєктів в галузі інформаційних технологій / Забезпечення функціонування Фонду розвитку інновацій	450000	30000	1500000
Національна програма інформатизації	2205274,6	–	300000
Збирання, обробка та розповсюдження офіційної інформаційної продукції	268543,9	1934977,9	1510196,2
Здійснення заходів у сфері інформаційної безпеки	50000	40500	40500
РАЗОМ	**4 063 475**	**2 678 439,5**	**4 413 913,6**

Примітка. Складено автором на основі [50; 51; 52].

Показовим є те, що бюджетний показник «Здійснення заходів у сфері захисту національного інформаційного простору» для Міністерства культури та інформаційної політики України в структурі видатків Державного бюджету України був запроваджений лише у 2018 році. Водночас результати аналізу розподілу відповідних коштів свідчать про тенденцію до їх скорочення (рис. 2.1). Разом із тим інші бюджетні показники, дотичні до сфери захисту

інформаційного простору держави та організаційно-функціонального забезпечення публічного управління, які загалом сприяють посиленню національної стійкості (табл. 2.3), характеризуються відносною стабільністю з певним зростанням обсягів фінансування у сфері національної безпеки й оборони.

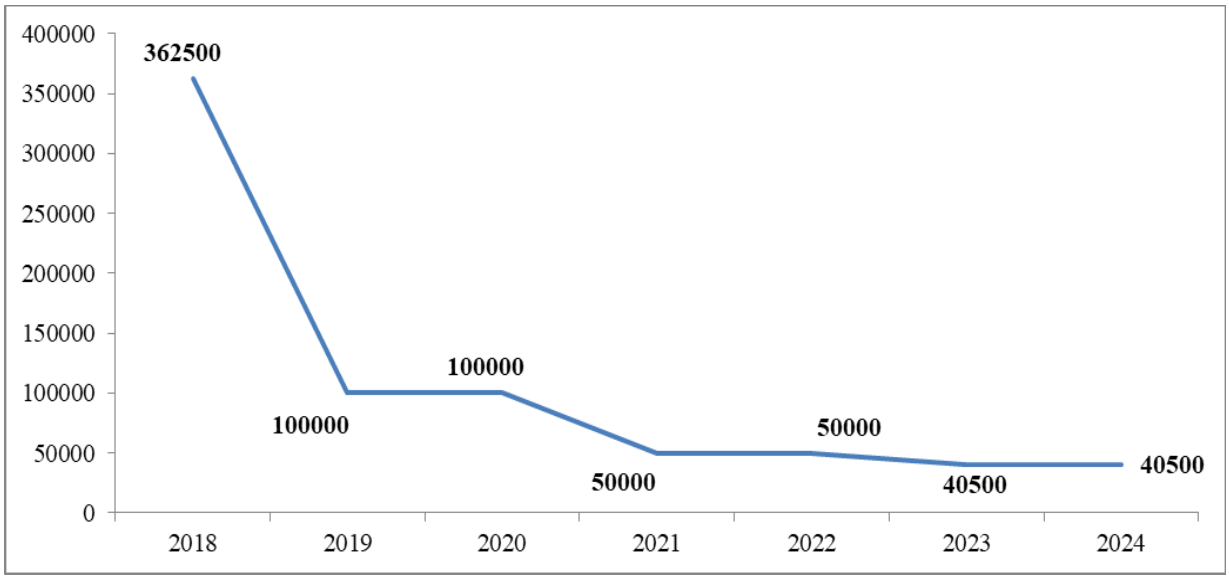

Рис. 2.1. Динаміка видатків Державного бюджету України на здійснення заходів у сфері захисту національного інформаційного простору

Примітка. Складено автором на основі [50; 51; 52].

Глобальний інформаційний простір формується та розвивається надзвичайно динамічно, а в інформаційній сфері людства відбуваються масштабні трансформаційні процеси, що мають характер революційних змін. Такі процеси актуалізують нові глобальні виклики й загрози, які становлять реальну небезпеку для безпеки людства та міжнародного правопорядку, тоді як наслідки застосування сучасних засобів інформаційного впливу за своїм руйнівним потенціалом можуть бути співмірними з використанням зброї масового ураження [53].

Розвиваючи зазначену проблематику, В. Копанчук виокремлює низку загроз національній безпеці України в інформаційній сфері. До них, зокрема, належать недосконаліть нормативно-правового забезпечення інформаційної безпеки на галузевому рівні; недостатній рівень розвитку національної інформаційно-телекомунікаційної інфраструктури; непослідовність

державної політики у сфері інформаційної безпеки, яка не завжди ґрунтується на принципах системності, комплексності та результативності, а також перевантаженість і неефективність механізмів державного управління та регулювання в цій сфері. Окрім того, серед загроз визначено відсутність дієвих механізмів реалізації інформаційно-психологічних операцій, недостатню сформованість системи активного кіберзахисту інформаційного простору держави та спроможностей до надання асиметричної відповіді агресору, ведення іншими державами інформаційної війни проти України, концентрацію загальнонаціональних засобів масової інформації в руках окремих груп стейкхолдерів, а також дезінформацію громадян України й застосування щодо них інформаційно-психологічних маніпулятивних технологій [54, с. 196–197].

За таких складних умов досягнення належного та стабільного функціонування національного інформаційного простору є надзвичайно складним завданням, однак воно залишається цілком реалістичним за умови системного та цілеспрямованого підходу.

У сучасних умовах розвитку України розроблення загальнодержавних документів стратегічного значення, пов’язаних із забезпеченням безпеки держави загалом та її окремих складових, зокрема інформаційної безпеки, доцільно орієнтувати на три альтернативні підходи, запропоновані О. Резніковою. Йдеться про зменшення негативного впливу загроз різної природи або забезпечення швидкого відновлення системи публічного управління після надзвичайних і кризових ситуацій; визначення пріоритетності превентивних чи реактивних заходів державного реагування на загрози; а також зосередження уваги на забезпеченні готовності до прогнозування загроз, впровадженні ефективного кризового менеджменту та нарощуванні безпекових спроможностей держави [11, с. 113].

Таким чином, для реалізації стратегічних документів і практичних заходів у сфері забезпечення інформаційної безпеки принципово важливим є вибудовування сталої співпраці та ефективної взаємодії між державою і

суспільством. Такий формат взаємовідносин здатний забезпечити суттєві позитивні результати: для суспільства в цілому – активізацію участі у забезпеченні власної безпеки, підвищення загального рівня кібербезпеки та розвиток інститутів громадянського суспільства; для окремих громадян – формування навичок протидії інформаційним загрозам, зростання рівня медіаграмотності та цифрової компетентності; для приватного сектору – посилення спроможностей у сфері протидії інформаційним загрозам, зміцнення корпоративної безпеки та налагодження ефективних комунікацій; для інститутів громадянського суспільства – розширення інструментарію участі у процесах формування й реалізації державної політики у безпековій сфері, а також ініціювання впровадження інноваційних підходів; для органів публічної влади – отримання додаткових експертних оцінок, використання досвіду громадського сектору й міжнародних організацій, залучення громадських інституцій до практичної реалізації державної політики, а також до моніторингу й оцінювання її результативності.

Отже, базовими засадами формування державної системи інформаційної безпеки мають стати дотримання принципу законності, чітке розмежування повноважень між суб'єктами, добровільність участі стейкхолдерів, колегіальність управління, стабільність ключових елементів системи, її здатність до адаптації в умовах змін, раціональне поєднання універсальних і диференційованих механізмів забезпечення інформаційної безпеки, поетапність упровадження відповідних заходів та забезпечення сталості як цієї підсистеми, так і системи національної безпеки держави загалом. Сучасні реалії істотно посилюють актуальність і нагальність формування та реалізації виваженої державної політики у сфері інформаційної безпеки.

