Міністерство освіти і науки України
Національний технічний університет
«Дніпровська політехніка»
Навчально-науковий інститут державного управління
Кафедра державного управління і місцевого самоврядування

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеня магістра

Здобувача вищої освіти *Полішка Миколи Сергійовича*

академічної групи *281м-23-2 ІДУ*

спеціальності *281 Публічне управління та адміністрування*

За освітньо-професійною програмою *Цифрове врядування*

на тему: *«Забезпечення інформаційної безпеки в умовах цифрової трансформації: публічно-управлінський аспект»*

Керівники	Прізвище, ініціали	Оцінка за шкалою		Підпис
		рейтинговою	інституційною	
кваліфікаційної роботи	Шумляєва І. Д.			
розділів:				

Рецензент:				

Нормоконтролер:	Кравцов О. В.			

Дніпро
2024

РЕФЕРАТ

Пояснювальна записка кваліфікаційної роботи ступеня магістра на тему «Забезпечення інформаційної безпеки в умовах цифрової трансформації: публічно-управлінський аспект».

73 стор., 4 табл., 68 джерел.

ПУБЛІЧНЕ УПРАВЛІННЯ, ІНФОРМАЦІЙНА БЕЗПЕКА, ІНФОРМАЦІЙНА ГРАМОТНІСТЬ, КІБЕРБЕЗПЕКА, НАЦІОНАЛЬНА БЕЗПЕКА, ЦИФРОВА ТРАНСФОРМАЦІЯ, МОНІТОРИНГ.

Об’єктом дослідження є суспільні процеси, що виникають під час формування системи інформаційної безпеки в Україні.

Предметом дослідження є публічно-управлінський аспект забезпечення інформаційної безпеки в умовах цифрової трансформації.

Метою кваліфікаційної роботи є теоретико-прикладне обґрунтування публічно-управлінських засад забезпечення інформаційної безпеки в Україні з урахуванням цифрової трансформації.

У першому розділі досліджуються теоретичні засади забезпечення інформаційної безпеки в публічному управлінні. Другий розділ присвячено зарубіжному та вітчизняному досвіду забезпечення інформаційної безпеки. У третьому розділі розглядаються шляхи вдосконалення інформаційної безпеки в Україні.

Сфера практичного застосування результатів роботи – органи державної влади, органи місцевого самоврядування, інститути громадянського суспільства.

ABSTRACT

Explanatory note of the master's degree qualification thesis on the topic «Ensuring information security in the conditions of digital transformation: the public administration aspect».

73 pages, 4 tables, 68 references.

PUBLIC ADMINISTRATION, INFORMATION SECURITY, INFORMATION LITERACY, CYBERSECURITY, NATIONAL SECURITY, DIGITAL TRANSFORMATION, MONITORING

The object of the study is the social processes arising during the formation of the information security system in Ukraine.

The subject of the study is the public administration aspect of ensuring information security in the context of digital transformation.

The aim of the qualification work is the theoretical and applied justification of the public administration foundations for ensuring information security in Ukraine, considering the digital transformation.

The first chapter explores the theoretical foundations of information security in public administration. The second chapter is dedicated to international and domestic experiences in ensuring information security. The third chapter focuses on ways to improve information security in Ukraine.

Scope of practical application of the research results: local self-government bodies, state authorities, and civil society institutions.

ЗМІСТ

ВСТУП

В умовах цифрової трансформації забезпечення інформаційної безпеки набуває особливої важливості, адже стрімкий розвиток технологій супроводжується зростанням ризиків, пов’язаних із кібератаками, витоком даних та маніпуляцією інформацією. Завдання держави в інформаційній сфері стосуються створення умов для гармонійного розвитку інформаційної інфраструктури, реалізації конституційних прав і свобод людини та громадянина у сфері отримання інформації та користування нею для забезпечення непорушності конституційного ладу, суверенітету та територіальної цілісності, політичної, економічної та соціальної стабільності, у безумовному дотриманні законності та правопорядку, розвитку рівноправного та взаємовигідного міжнародного співробітництва.

Неухильне зростання загроз застосування інформаційних та комунікаційних технологій у військово-політичних цілях, у тому числі як інформаційна зброя, зумовлює необхідність забезпечення інформаційної безпеки України в цілому та органів публічного управління зокрема. Інформаційна безпека також стає невід’ємною складовою національної безпеки, оскільки від неї залежить стабільність функціонування державних установ, захист персональних даних громадян і довіра до цифрових інновацій.

Відповідно до Стратегії інформаційної безпеки, затвердженої Указом Президента України від 28 грудня 2021 р. № 685/2021, передбачено, що забезпечення інформаційної безпеки визнається однією із найважливіших функцій нашої країни. Згідно із Стратегією кібербезпеки України, затвердженою Указом Президента України від 26 серпня 2021 р. № 447, в Україні запроваджуються численні ініціативи, спрямовані на розвиток кіберзахисту, які охоплюють як державний, так і приватний сектори. Створено сучасні інституції та механізми моніторингу й реагування на кіберзагрози, що дозволяють оперативно виявляти й нейтралізувати небезпеки.

Водночас забезпечення інформаційної безпеки в умовах цифрової трансформації супроводжується низкою проблем і перешкод, які потребують приділення більшої уваги. Однією з ключових труднощів є швидка еволюція загроз, які стають дедалі складнішими й технологічно витонченішими. Це вимагає постійного оновлення інструментів захисту, що часто обмежується недостатністю ресурсів або технічних можливостей. У зв'язку з цим, дослідження публічно-управлінського аспекту забезпечення інформаційної безпеки є актуальними, а глибокий аналіз сучасних загроз, розробка інноваційних підходів до їх подолання та адаптація кращих міжнародних практик є критично важливими для забезпечення ефективного захисту інформаційного простору.

Питання забезпечення необхідного та достатнього рівня інформаційної безпеки, а також формування систем забезпечення інформаційної безпеки розглядалися в працях багатьох вітчизняних науковців, серед яких: Н. Авер'янова, Я. Бєлошевич, І. Бондар, Р. Бондаренко, Л. Браілко, Т. Воропаєва, І. Залєвська, І. Котерлін, В. Михальчук, В. Новицький, Д. Смотрич, В. Фурашев, І. Шопіна, та інші. Не применшуючи значення наукового внеску цих та інших авторів, важливим залишається здійснення подальших досліджень щодо забезпечення інформаційної безпеки в Україні в контексті цифрової трансформації, що обумовило вибір даної теми кваліфікаційної роботи ступеня магістра.

Об'єктом дослідження є суспільні процеси, що виникають під час формування системи інформаційної безпеки в Україні.

Предметом дослідження є публічно-управлінський аспект забезпечення інформаційної безпеки в умовах цифрової трансформації.

Метою кваліфікаційної роботи є теоретико-прикладне обґрунтування публічно-управлінських засад забезпечення інформаційної безпеки в Україні з урахуванням цифрової трансформації.

Досягнення поставленої мети передбачає вирішення таких завдань:

– проаналізувати теоретичні підходи до змісту інформаційної безпеки в публічному управлінні;

– дослідити нормативно-правові засади забезпечення інформаційної безпеки в органах публічної влади;

– визначити сучасний стан забезпечення інформаційної безпеки в Україні та зарубіжних країнах;

– з'ясувати проблеми забезпечення інформаційної безпеки в Україні як складової національної безпеки;

– обґрунтувати напрями забезпечення інформаційної безпеки в органах публічної влади України;

– розробити пропозиції щодо покращення здійснення моніторингу та оцінки забезпечення інформаційної безпеки в органах публічної влади.

Для досягнення поставленої мети та завдань магістерської роботи використовувалися загальнонаукові та спеціальні методи дослідження, а саме: системний підхід використано для дослідження взаємодії окремих елементів інформаційної безпеки як складової національної безпеки; структурно-функціональний аналіз застосовано для з'ясування побудови системи інформаційної безпеки, її функцій; компаративний підхід дозволив порівняти особливості забезпечення інформаційної безпеки в Україні та європейських країнах; історичний підхід використано для з'ясування витоків та еволюції інформаційної безпеки у хронологічній послідовності; аналіз – для дослідження окремих елементів, ознак і властивостей інформаційної безпеки, а синтез – для вивчення і відображення її цілісності як суб'єкта цифрової трансформації; індукції, дедукції, моделювання та прогнозування – для обґрунтування напрямів і формулювання відповідних пропозицій щодо забезпечення інформаційної безпеки в умовах цифрової трансформації.

Відповідно до мети, завдань та предмету дослідження кваліфікаційна робота складається зі вступу, трьох розділів, що включають шість підрозділів, висновків і списку використаних джерел.

РОЗДІЛ 1
ТЕОРЕТИЧНІ ЗАСАДИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ПУБЛІЧНОМУ УПРАВЛІННІ

1.1. Сутнісна характеристика інформаційної безпеки в публічному управлінні

Інформаційна безпека є невід'ємною частиною загальної безпеки держави, організацій та окремих осіб, забезпечуючи захист даних, інформаційних систем і технологій від різноманітних загроз, що виникають у процесі їх обробки, зберігання та передачі. З розвитком цифрових технологій та інформаційних систем важливість інформаційної безпеки лише зростає, адже захисту підлягають не лише фізичні об'єкти, але й абстрактні елементи інформаційної інфраструктури. У цьому контексті необхідно розглянути поняття інформаційної безпеки, її основні складові та функції, а також методи та інструменти, які використовуються для забезпечення належного рівня захисту в умовах постійно змінюваних загроз.

Поняття інформаційної безпеки має багатогранне визначення, що описує її суть, роль та значущість у житті суспільства. Дослідженнями сутності інформаційної безпеки, а також засад її забезпечення займалася низка вітчизняних науковців, зокрема І. Шопіна, В. Новицький, Р. Бондаренко, В. Михальчук, Н. Авер'янова, Т. Воропаєва, Д. Смотрич, Л. Браілко та інші. На основі доробок вітчизняних фахівців [1–5], а також нормативно-правових актів проаналізуємо ознаки та основний зміст інформаційної безпеки.

Так, визначення інформаційної безпеки закріплено у Законі України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки». В ньому зазначається, що інформаційна безпека – це стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні

наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації [6].

Інформаційна безпека – це спільна відповідальність держави, організацій і кожного громадянина. Держави розробляють закони, компанії впроваджують сучасні технології захисту, а користувачі повинні дотримуватися правил безпечної поведінки в цифровому середовищі. З іншого боку, інформаційна безпека є набором інструментів і методик, що призначений захищати дані від несанкціонованого доступу та змін при зберіганні та передачі на апаратному та фізичному рівнях.

На думку В. Шемчука, з правової позиції інформаційну безпеку слід розглядати як правовідносини, які виникають при здійсненні захисних і превентивних заходів в інформаційному середовищі суспільства та держави [7, с. 34]. Як зауважують О. Малашко та М. Коваліва, доктрина інформаційної безпеки має недолік, оскільки інформаційна безпека розглядається як статичний стан. На думку науковців, цей підхід викликає протиріччя з однією з її основних характеристик – динамічністю. Інформаційна безпека, що є частиною системи національної безпеки, сама власне є системою [8].

Важливим фактором є те, що захищена інформація може представлятися у різних формах, зокрема електронній і фізичній, матеріальній та нематеріальній.

Інформаційну безпеку розглядають у двох аспектах (широкому та вузькому), кожен з яких можна класифікувати на такі види:

1. У широкому аспекті:

– за джерелом походження повноважень щодо здійснення заходів із забезпечення інформаційної безпеки (природні права і свободи людини, Конституція України, закони України, підзаконні правові акти);

– за видами суб'єктів, які забезпечують інформаційну безпеку (людина і громадянин, інститути громадянського суспільства, органи державної влади, органи місцевого самоврядування, військові формування, підприємства, установи та організації всіх форм власності);

– за ступенем обов'язковості здійснення заходів із забезпечення інформаційної безпеки: основна (для спеціально уповноважених органів публічної влади та військових формувань); факультативна (для інших органів публічної влади); делегована (для підприємств, установ та організацій, яким повноваження щодо здійснення заходів інформаційної безпеки делеговано відповідними правовими актами; необов'язкова (для громадян і суб'єктів громадянського суспільства).

2. У вузькому аспекті:

– за критерієм суб'єктів, охоплених заходами інформаційної безпеки (інформаційна безпека людини, корпорацій, органів державної влади та місцевого самоврядування, громадянського суспільства і держави в цілому);

– за критерієм інформаційних загроз (політична інформаційна безпека, воєнна інформаційна безпека, економічна інформаційна безпека, екологічна інформаційна безпека тощо);

– за критерієм досягнутих результатів (досконала і недосконала інформаційна безпека) [9, с. 61 – 62].

У сучасному суспільстві всі сфери життя функціонують з урахуванням розвиненої інформаційної структури. Економічна, політична та військова міць будь-якої держави у світі безпосередньо залежить від національного інформаційного ресурсу. Інформація, що проникає в усі сфери діяльності держави, набуває конкретного політичного, матеріального і вартісного виразу, що визначається низкою факторів, у тому числі й розмірами завданих збитків, викликаних зниженням її якості. Інформаційна безпека є одним із основних показників якості такої інформації. Саме тому інформаційна безпека та способи її забезпечення в останні роки набувають особливої актуальності у процесі публічного управління. Забезпечення інформаційної безпеки органів державної влади в Україні є одним із пріоритетних завдань держави, а також як важливий елемент національної безпеки.

Інтереси держави в інформаційній сфері полягають у створенні умов для:

– гармонійного розвитку інформаційної інфраструктури;

– реалізації конституційних прав і свобод людини та громадянина в галузі отримання інформації та користування нею з метою забезпечення непорушності конституційного ладу, суверенітету та територіальної цілісності, політичної, економічної та соціальної стабільності, у безумовному забезпеченні законності та правопорядку, розвитку рівноправного та взаємовигідного міжнародного співробітництва.

Інформаційна безпека України – це такий стан захищеності від внутрішніх та зовнішніх загроз національних інтересів в інформаційній сфері, що визначається сукупністю збалансованих потреб у забезпеченні сталого розвитку особистості, суспільства та держави. Відповідно інформаційна безпека нерозривно пов'язана з інформаційною безпекою публічних органів нашої країни. І саме органи публічної влади є тією силою, яка має забезпечувати інформаційну безпеку, використовуючи організаційно-правові та технологічні засоби.

Інформаційна безпека органів публічної влади має сприяти:

– зростанню довіри громадян до цифрових послуг, що надаються на порталах органів публічної влади;

– зміцненню гарантій недоторканності життя людей під час використання інформаційних та телекомунікаційних технологій;

– посилення співпраці громадянського суспільства, бізнесу та держави в різних галузях (зокрема, із використанням електронних технологій);

– інформаційну підтримку участі громадян в управлінні державою;

– розвитку та впровадженню інформаційних технологій в діяльності органів державної влади;

– забезпечення захисту національних інтересів в інформаційній сфері від внутрішніх та зовнішніх загроз;

– покращенню надання послуг зв'язку та обробки інформації громадянам та організаціям.

На рівні установ та організацій також нині актуалізується питання створення належної системи управління інформаційною безпекою, як частини

загальної системи управління, що базується на аналізі ризиків. Вона призначена для проєктування, впровадження, контролю, супроводу та вдосконалення заходів у галузі інформаційної безпеки. Цю систему становлять організаційні структури, політика, дії щодо планування, обов'язки, процедури, процеси та ресурси. Найбільш значущою метою більшості систем інформаційної безпеки є захист організацій, установи та її знань від знищення чи витоку. У той же час, заходи з інформаційної безпеки не повинні обмежувати або ускладнювати процеси обміну інформацією у внутрішніх відносинах організацій, оскільки це може поставити під загрозу її розвиток.

Новітнє поняття інформаційного менеджменту, висунуте К. Фокіною-Мезенцевою, визначається як процес управління та організації обробки інформації на базі комп'ютерних технологій із застосуванням управлінських інформаційних систем [10, с. 63]. За такого підходу система управління інформаційною безпекою повинна забезпечувати гарантію досягнення таких цілей як забезпечення: конфіденційності критичної інформації, неможливості несанкціонованого доступу до інформації з обмеженим доступом, цілісності інформації та пов'язаних з нею процесів (створення, введення, обробки та виведення) тощо. Досягнення поставлених цілей можливе в ході вирішення основних завдань, зокрема: визначення відповідальних за інформаційну безпеку; виявлення ризиків інформаційної безпеки та проведення їх експертної оцінки; розробка політик та правил доступу до інформаційних ресурсів; розробка системи управління ризиками інформаційної безпеки, у тому числі методи їх оцінки, контролю інформаційної безпеки.

До основних функцій системи управління інформаційною безпекою слід віднести: виявлення та аналіз ризиків інформаційної безпеки; планування та практична реалізація процесів, спрямованих на мінімізацію ризиків інформаційної безпеки; контроль цих процесів; внесення до процесів мінімізації інформаційних ризиків необхідних коригувань. Узагальнення дозволяє серед багатьох функцій інформаційної безпеки виділити такі:

– захист конфіденційності, оскільки інформаційна безпека забезпечує захист приватної та конфіденційної інформації від несанкціонованого доступу, а персональні дані користувачів, можуть бути вразливими до витоку чи викрадення;

– забезпечення цілісності даних важливо гарантувати, тому що інформація залишається точною та незмінною під час її зберігання чи передачі, і будь-яке порушення цілісності може спричинити серйозні наслідки, наприклад, неправильні діагнози в медицині або фінансові втрати в бізнесі;

– забезпечення доступності інформації, оскільки інформаційна безпека гарантує, що дані залишаються доступними для уповноважених осіб у потрібний час, а кібератаки, технічні проблеми чи природні катастрофи можуть ускладнити доступ до критично важливих систем;

– захист національної безпеки обумовлений тим, що на рівні держави інформаційна безпека має стратегічне значення для запобігання кіберзагрозам, шпигунству чи саботажу, тоді як захист інформаційних систем уряду та військових структур є основою стабільності та незалежності країни;

– боротьба з кіберзлочинністю у світі, де кіберзлочини (хакерські атаки, фішинг, крадіжка даних) стали звичною справою, а інформаційна безпека дозволяє запобігати збиткам і забезпечувати дотримання прав користувачів.

