МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Харківський національний університет імені В. Н. Каразіна
Бахмутський навчально-науковий професійно-педагогічний інститут
Кафедра економіки підприємств та менеджменту

До захисту допущено
Завідувач кафедри
(підпис) Ганна МИХАЛЬЧЕНКО (ім'я, прізвище)
«09» грудня 2024 року

КВАЛІФІКАЦІЙНА РОБОТА (ПРОЄКТ)

рівень вищої освіти другий (магістерський)

спеціальність 281 Публічне управління та адміністрування

освітньо-професійна програма Публічне управління та адміністрування

тема «Цифрові технології у публічному управлінні в секторі національної безпеки України»

Виконав(ла)

здобувач(ка) групи БЗ-Пу23мг
(шифр групи)

Олександр СТОКОЛОС (підпис)
(ім'я, прізвище)

Керівник роботи
к.е.н. Юлія РОМАНУША (підпис)
(науковий ступінь, вчене звання, ім'я, прізвище)

Рецензент роботи
к.е.н. доц. Марина ПЕТЧЕНКО (підпис)
(науковий ступінь, вчене звання, ім'я, прізвище)

Консультант
(науковий ступінь, вчене звання, ім'я, прізвище) (підпис)

Засвідчую, що у цій роботі немає цитат та вилучень з праць інших авторів без відповідних посилань
здобувач (ка) (підпис)

Харків – 2024

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Харківський національний університет імені В. Н. Каразіна

Факультет/ННІ Бахмутський навчально-науковий професійно-педагогічний інститут

Кафедра Економіки підприємств та менеджменту

Рівень вищої освіти другий (магістерський)

Спеціальність 281 Публічне управління та адміністрування

Освітньо-професійна програма Публічне управління та адміністрування

ЗАТВЕРДЖУЮ

Завідувач кафедри

_____ Ганна МИХАЛЬЧЕНКО

(підпис) (ім'я, прізвище)

«09» грудня 2024 року

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ (ПРОЄКТ)

Стоколос Олександр Євгенович

(прізвище, ім'я, по батькові здобувача)

1. Тема роботи Цифрові технології у публічному управлінні в секторі національної безпеки України

керівник роботи Романуша Юлія Володимирівна, к. е. н.

(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом по університету від «08» жовтня 2024 року № 5101-5/3232

2. Строк подання здобувачем роботи «02» грудня 2024 р.

3. Перелік питань, які потрібно розробити: Концептуальні засади використання цифрових технологій у публічному управлінні в секторі національної безпеки. Аналіз стану використання цифрових технологій у секторі національної безпеки України. Напрями удосконалення використання цифрових технологій у публічному управлінні в секторі національної безпеки України

4. План роботи

№ з/п	Назви етапів роботи
1	Огляд літературних джерел, нових розробок, опублікованих даних та іншої інформації, пов'язаної з темою роботи
2	Обґрунтування теоретичної бази обраної проблеми
3	Розробка напрямів удосконалення застосування цифрових технологій у сфері публічного управління національною безпекою
4	Оформлення першого варіанту тексту, подання його на ознайомлення науковому керівнику
5	Усунення недоліків, написання остаточного варіанту тексту, оформлення дипломної роботи
6	Подання роботи на кафедру, перевірка на плагіат та зовнішнє рецензування роботи
7	Захист дипломної роботи у ЕК

5. Дата видачі завдання «08» жовтня 2024 р.

Здобувач(ка) _____ Олександр СТОКОЛОС
(підпис) (ім'я, прізвище)

Керівник роботи _____ Юлія РОМАНУША
(підпис) (ім'я, прізвище)

РЕФЕРАТ

Тема кваліфікаційної роботи: «Цифрові технології у публічному управлінні в секторі національної безпеки України».

Дипломна робота містить: 99 сторінок, 20 таблиць, 6 рисунків та 76 джерел.

Об'єктом дослідження є процес використання цифрових технологій у сфері публічного управління сектором національної безпеки України.

Предметом дослідження кваліфікаційної роботи є теоретичні та організаційні положення формування та реалізації механізмів цифровізації сфери публічного управління сектором національної безпеки України.

Мета кваліфікаційної роботи полягає у дослідженні стратегічних підходів, сучасних викликів та перспектив впровадження цифрових технологій у сферу публічного управління сектором національної безпеки України та розробка пропозицій щодо їх оптимізації.

Для виконання цієї мети виконано такі завдання: охарактеризовано та обґрунтовано концептуальні засади цифровізації сфери публічного управління сектором національної безпеки; проаналізовано сучасний стан використання цифрових технологій у секторі національної безпеки України; досліджено міжнародний досвід цифровізації у сфері національної безпеки та визначено можливості його адаптації до українських реалій; запропоновано напрями вдосконалення цифрових технологій у публічному управлінні сектором національної безпеки України.

КЛЮЧОВІ СЛОВА: ЦИФРОВІ ТЕХНОЛОГІЇ, ПУБЛІЧНЕ УПРАВЛІННЯ, НАЦІОНАЛЬНА БЕЗПЕКА, КІБЕРБЕЗПЕКА, ЦИФРОВІЗАЦІЯ УПРАВЛІННЯ

ABSTRACT

Graduation work on the theme: «Digital technologies in public administration in Ukraine's national security sector».

Graduation work contains: 99 pages, 20 tables, 6 figures, 76 references.

The object of the research is the process of utilizing digital technologies in the public administration of Ukraine's national security sector.

The subject of the research of the theoretical and organizational provisions for the development and implementation of digitalization mechanisms in the public administration of the national security sector in Ukraine.

The purpose of the thesis is to investigate strategic approaches, contemporary challenges, and prospects for implementing digital technologies in the public administration of Ukraine's national security sector and to develop proposals for their optimization.

To accomplish this goal, the following tasks have been accomplished: the study outlines and substantiates the conceptual foundations of digitalization in public administration within the national security sector, analyzes the current state of digital technologies in Ukraine's national security, examines international experiences in digitalization, and identifies possibilities for adapting them to Ukrainian realities. Additionally, it proposes directions for improving digital technologies in public administration related to national security.

KEYWORDS: DIGITAL TECHNOLOGIES, PUBLIC ADMINISTRATION, NATIONAL SECURITY, CYBERSECURITY, MANAGEMENT DIGITALIZATION

ЗМІСТ

ВСТУП

Актуальність. У сучасних умовах повномасштабного військового вторгнення російської федерації на територію України та постійному підвищенні рівня кіберзагроз, - питання забезпечення національної безпеки набуває особливого значення. Глобальні процеси цифровізації охоплюють усі сфери суспільного життя, зокрема безпекову. Їх роль у зміцненні державного суверенітету, координації міжвідомчої взаємодії та оптимізації управлінських процесів важко переоцінити. Цифрові технології відкривають нові можливості для підвищення ефективності управління шляхом впровадження систем автоматизації, великих даних (Big Data), штучного інтелекту, блокчейн-технологій та геоінформаційних систем. Водночас цифровізація сприяє зміцненню прозорості, підзвітності органів державної влади та інтеграції України у глобальний цифровий простір. Це дозволяє швидше реагувати на внутрішні й зовнішні загрози, прогнозувати їх розвиток і підвищувати ефективність управлінських рішень. У цьому контексті сектор національної безпеки України є не лише одним із головних напрямків цифрової трансформації, а також виступає стратегічним елементом державної політики у відповідь на гібридні загрози сучасності. Це обумовлює наукову та практичну цінність обраного напряму дослідження.

Об'єктом дослідження є процес використання цифрових технологій у сфері публічного управління сектором національної безпеки України.

Предметом дослідження кваліфікаційної роботи є теоретичні та організаційні положення формування та реалізації механізмів цифровізації сфери публічного управління сектором національної безпеки України.

Мета кваліфікаційної роботи полягає у дослідженні стратегічних підходів, сучасних викликів та перспектив впровадження цифрових технологій у сферу публічного управління сектором національної безпеки України та розробка пропозицій щодо їх оптимізації.

Завданнями кваліфікаційної роботи є:

- охарактеризувати та обґрунтувати концептуальні засади цифровізації сфери публічного управління сектором національної безпеки;

- проаналізувати сучасний стан використання цифрових технологій у секторі національної безпеки України;

- дослідити міжнародний досвід цифровізації у сфері національної безпеки та визначити можливості його адаптації до українських реалій;

- сформулювати напрями вдосконалення цифрових технологій у публічному управлінні сектором національної безпеки України.

Методи дослідження: для реалізації мети та завдань дослідження використовувався комплекс методів, серед яких слід виділити: системно-аналітичний (аналіз наукової літератури, визначення об'єкта і предмета дослідження); порівняльний (дослідження понятійно-категоріального апарату, співвідношення понять); формально-логічний (визначення класифікаційних ознак цифрових технологій, які використовуються у сфері публічного управління національною безпекою); метод математично-статистичної та графічної обробки даних (під час визначення кількісних показників, що знайшли відображення у таблицях).

Інформаційна база: законодавчі акти України, методичні положення, статистичні дані та аналітичні відомості Міністерства цифрової трансформації, Служби безпеки України, Державного центру кіберзахисту та протидії кіберзагрозам CERT-UA, наукові праці українських і зарубіжних учених та інтернет-джерела.

Перспективи використання результатів дослідження. Висновки і матеріали кваліфікаційної роботи можуть бути використані при розробці рекомендацій щодо цифровізації сфери публічного управління в секторі національної безпеки.

Результати роботи обговорювались і були апробовані на VIII Міжнародній науково-практичній конференції здобувачів вищої освіти та молодих учених «Студенти та молодь – для майбутнього країни» (14-15 листопада 2024 р., м. Бахмут-Харків) на тему «Цифрові технології як інструмент забезпечення національної безпеки: міжнародний досвід і перспективи для України».

РОЗДІЛ 1
КОНЦЕПТУАЛЬНІ ЗАСАДИ ВИКОРИСТАННЯ ЦИФРОВИХ ТЕХНОЛОГІЙ У ПУБЛІЧНОМУ УПРАВЛІННІ В СЕКТОРІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

1.1. Визначення сутності, основних характеристик та класифікаційних ознак цифрових технологій

Цифрові технології стають невід'ємною складовою сучасних систем управління, включаючи сферу національної безпеки. У державних структурах, відповідальних за безпеку, цифрові рішення дозволяють підвищити ефективність управління, оптимізувати процеси та покращити взаємодію між різними відомствами. Впровадження таких технологій у публічне управління сектором національної безпеки України стає особливо актуальним в умовах поточних військових конфліктів і загроз.

Цифрові технології – це широкий набір інструментів та рішень, що використовуються для збору, обробки та аналізу даних за допомогою комп'ютерних систем і мереж. У сфері національної безпеки такі технології застосовуються для захисту державних інтересів, координації дій між відомствами, моніторингу ризиків та оперативного реагування на загрози.

Цифрові технології є фундаментальною складовою модернізації публічного управління в умовах глобалізації, особливо у сфері національної безпеки. Вони охоплюють широкий спектр засобів, включаючи інформаційні системи, програмне забезпечення, хмарні сервіси, технології штучного інтелекту (AI), блокчейн та Інтернет речей (IoT). Їх основна мета — автоматизація управлінських процесів, підвищення ефективності комунікації, швидкості аналізу та забезпечення прозорості управлінських рішень.

У сучасному світі цифровізація стає невід'ємною складовою стратегій національної безпеки. В основі поняття «цифровізація» лежить поняття

«цифрові технології», дослідженою сутності та визначенню класифікаційних ознак яких присвятили свої праці як вітчизняні та закордонні дослідники, основні підходи яких представлено у табл. 1.1.

Таблиця 1.1

Узагальнення підходів вітчизняних та закордонних науковців до визначення сутності поняття «цифрові технології»

Автор, джерело	Науковий підхід до розуміння сутності
Биков В. Ю. [1]	Цифрові технології - сукупність методів і засобів, що забезпечують обробку, зберігання та передачу інформації в цифровій формі, сприяючи розвитку інформаційного суспільства.
Жалдак М. І. [2]	Цифрові технології охоплюють комп'ютерні та телекомунікаційні засоби, які забезпечують автоматизацію інформаційних процесів у різних сферах діяльності.
Спірін О. М. [3]	Трактує цифрові технології як інструменти, що забезпечують ефективну обробку та передачу інформації, сприяючи підвищенню продуктивності та якості в освітньому процесі.
Фамілярська Л. [4]	Узагальнює підходи науковців до визначення цифрових технологій, підкреслюючи їх роль у формуванні інформаційного освітнього середовища.
Васильєва Т. А. [5]	Розглядає цифрові технології як інструменти, що забезпечують інноваційну освітню діяльність та стимулюють трансфер знань у реальний сектор економіки.
Литвинова С. [6]	Підкреслює, що цифрові технології є потужним засобом отримання, оброблення, передання, аналізу та інтерпретації різноманітної інформації, особливо в освітньому процесі.
Гончарова О. [7]	Зазначає, що цифрові технології відіграють усе більшу роль в освіті, сприяючи забезпеченню її доступності та відкритості, підвищенню якості навчання.
Сухонос В. [8]	Розглядає цифрові технології як інструменти, що дозволяють інтенсифікувати освітній процес, зробити його мобільним, диференційованим та індивідуальним.
Мельник О. [9]	Підкреслює, що цифрові технології дозволяють педагогам модернізувати цілі, зміст, методи, засоби й організаційні форми навчання.
Гевко І. В. [10]	Зазначає, що використання сучасних інформаційних технологій є основою професійного зростання педагога та підвищення якості освіти.
Берназюк О.О. [11]	«Цифрові технології у публічному управлінні – це єдина система взаємопов'язаних засобів та прийомів, за допомогою яких здійснюється збір, обробка, фіксація, зберігання вхідної, а також формування та поширення вихідної інформації особливим – цифровим способом, організована на всіх рівнях та у всіх сферах публічного управління, яка дозволяє підвищити ефективність публічного управління, автоматизувати деякі його процеси».

Джерело: узагальнено на підставі [1-11]

Узагальнюючи дані табл. 1.1, зроблено висновок, що цифрові технології є універсальним інструментом, застосування якого активно досліджується в освітній, управлінській, інформаційній та безпековій сферах, з метою оптимізації процесів, підвищення їх ефективності й забезпечення сталого розвитку. Так, багато дослідників акцентують увагу на впровадженні цифрових технологій для підвищення доступності та якості освітнього процесу, оскільки вони допомагають автоматизувати навчання, створювати інтерактивні середовища, стимулювати інноваційну діяльність у цій галузі. Також наголошується на важливості цифрових технологій у автоматизації управлінських процесів, покращенні прозорості та ефективності прийняття рішень, оскільки вони забезпечують інтеграцію інформаційних систем, збору й аналізу даних, що є важливою здатністю для державного управління та національної безпеки. Науковці підкреслюють стратегічну роль цифрових технологій у створенні інтегрованих інформаційних платформ для обробки, передачі та аналізу великих обсягів даних. Дослідники також підкреслюють стратегічне значення цифрових технологій у забезпеченні кібербезпеки, управлінні кризовими ситуаціями, а також під час моніторингу загроз. У соціальній сфері цифрові технології розглядаються як інструмент інтеграції та модернізації соціальних процесів дія яких спрямована на покращення комунікації між різними групами суспільства.

Отже, як зазначають дослідники, цифрові технології забезпечують не тільки оперативність і точність управлінських процесів, але й дозволяють зміцнити довіру громадян до державних інституцій завдяки прозорості й доступності інформації. У випадку України це є особливо важливим з огляду на актуальні виклики, пов’язані із зовнішньою агресією, кіберзагрозами та необхідністю мобілізації ресурсів.

Стратегічна роль цифрових технологій обумовлюється їх значущістю у впровадженні концепції «Smart Governance» (розумного врядування), яка є сучасним підходом до державного управління, що спрямований на ефективність, прозорість, інноваційність і орієнтованість на громадян. Вони

забезпечують нові способи взаємодії між державними органами, громадянами та бізнесом, завдяки чому публічне управління стає більш гнучким, інтегрованим та адаптивним. Так, на думку науковців, «Smart Governance» розглядається як основа для розумного, відкритого та партисипативного уряду, що відіграє ключову роль у розвитку розумних міст, розбудова яких сьогодні є дуже актуальним завданням в Україні [12].

Узагальнення основних напрямів, у яких цифрові технології сприяють впровадженню концепції «Smart Governance» наведено в табл. 1.2.

Таблиця 1.2

Напрями використання цифрових технологій при впровадженні концепції «Smart Governance»

Напрям	Характеристика напряму	Приклад використання
1	2	3
Цифровізація адміністративних процесів	Автоматизація управлінських процедур, з метою зменшення залежності від паперової бюрократії та скорочення часу на ухвалення рішень.	Використання цифрової платформи «Дія» в Україні, яка дозволяє громадянам отримувати послуги в режимі онлайн без черг і посередників.
Використання великих даних (Big Data)	Можливість аналізувати масиви інформації для виявлення ключових тенденцій, прогнозування потреб громадян і оцінювання ризиків.	У містах Європи великі дані використовуються для планування трафіку, зменшення заторів і оптимізації громадського транспорту
Прозорість і підзвітність держави	Цифрові технології сприяють відкритості даних і підвищенню довіри громадян до органів влади. Це реалізується через: - створення платформ відкритих даних, де громадяни можуть отримувати доступ до інформації про бюджет, видатки та результати діяльності державних установ; - використання блокчейн-технологій для забезпечення прозорості транзакцій і державних закупівель.	Естонія впровадила блокчейн у свою систему e-Residency, забезпечуючи прозорість і захищеність операцій
Інтерактивна взаємодія з громадянами	Розумне врядування передбачає постійну комунікацію з громадянами, використовуючи цифрові платформи для:	Впровадження в Україні платформи електронних петицій. Ця ініціатива дозволяє громадянам напряму

Продовження табл. 1.2.

1	2	3
	1. Проведення електронних опитувань, збору ідей і пропозицій щодо управлінських рішень; 2. Впровадження електронного голосування, як це реалізовано у Швейцарії та Естонії. 3. Надання громадянам доступу до послуг у режимі 24/7 через мобільні застосунки та онлайн-платформи.	звертатися до органів державної влади із пропозиціями, ініціативами або вимогами, зібравши необхідну кількість підписів.
Забезпечення безпеки та захисту даних	Цифрові технології підвищують рівень кіберзахисту, що є основою «Smart Governance». Це включає: 1. Використання кібербезпекових рішень для захисту персональних даних громадян і державних систем. 2. Моніторинг загроз у реальному часі за допомогою AI-технологій.	У Сингапурі використовується інтегрована система розумного моніторингу, яка прогнозує ризики на основі аналізу даних з камер, сенсорів і IoT-пристроїв.
Інновації в міському управлінні (Smart Cities)	У рамках «Smart Governance» цифрові технології активно використовуються для управління міськими ресурсами та інфраструктурою. Це включає: 1. Використання IoT для моніторингу та управління критичною інфраструктурою (вода, електроенергія, дороги). 2. Впровадження розумних систем енергозбереження, що дозволяють оптимізувати витрати ресурсів. 3. Автоматизовані системи безпеки в міському просторі (розпізнавання облич, аналіз поведінки).	У Барселоні завдяки IoT контролюються витрати енергії та управління відходами.
Розвиток державних і приватних партнерств (PPP)	Цифрові технології створюють платформу для ефективного співробітництва між державою, бізнесом і громадянським суспільством.	Одним із прикладів успішного впровадження державного і приватного партнерства є український проєкт «Цифрова країна», створений за участі Міністерства цифрової трансформації України у співпраці з Microsoft, Google, Visa та іншими.

Таким чином, використання цифрових технологій не лише забезпечує ефективність та прозорість державного управління, а також лежить в основі формування нового рівня взаємодії між владою, бізнесом і суспільством. Концепція «Smart Governance» дозволяє інтегрувати передові технології у повсякденну практику управління, роблячи його інноваційним, орієнтованим на громадян і стійким до викликів сучасності.

Різноманіття сфер застосування цифрових технологій та їх різнопланового функціонального призначення обумовили різноплановість у підходах науковців до визначення їх ознак класифікації.

Узагальнення поглядів науковців до визначення різних сфер застоування цифрових технологій дозволило виділити їх класифікаційні ознаки:

1. За функціональним призначенням:

- інформаційно-комунікаційні технології (ІКТ) - засоби, що забезпечують збір, обробку, зберігання та передачу інформації. До них належать комп'ютери, мережеве обладнання, програмне забезпечення тощо;

- технології автоматизації - системи, що автоматизують виробничі та управлінські процеси, такі як робототехніка, системи управління виробництвом;

- аналітичні технології - інструменти для аналізу великих обсягів даних, включаючи системи бізнес-аналітики та штучного інтелекту.

2. За рівнем інтеграції та взаємодії:

- окремі технології - самостійні рішення, що виконують специфічні функції;

- інтегровані системи - комплекси технологій, об'єднані для забезпечення комплексного підходу до вирішення завдань.

3. За галузевим застосуванням:

- освітні технології - інструменти для підтримки та вдосконалення навчального процесу, такі як електронні підручники, платформи дистанційного навчання;

- медичні технології - системи для діагностики, лікування та управління медичними даними;

- фінансові технології (FinTech) - рішення для автоматизації та оптимізації фінансових послуг, включаючи онлайн-банкінг, мобільні платежі.

4. За ступенем інноваційності:

- традиційні технології - використовуються протягом тривалого часу та є стандартом у певній сфері;

- інноваційні технології - нові розробки, що пропонують покращені або принципово нові способи вирішення завдань.

5. За способом взаємодії з користувачем:

- інтерфейсні технології - засоби, що забезпечують взаємодію користувача з системою, такі як графічні інтерфейси, голосові помічники;

- фонові технології - працюють без прямої взаємодії з користувачем, наприклад, серверні обчислення, хмарні сервіси.

Отже, узагальнення підходів науковців до класифікації цифрових технологій дозволяє систематизувати їх види у відповідоності до різних сфер використання.

Розкриваючи мету дослідження, варто розглянути класифікацію цифрових технологій саме у сфері публічного управління національною безпекою, узагальнення якої наведено на рис.1.1.

Таким чином, рис.1.1. комплексно демонструє системний підхід до класифікації цифрових технологій, охоплюючи їхнє функціональне призначення, галузеву спеціалізацію, рівень інтеграції та інноваційність. Так, за галузевим застосуванням цифрові технології орієнтуються на управління безпекою, включаючи моніторинг, прогнозування ризиків та управління кризами. Це вказує на їх спеціалізовану спрямованість для вирішення загроз та координації дій у секторі національної безпеки. Інформаційно-аналітичні, (спрямовані на обробку даних і підтримку прийняття рішень), управлінські, (для забезпечення координації між органами влади), операційні (орієнтовані на автоматизацію реагування на загрози у реальному часі), - визначення

цифрових технологій за функціональним призначенням. Використання на практиці запропонованої системи класифікації цифрових технологій дозволяє чітко структурувати їхнє використання у сфері національної безпеки, підкреслюючи важливість адаптації як новітніх, так і традиційних рішень для управління загрозами.