РОЗДІЛ 3
НАПРЯМИ УДОСКОНАЛЕННЯ ПУБЛІЧНОГО УПРАВЛІННЯ В СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УМОВАХ ВОЄННОГО СТАНУ

3.1. Моделювання публічного управління в сфері інформаційної безпеки як складової національної безпеки України

Сучасні умови розвитку України, зумовлені тривалим воєнним протистоянням та зростанням масштабів гібридних загроз, актуалізують необхідність переосмислення підходів до публічного управління у сфері інформаційної безпеки як невід'ємної складової національної безпеки. Інформаційна безпека дедалі більше розглядається не лише як окремий напрям державної політики, а як системоутворюючий елемент, що безпосередньо впливає на стійкість держави, ефективність функціонування інститутів влади, захист суверенітету та реалізацію національних інтересів в умовах постійних інформаційних і кібернетичних загроз.

У цьому контексті особливого значення набуває моделювання публічного управління у сфері інформаційної безпеки, яке дає змогу концептуалізувати взаємозв'язки між суб'єктами управління, визначити логіку прийняття управлінських рішень, окреслити функціональні рівні та механізми координації дій у межах системи національної безпеки. Застосування модельного підходу створює підґрунтя для формування цілісного бачення організації публічного управління інформаційною безпекою, адаптованого до умов воєнного стану та спрямованого на підвищення ефективності реагування держави на сучасні виклики й загрози в інформаційному просторі.

Моделювання публічного управління захистом інформаційного простору в контексті застосування ризик-орієнтованого підходу набуває особливої актуальності в сучасних умовах, коли забезпечення інформаційної безпеки перетворюється на одне з ключових завдань держави. Значущість цієї проблематики посилюється на тлі геополітичної нестабільності та зростання

масштабів гібридних загроз. Практико-орієнтований підхід до моделювання публічного управління створює можливості для формування інструментарію управління ризиками, пов'язаними з потенційними загрозами й уразливостями інформаційного простору, зокрема шляхом аналізу можливих сценаріїв розвитку загроз, прогнозування їхніх наслідків та обґрунтування стратегій захисту і протидії.

Необхідність моделювання публічного управління захистом інформаційного простору зумовлюється постійним зростанням технологічних можливостей і ускладненням характеру загроз, спрямованих на інформаційний простір держави. Застосування модельного підходу дозволяє забезпечити більш результативне реагування на виклики сучасного інформаційного середовища та сприяє захисту національних інтересів у динамічному цифровому просторі.

Інформаційна сфера держави та питання забезпечення її належного захисту традиційно перебувають у центрі підвищеної уваги, оскільки недооцінювання або ігнорування ролі інформаційних чинників у системі гарантування національної безпеки здатне призвести до незворотних втрат і мати відчутний негативний вплив на подальший розвиток ключових складових державності.

У період повномасштабної збройної агресії проти України інформаційна дестабілізація з боку держави-агресора зосереджується на чотирьох базових напрямах, а саме:

– дискредитації військово-політичного керівництва держави;

– провокуванні розколу української еліти з підривом основ державності;

– деморалізації сил безпеки та сил оборони;

– здійсненні інформаційно-психологічного впливу з метою дезорієнтації населення [55].

З метою підвищення результативності управління ризиками в умовах надзвичайних ситуацій доцільним є розвиток низки взаємопов'язаних складових, зокрема:

- системи моніторингу, аналізу ризиків і прогнозування надзвичайних ситуацій як базису діяльності зі зниження їх рівня;

- системи запобігання надзвичайним ситуаціям та механізмів державного регулювання ризиків;

- системи ліквідації надзвичайних ситуацій з урахуванням вимог оперативного реагування, застосування відповідних технічних засобів і сучасних технологій проведення аварійно-рятувальних та інших невідкладних робіт;

- системи підготовки керівного складу органів управління, фахівців і населення у сфері зменшення ризиків та масштабів надзвичайних ситуацій;

- системи страхування ризиків.

Звертаючись до стандартизованої методології управління ризиками [56], варто зазначити, що цей процес має безперервний характер і відіграє важливу роль у формуванні стратегії діяльності, досягненні визначених цілей та ухваленні обґрунтованих управлінських рішень. Управління ризиками передбачає систематичне застосування відповідних політик, процедур і методів до діяльності, пов'язаної з комунікацією та консультуванням, визначенням контексту, ідентифікацією та оцінюванням ризиків, їх опрацюванням, моніторингом і аналізом, а також документуванням і формуванням звітності.

Загальновизнані принципи, на яких має ґрунтуватися система управління ризиками, охоплюють:

- інтегрованість, що передбачає включення управління ризиками до всіх напрямів діяльності організації;

- структурованість і повноту, які забезпечують узгодженість та порівнюваність результатів;

- налаштованість системи управління ризиками відповідно до зовнішнього і внутрішнього контексту та стратегічних цілей організації;

- залучення стейкголдерів, що дає змогу враховувати їхній досвід, бачення та сприйняття ризиків;

- динамічність, яка полягає у своєчасному прогнозуванні, виявленні та реагуванні на зміни ризиків;

- використання найкращої доступної інформації з урахуванням її обмежень і невизначеностей;

- урахування людських і культурних чинників, що впливають на всі етапи управління ризиками;

- орієнтацію на постійне вдосконалення шляхом навчання та накопичення практичного досвіду [56].

Проєктуючи зазначену методологію на інформаційну сферу держави з метою забезпечення захисту її інформаційного простору, доцільно звернутися до підходу, який передбачає послідовне виконання таких етапів:

- збір інформації про об'єкт із використанням публікацій у неафільованих засобах масової інформації;

- побудова графіка динаміки появи повідомлень про об'єкт у мережевих медіа;

- аналіз цієї динаміки в ретроспективі 6–12 місяців із застосуванням методів аналізу часових рядів та контент-аналізу публікацій у граничних точках, визначення моментів, тривалості й періодичності впливу та їх прив'язки до інших значущих подій;

- ідентифікація джерел, що поширюють найбільшу кількість матеріалів із негативною тональністю;

- встановлення першоджерел публікацій;

- визначення ймовірних «замовників» або осіб, які здійснюють вплив на редакційну політику окремих медіа;

- окреслення та ранжування сфер спільних інтересів об'єкта і потенційних «замовників»;

- формування критеріїв інформаційного впливу на основі найбільш рейтингових інтересів;

- моделювання інформаційних впливів із виявленням зв'язків між «замовниками», аналізом динаміки їхнього впливу, прогнозуванням подальшого розвитку ситуації та визначенням критичних точок;

- прогнозування наступних кроків впливу шляхом аналізу аналогічних процесів щодо інших об'єктів у ретроспективі;

- оцінювання ймовірних наслідків; а також організацію заходів інформаційної протидії.

У розвиток викладених підходів до управління ризиками та організації інформаційної протидії доцільним є конкретизувати інституційно-функціональні механізми постійного спостереження за станом інформаційного простору держави як необхідної умови своєчасного виявлення та нейтралізації деструктивних впливів.