Крім цього, якісне публічне управління у сфері інформаційної безпеки має базуватися на таких принципах:

– комплексний підхід в управлінні інформаційною безпекою має бути всеосяжним, охоплювати всі компоненти інформаційної системи та враховувати всі актуальні ризики, що існують в певній інформаційній системі та за її межами;

– високий рівень керованості;

– адекватність інформації, що використовується та генерується;

– ефективність як оптимальний баланс між можливостями, продуктивністю та витратами;

– безперервність публічного управління;

– процедурний підхід як зв’язок процесів управління у цикл планування, впровадження, перевірки, коригування та підтримка нерозривного зв’язку між етапами.

Усе зазначене вище безпосередньо пов’язано із питаннями цифрової грамотності та цифрової компетентності, зважаючи на те, що інформація як об’єкт інформаційної безпеки може існувати як матеріально (на паперових носіях), так і не матеріально (на електронних і хмарних носіях). Так, цифрова компетентність (або цифрова грамотність) визнана Європейським Союзом однією з 8 ключових компетенцій для повноцінної життєдіяльності. У 2016 р. ЄС представив фреймворк Digital Competence (DigComp 2.0), де було презентовано концептуальну еталонну модель Системи цифрової компетентності громадян (табл. 1.1) [11].

У 2017 р. на конференції у Брюсселі було представлено оновлену Рамку цифрової компетентності для громадян (DigComp 2.1: Digital Competence Framework for Citizens), де компетентності залишились без змін [12]. У березні 2022 р. Європейською комісією було оприлюднено Рамку цифрових компетентностей громадян DigComp 2.2 [13], в якій суттєво було розширено частину «Приклади знань, навичок та ставлення, що застосовуються до кожної компетентності».

Загалом цифрова компетентність полягає у впевненому та критичному використанні інформаційно-комунікаційних технологій для створення, пошуку, обробки та обміну інформацією як у професійній діяльності, так і в особистому чи публічному спілкуванні.

Ця компетенція охоплює знання та навички роботи з цифровими технологіями для організації навчального процесу, вміння критично аналізувати інформаційні ресурси та оцінювати їхню доцільність у майбутній професійній діяльності, а також використовувати технологічні інновації. З огляду на це важливо визначити умови формування цифрової компетентності, розробити структурно-функціональну модель її впровадження, створити освітні технології для її розвитку та підготувати навчально-методичні матеріали для цього.

Таблиця 1.1

Концептуальна еталонна модель DigComp 2.0 [11]

№ з/п	Сфери компетентності	Компетенції
1	Інформація та уміння працювати з даними	1.1 Перегляд, пошук і фільтрація даних, інформації та цифрового контенту. 1.2 Оцінка даних, інформації та цифрового контенту. 1.3 Управління даними, інформацією та цифровим контентом.
2	Комунікація та співробітництво	2.1 Взаємодія за допомогою цифрових технологій. 2.2 Обмін за допомогою цифрових технологій. 2.3 Реалізація громадянської позиції за допомогою цифрових технологій. 2.4 Співробітництво за допомогою цифрових технологій. 2.5 Мережевий етикет. 2.6 Управління цифровою ідентичністю.
3	Створення цифрового контенту	3.1 Розробка цифрового контенту. 3.2 Інтеграція та перероблення цифрового контенту. 3.3 Авторське право і ліцензії. 3.4 Програмування.
4	Безпека	4.1 Захист пристроїв. 4.2 Захист персональних даних і приватності. 4.3 Захист здоров'я і благополуччя. 4.4 Захист навколишнього середовища.
5	Розв'язання проблем	5.1 Розв'язання технічних проблем. 5.2 Визначення потреб і технологічних заходів реагування. 5.3 Творче використання цифрових технологій. 5.4 Виявлення прогалин у цифровій компетентності.

На веб-сайті освітнього порталу Дія.Освіта, розробленого Міністерством цифрової трансформації України, висвітлено класифікацію рівнів володіння цифровими компетентностями [14], що висвітлені в таблиці 1.2.

У свою чергу, цифрова грамотність є частиною цифрової компетентності і стосується базових знань і навичок роботи з цифровими пристроями та ресурсами. Вона передбачає здатність користуватися комп'ютерами, смартфонами, інтернетом та програмами.

Цифрова грамотність є ключовою складовою сучасного інформаційного суспільства. Оскільки кожен користувач Інтернету щодня стикається з великим обсягом інформації, важливо вміти розрізняти достовірну та недостовірну

інформацію. Навички перевірки джерел, аналізу та порівняння фактів відіграють важливу роль, забезпечуючи ефективне та відповідальне використання медіа як у професійній сфері, так і в особистому житті.

Таблиця 1.2

Рівні володіння цифровими компетентностями [14]

Рівні володіння		Складність завдань	Автономність роботи	Пізнавальний домен
Базовий	A1	Прості завдання	З керівником	Запам'ятовування
	A2		Самостійно або з керівником за необхідності	
Середній	B1	Чітко визначені і шаблонні завдання, прості проблеми	Самостійно	Розуміння
	B2	Завдання та чітко визначені нешаблонні проблеми	Самостійно і відповідно до власних потреб	
Високий	C1	Завдання та проблеми різного ступеня складності	Керує роботою інших користувачів	Застосування та оцінювання
	C2	Складні завдання з обмеженим колом можливих рішень	Інтегрований внесок у професійну практику та керування іншими користувачами	Оцінювання та творчість

Цифрова грамотність відіграє важливу роль у різних аспектах життя. У повсякденному житті вона дозволяє використовувати онлайн-банкінг, здійснювати покупки через інтернет та ефективно організовувати свій бюджет за

допомогою цифрових інструментів. Вона також забезпечує безпечне користування соціальними мережами та захист приватної інформації.

У професійній сфері цифрова грамотність стала обов'язковою вимогою. Більшість професій вимагають базових навичок роботи з електронною поштою, документами та даними. Володіння додатковими цифровими компетенціями дає конкурентну перевагу на ринку праці.

В освіті цифрова грамотність відкриває доступ до сучасних платформ для навчання, таких як Moodle, Google Classroom або Zoom. Вона сприяє ефективному пошуку, використанню та аналізу навчальних матеріалів, що підвищує якість навчального процесу.

У громадському житті цифрова грамотність дає змогу брати участь у процесах е-урядування, наприклад, подавати податкові декларації чи записуватися на прийом до лікаря онлайн. Крім того, вона сприяє розвитку критичного мислення під час роботи з медіаконтентом, що допомагає формувати активну громадянську позицію.

Сутнісні відмінності цифрової грамотності та цифрової компетентності наведено в порівняльній таблиці 1.3.

Таблиця 1.3

Порівняння цифрової компетенції та цифрової грамотності

Цифрова компетенція	Цифрова грамотність
Включає розширені навички критичного та етичного використання цифрових технологій	Стосується базових навичок користування технікою
Зосереджена на результатах і адаптації до нових технологій	Спрямована на використання інструментів
Ширше поняття, що охоплює грамотність і додаткові навички	Входить до складу цифрової компетентності

Таким чином, аналіз досліджень поняття цифрової грамотності [15; 16; 17] дає можливість надати її сутнісну характеристику. Цифрова грамотність – це здатність людини ефективно знаходити, аналізувати та створювати зрозумілу

інформацію, використовуючи текст та інші засоби масової комунікації на різних цифрових платформах. За визначенням Американської бібліотечної асоціації (ALA), це вміння застосовувати інформаційні та комунікаційні технології для пошуку, оцінки, створення і передачі інформації, що вимагає як інтелектуальних, так і технічних навичок [18].

До складових цифрової грамотності відносяться:

– навички роботи з цифровими пристроями: вміння працювати з комп'ютерами, планшетами, смартфонами та іншими цифровими пристроями; використання основного програмного забезпечення, таких як текстові редактори, електронні таблиці чи веб-браузери;

– інформаційна грамотність: здатність шукати інформацію в інтернеті, оцінювати її достовірність і використовувати ефективно; критичне ставлення до інформації: розпізнавання фейкових новин, пропаганди чи маніпулятивного контенту;

– медіаграмотність: вміння створювати мультимедійний контент (зображення, відео, аудіо); розуміння правил авторського права та принципів використання відкритих даних;

– онлайн-комунікація: знання правил ефективного та етичного спілкування у цифровому середовищі (нетикет); використання електронної пошти, месенджерів та соціальних мереж;

– цифрова безпека: навички захисту особистих даних; використання антивірусного програмного забезпечення, складних паролів та інших інструментів безпеки;

– технічна грамотність: знання основних принципів роботи комп'ютерів і мереж; уміння вирішувати технічні проблеми або налаштовувати пристрої.

Інформаційна безпека держави є складним і багатогранним процесом, який охоплює такі ключові напрями:

– забезпечення захисту персональних даних;

– захист фінансової інформації;

– охорона державної таємниці;

– контроль та регулювання інформаційного простору для протидії фейкам, дезінформації та іншим аспектам інформаційної війни;

– формування позитивного іміджу держави на міжнародній арені;

– інформаційна підтримка процесів публічного управління;

– цифровізація та автоматизація управлінських процесів;

– координація впровадження сучасних цифрових технологій [19, с. 199].

У зв'язку з цим, постає необхідність створення сучасних підходів, впровадження інформаційних технологій для реалізації публічного управління інформаційною безпекою, яке визначається як процес керування заходами, що спрямовані захищати конфіденційну інформацію від несанкціонованого доступу, розголошення, використання, знищення на державному рівні, рівнях організацій або громадян.

1.2. Нормативно-правові засади забезпечення інформаційної безпеки в органах публічної влади

Нормативно-правові засади забезпечення інформаційної безпеки в органах публічної влади є ключовим елементом у забезпеченні ефективного функціонування держави та захисту її національних інтересів. Вони охоплюють правові, організаційні, технічні та інші аспекти, що регулюють обіг, захист і використання інформації. Важливість нормативно-правових засад забезпечення інформаційної безпеки важко переоцінити, адже вони є основою для формування організованої, ефективної та безпечної інформаційної системи держави. Правова основа створює регуляторні механізми, які дозволяють державним органам, бізнесу та суспільству діяти в межах чітко визначених правил, спрямованих на захист інформації, запобігання загрозам та зміцнення національної безпеки.

Нормативно-правові засади забезпечення інформаційної безпеки створюють єдину систему захисту інформації. Вони визначають загальні принципи організації захисту інформації, стандарти безпеки та критерії оцінки ризиків, вимоги до органів державної влади, які відповідають за впровадження

заходів безпеки. Наявність таких засад дозволяє уникнути хаосу, забезпечуючи системний підхід до захисту інформаційного простору.

Нормативно-правові акти створюють чіткі правила, які визначають, як суб'єкти інформаційного простору – урядові органи, бізнес і громадяни – повинні діяти для запобігання інформаційним загрозам. Крім того, нормативно-правові акти сприяють зміцненню міжнародного співробітництва у сфері інформаційної безпеки. Участь держав у глобальних ініціативах, таких як угоди з кібербезпеки, дає змогу інтегрувати найкращі практики та стандарти, наприклад ISO/IEC, у національне законодавство. Це допомагає адаптувати систему інформаційної безпеки до сучасних умов глобалізації та взаємозалежності інформаційних просторів.

Під нормативно-правовим регулюванням інформаційної безпеки України розуміють форму владного правового впливу на суспільні інформаційні відносини, що здійснюється державою з метою їх упорядкування, закріплення і забезпечення [20, с. 117]. У свою чергу, нормативно-правові акти регулюють, яким чином має забезпечуватися доступ громадян до інформації, її прозорість і захист конфіденційності. Це створює баланс між потребою вільного обігу інформації та необхідністю її захисту.

До основних завдань нормативно-правових засад забезпечення інформаційної безпеки входять:

– захист персональних даних громадян від незаконного використання;

– забезпечення прозорості державного управління;

– попередження дискримінації або порушення прав на інформацію.

На сьогодні сучасний інформаційний простір є полем для різноманітних загроз, таких як кібератаки, дезінформація, пропаганда та маніпуляції громадською думкою. Нормативно-правова база створює основу для визначення ключових загроз, розробки механізмів реагування на них, залучення відповідальних структур до протидії цим викликам.

Варто зазначити, що без чіткої нормативної бази співпраця між різними державними установами у сфері інформаційної безпеки була б хаотичною та

малоефективною. Правові засади дозволяють визначити повноваження кожного органу, встановити механізми взаємодії, забезпечити відповідальність за неналежне виконання обов'язків.

Слід виокремити, що інформаційна безпека є фундаментом для розвитку сучасних цифрових технологій і сервісів. Чіткі правила забезпечення безпеки стимулюють впровадження інновацій, захищають цифрові активи, забезпечують довіру до електронного урядування. Правова регуляція в цій сфері надає бізнесу та громадянам впевненість у тому, що їхні дані та операції перебувають під захистом.

Отже, нормативно-правові акти не лише встановлюють правила, а й створюють основу для формування культури інформаційної безпеки серед державних службовців, громадян і бізнесу. Вони мотивують до підвищення кваліфікації, інформування про загрози та способи їх уникнення. Відтак, нормативно-правова база забезпечення інформаційної безпеки є такою, що дозволяє проводити даний процес в органах публічної влади.

Нормативно-правове забезпечення інформаційної безпеки в органах публічного управління являє собою сукупність міжнародних і вітчизняних правил поведінки щодо всіх видів інформаційної безпеки їх діяльності, відображених у нормах різної юридичної сили, які також гарантуються силою державного впливу. Сукупність нормативно-правових актів, що регламентує сферу інформаційної безпеки органів публічного управління можна поділити на два рівні: міжнародний та вітчизняний (національний). Міжнародний рівень включає міжнародні нормативно-правові акти під різними назвами (договори, конвенції, декларації, пакти, меморандуми тощо) та міжнародні стандарти в галузі інформаційної безпеки.

Вищим актом за юридичною силою в Україні є Конституція, ст. 17 якої визначає, що захист суверенітету та територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього Українського народу [21]. Таким чином, ця стаття вже на конституційному рівні закріпила поняття «інформаційна безпека»

та закріпила його конституційно-правовий статус. Крім цього, забезпечення інформаційної безпеки визначено як пріоритетна функція держави.

Разом із цим, стаття 34 Конституції України закріплює положення про те, що кожен має право вільно збирати, зберігати, використовувати та розповсюджувати інформацію усно, письмово чи іншим способом – на свій вибір, а також можливість обмеження права на свободу думки і слова, вільне вираження своїх поглядів і переконань у випадку, якщо таке обмеження здійснюється в інтересах національної безпеки, територіальної цілісності або громадського порядку з метою запобігання заворушенням чи злочинам, для охорони здоров'я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя. Офіційне тлумачення положень цієї статті можемо знайти у Рішенні Конституційного Суду № 2-рп/2012 від 20 січня 2012 р. [22].

Законодавчий рівень нормативно-правової бази досліджуваної сфери представлений низкою засадничих законів. Так, основу законодавства щодо інформаційної безпеки становлять такі закони:

– «Про інформацію» від 02 жовтня 1992 р. № 2657-XII [23];

– «Про захист інформації в інформаційно-телекомунікаційних системах» від 05 липня 1994 р. № 80/94-ВР [24];

– «Про телекомунікації» від 18 жовтня 2003 р. № 1280-IV [25];

– «Про захист персональних даних» від 01 червня 2010 р. № 2297-VI [26];,

– «Про електронні документи та електронний документообіг» від 22 травня 2023 р. № 851-IV [27];,

– «Про електронні довірчі послуги» від 05 жовтня 2017 р. № 2155-VIII [28]

– «Про Національну поліцію» від 02 лютого 2015 р. № 580-VIII [29];

– «Про національну безпеку України» від 21 червня 2018 р. № 2469-VIII [30];

– «Про національну інфраструктуру геопросторових даних» від 13 квітня 2020 р. № 554-IX [31];

– «Про доступ до публічної інформації» від 13 січня 2011 р. № 2939-VI [32];

– «Про основні засади забезпечення кібербезпеки України» від 05 жовтня 2017 р. № 2163-VIII [33] тощо.

Так, ст. 3 Закону України «Про національну безпеку України» закріпила, що державна політика у сферах національної безпеки і оборони спрямовується на забезпечення воєнної, зовнішньополітичної, державної, економічної, інформаційної, екологічної безпеки, безпеки критичної інфраструктури, кібербезпеки України та на інші її напрями. У ст. 19 цього Закону на Службу безпеки України покладено обов'язки здійснювати контррозвідувальний захист державного суверенітету, конституційного ладу і територіальної цілісності, оборонного і науково-технічного потенціалу, кібербезпеки, інформаційної безпеки держави, об'єктів критичної інфраструктури [30].