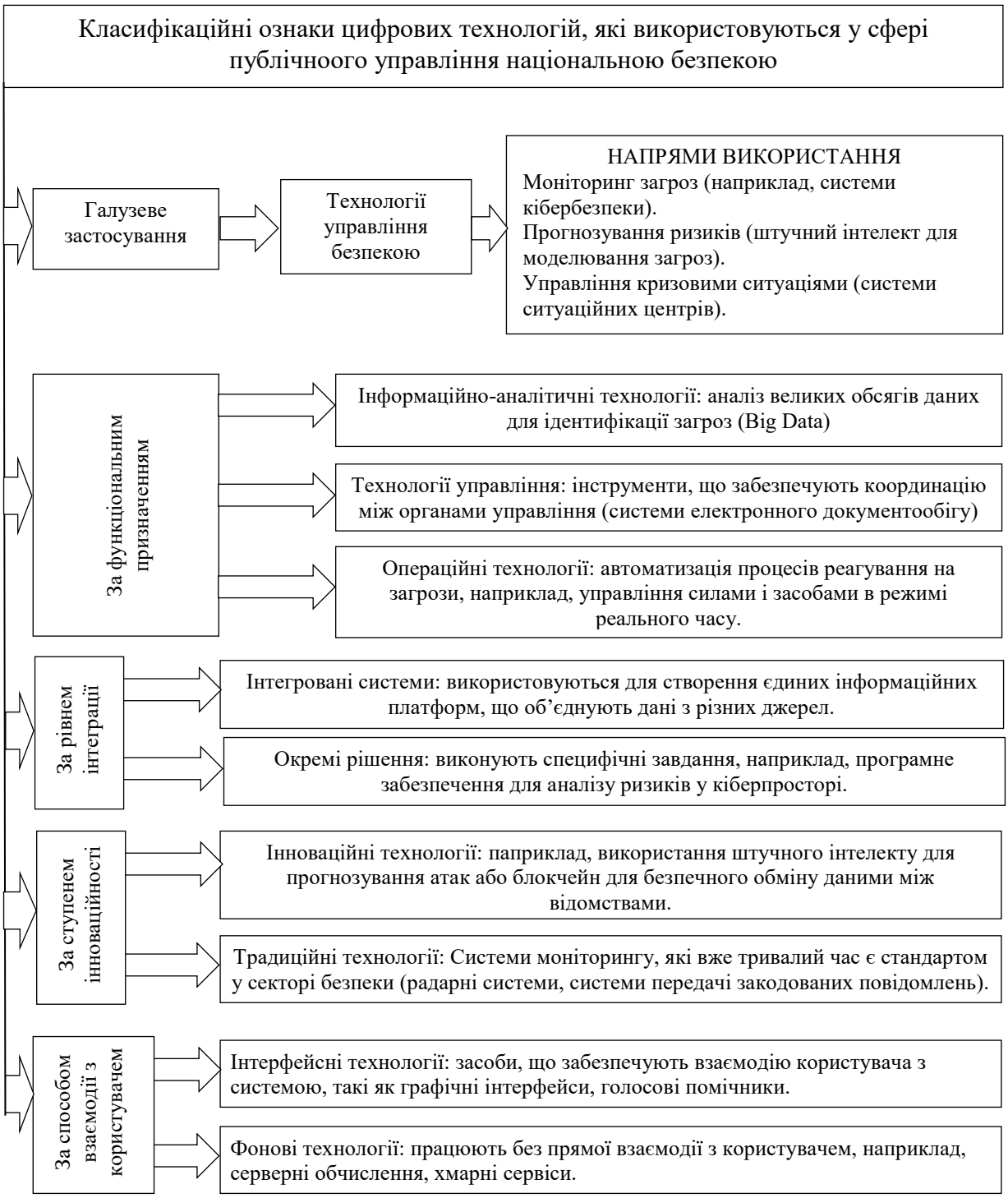

Рис. 1.1. Класифікаційні ознаки цифрових технологій, які використовуються у сфері публічного управління національною безпекою

Впровадження цифрових технологій у публічному управлінні національною безпекою України включає кілька ключових напрямків:

1. *Системи кібербезпеки*. Однією з головних задач цифровізації сектору національної безпеки є захист від кібератак. Україна постійно зазнає кібератак, спрямованих на державні установи, енергетичну інфраструктуру, банки та інші критичні об'єкти. Використання сучасних технологій, таких як аналітика великих даних, інструменти штучного інтелекту та автоматизації виявлення загроз, є основою для посилення кіберзахисту держави.

2. *Інформаційні системи* та управління даними. Оперативна обробка великих масивів даних стає важливим елементом для виявлення ризиків та своєчасного реагування на загрози. У цьому контексті технології Big Data допомагають аналізувати дані з різних джерел, наприклад, з соціальних медіа, щоб прогнозувати потенційні кризи та загрози.

3. *Автоматизовані системи управління (АСУ)*. У сфері оборони та національної безпеки автоматизовані системи управління допомагають ефективніше координувати дії військових та урядових відомств. Цифрові системи забезпечують швидший обмін інформацією між підрозділами, що особливо важливо в умовах військових операцій або кризових ситуацій.

4. *Геоінформаційні системи (ГІС).* ГІС використовуються для моніторингу та оцінки загроз в реальному часі. Наприклад, ці системи можуть забезпечувати картографічну підтримку для військових операцій або координації дій під час надзвичайних ситуацій, таких як стихійні лиха.

5. *Штучний інтелект (ШІ) та машинне навчання.* Використання ШІ в секторі безпеки включає автоматизоване виявлення загроз, прогнозування розвитку кризових ситуацій та підвищення ефективності аналізу великих масивів інформації. У сфері національної безпеки це допомагає розробляти ефективні стратегії для протидії сучасним загрозам.

Таким чином, цифрові технології є невід'ємною складовою публічного управління, особливо у сфері національної безпеки. Вони сприяють модернізації процесів, підвищенню прозорості та ефективності управлінських рішень.

1.2. Теоретичні основи цифровізації сфери публічного управління

Цифровізація сфери публічного управління є невіддільною складовою трансформаційних процесів сучасного суспільства. Її теоретичні основи формуються на перетині концепцій електронного урядування (e-government), цифрового врядування (digital governance) та цифрової трансформації (digital transformation). В основі цих підходів лежить прагнення підвищити ефективність, прозорість і підзвітність державного управління за допомогою цифрових технологій.

Електронне урядування є початковою точкою цифровізації публічного управління. Його головна мета — забезпечити доступ громадян до державних послуг через використання інформаційно-комунікаційних технологій (ІКТ). У дослідженні [13], електронне урядування — це управлінська модель, яка сприяє трансформації традиційних адміністративних процесів у цифровий формат, зменшуючи вплив бюрократичних бар'єрів та пришвидшуючи обмін інформацією.

У світовій практиці прикладами успішного електронного урядування є естонська система e-Estonia, яка дозволяє громадянам виконувати більшість державних послуг онлайн, та система GovTech у Сінгапурі, що включає інтегровані платформи для управління містами та безпекою. В Україні впровадження застосунку «Дія» стало ключовим кроком у розвитку електронного урядування, забезпечивши громадянам доступ до понад 70 державних послуг [11].

На думку Мохової Ю.Л., «електронне урядування (е-урядування) є ключовим елементом ефективної урядової діяльності та сучасного демократичного суспільства, який забезпечує вільний та оперативний доступ населення до інформації та відкритого діалогу між державою та громадськістю за допомогою застосування інформаційних технологій [14]».

Дослідження джерел літератури свідчить також про різні наукові підходи до визначення поняття електронного урядування. Так, в соціальних

науках поняття «governance» з'явилося вперше у 1937 р. у статті американського економіста Роналда Коуза «The nature of the firm» [15]. Він пов'язував його з менеджментом в комерційній діяльності або діяльністю неурядових організацій, погодженням політик, процесів, а також з правом прийняття рішень у сфері своєї компетенції. Різноманітність підходів науковців до визначення сутнісних ознак поняття «електронне урядування» пояснюється багатьма чинниками, узагальнені погляди вітчизняних та зарубіжних науковців у дослідженні цього питання наведено в табл. 1.3.

Таблиця 1.3

Підходи вітчизняних та зарубіжних науковців до розуміння терміну «електронне урядування»

Автор, джерело	Визначення
Antiroikko A. [16]	Координація і використання різних форм формальної і неформальної взаємодії і інституційних перетворень у формуванні державної політики, стратегії розвитку держави і розвитку процесів, які покращують сервісні функції держави, з метою реалізації потреб колективного інтересу сторін, що взаємодіють з державою.
Yong J. [17]	Використання ІКТ державою з метою розширити доступ і поліпшити якість послуг, що надаються партнерам по взаємодії: громадянам, представникам бізнесу, державним службовцям. Цей підхід передбачає також «зворотній зв'язок» громадян з державою, за допомогою якого громадяни висловлюють свою думку про якість державних послуг.
Демкова М., Фігель М. [18]	Спосіб організації державної влади за допомогою систем локальних інформаційних мереж та сегментація глобальної інформаційної мережі, яка забезпечує функціонування певних служб в режимі реального часу та робить максимально простим і доступним щоденне спілкування громадянина з офіційними установами.
Почепцов Г. [19]	Це не просто система надання державою та її органами послуг (у тому числі й відповідної інформації) громадянам на основі їх активної взаємодії за допомогою сучасних інформаційних і комунікаційних технологій, а й передусім модернізація самого процесу державного управління відповідно до нових умов суспільного розвитку
Спасібов Д. [20]	Форма організації публічного управління, що сприяє підвищенню ефективності, відкритості та прозорості діяльності органів державної влади та органів місцевого самоврядування з використанням ІКТ для формування нового типу держави, орієнтованої на задоволення потреб громадян.
Чукут С. [21]	Модернізація всієї системи державного управління, яка охоплює як надання якісних послуг для громадян і бізнесу, так і налагодження новітніх комунікативних каналів між владою і громадянським суспільством, реінжиніринг всієї державної служби

Джерело: узагальнено на підставі [16-21]

Отже, аналіз теоретичного досвіду розуміння поняття «електронне урядування» дозволив виокремити найбільш поширені його варіанти визначення:

1) як форма організації державного управління, яка з використанням інформаційно-комунікаційних технологій сприяє відкритості та прозорості функціонування органів державного управління, підвищенню їх ефективності зі спрямуванням на формування уряду, який у кінцевому розумінні орієнтується на задоволення потреб суспільства;

2) як система оптимізації процесу політичної участі громадян в програмах уряду з використанням мережі Інтернет та інших технічних засобів, шляхом зміни внутрішніх та зовнішніх відносин, а також надання адміністративних послуг населенню;

3) як система взаємодії громадськості з органами державного управління шляхом використанням ІКТ, спрямована на оптимізацію термінів надання якісних державних послуг, підвищення їх доступності, зниження адміністративного навантаження на організації та на громадян.

Таким чином, проведені теоретичні дослідження підтверджують відсутність єдності у поглядах науковців до визначення терміна «е-урядування». Різноманітність трактувань поняття «електронне урядування» пояснюється існуванням різних принципів, а також впливом чинників зовнішнього та внутрішнього середовища (існуюча форма державного управління, складність системи, бізнес-процеси, обрана концепція діяльності, етап автоматизації, сукупність методів управління, система міжвідомчої взаємодії, концепція підвищення ефективності та прозорості діяльності органів державної влади). Але, разом з тим, найбільш вживаним та доцільним визначенням е-урядування є розуміння його як системи, яка дає змогу бізнесу та громадськості брати широку участь у державному управлінні, що дозволяє підвищувати прозорість та ефективність функціонування органів державної влади на засадах розширення використання цифрових технологій.

Спираючись на розуміння сутності електронного урядування, можна

сказати, що воно більш за все асоціюється лише з державним управлінням, але, разом з тим, електронне урядування повинно включати в себе управління з боку органів місцевого самоврядування особливо в умовах децентралізації та деконцентрації публічної влади. Електронне урядування передбачає функціонування всіх рівнів у якості єдиної системи при їх електронній взаємодії [22, с. 68].

Здобутки досліджень науковців підтверджують існування низки типів (моделей) електронного урядування, найбільш поширеним є підхід Чжиюань Фан, яка визначила вісім моделей електронного уряду в залежності від типу взаємодії між зацікавленими сторонами [22].

Електронний уряд місцевого рівня може охоплювати від одного органу місцевого самоврядування чи органу місцевої виконавчої влади до цілого регіону.

Таким чином, електронне урядування будується на електронній взаємодії органів публічної влади з громадськістю, представниками секторів бізнесу та некомерційних або громадських організацій здійснюється шляхом залучення інформаційних представництв, на які покладені функції реєстрації звернень громадян і організацій та надання необхідної інформації для розв'язання поставлених проблем звернення.

Належну увагу визначення сутнісних ознак електронного урядування наведено у дослідженнях Мохової Ю.Л., яка визначає *метою е-урядування* розвиток електронної демократії задля «забезпечення прозорості влади для громадських організацій, бізнесу, суспільства, досягнення високих стандартів якості електронних державних послуг» [14, с. 47].

До основних *цілей е-урядування* доречно віднести:

1) економію адміністративних витрат та спрощення процедур;

2) підвищення доступності та якості державних послуг для бізнесу та суспільства;

3) забезпечення дієвого контролю за ефективністю та результативністю діяльності органів державної влади, підвищення якості управлінських

процесів;

4) забезпечення прозорості діяльності уряду, розширення електронного доступу громадян до процесу експертизи та підготовки проектів управлінських рішень [14, с. 47].

Теоретико-практичний базис функціонування е-урядування в державному управлінні формують його принципи, сукупність яких повинна враховуватися при розробці та впровадженню механізмів е-урядування в Україні.

Відповідно до того, що існує багато підходів у науці та практиці до визначення сутності е-урядування, разом з тим, відзначена також і різноманітність у розумінні системи принципів е-урядування. Так, у дослідженнях ОЕСР виділяються три ключові принципи е-урядування: відкритість уряду та залучення суспільства; комплексні підходи до розподілу соціальної цінності; отримання бажаного ефекту та прибутку від інвестування в ІКТ [23]. У загальній міжнародній практиці систематизовано наступні принципи розвитку е-урядування: принцип прозорості, системності, сумісності, стандартизації, ефективності, безпеки даних, єдиної інформаційної бази, адаптації, продуктивності системи та ін. [24].

Узагальнення принципів е-урядування з визначенням їх характеристики представлено у табл. 1.4.

Таблиця 1.4

Узагальнені принципи е-урядування [23, 24]

Принцип	Характеристика
1	2
За підходом ОЕСР	
Залучення суспільства і відкритість уряду	Перетворення ІКТ в основний елемент стратегії розвитку прозорості, відкритості та участі широких мас населення в управлінських процесах. ІКТ використовуються для широкого включення громадськості в процес участі суспільства у формуванні державної політики у всіх сферах життя. Залучення в сферу прийняття рішень і управління суспільством нових недержавних суб'єктів (індивідуальних і колективних), створення інформаційної культури в суспільстві, зміцнення суспільної довіри до рівня безпеки і захисту громадян від втручання в особисте життя.
Комплексні підходи до розподілу соціальної цінності	Прийняття і розвиток спільної урядової стратегії для комплексного застосування ІКТ, формулювання єдиного підходу до майбутньої моделі застосування ІКТ в управлінні державою. У формуванні стратегії повинні взяти участь представники від неурядових організацій, що представляють всіх членів суспільства.

Продовження табл. 1.4

1	2
Отримання бажаного ефекту від інвестування в ІКТ	Спрямована на отримання ефекту від інвестування в електронну державу. Має постійно відбуватися пошук нових можливостей залучення неурядового сектору в проекти впровадження ІКТ та мобілізації їх потенціалу.
У загальній міжнародній практиці	
Принцип максимального розкриття	Вся інформація, якою володіють публічні органи, підлягає розкриттю; винятки повинні бути максимально обмежені і публічні органи повинні довести виникнення та правомірність таких винятків.
Принципи е-урядування	Поєднують у собі технологічні принципи, якими слід керуватися, створюючи інформаційну систему «е-уряд».
Принцип системності	Передбачає встановлення між структурними елементами інформаційної системи зв'язків, для цілісності функціонування публічної адміністрації.
Принцип розвитку (відкритості)	Враховує можливість поповнення і оновлення функцій та складу інформаційної системи «Електронний уряд» без порушення її функціонування.
Принцип сумісності	Створенні системи мають бути реалізовані через інформаційні інтерфейси, завдяки яким вона може взаємодіяти з іншими системами згідно з установленими правилами (наприклад, з аналогічними системами країн Співдружності Незалежних держав та Європейського союзу (ЄС)).
Принцип стандартизації	Забезпечує стандартизацію інформаційної системи та її складових для мінімізації всіх видів витрат, уніфікації прийомів, методів та інструкцій, якими керується користувач при роботі з системою.
Принцип ефективності	Раціональне співвідношення між витратами на створення інформаційної системи «Електронний уряд» і цільовими ефектами, досягнутими завдяки її функціонуванню, причому вони можуть мати не тільки грошову форму, а й форму економії часу, підвищення якості та зручності адміністративних послуг.
Принцип нових завдань	Забезпечує врахування при визначенні переліку завдань, які доцільно включити до інформаційної системи, основних технологічних операцій оброблення документів та завдань, що випливають з потреби забезпечення повноти, вчасності й оптимальності прийняття державних рішень, які раніше не виконувалися через обмежені можливості оброблення інформації.
Принцип безпеки даних	Інформаційні ресурси мають бути надійно захищені і при їх безпосередній обробці та зберіганні в системі, і в момент обміну між комп'ютерами; потрібно виключити можливість несанкціонованого доступу до даних; всі операції в системі реєструються, будь-яке порушення системи безпеки виявляється.
Принцип єдиної інформаційної бази	Вимагає застосування єдиної системи класифікації та кодування одних і тих самих структурних одиниць державних інформаційних ресурсів.
Принцип продуктивності системи	Випливає із значної нерівномірності надходження потоків інформації, яку слід обробляти в певні проміжки часу, і жорстких вимог до термінів її оброблення.
Принцип адаптації	Придатність інформаційної системи до модифікації та розширення.

Отже, враховуючи світовий досвід у впровадженні е-урядування та виокремлення низки принципів, варто підкреслити їх стратегічну роль та

зазначити, що вони мають стати основою розробки усіх механізмів забезпечення розвитку та впровадження е-урядування в державі.

Спираючись на те, що кожен механізм містить у собі систему суб'єктів та об'єктів управління, має показники, за якими можна оцінити його функціонування, та інструменти та важелі досягнення поставлених цілей, варто зупинитися на аналізі інструментів електронного урядування, до яких у дослідженнях Мохової Ю.Л. відносяться наступні: інформаційно-аналітичне забезпечення прийняття управлінських рішень, автоматизація обробки великих об’ємів даних, автоматизація та оптимізація, впровадження електронних форм взаємодії, формування Інтернет-порталів, поширення е-демократії, доступ до відкритих даних та ін. Саме інструменти е-урядування здатні забезпечити значне покращення якості обслуговування юридичних та фізичних осіб, підвищити прозорість діяльності органів державної влади та довіру населення до них [14, 24].

Набутий досвід та практика свідчать, що врахування тенденцій минулого є ефективним та раціональним кроком при плануванні розвитку явищ на майбутнє. Отже, при пошуку способів стрімкого розвитку інформаційно-комунікаційних технологій в публічному секторі необхідно враховувати етапи розвитку електронного урядування з виокремленням етапів і порядку дій, необхідних для формування ідеальної моделі електронного уряду. Вирішення цього питання неможливе без вивчення результатів досліджень Департаменту з економічних і соціальних питань Організації Об'єднаних Націй, де запропоновано 5 етапів стану розвитку електронного урядування [25]:

1. *Початкова присутність (emerging presence)* – у країни може бути тільки один або кілька офіційних веб-сайтів національного уряду, які пропонують статистичну інформацію користувачеві і служать інструментами зв'язку з громадськістю;

2. *Просунута присутність (enhanced presence)* – число урядових веб-сторінок збільшується, користувачі мають більше можливостей для доступу

до інформації;

3. *Інтерактивна присутність (interactive presence)* – обмін між користувачами і постачальниками послуг стає більш симетрично розвиненим, форми документів можуть бути завантажені з сайтів, наявна можливість подати заяву онлайн;

4. *Транзакційна присутність (transactional presence)* – користувачі можуть легко отримати доступ до послуг, розташованих по групах в залежності від їх потреб, і здійснювати формальні угоди в режимі «онлайн», такі як оплата податків і оплата реєстраційних внесків;

5. *Мережева присутність (networked presence)* – повна інтеграція всіх онлайн державних послуг за допомогою універсального порталу за принципом «єдиного вікна».

Цифрове врядування розширює межі електронного урядування, акцентуючи увагу на активній взаємодії між державою та громадянами. Ця концепція включає використання цифрових платформ для залучення громадян до процесу прийняття рішень, підвищуючи прозорість управління. У дослідженні [26] цифрове врядування сприяє розвитку інноваційних моделей взаємодії між суспільством і державними інституціями, особливо в контексті розумних міст (Smart Cities), де використовуються штучний інтелект, IoT та великі дані для управління міськими ресурсами.

Україна також робить перші кроки в цьому напрямку: система електронних петицій дозволяє громадянам напряму звертатися до органів влади, впливаючи на формування політики. У світі яскравим прикладом є платформа MyGov у Великій Британії, яка об'єднує численні сервіси для громадян у єдину екосистему, забезпечуючи інтерактивну взаємодію.

Отже, розвиваючись в умовах цифровізації, постійне впровадження ІКТ в систему суспільно-політичних відносин дає змогу розширити можливості громадської участі, створити умови для формування якісно нового рівня активності та участі громадян, які користуються сучасними інформаційними технологіями не тільки в особистих цілях, а й в цілях

суспільно-політичної участі на місцевому рівні публічного управління. Електронну участь громадян в управлінні, у більш широкому розумінні прийнято називати електронною демократією, яка уособлює комплекс інструментів, в яких персональні комп'ютери, ноутбуки, смартфони та загальнодоступні мережі використовуються для розвитку і захисту основних демократичних цінностей, таких як розповсюдження інформації та комунікація, участь громадян в процесах прийняття рішень (шляхом нарад і голосувань), об'єднання інтересів громадян [27, с. 38].