У цьому контексті запропоновано створення трирівневої підсистеми моніторингу інформаційних процесів в інформаційному просторі держави, в межах якої:

- перший, операторний рівень передбачає виявлення, первинну класифікацію та індикацію деструктивних інформаційних процесів за визначеними джерелами можливого впливу;

- другий рівень орієнтований на узагальнення даних, отриманих на першому рівні, за відповідними класифікаційними ознаками та здійснення вагової обробки формалізованих повідомлень;

- третій рівень спрямований на встановлення факту негативного інформаційно-психологічного впливу й оцінювання його інтенсивності на основі інформації другого рівня, що забезпечується функціонуванням головного інформаційного (ситуаційного) центру.

Ми пропонуємо модель моніторингу інформаційного простору, яка розглядається як комплексна система послідовних і взаємопов'язаних управлінських дій. До її ключових складових віднесено:

1. Оперативне виявлення інформаційного впливу;

2. Подальший аналіз та оцінювання рівня такого впливу;

3. Формування аналітичних висновків і ухвалення рішень щодо доцільності застосування заходів протидії;

4. Прогнозування подальшого розвитку ситуації;

5. Планування відповідних заходів реагування;

6. Безпосереднє реагування на виявлені інформаційні загрози;

7. Контроль ефективності реалізованих дій із можливістю їх корегування;

8. Здійснення превентивних інформаційних заходів, спрямованих на недопущення або мінімізацію негативних впливів.

Підходи, засновані на принципах ризик-менеджменту, є поширеними як у міжнародній, так і у вітчизняній практиці та застосовуються в різних сферах публічного управління. Основною метою управління ризиками є утримання їх на прийнятному для органів державної влади рівні. Досягнення цієї мети потребує наявності ефективного інструментарію у вигляді методичного підходу до оцінювання ризиків інформаційної безпеки, який орієнтований на визначення критеріїв оцінки ризиків та меж їх прийнятності, забезпечення обґрунтованості й внутрішньої узгодженості сукупності ризиків, актуальних для конкретної системи, а також ідентифікацію ризиків з урахуванням таких властивостей інформаційних активів, як конфіденційність, цілісність і доступність.

Крім того, важливим завданням у межах цього підходу є визначення власників ризиків – фізичних або юридичних осіб, структурних підрозділів, керівників, фахівців з інформаційної безпеки та інших працівників органів державної влади, які наділені відповідними повноваженнями щодо управління ризиками. Методичний підхід також передбачає оцінювання потенційних втрат у разі реалізації ризику, опосередковане апостеріорне визначення ймовірності його настання та кількісних параметрів, а також зіставлення ідентифікованих ризиків із встановленими критеріями з метою визначення пріоритетних напрямів їх подальшого опрацювання.

Особливої значущості в цьому контексті набувають процеси прогнозування й комплексного аналізу всього спектра загроз національній безпеці в інформаційній сфері. Причини виникнення таких загроз потребують своєчасного виявлення та системного аналізу з метою оцінювання характеру й масштабів їх впливу, а також розроблення адекватних шляхів, методів і засобів подальшої нейтралізації. Загрози, джерелом яких є інформаційний простір, на сучасному етапі світового розвитку характеризуються підвищеною актуальністю, оскільки вони реалізуються з активним використанням інформаційно-комунікаційних технологій, поширюються в глобальному інформаційному середовищі, відзначаються високою швидкістю розповсюдження значних обсягів інформації та можуть ініціюватися з будь-якої точки світу.

3.2. Стратегічні пріоритети розвитку публічного управління в сфері інформаційної безпеки

Світові глобалізаційні процеси зумовлюють глибокі трансформації у здійсненні одного з базових видів управління суспільством – соціального управління, розширюючи та ускладнюючи його форми й методи, а також впливаючи на стиль і формат управлінської діяльності як цілеспрямованого впливу сучасних держав на стан і динаміку суспільних процесів та відносин з метою досягнення визначених цілей і реалізації функцій організованих соціальних систем.

Сучасний етап суспільного розвитку характеризується формуванням нової якості управління – інформаційної, яка є визначальною для новітньої історичної фази розвитку суспільства. У цих умовах інформація набула статусу системоутворювального чинника, оскільки в більшості сфер суспільного життя домінують процеси її виробництва, використання та споживання, що суттєво впливає на механізми функціонування держави та суспільства.

Водночас зазначені процеси поряд із очевидними перевагами, пов'язаними з розвитком ефективної інформаційно-комунікативної взаємодії, розширенням доступу до глобальних інформаційних ресурсів і задоволенням зростаючих потреб у інформаційних продуктах і послугах, супроводжуються появою значної кількості ризиків, загроз і небезпек, здатних порушити стабільне функціонування соціальних інститутів та завдати шкоди суспільному розвитку.

Зокрема, інформаційна агресія проявляється у цілеспрямованому впливі на свідомість і світогляд людини, формування уявлень про навколишню дійсність, а в ширшому, загальнодержавному вимірі – на національну безпеку України в інформаційній сфері з метою заподіяння істотної шкоди окремим сферам життєдіяльності суспільства [57, с. 59]. Така загроза має виразний ідеологічний характер, характеризується значним маніпулятивним потенціалом і здійснює прямий або опосередкований вплив на масову свідомість.

Поряд із цим важливою загрозою виступає інформаційна експансія, яка розглядається як інституціоналізована система, сформована в середовищі засобів масової комунікації, а також сукупність методів, що застосовуються для пропагандистського забезпечення певних геополітичних інтересів [58, с. 40]. Вона реалізується, зокрема, через вплив на вищі органи політичного керівництва інших держав з метою лобіювання власних стратегічних цілей і ухвалення відповідних рішень, втручання у геополітичні стратегії, а також формування суспільно-політичних настроїв населення шляхом проведення інформаційно-психологічних операцій, спрямованих на здійснення тиску на владу.

На сучасному етапі підвищена увага до проблем гарантування інформаційної безпеки України зумовлена активізацією антиукраїнських інформаційних впливів, спрямованих на поширення ідей сепаратизму, насильства та національної ворожнечі, що водночас виступають спробами підриву національної ідентичності, руйнування міжнаціональної злагоди,

посягання на конституційний лад і територіальну цілісність держави [59, с. 28].

Суттєву загрозу інформаційному простору держави становить також інформаційна інтервенція, яка в наукових джерелах трактується як насильницьке втручання одного чи кількох суб'єктів інформаційних відносин у діяльність інших, що реалізується через комплекс агресивних дій, спрямованих на формування суспільної думки, вплив на процеси ухвалення рішень усередині держави та досягнення наперед визначених політичних чи соціальних результатів [60, с. 55].

Окреслений спектр сучасних загроз інформаційній безпеці зумовлює необхідність адекватного та системного реагування на них і спонукає держави до пошуку новітніх методів і способів протидії, що знаходить відображення у чіткій фіксації стратегічних пріоритетів на рівні прогнозних документів, програм і стратегій. Реалізація таких підходів передбачає ухвалення комплексу практичних рішень вищим політичним керівництвом держави, спрямованих на формування ефективної міжвідомчої взаємодії, зміцнення інформаційної стійкості, а також імплементацію заходів зі стримування та нейтралізації загроз і небезпек в інформаційному просторі.

Серед стратегічних напрямів розвитку та ключових пріоритетів державної політики доцільно виокремити формування національної системи стійкості, у межах якої забезпечення інформаційної стійкості держави розглядається як одна з її базових підсистем. У цьому контексті особливої актуальності набуває питання побудови дієвого інституційного механізму державного регулювання, який, зокрема, може реалізовуватися через розроблення та впровадження відповідної методології паспортизації загроз національній безпеці, у тому числі в частині захисту національного інформаційного простору в умовах надзвичайних ситуацій.