Крім цього, Закон України «Про інформацію» регулює відносини, які стосуються створення, збирання, отримання, зберігання, використання, розповсюдження, охорони та захисту інформації. Відповідно його норми визначають порядок здійснення всіх видів інформаційної діяльності та формують основні напрями державної інформаційної політики. статтею 3 Закону України «Про інформацію» закріплені основні напрями державної інформаційної політики, в яку входить забезпечення інформаційної безпеки України. Під захистом інформації в цьому законі передбачено розуміти сукупність правових, адміністративних, організаційних, технічних та інших заходів, які забезпечують збереження, цілісність інформації та належний порядок доступу до неї. Важливість даного нормативно-правового акта у тому, що він визначає відповідальність осіб порушення законодавства про інформації. Тобто порушення законодавства України про інформацію тягне за собою дисциплінарну, цивільно-правову, адміністративну або кримінальну відповідальність відповідно до законів України [23].

Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» регулює відносини в галузі захисту інформації в

інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах. Закон чітко визначає, що об'єктами захисту в системі є інформація, що обробляється в ній, та програмне забезпечення, яке призначене для обробки цієї інформації. Крім того, Законом визначається порядок доступу до інформації, а також відносини між: власником інформації та власником системи; власником системи та користувачем; власниками систем [24].

Закон України «Про телекомунікації» закріпив правову основу діяльності у сфері телекомунікацій та визначає повноваження держави та її органів з управління та регулювання зазначеної діяльності, а також встановлює права, обов'язки та принципи відповідальності фізичних осіб та юридичних осіб, які беруть участь у цій діяльності або користуються телекомунікаційними послугами. Закон уточнює та розширює ст. 31 Конституції України, в якій йдеться про те, що кожному гарантується таємниця листування, телефонних розмов, телеграфної та іншої кореспонденції, оскільки закріплює норми щодо забезпечення охорони таємниці телефонних розмов, телеграфної та іншої кореспонденції, безпеки телекомунікацій [21]. З адміністративно-правового погляду цей Закон є важливим також й тому, що врегулював порядок здійснення державного управління у сфері телекомунікацій, визначаючи органи державного управління та їх компетенцію, закріпив питання державного регулювання у сфері телекомунікацій та забезпечення контролю та нагляду за ринком телекомунікацій.

Також до системи законів щодо інформаційної безпеки слід віднести Закон України «Про захист персональних даних», який регулює правові відносини, пов’язані із захистом та обробкою персональних даних, спрямований на захист основних прав і свобод людини та громадянина, зокрема забезпечення права на невтручання в особисте життя, у зв’язку з обробкою персональних даних. Він також поширюється на діяльність з обробки персональних даних, що здійснюється повністю або частково із застосуванням автоматизованих засобів, а також на діяльність з обробки персональних даних, що містяться в картотеці

або підлягають внесенню до картотеки, із застосуванням неавтоматизованих засобів [26].

Положення щодо забезпечення захисту життєво важливих інтересів людини та громадянина, суспільства та держави, національних інтересів України у кіберпросторі вміщено у Законі України «Про основні засади забезпечення кібербезпеки України». Цей Закон визначає основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їх діяльності щодо забезпечення кібербезпеки [33].

Основними суб'єктами національної системи кібербезпеки, згідно із цим Законом, є: Державна служба спеціального зв'язку та захисту інформації України, Національна поліція України, Служба безпеки України, Міністерство оборони України та Генеральний штаб Збройних Сил України, розвідувальні органи та Національний банк України. До суб'єктів, які прямо здійснюють заходи із забезпечення кібербезпеки відповідно до своєї компетенції, ст. 5 Закону України «Про основні засади забезпечення кібербезпеки України» віднесено: центральні органи виконавчої влади; місцеві державні адміністрації; органи місцевого самоврядування; правоохоронні, розвідувальні і контррозвідувальні органи, суб'єкти оперативно-розшукової діяльності; Збройні Сили України, інші військові формування, утворені відповідно до закону; Національний банк України; підприємства, установи та організації, віднесені до об'єктів критичної інфраструктури; суб'єкти господарювання, громадяни України та об'єднання громадян, інші особи, які провадять діяльність та/або надають послуги, пов'язані з національними інформаційними ресурсами, інформаційними електронними послугами, здійсненням електронних правочинів, електронними комунікаціями, захистом інформації та кіберзахистом [33].

До законів, які становлять правові засади забезпечення інформаційної безпеки України слід віднести Закон України «Про електронні документи та електронний документообіг» [27] закріпив основні організаційно-правові засади електронного документообігу та використання електронних документів. Закон

України «Про електронні довірчі послуги» [28] регулює правові та організаційні засади надання електронних довірчих послуг, а також правові та організаційні засади здійснення електронної ідентифікації [27]. Законом України «Про національну інфраструктурі геопросторових даних» регламентуються правові та організаційні засади створення, функціонування та розвитку національної інфраструктури геопросторових даних, спрямованої на забезпечення ефективного прийняття органами державної влади та органами місцевого самоврядування управлінських рішень, задоволення потреб суспільства у всіх видах географічної інформації, інтегрування у глобальну та європейську геопросторових даних [31]. Закон України «Про доступ до публічної інформації» закріпив порядок здійснення та забезпечення права кожного на доступ до інформації, яка перебуває у володінні суб'єктів владних повноважень, інших розпорядників публічної інформації, визначених цим Законом, та інформації, що становить суспільний інтерес [32].

Підзаконні нормативно-правові акти спрямовані на деталізацію окремих положень Конституції та законів України, тому мають відповідний предметний напрямок, регламентуючи конкретну сферу суспільних відносин чи напрями діяльності органів публічного управління. Для забезпечення інформаційної безпеки в державі на рівні центральних органів виконавчої влади вони відіграють суттєву роль, оскільки передбачають механізм реалізації законодавчих положень. Для недопущення суперечностей між ними важливою є їх класифікація на групи, зокрема залежно від суб'єкта їх прийняття. Наприклад, Президент України видає укази (здебільшого мають загальний характер) та розпорядження (мають індивідуальний характер).

Важливим указом Президента України у сфері інформаційної безпеки є Указ від 15 березня 2016 р. № 96/2016, яким закріплена Стратегія кібербезпеки України, основна мета якої полягає у створенні умов для безпечного функціонування кіберпростору, його використання на користь людини, суспільства та держави. Відповідно до цього указу, були затверджені й інші нормативно-правові акти, які стосуються: створення Національного

координаційного центру кібербезпеки та положення про його діяльність; заходів щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України та інші [34].

Доктрина інформаційної безпеки України, що затверджена Указом Президента України від 25 лютого 2017 р. № 47/2017, була прийнята, враховуючи існування комплексного характеру існуючих загроз національній безпеці у сфері захисту інформації, що потребувало у зв'язку із використанням РФ нових інформаційних технологій впливу на громадян, визначення актуальних інноваційних заходів стосовно формування відповідної часу системи захисту інформаційного простору [35]. Водночас вона не досягла рівня належного стану за багатьма показниками і була виконана тільки на 40%.

Серед позитивів слід виділити: прийняття Закону України «Про основні засади забезпечення кібербезпеки України»; деяке вдосконалення нормативного забезпечення деяких аспектів кіберзахисту об'єктів критичної інформаційної інфраструктури; створено центри (у якості підрозділів) стосовно забезпечення кібербезпеки/ кіберзахисту в Державній службі спеціального зв'язку та захисту інформації України, Службі безпеки України, Національному банку України, Міністерстві інфраструктури України, Міністерстві оборони України, Збройних Силах України; покращено координацію діяльності органів безпеки і оборони в частині забезпечення кібербезпеки шляхом створення робочого органу РНБО (Національний координаційний центр кібербезпеки); здійснення співпраці щодо кібербезпеки із США, Великою Британією, Німеччиною, Нідерландами, Японією, на наднаціональному рівні із ЄС та НАТО, зокрема проводилися навчання у цьому напрямі за участю іноземних країн і міжнародних інституцій.

До проблем виконання цієї Доктрини слід віднести такі проблеми та недоліки: неналежна координації діяльності державних органів системи кібербезпеки, що дозволяє вирішувати тільки поточні завдання; відсутність швидкого обміну інформацією в частині кіберзагроз; не сформована система підготовки та перепідготовки кадрів; відсутність ефективної моделі державно-

приватного партнерства; недостатня організація наукового супроводу здійснення наукових досліджень у сфері кібербезпеки.

У зв’язку з цим, Указом Президента України від 26 серпня 2021 р. № 447/2021 було затверджено нову Стратегію кібербезпеки України, яка розглядає кібербезпеку у глобальному контексті, визначаючи її забезпечення одним із пріоритетним напрямів реалізації політики національної безпеки в Україні, зважаючи на РФ, як джерело загрози кібербезпеці. Нова Стратегія врахувала досвід реалізації попередніх документів, а також існуючі проблеми кібербезпекового середовища і положення Стратегії кібербезпеки ЄС на цифрове десятиліття, стратегій кібербезпеки окремих держав-членів ЄС та держав-членів НАТО [36].

Верховна Рада України видає не лише законодавчі акти, але й підзаконні акти, які є основою нормативно-правового регулювання інформаційної безпеки органів публічного управління. Так, рішенням Верховної Ради України від 16 квітня 2020 р. №563-IX було прийнято постанову «Про прийняття за основу проекту Закону України про внесення змін до деяких законодавчих актів України щодо посилення захисту телекомунікаційних мереж», яка спрямована на посилення протидії пошкодженням, руйнуванням телекомунікаційних мереж, каналів кабельного електрозв'язку, будівель, веж (щогл), опор, антен, та інших станційних, лінійних та лінійно-кабельних споруд, призначених для утворення телекомунікаційних мереж [37].

Чималу роль у забезпеченні інформаційної безпеки органів публічного управління в Україні відіграють постанови та розпорядження Кабінету Міністрів України, серед яких слід виділити ті, які стосуються щорічного затвердження плану заходів щодо реалізації Стратегії кібербезпеки України, затвердження правил забезпечення захисту інформації у інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, схвалення документів щодо інформаційно-телекомунікаційного забезпечення правоохоронних органів, діяльність яких пов’язана з боротьбою зі злочинністю. На рівні центральних органів виконавчої влади видаються накази, інструкції та розпорядження

міністерств, служб, державних інспекцій та інших центральних органів виконавчої влади щодо інформаційної безпеки в Україні.

Разом з цим, існують міжнародні стандарти, що пов’язані із забезпеченням інформаційної безпеки. Сьогодні міжнародні стандарти у сфері інформаційної безпеки розробляються спільно Міжнародною організацією зі стандартизації (ISO) та Міжнародною електротехнічною комісією (IEC). Система управління інформаційною безпекою ґрунтується на ряді ключових стандартів.

Так, Британський стандарт BS 7799-1:2005 є першою частиною цього комплексу й описує кодекс практик для управління інформаційною безпекою, який включає 127 механізмів контролю. Ці механізми базуються на кращих практиках і служать основою для створення системи управління інформаційною безпекою в організаціях. BS 7799-2:2005, друга частина стандарту, містить специфікацію систем управління інформаційною безпекою. Вона також визначає критерії для проведення сертифікації таких систем. Третя частина стандарту, BS 7799-3:2006, зосереджується на управлінні ризиками в сфері інформаційної безпеки.

Міжнародний стандарт ISO/IEC 17799:2005, розроблений на основі BS 7799-1:2005, присвячений практичним правилам управління інформаційною безпекою в інформаційних технологіях. Він спрямований на створення рекомендацій щодо впровадження заходів безпеки. У свою чергу, ISO/IEC 27000 пропонує глосарій і термінологію для опису системи управління інформаційною безпекою, а ISO/IEC 27001 визначає вимоги до проєктування, реалізації, підтримки та вдосконалення таких систем.

Стандарт ISO/IEC 27002, раніше відомий як ISO/IEC 17799:2005, надає довідкову інформацію щодо вибору та впровадження заходів безпеки під час створення систем управління інформаційною безпекою. Нарешті, ISO/IEC 27005, який відповідає BS 7799-3:2006, пропонує керівництво з управління ризиками інформаційної безпеки, включаючи рекомендації для адаптації цих підходів до конкретних умов певної організації.

Ці стандарти забезпечують інтегрований підхід до створення, підтримки та сертифікації систем управління інформаційною безпекою, дозволяючи організаціям ефективно реагувати на загрози та мінімізувати ризики [38].

Таким чином, нормативно-правове забезпечення інформаційної безпеки в Україні є обширним і охоплює законодавчі, організаційні, технічні та міжнародно-правові механізми, спрямовані на захист інформаційного простору, забезпечення кібербезпеки, протидію дезінформації, захист персональних даних та підтримку інформаційного суверенітету держави.

Однак, на сьогодні все одно постають нові виклики, зокрема пов’язані з розвитком технологій, зростанням кіберзагроз, активізацією інформаційної війни та необхідністю посилення захисту критичної інфраструктури. Для їх вирішення потрібне удосконалення вже існуючих нормативно-правових актів, а також ухвалення нових, які відповідатимуть сучасним умовам і викликам.

РОЗДІЛ 2
ЗАРУБІЖНИЙ ТА ВІТЧИЗНЯНИЙ ДОСВІД ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

2.1. Стан забезпечення інформаційної безпеки в України та зарубіжних країнах

У сучасному світі інформація стала одним із найважливіших ресурсів, що визначають не лише ефективність публічного управління, але й здатність країни протистояти внутрішнім і зовнішнім викликам. Інформаційна безпека в умовах глобалізації та цифрової трансформації є одним із ключових чинників національної безпеки, що потребує особливої уваги з боку державних інститутів. Для України, яка перебуває в умовах геополітичної нестабільності, військової агресії та економічних викликів, питання інформаційної безпеки набуває стратегічного значення, особливо в контексті функціонування органів публічного управління.

Публічне управління залежить від обігу інформації, яка використовується для прийняття рішень, забезпечення комунікації з громадянами, підтримки економіки та захисту національних інтересів. Інформаційні ресурси, якими володіють органи влади, включають дані про економічні процеси, обороноздатність, демографічну ситуацію, інфраструктуру та інші критично важливі аспекти державного управління. Втрата, викривлення чи несанкціонований доступ до такої інформації може спричинити серйозні наслідки для безпеки та стабільності держави. У контексті повномасштабної військової агресії особливої важливості набувають процеси реалізації функцій публічного управління в системі забезпечення інформаційної безпеки.

Задля проведення якісного публічного управління інформаційною безпекою в Україні варто визначити слабкі, сильні сторони системи інформаційної безпеки, а також її можливості та потенційні виклики. Так, загрози, пов’язані з інформаційною безпекою, набувають усе більшого

масштабу. Дослідження цих загроз дозволяє зрозуміти, які слабкі місця існують в інформаційних системах і процесах управління, а також визначити методи їх нейтралізації. Це є запорукою попередження серйозних інцидентів.

Аналіз наукових джерел [39-41] дозволяє можна виокремити низку загроз у сфері інформаційної безпеки України. Як відзначає Є. Вознюк, до головних загроз, які негативно впливають на основи інформаційної системи, приводять до втрати інформації або її надійності, знищення чи збою функціонування, відносяться: розголошення інформації, витік інформації, несанкціонований доступ до інформації. Також сюди можна віднести розвиток «нових видів війни, або удосконалення старих (гібридна війна, асиметрична війна, еджихад, iWar); новітніх засобах впливу, зброї; гібридних загрозах; посиленні новітніх компонентів гібридної війни – «мутація пристосованості» – війна свідомості». [39].

На думку В. Редзюка та Н. Редзюк, до загроз інформаційній безпеці України слід віднести такі:

– зменшення довіри до державних інституцій та поширення фейкової інформації внаслідок інформаційної агресії рф, що спрямована на дестабілізацію суспільства;

– значні втрати інформації, порушення функціонування систем приватності громадян внаслідок кібератак;

– вразливість користувачів до фішингу, кібершахрайства та інших онлайн-загроз через недостатній рівень цифрової грамотності [40].

У свою чергу, А. Дикий, К. Наумчук, Т. Тростенюк зазначають, що основною загрозою є процес віртуалізації, що проявляється у соціальному відчуженні людини, зміні її свідомості та зосередженні на віртуальному середовищі замість реального. Швидкий розвиток інформаційних технологій створює ще одну небезпеку – поступове перетворення людини на залежний елемент інформаційних систем, що обмежує її автономність. У зв’язку з цим постає необхідність не лише захищати інформацію, але й дбати про безпеку суспільства в цілому, адже воно є джерелом і носієм усіх глобальних загроз [41].

Дослідження цих загроз дозволяє зрозуміти, які слабкі місця існують в інформаційних системах і процесах управління, а також визначити методи їх нейтралізації. Це є запорукою попередження серйозних інцидентів, таких як компрометація персональних даних громадян, злам державних інформаційних ресурсів чи підрив довіри до ключових органів влади. В умовах, коли інформаційна безпека безпосередньо пов’язана з національною безпекою, вивчення загроз стає невід’ємною частиною формування стратегії захисту держави.

Слабкі сторони інформаційної безпеки публічного управління в Україні є наслідком багатьох системних і структурних проблем, що були висвітлені в працях різних дослідників. Як зазначають В. Редзюк та Н. Редзюк, розвиток інформаційних технологій одночасно створює нові можливості та ризики для інформаційного простору України, які загострюються в умовах гібридної війни. Однією з основних слабких сторін є недостатня захищеність інформаційної інфраструктури державних органів, яка часто стає об’єктом кібератак, що загрожують конфіденційності та цілісності інформації [40].

На думку Є. Вознюк, проблеми інформаційної безпеки України також пов'язані з технічною застарілістю обладнання, що використовується в державних установах. Це обмежує можливості протидії сучасним кіберзагрозам. Відсутність належного фінансування та ресурсів для модернізації систем захисту погіршує ситуацію, оскільки багато установ працюють на морально застарілих технологіях, що не відповідають актуальним стандартам безпеки [39].