Задля розвитку електронної демократії використовуються інтернет-технології, використання яких дозволяє проводити електронні консультації з громадянами та залучати їх до участі в електронних політичних форумах та виборах. З практичної точки зору, електронна участь громадян в урядуванні передбачає:

1. Електронне включення:

- електронне консультування – органи влади через Інтернет звертаються до громадян з метою отримання їхньої думки щодо вироблення відповідної політики чи обговорення рішень;

- електронна участь – активна участь громадян на основі підтримки зворотного зв'язку за допомогою сучасних інформаційно-комунікаційних технологій у процесі прийняття рішень і виробленні політики.

2. Електронне партнерство - поглиблений етап взаємодії громадян із владою, де відповідальність за прийняття рішень покладається на обидві сторони, передбачає внесок кожного у розвиток громадянського суспільства [27, с. 38].

Отже, для удосконалення публічного управління щодо розвитку електронного урядування необхідно обґрунтувати *цілі управління* та поставити конкретні *завдання*, які будуть релевантні певним умовам на конкретному етапі розвитку інформаційного суспільства.

Цифрова трансформація публічного управління — це процес глибоких змін у структурі, культурі та функціонуванні державних установ під впливом

цифрових технологій. Цей підхід вимагає інтеграції інноваційних технологій, таких як блокчейн, хмарні обчислення та штучний інтелект. Як зазначають дослідники [28], цифрова трансформація базується на трьох складових: технологічній (впровадження нових інструментів), організаційній (зміна бізнес-процесів) та культурній (підвищення цифрової грамотності держслужбовців).

У країнах ЄС цей процес підтримується через програму «Цифрова Європа», яка фінансує проєкти з розвитку цифрових навичок і впровадження технологій у державному управлінні. В Україні державна програма цифрової трансформації включає створення єдиного реєстру послуг, модернізацію інфраструктури кібербезпеки та запровадження електронних виборів.

Цифровізація публічного управління має численні переваги, зокрема підвищення ефективності, зниження адміністративних витрат, забезпечення доступності державних послуг та інтеграцію громадян у процеси управління. Проте ключовими викликами залишаються кібербезпека, низький рівень цифрової грамотності населення та брак фінансування на розробку і впровадження цифрових рішень.

Таким чином, теоретичні основи цифровізації сфери публічного управління охоплюють концепції електронного урядування, цифрового врядування та цифрової трансформації. Вони дозволяють модернізувати адміністративні процеси, зробити їх прозорими й ефективними, а також забезпечити залучення громадян до управлінських рішень.

1.3. Нормативно-правові засади цифровізації в секторі національної безпеки України

Цифровізація сектору національної безпеки України є невід’ємною складовою успішності сучасного публічного управління, основною метою якого є посилення безпеки та стійкості держави до зовнішніх і внутрішніх загроз. Важливість цього процесу визначається необхідністю адаптації до

глобальних викликів інформаційного середовища, кіберзагроз та технологічного розвитку. Нормативно-правові засади утворюють основу у напрямі впровадження цифрових технологій, забезпечуючи тим самим правову визначеність, координацію дій і формування відповідних механізмів.

Національна безпека є одним із стратегічних пріоритетів державної політики України. Публічне управління в цій сфері базується на нормативно-правових актах, які забезпечують координацію діяльності державних органів, правове регулювання впровадження сучасних підходів до управління, а також захист від зовнішніх і внутрішніх загроз. Це забезпечення включає закони, стратегії, укази Президента України, постанови Кабінету Міністрів України та інші нормативно-правові акти.

Узагальнення нормативно-правової бази, положень стратегій розвитку кібербезпеки та інших документів щодо регулювання питань цифровізації сетора національної безпеки представлено у табл. 1.5.

Таблиця 1.5

Нормативно правове та інформаційне забезпечення цифровізації в секторі національної безпеки України

Назва	Основний зміст
1	2
1. Базові закони про інформаційні технології та кібербезпеку	
Закон України «Про національну програму інформатизації» (втратив чинність) [29]	Став фундаментом для розвитку інформаційного суспільства в Україні, визначаючи механізми реалізації національної програми інформатизації. Основний акцент зроблено на створенні умов для інтеграції сучасних цифрових технологій у всі сфери суспільного життя.
Закон України «Про основні засади забезпечення кібербезпеки України» [30]	Регулює правові та організаційні засади забезпечення кібербезпеки. Він встановлює принципи захисту критичної інформаційної інфраструктури та визначає відповідальні органи, включаючи Державну службу спеціального зв'язку та захисту інформації України, СБУ та Міністерство цифрової трансформації.
Закон України «Про національну безпеку України» [31]	Є основним документом, який визначає засади державної політики у сфері національної безпеки та оборони. Він регулює принципи управління, включаючи демократичний цивільний контроль, координацію між відомствами, а також основи кібербезпеки та інформаційної безпеки. У статті 18 закону підкреслено роль цифровізації в національній безпеці, яка включає створення сучасних інформаційних систем для моніторингу загроз і оперативного реагування.

Продовження табл. 1.5

1	2
Закон України «Про оборону України» [32]	Цей закон регулює діяльність органів публічного управління в оборонній сфері. Він включає положення щодо мобілізаційної підготовки, координації дій силових структур та співпраці з іншими державними органами.
Закон України «Про Державну службу спеціального зв'язку та захисту інформації України» [33]	Визначає функції служби, яка відповідає за технічний захист інформації, створення та функціонування державних інформаційних систем, а також розвиток цифрових засобів комунікації в секторі безпеки.
2. Стратегії та укази Президента України	
Стратегія кібербезпеки України (2021-2025 рр.) [34]	Затверджена Указом Президента України від 26 серпня 2021 року № 447/2021, стратегія регулює розвиток системи кіберзахисту. Основними напрямами є: 1. Створення механізмів виявлення та реагування на кіберзагрози. 2. Підвищення рівня захищеності критичної інформаційної інфраструктури. 3. Впровадження стандартів кібербезпеки в державному управлінні.
Стратегія інформаційної безпеки (2021 р.) [35]	Ця стратегія визначає завдання щодо протидії інформаційним атакам, впровадження інформаційної стійкості держави та громадянського суспільства, а також розвитку цифрових інструментів для моніторингу та аналізу інформаційних загроз.
Доктрина інформаційної безпеки України (2017 р.) [36]	Документ акцентує увагу на необхідності протидії інформаційній агресії, зокрема в умовах гібридної війни. Важливе місце в доктрині займає впровадження сучасних технологій моніторингу та аналізу інформаційних потоків.
3. Нормативно-правове регулювання кібербезпеки та інформаційної безпеки	
Закон України «Про основні засади забезпечення кібербезпеки України» (2017 р.) [37]	Цей закон регулює: 1. Захист державних інформаційних ресурсів і критичної інфраструктури. 2. Координацію дій між Національним координаційним центром кібербезпеки, Держспецзв'язку, СБУ та іншими органами. 3. Впровадження міжнародних стандартів кібербезпеки в національне законодавство.
Постанова Кабінету Міністрів України № 373 «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» (2006 р.) [38]	Встановлює вимоги до організації технічного захисту інформації, що є критично важливим у національній безпеці.
Постанова Кабінету Міністрів України № 518 (2020 р.) «Про реалізацію експериментального проєкту з впровадження системи моніторингу кіберзагроз» [39]	Документ спрямований на розвиток інструментів моніторингу та реагування на кіберінциденти.

Джерело: узагальнено автором на підставі [29-38]

Таким чином, аналіз даних табл. 1.5 дозволяє надати оцінку основних нормативно-правових актів та стратегій, які забезпечують цифровізацію в

секторі національної безпеки України. Її чітка структуризація з розподілом на три основні категорії: базові закони, стратегії та укази Президента, а також нормативно-правові акти у сфері кібербезпеки та інформаційної безпеки дає змогу відобразити ключові аспекти цифровізації в державному управлінні. Так, базові закони утворюють фундамент для цифровізації та кібербезпеки. Зокрема, Закон «Про національну безпеку України» виділяє роль цифровізації у створенні інформаційних систем для моніторингу загроз. Водночас Закон «Про основні засади забезпечення кібербезпеки України» встановлює організаційні засади захисту критичної інформаційної інфраструктури, підкреслюючи координацію між відповідальними відомствами, такими як СБУ та Держспецзв'язку. Кожен із цих законів виконує специфічну роль у системі безпеки, доповнюючи один одного. Разом з тим, існуючі стратегії та укази Президента визначають загальні напрями та пріоритети державної політики. Так, «Стратегія кібербезпеки» акцентує увагу на стандартах захисту інформації, механізмах реагування на кіберзагрози та підвищенні захищеності критичної інфраструктури. Водночас, «Стратегія інформаційної безпеки орієнтована на протидію інформаційним атакам та розвиток інформаційної стійкості», Доктрина інформаційної безпеки додає аспект протидії інформаційній агресії, що є особливо актуальним у контексті гібридної війни. Ці стратегії формують рамки для конкретних практичних дій у сфері цифровізації. Нормативно-правове регулювання кібербезпеки забезпечується дією Постанови Кабінету Міністрів України № 373 (регулює захист інформації в телекомунікаційних системах), тоді як Постанова № 518 запроваджує експериментальні проєкти для моніторингу кіберзагроз. Ці акти є прикладом того, як держава впроваджує практичні рішення у сфері кібербезпеки, посилюючи технічну базу реагування на загрози.

Усі зазначені вище документи діють у єдиній системі взаємозв'язків та створюють правове підґрунтя для цифровізації в секторі національної безпеки.

Отже, як було зазначено вище, цифрова трансформація є пріоритетним напрямом розвитку сучасного державного управління. З цього виходить, що у контексті її розбудови в Україні обумовлюється необхідність регулювання цього процесу низкою стратегій і програм, які визначають ключові напрями інтеграції цифрових технологій у різні сфери суспільного життя.

При аналізі питання щодо нормативно-правового забезпечення діяльності публічного управління у сфері національної безпеки України, варто звернутися до видання «Правова база української кібербезпеки: загальний огляд і аналіз» [40]. Згідно наведених даних, можна виділити кілька ключових складових публічного управління у сфері національної безпеки України. Основні елементи включають нормативно-правове регулювання, координацію між державними органами, захист критичної інфраструктури та інтеграцію міжнародного досвіду.

Нормативно-правове регулювання є базовою складовою системи, що визначає рамки діяльності держави у сфері кібербезпеки. Це включає Закон України «Про основні засади забезпечення кібербезпеки України» [37], який закладає основи захисту критичної інформаційної інфраструктури, та Стратегію кібербезпеки [34], яка визначає пріоритети і стратегічні напрямки для розвитку цієї сфери. У документі наголошується на потребі вдосконалення законодавства, щоб ліквідувати термінологічні та процедурні розбіжності.

Координація між державними органами відіграє вирішальну роль у забезпеченні ефективного управління кібербезпекою. У документі [40] зазначено, що в Україні спостерігається дублювання повноважень між різними агенціями, такими як Державна служба спеціального зв’язку та захисту інформації, Служба безпеки України та інші структури. Це ускладнює оперативне реагування на кіберзагрози. Для вирішення цієї проблеми пропонується створення централізованого координаційного органу, який би об’єднував зусилля різних суб’єктів і забезпечував узгодженість їхніх дій [40].

Захист критичної інфраструктури є важливим аспектом публічного управління в цій сфері. У документі [40] підкреслюється, що критична інфраструктура потребує кращого нормативного регулювання. Відсутність підзаконних актів і механізмів аудиту значно знижує ефективність захисту таких об'єктів. Рекомендується розробка нових підходів до категоризації об'єктів інфраструктури, а також до впровадження спільних стандартів для їхнього захисту.

Інтеграція міжнародного досвіду є невіддільною частиною вдосконалення системи національної безпеки. Україна ратифікувала Будапештську конвенцію, частково впроваджує положення Директиви NIS та співпрацює з міжнародними організаціями. Водночас у документі [40] наголошено на необхідності посилення міжнародної взаємодії, особливо в аспектах обміну інформацією про кіберзагрози та кращі практики захисту.

Таким чином, публічне управління у сфері національної безпеки України базується на нормативно-правовій основі, міжвідомчій координації, захисті критичної інфраструктури та міжнародній співпраці. Подальший розвиток цієї системи вимагає комплексного підходу та врахування сучасних викликів у сфері кібербезпеки.

Отже, удосконалення системи публічного управління у сфері національної безпеки України слід базувати на аналізі нормативно-правових засад та актуальних викликів цифровізації. Основною передумовою успішного розвитку є цілісна нормативна база, яка визначає ключові напрями діяльності. Зокрема, такі документи, як Закон України «Про основні засади забезпечення кібербезпеки України» та Стратегія кібербезпеки України, задають правову рамку для регулювання, захисту критичної інфраструктури, а також координації між органами публічного управління.

Ключовими елементами управління національною безпекою є чіткий розподіл повноважень між державними органами, координація їхніх дій та створення спеціалізованих механізмів захисту. Важливою складовою також є

інтеграція міжнародного досвіду, який сприяє підвищенню ефективності управління, розробці та впровадженню сучасних стандартів кібербезпеки.

Разом з тим, необхідно приділяти увагу захисту критичної інформаційної інфраструктури, яка відіграє стратегічну роль у забезпеченні стабільності держави. Аналіз чинних нормативно-правових актів підтвердив наявність необхідності їх модернізації для усунення розбіжностей та врахування технологічних змін. Крім того, впровадження практик міжнародної взаємодії сприяє покращенню готовності України до протидії сучасним загрозам.

Отже, успішність публічного управління у сфері національної безпеки залежить від комплексності підходу, координації між відомствами, удосконалення правового забезпечення та використання передових цифрових технологій. Такий підхід дозволить створити ефективну систему кіберзахисту, здатну відповідати викликам сучасного світу.

Аналіз перспективних напрямів досліджень поставленої проблеми мають значний потенціал, оскільки сфера публічного управління національною безпекою потребує постійного вдосконалення через динамічний розвиток технологій, зміну геополітичної ситуації та зростання кіберзагроз. Основними перспективами подальших досліджень є удосконалення нормативно-правової бази, інтеграція інноваційних цифрових рішень, аналіз міжнародного досвіду та розвиток кадрового потенціалу.

Перш за все, важливим є дослідження шляхів гармонізації українського законодавства зі стандартами міжнародних організацій, таких як НАТО та ЄС. Це включає вивчення вимог Директиви NIS, норм Будапештської конвенції та адаптацію їх до реалій української системи управління. Аналіз ефективності існуючих правових інструментів дозволить ідентифікувати прогалини та розробити механізми їх усунення.

Інтеграція інноваційних технологій у систему публічного управління національною безпекою є ще однією перспективною сферою досліджень. Особливої уваги потребує впровадження штучного інтелекту, блокчейн-

технологій, інструментів для обробки великих даних (Big Data) та хмарних обчислень для моніторингу, аналізу й прогнозування загроз. Подальші дослідження можуть бути спрямовані на створення ефективних моделей цифровізації управлінських процесів, а також на розробку платформ для оперативного обміну інформацією між органами влади.

Міжнародний досвід також є важливим напрямом для досліджень. Вивчення системи кібербезпеки країн Балтії, програм Smart Nation у Сингапурі чи інтегрованих систем X-Road в Естонії може стати основою для впровадження подібних рішень в Україні. Порівняльний аналіз міжнародних практик допоможе розробити ефективні механізми управління, які враховуватимуть специфіку української правової, соціальної та технологічної системи.

Крім того, перспективним є вивчення кадрового потенціалу в сфері національної безпеки. Це включає дослідження потреб у підготовці фахівців із кібербезпеки, розвитку цифрових компетенцій держслужбовців та створення навчальних програм для підвищення кваліфікації.

Таким чином, дослідження у сфері публічного управління національною безпекою зосереджуватимуться на вдосконаленні нормативно-правової бази, інтеграції інновацій, вивченні міжнародного досвіду та розвитку людського капіталу. Такий підхід сприятиме створенню ефективної, стійкої та адаптивної системи управління, яка відповідатиме викликам сучасного світу.

РОЗДІЛ 2
АНАЛІЗ СТАНУ ВИКОРИСТАННЯ ЦИФРОВИХ ТЕХНОЛОГІЙ У СЕКТОРІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ

2.1. Аналіз діяльності системи публічного управління у сфері забезпечення національної безпеки

Забезпечення національної безпеки є одним із ключових завдань держави. У сучасних умовах, коли Україна стикається з викликами військової агресії, кіберзагрозами та інформаційними атаками, роль публічного управління набуває особливого значення. Основою ефективної роботи системи національної безпеки є взаємодія державних інституцій, які використовують цифрові технології для координації, аналізу та реагування на загрози.

У підходах науковців національна безпека розглядається як безпека і захист національного майна держави, яке включає громадян, економіку та інститути, вважається обов'язком національного уряду. У такій системі стан національної безпеки повністю забезпечується силами правоохоронних органів та збройними силами України. Разом з тим, лише правоохоронні органи здатні забезпечити довготривалий стан безпеки на території, в умовах адміністративних режимів.

Відповідно до ст. 12 «Склад сектору безпеки і оборони» Закону України «Про національну безпеку України» від 21 червня 2018 року № 2469-VIII, до зазначеного сектору входять ключові складові, функції яких визначаються діючим законодавством України. До складу сектору безпеки і оборони входять:

1) Міністерство оборони України;

2) Збройні Сили України;

3) Державна спеціальна служба транспорту;

4) Міністерство внутрішніх справ України;

5) Національна гвардія України;

6) Національна поліція України;

7) Державна прикордонна служба України;

8) Державна міграційна служба України;

9) Державна служба України з надзвичайних ситуацій;

10) Служба безпеки України;

11) Управління державної охорони України;

12) Державна служба спеціального зв'язку та захисту інформації України;

13) Апарат Ради національної безпеки і оборони України;

14) розвідувальні органи України [41].

Отже, актуальним питанням вдосконалення організації державної підсистеми забезпечення національної безпеки є оптимізація її функцій. Модель, що міститься в Законі України «Про національну безпеку України», потребує корегування, оскільки виділення в ній основних функцій проведено не за єдиним, комплексним критерієм. Основними функціями, які розкривають зміст публічного управління діяльністю органів національної безпеки є такі, перелік яких наведено в табл. 2.1.

Таблиця 2.1

Функціональний зміст публічного управління діяльністю правоохоронних органів у сфері національної безпеки

№	Функція	Зміст діяльності органу влади
1	2	3
1.	Стратегічна	Визначення та узгодження життєво важливих національних інтересів особистості, суспільства і держави, формування на цій основі національних інтересів країни.
2.	Цілепокладання	Визначення цілей та завдань забезпечення національної безпеки в соціальній, економічній, екологічній та іншій сферах.
3.	Системна	Удосконалення системи забезпечення національної безпеки в означених сферах, приведення її у відповідність з якісними змінами обстановки у сфері системи безпеки, характером і спрямованістю загроз та викликів в ній, розробка та розвиток системи заходів забезпечення національної безпеки.
4.	Прогнозування	Виявлення, оцінка та прогнозування внутрішніх і зовнішніх викликів та загроз національним інтересам особистості, суспільства і держави, здійснення комплексу оперативних та довготривалих заходів.

Продовження табл. 2.1

1	2	3
5.	Ресурсна	Створення і підтримка в готовності сил та засобів забезпечення національної безпеки. Створення мобілізаційних ресурсів і визначення порядку їх розгортання.
6.	Планування	Управління силами і засобами забезпечення національної безпеки в повсякденних умовах і при надзвичайних ситуаціях.
7.	Інформаційна	Інформаційне забезпечення діяльності суб'єктів забезпечення національної безпеки.
8.	Оптимізації	Здійснення системи заходів щодо відновлення оптимального функціонування об'єктів нацбезпеки в регіонах, що постраждали в результаті виникнення надзвичайної ситуації.
9.	Зовнішньо-системна	Участь у заходах щодо забезпечення національної безпеки за межами держави відповідно до міжнародних договорів та угод, укладених або визнаних нею.

Таким чином, чітко визначено специфіку завдань військових формувань та правоохоронних органів держави, як їх особливі конституційні повноваження. Функції громадянського суспільства у сфері правоохорони і національної безпеки є можливість систематизувати таким чином:

1) методичне керівництво діяльністю громадських структур, організація взаємодії між ними і, державою з метою захисту національних інтересів (у соціальній, економічній та ін. сферах);

2) створення мережі органів громадської експертизи законодавства з питань забезпечення нацбезпеки при центральних і регіональних представницьких органах;

3) проведення незалежних експертиз джерел небезпек і загроз, формування банку даних інформації про стан захищеності національних інтересів і визначенні шляхів протидії цим загрозам;

4) боротьба з соціальними і моральними деформаціями та викривленнями, службовою безвідповідальністю і некомпетентністю державних службовців;

5) проведення безпосереднього інформаційно-пропагандистського впливу на носіїв загроз нацбезпеці в напрямку спонукання їх до відмови від антигромадської діяльності, переорієнтації їх антисоціальних установок на соціально-позитивні;

6) безпосереднє реагування на ситуації, що загрожують життю і

здоров'ю громадян, їх власності, соціально-культурному середовищі проживання, правопорядку;

7) протидію загрозам нацбезпеці шляхом самостійного або спільно з державними інститутами прийняття відповідних заходів безпеки в цій галузі;

8) соціальна мобілізація населення на протидію певним загрозам нацбезпеки шляхом надання позитивного впливу на соціальні цінності населення, на їхнє ставлення до загроз цій безпеці, формування активної позиції громадян і залучення їх в боротьбу із загрозами безпеці;

9) надання консалтингових та інших послуг з організації служб безпеки в соціальних організаціях;

10) забезпечувати на основі законності захист приватних сфер життя людини і громадянина;

11) розробка пропозицій щодо оновлення законодавчих актів з проблем забезпечення нацбезпеки;

12) забезпечувати реальні гарантії прав і свобод людини, рівний доступ до участі в державних і суспільних справах;

13) здійснювати функцію соціального контролю по відношенню до своїх членів, оскільки воно незалежно від держави, має у своєму розпорядженні засоби і санкціями, за допомогою яких може змусити індивіди дотримуватися суспільні норми, забезпечити соціалізацію та виховання громадян;

14) участь в розробці нових технічних засобів і соціальних технологій, орієнтованих на забезпечення безпеки в соціальній, економічній та ін. сферах;

15) політичної культури і соціальної відповідальності за долю майбутніх поколінь;

16) виконання комунікаційної функції (у демократичному суспільстві проявляється розмаїття інтересів. Найширший спектр цих інтересів єрезультатом тих свобод, якими володіє громадянин в умовах демократії;

17) розвиток творчості, ініціативи, волонтерства, благодійності та

меценатства, а також патріотизму та культури у громадян;

18) популяризація правил безпеки поведінки громадян в побуті, на службі, на відпочинку, у громадських місцях, залучення громадян через громадські об'єднання в практичну діяльність щодо забезпечення нацбезпеки;

19) підготовка, перепідготовка та підвищення кваліфікації громадян для роботи в недержавних структурах забезпечення національної безпеки;

20) участь в реалізації міжнародних програм із забезпечення національної безпеки (у соціальній, економічній та ін. сферах) [42].