Вважаємо, що зазначений інституційний механізм може бути суттєво доповнений і розширений шляхом створення національного реєстру загроз національній безпеці в інформаційній сфері. Такий інструмент доцільно

формувати із застосуванням ризик-орієнтованого підходу до моделювання публічного управління захистом інформаційного простору в чотирьох режимах його функціонування: повсякденному, режимі підвищеної готовності, надзвичайної ситуації та надзвичайного стану, що забезпечить адаптивність управлінських рішень до зміни рівня загроз.

Поняття Національного реєстру загроз як публічно доступної форми узагальнених результатів оцінювання загроз національній безпеці України було запропоновано фахівцями Національного інституту стратегічних досліджень під керівництвом О.О. Резнікової. Зазначений реєстр має охоплювати загальний огляд безпекового середовища України з урахуванням реальних і потенційних загроз національній безпеці; детальний опис надзвичайних і кризових ситуацій, їх загальну характеристику та ймовірні наслідки в середньостроковій перспективі; характеристику механізмів і процедур реагування на надзвичайні та кризові ситуації, передбачених чинним законодавством, а також рекомендації й алгоритми дій у разі їх виникнення; методологію та методику проведення оцінювання ризиків у сферах забезпечення національної безпеки держави [61, с. 46].

Логічним продовженням зазначених ініціатив має стати впровадження ефективно функціонуючої національної системи стійкості та її окремих складових. У цьому контексті заслуговує на увагу візуалізація циклу забезпечення національної стійкості, запропонована О.О. Резніковою, що представлена на рис. 3.1, яка відображає послідовність і взаємозв'язок ключових етапів управління загрозами та кризовими ситуаціями.

У поданій візуалізації національна система стійкості постає як безперервний циклічний процес, у межах якого взаємопов'язані етапи запобігання, підготовки, реагування та відновлення забезпечують адаптацію держави до змін безпекового середовища. Такий підхід демонструє, що управління загрозами не зводиться до разових реактивних дій, а передбачає постійний аналіз ризиків, накопичення даних, коригування управлінських рішень і вдосконалення механізмів реагування.

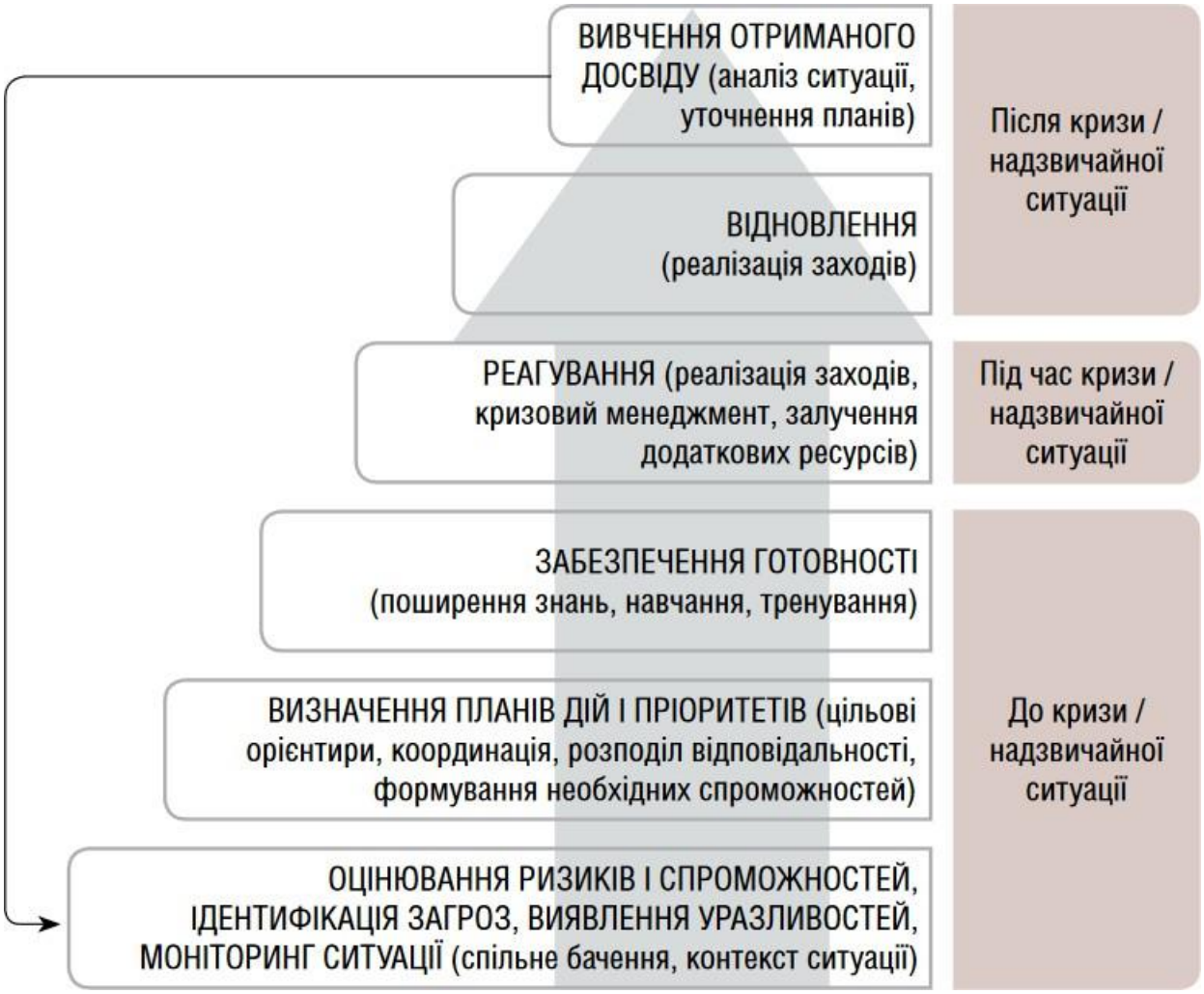

Рис. 3.1. Цикл забезпечення національної стійкості

Джерело: [11, с. 84].

Інтеграція інформаційної стійкості в загальний цикл забезпечення національної стійкості підкреслює її системоутворюючу роль, оскільки інформаційна сфера пронизує всі етапи управління кризами – від раннього виявлення загроз і формування готовності до реалізації заходів протидії та післякризового відновлення. Це дає підстави розглядати інформаційну безпеку не як ізольований напрям державної політики, а як ключовий елемент комплексного публічного управління в умовах надзвичайних і кризових ситуацій.

З метою формування національної моделі стійкості Д. Теперік пропонує її концептуалізацію у вигляді «маяка» (beacon), що відображає комплексний і людиноцентрований характер забезпечення стійкості держави та суспільства. У межах цієї моделі виділяються взаємопов’язані складові, кожна з яких

виконує окрему функціональну роль у підготовці, реагуванні та відновленні в умовах надзвичайних і кризових ситуацій.

Компонент Behaviour (поведінка) розглядається як ціннісна та світоглядна основа стійкості, що визначає ставлення суб'єктів до ризиків і криз та формує орієнтований на дії підхід до управління надзвичайними ситуаціями й виживання в умовах нестабільності.

Evaluation (оцінювання) передбачає постійне пізнання власних сильних і вразливих сторін, а також систематичне оцінювання загроз, що дозволяє підвищувати рівень готовності суспільства до непередбачуваних подій. Здатність до самоаналізу, самонавчання й трансформації на основі результатів оцінювання розглядається як умова безперервного вдосконалення політик, планування та навчальних практик у сфері безпеки.