Наголошуючи на організаційній розпорошеності та дублюванні функцій серед державних органів, які відповідають за інформаційну безпеку А. Дикий, К. Наумчук та Т. Тростенюк наголошують на відсутності чіткої координації між ними, що ускладнює ефективне реагування на загрози. Крім того, законодавча база є недостатньо розвинутою, що створює прогалини в регулюванні питань кібербезпеки, особливо у сфері захисту даних з обмеженим доступом [41].

Науковці також підкреслюють проблему низької цифрової грамотності, яка стосується як державних службовців, так і пересічних громадян. Брак

обізнаності щодо основ кібербезпеки призводить до того, що користувачі стають мішенню для фішингових атак і кібершахрайства. Ця проблема посилюється на тлі поширення фейкової інформації та дезінформації, що викликає недовіру до державних установ і загрожує внутрішній стабільності.

На підставі вищенаведеного можна зробити висновок, що ключові слабкі сторони інформаційної безпеки України включають технічну застарілість, неефективну координацію між органами управління, прогалини в законодавстві та недостатню освіченість користувачів у питаннях кібербезпеки. Для подолання цих проблем необхідним є системний підхід, спрямований на модернізацію інфраструктури, покращення координації та розвиток кіберграмотності серед усіх учасників інформаційного простору.

Сильні сторони інформаційної безпеки публічного управління в Україні базуються на ряді досягнень, які створюють передумови для ефективного захисту національного інформаційного простору. Як зазначають В. Редзюк і Н. Редзюк, Україна досягла значного прогресу у впровадженні стратегій протидії дезінформації та кіберзагрозам. Урядові ініціативи, зокрема створення національної доктрини інформаційної безпеки, спрямовані на формування комплексної системи захисту інформаційних ресурсів держави. Однією з ключових сильних сторін є впровадження заходів кіберзахисту критично важливих об’єктів інфраструктури та покращення нормативно-правової бази у цій сфері [40].

Як підкреслює Є. Вознюк, Україна має досвід успішної протидії гібридним загрозам, зокрема у сфері інформаційної війни. Впровадження спеціалізованих центрів реагування на кіберінциденти, таких як ситуаційні центри при Службі безпеки України та Держспецзв’язку, стало важливим етапом у зміцненні інформаційної безпеки. Українські фахівці активно беруть участь у міжнародних програмах кіберзахисту, що забезпечує обмін досвідом та підвищує рівень готовності до нових викликів [39].

На думку А. Дикого, К. Намчук та Т. Тростенюк, одним із сильних аспектів є міжнародна співпраця України у сфері кібербезпеки. Зокрема, Україна активно

співпрацює з НАТО та Європейським Союзом у розробці спільних програм і стратегій. Ратифікація Будапештської конвенції про кіберзлочинність дозволила вдосконалити механізми боротьби з кіберзлочинами, а підтримка міжнародних партнерів сприяла розвитку технічних можливостей для захисту інформаційних систем [41].

Можливості для покращення інформаційної безпеки в Україні охоплюють широкий спектр ініціатив, спрямованих на інтеграцію передових технологій, міжнародного досвіду та розвиток національного потенціалу.

По-перше, це активна співпраця з такими організаціями, як НАТО та Європейський Союз, створює умови для впровадження найкращих практик кіберзахисту, підвищення технічної оснащеності та обміну знаннями, що дозволяє Україні ефективніше протистояти глобальним загрозам.

По-друге, це розвиток цифрових технологій і інновацій, зокрема штучного інтелекту та машинного навчання, відкриває перспективи для модернізації систем захисту інформації, підвищення їх ефективності у виявленні та запобіганні кіберзагрозам.

По-третє, має місце розвиток державно-приватного партнерства, як ще одного важливого напряму, який дозволяє мобілізувати ресурси приватного сектору для впровадження сучасних технологій, одночасно сприяючи розвитку внутрішнього IT-сектору, створенню нових робочих місць і зміцненню економіки.

По-четверте, освітні програми, спрямовані на підвищення кіберграмотності серед державних службовців і громадян, здатні значно зменшити уразливість до кібератак, сприяти формуванню культури інформаційної безпеки та підвищити довіру громадян до державних інституцій [39-41].

Ці можливості, поєднуючись із системним підходом до їх реалізації, можуть стати основою для створення стійкої та ефективної системи інформаційної безпеки, яка відповідає викликам сучасного світу.

На основі проведеного аналізу проілюстровано SWOT-аналіз публічного управління інформаційною безпекою в Україні (табл. 2.1).

Таблиця 2.1

SWOT-аналіз публічного управління інформаційною безпекою в Україні [39-41]

Сильні сторони (Strengths)	**Слабкі сторони (Weaknesses)**
Розвиток нормативно-правової бази, зокрема Доктрини інформаційної безпеки України.	Застарілість технічної інфраструктури та програмного забезпечення в державних установах.
Впровадження ситуаційних центрів реагування на кіберзагрози при СБУ та Держспецзв'язку.	Недостатня координація між органами, відповідальними за інформаційну безпеку.
Міжнародна співпраця з НАТО, ЄС та іншими партнерами у сфері кібербезпеки.	Низький рівень кіберграмотності серед державних службовців та населення.
Зростаючий досвід протидії гібридним загрозам та інформаційній війні.	Недостатнє фінансування на модернізацію засобів захисту інформації.
Можливості (Opportunities)	**Загрози (Threats)**
Інтеграція передових технологій, зокрема штучного інтелекту та машинного навчання, у системи кіберзахисту.	Посилення гібридних загроз, включаючи дезінформацію та кібератаки.
Розвиток державно-приватного партнерства для впровадження сучасних рішень у сфері кібербезпеки.	Розвиток нових методів кіберзлочинності, зокрема використання шкідливого програмного забезпечення.
Підвищення кіберграмотності через освітні програми та інформаційні кампанії.	Зовнішній вплив на інформаційний простір України з метою дестабілізації.
Залучення міжнародного досвіду для посилення національного потенціалу кібербезпеки.	Відсутність достатньо розвинених механізмів для протидії новітнім кіберзагрозам.

Отже, до напрямів, які постійно у полі зору органів публічної влади України є вдосконалення законодавства, поступове впровадження кіберзахисту, активна міжнародна співпраця та заходи з підвищення цифрової грамотності. Ці досягнення є важливими передумовами для подальшого зміцнення інформаційної безпеки, зокрема в умовах зростаючих гібридних загроз.

Слід зазначити, що аналіз і впровадження іноземного досвіду забезпечення інформаційної безпеки є важливим кроком для створення ефективної системи захисту інформаційного простору в Україні. Органи публічної влади відіграють центральну роль у забезпеченні національної безпеки, зокрема в інформаційній

сфері, оскільки саме вони є ключовими суб'єктами управління, які ухвалюють рішення щодо захисту критичної інфраструктури, державних даних і комунікаційних мереж. У цьому контексті вивчення досвіду таких країн, як США, Франція, Велика Британія та Німеччина має стає важливим інструментом для підвищення ефективності управлінських процесів та впровадження сучасних стандартів безпеки в Україні.

США мають одну з найбільш розвинених систем забезпечення інформаційної безпеки у світі, що базується на інтеграції державних і приватних інститутів. Вітчизняні вчені [42; 43; 44; 45;] наголошують на тому, шо для органів публічної влади України вивчення і впровадження такого досвіду могло б стати основою для формування надійної системи інформаційної безпеки, що відповідала б сучасним викликам. У цьому контексті важливо не лише переймати технічні рішення, але й адаптувати нормативно-правові механізми та організаційні підходи до національних реалій. Інтеграція передового досвіду, таких як багаторівневий захист, навчання персоналу та співпраця з приватним сектором, дозволить Україні підвищити ефективність державного управління в умовах сучасних загроз.

У сучасному контексті, з огляду на постійне зростання кіберзагроз, система інформаційної безпеки США залишається орієнтиром для багатьох країн світу. Розвиток інформаційної безпеки в США почався ще в середині XX століття, в умовах «холодної війни». Протидія радянській пропаганді, необхідність захисту державних таємниць, а також військових комунікацій сприяли усвідомленню важливості створення механізмів захисту інформаційних ресурсів. У 1974 р. були ухвалені перші закони, спрямовані на захист особистих даних громадян і державної інформації, включаючи Закон про таємницю та Закон про охорону особистих даних. Ці акти стали базою для регулювання інформаційної безпеки на державному рівні [42].

У 1980-х роках президент Р. Рейган ініціював підписання Закону «Про свободу інформації», який гарантував прозорість діяльності урядових органів, одночасно зобов'язуючи забезпечувати безпеку несекретної, але критично

важливої інформації. Водночас у цей період були прийняті директиви, такі як PD/NSC-24, що регулювали захист систем зв'язку, включаючи автоматизовані інформаційні системи [43].

Наприкінці 1990-х рр. у було США посилено сферу інформаційної безпеки шляхом ухвалення ключових законів, зокрема Закону про вдосконалення інформаційної безпеки (1997 р.), а також низки директив, які закріпили стандарти захисту інформаційних систем. Одним із важливих кроків стало створення Національного плану захисту критично важливої інфраструктури, що визначив головні напрями діяльності уряду, бізнесу та громадянського суспільства у сфері кібербезпеки [44].

Теракти 11 вересня 2001 р. стали переломним моментом у політиці національної безпеки США. Відтоді інформаційна безпека була включена до пріоритетів внутрішньої безпеки. У 2002 р. Конгрес ухвалив Закон про внутрішню безпеку, який передбачав створення Міністерства внутрішньої безпеки (МВБ). Це відомство об'єднало кілька ключових структур, включаючи Федеральне бюро розслідувань (ФБР), Агентство національної безпеки (АНБ) і Національний центр захисту інфраструктури [43].

Американська система інформаційної безпеки ґрунтується на взаємодії кількох ключових установ. Агентство національної безпеки (АНБ) відіграє провідну роль у захисті державних інформаційних ресурсів. АНБ займається шифруванням комунікацій, моніторингом кіберзагроз, координацією зусиль між державним і приватним секторами, а також розробкою стандартів захисту. Відомим проектом АНБ є «Ешелон» – глобальна система перехоплення даних, яка забезпечує стратегічну перевагу США у зборі розвідувальної інформації [44].

Кіберкомандування Міністерства оборони (USCYBERCOM), створене у 2010 р., є ще однією ключовою установою. Його завдання полягають у захисті інформаційних систем Міністерства оборони, реагуванні на кіберзагрози та проведенні наступальних операцій у кіберпросторі. Особливу увагу командування приділяє підготовці військових фахівців і впровадженню новітніх технологій у сфері кіберзахисту. Важливим аспектом діяльності USCYBERCOM

є проведення навчань та тренувань для підвищення рівня готовності до кіберзагроз [45].

Сьогодні інформаційна безпека в США є однією з найпріоритетніших сфер національної політики. У 2018 р. була затверджена Національна стратегія кібербезпеки, яка фокусується на захисті критичних об'єктів інфраструктури, таких як енергетика, транспорт і фінанси. Особливу увагу приділено співпраці з приватним сектором, який відіграє важливу роль у забезпеченні безпеки кіберпростору. Також серед спеціальних законів США щодо безпеки інформації слід виділити Національну стратегію фізичного захисту об'єктів життєзабезпечення. Разом ці стратегії передбачають побудову уніфікованої державної системи, спрямованої на протидію злочинності в інформаційній сфері та інформаційному тероризму, зокрема шляхом утворення територіальних, відомчих та приватних центрів протидії інформаційним загрозам [46, с. 93].

Відтак, досвід США у забезпеченні інформаційної безпеки свідчить про необхідність комплексного підходу, який включає законодавче регулювання, інституційну підтримку, технологічні інновації та міжнародну співпрацю. Сучасні виклики, такі як зростання кіберзагроз і посилення глобальної конкуренції у сфері інформаційних технологій, підкреслюють важливість подальшого розвитку цієї сфери. Американська модель є зразковою не лише для розвинених країн, але й для тих, хто прагне вдосконалити власну систему інформаційної безпеки.

У Франції в законодавстві інформаційна безпека означена як самостійна складова національної безпеки. Основні пріоритети цієї сфери відображені у Білій книзі оборони та національної безпеки (1972, 1994, 2008, 2013 рр.). Сучасний документ часів Е. Макрона, прийнятий у 2017 р., отримав іншу назву – «Стратегічний оборонний огляд та національна безпека» [47, с. 189]. Згідно з останньою, у Франції передбачено вирішення таких актуальних завдань:

– попередження загроз у кіберпросторі,

– збільшення наукового, технічного та кадрового потенціалу у сфері захисту інформації,

– створення особливих гарантій захисту персональних даних, захист інтелектуальної власності в Інтернеті,

– охорона національного медійного простору, гарантування психологічної недоторканності особистості [48].

Прийнята у 2015 р. Національна кіберстратегія Франції окремо виділяє питання щодо цифрових платформ, включаючи також і соціальні мережі, які негативно можуть впливати на створення цінностей, що суперечать інтересам Франції і можуть бути використані для поширення дезінформації. Такі порушення є приводом для притягнення до відповідальності згідно законодавству про національну безпеку й оборону. Крім цього, Кримінальний кодекс Франції, що набув чинності у 1993 р., передбачає застосування санкцій за атаки на систему автоматизованої інформації, а також створення перешкод для роботи інформаційної системи [49, с. 223].

Серед державних органів Франції у контексті даного дослідження слід виділити: Національну агенцію з безпеки інформаційних систем (ANSSI), Службу аудіовізуальних матеріалів при Канцелярії Президента Франції, Міжвідомчий директорат з питань інформаційних систем та зв'язку (DISIC), Директорат з розвитку засобів масової інформації (DDM) та інші [47, с. 190]. Наприклад, Національна агенція з безпеки інформаційних систем, яка створена на базі декількох структур, є міжвідомчою за своїм статусом і займається координаційною діяльністю щодо державних органів влади у сфері кібербезпеки, а також бере участь у формуванні та реалізації загальної стратегії кіберзахисту [49, с. 223].

Основними способами протидії загрозам у сфері інформаційної безпеки у Франції є:

– координація та взаємодія щодо вирішення питань захисту інтересів держави в інформаційній сфері;

– проведення відкритих та закритих заходів стосовно виявлення незаконного втручання в інформаційні системи;

– підготовка кібервійськ на професійній основі.

Досвід Франції є позитивним для України, оскільки детальна регламентація загроз інформаційній безпеці та одночасна формалізація завдань, форм та методів діяльності уповноважених суб’єктів сприяє підвищенню ефективності політики в даній сфері.

У Великій Британії інформаційна політика ґрунтується на таких принципах:

– технологічна нейтральність законів;

– активізація міжнародного співробітництва у сфері захисту інформації;

– підтримка та захист інтересів користувачів комп'ютерних та телекомунікаційних систем;

– розвиток електронної комерції в усіх галузях господарювання;

– розвиток автоматизованих систем обміну науково-технічною інформацією.

Така державна політика інформаційної безпеки дозволяє узгодити координацію діяльності органів публічної влади на загальнодержавному та місцевому рівні захисту інтересів держави в інформаційній сфері, оскільки зростає функціональність механізмів інформаційної безпеки [50, с. 103]. На особливу увагу заслуговує принцип технологічної нейтральності законів у сфері інформаційної безпеки, що означає, як вбачається, що на законодавчому рівні може бути регламентовано тільки основні засади інформаційної безпеки, що визначають виключно рівень захищеності інтересів держави у цій сфері. Що стосується підзаконного рівня, то на ньому встановлюються більш конкретизовані та індивідуалізовані аспекти щодо окремих сфер інформаційної діяльності. Такий підхід дозволяє уникнути колізій у законодавстві, які можуть виникати у зв’язку із специфікою такої діяльності.

У Німеччині інформаційна політика побудована на принципах обміну інформацією на всіх рівнях, розвитку інформаційних і комунікаційних систем, вільної конкуренції в інформаційній сфері, чіткої правової регламентації інформаційних відносин залежно від рівня діяльності. До перспективних напрямів забезпечення інформаційної безпеки Німеччини відносять:

становлення інформаційного суспільства, створення інформаційної економіки, розвиток нових інформаційних супермагістралей, інформатизація державного управління, лібералізація комунікацій, підтримка національних виробників інформаційної продукції, розвиток державного та приватного інформаційного бізнесу [51, с. 143].

Загалом Німеччина обрала таку стратегію інформаційної безпеки, в якій всі концептуальні підходи засновані на балансі інтересів держави та громадськості, що закріплено на законодавчому рівні. Про це свідчить те, що законодавство про інформаційну безпеку Німеччини складається з актів, які регламентують окремі аспекти захисту інформаційних інтересів держави та суспільства, зокрема: Федеральний Закон «Про мовну діяльність (Телемедіа)», Федеральний Закон «Про охорону персональних даних», Федеральний Закон «Про порядок доступу до інформації Федерального уряду», Федеральний Закон «Про телекомунікації».

У частині законодавства щодо сфери кібербезпеки у ФРН сформовано систему нормативно-правових актів, що відповідають актам ЄС, зокрема Директиві про безпеку мережевих та інформаційних систем [52, с. 39]. Серед основних актів Німеччини слід назвати: Закон про підвищення безпеки систем інформаційних технологій від 17 липня 2015 р. [53], Положення (регламент) про визначення критичної інфраструктури від 22 квітня 2016 р. [54]; Закон про підвищення безпеки систем інформаційних технологій 2.0. від 18 травня 2021 р. [55]; Закон про Федеральне управління з інформаційної безпеки; Закон про підвищення безпеки систем інформаційних технологій (2021 р.) та ін. На нашу думку, така конкретизація відносин на законодавчому рівні і детальна регламентація дозволяє максимально врегулювати види суспільних відносин, які виникають у зв’язку із забезпеченням інформаційної безпеки в країні.