Національні інтереси, які є гармонійним поєднанням особистісних, суспільних і державних інтересів, виступають загальним об'єктом національної безпеки. Водночас слід уточнити, що ці інтереси визначаються життєво важливими потребами та ціннісними пріоритетами, сформованими в процесі історичного розвитку українського народу та інших народів, які проживають на території України. Таким чином, особистісні, суспільні та державні інтереси можна вважати основними категоріями об'єктів національної безпеки.

Безпосередніми ж об'єктами є конкретні аспекти цих інтересів у таких сферах, як економіка, соціальні відносини, політика, екологія та інші.

Феномен національної безпеки розглядається через два аспекти: якісний і кількісний. Якісний аспект полягає в тому, що безпека середовища функціонування національної політико-правової системи є визначеною якістю, яка характеризується відсутністю загроз для цієї системи. Кількісний аспект відображає рівень безпеки, що залежить від кількості джерел загроз, окремих факторів і умов, які формують агресивне середовище для функціонування національної політико-правової системи [42].

У цьому контексті необхідно зазначити, що пріоритети державної політики щодо забезпечення національної безпеки й оборони визначаються у наступних державних документах (а також в інших документах, які регламентують питання національної безпеки й оборони, підлягають

схваленню Радою національної безпеки і оборони України та затверджуються через укази Президента України):

1) Стратегія національної безпеки України;

2) Стратегія воєнної безпеки України;

3) Стратегія кібербезпеки України;

4) Концепція розвитку сектору безпеки і оборони України [42].

Основним державним органом спеціального призначення, діяльність якого спрямована на виконання правоохоронних функцій є Служба безпеки України (СБУ).

СБУ підпорядковується Президенту України, а її діяльність регулюється законодавством України, зокрема Законом України «Про Службу безпеки України» [43].

Згідно даних [44] структура управління Служби безпеки України має такі складові, рис. 2.1.

Рис. 2.1. Структура управління Служби безпеки України [44]

Основними завданнями СБУ під час повномасштабного вторгнення рф на територію України є наступні [44]:

1. Протидія розвідувально-підривній і диверсійній діяльності ворожих спецслужб;
2. Захист національної державності;
3. Кібербезпека;
4. Протидія пропаганді та дезінформачії;
5. Контррозвідувальне забезпечення військових формувань;
6. Боротьба з тероризмом;
7. Охорона державної таємниці;
8. Розслідування воєнних злочинів окупантів;
9. Виконання бойових і спеціальних завдань;
10. Запровадження санкцій до російського бізнесу;
11. Обмін полоненими;
12. Інформаційно-аналітична діяльність;
13. Лікування та реабілітація військовослужбовчів сил оборони.

Аналіз основних показників діяльності Служби безпеки України за період с початку повномасштабної війни (станом на березень 2024 р.) проведено на підставі статистичної звітності СБУ, яка міститься у публічному доступі на офіційному сайті, результати подано в табл. 2.2-2.4 [44].

Таблиця 2.2

Результати протидії розвідувально-підривній і диверсійній діяльності ворожих спецслужб (станом на березень 2024 р.)

Результат діяльності	Всього	з них		
		Державна зрада (ст. 111 ККУ)	Диверсія (ст. 113 ККУ)	Передача інформачії про ЗСУ (ст. 114-2 ККУ)
Розпочато кримінальних проваджень	3088	2535	77	476
Обвинувальні вироки суду	499	384	8	107
Кількість осіб, яким повідомлено про підозру	2533	2168	52	313
Разом	6120	5087	137	896

Джерело: узагальнено автором за даними [44]

Графічно структуру результатів протидії розвідувально-підривній і диверсійній діяльності ворожих спецслужб (станом на березень 2024 р.)

роботи СБУ приведено на рис. 2.2.

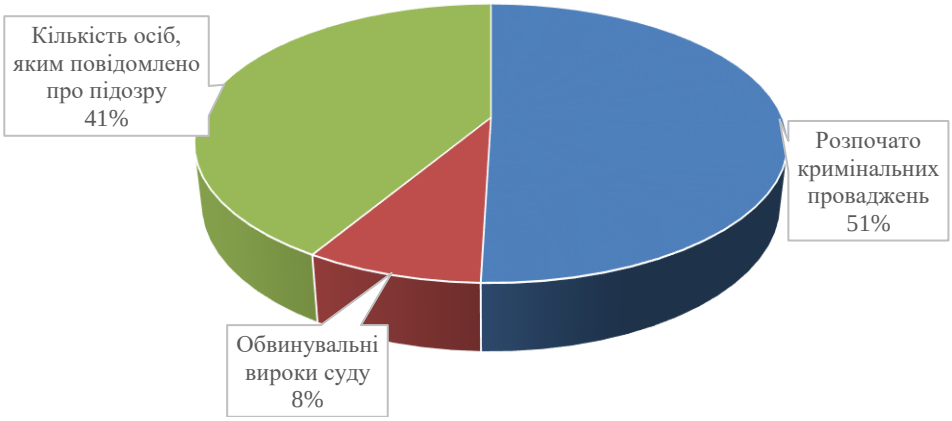

Рис. 2.2. Структура результатів роботи СБУ щодо протидії розвідувально-підривній і диверсійній діяльності ворожих спецслужб (станом на березень 2024 р.)

Джерело: узагальнено автором за даними [44]

За результатами табл. 2.2 зроблено висновок, що кількість розпочатих кримінальних проваджень та повідомлених підозр значно перевищує кількість обвинувальних вироків. Це свідчить про активну роботу СБУ на етапі викриття злочинів і збору доказів, але також демонструє, що частина проваджень ще перебуває на стадії судового розгляду. Загалом розпочато 3088 проваджень, з яких більшість стосується державної зради (2535 випадків). Це підкреслює стратегічну важливість боротьби з агентами ворога в умовах війни. Підозри повідомлено 2533 особам, що є високим показником залучення підозрюваних до відповідальності. Водночас обвинувальних вироків — 499. Найбільшу частку з них (384 вироки) становлять справи про державну зраду.

З аналізу табл. 2.3 видно, що робота Служби безпеки України у напрямі викриття колаборантів охоплює значну кількість справ, що дозволило зробити наступні висновки: розпочато 7230 кримінальних провадження, що демонструє високий рівень активності щодо розслідування злочинів, пов'язаних із колабораціонізмом; обвинувальних вироків винесено 915, що

свідчить про завершення частини проваджень і притягнення винних до відповідальності; підозри повідомлено 5489 особам, що вказує на значну кількість ідентифікованих осіб, які брали участь у колаборaційній діяльності.

Таблиця 2.3

Показники діяльності СБУ у напрямі викриття колаборантів (станом на березень 2024 р.)

Результат діяльності	Всього	з них		
		Посягання на територіальну цілісність і недоторканність України (ст. 110 ККУ)	Колаборaційна діяльність та пособництво державі-агресору (ст. 111-1 і 111-2 ККУ)	(ст. 109 ККУ)
Розпочато кримінальних проваджень	7230	636	6478	116
Обвинувальні вироки суду	915	164	715	36
Кількість осіб, яким повідомлено про підозру	5489	594	4816	79
Разом	13634	1394	12009	231

Джерело: узагальнено автором за даними [44]

Отже, висока активність СБУ у боротьбі з колаборaційною діяльністю демонструє її пріоритетність у поточних умовах війни. Кількість обвинувальних вироків (915) у порівнянні з кількістю проваджень (7230) підкреслює необхідність пришвидшення судових процесів, щоб більша кількість справ доходила до вироків.

Колаборaційна діяльність (ст. 111-1, 111-2) є найбільш поширеною категорією, що свідчить про значну загрозу такого типу злочинів для державної безпеки.

Беручи до уваги отримані результати аналізу, можна надати рекомендації для оптимізації цього напряму діяльності СБУ:

1. Оптимізувати судові процеси з метою збльшення кількості вироків у розпочатих справах;

2. Посилити інформаційно-аналітичну роботу з метою оперативного виявлення нових осіб, причетних до колаборaційної діяльності;

3. Розвивати міжнародну співпрацю для збору доказів і притягнення до відповідальності осіб, які здійснюють злочини за межами України.

Результати проведеного аналізу відображають значні зусилля СБУ у

напрямі викриття злочинів проти держави та сприяють покращенню їх ефективності у майбутньому.

Таблиця 2.4

Кількість знищених сил та засобів ворога на передовій (станом на березень 2024)

Вид	Кількість
Танки	799
БМП	1298
Артилерійські системи	674
Безпілотники	888
Кораблі, катери, човни та інші плавзасоби	46
Системи РЕР/РЕБ та ППО	432
Окупанти	8030

Джерело: узагальнено автором за даними [44]

Так, дані табл. 2.4 демонструють значні досягнення у нейтралізації військових ресурсів ворога на передовій. Отримані результати підтверджують ефективність дій СБУ та інших оборонних структур у знищенні техніки та живої сили противника. Найбільша кількість втрат припадає на живу силу (окупантів) та бронетехніку.

Аналіз за категоріями знищеної техніки дозволив зробити наступні висновки:

- знищено 799 одиниць танків, що є стратегічно важливою метою, оскільки танки забезпечують основну ударну силу противника. Це свідчить про активне використання сучасних протитанкових засобів та ефективність їх застосування;
- 1298 знищених БМП підтверджують високий рівень ураження бронетехніки, яка забезпечує мобільність і захист піхоти. Значна кількість таких втрат у ворога свідчить про систематичну роботу з перешкоджання його наступальним можливостям;
- знищено 674 артилерійські системи, які відіграють критичну роль у завданні масованих ударів. Ефективна боротьба з артилерією ворога допомагає знижувати інтенсивність обстрілів позицій українських військ та цивільних об’єктів;

- 888 знищених безпілотників є важливим показником боротьби із сучасними засобами розвідки та ударної авіації ворога. Цей показник відображає високий рівень готовності до протидії технологічним загрозам;

- знищено 46 одиниць плавзасобів, що свідчить про значну роботу у Чорноморському регіоні. Ці втрати впливають на здатність ворога забезпечувати військові перевезення та маневри морем;

- уражено 432 системи радіоелектронної розвідки/боротьби та протиповітряної оборони. Це важливо для зниження ефективності повітряного прикриття ворога та забезпечення переваги у повітрі;

- знищено 8030 окупантів, що є значним результатом у зменшенні чисельності особового складу ворога. Це напряму впливає на бойові можливості противника.

Варто визначити особливості сфери національної безпеки України як предмета публічного управління та адміністрування, що являє собою сукупність взаємопов'язаних суспільно-правових інститутів, які забезпечують функціонування цієї сфери, а також розроблено архітектоніку сфери національної безпеки України, яку пропонується розуміти як сукупність кількох базових компонентів: об'єкти національної безпеки України; система законодавства про національну безпеку України; суб'єкти публічного адміністрування у сфері національної безпеки України; інститут юридичної відповідальності за порушення законодавства у сфері національної безпеки України.

Об'єкт публічного управління у сфері *національної безпеки України* – суспільні відносини, що виникають із приводу створення відповідних правових норм, визначення адміністративно-правового статусу учасників цієї групи суспільних відносин, попередження та припинення відповідних правопорушень і притягнення до юридичної відповідальності за порушення встановленого режиму національної безпеки України.

Правовою основою діяльності суб'єкта публічного управління у сфері *національної безпеки України* стають норми національного права, а в процесі

своєї діяльності дані суб'єкти використовують виключно форми та методи публічного адміністрування.

У сукупності форм публічного адміністрування у сфері національної безпеки України важливо виокремити їх основні групи – правові та організаційні (які не пов'язуються з реалізацією державно-владних повноважень суб'єктами публічного адміністрування, а здебільшого сприяють їх здійсненню) [42].

Отже, таким чином, основні напрями удосконалення системи публічного управління у галузі забезпечення національної безпеки можливо сформулювати наступним чином: вдосконалення правової основи діяльності органів виконавчої влади, наділених компетенцією у сфері забезпечення національної безпеки; вдосконалення структури державних органів виконавчої влади, наділених компетенцією у сфері забезпечення національної безпеки; вдосконалення законодавства в окремих сферах, безпосередньо пов'язаних зі сферою забезпечення національної безпеки; приведення до єдиної стійкої системи нормативно-правових актів, що регламентують окремі види безпеки й аспекти її забезпечення; формування ефективного понятійного апарату, що виключає неоднозначне тлумачення, як при розробці нормативних актів, так і в процесі їх правозастосування у практиці органів державної влади.

2.2. Роль цифрових технологій у забезпеченні національної безпеки України

Цифрові технології відіграють ключову роль у забезпеченні безпеки держави, сприяючи ефективному управлінню, захисту критичної інфраструктури та швидкому реагуванню на сучасні виклики. Вони дозволяють моніторити кіберзагрози, аналізувати великі масиви даних, координувати дії органів влади та здійснювати інформаційну боротьбу. Інструменти, такі як системи кіберзахисту CERT-UA, платформа «Дія»,

безпілотники та автоматизовані системи управління, забезпечують ефективність у військовій, економічній та соціальній сферах. Крім того, цифрові рішення зміцнюють міжнародну співпрацю, інтегруючи Україну у глобальні системи безпеки, що дозволяє протидіяти гібридним загрозам і зберігати суверенітет держави.

Кібербезпека є одним із ключових напрямів забезпечення національної безпеки України. Сучасні виклики, такі як масштабні кібератаки, зростання шкідливого програмного забезпечення, інформаційна агресія, вимагають створення надійної системи кіберзахисту. В Україні поступово розвивається національна система кібербезпеки, яка базується на міжнародних стандартах і співпраці.

У сучасних умовах цифровізації значна чисельність випадків, які несуть небезпеку як для всієї держави, так і для окремих громадян, трапляється через цифрові канали, які викликають комп'ютерні надзвичайні ситуації. З метою протидії таким надзвичайним ситуаціям в Україні функціонує CERT-UA. CERT-UA (Computer Emergency Response Team of Ukraine) - це команда реагування на комп'ютерні надзвичайні ситуації в Україні. Її діяльність спрямована на забезпечення кібербезпеки та протидію кіберзагрозам. CERT-UA відіграє ключову роль у захисті національного кіберпростору, виконуючи функції, які представлено на рис. 2.3 [45].

Таким чином, в умовах гібридної війни, рис. 2.3, CERT-UA стала одним із ключових інструментів протидії кібератакам на критичну інфраструктуру України, включаючи енергетику, транспорт, зв'язок та фінансовий сектор. Її діяльність допомагає зберігати стійкість інформаційних систем держави навіть під час інтенсивного зовнішнього впливу.

Загалом, команда CERT-UA забезпечує надійну платформу для оперативного реагування на кіберзагрози, посилення національної кібербезпеки та розвитку культури кіберзахисту в Україні.

Кіберпростір є важливою складовою національної безпеки, і Україна стикається з постійними загрозами.

Рис. 2.3. Функції CERT-UA у захисті національного кіберпростору

Джерело: узагальнено за даними [45]

У 2023 році кількість кіберінцидентів значно зросла. За даними CERT-UA [45], кількість критичних подій інформаційної безпеки збільшилася на 62,5 % у порівнянні з попереднім роком. Так, результати роботи системи виявлення вразливостей та реагування на кіберінциденти у 2023 році (за даними CERT-UA) представлено в табл. 2.5.

Таблиця 2.5

Результати роботи системи виявлення вразливостей та реагування на кіберінциденти у 2023 році (за даними CERT-UA)

Показник	Кількість
Опрацьовано подій	18 мільярдів
Детектовано підозрілих подій інформаційної безпеки (ІБ)	133 мільйони
Опрацьовано критичних подій ІБ	148 тисяч
Зафіксовано кіберінцидентів	1105
Зростання кількості кіберінцидентів порівняно з 2022 роком	+62,5%

Джерело: узагальнено за даними CERT-UA [45]

Таким чином, за даними табл. 2.5, у 2023 році команда CERT-UA опрацювала понад 18 мільярдів подій, пов’язаних із кібербезпекою, з яких 133 мільйони було ідентифіковано як підозрілі. Кількість критичних подій інформаційної безпеки становила 148 тисяч, що свідчить про активізацію кіберзлочинців, особливо у сфері державного сектору та критичної інфраструктури. CERT-UA зафіксувала 1105 кіберінцидентів, що на 62,5 % більше, ніж у 2022 році, що підтверджує зростання інтенсивності атак.

Інформаційна безпека — це ключовий елемент забезпечення стійкості держави. Це також стан захищеності інформації, інформаційних систем і ресурсів від несанкціонованого доступу, використання, зміни, розголошення чи знищення. Вона забезпечує конфіденційність, цілісність і доступність даних, а також захищає від внутрішніх та зовнішніх загроз. Інформаційна безпека охоплює технічні, організаційні та правові заходи, які спрямовуються на протидію кіберзагрозам, збереження державних таємниць, запобігання поширенню дезінформації та гарантування стійкості до інформаційних атак.

За даними звіту CERT-UA, кількість шкідливого програмного забезпечення, спрямованого на українські державні установи, у 2023 році зросла на 95,8 % [45]. Узагальнення інформації щодо основних типів кіберзагроз та подій інформаційної безпеки у 2023 році представлено у табл. 2.6.

Таблиця 2.6

Основні типи кіберзагроз та подій інформаційної безпеки у 2023 році

Категорія загроз	Кількість зафіксованих подій
Шкідливий програмний код	1516861
Збір інформації зловмисником	133 000+
Несанкціонований доступ	75 000
Атаки на відмову в обслуговуванні (DDoS)	50 000

Джерело: узагальнено за даними CERT-UA [45]

Важливу роль у протидії таким загрозам, наведених у табл. 2.6, відіграє блокування ворожих ресурсів. У 2023 році було заблоковано понад 1500 проросійських платформ, що поширювали дезінформацію та намагалися дестабілізувати ситуацію в Україні [45].

Цифрові технології стали основою сучасної війни, значно підвищуючи ефективність, точність і швидкість дій військових сил. У військовій сфері України цифрові технології використовуються у сферах розвідки, управління, бойових операцій, логістики та кібербезпеки. Їх впровадження дозволяє українським військовим адаптуватися до складних умов сучасної війни, особливо в умовах протистояння агресії з боку росії.

Узагальнення інформації щодо можливих сфер використання цифрових технологій з описом їх дії в межах цієї сфери та прикладом застосування представлено в табл. 2.7.

Отже, використання цифрових технологій у військовій сфері є одним із ключових факторів, що визначають ефективність та рівень обороноздатності сучасних збройних сил. Для України, яка протистоїть агресії росії в умовах гібридної війни, інтеграція цифрових рішень покликана забезпечувати не лише перевагу на полі бою, а й стратегічну стійкість перед зовнішніми та внутрішніми загрозами.

Таблиця 2.7

Напрями використання цифрових технологій у військовій сфері з метою підвищення обороноздатності держави

Сфера	Дія	Приклад застосування
Управління безпілотними літальними апаратами (БПЛА)	Розвідка	БПЛА надають можливість отримувати в режимі реального часу точні дані про місцезнаходження ворога, його техніку та бойові позиції.
	Коригування артилерійського вогню	Використання дронів для наведення значно підвищує ефективність артилерійських обстрілів, знижуючи витрати боєприпасів
	Дрони-камікадзе	У 2023–2024 роках Україна активно використовувала ударні безпілотники для знищення бронетехніки, систем ППО, РЕБ і живої сили противника.
Автоматизовані системи управління військами	Оперативне управління	Використання АСУ дозволяє в режимі реального часу координувати дії підрозділів, аналізувати ситуацію на полі бою та швидко реагувати на зміни.
	Планування операцій	Цифрові платформи використовуються для моделювання сценаріїв та визначення оптимальних шляхів виконання бойових завдань.
Геоінформаційні системи (ГІС)	Аналіз місцевості	ГІС дозволяють враховувати особливості ландшафту, дорожню інфраструктуру та природні умови під час планування операцій.
	Координація підрозділів	Завдяки ГІС військові отримують детальні карти з розташуванням своїх та ворожих сил, що забезпечує ефективну координацію.
Кібербезпека у військовій сфері	Захист командних пунктів	Використання спеціалізованих систем шифрування для захисту зв’язку.
	Виявлення кібератак	Моніторинг і захист від спроб зламу військових мереж.
	Атаки на інфраструктуру ворога	Українські військові розробляють і застосовують методи цифрових атак для порушення роботи систем управління противника.
Використання штучного інтелекту (ШІ)	Аналіз великих даних	ШІ використовується для обробки розвідувальної інформації, виявлення патернів та аналізу поведінки противника.
	Автоматизація рутинних процесів	ШІ дозволяє автоматично виявляти загрози, класифікувати дані та надавати рекомендації командуванню
	Розпізнавання цілей	Технології ШІ використовуються для точного виявлення ворожих об’єктів, таких як техніка, живі сили чи інфраструктура
Інтеграція з міжнародними системами	Обмін розвідданими	Використання цифрових платформ для передачі та аналізу інформації про ворога.
	Міжнародні навчання	Участь у тренуваннях, що базуються на використанні цифрових технологій.
Логістика та забезпечення	Оптимізації постачання	Впровадження автоматизованих систем обліку та логістики забезпечує своєчасну доставку озброєння та ресурсів
	Контроль за використанням ресурсів	Технології дозволяють ефективно розподіляти запаси, уникаючи перевитрат.

Застосування безпілотних літальних апаратів (БПЛА) дозволяє вирішувати широкий спектр завдань - від розвідки до точкового ураження критично важливих об’єктів ворога. Дрони забезпечують оперативність та точність, знижуючи витрати ресурсів і мінімізуючи ризики для особового складу. Водночас, автоматизовані системи управління військами (АСУ) стали основою для швидкого прийняття рішень, координації підрозділів та адаптації до змінюваних умов бою. Ці технології підвищують ефективність артилерійських ударів, дозволяючи українським силам завдавати максимальної шкоди противнику.