Важливе місце в моделі займає Agility (гнучкість), яка відображає необхідність оперативної адаптації до мінливого характеру ризиків і загроз. Гнучкість проявляється у здатності швидко коригувати оцінки ситуації, втручатися в розвиток кризових процесів та переглядати управлінські рішення залежно від рівня загроз – від локального до міжнародного.

Commitment (зобов'язання) акцентує увагу на мотиваційній складовій стійкості, що ґрунтується на спільних цінностях, громадянській відповідальності та готовності до участі в колективних діях. У цьому контексті підкреслюється роль громадянської участі, міжсекторальної співпраці та мобілізації різних видів ресурсів для подолання кризових ситуацій.

Складова Operationalisation (операціоналізація) орієнтована на інституційний вимір стійкості та передбачає системне розроблення політик, процедур, алгоритмів і протоколів реагування, що забезпечують ефективність індивідуальних, колективних і державних дій у кризових умовах. При цьому наголошується на врахуванні соціальної стратифікації, різноманітності потреб та впливу внутрішніх і зовнішніх чинників.

Завершальним елементом моделі є Networking (мережева взаємодія), що підкреслює міждисциплінарний характер стійкості та необхідність

формування горизонтальних мереж співпраці. Такі мережі, засновані на довірі та принципі «команди команд», забезпечують обмін знаннями, навичками й досвідом, сприяють швидкому відновленню спільнот і підвищують кількість бенефіціарів у посткризовий період [62, с. 18–20].

У сукупності зазначена модель дозволяє розглядати національну стійкість як багатовимірний процес, у якому поєднуються поведінкові, інституційні, мережеві та управлінські складові, що є особливо актуальним для розвитку публічного управління в сфері інформаційної безпеки. Вказана система має передбачати забезпечення функціонування базових елементів, з-поміж яких:

– безпека та захищеність об'єктів критичної інфраструктури (кібербезпека, захищеність та безперебійне функціонування інформаційних та комунікаційних послуг);

– суспільна стійкість, зокрема, до інформаційних впливів.

Стратегічні напрями та пріоритети державної політики у контексті формування більш стійкого інформаційного середовища в умовах сучасних загроз і викликів доцільно зосередити на комплексі взаємопов'язаних заходів. До них належать виявлення, запобігання та стримування дезінформації й інформаційних маніпуляцій, що підривають суспільну довіру та інформаційну стійкість, а також забезпечення належного рівня кібербезпеки як ключової умови захисту інформаційної інфраструктури держави.

Важливими пріоритетами залишаються гарантування відкритості діяльності органів публічної влади та розширення доступу суспільства до інформації, що сприяє підвищенню прозорості управлінських процесів і зміцненню демократичних інститутів. Окрему увагу необхідно приділяти забезпеченню інституційної незалежності медіарегуляторів, інвестуванню в розвиток медіаграмотності населення та створенню умов для доступу громадян до якісного, достовірного й соціально значущого інформаційного контенту.

Не менш вагомими є завдання мобілізації колективних дій і розвитку міжсуб'єктної взаємодії між органами державної влади, громадянським суспільством і приватним сектором, а також упровадження проактивного підходу до реалізації стратегічного курсу держави у сфері інформаційної безпеки. Сукупність зазначених напрямів формує основу для підвищення стійкості національного інформаційного середовища та ефективного реагування на сучасні інформаційні виклики.

Окреслені вище тенденції дають підстави стверджувати, що органічним елементом національної системи стійкості доцільно розглядати підсистему забезпечення інформаційної стійкості держави, яка відіграє ключову роль у протидії сучасним гібридним та інформаційним загрозам.

У трактуванні дослідниці А. Рантамякі стійкість розуміється як здатність людей, організацій або суспільств ефективно долати порушення стабільного функціонування систем чи кризові явища. При цьому інформаційна стійкість не має лінійного характеру, а постає як повторюваний, циклічний процес, що перебуває у постійному розвитку та потребує безперервного вдосконалення на етапах до виникнення, під час перебігу та після завершення надзвичайних і кризових ситуацій [63, с. 284].

З урахуванням нормативно закріпленого розуміння національної стійкості [64], підсистему забезпечення інформаційної стійкості держави доцільно інтерпретувати як її спроможність ефективно протидіяти реальним і потенційним загрозам та викликам в інформаційній сфері, забезпечувати їх своєчасне передбачення і прогнозування, адаптуватися до динамічних змін безпекового середовища, підтримувати стабільне функціонування та оперативно відновлюватися до бажаного стану рівноваги після надзвичайних і кризових ситуацій.

Візуалізацію підсистеми забезпечення інформаційної стійкості держави представлено у вигляді відповідної моделі на рис. 3.2, яка відображає її структурні елементи, логіку взаємодії та місце в загальній системі національної стійкості.