Таким чином, досвід розвинених країн, таких як США, Франція та Німеччина, у сфері забезпечення інформаційної безпеки є надзвичайно цінним і необхідним для України. Ці країни мають багаторічний досвід розробки, впровадження та вдосконалення стратегій і технологій захисту інформації, протидії кіберзагрозам і забезпечення стійкості інформаційних систем. Їхній

підхід базується на глибокій інтеграції сучасних технологій, правових норм, а також чіткої міжвідомчої координації, що є важливим орієнтиром для нашої держави.

Однак, застосування цього досвіду вимагає ретельної апробації в українських реаліях. Україна стикається зі специфічними викликами, серед яких – агресивна інформаційна та кібернетична діяльність з боку сусідніх країн, недостатня розвиненість окремих компонентів інфраструктури та обмежені ресурси. Тому запозичення міжнародних практик має супроводжуватися їх адаптацією до українських умов, враховуючи місцеву законодавчу базу, соціально-політичні особливості та рівень технічного розвитку.

Впровадження таких адаптованих рішень дозволить не лише підвищити рівень інформаційної безпеки в Україні, а й створить умови для ефективної інтеграції в міжнародну систему захисту інформаційного простору.

2.2. Проблеми забезпечення інформаційної безпеки в Україні як складової національної безпеки

Інформаційна безпека як складова національної безпеки відіграє центральну роль у системі публічного управління, адже вона забезпечує стабільність функціонування держави, захист інтересів громадян та національного суверенітету в умовах глобалізації та цифрової трансформації. У сучасному світі інформація стала стратегічним ресурсом, здатним впливати на політичну, економічну, соціальну та оборонну сфери держави. Її захист є критично важливим для забезпечення стійкості до внутрішніх та зовнішніх загроз, які постійно зростають у цифровому середовищі.

Правові засади національної безпеки України закріплені Законом України «Про національну безпеку України» від 21 червня 2018 р. Закон наголошує на необхідності:

– захисту державного суверенітету в інформаційному просторі;

– протидії зовнішнім і внутрішнім інформаційним загрозам, зокрема пропаганді, дезінформації та кібератакам;

– розвитку інформаційної грамотності громадян для критичного мислення та стійкості до маніпуляцій [30].

Сучасна інформаційна безпека визначається як процес і стан захищеності інформаційного простору, інформаційних ресурсів та систем від реальних і потенційних загроз, які можуть порушити національний суверенітет, стабільність економіки, політичну безпеку чи громадську довіру. Її значення зростає в умовах стрімкого зростання масштабів використання інформаційних технологій, що не лише створюють нові можливості, але й відкривають простір для кібератак, дезінформації, пропаганди та інших форм впливу. У роботах дослідників, таких як В. Чалапко, наголошується, що інформаційна безпека забезпечує надійне функціонування інших компонентів національної безпеки, таких як економічна, військова, соціальна та екологічна безпека, а також сприяє зміцненню конкурентоздатності держави та суспільства в глобальному середовищі [56].

Гібридні війни та зростання напруженості у світі ще більше підкреслюють значення інформаційної безпеки для сучасної держави. У сучасних умовах інформаційна сфера стає полем для маніпуляцій і дезінформаційного впливу, що здатний дестабілізувати державні інститути. За даними А. Войціховського, у рамках національної безпеки інформаційна безпека забезпечує стійкість суспільної свідомості до зовнішніх і внутрішніх загроз, зберігає морально-психологічний баланс суспільства та запобігає руйнуванню його духовних і культурних основ. Саме маніпулювання суспільною свідомістю та дезінформація, що використовуються в сучасних інформаційних війнах, є ключовими загрозами, які потребують відповідних механізмів протидії. Як зазначає А. Войціховський, інформаційна безпека є не тільки складовою національної безпеки, а й самостійним напрямом, що вимагає інтеграції технологічних, правових і організаційних рішень [57].

Відповідно до концепцій національної безпеки, інформаційна безпека інтегрує різноманітні аспекти, включаючи кібербезпеку, захист конфіденційності даних, інформаційних систем та критичної інфраструктури. Це також передбачає захист інформаційного суверенітету держави. Як зазначає М. Шевчук, ефективна інформаційна безпека є не лише станом захищеності, але й постійним процесом діяльності компетентних органів, спрямованим на попередження та протидію загрозам, що включає активні заходи впливу в інформаційному просторі. Вона передбачає як короткострокову реакцію на виклики, так і довгострокову стратегію сталого розвитку інформаційної сфери держави [58].

Україна, як і більшість країн світу, стикається з численними викликами в інформаційній сфері. З початком гібридної агресії з боку російської федерації інформаційна війна стала одним із ключових інструментів впливу на суспільну свідомість, політичні процеси та економічну стабільність держави. За оцінками М. Шевчука, проблема інформаційної безпеки України полягає не лише у протидії зовнішнім загрозам, але й у необхідності розвивати власну інформаційну стратегію, спрямовану на зміцнення інформаційного суверенітету. В умовах сучасних загроз ефективна інформаційна безпека передбачає створення системи, яка здатна своєчасно виявляти, запобігати та нейтралізувати загрози в інформаційному просторі [58].

Глобалізація та розвиток інформаційного суспільства зробили кіберпростір новим полем для міжнародного протистояння. Створення глобального інформаційного простору забезпечує безпрецедентні можливості для обміну інформацією, але також створює нові ризики для держав. Зокрема, до основних загроз належать кібератаки, інформаційний тероризм, пропаганда та маніпуляції громадською думкою. Як наголошує В. Чалапко, у цьому контексті міжнародне співробітництво в сфері інформаційної безпеки є важливим кроком для зміцнення безпеки на національному рівні [56].

Разом з цим, варто звернути увагу на те, що зовнішні інформаційні загрози є одними з найсерйозніших викликів у сфері національної безпеки нашої

держави. До таких загроз можна віднести недостатню поінформованість українців, які перебувають за кордоном, про зовнішню та внутрішню політику країни; поширення дезінформації про ці аспекти; вплив міжнародних організацій та структур на різні сфери, зокрема військову, економічну, політичну й інформаційну, що може впливати на політичну систему України та ухвалення ключових рішень. Крім того, особливу проблему становлять утиски інформаційних прав і свобод українських громадян, які проживають за межами країни.

Зокрема, в політичній сфері інформаційні загрози негативно впливають на функціонування системи державного управління, процес підготовки, ухвалення та реалізації політичних рішень, а також на виборчі системи і процедури проведення виборів.

В економічній сфері такі загрози позначаються на ефективності роботи банківської системи та управління корпоративними правами. Це може проявлятися у формі корпоративних конфліктів, банківського шпигунства або хакерських атак, що дестабілізують економічне середовище.

У суспільній сфері інформаційні загрози впливають на механізми формування громадської думки, створення та функціонування політичних партій, громадських рухів і релігійних організацій. Це може призвести до порушення основних прав і свобод громадян, створюючи загрозу для їхніх конституційних прав.

У військовій сфері інформаційні загрози спричиняють перекручування фактів військової історії, загострення ситуації в місцях розташування військових підрозділів, провокують військові злочини, дезертирство, втрату бойового духу серед військовослужбовців і підривають обороноздатність держави.

У науково-технічній сфері ці загрози впливають на системи збереження інновацій та інтелектуальної власності, на діяльність фундаментальних і прикладних досліджень, а також на бази даних конфіденційного характеру, ставлячи під загрозу безпеку стратегічної інформації [59].

На нашу думку, забезпечення інформаційної безпеки має бути пріоритетом державної політики, адже вона напряму впливає на ефективність усієї системи національної безпеки. Сучасна державна стратегія має враховувати не тільки технічні аспекти, але й культурні та соціальні фактори, які формують інформаційну стійкість громадян. Важливим елементом тут є освіта та просвіта в сфері інформаційної грамотності, що дозволить громадянам розпізнавати дезінформацію та протидіяти маніпулятивному впливу.

Ефективна інформаційна безпека передбачає гармонійне поєднання кількох напрямів:

– захист інформаційної інфраструктури;

– розвиток національних технологій кіберзахисту;

– міжнародне співробітництво у сфері боротьби з інформаційними загрозами та формування стійкого до деструктивного впливу інформаційного суспільства.

Зрештою, це дозволить державі не лише забезпечити стабільність та безпеку, але й посилити свій вплив на міжнародній арені.

Кібербезпека, як складова інформаційної безпеки, так само відіграє значну роль у підтримці національної безпеки України. Відповідно до Закону України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 р. № 2163-VIII, кібербезпека – це захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі [33].

Це включає забезпечення сталого розвитку кіберпростору і його використання без загроз національній безпеці, правам і свободам людини, а також інтересам юридичних осіб та держави. Закон України "Про основні засади забезпечення кібербезпеки України" формує правові засади для запобігання,

виявлення і реагування на кіберзагрози, а також для ліквідації їх наслідків і відновлення нормального функціонування систем після інцидентів.

Принципи забезпечення кібербезпеки охоплюють системний підхід до регулювання кіберзахисту, враховуючи організаційні, правові, інженерно-технічні та криптографічні заходи. Закон акцентує увагу на важливості забезпечення недоторканності кіберпростору, підтримання його стабільності та надійності. У сфері кібербезпеки також передбачено міжнародну співпрацю, спрямовану на створення довіри між державами, спільну протидію кіберзагрозам, а також розслідування та запобігання кіберзлочинам. Особливий акцент зроблено на демократичному цивільному контролі за діяльністю правоохоронних органів і військових формувань, які забезпечують кібербезпеку

Основні принципи кібербезпеки, закладені у Законі України «Про основні засади забезпечення кібербезпеки України», відображають багатовимірний підхід до захисту життєво важливих інтересів особи, суспільства та держави в умовах постійних кіберзагроз. Ці принципи спрямовані на забезпечення безпеки у кіберпросторі, підтримку його стабільного розвитку та ефективного функціонування без загрози національним інтересам.

Одним із ключових принципів є визнання пріоритетності прав і свобод людини та громадянина, що вимагає дотримання їхнього захисту навіть у випадку необхідності боротьби з кіберзагрозами. Державна політика базується на балансі між необхідністю забезпечення безпеки та свободою використання кіберпростору для комунікацій, підприємництва і суспільного розвитку. Важливим є також інтеграція ризик-орієнтованого підходу, що передбачає прогнозування та мінімізацію ризиків, оцінку ймовірних загроз, щоб реагувати на них у найефективніший спосіб.

Держава прагне до побудови взаємодії між органами влади, приватним сектором і громадянським суспільством, щоб забезпечити спільне управління кіберризиками. Міжнародне співробітництво також є фундаментальним принципом, оскільки глобальний характер кіберзагроз вимагає консолідації

зусиль різних країн для спільного запобігання злочинам, розслідування інцидентів та підтримки стабільності у кіберпросторі.

Прозорість і демократичний контроль над діяльністю органів, що відповідають за кібербезпеку, також мають критичне значення. Це забезпечує довіру суспільства до прийнятих заходів і захищає від зловживання владою. Окремо держава закріплює пріоритетність захисту критичної інфраструктури, як-от енергетичних систем, банківських установ, транспортних мереж, інформаційних ресурсів, які є основою функціонування суспільства та економіки. Усі ці принципи формують цілісну систему кіберзахисту, яка здатна оперативно реагувати на загрози та сприяти розвитку інформаційного середовища України.

Важливу роль відіграє координація між суб'єктами національної системи кібербезпеки, до яких належать Державна служба спеціального зв'язку та захисту інформації України, СБУ, Міноборони, Національна поліція та інші державні органи. Ці установи мають право проводити аудит інформаційної безпеки, здійснювати реагування на кіберінциденти та вживати запобіжних заходів для захисту критичної інфраструктури та інформаційних ресурсів держави.

Окрім цього, органи державної влади повинні забезпечувати впровадження сучасних технологій кіберзахисту, розвивати механізми моніторингу кіберзагроз і стимулювати дотримання стандартів кібергігієни серед співробітників. Це включає навчання державних службовців основам кіберзахисту, формування культури безпечного використання технологій і запровадження політики реагування на інциденти у цифровому середовищі.

Особливістю державного підходу до кібербезпеки є тісна взаємодія з приватним сектором та міжнародними партнерами, що дозволяє обмінюватися досвідом і ресурсами для ефективнішого протистояння глобальним кіберзагрозам. Водночас органи державної влади прагнуть не втручатися в приватні інформаційні ресурси, якщо вони не містять даних, захищених законом, або критично важливих для національної безпеки.

Для посилення ефективності кібербезпеки, Україна активно інтегрує кращі практики та стандарти міжнародної спільноти, включаючи рекомендації НАТО та ЄС, і розвиває національні стратегії у цій сфері з урахуванням сучасних викликів і ризиків.

Відповідно до Закону України "Про основні засади забезпечення кібербезпеки України", мають місце кіберзагрози – наявні та потенційно можливі явища і чинники, що створюють небезпеку життєво важливим національним інтересам України у кіберпросторі, справляють негативний вплив на стан кібербезпеки держави, кібербезпеку та кіберзахист її об’єктів [33].

Аналіз кіберзагроз є критично важливим для органів публічної влади, оскільки це забезпечує їхню готовність до сучасних викликів цифрової епохи. Ось чотири ключові аспекти, що підкреслюють важливість такого аналізу:

1. Прогнозування ризиків і попередження атак. Аналіз кіберзагроз дозволяє виявляти потенційні загрози ще до того, як вони стануть реальними. Це дає можливість запобігти атакам, підготувати відповідні механізми захисту та мінімізувати наслідки можливих інцидентів.

2. Оцінка вразливостей. Завдяки аналізу можна виявити слабкі місця в інформаційних системах та мережах. Це дозволяє посилити захист, знизити ризики для державних даних та забезпечити стабільну роботу органів влади.

3. Захист від сучасних типів атак. Кіберзагрози постійно змінюються: з'являються нові види шкідливого програмного забезпечення, методи фішингу, атаки на хмарні сервіси тощо. Аналіз дає змогу органам влади бути на крок попереду, розуміючи тенденції у кіберзагрозах і адаптуючи заходи захисту відповідно до них.

4. Захист критичної інформації та сервісів. Органи публічної влади управляють даними, які мають високу цінність: особисті дані громадян, державні таємниці, стратегічну інформацію. Аналіз кіберзагроз дозволяє ідентифікувати, хто та чому може бути зацікавлений у цих даних, і вжити заходів для їхнього захисту.

Аналіз кіберзагроз не лише допомагає запобігти атакам, а й дозволяє будувати системи захисту, орієнтовані на майбутнє. У світі, де кіберзагрози стають невід'ємною частиною глобального середовища, їхній аналіз є необхідною умовою для стабільного функціонування державних структур.

Відтак, кіберзагрози для органів публічної влади України охоплюють широкий спектр ризиків, що виникають на тлі цифрової трансформації, геополітичної напруженості та активізації інформаційної війни. Ці загрози вражають державні інформаційні системи, порушують їхню роботу, підривають довіру громадян до цифрових послуг і створюють небезпеку для національної безпеки.

Однією з основних проблем є збільшення кількості кібератак, які спрямовані на центральні та місцеві органи влади, а також на критичну інфраструктуру. У 2023 р. кількість таких інцидентів зросла на 15,9%, досягнувши понад 2 500 випадків. Серед них найбільшу загрозу становили цілеспрямовані атаки на урядові установи, оборонний сектор і об’єкти критичної інфраструктури. Російська агресія у кіберпросторі стала невід’ємною частиною військових дій, що підтверджується високим рівнем організації та постійністю атак [60].

Окрему небезпеку становить поширення дезінформації, яка використовується як інструмент інформаційної війни. Вона спрямована на дестабілізацію політичної ситуації в країні, дискредитацію державних інституцій і маніпуляцію громадською думкою. Такі кіберзагрози набувають особливого значення під час виборчих процесів, коли маніпуляції можуть впливати на легітимність і довіру до результатів голосування.

Інша проблема полягає у внутрішніх викликах, зокрема низькому рівні обізнаності державних службовців щодо кібербезпеки. Недостатня цифрова грамотність і брак навичок у сфері кіберзахисту часто стають причиною помилок, що призводять до компрометації інформаційних систем. Для підвищення ефективності кіберзахисту необхідно забезпечити регулярне

навчання, впровадження політики кібергігієни та інтеграцію сучасних технологій, зокрема штучного інтелекту.

Недоліки в нормативно-правовому забезпеченні також створюють ризики. Нечітке регулювання, відсутність єдиної системи обміну інформацією між державними органами та недостатність фінансування для кіберзахисту ускладнюють ефективну протидію загрозам. Розвиток координаційних механізмів між різними відомствами є критично важливим для зміцнення захисту державних інформаційних ресурсів.

В умовах глобалізації та посилення міжнародної співпраці Україна активно інтегрує кращі практики та стандарти кібербезпеки. Проте важливо забезпечити не лише технічну модернізацію, а й створення культури безпеки серед громадян та службовців, які взаємодіють з державними цифровими сервісами. Це дозволить зменшити вразливість систем і підвищити рівень довіри до державного управління.

Таким чином, кіберзагрози органів публічної влади України є багатогранною проблемою, яка потребує інтегрованого підходу. Розвиток нормативно-правової бази, впровадження інноваційних технологій і навчання кадрів є ключовими елементами забезпечення кібербезпеки в державному секторі.