Геоінформаційні системи (ГІС) сприяють аналізу місцевості, ефективному плануванню операцій та координуванню дій військових підрозділів. Використання ШІ та аналітичних платформ допомагає обробляти великі обсяги розвідувальної інформації, прогнозувати поведінку ворога та оптимізувати логістичні процеси. Застосування штучного інтелекту стає рушійною силою у розробці сучасних військових стратегій.

Кібербезпека займає окреме місце у військовій сфері, оскільки інформаційні системи стають мішенню для атак ворога. Захист комунікацій, командних пунктів та баз даних є критично важливим для забезпечення оперативного управління. Окрім цього, Україна активно використовує можливості цифрових атак для послаблення інфраструктури противника.

Інтеграція цифрових технологій у військову сферу України є результатом активної співпраці з міжнародними партнерами, такими як НАТО, ЄС та провідні країни світу. Ця співпраця дозволяє впроваджувати передові стандарти, проводити спільні навчання та отримувати технічну допомогу. Водночас розвиток власних цифрових рішень, адаптованих до специфіки бойових дій в Україні, зміцнює обороноздатність країни.

Цифровізація логістики та забезпечення є ще одним важливим компонентом, який дозволяє оптимізувати розподіл ресурсів, забезпечувати своєчасну доставку озброєння та підвищувати контроль за використанням запасів. Це знижує ймовірність перевитрат і підвищує ефективність

управління матеріально-технічним забезпеченням.

У підсумку, цифрові технології стали не лише важливим інструментом у військовій сфері, але й визначальним чинником у сучасній війні. Їхнє впровадження забезпечує швидкість, точність і адаптивність військових дій, знижуючи втрати і сприяючи досягненню стратегічних цілей. Для України розвиток цифрових технологій у військовій сфері є не лише викликом, але й перспективою, що відкриває нові горизонти для зміцнення національної безпеки та інтеграції у глобальні оборонні структури.

Цифрові технології в умовах сучасної війни та глобальних викликів стали невід’ємною складовою національної безпеки. Вони забезпечують ефективне управління державними ресурсами, зниження ризиків та швидке реагування на загрози, пов’язані з військовою агресією, кіберзагрозами, інформаційною війною та економічними викликами. Україна активно інтегрує цифрові рішення в сферу національної безпеки, що дозволяє підвищити ефективність державного управління у кризових ситуаціях.

2.3. Міжнародний досвід використання цифрових технологій у сфері національної безпеки

У сучасному світі цифрові технології стали невід'ємною складовою національної безпеки, забезпечуючи ефективний захист державних інтересів та громадян. Міжнародний досвід свідчить про існування різноманітних підходів до інтеграції цифрових рішень у сферу безпеки, що дозволяє країнам адаптуватися до нових викликів та загроз.

Сполучені Штати Америки є лідером у впровадженні цифрових технологій для забезпечення національної безпеки. Агентство національної безпеки (NSA) активно використовує передові методи кіберрозвідки та аналізу даних для виявлення потенційних загроз. Програми масового збору даних, такі як PRISM, дозволяють відстежувати комунікації та виявляти підозрілі активності, що сприяє запобіганню терористичних актів та інших

загроз [46].

У поглядах А.В. Войціховського зазначено, що у Європейському Союзі питання кібербезпеки регулюються Директивою NIS (Network and Information Security), яка встановлює вимоги до забезпечення безпеки мереж та інформаційних систем. Європейське агентство з кібербезпеки (ENISA) координує зусилля країн-членів у сфері кіберзахисту, надаючи рекомендації та підтримку у впровадженні передових технологій [48].

Ізраїль відомий своєю розвиненою кіберіндустрією та інноваційними підходами до забезпечення безпеки. Країна активно інвестує в розвиток стартапів у сфері кібербезпеки, що дозволяє впроваджувати новітні технології для захисту критичної інфраструктури та державних установ. Ізраїльські компанії розробляють рішення для виявлення та нейтралізації кібератак, що підвищує стійкість країни до цифрових загроз

У Китаї цифрові технології використовуються для моніторингу та контролю інформаційного простору. Система «Великий китайський фаєрвол» обмежує доступ до певних іноземних ресурсів, забезпечуючи контроль над інформаційними потоками. Крім того, Китай активно розвиває технології штучного інтелекту для аналізу великих обсягів даних, що сприяє виявленню потенційних загроз на ранніх етапах

Велика Британія впровадила Національну стратегію кібербезпеки, яка передбачає розвиток кіберзахисних можливостей та співпрацю з приватним сектором. Національний центр кібербезпеки (NCSC) надає рекомендації та підтримку організаціям у сфері кіберзахисту, сприяючи підвищенню загальної стійкості країни до цифрових загроз [48].

У Німеччині Федеральне відомство з інформаційної безпеки (BSI) відповідає за координацію заходів у сфері кібербезпеки. Країна активно впроваджує стандарти безпеки для критичної інфраструктури та розробляє національні стратегії для протидії кіберзагрозам [49].

Франція створила Агентство національної безпеки інформаційних систем (ANSSI), яке відповідає за захист державних інформаційних систем та

координацію заходів у сфері кібербезпеки. Країна активно співпрацює з міжнародними партнерами для обміну інформацією та спільної протидії кіберзагрозам [48].

У Південній Кореї уряд активно інвестує в розвиток кіберзахисних технологій та співпрацює з приватним сектором для забезпечення національної безпеки. Країна розробила національну стратегію кібербезпеки, яка передбачає підвищення стійкості до кібератак та розвиток людських ресурсів у цій сфері [48].

Австралія впровадила Національну стратегію кібербезпеки, яка спрямована на захист критичної інфраструктури та підвищення обізнаності громадян щодо кіберзагроз. Уряд співпрацює з приватним сектором та міжнародними партнерами для забезпечення ефективного кіберзахисту

Канада створила Центр кібербезпеки, який координує заходи у сфері кіберзахисту та надає підтримку організаціям у впровадженні передових технологій. Країна активно розвиває національну стратегію кібербезпеки та співпрацює з міжнародними партнерами для протидії кіберзагрозам

Узагальнення міжнародного досвіду використання цифрових технологій у сфері національної безпеки представлено у табл. 2.8.

Таблиця 2.8

Узагальнення міжнародного досвіду використання цифрових технологій у сфері національної безпеки

Країна	Напрям використання цифрових технологій для забезпечення національної безпеки	Практичний приклад, джерело
1	2	3
США	Використання штучного інтелекту для аналізу великих даних і прогнозування загроз.	Програма PRISM, яка аналізує масиви комунікацій для виявлення терористичних загроз [50].
Ізраїль	Інноваційні системи кіберзахисту та моніторинг загроз у реальному часі.	Розробка системи Cybereason, яка виявляє шкідливе програмне забезпечення та координує захист у масштабах країни [51].
Європейський Союз	Гармонізація законодавства у сфері кібербезпеки та захист цифрових продуктів.	Прийняття Директиви NIS2 для підвищення рівня безпеки цифрових мереж у країнах-членах ЄС [52].

Продовження табл. 2.8

1	2	3
Китай	Контроль інформаційного простору та застосування штучного інтелекту для аналізу загроз.	Система «Великий китайський фаєрвол», яка блокує небезпечні ресурси та аналізує онлайн-комунікації [53].
Велика Британія	Розробка національної стратегії кібербезпеки та захист критичної інфраструктури.	Створення Національного центру кібербезпеки (NCSC) для координації заходів у сфері кіберзахисту та надання рекомендацій організаціям [54].
Німеччина	Захист критичної інфраструктури та розвиток національної стратегії кібербезпеки.	Федеральне відомство з інформаційної безпеки (BSI) відповідає за координацію заходів у сфері кібербезпеки та розробку стандартів безпеки [55].
Франція	Захист державних інформаційних систем та координація заходів у сфері кібербезпеки.	Агентство національної безпеки інформаційних систем (ANSSI) відповідає за захист державних інформаційних систем та співпрацю з міжнародними партнерами [56].
Південна Корея	Інвестиції в розвиток кіберзахисних технологій та співпраця з приватним сектором.	Розробка національної стратегії кібербезпеки, яка передбачає підвищення стійкості до кібератак та розвиток людських ресурсів у цій сфері [57].
Австралія	Захист критичної інфраструктури та підвищення обізнаності громадян щодо кіберзагроз.	Впровадження Національної стратегії кібербезпеки, яка спрямована на захист критичної інфраструктури та співпрацю з приватним сектором [58].
Канада	Координація заходів у сфері кіберзахисту та підтримка організацій у впровадженні передових технологій.	Створення Центру кібербезпеки, який координує заходи у сфері кіберзахисту та надає підтримку організаціям у впровадженні передових технологій [59].

Джерело: узагальнено на підставі [50-59]

Таким чином, табл. 2.8 відображає широкий спектр підходів різних країн до використання цифрових технологій у сфері національної безпеки, демонструючи залежність стратегій від пріоритетів кожної держави. Так,

США та Ізраїль є лідерами у впровадженні штучного інтелекту для прогнозування та реагування на кіберзагрози. Програми, такі як PRISM у США, та інноваційні платформи типу Cybereason в Ізраїлі, забезпечують високий рівень захисту шляхом аналізу великих даних і моніторингу мереж у реальному часі. Європейський Союз фокусується на гармонізації законодавства та захисті цифрових продуктів через директиву NIS2, що посилює кіберстійкість країн-членів. Китай використовує контрольовані цифрові екосистеми, такі як «Великий китайський фаєрвол», для моніторингу інформаційних потоків, що дозволяє забезпечити внутрішню стабільність та уникати зовнішніх загроз. Велика Британія, Німеччина та Франція розвивають національні центри кібербезпеки, які координують захист критичної інфраструктури, пропонують рекомендації для державних та приватних структур і сприяють міжнародній співпраці. Австралія та Канада роблять акцент на підвищенні обізнаності громадян, забезпеченні безпеки критичної інфраструктури та співпраці з приватним сектором для посилення кіберзахисту.

Таким чином, узагальнений аналіз табл. 2.8 свідчить про те, що *цифрові технології стали ключовим елементом національної безпеки у світі.* Водночас країни адаптують свої стратегії використання цифрових технологій залежно від геополітичних умов, технічних ресурсів і внутрішніх пріоритетів.

Отже, аналіз міжнародного досвіду використання цифрових технологій у національній безпеці дозволив виокремити найбільш успішні практики. Так, в США використовують штучний інтелект та великі дані для виявлення терористичних загроз, аналізу поведінкових моделей та захисту кіберпростору. Кіберкомандування США активно впроваджує технології для моніторингу кіберзагроз та швидкого реагування на них. Ізраїль є лідером у сфері кібербезпеки. Завдяки інноваційним цифровим рішенням, країна забезпечує захист своїх державних систем від кібератак. Однією з ключових технологій є аналітика великих даних, яка дозволяє своєчасно ідентифікувати

загрози.

До основних напрямів впливу кіберзагроз на обороноздатність країни відносяться наступні:

1. Компрометація конфіденційності інформації. У разі викрадення або поширення конфіденційної інформації може постраждати здатність країни захищатися, оскільки противники можуть використовувати ці дані для планування атак.

2. Порушення комунікаційних каналів. Атаки на комунікаційні мережі можуть дезорганізувати військові операції та оперативне управління, що послабить захист на стратегічному рівні.

3. Зниження ефективності оборонних систем. Кібератаки можуть порушити функціонування систем раннього попередження, контролю озброєнь та інших важливих елементів оборонної інфраструктури.

4. Економічні збитки. Ураження інфраструктури і необхідність захисту від кіберзагроз можуть призвести до значних економічних втрат, що опосередковано впливатиме на ресурсне забезпечення оборонного сектора.

Найбільш відомі випадки кіберзагроз на обороноздатність та безпеку держави у світі та в Україні узагальнено у табл. 2.9 [60].

Таблиця 2.9

Світовий досвід найбільш впливових кіберзагроз на обороноздатність і безпеку держав

Випадок кіберзагрози, країна, рік	Опис події	Характеристика впливу
1	2	3
Кібератака на Естонію (2007)	Під час ескалації політичної напруги з росією в 2007 році Естонія зазнала масованої DDoS-атаки, яка вивела з ладу основні урядові сайти, банківські системи та ЗМІ.	Ця атака на кілька тижнів паралізувала значну частину інфраструктури країни, порушивши комунікацію та обслуговування населення. Подія продемонструвала необхідність у створенні кіберармії та спеціалізованих центрів захисту в ЄС і НАТО для реагування на подібні загрози.
Кібератака на Іранську ядерну програму (Stuxnet, 2010)	Шкідливе ПЗ Stuxnet, розроблене, ймовірно, США та Ізраїлем, було спрямоване на іранські центрифуги для збагачення урану, що дестабілізувало роботу.	Ця атака порушила функціонування іранської ядерної програми та затримала процес збагачення урану. Stuxnet став першим відомим прикладом використання кіберзброї для фізичного руйнування стратегічного об’єкта.

Продовження табл. 2.9

1	2	3
Кібератака NotPetya на Україну (2017)	У червні 2017 року вірус NotPetya уразив державні установи, банки, енергетичні компанії та транспортну інфраструктуру України, а також зачепив інші країни.	Атака призвела до масштабних збоїв у роботі українських державних органів і критичної інфраструктури. NotPetya показала, як кібератака може паралізувати діяльність цілої країни, вивівши з ладу частину оборонного сектора та системи управління.
Атака на системи електропостачання в Україні (2015, 2016)	У 2015 році кібератака на українські енергокомпанії призвела до відключення електроенергії в декількох регіонах країни. У 2016 році схожа атака вразила Київську електростанцію.	Це була одна з перших кібератак, яка вивела з ладу енергетичну інфраструктуру, безпосередньо впливаючи на цивільних і оборонні структури. Події продемонстрували вразливість критичної інфраструктури перед кіберзагрозами і підкреслили важливість кіберзахисту для забезпечення національної безпеки.
Кібератаки з боку APT-груп на США	Уряди та організації США неодноразово ставали жертвами APT-груп (Advanced Persistent Threat), пов'язаних з іноземними державами, зокрема з Китаєм і росією. Наприклад, атаки групи APT29 (пов’язують з росією) у 2016 році націлювалися на електронні системи Демократичної партії.	Викрадення конфіденційних документів і злам систем виборчих органів викликали значний політичний резонанс і показали вразливість національної безпеки США до втручання в державні процеси.
Атака на Міненерго та Міністерство оборони Франції (2019)	Кібератака на сервери Міністерства оборони Франції та французькі енергетичні компанії, яку приписують групам з-за кордону, мала на меті вивід з ладу критично важливих систем.	Цей інцидент привернув увагу до ризиків для оборонної промисловості, показавши, що кіберзагрози можуть порушити безперебійну роботу стратегічних секторів економіки та безпеки.

Отже, для забезпечення ефективного захисту від кіберзагроз у секторі національної безпеки потрібна розвинена кіберінфраструктура, постійний моніторинг і аналіз загроз, а також міжнародне співробітництво для запозичення найкращих практик у сфері кібербезпеки.

Таким чином, сучасні реалії та виклики у сфері національної безпеки обумовлюють необхідність державам приділяти особливу увагу впровадженню цифрових технологій для захисту своїх громадян, критичної інфраструктури та інформаційного простору. Кіберзагрози стають

глобальними, а їхній вплив охоплює не лише локальні сфери, а й міжнародні відносини, економіку та обороноздатність держав. У відповідь на ці виклики країни розробляють та впроваджують національні стратегії кібербезпеки, які включають інноваційні підходи, регулювання та міжнародну співпрацю.

Відображення основних ініціатив провідних країн світу у сфері кібербезпеки з висвітленням ключових напрямів використання цифрових технологій та практичні приклади їх застосування представлено у табл. 2.10. Цей аналіз демонструє, як різні держави адаптують свої стратегії відповідно до власних потреб та рівня технологічного розвитку [61].

Таблиця 2.10

Основні ініціативи держав світу у сфері кібербезпеки

Країна/Регіон	Ініціатива/Стратегія	Ключові напрями
США	Імплементаційний план Національної стратегії кібербезпеки	Захист критичної інфраструктури, розвиток кіберкадрів
Європеський Союз	Закон про кіберстійкість	Безпека цифрових продуктів, регулювання ринку
Китай	Створення «бар'єру кібербезпеки»	Контроль над внутрішнім кіберпростором
Україна	Стратегія кібербезпеки	Гармонізація законодавства з ЄС, кібердипломатія

Джерело: узагальнено на підставі [61]

Отже, табл. 2.10 висвітлює ключові стратегії у сфері кібербезпеки. Так, імплементаційний план Національної стратегії кібербезпеки в США, підкреслює важливість захисту критичної інфраструктури та розвитку висококваліфікованих кадрів. Це дозволяє створювати стійкі системи управління та мінімізувати ризики від зловживання вразливостями. Прийняття Закону про кіберстійкість в ЄС спрямоване на регулювання безпеки цифрових продуктів, що стає важливим у контексті цифрової інтеграції Європи. Регіон ставить за мету встановити високі стандарти кіберзахисту на законодавчому рівні. Створення «бар'єру кібербезпеки» в Китаї демонструє прагнення до повного контролю над внутрішнім кіберпростором, що дозволяє ефективно регулювати інформаційні потоки та захищати власні мережі. Реалізація Стратегії кібербезпеки в Україні має на меті гармонізацію з європейським законодавством і розвиток

кібердипломатії. Ця ініціатива є важливою складовою інтеграції країни до глобального інформаційного простору.

Кіберзагрози є глобальною проблемою, що впливає на всі регіони світу, проте характер і масштаби цих загроз варіюються залежно від рівня технологічного розвитку, геополітичної ситуації та стану національної безпеки в кожній країні. У різних регіонах пріоритетними залишаються атаки на критичну інфраструктуру, програми-вимагачі, інформаційні операції та кібершпигунство.

Основні виклики у сфері кібербезпеки за регіонами у 2023 році представлені у табл. 2.11 [61].

Таблиця 2.11

Основні виклики у сфері кібербезпеки за регіонами (за даними 2023 р.)

Регіон	Основні загрози	Приклад
Європа	Атаки на державні установи та критичну інфраструктуру	Китайська кампанія PlugX, атаки GhostWriter
США	Програми-вимагачі, зловживання вразливостями	Витік даних через MOVEit (понад 11 млн людей постраждали)
Азія	Інформаційні операції, кібершпигунство	Програми-шпигуни у Google Play
Африка	Атаки на портали держпослуг	DDoS-атака на портал eCitizen у Кенії

Джерело: узагальнено на підставі [61]

Отже, аналіз даних табл. 2.11 дозволяє побачити характер зміни загрози залежно від географічного контексту, а також зрозуміти актуальність аспектів кіберзахисту для конкретних країн та регіонів. Інформація підкреслює важливість адаптації національних стратегій до особливостей глобальних кіберзагроз. Таблиця розкриває різноманітні кіберзагрози, з якими стикаються різні регіони світу. Так, у Європі основною загрозою залишаються атаки на критичну інфраструктуру, зокрема через групу GhostWriter, що спеціалізується на впливі на державні установи. Це свідчить про те, що вороги обирають стратегічно важливі цілі для дестабілізації регіону. У США - програми-вимагачі, наприклад MOVEit, завдають значних економічних збитків та спричиняють витоки персональних даних мільйонів людей. Це підкреслює необхідність посилення політики кібербезпеки для

захисту громадян. В Азії інформаційні операції та кібершпигунство залишаються пріоритетними загрозами. Програми-шпигуни, розміщені у Google Play, вказують на те, що навіть загальнодоступні платформи можуть використовуватись для збору чутливої інформації. В Африці траплялися DDoS-атаки на портали держпослуг, зокрема, з eCitizen у Кенії, що наголошує на важливості зміцнення захисту онлайн-сервісів, які стали критично важливими для громадян.

Таким чином, аналіз використання цифрових технологій у секторі національної безпеки України дозволив визначити ключові аспекти їх ролі у зміцненні обороноздатності держави, управлінні кризовими ситуаціями та протидії сучасним загрозам. Цифрові технології, такі як системи моніторингу, кіберзахисту та автоматизації процесів, є основою для ефективної роботи органів публічного управління. Їхнє впровадження забезпечує зниження ризиків, оперативність реагування та координацію між різними структурами безпеки.

Аналіз вітчизняного та міжнародного досвіду використання цифрових технологій у сфері національної безпеки свідчить, що Україна демонструє значний прогрес у розвитку кібербезпеки, інтеграції інноваційних рішень, таких як CERT-UA, та впровадженні автоматизованих систем управління. Водночас, міжнародні практики — зокрема, США, Європейського Союзу, Ізраїлю та Китаю — дають змогу краще адаптувати національні стратегії до сучасних викликів.

Використання цифрових технологій у військовій сфері, розвідці та логістиці дозволяє Україні успішно протистояти гібридним загрозам і зміцнювати стратегічну стійкість. Розвиток безпілотних літальних апаратів, штучного інтелекту та геоінформаційних систем став визначальним чинником у досягненні переваги над ворогом.

Отже, результати аналізу підтверджують необхідність подальшого вдосконалення цифрових технологій, підвищення рівня кіберзахисту та інтеграції міжнародного досвіду у національні системи безпеки України.

РОЗДІЛ 3
НАПРЯМИ УДОСКОНАЛЕННЯ ВИКОРИСТАННЯ ЦИФРОВИХ ТЕХНОЛОГІЙ У ПУБЛІЧНОМУ УПРАВЛІННІ В СЕКТОРІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ

3.1. Стратегічні підходи до цифровізації сектору національної безпеки

Попередніми дослідженнями доведено, що цифровізація сектору національної безпеки є стратегічним пріоритетом для України, яка стикається зі складними викликами в умовах гібридної війни. Ефективна інтеграція цифрових технологій у публічне управління вимагає обгрунтованих стратегічних підходів, які враховують міжнародний досвід, особливості національної безпеки та тенденції цифрової трансформації.

Цифровізація сектору національної безпеки повинна базуватися на *довгостроковому стратегічному плануванні*. Основою для таких підходів є прийнята у 2021 році «Стратегія кібербезпеки України» [34], яка визначає основні цілі та завдання цифрової трансформації у цій сфері. Стратегія акцентує увагу на гармонізації з міжнародними стандартами, інтеграції інноваційних технологій та розвитку міжвідомчої співпраці. Разом з тим, особливе значення має створення національної системи раннього виявлення загроз. Ця система повинна поєднувати в собі сучасні алгоритми штучного інтелекту, обробку великих даних та геоінформаційні технології. Такий підхід дозволяє прогнозувати можливі загрози, аналізувати ризики та вчасно реагувати на інциденти.