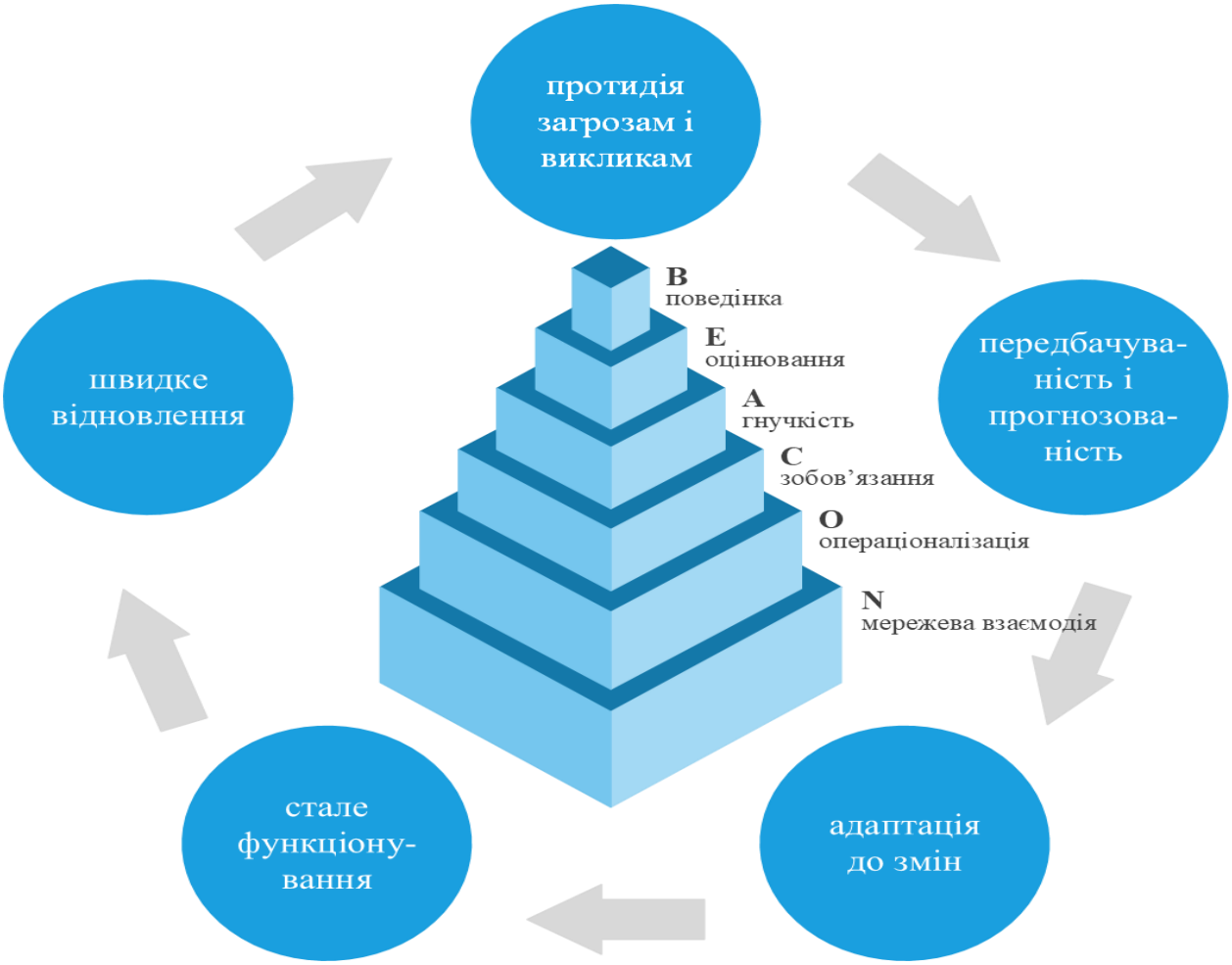

Рис. 3.2. Модель підсистеми забезпечення інформаційної стійкості держави

Примітка. Складено автором.

Представлена модель розглядається як циклічний, повторюваний і безперервний процес, у межах якого забезпечення інформаційної стійкості держави ґрунтується на взаємопов'язаній реалізації п'яти ключових компонентів.

1. Протидія загрозам і викликам передбачає своєчасне виявлення, аналіз та нейтралізацію деструктивних інформаційних впливів, включаючи дезінформаційні кампанії, інформаційно-психологічні операції та кібератаки. Реалізація цього компонента спрямована на мінімізацію негативного впливу загроз на функціонування державних інституцій, суспільну стабільність і національні інтереси в інформаційній сфері.

2. Передбачуваність і прогнозованість полягає у здатності системи інформаційної безпеки здійснювати випереджувальне оцінювання ризиків і загроз на основі аналізу тенденцій розвитку інформаційного середовища. Це

забезпечує формування сценаріїв можливого розвитку подій, підвищує готовність органів публічного управління до реагування та сприяє ухваленню обґрунтованих управлінських рішень у кризових умовах.

3. Адаптація до змін відображає спроможність системи гнучко реагувати на трансформації інформаційного простору, технологічні інновації та зміну характеру загроз. Адаптивність забезпечується шляхом коригування стратегій, механізмів і інструментів публічного управління відповідно до динаміки внутрішнього та зовнішнього безпекового середовища.

4. Стале функціонування означає підтримання безперервної та ефективної роботи ключових інформаційних процесів, інфраструктури та комунікацій навіть за умов підвищеного ризику або кризових ситуацій. Даний компонент спрямований на збереження керованості, інституційної спроможності та довіри суспільства до державних інформаційних інститутів.

5. Швидке відновлення характеризує здатність системи оперативно повертатися до бажаного рівня функціонування після інформаційних інцидентів, надзвичайних або кризових ситуацій. Це включає відновлення інформаційних ресурсів і комунікацій, усунення наслідків деструктивних впливів та врахування набутого досвіду для подальшого вдосконалення механізмів забезпечення інформаційної стійкості.

У сукупності зазначені компоненти формують цілісну модель забезпечення інформаційної стійкості держави, яка відповідає логіці безперервного циклу публічного управління та спрямована на підвищення стійкості інформаційного простору в умовах сучасних викликів і загроз.

Узагальнюючи викладене, слід зазначити, що забезпечення інформаційної стійкості держави в сучасних умовах постає як багатовимірний і безперервний процес, який інтегрує інструменти протидії інформаційним загрозам, механізми прогнозування та адаптації до змін, а також підтримання стабільного функціонування інформаційного простору. Запропонована модель акцентує увагу на необхідності системного поєднання реактивних і проактивних підходів у публічному управлінні, що дозволяє мінімізувати

негативний вплив деструктивних інформаційних процесів і забезпечити готовність держави до реагування на кризові явища.

Разом із цим, циклічний характер моделі інформаційної стійкості підкреслює важливість постійного вдосконалення управлінських механізмів з урахуванням динаміки інформаційного середовища та накопиченого практичного досвіду. Взаємозв'язок таких компонентів, як передбачуваність, адаптивність, стале функціонування та швидке відновлення, створює підґрунтя для формування цілісної підсистеми національної стійкості, здатної забезпечити захист національних інтересів України та підтримати ефективність публічного управління в сфері інформаційної безпеки.

ВИСНОВКИ

У магістерській роботі запропоновано розв'язання актуальної проблеми, що полягає в обґрунтуванні теоретичних засад та розробці практичних рекомендацій щодо розвитку публічного управління в сфері інформаційної безпеки в Україні в умовах воєнного стану.

1. Встановлено, що в умовах воєнного стану публічне управління у сфері інформаційної безпеки набуває особливої ваги як інструмент забезпечення стійкості держави та протидії інформаційним загрозам. Інформаційний простір розглядається як сукупність інформаційних ресурсів, технологій, телекомунікаційних систем і мереж, що забезпечують інформаційну взаємодію організацій і громадян та задоволення їх інформаційних потреб. Загрози національній безпеці в інформаційній сфері мають комплексний характер і проявляються через вплив на свідомість і поведінку людей та негативний вплив на інформаційні ресурси держави, що зумовлює необхідність захисту інформаційного суверенітету, розвитку інформаційної інфраструктури та реалізації стратегій протидії інформаційним і кіберзагрозам. Реалізація державної політики у зазначеній сфері потребує вдосконалення нормативно-правового регулювання, підтримки національного контенту, розвитку стратегічних комунікацій і забезпечення доступу населення до достовірної інформації як основи ефективного реагування на зовнішні інформаційні впливи.

2. З'ясовано, що зарубіжний досвід публічного управління у сфері інформаційної безпеки ґрунтується на інституційному зміцненні державних механізмів реагування на інформаційні та кіберзагрози, розвитку координації між органами влади, а також посиленні нормативно-правового регулювання. Практика США демонструє нерозривний зв'язок інформаційної безпеки з національною та воєнною безпекою, що забезпечується багаторівневою системою органів, стратегічним плануванням і значними фінансовими ресурсами, спрямованими на захист кіберпростору та критичної інформаційної інфраструктури. Європейський підхід характеризується

системністю та уніфікацією правил, пріоритетністю захисту персональних даних, розвитком спеціалізованих інституцій і механізмів співробітництва між державами-членами, а також впровадженням комплексних заходів протидії дезінформації. Отримані результати свідчать про доцільність врахування кращих зарубіжних практик для підвищення ефективності публічного управління інформаційною безпекою в умовах воєнного стану.

3. Визначено, що нормативно-правове регулювання інформаційної безпеки в Україні має комплексний і багаторівневий характер та формується на основі конституційних положень, профільних законів і стратегічних документів, які визначають інформаційну та кібербезпеку як складові національної безпеки держави. Правове поле охоплює питання протидії інформаційним загрозам, дезінформації та кібератакам, захисту критичної інформаційної інфраструктури, розвитку стратегічних комунікацій, забезпечення інформаційного суверенітету та підвищення стійкості держави в умовах воєнного стану. Водночас наявні виклики засвідчують потребу в подальшому удосконаленні законодавчих і організаційних механізмів координації, реагування та системного оновлення нормативної бази відповідно до динаміки сучасних загроз.