РОЗДІЛ 3
ШЛЯХИ ВДОСКОНАЛЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ОРГАНАХ ПУБЛІЧНОЇ ВЛАДИ УКРАЇНИ

3.1. Напрями покращення забезпечення інформаційної безпеки в органах публічної влади України

Цифрова трансформація органів публічної влади є одним із ключових чинників підвищення ефективності державного управління, прозорості та відкритості для громадян. У сучасних умовах цифровізація не лише оптимізує процеси управління, але й сприяє побудові довіри між суспільством та владою, забезпечуючи доступ до державних послуг і оперативність їх надання.

Для України, яка перебуває в процесі масштабних реформ та протидіє зовнішнім викликам, розвиток цифрової трансформації в органах публічної влади є пріоритетом. Це передбачає вдосконалення електронних сервісів, модернізацію інформаційної інфраструктури, підвищення рівня кібербезпеки та впровадження інноваційних підходів до управління даними. Однак ефективність цих змін залежить від наявності чітких стратегічних напрямів і комплексного підходу до їх реалізації. Підвищення цифрової кваліфікації державних службовців та посадових осіб є важливим напрямом реформ в умовах сучасного інформаційного та технологічного прогресу. Враховуючи глобальні зміни в економіці та суспільстві, цифрові технології стали невід'ємною частиною управлінської діяльності. Впровадження новітніх цифрових інструментів у державне управління не лише підвищує ефективність роботи державних установ, але й сприяє розвитку демократії, прозорості та підвищенню якості надання публічних послуг.

Концепція безперервного професійного розвитку, яка ґрунтується на ідеї навчання протягом усього життя, передбачає для державних службовців отримання нових знань, а також вдосконалення вже наявних професійних умінь

і навичок [64, с. 9]. Зважаючи на це, процесу підвищення кваліфікації державних службовців приділяється особлива увага з боку держави.

До основних нормативно-правових актів, що регламентують підвищення рівня професійної компетентності державних службовців, відносяться:

– Закон України «Про державну службу» від 10.12.2015 № 889-VIII [61];

– Положення про систему професійного навчання державних службовців, затверджене постановою Кабінету Міністрів України від 06.02.2019 № 106 [62].

Разом з цим, є й інші нормативно-правові акти, що регулюють процес підвищення кваліфікації державних службовців. Зокрема, Міністерство цифрової трансформації України та Національне агентство з питань державної служби підписали меморандум про співпрацю в сфері розвитку та формування цифрових компетентностей серед публічних службовців. Згідно з цим документом, цифрова грамотність була включена до вимог для управління організацією роботи та персоналом, а також до списку потреб професійного навчання, які враховуються при оцінці результатів роботи державних службовців.

Згідно з Постановою Кабінету Міністрів України від 6 лютого 2019 р. №106, було затверджено Положення «Про систему професійного навчання державних службовців, голів місцевих державних адміністрацій, їх перших заступників та заступників, посадових осіб місцевого самоврядування та депутатів місцевих рад», з останніми змінами, внесеними 30 грудня 2022 р. (№1494) [62]. У цьому документі зазначено, що для ефективного виконання професійних обов'язків державні службовці повинні постійно оновлювати свої професійні навички через освітні програми, підвищення кваліфікації, стажування та самоосвіту.

Крім цього, 3 березня 2021 р. Кабінет Міністрів України схвалив Концепцію розвитку цифрових компетентностей до 2025 року [63]. Вона передбачає підвищення рівня цифрової грамотності, формування та розвиток цифрової компетентності серед державних службовців, вдосконалення процесу оцінювання кандидатів на державну службу, розробку навчальних курсів та

тренінгів з цифрової грамотності, а також запровадження єдиного підходу до змісту та методів підвищення кваліфікації в цій сфері, надаючи методичну підтримку конкурсним комісіям для оцінки рівня цифрових навичок.

Загалом, компетенція у сфері цифрових технологій повинна сприйматися не лише як знання, що мають відношення до технічних навичок, але й як знання, більшою мірою зосереджені на когнітивних, соціальних та емоційних аспектах роботи і життя в цифровому середовищі [64].

Цифрова компетентність – багатогранний еволюціонуючий процес, що постійно змінюється при появі нових технологій [65, с. 6].

При вивченні структури цифрової компетентності державних службовців можна виділити три основні категорії навичок: базові; професійні; комплементарні. Перша категорія охоплює основні цифрові вміння, такі як використання Інтернету, сканування та розпізнавання документів, а також робота з офісними програмами для виконання щоденних завдань. Друга категорія зосереджена на більш складних навичках, що включають управління та створення цифрового контенту – наприклад, розробка веб-сайтів, чат-ботів, створення каналів і груп у месенджерах, налаштування систем електронного документообігу та ведення електронних архівів, а також робота з хмарними даними. Третя категорія включає навички, які необхідні для вирішення нових завдань, таких як планування бізнес-процесів, розвиток цифрових комунікацій у громадах через соціальні мережі, а також використання даних для аналізу та прогнозування соціальної політики, оцінки ефективності заходів у сфері соціального забезпечення. До цієї групи також належать навички управління проектами та взаємодії з громадянами через електронні сервіси та інструменти [66].

Таким чином, постає важливе питання удосконалення системи розвитку цифрової грамотності серед публічних службовців. Україна може орієнтуватися на рекомендації європейських експертів, які включають низку заходів для управління цифровими навичками та талантами. Ці заходи охоплюють три основні аспекти:

– по-перше, створення середовища для підтримки цифрової трансформації, що передбачає формування цифрової культури серед публічних службовців і культури безперервного навчання;

– по-друге, визначення необхідних навичок для цифрової держави, включаючи розвиток компетентностей, які потрібні для ефективного використання цифрових інструментів, таких як цифрова грамотність, когнітивні та соціально-емоційні навички, пов’язані з цифровим урядуванням;

– по-третє, створення ефективної цифрової робочої сили, що включає розробку стратегії відбору кадрів, справедливу систему мотивації та винагороди, планування кар’єрного росту публічних службовців та інвестиції в їх професійний розвиток [67].

Виходячи з вищезазначеного, варто визначити чіткі пропозиції та заходи щодо реалізації підвищення цифрової кваліфікації державних службовців та посадових осіб.

Підвищення цифрової кваліфікації державних службовців та посадових осіб є важливим кроком для ефективної роботи державних органів і реалізації стратегічних цілей цифрової трансформації країни. Сучасний світ вимагає від державних інституцій швидкої адаптації до змін, що стосуються інформаційних технологій. Відповідно, одним із пріоритетних завдань є створення ефективної системи навчання та розвитку цифрових компетенцій серед представників державної служби.

Для того, щоб забезпечити всебічний розвиток цифрових навичок серед державних службовців, необхідно розробити національну стратегію цифрової трансформації, яка має визначати чіткі цілі, завдання та заходи, спрямовані на підвищення рівня цифрових компетенцій на всіх етапах державної служби. Одна з основних складових такої стратегії – це розробка та впровадження регулярних програм навчання для службовців. Ці курси мають бути орієнтовані на розвиток навичок роботи з цифровими інструментами, знання законодавства в сфері електронного урядування, роботи з даними, кібербезпеки та електронного документообігу. Курси повинні бути доступні для службовців на різних рівнях,

починаючи від початкових і закінчуючи спеціалізованими програмами для керівників, які охоплюють стратегію цифровізації та управління змінами.

Системи навчання мають бути інтегровані в загальну професійну підготовку державних службовців, щоб забезпечити безперервне вдосконалення їхніх навичок. Зокрема, можна впровадити модульні навчальні курси, що дозволяють службовцям набути необхідних знань на етапах їх кар'єри. Паралельно з навчанням повинні проводитися сертифікації, які підтверджують рівень цифрових навичок, що стане важливим інструментом для оцінки кваліфікації співробітників. Додатково до внутрішнього навчання необхідно налагодити співпрацю з освітніми установами, бізнес-освітніми платформами та міжнародними організаціями, щоб забезпечити доступ до сучасних технологій навчання і новітніх знань.

Окремим напрямом є обов'язкове тестування кандидатів на державну службу щодо рівня їх цифрових компетенцій. Відбір на посади в органах державної влади повинен включати перевірку базових навичок роботи з інформаційними системами, знання норм і стандартів у сфері електронного урядування, а також уміння працювати з великими даними та іншими цифровими інструментами. Така практика дозволить забезпечити не лише високий рівень професіоналізму серед новопризначених службовців, але й сприятиме їхній швидшій адаптації до специфіки роботи в умовах цифрової трансформації.

Важливим аспектом є інтеграція цифрових інструментів у внутрішні процеси державних органів. Це передбачає використання єдиних платформ для комунікацій та обміну інформацією, а також автоматизацію рутинних адміністративних завдань, що дозволить оптимізувати роботу державних установ. Впровадження інструментів для аналізу даних дозволить не лише зекономити час, але й підвищити ефективність прийняття рішень. Крім того, державні службовці повинні мати доступ до сучасних технологій, що полегшують їхню роботу, таких як електронні системи документообігу, платформи для онлайн-послуг та інші інноваційні рішення.

Забезпечення кібербезпеки є ще однією важливою складовою цього процесу. Усі державні службовці повинні пройти курси з кібербезпеки, що навчать їх виявляти та запобігати кіберзагрозам, правильно реагувати на інциденти і захищати дані громадян. Крім того, варто впровадити програми симуляції реальних кіберінцидентів, щоб службовці могли отримати практичний досвід в управлінні кризовими ситуаціями.

Система мотивації також має важливе значення для підтримки високого рівня кваліфікації серед державних службовців. Варто запровадити програми заохочення для тих, хто успішно завершить курси або демонструє високі результати в оцінках цифрових навичок. Це можуть бути як фінансові бонуси, так і можливість кар'єрного зростання, просування на більш відповідальні посади. Крім того, створення можливості для кар'єрного зростання залежно від рівня цифрових компетенцій сприятиме створенню більш мотивованої та висококваліфікованої команди.

Оновлення технічної інфраструктури є невід’ємною частиною цієї трансформації. Це означає, що кожен державний орган має бути оснащений сучасною технікою та програмним забезпеченням, яке відповідає найвищим стандартам безпеки та ефективності. Крім того, необхідно забезпечити доступ до високошвидкісного Інтернету у всіх державних установах, включаючи віддалені райони, де підключення до мережі може бути обмеженим.

Загалом, комплексний підхід до підвищення цифрової кваліфікації державних службовців, що включає стратегію навчання, тестування, мотивації та інфраструктурні вдосконалення, створить умови для ефективної роботи державних органів у сучасному цифровому середовищі та сприятиме розвитку інноваційної та прозорої державної служби.

У свою чергу, впровадження новітнього програмно-технічного забезпечення в органах публічної влади є важливою складовою цифрової трансформації державного управління, яка дозволяє підвищити ефективність, прозорість, а також доступність та зручність надання публічних послуг громадянам. Цей процес включає модернізацію технологічної інфраструктури,

інтеграцію новітніх технологій, розробку нових інформаційних систем, а також забезпечення високого рівня безпеки даних і кіберзахисту. Запровадження програмно-технічного забезпечення має на меті не тільки автоматизацію внутрішніх процесів державних установ, але й створення умов для розвитку електронного урядування, покращення якості взаємодії держави з громадянами та підприємствами.

Упровадження новітнього програмно-технічного забезпечення для забезпечення інформаційної безпеки органів державної влади є не лише технічним, а й важливим публічно-управлінським завданням. Для ефективного використання таких засобів необхідно враховувати стратегічні, організаційні, правові та фінансові аспекти, які впливають на функціонування державної інфраструктури безпеки.

Першим етапом упровадження нового програмно-технічного забезпечення є оновлення технічної інфраструктури. Це включає модернізацію комп'ютерних мереж, серверного обладнання та забезпечення установ необхідними пристроями, такими як комп'ютери, планшети, мобільні пристрої, а також периферійні пристрої для обробки документів, зберігання та обміну даними. Застосування сучасних засобів зберігання та обробки даних дозволяє оптимізувати процеси документообігу, забезпечити швидкий доступ до інформації та дозволити державним органам працювати з великими обсягами даних (так звані великі дані або Big Data). Це дозволяє суттєво зменшити час на виконання адміністративних процедур, підвищити точність і знизити ймовірність людських помилок.

Другим важливим етапом є розробка та впровадження нових програмних продуктів, що відповідають специфічним потребам органів публічної влади. Для цього можуть бути створені спеціалізовані програмні рішення, такі як платформи для управління проектами, системи автоматизації документообігу, електронного підпису та контролю за виконанням завдань. Важливою частиною програмно-технічного забезпечення є також розробка систем для збирання, обробки та аналізу даних. Це включає інтеграцію технологій штучного інтелекту для

автоматизації рутинних операцій, аналізу великих обсягів даних та надання аналітичних інструментів для прийняття рішень. Крім цього, ці системи повинні бути сумісні між собою і забезпечувати безперебійну передачу даних між різними державними органами, що дозволяє створювати єдину цифрову екосистему для управління державними процесами.

Особливу увагу варто приділити розвитку платформ для взаємодії з громадянами, адже це один із важливих аспектів цифрової трансформації. Впровадження електронних порталів, через які громадяни можуть отримувати публічні послуги, подати заяви або звернення, є важливим етапом на шляху до розвитку електронного урядування. Такі платформи повинні бути інтуїтивно зрозумілими, безпечними та доступними для всіх категорій населення, зокрема з урахуванням потреб людей з обмеженими можливостями. Водночас, важливим аспектом є інтеграція цих платформ із національними базами даних і реєстрами, що дозволяє автоматизувати перевірку інформації та значно знизити час, необхідний для обробки запитів.

Одним з ключових аспектів впровадження новітнього програмно-технічного забезпечення є забезпечення високого рівня безпеки даних. З огляду на постійно зростаючі кіберзагрози, необхідно вжити комплексних заходів для захисту інформаційних систем від несанкціонованого доступу, витоку або пошкодження даних. Це включає впровадження сучасних засобів криптографії для захисту персональних даних та інших конфіденційних відомостей, а також створення резервних копій даних і розробку стратегій реагування на інциденти безпеки. Важливим є також проведення регулярних аудиторських перевірок систем на відповідність сучасним стандартам безпеки.

Невід’ємною частиною новітнього програмно-технічного забезпечення є також системи для ефективного управління проектами та контролю за виконанням завдань. Застосування спеціалізованих програмних продуктів для управління ресурсами та проектами допомагає ефективно розподіляти завдання між співробітниками, контролювати виконання, автоматично генерувати звіти і прогнози, а також швидко коригувати робочі процеси в разі необхідності. Це

дозволяє покращити внутрішнє управління та сприяє підвищенню продуктивності державних органів.

Також важливим аспектом є моніторинг і аналіз подій безпеки в реальному часі, що забезпечується через системи управління безпекою інформації (SIEM). Вони дозволяють збирати та аналізувати журнали подій з усіх державних органів для виявлення потенційних загроз і швидкого реагування на інциденти. Інтеграція цих засобів допомагає створити єдину інформаційну систему безпеки, яка забезпечує належний захист для всіх рівнів державної влади.

Не менш важливим є розвиток інтерфейсів для мобільних пристроїв, що дасть змогу службовцям державних органів мати доступ до необхідної інформації та виконувати завдання навіть поза робочим місцем. Це також забезпечить більш швидку і зручну взаємодію з громадянами, адже за допомогою мобільних додатків можна буде отримувати від них запити або надавати доступ до важливої інформації, що має відношення до їхніх прав та обов’язків.

Крім того, впровадження новітніх програмно-технічного забезпечення має включати стратегію оновлення технологій на регулярній основі. Це означає, що програмне та апаратне забезпечення повинно бути не тільки сучасним, але й здатним до швидкої адаптації до нових технологій та інновацій. Державні органи повинні створити системи для постійного моніторингу технологічних змін і своєчасного оновлення використовуваних технологій, що дозволить уникнути застарілих систем і забезпечити їх ефективність у довгостроковій перспективі.

Для успішного впровадження нового програмно-технічного забезпечення також необхідно навчання персоналу. Оскільки зміни, пов'язані з впровадженням нових технологій, можуть бути складними, важливо забезпечити відповідне навчання для державних службовців. Це не лише допоможе ефективно освоїти нові інструменти, але й дозволить краще зрозуміти їх потенціал для оптимізації робочих процесів.

Впровадження новітнього програмно-технічного забезпечення органів публічної влади є важливим етапом на шляху до розвитку цифрового

урядування, який дозволяє підвищити ефективність, прозорість і доступність державних послуг, знизити витрати та покращити взаємодію з громадянами.

Впровадження технічного забезпечення, що використовує біометричні дані державних службовців, є важливим кроком у забезпеченні високого рівня безпеки, а також в автоматизації процесів доступу, ідентифікації та моніторингу діяльності державних установ. Це дає можливість суттєво покращити як безпеку, так і ефективність роботи органів публічної влади, а також забезпечити точну ідентифікацію осіб, що взаємодіють із державними системами.

Основною метою використання біометричних даних є покращення процесу ідентифікації державних службовців для доступу до різноманітних ресурсів, систем і сервісів, що зберігають конфіденційну або критично важливу інформацію. Використання біометрії дозволяє замінити традиційні методи доступу, такі як паролі або карти доступу, що можуть бути вкрадені або забуті. Біометричні дані, такі як відбитки пальців, розпізнавання обличчя або сітківки ока, забезпечують більш високий рівень захисту, оскільки вони є унікальними для кожної людини та складними для підробки або несанкціонованого доступу.