Стратегічне планування цифровізації в Україні є комплексним і багатоетапним процесом, який спрямований на інтеграцію сучасних технологій у всі сфери державного управління, включаючи сектор національної безпеки. Цей процес враховує міжнародний досвід, національні

потреби та сучасні виклики цифрової трансформації.

Узагальнено етапи процесу стратегічного планування цифровізації в Україні можна представити у вигляді табл. 3.1.

Таблиця 3.1

Етапи процесу стратегічного планування цифровізації в Україні

Етап	Характеристика етапу	Напрям впровадження
1. Формування стратегічного бачення	На початковому етапі формулюється загальне бачення цифровізації, яке відповідає національним пріоритетам і глобальним тенденціям. Це бачення включає визначення ключових напрямків розвитку, таких як кібербезпека, цифровізація критичної інфраструктури, автоматизація державного управління та впровадження інноваційних технологій, зокрема штучного інтелекту і блокчейну.	Стратегічні напрями цифрової трансформації держави визначені у низьцы нормативно-правових актах. Зокрема, 17 лютого 2021 року Кабінет Міністрів України затвердив перелік 94 проєктів цифрової трансформації, що охоплюють різні сфери державного управління та суспільного життя [62]. 3 березня 2021 року уряд схвалив «Концепцію розвитку цифрових компетентностей до 2025 року» [63]. яка передбачає навчання 6 мільйонів українців цифрової грамотності та впровадження національної онлайн-платформи «Дія.Цифрова освіта» [64].
2. Розробка національних стратегій та нормативно-правової бази	Планування цифровізації супроводжується розробкою нормативних документів, які регулюють впровадження технологій. Законодавчі ініціативи спрямовані на гармонізацію українських стандартів із міжнародними, такими як директива NIS2 ЄС. Це дозволяє забезпечити ефективну інтеграцію України у глобальний цифровий простір.	«Стратегія кібербезпеки України на 2021-2025 рр.» [34]. є прикладом комплексного підходу до вирішення питань безпеки в умовах цифровізації.
3. Визначення пріоритетів та ресурсів	Наступним кроком є пріоритизація напрямків цифровізації. Держава визначає критично важливі об'єкти, які потребують цифрової трансформації, наприклад, енергетика, транспорт, військова сфера та охорона здоров'я. Для реалізації цифровізації залучаються внутрішні та зовнішні ресурси.	Україна активно співпрацює з міжнародними партнерами, зокрема, ЄС, НАТО та Світовим банком, для отримання технічної і фінансової підтримки.
4. Розвиток інституційної спроможності	Ефективне впровадження цифрових технологій потребує створення або модернізації інституцій, відповідальних за реалізацію цифрових стратегій. Крім того, важливу роль відіграє Національний координаційний центр кібербезпеки, який реалізує стратегії в рамках безпекового сектору.	Міністерство цифрової трансформації України координує впровадження національних ініціатив у сфері цифровізації, забезпечуючи міжвідомчу співпрацю. Наприклад, функціонування Національного координаційного центру кібербезпеки (НКЦК) під час відбиття масштабних кібератак на українські державні органи в січні

Продовження табл. 3.1

1	2	3
		2022 року. Тоді хакери здійснили атаки на понад 70 державних вебсайтів, включаючи портали урядових органів. НКЦК швидко координував дії з реагування, забезпечуючи співпрацю між CERT-UA, Держспецзв'язку та іншими органами. У результаті вдалось оперативно відновити роботу постраждалих ресурсів і запобігти поширенню шкідливого програмного забезпечення [45]. Цей випадок демонструє, як НКЦК реалізує стратегічні завдання кіберзахисту в умовах реальних загроз, забезпечуючи безпеку критично важливої інформаційної інфраструктури України.
5. Розробка технічних рішень та впровадження пілотних проєктів	На цьому етапі реалізуються конкретні технічні рішення для забезпечення стратегічних цілей цифровізації. Пілотні проєкти стають основою для перевірки ефективності нових технологій та підходів.	Успішне впровадження платформи «Дія», яка стала інструментом цифрового державного управління та значно спростила доступ громадян до державних послуг.
6. Моніторинг та оцінка результатів	Завершальним етапом є моніторинг впроваджених ініціатив і оцінка їхньої ефективності. Для цього використовуються показники успішності (KPI), які дозволяють виміряти вплив цифровізації на управління, економіку та безпеку. Регулярний аудит результатів сприяє виявленню слабких місць і дозволяє своєчасно адаптувати стратегії відповідно до нових викликів.	Прикладом успішного моніторингу та оцінки результатів у сфері цифровізації національної безпеки України є система «Дія.Освіта» [65], впроваджена Міністерством цифрової трансформації. У рамках моніторингу проєкту регулярно оцінюється ефективність використання платформи для підвищення цифрової грамотності населення. Наприклад, станом на 2023 рік понад 1,5 мільйона українців пройшли навчання на платформі, що свідчить про зростання обізнаності громадян у питаннях цифрової безпеки. Результати цих оцінок використовуються для адаптації навчальних програм, розширення доступу до платформи в регіонах і вдосконалення інструментів для моніторингу прогресу користувачів, що дозволяє ефективніше досягати стратегічних цілей цифровізації.

Джерело: власна розробка

Отже, дані, представлені у табл. 3.1, відображають систематизований процес стратегічного планування цифровізації в Україні, що охоплює всі

ключові етапи – від формування стратегічного бачення до моніторингу й оцінки результатів. Кожен із цих етапів відіграє важливу роль у забезпеченні ефективної інтеграції цифрових технологій у державне управління та національну безпеку.

Так, згідно табл. 3.1, *формування стратегічного бачення* є базовим етапом, який задає загальні орієнтири для цифрової трансформації країни. Затвердження урядом України ключових концепцій, таких як «Концепція розвитку цифрових компетентностей до 2025 року», демонструє чітке прагнення до інтеграції сучасних технологій у всі сфери суспільного життя. Це сприяє системній реалізації державних проєктів, таких як «Дія», що забезпечує централізований доступ до послуг для громадян.

Етап *розробки національних стратегій та нормативно-правової бази* підкреслює необхідність гармонізації законодавства з міжнародними стандартами. Впровадження «Стратегії кібербезпеки України на 2021-2025 роки» є прикладом адаптації державою світових практик до локальних умов. Цей етап спрямований на створення правової основи, яка забезпечує інтеграцію України у глобальний цифровий простір.

На етапі *визначення пріоритетів та ресурсів* акцент зроблено на ідентифікації найбільш важливих напрямків цифровізації, зокрема у сфері енергетики, транспорту, військової безпеки. Успішна співпраця з міжнародними організаціями, такими як НАТО та ЄС, свідчить про те, що Україна активно залучає зовнішні ресурси для зміцнення своїх позицій.

Етап *розвитку інституційної спроможності* вказує на необхідність координації дій між державними структурами. Діяльність Національного координаційного центру кібербезпеки, продемонстрована під час відбиття масштабних кібератак у січні 2022 року, є яскравим прикладом того, як інституції реагують на загрози в реальному часі, забезпечуючи захист критичної інформаційної інфраструктури.

Розробка технічних рішень та впровадження пілотних проєктів підкреслює важливість інноваційних рішень для досягнення стратегічних

цілей. Впровадження платформи «Дія» стало не лише технологічним проривом, але й символом нової ери цифровізації в Україні. Цей проєкт значно полегшив взаємодію громадян з державними органами.

На завершальному етапі – *моніторинг та оцінка результатів* – важливим є аналіз досягнень та недоліків для коригування стратегій. Використання системи «Дія.Освіта» для підвищення цифрової грамотності населення демонструє, як моніторинг сприяє вдосконаленню навчальних програм і розширенню доступу до технологій у регіонах.

Отже, у підсумку, таблиця 3.1 ілюструє послідовність і комплексність процесу стратегічного планування цифровізації в Україні. Її ключові етапи підтверджують, що країна рухається в правильному напрямку, інтегруючи передові технології для забезпечення національної безпеки та підвищення ефективності державного управління.

У процесі цифровізації сектору національної безпеки важливо враховувати досвід провідних країн світу, таких як США, Ізраїль, Європейський Союз. Наприклад, у США впроваджено стратегічний підхід до розвитку кібербезпеки через створення Національного центру кібербезпеки (NCSC), що дозволяє координувати дії урядових структур і приватного сектору. В Ізраїлі активна роль відводиться кіберінноваціям, які підтримуються на державному рівні.

Врахування міжнародного досвіду допомагає адаптувати українські стратегії до сучасних умов, підвищуючи ефективність захисту інформаційного простору. Інтеграція таких підходів сприяє формуванню ефективної системи кібербезпеки, здатної протистояти сучасним викликам.

У процесі цифровізації сектору національної безпеки важливо враховувати досвід провідних країн світу, таких як США, Ізраїль, Європейський Союз. Так, результати досліджень другого розділу свідчать, що, у США впроваджено стратегічний підхід до розвитку кібербезпеки через створення Національного центру кібербезпеки (NCSC), що дозволяє координувати дії урядових структур і приватного сектору. В Ізраїлі активна

роль відводиться кіберінноваціям, які підтримуються на державному рівні.

Врахування міжнародного досвіду може стати підставою адаптації українських стратегій до сучасних умов та підвищити ефективність захисту інформаційного простору. Інтеграція таких підходів може сприяти формуванню ефективної системи кібербезпеки, здатної протистояти сучасним викликам. Етапи інтеграції міжнародного досвіду у вдосконалення використання цифрових технологій у національній безпеці України представлено на рис. 3.1.

Рис. 3.1. Етапи інтеграції міжнародного досвіду у вдосконалення використання цифрових технологій у національній безпеці України

Отже, на рис. 3.1 запропоновано етапи послідовного процесу інтеграції міжнародного досвіду у вдосконалення цифрових технологій у національній безпеці України. Цей процес структурований у сім ключових етапів, які формують логічну та системну модель впровадження найкращих практик світового рівня у національний контекст. Так, на першому етапі – *аналіз та адаптації міжнародних практик* – передбачено дослідження досвіду провідних країн, таких як США, Ізраїль, Велика Британія та ЄС. Цей етап акцентує увагу на адаптації стратегій і технологій, які відповідають українським реаліям. Особливу роль відіграє визначення тих інструментів, що ефективно працюють в інших країнах, і їх адаптація під локальні потреби. Другий етап – *гармонізація законодавства* – забезпечує нормативну відповідність між українськими правовими актами та міжнародними стандартами, наприклад, як директива NIS2 ЄС. Це дозволяє інтегрувати передові технології, зокрема блокчейн, штучний інтелект і великі дані, у національну правову систему, що є основою для подальшої цифровізації. На третьому етапі – *розбудова інституційної інфраструктури* – увага приділяється створенню нових або модернізації існуючих структур, які відповідальні за впровадження цифрових технологій. Зокрема, важливим є розвиток Національного координаційного центру кібербезпеки, що функціонує як стратегічний орган для координації дій у сфері кіберзахисту. Четвертий етап – *навчання та підготовка кадрів* – підкреслює необхідність розвитку людського потенціалу. Залучення міжнародних експертів, проведення тренінгів та підготовка спеціалістів сприяє формуванню висококваліфікованих фахівців, здатних ефективно застосовувати цифрові технології у сфері безпеки. На п’ятому етапі – *запуск спільних пілотних проєктів* – йдеться про реалізацію тестових рішень у співпраці з міжнародними партнерами. Це дозволяє Україні перевірити ефективність нових технологій, таких як системи раннього виявлення загроз, до їхнього масштабного впровадження. Шостий етап – *міжнародна координація та обмін даними* – є критично важливим у сучасному глобальному середовищі.

Україна бере участь у платформах на кшталт MISP (Malware Information Sharing Platform), що сприяє обміну інформацією про загрози з міжнародними партнерами. На сьомому етапі – *оцінка ефективності та вдосконалення* – увага зосереджується на моніторингу результатів реалізованих ініціатив. Це дозволить виявити сильні сторони та недоліки впроваджених технологій, що є основою для подальшого вдосконалення процесів. Таким чином, рис. 3.1 відображає комплексний підхід до інтеграції міжнародного досвіду у процес вдосконалення цифрових технологій у національній безпеці України. Запропонована послідовність етапів забезпечує системність і логіку процесу, що дозволяє досягати стратегічних цілей цифровізації. Такий підхід гарантує, що Україна зможе ефективно реагувати на сучасні виклики та посилювати свою кіберстійкість.

Міжвідомча координація та співпраця є одним із ключових аспектів забезпечення ефективної цифровізації у сфері національної безпеки. Цей процес передбачає взаємодію між різними державними органами, а також залучення приватного сектору, наукових установ і міжнародних партнерів. Його мета полягає у створенні єдиного інтегрованого механізму для впровадження цифрових технологій і протидії сучасним загрозам.

Без ефективної взаємодії між органами державної влади реалізація стратегій цифровізації може стикатися з фрагментацією даних, дублюванням функцій та повільним реагуванням на загрози. Саме тому ключовим завданням міжвідомчої координації є усунення цих бар’єрів та забезпечення синхронізованої діяльності. У сфері національної безпеки це особливо важливо, оскільки кіберзагрози, інформаційні атаки та інші виклики вимагають швидкої та узгодженої відповіді.

В Україні координацію у сфері цифровізації безпекового сектору забезпечує Національний координаційний центр кібербезпеки (НКЦК), що функціонує при Раді національної безпеки і оборони України (РНБО). Центр відіграє провідну роль у створенні єдиної системи кіберзахисту країни [66].

НКЦК координує діяльність державних установ, таких як:

1. *Державна служба спеціального зв'язку та захисту інформації України (ДССЗЗІ)*, яка відповідає за захист інформаційних систем держави;

2. *Міністерство цифрової трансформації*, яке впроваджує цифрові інновації та забезпечує їхнє використання у державному управлінні;

3. *Служба безпеки України (СБУ)*, що займається виявленням та нейтралізацією загроз у сфері кібербезпеки.

Прикладом успішної міжвідомчої координації є спільна діяльність НКЦК і CERT-UA (група реагування на кіберінциденти), які оперативно відбили масовані кібератаки на державні ресурси у 2022 році, забезпечивши відновлення роботи понад 70 урядових вебсайтів.

У сучасних умовах кіберзагрози часто мають транснаціональний характер, що вимагає тісної співпраці з міжнародними партнерами. Україна активно співпрацює з організаціями, такими як НАТО, ЄС, та платформами обміну даними, серед яких MISP (Malware Information Sharing Platform).

Залучення міжнародного досвіду та підтримки дозволяє не лише підвищити технічну спроможність, а й забезпечити інтеграцію в глобальні мережі кібербезпеки. Наприклад, участь України у програмі NATO Cyber Defense Pledge сприяє зміцненню національної безпеки через обмін знаннями, навчання кадрів і отримання технічної допомоги.

Для забезпечення оперативної координації міжвідомчі структури використовують сучасні автоматизовані системи обміну даними. Це дозволяє швидко передавати інформацію про загрози, реагувати на кіберінциденти та забезпечувати інтеграцію між різними структурами.

Одним із таких прикладів є впровадження Національної платформи кіберзахисту, яка об’єднує дані про інциденти з різних джерел, таких як державні установи, приватний сектор і міжнародні партнери.

але, разом з тим, попри досягнення, процес міжвідомчої співпраці стикається з низкою викликів. До них належать:

1. Недостатня автоматизація процесів;

2. Відсутність єдиної платформи для обміну інформацією в реальному

часі;

3. Брак фінансування для впровадження технологічних рішень.

Для подолання цих викликів важливим та перспективним завданням є вдосконалення нормативно-правової бази, розвиток людського капіталу та залучення додаткових ресурсів через міжнародну співпрацю.

Отже, міжвідомча координація та співпраця є основою ефективного впровадження цифрових технологій у сектор національної безпеки. Вона забезпечує узгодженість дій між різними структурами, підвищує оперативність реагування на виклики та сприяє інтеграції України до глобального кіберпростору. Завдяки впровадженню сучасних платформ обміну даними, міжнародній підтримці та узгодженню дій, держава може успішно протидіяти сучасним загрозам і розвивати стійку цифрову екосистему.

Таким чином, стратегічні підходи до цифровізації сектору національної безпеки України повинні враховувати глобальні тенденції, національні особливості та сучасні технологічні можливості. Лише при умові довгострокового планування, інтеграції міжнародного досвіду та забезпечення міжвідомчої співпраці можна досягти ефективної цифрової трансформації. Україна, яка перебуває в умовах зовнішніх і внутрішніх викликів, потребує комплексного підходу до цифровізації для зміцнення своєї національної безпеки.

3.2. Технологічні інновації як інструмент зміцнення національної безпеки

У сучасному світі технологічні інновації стали визначальним фактором у забезпеченні національної безпеки. Постійний розвиток військових технологій, цифрових рішень та засобів кіберзахисту значно змінює характер сучасних загроз та підходи до їх подолання. Країни, що впроваджують новітні технології, здатні ефективніше реагувати на виклики, посилювати

свою обороноздатність та підвищувати стійкість державних інституцій до зовнішніх і внутрішніх загроз.

Для нашої державаи питання технологічних інновацій є особливо актуальним у контексті повномасштабного вторгнення на територію України з боку російської федерації та глобальних кіберзагроз. Збройні сили України, органи безпеки та державне управління стикаються з потребою швидкої адаптації до сучасних умов, що передбачає активне використання таких технологій, як безпілотні літальні апарати, штучний інтелект, кіберзахист і системи ситуаційної обізнаності. Ці інструменти не лише підвищують ефективність оборонних структур, але й забезпечують критичну інформаційну перевагу на полі бою та в інформаційному просторі. Види технологічних інновацій спрямованих на зміцнення національної безпеки України представлено на рис. 3.2.

Рис. 3.2. Види технологічних інновацій спрямованих на зміцнення національної безпеки України

Так, за даними рис. 3.2, де узагальнено представлено напрями та види інноваційних технологій у сфері національної безпеки з метою зміцнення її рівня, є можливість провести аналіз кожного із запропонованих видів:

1. Безпілотні літальні апарати (БПЛА).

Використання БПЛА стало невід'ємною частиною сучасних військових операцій. В Україні організація «Аеророзвідка» займається розробкою та

впровадженням безпілотних систем для розвідки та коригування артилерійського вогню. Це дозволяє зменшити ризики для особового складу та підвищити точність ударів [67].

2. Кібербезпека.

Зростання кіберзагроз вимагає впровадження передових технологій для захисту критичної інфраструктури. Україна розробила та впроваджує «Стратегію кібербезпеки на 2021-2025 роки», яка передбачає розвиток національної системи кіберзахисту та інтеграцію з міжнародними стандартами [66].

3. Штучний інтелект (ШІ).

Впровадження штучного інтелекту у військову сферу дозволяє автоматизувати процеси аналізу даних, прогнозування загроз та прийняття рішень. Українські розробники працюють над створенням систем, що використовують ШІ для обробки розвідувальної інформації та управління безпілотними системами [68].

4. Системи ситуаційної обізнаності.

Розробка та впровадження систем, які забезпечують командирів актуальною інформацією про бойову обстановку, є критично важливими. Україна впроваджує систему «Дельта», яка інтегрує дані з різних джерел для надання повної картини поля бою в режимі реального часу [69].

5. Інноваційні платформи та кластери.

Для стимулювання розробки новітніх технологій у сфері оборони створюються інноваційні платформи. Наприклад, платформа Brave1 об'єднує розробників, інвесторів та військових для спільної роботи над інноваційними проєктами [70].

Таким чином, технологічні інновації відіграють ключову роль у зміцненні національної безпеки України. В умовах сучасних викликів впровадження новітніх технологій стало необхідністю для забезпечення обороноздатності держави. Використання інновацій дозволяє значно підвищити ефективність військових операцій, посилити захист критичної

інфраструктури та забезпечити оперативну обробку інформації для ухвалення стратегічних рішень.

Разом з тим, технологічні інновації є важливим чинником забезпечення національної безпеки, особливо в умовах зростаючих загроз та швидкої еволюції способів ведення війни. Використання безпілотників, штучного інтелекту, кіберзахисту та систем ситуаційної обізнаності дозволяє державам підвищувати свою обороноздатність, ефективно реагувати на виклики та адаптуватися до нових умов.

З метою визначення порівняльних характеристик у напрямі впровадження технологічних інновацій в Україні у порівнянні з Ізраїлем (як однієї з найбільш інноваційних держав у сфері безпеки) та США (лідера у розробці військових і цифрових технологій) складено табл. 3.2.

Таблиця 3.2

Порівняльний аналіз використання основних технологій у сфері національної безпеки в Україні з Ізраїлем та США

Технологія	Україна	Ізраїль	США
1	2	3	4
Безпілотні літальні апарати (БПЛА)	Активно використовуються для розвідки та коригування артилерії (організація «Аеророзвідка»). Виробництво розвивається, але залежить від імпорту комплектуючих.	Один із світових лідерів у виробництві та використанні БПЛА для розвідки, ударних операцій (системи Heron, Hagor).	Масове використання та експорт. Розробляються багатофункціональні системи, такі як MQ-9 Reaper.
Кібербезпека	Розвивається швидко, особливо через актуальність кіберзагроз у війні. Стратегія кібербезпеки 2021–2025.	Світовий лідер у кібербезпеці. Використовуються потужні системи моніторингу CyberArk, Check Point.	Високий рівень автоматизації захисту критичної інфраструктури. Активно працює Агентство з кібербезпеки (CISA).
Штучний інтелект (ШІ)	На початкових етапах. Використовується для аналізу розвідданих та створення систем ситуаційної обізнаності.	Впроваджений у всі сфери національної безпеки (аналітика даних, автономні системи, виявлення загроз).	Використовується у військових програмах, розвідці, прогнозуванні ризиків. Акцент на автономних системах.
Системи ситуаційної обізнаності	Система «Дельта» інтегрує розвіддані, дані з БПЛА та супутників. Впроваджується у військовій сфері.	Широке використання передових систем у реальному часі. Приклад: система Iron Dome інтегрує різні види даних для відбиття ракетних загроз.	Масштабні системи, як-от Distributed Common Ground System (DCGS), для збору даних на стратегічному рівні.

Продовження табл. 3.2

1	2	3	4
Інноваційні платформи	Brave1 об'єднує розробників і військових для створення оборонних технологій.	Державна підтримка стартапів через програми, як-от INCD (Ізраїльський центр інновацій у кібербезпеці).	DARPA фінансує розробку інновацій у сферах штучного інтелекту, робототехніки та захисту інформації.