4. Під час проведеного аналізу доведено, що в умовах воєнного стану забезпечення інформаційної безпеки України набуло системного й стратегічного характеру, оскільки інформаційний простір став повноцінним полем протиборства з державою-агресором. Аналіз засвідчив зростання ролі нормативно-правових, організаційних та фінансових механізмів у протидії інформаційним і кіберзагрозам, активізацію державної політики у сфері стратегічних комунікацій, кіберзахисту та протидії дезінформації, а також посилення взаємодії між органами публічної влади, приватним сектором і громадянським суспільством. Водночас виявлено наявність проблем координації, ресурсного забезпечення та адаптації системи публічного управління до динамічних умов воєнного протистояння, що підтверджує необхідність подальшого удосконалення механізмів забезпечення

інформаційної безпеки з метою підвищення національної стійкості держави.

5. Узагальнено підходи до моделювання публічного управління у сфері інформаційної безпеки як складової національної безпеки України з урахуванням сучасних воєнних і гібридних викликів, що дало змогу розкрити системний характер управлінських впливів у національному інформаційному просторі. Обґрунтовано доцільність застосування ризик-орієнтованого підходу як методологічної основи управління інформаційними загрозами, що забезпечує інтеграцію процесів моніторингу, аналізу, прогнозування та реагування.

Доведено, що запропонована трирівнева підсистема моніторингу інформаційних процесів і модель управління ризиками сприяють підвищенню обґрунтованості управлінських рішень, своєчасному виявленню деструктивних інформаційно-психологічних впливів та формуванню ефективних механізмів протидії, що в сукупності підсилює інформаційну стійкість держави в умовах воєнного стану.

6. Запропоновано стратегічні напрями та пріоритети розвитку публічного управління в сфері інформаційної безпеки в контексті формування національної системи стійкості, в межах якої інформаційна стійкість визначається як її органічна та системоутворююча підсистема. Показано, що забезпечення стійкого інформаційного середовища потребує комплексного поєднання заходів із протидії дезінформації та інформаційним маніпуляціям, гарантування кібербезпеки, відкритості та прозорості діяльності органів публічної влади, розвитку медіаграмотності, незалежності медіарегуляторів і міжсуб'єктної взаємодії.

Обґрунтовано, що запропонована циклічна модель інформаційної стійкості, орієнтована на протидію загрозам, передбачуваність, адаптацію до змін, стале функціонування та швидке відновлення, створює підґрунтя для підвищення адаптивності публічного управління, посилення інформаційної безпеки та захисту національних інтересів України в умовах сучасних викликів і кризових ситуацій.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Конституція України : Закон України від 28.06.1996 № 254к/96-ВР // База даних «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/go/254%D0%BA/96-%D0%B2%D1%80

2. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки» : Указ Президента України від 28.12.2021 № 685/2021. *Офіційний вісник України*. 2022. № 3. С. 22.

3. Bell D. The Coming of Post-Industrial Society : a Venture in Social Forecasting. New York : Basic Books, 1999. 507 p.

4. Wiener N. Cybernetics: Or Control and Communication in the Animal and the Machine. 2nd ed. Cambridge : The M.I.T. Press, 1985. 212 p.

5. Мак-Люен М. Галактика Ґутенберґа. Становлення людини друкованої книги / пер. з англ. А. А. Галушки, В. І. Постнікова. Київ: Ніка-Центр, 2015. 388 с.

6. Тоффлер Е. Третя хвиля / з англ. пер. А. Євса. Київ: ВД “Всесвіт”, 2000. 480 с.

7. Shannon C. E. A Mathematical Theory of Communication. The Bell System Technical Journal. 1948. Vol. 27. P. 379–423, 623–656.

8. Буньківська О. В. Інформаційний простір: соціокультурна сутність, стан та проблеми функціонування в Україні : дис. … канд. культурології : 26.00.01 – теорія й історія культури / Київ. нац. ун-т культури і мистецтв. Київ, 2009. 163 с.

9. Єсімов С. С. Інформаційний простір у контексті інформаційного права. *Вісник Нац. ун-ту “Львів. політехніка”*. Серія : Юр. науки. 2015. № 825. С. 31–36.

10. Нестеренко О. В. Методологія побудови систем інформаційно-аналітичного забезпечення адміністративного управління : дис. д-ра техн. наук

: спец. 05.13.06 “Інформ. технології” / Ін-т телекомунікацій і глобального інформ. простору НАН України. Київ, 2020. 435 с.

11. Резнікова О. Національна стійкість в умовах мінливого безпекового середовища : монографія. Київ : НІСД, 2022. 456 с.

12. Торічний В. О. Інформаційне забезпечення безпеки держави в умовах інформаційного суспільства: державно-управлінський аспект : монографія. Харків : НУЦЗУ, 2020. 274 с.

13. Теоретико-методологічні засади паспортів загроз національній безпеці України : монографія / Г. П. Ситник, В. І. Абрамов, В. А. Мандрагеля [та ін.]; під заг. ред. Г. П. Ситника, Л. М. Шипілової. Київ : НАДУ, 2012. 163 с.

14. Про національну безпеку України : Закон України від 21.06.2018 № 2469-VIII // База даних «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/go/2469-19

15. Енциклопедичний словник з державного управління / уклад. : Ю.П. Сурмін, В. Д. Бакуменко, А. М. Михненко [та ін.] ; за ред. Ю.В. Ковбасюка, В. П. Трощинського, Ю. П. Сурміна. Київ : НАДУ, 2010. 820 с.

16. Любовець Г. В., Король В. Г. Аналіз підходів до моніторингу інформаційного простору в Україні. *Держава та регіони*. Серія : Соціальні комунікації. 2015. № 3. С. 10–16.

17. Прав Р. Ю. Механізми формування і реалізації політики державної безпеки в інформаційній сфері : дис. … канд. держ. упр. : спец. 25.00.05 “Держ. упр. у сфері держ. безпеки та охорони гром. порядку” / ПрАТ “ВНЗ “МАУП”. Київ, 2020. 263 с.

18. Власенко О. В. Механізми державного регулювання захисту громадян від негативних інформаційних впливів : дис. … канд. держ. упр. : спец. 25.00.02 “Механізми держ. упр.” / Нац. акад. держ. упр. при Президентові України. Київ, 2012. 190 с.

19. Палій С. А. Формування та реалізація державної політики у сфері інформаційної безпеки у країнах ЄС: досвід для України : дис. … канд. держ.

упр. : спец. 25.00.02 “Механізми держ. упр.” / ПрАТ “ВНЗ “МАУП”. Київ, 2021. 237 с.

20. Литвиненко Н. П., Ополинська Д. Національні інтереси України в інформаційній сфері. *Актуальні проблеми міжнародних відносин*. 2010. Вип. 94, ч. ІІ. С. 67–71.

21. Чмир Я. Сучасні проблеми інформаційної безпеки України та перспективні напрями їх вирішення. *Наукові праці МАУП*. Політичні науки та публічне управління. 2022. Вип. 2 (62). С. 149–154.

22. Rozporządzenie Rady Ministrów w sprawie ustanowienia Pełnomocnika Rządu do spraw Bezpieczeństwa Przestrzeni Informacyjnej Rzeczypospolitej Polskiej z dnia 11 sierpnia 2022 r. Dziennik Ustaw Rzeczypospolitej Polskiej. 17 sierp. 2022 r. Poz. 1714. S. 1–2.