Одним з перших кроків у впровадженні біометричних систем є оснащення державних установ спеціальним технічним обладнанням, таким як сканери відбитків пальців, камери для розпізнавання обличчя, системи для сканування сітківки ока, а також відповідними програмними продуктами для обробки та збереження біометричних даних. Це обладнання має бути інтегровано з існуючими інформаційними системами органів влади, що дозволяє автоматично порівнювати біометричні дані з даними в реєстрах або базах даних.

У сфері управління доступом це означає, що державні службовці можуть використовувати біометричні дані для доступу до закритих інформаційних систем, серверів, реєстрів або документів. Встановлення систем контролю доступу на основі біометрії дозволяє забезпечити тільки авторизованим особам доступ до важливої інформації, значно підвищуючи рівень захисту від несанкціонованого доступу та витоку даних. Водночас система може вести журнал усіх доступів, що дозволяє здійснювати аудит і нагляд за тим, хто і коли

здійснював доступ до конкретної інформації, що підвищує рівень контролю за використанням чутливої інформації.

Біометричні дані також можуть бути використані для забезпечення більш ефективного моніторингу діяльності держслужбовців, включаючи реєстрацію їхньої присутності на робочому місці. Системи для реєстрації робочого часу, що використовують біометричні технології (наприклад, за допомогою відбитків пальців або розпізнавання обличчя), дозволяють автоматично фіксувати початок і кінець робочого дня, а також інші моменти, пов'язані з присутністю на робочому місці. Це не лише сприяє підвищенню дисципліни, але й допомагає органам публічної влади більш ефективно управляти ресурсами та оптимізувати робочі процеси.

Інтеграція біометрії може бути також застосована у системах для контролю виконання адміністративних процесів, коли службовці мають підтвердити свою особистість для подальшого виконання конкретних дій, таких як підписання документів, зміна інформації в реєстрах або підтвердження інформації в системах електронного урядування. Наприклад, використання біометрії для ідентифікації при підписанні документів через електронні системи дає можливість забезпечити високий рівень автентифікації і уникнути підробки або неправомірних змін в офіційних реєстрах.

Також важливим аспектом є забезпечення конфіденційності біометричних даних. Всі біометричні дані повинні зберігатися в захищених інформаційних системах із використанням сучасних методів криптографії, щоб запобігти можливості їх витоку чи несанкціонованого використання. Водночас державні органи мають дотримуватися стандартів і норм щодо збору, обробки і зберігання біометричних даних, гарантуючи їхній захист і відповідність законодавству в галузі захисту персональних даних.

Впровадження біометричних технологій має не лише практичне значення, але й допомагає зміцнити довіру громадян до державних органів. Завдяки використанню біометрії у процесах ідентифікації та авторизації, державні установи можуть забезпечити надійність та прозорість виконання

адміністративних процедур, а також сприяти підвищенню рівня безпеки, що є критично важливим у сучасному цифровому світі.

Загалом, використання біометричних даних у технічному забезпеченні органів публічної влади дозволяє створити більш безпечне, ефективне та прозоре середовище для виконання державних функцій. Це сприяє не лише підвищенню внутрішньої ефективності адміністративних процесів, а й розвитку довіри серед громадян до цифрових державних послуг, що є важливим елементом у забезпеченні сталого розвитку цифрового урядування.

3.2 Здійснення моніторингу та оцінка забезпечення інформаційної безпеки в органах публічної влади

Здійснення моніторингу та оцінки забезпечення інформаційної безпеки є одним із ключових елементів для забезпечення належного рівня захисту даних у будь-якій організації, зокрема в органах публічної влади. У світі, де інформація є однією з найбільш цінних ресурсів, важливо не лише забезпечити її захист від різноманітних загроз, а й постійно спостерігати стан її безпеки, а також оцінювати ефективність вжитих заходів. Так, основні засади здійснення моніторингу оцінки рівня інформаційної безпеки полягають у такому:

– достовірність означає створення та використання бази даних та показників, які найкраще і найповніше відображають поточний стан інформаційної безпеки, а також виконання національних стратегічних завдань у цій сфері;

– системність забезпечує організований збір та аналітичний аналіз даних про стан інформаційної безпеки за єдиною методологією, відповідно до затвердженого набору показників та визначеного графіка, з використанням статистичних спостережень і спеціальних досліджень;

– своєчасність дає можливість оперативно реагувати на зміни та приймати необхідні управлінські рішення в реальному часі;

– комплексність забезпечує безперервний моніторинг розвитку показників інформаційної безпеки, узгоджуючи його з національними стратегіями, використовуючи наявні інформаційні ресурси, механізми спостереження та інструменти статистики на державному та відомчому рівнях [68, с. 295 – 296].

Разом з цим, система моніторингу та оцінки рівня інформаційної безпеки реалізується поетапно, що дозволяє здійснювати глибоке, комплексне та об'єктивне оцінювання стану безпеки та визначати конкретні заходи для її посилення на кожному етапі.

На першому етапі проводиться прогнозування потенційних зовнішніх загроз та небезпек для інформаційної безпеки. Другий етап зосереджений на виборі методичних інструментів для захисту державних інтересів від цих загроз. Саме на цьому етапі визначаються способи та форми діяльності, спрямовані на нейтралізацію можливих загроз.

На третьому етапі розробляються конкретні заходи для протидії загрозам, використовуючи методи, визначені на попередньому етапі. Результатом цього етапу є створення системи забезпечення інформаційної безпеки, яка відповідає поточним викликам та загрозам.

Четвертий етап передбачає опис цієї системи з урахуванням її кількісних та якісних параметрів. Кількісна оцінка інформаційної безпеки дозволяє визначити рівень загроз та конкретні показники стану безпеки, а також встановити їх порогові значення.

На завершальному етапі формулюється оптимальний набір показників для моніторингу та визначаються індикативні та порогові значення для кожного з них. Ці значення дозволяють оцінити поточний стан інформаційної безпеки та визначити її потенціал. В результаті, система показників стає основою для моніторингу та оцінки стану інформаційної безпеки.

Моніторинг не лише дозволяє оцінювати поточний стан цієї сфери, але й виявляти слабкі місця в системі, обирати найбільш ефективні рішення та формулювати практичні рекомендації щодо її покращення та зміцнення [68, с. 296].

Таким чином, для здійснення моніторингу та оцінки забезпечення інформаційної безпеки в органах публічної влади необхідно впровадити комплекс заходів, що охоплюють як технічні, так і організаційні аспекти. Першим кроком повинно стати визначення єдиної стратегії моніторингу, що враховує не тільки поточний стан інформаційної безпеки, а й можливі майбутні загрози та вразливості. Така стратегія повинна бути адаптована до специфіки органу, його інформаційних систем та рівня загроз, з якими він стикається.

Важливим кроком є створення ефективної системи збору та обробки даних про стан інформаційної безпеки, що має включати як постійну автоматизовану моніторингову систему, так і періодичні аудити безпеки. Використання спеціалізованих засобів для виявлення загроз, таких як системи управління подіями безпеки (SIEM), дозволяє отримувати в реальному часі інформацію про потенційні інциденти безпеки, аналізувати її та оперативно реагувати на будь-які аномалії або вторгнення. Крім того, важливо проводити постійне тестування на проникнення (пентести) для виявлення уразливих місць у інформаційних системах і програмному забезпеченні, яке використовується.

Наступним кроком є проведення глибокої оцінки загроз, що включає вивчення не тільки технічних аспектів безпеки, а й аналіз соціальних, організаційних та юридичних факторів, які можуть вплинути на безпеку інформації. Зокрема, необхідно аналізувати людський фактор — рівень підготовки персоналу, правильність виконання ними процедур безпеки та готовність до реагування на можливі інциденти.

Невід'ємною частиною оцінки безпеки є також використання методів прогнозування, які дозволяють спрогнозувати можливі загрози в умовах постійної еволюції технологій та нових форм кібератак. Оцінка ймовірних ризиків повинна ґрунтуватися на аналізі попередніх інцидентів безпеки, тенденцій у кіберзлочинності, а також на глобальних змінах в політиці безпеки.

Одним із важливих елементів моніторингу є система резервного копіювання даних та план відновлення після катастроф. Оцінка ефективності цієї системи дозволяє вчасно виявити слабкі місця в збереженні та відновленні

даних, що критично важливо для забезпечення безперервності роботи органів публічної влади. Регулярне тестування відновлення після аварій є обов'язковим для перевірки працездатності таких систем.

Ще одним важливим елементом є забезпечення належного рівня навчання та підвищення кваліфікації персоналу щодо питань інформаційної безпеки. Організація регулярних тренінгів і навчань з кібербезпеки для співробітників, тестування на знання процедур безпеки та проведення інсценованих кібератак дозволить перевірити готовність до реагування на реальні загрози. Для цього можна розробити індивідуальні навчальні програми, орієнтуючись на специфіку кожного підрозділу органу публічної влади.

Не менш важливою є інтеграція інструментів моніторингу інформаційної безпеки з іншими управлінськими системами та державними реєстрами. Це дозволить мати єдину платформу для аналізу і прийняття рішень, що базуються на всебічній інформації. Участь усіх органів, що відповідають за інформаційну безпеку в державі, в загальному процесі моніторингу забезпечить комплексний підхід і дозволить краще реагувати на міжвідомчі та міжнародні загрози.

Регулярний аудит системи інформаційної безпеки є ще одним важливим етапом, що дозволяє перевіряти відповідність наявних політик, процедур та технічних засобів міжнародним стандартам, таким як ISO 27001, NIST або іншим регуляторним вимогам. Оцінка на відповідність цим стандартам сприяє поліпшенню якості заходів безпеки та підвищенню рівня довіри до організації.

Нарешті, на основі зібраних даних, аналізу результатів тестувань і оцінки зовнішніх загроз, необхідно розробляти детальні стратегії для удосконалення існуючих заходів безпеки, визначати пріоритети для подальших інвестицій в технології безпеки та розробляти рекомендації для посилення кадрової політики в галузі кібербезпеки. Така стратегія має враховувати як поточні виклики, так і прогнози розвитку нових загроз.

Усі ці заходи повинні бути інтегровані в єдину систему управління інформаційною безпекою, що дозволяє здійснювати постійний моніторинг,

аналіз і удосконалення безпеки в режимі реального часу, тим самим забезпечуючи сталий захист інформації в органах публічної влади.

Разом з цим, важливою залишається інтеграція в систему моніторингу автоматизованих інструментів для аналізу великих даних та штучного інтелекту, які здатні швидко виявляти аномалії, які можуть свідчити про порушення або загрози. Використання таких технологій дозволить вчасно реагувати на нові та складні загрози, які можуть бути непомітні для традиційних систем моніторингу, наприклад, кібератаки на основі складних алгоритмів або нестандартні форми проникнення в мережі.

Також важливо забезпечити взаємодію між державними, приватними та міжнародними організаціями з питань інформаційної безпеки. Спільний обмін інформацією та кращими практиками допоможе знижувати ризики від глобальних загроз, таких як кібертероризм або атаки на критичну інфраструктуру. Це вимагає створення платформ для спільного реагування на кіберінциденти, обміну даними про нові загрози та спільної розробки нових стратегій захисту. Створення таких платформ на національному та міжнародному рівнях також дозволить покращити координацію дій у разі масштабних кібератак.

Паралельно з технічними заходами важливо забезпечити правову та нормативну підтримку. Оцінка інформаційної безпеки повинна базуватися на чітко визначених законах і нормах, що регулюють обробку, зберігання та передачу інформації. Вони повинні бути адаптовані до сучасних викликів, таких як обробка великих обсягів даних, захист особистої інформації громадян, а також забезпечення права на конфіденційність у цифровому середовищі. Використання механізмів правового захисту та національних стандартів забезпечить довіру громадян до державних структур і надасть змогу правильно реагувати на інциденти з інформаційною безпекою на всіх етапах.

Важливу роль відіграє і забезпечення доступу до результатів моніторингу на всіх рівнях керівництва. Рішення, що приймаються на основі цих результатів, мають бути підкріплені об'єктивними та достовірними даними. Для цього слід

створити зрозумілі механізми звітності та аудиту для всіх учасників процесу управління безпекою. Це дозволить не тільки своєчасно реагувати на зміни, але й зберігати довіру до системи, забезпечуючи відкритість і прозорість прийняття рішень.

Оцінка інформаційної безпеки також повинна включати в себе моніторинг ефективності заходів, що вже були вжиті. Для цього необхідно визначити механізми зворотного зв'язку та вбудувати в систему моніторингу інструменти для самооцінки та оцінки результатів проведених заходів безпеки. Це дозволить вчасно коригувати стратегії безпеки, адаптувати їх до нових умов і загроз.

Механізми зворотного зв’язку є ключовим інструментом для розуміння, наскільки ефективними є застосовані заходи безпеки. Вони можуть включати як автоматизовані системи збору даних про стан інфраструктури, так і регулярне опитування персоналу щодо дотримання політик безпеки та виявлення проблемних аспектів. Наприклад, періодичні внутрішні аудити можуть виявити, чи дотримуються співробітники встановлених правил, а також наскільки ефективно працюють технічні заходи, такі як обмеження доступу або система захисту даних.

Введення інструментів для самооцінки до системи моніторингу дозволяє органам публічної влади оцінювати ефективність своєї роботи без зовнішнього втручання. Самооцінка може включати аналіз відповідності стандартам і нормам, що регулюють інформаційну безпеку, наприклад, вивчення виконання внутрішніх регламентів та порівняння результатів із встановленими цілями. До таких інструментів можна віднести чек-листи для перевірки ключових аспектів безпеки, автоматизовані звіти про виконання процедур і програмні рішення, що надають статистику про вразливості.

Нарешті, необхідно розвивати систему оцінки та аналізу не лише технічних аспектів, але й організаційних та людських факторів. Людський фактор залишається однією з основних причин успіху або невдачі інформаційних атак. Регулярне навчання персоналу, проведення симуляцій та тестів на виявлення вразливих місць у поведінці співробітників, підвищення

їхньої обізнаності щодо кіберзагроз дозволить значно знизити рівень ризику, пов'язаного з людським фактором.

Таким чином, комплексна та багатоетапна система моніторингу та оцінки забезпечення інформаційної безпеки є основою для створення стійкої та надійної інфраструктури захисту інформаційних ресурсів органів публічної влади. Завдяки такому підходу забезпечується не лише ефективне реагування на поточні загрози, а й можливість адаптації до змінюваних умов та нових викликів у довгостроковій перспективі. Система, що охоплює всі етапи від виявлення загроз до оцінки результатів вжитих заходів, дозволяє створити повну картину стану інформаційної безпеки. Це сприяє ухваленню обґрунтованих рішень щодо вдосконалення захисту, забезпечуючи гнучкість і здатність органів публічної влади швидко реагувати на нові ризики. В кінцевому підсумку, така система забезпечує сталий захист інформаційних ресурсів і сприяє підтримці довгострокової стабільності в управлінні безпекою в умовах постійних змін та еволюції загроз.

ВИСНОВКИ

У результаті проведеного дослідження публічно-управлінського аспекту забезпечення інформаційної безпеки в умовах цифрової трансформації були зроблені узагальнення, а також сформульовані такі положення та рекомендації.

1. Аналіз теоретичних підходів до змісту інформаційної безпеки в публічному управлінні засвідчив, що інформаційна безпека є станом захищеності життєво важливих інтересів людини, суспільства і держави, при якому попереджається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації. Визначено, що цифрова компетентність є багатогранним процесом, що постійно змінюється за появи нових технологій, і складається з трьох основних категорій навичок (базові, професійні, комплементарні), а цифрова грамотність є частиною цифрової компетентності і стосується базових знань і навичок роботи з цифровими пристроями та ресурсами.

2. Дослідження нормативно-правової бази забезпечення інформаційної безпеки в органах публічної влади дозволило класифікувати уміщені в ній норми залежно від міжнародної та національної спрямованості щодо всіх видів інформаційної безпеки. Міжнародний рівень включає міжнародні нормативно-правові акти під різними назвами (договори, конвенції, декларації, пакти, меморандуми тощо) та стандарти в галузі інформаційної безпеки. Національний рівень включає закони та підзаконні правові акти, які приймаються з метою здійснення правового впливу на інформаційні відносини та їх упорядкування, закріплення і забезпечення, створюючи баланс між потребою вільного обігу інформації та необхідністю її захисту, що гарантуються силою державного впливу. Виділено основні завдання вітчизняного нормативно-правового регулювання сфери інформаційної безпеки: захист персональних даних громадян від

незаконного використання; забезпечення прозорості публічного управління; попередження дискримінації або порушення прав на інформацію.

3. Визначено сучасний стан інформаційної безпеки України, що відображено у SWOT-аналізі публічного управління інформаційною безпекою в Україні, проведений на основі даних про слабкі та сильні сторони, а також можливості та загрози інформаційній безпеці. Виділено ініціативи, які можуть бути застосовані для покращення інформаційної безпеки в Україні, що спрямовано на інтеграцію передових технологій та розвиток національного потенціалу з урахуванням міжнародних практик.

Аналіз досвіду зарубіжних країн у сфері забезпечення інформаційної безпеки (Німеччини, Франції, Великої Британії, США) засвідчив особливості кожної країни під час: формування нормативно-правової бази; створення спеціальних служб, державних організацій та відомств, основним напрямом роботи яких є забезпечення інформаційної безпеки, моніторинг і контроль виконання норм інформаційної безпеки. Практика провідних країн світу демонструє необхідність комплексного підходу до публічно-управлінських засад забезпечення інформаційної безпеки, який включає законодавче регулювання, інституційну підтримку, технологічні інновації та міжнародну співпрацю.