Отже, за даними табл. 3.2, зроблено висновок, що Україна активно розвиває використання БПЛА у військових операціях, що стало особливо актуальним у контексті війни з росією. Проте, на відміну від Ізраїлю, який має власне масштабне виробництво та експорт цих систем, Україна значною мірою залежить від імпорту комплектуючих. США, з наявністю розвиненої інфраструктури, також є лідером у цьому напрямку, створюючи багатофункціональні системи для глобального використання. В Україні кібербезпека стала критичним напрямком у зв’язку з гібридною війною, але вона ще перебуває на етапі розвитку. Ізраїль є світовим лідером, відомим своїми передовими рішеннями у сфері кіберзахисту, зокрема розробками таких компаній, як CyberArk. У США впроваджені високотехнологічні автоматизовані системи захисту критичної інфраструктури, що координуються через Агентство з кібербезпеки (CISA). Використання штучного інтелекту в Україні ще обмежене, проте спостерігається зростання його ролі у військових та аналітичних системах. Ізраїль та США значно випереджають Україну у цьому напрямку. Наприклад, Ізраїль активно використовує автономні дрони та аналітичні платформи для виявлення загроз, тоді як у США розробляються цілі програми на базі штучного інтелекту для автоматизації військових операцій. Українська система «Дельта» є перспективним проєктом, який довів свою ефективність під час бойових дій, рис. 3.3. Водночас Ізраїль активно використовує інтегровані системи, такі як Iron Dome, для забезпечення точного моніторингу та оперативного реагування. США мають глобальні системи, що забезпечують стратегічний рівень обізнаності через інтеграцію супутникових,

радіоелектронних і розвідувальних даних.

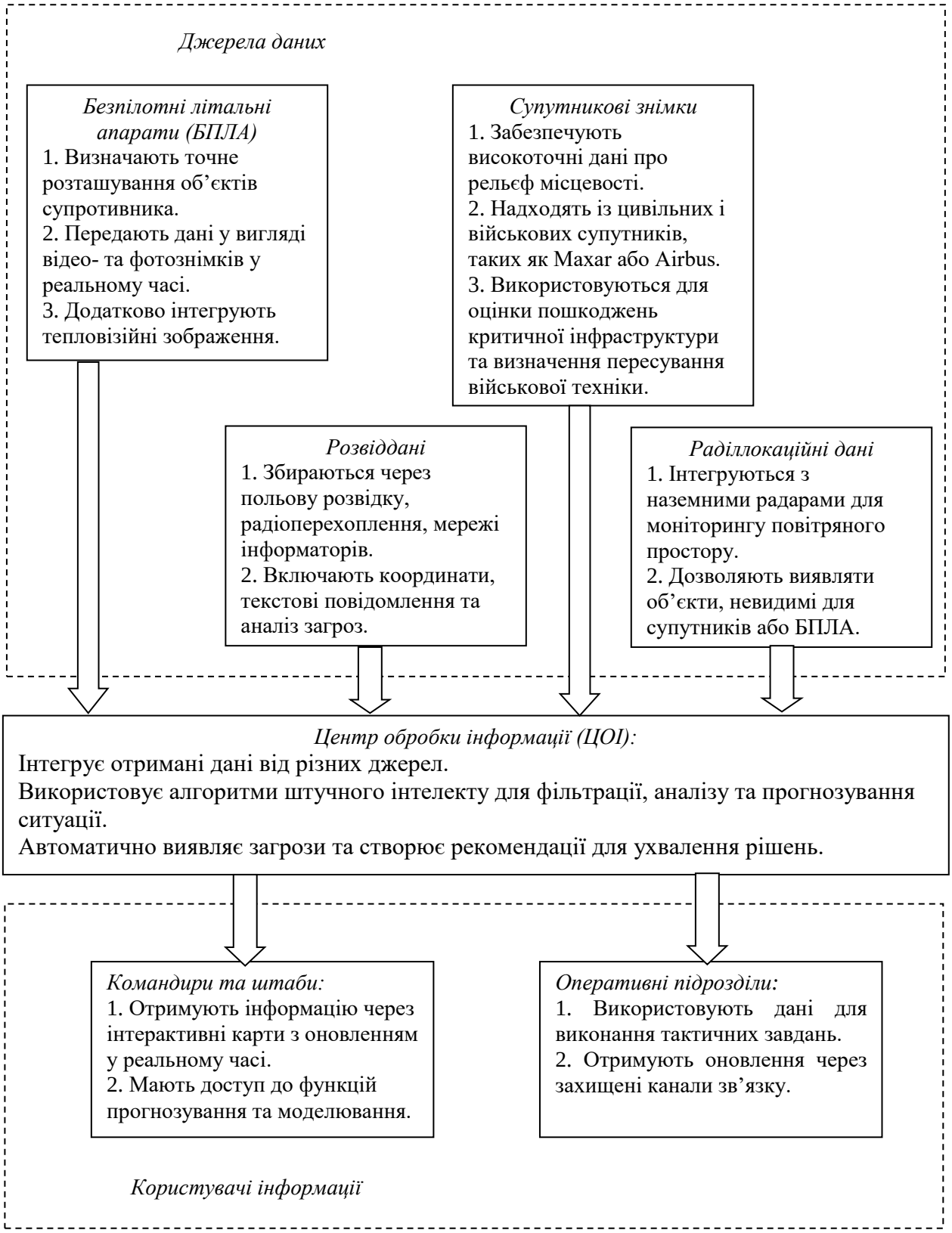

Рис. 3.2. Структура системи ситуаційної обізнаності «Дельта»

Джерело: узагальнено на підставі [69]

Щодо використання інноваційних платформ, в Україні - це Brave1, який є перспективним українським проєктом, який допомагає об’єднати державу, військових та приватний сектор. Водночас Ізраїль має багаторічний досвід створення інноваційних платформ, таких як INCD, які активно залучають інвестиції у сферу кібербезпеки. У США агенція DARPA є провідною платформою для фінансування передових досліджень у військовій сфері.

Отже, Україна, незважаючи на обмежені ресурси, активно розвиває технологічний сектор, інтегруючи передовий міжнародний досвід у власну систему безпеки. Порівняння з Ізраїлем, відомим своїми інноваціями у сфері кібербезпеки та оборонних технологій, та США, які є світовим лідером у військових розробках, дозволяє визначити напрями, в яких Україна може зміцнити свої позиції. Успіх у застосуванні технологічних інновацій значною мірою залежить від їхньої інтеграції в існуючі системи національної безпеки. Для цього потрібні чітко сформульовані стратегії, підтримка держави, міжнародне співробітництво та залучення приватного сектору. Важливим аспектом також є підготовка кваліфікованих кадрів і забезпечення відповідної законодавчої бази.

3.3. Формування кадрового потенціалу для цифрової трансформації

Успішна цифрова трансформація національної безпеки України значною мірою залежить від наявності висококваліфікованих фахівців, здатних впроваджувати та підтримувати новітні технології. Формування такого кадрового потенціалу вимагає системного підходу, що включає розвиток освіти, підвищення кваліфікації та створення сприятливих умов для професійного зростання.

Розвиток цифрових компетенцій починається з *освітніх закладів*. В Україні впроваджуються програми, спрямовані на підготовку спеціалістів у

сфері інформаційних технологій та кібербезпеки. Зокрема, Кабінет Міністрів України схвалив Концепцію розвитку цифрових компетентностей до 2025 року, яка передбачає навчання громадян цифровим навичкам та підвищення конкурентоспроможності на ринку праці [64].

В Україні існує низка освітніх програм, спрямованих на підготовку фахівців у сфері національної безпеки. Ці програми реалізуються як у військових, так і в цивільних закладах вищої освіти.

1. Військові навчальні заклади:

Національний університет оборони України імені Івана Черняховського. Пропонує програми підготовки офіцерів для Збройних Сил України, включаючи спеціальності, пов'язані з національною безпекою та обороною [71].

Національна академія Служби безпеки України. Здійснює підготовку фахівців для Служби безпеки України за спеціальністю «Національна безпека» [72].

Національна академія Державної прикордонної служби України імені Богдана Хмельницького. Готує офіцерів для Державної прикордонної служби України, зокрема за напрямами, пов'язаними з національною безпекою [73].

2. Цивільні навчальні заклади:

Державний університет «Житомирська політехніка». Пропонує освітню програму «Національна безпека (за окремими сферами забезпечення і видами діяльності)», спрямовану на підготовку аналітиків та фахівців з менеджменту національної безпеки [74].

Національний університет «Острозька академія». Реалізує освітньо-професійну програму «Національна безпека (за окремими сферами забезпечення і видами діяльності)» на бакалаврському та магістерському рівнях [75].

Міжрегіональна академія управління персоналом (МАУП) Пропонує спеціальність «Національна безпека», яка готує фахівців для державного та приватного секторів безпеки [76].

Фахівці у сфері національної безпеки повинні володіти широким спектром компетенцій, які відповідають сучасним викликам, таким як кіберзагрози, гібридна війна та цифровізація державних структур.

Узагальнення змісту освітніх програм та дослідження вимог до фахівців у сфері національної безпеки, дозволило виокремити перелік ключових компетенцій та навичок, необхідних для ефективної роботи в цьому напрямі:

1. Технічні компетенції:

- знання у сфері кібербезпеки: розуміння принципів захисту інформаційних систем, виявлення та усунення кіберзагроз;
- робота з великими даними: вміння аналізувати, інтерпретувати та використовувати дані для прийняття рішень;
- використання штучного інтелекту: навички впровадження та роботи з алгоритмами ШІ для прогнозування ризиків і моделювання сценаріїв.
- інтеграція технологій: знання роботи систем ситуаційної обізнаності (наприклад, «Дельта») та розуміння принципів їх функціонування.

2. Стратегічні компетенції:

- планування безпекових заходів: здатність розробляти та реалізовувати стратегії захисту критичної інфраструктури;
- аналіз ризиків: уміння оцінювати загрози та визначати їхній вплив на національну безпеку;
- міжвідомча координація: навички управління проєктами, що включають взаємодію між різними державними органами.

3. Управлінські компетенції:

- лідерство: здатність організовувати роботу команд, приймати рішення в умовах невизначеності та ефективно розподіляти ресурси;
- комунікативні навички: уміння вести переговори, працювати в команді та координувати дії міжвідомчих структур;
- кризовий менеджмент: управління ситуаціями під час надзвичайних подій або атак.

4. Юридичні та етичні знання:

- знання нормативно-правової бази: орієнтація в законодавстві України та міжнародних актах, що регулюють сферу національної безпеки;

- етичні принципи: дотримання норм професійної етики, особливо під час роботи з конфіденційними даними.

5. Навички міждисциплінарної співпраці:

- міжнародна взаємодія: здатність працювати в рамках спільних ініціатив із партнерами з НАТО, ЄС та інших міжнародних організацій.

- розуміння економічних аспектів: знання впливу безпекових питань на економічну стабільність.

Отже, систематизація основних навичок та знань, які необхідних фахівцям для виконання завдань у таких напрямах, як кіберзахист, розвідка, робота з безпілотними літальними апаратами, інтеграція систем ситуаційної обізнаності та міжвідомча координація., - представлена у табл. 3.3. яка акцентує увагу на міждисциплінарному характері діяльності у сфері безпеки, де кожен напрямок має свої унікальні вимоги.

Таблиця 3.3

Вимоги ринку праці до компетенцій фахівців у сфері національної безпеки

Категорія компетенцій	Приклади навичок та знань
Технічні	Кібербезпека, робота з великими даними, використання ШІ, інтеграція систем ситуаційної обізнаності
Стратегічні	Планування заходів, аналіз ризиків, міжвідомча координація
Управлінські	Лідерство, комунікація, кризовий менеджмент
Юридичні та етичні	Знання законодавства, етичні принципи
Міждисциплінарна співпраця	Міжнародна взаємодія, розуміння економічних аспектів

Джерело: власна розробка

Отже, аналіз табл. 3.3 дозволяє окреслити конкретні професійні компетенції, які необхідно розвивати через спеціалізовані освітні програми, практичну підготовку та міжнародну співпрацю. Важливість цього підходу зростає в умовах сучасних викликів, коли національна безпека потребує

оперативних і комплексних рішень.

Сучасна сфера національної безпеки охоплює широкий спектр напрямків, кожен із яких має свої специфічні виклики та потребує особливих професійних навичок. Від кіберзахисту до роботи зі штучним інтелектом, від управління безпілотними системами до координації міжвідомчих дій — кожен напрямок вимагає від фахівців глибоких технічних знань, стратегічного мислення та готовності до роботи в умовах динамічних загроз.

Детальний аналіз джерел інформації щодо необхідних вмінь та навичок, у вузькому розумінні, наявність яких є бажаною у фахівців з національної безпеки України, дозволив сформувати табл. 3.4.

Таблиця 3.4

Вимоги до навичок фахівців

у різних напрямках сфери національної безпеки

Напрямок	Ключові навички
Кіберзахист	Виявлення загроз, реагування на інциденти, криптографія, тестування на проникнення, міжнародне співробітництво
Штучний інтелект (ШІ)	Розробка алгоритмів, обробка природної мови, робота з великими даними, прогнозування загроз, впровадження автономних систем
Безпілотні системи (БПЛА)	Управління БПЛА, технічне обслуговування, обробка даних з БПЛА, інтеграція з іншими системами
Системи ситуаційної обізнаності	Інтеграція даних, аналіз у реальному часі, робота з ГІС, координація дій
Розвідка та аналітика	Аналітичні здібності, радіоелектронна розвідка, OSINT, прогнозування загроз
Міжвідомча координація	Управління інформаційними потоками, кризовий менеджмент, міжнародне співробітництво

Джерело: власна розробка

Таким чином, систематизація ключових вмінь, необхідних для ефективного виконання завдань у різних секторах безпеки, дозволяє зрозуміти, способи інтеграції компетенцій для досягнення загальної мети — зміцнення національної безпеки держави.

Отже, як свідчать дані табл. 3.4, робота у сфері національної безпеки вимагає спеціалізованих навичок залежно від напряму діяльності. Підготовка таких фахівців є важливим кроком у зміцненні обороноздатності України та її здатності ефективно реагувати на сучасні виклики.

Більш грунтовний аналіз стратегічно важливих навичок фахівців у різних напрямках національної безпеки України, дозволив деталізувати вміння та навички по кожному напрямку окремо:

1. Кіберзахист.

Фахівці з кібербезпеки відіграють центральну роль у захисті критичної інфраструктури та інформаційних систем від атак. Вони повинні володіти такими навичками:

- виявлення загроз: уміння працювати із системами моніторингу, такими як SIEM (Security Information and Event Management), для аналізу подій у мережі;
- реагування на інциденти: здатність оперативно локалізувати та нейтралізувати кібератаки, включаючи роботу з CERT (Computer Emergency Response Team);
- криптографія: знання методів шифрування для захисту даних, що передаються в мережі;
- тестування на проникнення (Penetration Testing): навички перевірки систем на вразливості для запобігання майбутнім атакам;
- міжнародне співробітництво: розуміння процедур обміну інформацією про загрози через платформи, як-от MISP (Malware Information Sharing Platform).

2. Штучний інтелект (ШІ).

Штучний інтелект є важливим інструментом у розвідці, прогнозуванні загроз та автоматизації процесів. Для роботи у цій сфері фахівці повинні мати навички у таких сферах:

- розробка алгоритмів: уміння створювати та впроваджувати алгоритми машинного навчання для аналізу великих даних;
- обробка природної мови (NLP): використання технологій для аналізу текстів, що дозволяє автоматично обробляти розвідувальні дані або інформацію зі ЗМІ;
- робота з великими даними: знання інструментів для роботи з

великими обсягами інформації (Big Data), таких як Hadoop або Spark;

- автономні системи: здатність інтегрувати штучного інтелекту у робототехніку, зокрема безпілотні літальні апарати;
- прогнозування загроз: використання штучного інтелекту для моделювання та передбачення потенційних ризиків.

3. Безпілотні системи (БПЛА).

У сфері національної безпеки безпілотні системи застосовуються для розвідки, спостереження та ударних операцій. Необхідні навички:

- управління БПЛА: знання принципів навігації та пілотування безпілотних апаратів;
- технічне обслуговування: вміння проводити діагностику та ремонт апаратури;
- обробка даних з БПЛА: здатність аналізувати фото- та відеоматеріали, отримані під час польотів;
- інтеграція з іншими системами: синхронізація даних із супутниковими системами або наземними станціями.

4. Системи ситуаційної обізнаності.

Фахівці, які працюють із системами ситуаційної обізнаності, повинні забезпечувати комплексне розуміння бойової чи кризової обстановки. Навички включають:

- інтеграція даних: вміння об’єднувати інформацію з різних джерел (розвідка, БПЛА, супутники) у єдину систему;
- аналіз у реальному часі: здатність швидко оцінювати ситуацію та передавати рекомендації командуванню;
- робота з геоінформаційними системами (ГІС): знання платформ, наприклад ArcGIS, для створення карт і моделей місцевості;
- координація дій: забезпечення узгодженості між різними підрозділами на основі даних системи.

5. Розвідка та аналітика.

Розвідка є важливою складовою національної безпеки. Необхідні

навички для фахівців у цій сфері:

- аналітичні здібності: уміння обробляти великі обсяги розвідувальних даних для виявлення загроз;
- радіоелектронна розвідка: здатність перехоплювати та аналізувати сигнали з метою отримання інформації про дії супротивника;
- розвідка у відкритих джерелах (OSINT): використання інформації з відкритих джерел, таких як соціальні мережі, медіа тощо;
- прогнозування загроз: моделювання сценаріїв на основі отриманих даних.

6. Міжвідомча координація.

Фахівці, які займаються координацією дій між різними державними структурами, мають володіти такими навичками:

- управління інформаційними потоками: забезпечення чіткої передачі даних між відомствами;
- кризовий менеджмент: здатність організовувати роботу команд у надзвичайних ситуаціях;
- міжнародне співробітництво: вміння працювати в межах спільних операцій з міжнародними партнерами (НАТО, ЄС).

Також важливим завданням при формуванні кадрового потенціалу для цифрової трансформації є забезпечення *підвищення кваліфікації та безперервного навчання.* Для діючих фахівців важливо забезпечити можливості безперервного навчання та підвищення кваліфікації. Міністерство цифрової трансформації України активно розвиває платформу «Дія.Освіта», яка пропонує онлайн-курси з різних аспектів цифрових технологій. Це дозволяє спеціалістам оновлювати свої знання відповідно до сучасних вимог.

Інтеграція міжнародного досвіду є ключовою для підготовки кадрів. Україна співпрацює з міжнародними організаціями та країнами-партнерами для обміну знаннями та практиками у сфері цифрової трансформації. Наприклад, участь у програмі «Цифрова Європа» сприяє впровадженню

європейських стандартів та підходів у підготовці фахівців

Для залучення та утримання талановитих спеціалістів необхідно створювати умови, що сприяють їхньому професійному розвитку. Це включає конкурентоспроможну оплату праці, можливості кар'єрного зростання та участь у інноваційних проєктах. Важливим є також розвиток інноваційних платформ, таких як Brave1, які об'єднують розробників, військових та інвесторів для створення новітніх оборонних технологій

Формування кадрового потенціалу неможливе без розвитку загальної цифрової культури в суспільстві. Це передбачає підвищення обізнаності про важливість цифрових технологій, популяризацію IT-спеціальностей та стимулювання інтересу до науки та техніки серед молоді. Важливу роль у цьому відіграють освітні ініціативи та державні програми, спрямовані на розвиток цифрових навичок у населення.

Отже, формування кадрового потенціалу для цифрової трансформації національної безпеки України є багатогранним процесом, що вимагає скоординованих зусиль держави, освітніх закладів та приватного сектору. Інвестиції в освіту, підвищення кваліфікації, міжнародну співпрацю та розвиток цифрової культури є ключовими елементами цього процесу, що забезпечать успішну інтеграцію новітніх технологій у сферу національної безпеки.

Таким чином, результати проведеного детального аналізу стратегічних підходів до цифровізації, технологічних інновацій та формування кадрового потенціалу, утворюють основу для зміцнення національної безпеки України. Виокремлені ключові етапи планування цифровізації, які охоплюють процеси від формування стратегічного бачення до впровадження пілотних проєктів та оцінки результатів, - дозволяє забезпечити цілісність та послідовність у впровадженні цифрових технологій у сферу безпеки.

Доведено, що впровадження технічних інновацій є основою зміцнення національної безпеки України. Серед найбільш важливих технологічних інновацій виділено необхідність застосування наступних: використання

безпілотних літальних апаратів; штучного інтелекту; систем ситуаційної обізнаності та інноваційних платформ. Проведене порівняння з провідними країнами, такими як США та Ізраїль, демонструє перспективи і напрями розвитку України у впровадженні інновацій, що може стати основою адаптації найкращих міжнародних практик до національних реалій, що зміцнює обороноздатність та кіберстійкість держави.

Разом з тим, якісне та раціональне використання технологічних інновацій та розбудови цифровізації, зокрема у сфері національної безпеки, є неможливим без наявності у фахівців стратегічно важливих вмінь та навичок. Саме тому у роботі окреслено важливість кадрового потенціалу як рушійної сили цифрової трансформації. Підготовка фахівців у сфері національної безпеки вимагає системного підходу, який включає розвиток технічних, стратегічних, управлінських та міждисциплінарних навичок. Підвищення кваліфікації, міжнародна співпраця та створення сприятливих умов для професійного зростання є ключовими чинниками цього процесу.

Таким чином, розглянуті у розділі аспекти демонструють, що ефективна цифровізація сектору національної безпеки можлива лише за умов інтеграції технологічних рішень, стратегічного планування та підготовки кваліфікованих кадрів. Цей підхід дозволить Україні ефективно протидіяти сучасним загрозам та створювати стійку систему безпеки, яка відповідає викликам XXI століття.

ВИСНОВКИ

У магістерській кваліфікаційній роботі досліджено особливості впровадження цифрових технологій у сферу публічного управління сектором національної безпеки України, що є актуальним у сучасних умовах гібридної війни, зростання кіберзагроз та необхідності посилення інформаційної безпеки.

Розкрито сутність цифрових технологій як ключового інструменту модернізації управлінських процесів. На основі узагальнення підходів науковців встановлено, що їх застосування підвищує ефективність, прозорість і оперативність публічного управління. Визначено класифікаційні ознаки цифрових технологій, які використовуються у сфері публічного управління національною безпекою**.** Доведено, що цифровізація є фундаментом для реалізації стратегії забезпечення національної безпеки.

Встановлено, що удосконалення системи публічного управління у сфері національної безпеки України слід базувати на аналізі нормативно-правових засад та актуальних викликів цифровізації. Основною передумовою успішного розвитку є цілісна нормативна база, яка визначає ключові напрями діяльності. Зокрема, такі документи, як Закон України «Про основні засади забезпечення кібербезпеки України» та «Стратегія кібербезпеки України на 2021-2025 роки», задають правову засади регулювання, захисту критичної інфраструктури, а також координації між органами публічного управління.