23. Information and Privacy Commissioner of Ontario. URL : https://www.ipc.on.ca/

24. Information Commissioner’s Office. URL : https://ico.org.uk/

25. Проскура Г. М. Перспективи створення інституту інформаційного комісара в Україні. *Конституційно-правові академічні студії*. 2016. Вип. 1. С. 118–123.

26. Митко А. М., Кольцова І. І. Інформаційна безпека в контексті введення інституту інформаційного комісара (омбудсмена) в Україні. *Медіафорум: аналітика, прогнози, інформаційний менеджмент*. 2018. Т. 6. С. 112–122.

27. Perera D. US Federal Budget Proposes $27.5B for Cybersecurity. URL : https://www.bankinfosecurity.com/us-federal-budget-proposes-275b-for-cybersecurity-a-24575

28. Computer Security Act of 1987. URL : https://www.congress.gov/bill/100th-congress/house-bill/145/text

29. National Plan for Information Systems Protection. Version 1.0. An Invitation to a Dialogue. URL : https://irp.fas.org/offdocs/pdd/CIP-plan.pdf

30. USA Patriot Act. URL : https://www.congress.gov/107/plaws/publ56/PLAW-107publ56.htm

31. First National Strategy for Homeland Security. URL : https://www.dhs.gov/publication/first-national-strategy-homeland-security

32. Homeland Security Act of 2002. URL : https://www.congress.gov/bill/107th-congress/house-bill/5005/text

33. The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets. URL : https://www.dhs.gov/xlibrary/assets/Physical_Strategy.pdf

34. The National Strategy to Secure Cyberspace. URL : https://www.cisa.gov/sites/default/files/publications/cyberspace_strategy.pdf

35. Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних : конвенція Ради Європи від 28.01.1981. *Офіційний вісник України*. 2011. № 1. С. 701.

36. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) / EUR-Lex. URL : https://eur-lex.europa.eu/eli/reg/2016/679/oj

37. European Union Agency for Cybersecurity (ENISA). URL : https://www.enisa.europa.eu/

38. European Cybercrime Centre - EC3. URL : https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3

39. European Data Protection Supervisor (EDPS). URL : https://www.edps.europa.eu/_en

40. NIS Cooperation Group. URL : https://digital-strategy.ec.europa.eu/en/policies/nis-cooperation-group

41. Joint communication to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions. Action Plan against Disinformation. JOIN(2018) 36 final. 05.12.2018.

Brussels, 2018. URL : https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX% 3A52018JC0036

42. 2018 Code of Practice on Disinformation. URL : https://digital-strategy.ec.europa.eu/en/library/2018-code-practice-disinformation

43. Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року «Про Стратегію національної безпеки України» : Указ Президента України від 14.09.2020 № 392/2020. *Офіційний вісник України*. 2020. № 75. С. 127.

44. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» : Указ Президента України від 26.08.2021 № 447/2021. *Офіційний вісник України*. 2021. № 70. С. 42.

45. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII // База даних "Законодавство України" / ВР України. URL: https://zakon.rada.gov.ua/go/2163-19

46. Про рішення Ради національної безпеки і оборони України від 30 грудня 2021 року «Про Стратегію забезпечення державної безпеки» : Указ Президента України від 16.02.2022 № 56/2022. *Офіційний вісник України*. 2022. № 17. С. 7.

47. Global Cybersecurity Index 2020. URL : https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E

48. National Cyber Security Index. URL : https://ncsi.ega.ee/

49. Strengthening the role of ITU in building confidence and security in the use of information and communication technologies : Resolution 130 (Rev. Dubai, 2018). URL : https://www.itu.int/en/ITU-D/Cybersecurity/Documents/RES_130_rev_Dubai.pdf

50. Про Державний бюджет України на 2022 рік : Закон України від 02.12.2021 № 1928-IX // База даних "Законодавство України" / ВР України. URL : https://zakon.rada.gov.ua/laws/show/1928-20#Text

51. Про Державний бюджет України на 2023 рік : Закон України від 03.11.2022 № 2710-IX // База даних “Законодавство України” / ВР України. URL : https://zakon.rada.gov.ua/laws/show/2710-20#Text

52. Про Державний бюджет України на 2024 рік : Закон України від 09.11.2023 № 3460-IX // База даних “Законодавство України” / ВР України. URL : https://zakon.rada.gov.ua/laws/show/3460-20#Text

53. Пилипчук В. Г. Розвиток правової науки в інформаційній сфері: системні проблеми та пріоритети. *Право України*. 2013. № 9/2013. С. 146–161.

54. Копанчук В. О. Державна політика у сфері національної безпеки та охорони громадського порядку : дис. … докт. держ. упр. : спец. 25.00.05 “Держ. упр. у сфері держ. безпеки та охорони гром. порядку” / НУЦЗУ. Харків, 2020. 375 с.

55. Belton C. Kremlin runs disinformation campaign to undermine Zelensky, documents show. The Washington Post. 2024. Feb. 16th. URL : https://www.washingtonpost.com/world/2024/02/16/russian-disinformation-zelensky-zaluzhny/

56. ДСТУ ISO 31000:2018 (ISO 31000:2018, IDT). Менеджмент ризиків. Принципи та настанови = Risk management – Guidelines. [Чинний від 2019–01–01]. Вид. офіц. Київ, 2018. 16 с.

57. Радутний О. Е. Поняття та ознаки інформаційної агресії на законодавчому рівні в кримінально-правовій сфері. *Інформація і право*. 2015. № 2 (14). С. 58–63.

58. Саприкін О. Інформаційна експансія, інформаційна війна та інформаційна атака у засобах масової інформації на прикладі Євро-2012. *Вісник Книжкової палати*. 2013. № 1. С. 40–43.

59. Ільницька У. Інформаційна безпека України: сучасні виклики, загрози та механізми протидії негативним інформаційно-психологічним впливам. *Humanitarian vision*. 2016. Vol. 2, Num. 1. С. 27–32.

60. Діордіца І. В. Інформаційні інтервенції як загроза кібернетичній безпеці. *Науковий вісник Херсонського державного університету*. Серія : Юридичні науки. 2015. Вип. 6 (2). С. 50–56.

61. Національні системи оцінювання ризиків і загроз: кращі світові практики, нові можливості для України : аналіт. доп. / [О. О. Резнікова, К.Є. Войтовський, А. В. Лепіхов] ; за заг. ред. О. О. Резнікової. Київ : НІСД, 2020. 84 с.

62. Teperik D. The BEACON model for resilience building in the Baltics: key lessons to learn from Ukraine: policy brief. Riga, 2023. 28 p.

63. Rantamäki A. “Kun talo on tulessa, on keskustelua vaikea käydä” – Tapaustutkimus informaatioresilienssin ilmaantumisesta koronapandemian aikana. *Hallinnon tutkimus*. 2023. № 42(3). S. 284–302.

64. Про рішення Ради національної безпеки і оборони України від 20 серпня 2021 року «Про запровадження національної системи стійкості» : Указ Президента України від 27.09.2021 № 479/2021. Офіційний вісник України. 2021. № 79. С. 31.

Виконав: студент магістратури за спеціальністю 281 Публічне управління та адміністрування заочної форми навчання _____Кирил ВОРОБЙОВ

Наукова керівниця:
доцентка кафедри публічного управління та адміністрування, к.е.н., доцентка _____Леся ОМЕЛЬЧУК

Робота допущена до захисту:
завідувач кафедри публічного управління та адміністрування, д.держ.упр., професор _____Едуард ЩЕПАНСЬКИЙ