4. З’ясовано, що забезпечення інформаційної безпеки в Україні як складової національної безпеки стикається з низкою зовнішніх і внутрішніх проблем, оскільки відповідно до концепцій національної безпеки, інтегрує різноманітні аспекти, включаючи кібербезпеку, захист конфіденційності даних, інформаційних систем та критичної інфраструктури. Серед сучасних проблем забезпечення інформаційної безпеки, як складової національної безпеки в Україні, виділено військову агресію з боку Російської Федерації, кіберзагрози, недостатню обізнаність громадян у цій сфері, поширення дезінформації та інформаційні маніпуляції, що потребують застосування виважених кроків щодо їх подолання.

5. Обґрунтовано основні напрями забезпечення інформаційної безпеки в органах публічної влади України, до яких віднесено підвищення кваліфікації державних службовців та посадових осіб органів публічної влади, а також

проведення низки освітніх заходів, які сприятимуть підвищенню цифрової компетентності публічних службовців, а також покращенню цифрових навичок: базових (основні цифрові вміння), професійних (управління та створення цифрового контенту) і комплементарних (необхідні для вирішення нових завдань шляхом планування, використання даних для аналізу і прогнозування, оцінки ефективності тощо).

З метою досягнення позитивних результатів забезпечення інформаційної безпеки в органах публічної влади запропоновано використання новітнього програмно-технічного забезпечення на основі використання біометричних даних користувача для підвищення безпеки та захисту доступу до сенситивної інформації. Виокремлено етапи та ключові аспекти запровадження нового програмно-технічного забезпечення в органах публічної влади.

6. Розроблено пропозиції щодо здійснення моніторингу та оцінки забезпечення інформаційної безпеки в органах публічної влади, що стосуються необхідності впровадження комплексу заходів організаційного та технічного характеру, які базуються на засадах достовірності, системності, своєчасності та комплексності. Виділено етапи реалізації системи моніторингу та оцінки рівня інформаційної безпеки, що дозволить здійснювати глибоке, комплексне та об’єктивне оцінювання стану безпеки, а також визначати конкретні заходи для її посилення на кожній стадії.

Запропоновано заходи, які мають бути інтегровані в єдину систему управління інформаційною безпекою, зокрема: створення ефективної системи збору та обробки даних про стан інформаційної безпеки; проведення глибокої оцінки загроз; використання методів прогнозування; система резервного копіювання даних та план відновлення після катастроф; забезпечення належного рівня навчання та підвищення кваліфікації персоналу щодо питань інформаційної безпеки; інтеграція інструментів моніторингу інформаційної безпеки з іншими управлінськими системами та державними реєстрами; регулярний аудит системи інформаційної безпеки на основі зібраних даних, аналізу результатів тестувань і оцінки зовнішніх загроз.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Шопіна І. М. Інформаційна безпека цифрової трансформації. *Науковий вісник Львівського державного університету внутрішніх справ*. 2023. № 1. С. 28–35.

2. Новицький В. Я. Стратегічні засади забезпечення інформаційної безпеки в сучасних умовах. *Інформація і право*. 2022. №1 (40). С. 111–118.

3. Бондаренко Р. В., Михальчук В. М. Інформаційна безпека держави. *Інвестиції: практика та досвід*. 2021. №5. С. 95–101.

4. Авер'янова Н., Воропаєва Т. Інформаційна безпека України: соціально-філософські аспекти. *Молодий вчений*. 2020. № 10 (86). С. 297–303.

5. Смотрич Д., Браілко Л. Інформаційна безпека в умовах воєнного стану. *Науковий вісник Ужгородського університету.* 2023. С. 121–127.

6. Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки : Закон України від 09.01.2007 р. № 537-V. URL: https://zakon.rada.gov.ua/laws/show/537-16#Text (дата звернення: 28.11.2024).

7. Шемчук В.В. Інформаційна безпека та інформаційна оборона в контексті розвитку вітчизняної доктрини й законодавчої основи. *Вчені записки ТНУ імені В.І. Вернадського*. 2019. Т. 30 (69). № 4. С. 31–37.

8. Малашко О. Є., Ковалів М. В. Теоретична конструкція поняття «інформаційна безпека». *Інтернаука*. 2020. № 10. С. 20–33.

9. Онопрієнко С. Класифікація видів інформаційної безпеки як правової категорії. *Вісник Київського національного університету імені Тараса Шевченка*. 2022. № 1 (49). С. 60–62.

10. Фокіна-Мезенцева К. Інформаційна безпека у глобальному суспільстві. *Scientia fructuosa*. 2021. № 5. С. 61–71.

11. Vuorikari R., Punie Y., Carretero G., Van Den Brande G. DigComp 2.0: The Digital Competence Framework for Citizens. Update Phase 1: the Conceptual Reference Model. Luxembourg (Luxembourg). *Publications Office of the European*

Union. 2016. URL: https://publications.jrc.ec.europa.eu/repository/handle/JRC101254 (дата звернення: 28.11.2024).

12. Carretero Gomez S., Vuorikari R., Punie, Y. DigComp 2.1: The Digital Competence Framework for Citizens with eight proficiency levels and examples of use. *Publications Office of the European Union*. Luxembourg. 2017. URL: https://publications.jrc.ec.europa.eu/repository/handle/JRC106281 (дата звернення: 28.11.2024).

13. Vuorikari, R., Kluzer, S., Punie, Y. DigComp 2.2: The Digital Competence Framework for Citizens - With new examples of knowledge, skills and attitudes. *Publications Office of the European Union*. Luxembourg. 2022. URL: https://publications.jrc.ec.europa.eu/repository/handle/JRC128415 (дата звернення 28.11.2024).

14. Опис рамки цифрової компетентності для громадян України. *DigCompUa for Citizens 2.1*. URL: https://thedigital.gov.ua/storage/uploads/files/news_post/2021/3/mintsifra-oprilyudnyue-ramku-tsifrovoi-kompetentnosti-dlya-gromadyan/%D0%9E%D0%A0%20%D0%A6%D0%9A.pdf (дата звернення: 28.11.2024).

15. Крутова А. С., Ставерська Т. О. Цифрова грамотність як провідна компетентність майбутнього фахівця. *Механізми забезпечення сталого розвитку економіки : проблеми, перспективи, міжнародний досвід :* матеріали II міжнар. наук.-практ. конф. м. Харків, 23 квіт. 2021 р. С. 224–227.

16. Тілікіна Н. В. Медіа-, інформаційна і комп'ютерна грамотність як компоненти цифрової грамотності. *Scientific notes of Lviv University of Business and Law.* 2021. № 29. С. 46–56.

17. Козубцов І. М. Цифрова культура, цифрова грамотність, цифрова компетентність як сучасні освітні феномени. *Розвиток професійної культури майбутніх фахівців: виклики, досвід, стратегії, перспективи*. 2022. С. 153–156.

18. Digital Literacy. URL: https://literacy.ala.org/digital-literacy/ (дата звернення: 28.11.2024).

19. Філіпішина Л., Костик Є., Дзевелюк М. Публічне управління у сфері інформаційної безпеки (подолання сучасних загроз). *Актуальні питання у сучасній науці*. 2023. № 5 (11). С. 196–205.

20. Максименко Ю. Є. Теоретико-правові засади забезпечення інформаційної безпеки України: дис. … канд. юрид. наук: 12.00.01. Київ, 2007. 236 с.

21. Конституція України: від 28.06.1996 № 254к/96-ВР URL: https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text (дата звернення: 28.11.2024)

22. Рішення Конституційного Суду України у справі за конституційним поданням Жашківської районної ради Черкаської області щодо офіційного тлумачення положень частин першої, другої статті 32, частин другої, третьої статті 34 Конституції України від 20.01.2012 р. № 2-рп/2012 . Справа № 1-9/2012. URL: https://zakon.rada.gov.ua/laws/show/v002p710-12#Text (дата звернення: 28.11.2024).

23. Про інформацію : Закон України від 02.10.1992 р. № 2657-XII. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення: 28.11.2024).

24. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 05.07.1994 р. № 80/94-ВР. URL: https://zakon.rada.gov.ua/laws/show/80/94-вр#Text (дата звернення: 28.11.2024).

25. Про телекомунікації : Закон України від 18.11.2003 р. № 1280-IV. URL: https://zakon.rada.gov.ua/laws/show/1280-15#Text (дата звернення: 28.11.2024).

26. Про захист персональних даних : Закон України від 01.06.2010 р. № 2297-VI. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення: 28.11.2024).

27. Про електронні документи та електронний документообіг : Закон України від 22.05.2003 р. № 851-IV. URL: https://zakon.rada.gov.ua/laws/show/851-15#Text (дата звернення: 28.11.2024).

28. Про електронні довірчі послуги : Закон України від 05.10.2017 р. № 2155-VIII. URL: https://zakon.rada.gov.ua/laws/show/2155-19#Text (дата звернення: 28.11.2024).

29. Про Національну поліцію : Закон України від 02.07.2015 р. № 580-VIII. URL: https://zakon.rada.gov.ua/laws/show/580-19#Text (дата звернення 28.11.2024).

30. Про національну безпеку України : Закон України від 21.06.2018 р. № 2469-VIII. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text (дата звернення: 28.11.2024).

31. Про національну інфраструктуру геопросторових даних : Закон України від 13.04.2020 р. № 554-IX. URL: https://zakon.rada.gov.ua/laws/show/554-20#Text (дата звернення: 28.11.2024).

32. Про доступ до публічної інформації : Закон України від 13.01.2011 р. № 2939-VI. URL: https://zakon.rada.gov.ua/laws/show/2939-17#Text (дата звернення: 28.11.2024).

33. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 р. № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 28.11.2024).

34. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року "Про Стратегію кібербезпеки України": Указ Президента України від 15.03.2016 р. № 96/2016. URL: https://zakon.rada.gov.ua/laws/show/96/2016#Text (дата звернення: 28.11.2024).

35. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України» : Указ Президента України від 25.02.2017 р. № 47/2017. URL: https://zakon.rada.gov.ua/laws/show/47/2017#Text (дата звернення: 28.11.2024).

36. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України" : Указ Президента України від 26.08.2021 р. № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text (дата звернення: 28.11.2024).

37. Про прийняття за основу проекту Закону України про внесення змін до деяких законодавчих актів України щодо посилення захисту телекомунікаційних мереж : Постанова Верховної Ради України від 16.04.2020 р. № 563-IX. URL: https://zakon.rada.gov.ua/laws/show/563-IX#Text (дата звернення: 28.11.2024).

38. Мазник Л., Драган О. Інформаційна безпека організації як фактор посилення бренду роботодавця. *Київський економічний науковий журнал*. 2023. № 1. С. 39–44.

39. Вознюк Є. SWOT-аналіз стану інформаційної безпеки України. *Науковий часопис УДУ імені Михайла Драгоманова*. 2021. № 22 (30).

40. Редзюк В., Редзюк Н. Сучасні проблеми інформаційної безпеки України та напрями їх вирішення. *Публічне управління: концепції, парадигма, розвиток, удосконалення*. 2023. № 3. С. 59–65.

41. Дикий А. П., Наумчук К. М., Тростенюк Т. М. Аналіз сучасних загроз інформаційній безпеці держави. *Економічний простір*. 2021. № 176. С. 155–158.

42. Яковлєв П. О. Досвід державного регулювання забезпечення інформаційної безпеки зарубіжних держав (на приклади Сполучених Штатів Америки, Канади, Німеччини, Франції). *Вісник Харківського національного університету імені В. Н. Каразіна*. 2020. № 30. С. 106–113.

43. Шуляк Н. О. До питання про основи інформаційної та кібербезпеки США. *Науковий вісник Східноєвропейського національного університету імені Лесі Українки*. 2020. № 2 (406). С. 114–121.

44. Буга Л. В. Досвід США та Німеччини щодо забезпечення інформаційної безпеки в збройних силах. *Scientific Notes of Lviv University of Business and Law*. 2018. № 19. С. 174–178.

45. Ткачук Н. А. Досвід США зі створення та розбудови кіберкомандування: уроки для України. *Інтернаука*. 2023. № 11 (69). С. 69–77.

46. Алямкін Р. В., Федорін М. П. Правове забезпечення національної інформаційної безпеки. *Наукові записки Інституту законодавства Верховної*

Ради України. 2013. № 4. С. 91–96. URL: http://nbuv.gov.ua/UJRN/Nzizvru_2013_4_19 (дата звернення: 28.11.2024).

47. Шемчук В.В. Зарубіжний досвід забезпечення інформаційної безпеки держави. *Порівняльно-аналітичне право*. 2019. № 2. С. 34–40.

48. Нормативно-правове забезпечення інформаційної безпеки Франції. URL: https://studlib.info/politologiya/19119-sistema-zabezpechennya-informaciynoyi-bezpeki-franciyi/ (дата звернення: 28.11.2024).

49. Фурсай О. Система забезпечення інформаційної безпеки Франції. *Вісник Львівського університету*. 2021. Вип. 34. С. 222–227.

50. Рябоконь О. Державна інформаційна політика формування інформаційного суспільства: зарубіжний досвід. *Наукові праці Національної бібліотеки України імені В. І. Вернадського*. 2016. Вип. 43. С. 97–114.

51. Тронько О. В. Зарубіжний досвід правового регулювання інформаційної політики. *Право і суспільство*. 2017. № 5(2). С. 140–145.

52. Шевченко А. Є, Павлюх О. А., Санжарова Г. Ф. Національна правова база Германії в галузі кібербезпеки. *International scientific conference*. 2023. С. 39–41.

53. Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) vom 17. Juli 2015. URL: https://www.bsi.bund.de/DE/Das-BSI/Auftrag/Gesetze-und-Verordnungen/IT-SiG/1-0/it_sig-1-0.html (дата звернення: 28.11.2024).

54. Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritisverordnung – BSI-KritisV) vom 22. April 2016. URL: https://www.gesetze-im-internet.de/bsi-kritisv/BJNR095800016.html (дата звернення: 28.11.2024).

55. Zweites Gesetz zur Erhohung der Sicherheit informationstechnischer Systeme vom 18. Mai 2021. URL: https://www.bmi.bund.de/SharedDocs/downloads/DE/gesetzestexte/it-sicherheitsgesetz-2.html (дата звернення: 28.11.2024).

56. Чалапко В. В. Інформаційна безпека: до проблеми місця й ролі в системі національної безпеки. *Вісник Національного юридичного університету імені Ярослава Мудрого*. 2021. № 4 (51). С. 83–95.

57. Войціховський А. В. Інформаційна безпека як складова системи національної безпеки. *Вісник Харківського національного університету імені В.Н. Каразіна*. 2020. Вип. 29. С.281–288.

58. Шевчук М. О. До питання генези поняття інформаційної безпеки як складової національної безпеки. *Науковий вісник Ужгородського національного університету*. 2023. Вип. 78. С. 134–139.

59. Кравченко О. І. Інформаційна безпека як складова національної безпеки. *Інвестиції: практика та досвід*. 2023. № 18. С. 229-234.

60. Жарикова А. Кількість кібератак у 2023 році зросла на 16% – Держспецзв'язку. 2024. URL: https://www.epravda.com.ua/news/ 2024/01/31/709355/ (дата звернення: 28.11.2024).

61. Про державну службу: Закон України від 10.12.2015 р. № 889-VIII. URL: https://zakon.rada.gov.ua/laws/show/889-19#Text (дата звернення: 28.11.2024).

62. Про затвердження Положення про систему професійного навчання державних службовців, голів місцевих державних адміністрацій, їх перших заступників та заступників, посадових осіб місцевого самоврядування та депутатів місцевих рад: Постанова Кабінету Міністрів України від 06.02.2019 р. № 106. URL: https://zakon.rada.gov.ua/laws/show/106-2019-п#Text (дата звернення: 28.11.2024).

63. Співак М. В., Дубіна О. М. Цифрові компетентності державних службовців в умовах розвитку цифрового суспільства і виникнення кіберзагроз. *Київський часопис права*. 2024. Вип. 3. С. 184–191.

64. Куйбіда В. С., Петроє О. М., Федулова Л. І., Андрощук Г. О. Цифрові компетенції як умова формування якості людського капіталу: аналіт. зап. Київ : НАДУ. 2019. 28 с.

65. Олешко А. А., Гороховець Є. В. Інформаційно-комунікаційні технології та людський розвиток. *Інвестиції: практика та досвід*. 2019. № 16. С. 16–19.

66. Копняк К. В., Покиньчереда В. В. Формування цифрової компетентності державних службовців у процесі фахової підготовки. *Державне управління: удосконалення та розвиток*. 2021. № 10. URL: http://www.dy.nayka.com.ua/?op=1&z=2261 (дата звернення: 28.11.2024).

67. The OECD Framework for digital talent and skills in the public sector. *OECD Working Papers on Public Governance*. 2021. № 45. 78 p. URL: https://www.oecd.org/en/publications/the-oecd-framework-for-digital-talent-and-skills-in-the-public-sector_4e7c3f58-en.html (дата звернення: 28.11.2024).

68. Чубаєвський, В. І., Е. Ю. Терешенко Особливості моніторингу оцінки інформаційної безпеки України. *Інформаційно-аналітичне забезпечення управління фінансово-економічною безпекою держави, регіону, суб'єктів господарювання в умовах COVID-19 :* матеріали X міжн. наук.-практ. конф. м. Харків, 18–19 листопада 2021 р. С. 294–297.