Ключовими елементами управління національною безпекою є чіткий розподіл повноважень між державними органами, координація їхніх дій та створення спеціалізованих механізмів захисту. Важливою складовою також є інтеграція міжнародного досвіду, який сприяє підвищенню ефективності управління, розробці та впровадженню сучасних стандартів кібербезпеки.

Разом з тим, у дослідженні наголошується на необхідності приділення уваги захисту критичної інформаційної інфраструктури, яка відіграє стратегічну роль у забезпеченні стабільності держави. Аналіз чинних

нормативно-правових актів підтвердив наявність необхідності їх модернізації для усунення розбіжностей та врахування технологічних змін. Крім того, впровадження практик міжнародної взаємодії сприяє покращенню готовності України до протидії сучасним загрозам.

Проведений аналіз сучасного стану використання цифрових технологій у секторі національної безпеки України засвідчив, що їх інтеграція сприяє вдосконаленню міжвідомчої взаємодії, оперативному реагуванню на загрози та управлінню критичною інформаційною інфраструктурою. На основі порівняння національного та міжнародного досвіду виокремлено прогресивні практики цифровізації (включаючи інструменти кібербезпеки, штучного інтелекту, блокчейн-технологій), які можуть бути адаптовані до українських реалій. Такі рішення дозволяють забезпечувати високий рівень координації між державними органами в умовах надзвичайних ситуацій.

Результати аналізу основних показників діяльності Служби безпеки України за період с початку повномасштабної війни (станом на березень 2024 р.) свідчать, що кількість розпочатих кримінальних проваджень та повідомлених підозр значно перевищує кількість обвинувальних вироків. Це свідчить про активну роботу СБУ на етапі викриття злочинів і збору доказів, але також демонструє, що частина проваджень ще перебуває на стадії судового розгляду. Загалом розпочато 3088 проваджень, з яких більшість стосується державної зради (2535 випадків). Це підкреслює стратегічну важливість боротьби з агентами ворога в умовах війни. Підозри повідомлено 2533 особам, що є високим показником залучення підозрюваних до відповідальності. Водночас обвинувальних вироків — 499. Найбільшу частку з них (384 вироки) становлять справи про державну зраду. Відзначено високу активність СБУ у боротьбі з колабораційною діяльністю. Кількість обвинувальних вироків (915) у порівнянні з кількістю проваджень (7230) підкреслює необхідність пришвидшення судових процесів, щоб більша кількість справ доходила до вироків.

Колабораційна діяльність (ст. 111-1, 111-2) є найбільш поширеною

категорією, що свідчить про значну загрозу такого типу злочинів для державної безпеки.

Цифрові технології стали основою сучасної війни, значно підвищуючи ефективність, точність і швидкість дій військових сил. У військовій сфері України цифрові технології використовуються у сферах розвідки, управління, бойових операцій, логістики та кібербезпеки. Їх впровадження дозволяє українським військовим адаптуватися до складних умов сучасної війни, особливо в умовах протистояння агресії з боку росії.

Аналіз міжнародного досвіду використання цифрових технологій у національній безпеці дозволив виокремити найбільш успішні практики. Так, в США використовують штучний інтелект та великі дані для виявлення терористичних загроз, аналізу поведінкових моделей та захисту кіберпростору. Кіберкомандування США активно впроваджує технології для моніторингу кіберзагроз та швидкого реагування на них. Ізраїль є лідером у сфері кібербезпеки. Завдяки інноваційним цифровим рішенням, країна забезпечує захист своїх державних систем від кібератак. Однією з ключових технологій є аналітика великих даних, яка дозволяє своєчасно ідентифікувати загрози.

Аналіз вітчизняного та міжнародного досвіду використання цифрових технологій у сфері національної безпеки свідчить, що Україна демонструє значний прогрес у розвитку кібербезпеки, інтеграції інноваційних рішень, таких як CERT-UA, та впровадженні автоматизованих систем управління. Водночас, міжнародні практики — зокрема, США, Європейського Союзу, Ізраїлю та Китаю — дають змогу краще адаптувати національні стратегії до сучасних викликів.

Використання цифрових технологій у військовій сфері, розвідці та логістиці дозволяє Україні успішно протистояти гібридним загрозам і зміцнювати стратегічну стійкість. Розвиток безпілотних літальних апаратів, штучного інтелекту та геоінформаційних систем став визначальним чинником у досягненні переваги над ворогом.

На основі дослідження розроблено рекомендації щодо стратегічного вдосконалення цифровізації в секторі національної безпеки. Зокрема, запропоновано створення національної системи раннього виявлення загроз, яка базуватиметься на сучасних алгоритмах штучного інтелекту та геоінформаційних технологіях. Акцент зроблено на розвитку кадрового потенціалу, підвищенні цифрової грамотності працівників сектору, гармонізації нормативно-правової бази з міжнародними стандартами та активізації міжнародної співпраці в сфері кібербезпеки. Запропоновані підходи враховують міжнародний досвід та відповідають вимогам сучасного безпекового середовища.

Доведено, що впровадження технічних інновацій є основою зміцнення національної безпеки України. Серед найбільш важливих технологічних інновацій виділено необхідність застосування наступних: використання безпілотних літальних апаратів; штучного інтелекту; систем ситуаційної обізнаності та інноваційних платформ. Проведене порівняння з провідними країнами, такими як США та Ізраїль, демонструє перспективи і напрями розвитку України у впровадженні інновацій, що може стати основою адаптації найкращих міжнародних практик до національних реалій, що зміцнює обороноздатність та кіберстійкість держави.

Таким чином, у роботі повністю розкрито мету кваліфікаційної роботи – досліджено стратегічні підходи, сучасні викликі і перспективи цифровізації публічного управління в секторі національної безпеки України.

Отримані результати мають практичне значення для подальшого розвитку цифрових технологій у державному управлінні, підвищення рівня кібербезпеки та інтеграції України у глобальний цифровий простір.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Биков В. Ю. Цифрові технології в освітньому середовищі: основи, концепції та практика [Електронний ресурс]. – Режим доступу: https://lib.iitta.gov.ua/id/eprint/720330/1/3526-%D0%A2%D0%B5%D0%BA%D1%81%D1%82%20%D1%81%D1%82%D0%B0%D1%82%D1%82%D1%96-16187-1-10-20200430.pdf.

2. Жалдак М. І. Цифрові технології у професійній діяльності: навчальний посібник / М. І. Жалдак. – Київ: НАН України, 2021. – 123 с.

3. Спірін О. М. Інтеграція цифрових технологій у навчальний процес / О. М. Спірін // Науковий вісник. – 2020. – № 4. – С. 35-41.

4. Фамілярська Л. Цифрові інструменти для формування сучасного освітнього середовища [Електронний ресурс] / Л. Фамілярська // Вісник Кременчуцького національного університету. – 2022. – Режим доступу: https://visnikkrnu.kdu.edu.ua/statti/2022_1_1.pdf.

5. Васильєва Т. А. Інноваційна освітня діяльність в умовах цифровізації [Електронний ресурс] / Т. А. Васильєва // Науковий журнал СумДУ. – 2022. – Режим доступу: https://essuir.sumdu.edu.ua/bitstream/123456789/89990/1/Vasylieva_education.pdf.

6. Литвинова С. Впровадження цифрових технологій в освіті [Електронний ресурс] / С. Литвинова // Освіта і наука. – 2021. – № 2. – Режим доступу: https://essuir.sumdu.edu.ua/bitstream/123456789/89990/1/Vasylieva_education.pdf.

7. Гончарова О. Цифрові інструменти в організації навчального процесу [Електронний ресурс] / О. Гончарова // Матеріали конференції. – 2021. – Режим доступу: https://lib.iitta.gov.ua/id/eprint/734946/1/%D0%93%D0%BE%D0%BD%D1%87%D0%B0%D1%80%D0%BE%D0%B2%D0%B0_%D1%82%D0%B5%D0%B7%D0%B8.pdf.

8. Сухонос В. Цифрові технології як засіб інтенсифікації освітнього процесу [Електронний ресурс] / В. Сухонос // Український педагогічний журнал. – 2021. – № 4. – Режим доступу: https://lib.iitta.gov.ua/id/eprint/728620/1/UPJ_2021_04_web%20%281%29.pdf.

9. Мельник О. Сучасні підходи до інтеграції цифрових технологій у

навчання [Електронний ресурс] / О. Мельник // Вісник Полтавського педагогічного університету. – 2021. – Режим доступу: https://dspace.pnpu.edu.ua/bitstream/123456789/22317/1/12.pdf.

10. Гевко І. В. Використання цифрових технологій у професійному розвитку педагогів [Електронний ресурс] / І. В. Гевко // Науковий часопис НПУ ім. М. П. Драгоманова. – 2019. – № 145. – Режим доступу: https://nz.npu.edu.ua/article/view/NZ-npu-145.2019.04.

11. Берназюк О. О. Цифрові технології у сфері публічного управління: визначення основних понять [Електронний ресурс] / О. О. Берназюк // Науковий вісник Ужгородського національного університету. – 2017. – Режим доступу: https://dspace.uzhnu.edu.ua/jspui/bitstream/lib/34345/1/%D0%A6%D0%98%D0%A4%D0%A0%D0%9E%D0%92%D0%86%20%D0%A2%D0%95%D0%A5%D0%9D%D0%9E%D0%9B%D0%9E%D0%93%D0%86%D0%87%20%D0%A3%20%D0%A1%D0%A4%D0%95%D0%A0%D0%86%20%D0%9F%D0%A3%D0%91%D0%9B%D0%86%D0%A7%D0%9D%D0%9E%D0%93%D0%9E%20%D0%A3%D0%9F%D0%A0%D0%90%D0%92%D0%9B%D0%86%D0%9D%D0%9D%D0%AF.pdf.

12. Pereira G. V., Parycek P., Falco E., Kleinhans R. Smart governance in the context of smart cities: A literature review // Information Polity. – 2018. – Режим доступу: https://doi.org/10.3233/IP-170067.

13. Dunleavy P., Margetts H., Tinkler J., Bastow S. Digital Era Governance: IT Corporations, the State, and E-Government. – Oxford : Oxford University Press, 2006. – 320 p.

14. Мохова Ю. Л. Державні механізми розвитку електронного урядування в умовах цифрових трансформацій України : дис. ... докт. наук з держ. упр. : 25.00.02 / Мохова Юлія Леонідівна ; Чорноморський національний університет імені Петра Могили. – Миколаїв, 2021. – 490 с.

15. Kohler-Koch B. Interdependent European Governance. Linking EU and National Governance. – Oxford : Oxford University Press, 2003. – P. 10–12.

16. Antiroikko A. V. Introduction to Democratic E-Governance // E-Transformation in Governance: New Directions in Government and Politics. – Idea Group Publishing, 2004. – P. 22–51.

17. Yong J. S. L. E-Government in Asia: Enabling Public Service Innovation in the 21st Century. – Singapore : Times Editions, 2003.

18. Демкова М. С., Фігель М. В. Доступ до інформації та електронне урядування. – Київ : Факт, 2004. – 336 с.

19. Почепцов Г. Г., Чукут С. А. Інформаційна політика : навч. посіб. – Київ : Знання, 2006. – 663 с.

20. Спасібов Д. Електронне урядування в системі сучасних концепцій публічного управління // Теорія та практика державного управління. – 2018. – № 2 (61). – Режим доступу: http://www.kbuapa.kharkov.ua/e-book/tpdu/2018-2/index.html.

21. Чукут С. А. Тенденції та проблеми впровадження електронного урядування в Україні [Електронний ресурс]. – Режим доступу: https://ktpu.kpi.ua/wp-content/uploads/2016/02/Tezi_Tendentsiyi-ta-problemi-vprovadzhennya-elektronnogo-uryaduvannya.pdf.

22. Коновал В. О. Методологічні засади електронного урядування на місцевому рівні: поняття, принципи, моделі та передумови // Теорія та практика державного управління : зб. наук. пр. Харківського регіонального інституту державного управління. – Харків : ХРІДУ НАДУ, 2016. – Вип. 2 (53). – С. 65–72.

23. Organisation for Economic Co-operation and Development [Електронний ресурс]. – Режим доступу: https://www.oecd.org/.

24. Камінська Т. Зарубіжний досвід упровадження електронного врядування / Т. Камінська, А. Камінський, М. Пасічнік, С. Чукут. – Київ : НАДУ, 2008. – 200 с.

25. Стратегія розвитку інформаційного суспільства в Україні : розпорядження Кабінету Міністрів України від 15 травня 2013 р. № 386-р [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/386-2013-%D1%80#Text.

26. Pereira G. V., Parycek P., Falco E., Kleinhans R. Smart governance in the context of smart cities: A literature review // Information Polity. – 2018. – DOI: https://doi.org/10.3233/IP-170067.

27. Зелена книга з електронного урядування в Україні [Електронний ресурс]. – Режим доступу: http://e-

zakon.org/greenbook/documents/%D0%97%D0%95%D0%9B%D0%95%D0%9D%D0%90_%D0%9A%D0%9D%D0%98%D0%93%D0%90_14.11.2014.pdf.

28. Ciancarini P., Giancarlo R., Grimaudo G. Digital Transformation in the Public Administrations: a Guided Tour For Computer Scientists // arXiv preprint arXiv:2305.05551. – 2023. – Режим доступу: https://arxiv.org/abs/2305.05551.

29. Про інформацію : Закон України від 2 жовтня 1992 р. № 2657-XII [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/card/74/98-%D0%B2%D1%80.

30. Про основні засади забезпечення кібербезпеки України : Закон України від 5 жовтня 2017 р. № 2163-VIII [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/card/2163-19.

31. Про національну безпеку України : Закон України від 21 червня 2018 р. № 2469-VIII [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/card/2469-19.

32. Про оборону України : Закон України від 6 грудня 1991 р. № 1932-XII [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/card/1932-12.

33. Про Державну службу спеціального зв'язку та захисту інформації України : Закон України від 23 лютого 2006 р. № 3475-IV [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/card/3475-15.

34. Стратегія кібербезпеки України : затверджена Указом Президента України від 26 серпня 2021 р. № 447/2021 [Електронний ресурс]. – Режим доступу: https://cip.gov.ua/ua/news/strategiya-kiberbezpeki-ukrayini.

35. Стратегія інформаційної безпеки України : затверджена Указом Президента України від 28 грудня 2021 р. № 685/2021 [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/card/n0080525-21.

36. Доктрина інформаційної безпеки України : затверджена Указом Президента України від 25 лютого 2017 р. № 47/2017 [Електронний ресурс]. – Режим доступу: https://www.president.gov.ua/documents/472017-21374.

37. Про основні засади забезпечення кібербезпеки України : Закон України від 5 жовтня 2017 р. № 2163-VIII [Електронний ресурс]. – Режим

доступу: https://zakon.rada.gov.ua/laws/card/2163-19.

38. Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах : Постанова Кабінету Міністрів України від 29 березня 2006 р. № 373 [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/card/373-2006-%D0%BF.

39. Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури : Постанова Кабінету Міністрів України від 19 червня 2019 р. № 518 [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/card/518-2019-%D0%BF.

40. Міжнародна фундація виборчих систем (IFES). Правова база української кібербезпеки: загальний огляд і аналіз [Електронний ресурс]. – 2019. – Режим доступу: https://ifes.org.

41. Закон України «Про національну безпеку України» : закон № 2469-VIII від 21 червня 2018 р. URL: https://zakon.rada.gov.ua/laws/card/2469-19

42. Хоміч Ю. Г. Формування та реалізація публічноуправлінської діяльності в системі правоохоронних органів: теоретико-методологічні засади : дис. ... доктора філософії : 281 / Юрій Григорович Хоміч ; Навч.-наук. ін-т держ. упр. Нац. техн. ун-ту «Дніпровська політехніка». Дніпро, 2022. 239 с.

43. Про Службу безпеки України : Закон України від 25 березня 1992 р. № 2229-XII [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/card/2229-12.

44. Результати СБУ за час повномасштабного вторгнення РФ (станом на березень 2024 року) [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/card/2229-12

45. Державний центр кіберзахисту та протидії кіберзагрозам CERT-UA [Електронний ресурс]. – Режим доступу: https://cert.gov.ua/

46. Армія кібервоїнів: міжнародно-правовий досвід у сфері боротьби з кіберзлочинністю [Електронний ресурс] // Mind.ua. – Режим доступу: https://mind.ua/openmind/20270195-armiya-kibervoyiniv-mizhnarodno-pravovij-dosvid-u-sferi-borotbi-z-kiberzlochinnistyu

47. Реалізація правових механізмів забезпечення кібербезпеки України [Електронний ресурс] // Наукові праці. Серія: Право. – Режим доступу: https://periodicals.karazin.ua/law/article/view/15648.

48. Войціховський А. В. Інформаційна безпека як складова системи національної безпеки (міжнародний і зарубіжний досвід) [Електронний ресурс] // Вісник Харківського національного університету імені В. Н. Каразіна. Серія «Право». – 2020. – № 29. – С. 281–288. – Режим доступу: https://doi.org/10.26565/2075-1834-2020-29-38

49. Пугачов О. І. Зарубіжний досвід забезпечення інформаційної безпеки держави [Електронний ресурс] // Проблеми сучасних трансформацій. Серія: право, публічне управління та адміністрування. – 2024. – № 13. – Режим доступу: https://doi.org/10.54929/2786-5746-2024-13-02-07

50. US tech giants implicated in NSA data sharing [Електронний ресурс] // The Guardian. – Режим доступу: https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data

51. Cybereason [Електронний ресурс]. – Режим доступу: https://www.cybereason.com

52. European Commission strengthens cybersecurity framework [Електронний ресурс] // European Commission Press Corner. – Режим доступу: https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1239

53. Microsoft Exchange hack: Company blames China for cyberattack [Електронний ресурс] // BBC News. – Режим доступу: https://www.bbc.com/news/technology-56372188

54. National Cyber Security Centre (NCSC) [Електронний ресурс]. – Режим доступу: https://www.ncsc.gov.uk/

55. Федеральне відомство з інформаційної безпеки (BSI) [Електронний ресурс]. – Режим доступу: https://www.bsi.bund.de/

56. Агентство національної безпеки інформаційних систем (ANSSI) [Електронний ресурс]. – Режим доступу: https://www.ssi.gouv.fr/

57. Корейське агентство з питань інтернету та безпеки (KISA) [Електронний ресурс]. – Режим доступу: https://www.kisa.or.kr/eng/main.jsp

58. Департамент внутрішніх справ Австралії [Електронний ресурс]. – Режим доступу: https://www.homeaffairs.gov.au/about-us/our-portfolios/cyber-security/strategy

59. Центр кібербезпеки Канади (Canadian Centre for Cyber Security) [Електронний ресурс]. – Режим доступу: https://www.cyber.gc.ca/

60. Стоколос О. Є. Цифрові технології як інструмент забезпечення національної безпеки: міжнародний досвід і перспективи для України // Матеріали VIII Міжнародної науково-практичної конференції здобувачів вищої освіти та молодих учених «Студенти та молодь – для майбутнього країни» (14-15 листопада 2024 р., м. Бахмут-Харків). URL: https://www.nnppi.in.ua/index.php/abit/2-uncategorised/270-naukovi-konferentsiyi

61. Проєкт USAID «Кібербезпека критично важливої інфраструктури України». Cyber Digest. Огляд подій у сфері кібербезпеки, липень 2023 [Електронний ресурс]. – Режим доступу: https://www.cyberdigest-ua.org

62. Володимир Зеленський підтримує стратегію цифрової трансформації [Електронний ресурс] // Офіційне інтернет-представництво Президента України. – Режим доступу: https://www.president.gov.ua/news/volodimir-zelenskij-pidtrimuye-strategiyu-cifrovoyi-transfor-66605

63. Про схвалення Концепції розвитку цифрових компетентностей та затвердження плану заходів з її реалізації [Електронний ресурс] // Кабінет Міністрів України. – Режим доступу: https://www.kmu.gov.ua/npas/pro-shvalennya-koncepciyi-rozvitku-cifrovih-kompetentnostej-ta-zatverdzhennya-planu-zahodiv-z-yiyi-realizaciyi-167-030321

64. Кабмін схвалив Концепцію розвитку цифрових компетентностей до 2025 року [Електронний ресурс] // Міністерство цифрової трансформації України. – Режим доступу: https://thedigital.gov.ua/news/kabmin-skhvaliv-kontseptsiyu-rozvitku-tsifrovikh-kompetentnostey-do-2025-roku

65. Національна онлайн-платформа з цифрової грамотності «Дія.Освіта» [Електронний ресурс]. – Режим доступу: https://osvita.diia.gov.ua/

66. Рада національної безпеки і оборони України [Електронний ресурс]. – Режим доступу: https://www.rnbo.gov.ua/

67. Аеророзвідка [Електронний ресурс]. – Режим доступу: https://aerorozvidka.ngo/

68. Огляд цифрової трансформації економіки України [Електронний ресурс] // Національний інститут стратегічних досліджень. – Режим доступу: https://niss.gov.ua/news/komentari-ekspertiv/ohlyad-tsyfrovoyi-transformatsiyi-ekonomiky-ukrayiny

69. Що таке система «Дельта» і як вона задає тренди [Електронний ресурс] // Міністерство оборони України. – Режим доступу: https://mod.gov.ua/news/shho-take-sistema-delta-i-yak-vona-zadae-trendi

70. Ukraine launches Brave1 tech cluster to boost military capability [Електронний ресурс] // C4ISRNET. – Режим доступу: https://www.c4isrnet.com/unmanned/2023/04/26/ukraine-launches-brave1-tech-cluster-to-boost-military-capability

71. Національний університет оборони України імені Івана Черняховського [Електронний ресурс]. – Режим доступу: https://nuou.org.ua/

72. Національна академія Служби безпеки України [Електронний ресурс]. – Режим доступу: https://www.nasbu.edu.ua/

73. Національна академія Державної прикордонної служби України імені Богдана Хмельницького [Електронний ресурс]. – Режим доступу: https://nadpsu.edu.ua/

74. Житомирська політехніка [Електронний ресурс]. – Режим доступу: https://ztu.edu.ua/

75. Національний університет «Острозька академія» [Електронний ресурс]. – Режим доступу: https://www.oa.edu.ua/

76. Міжрегіональна Академія управління персоналом (МАУП) [Електронний ресурс]. – Режим доступу: https://maup.com.ua/